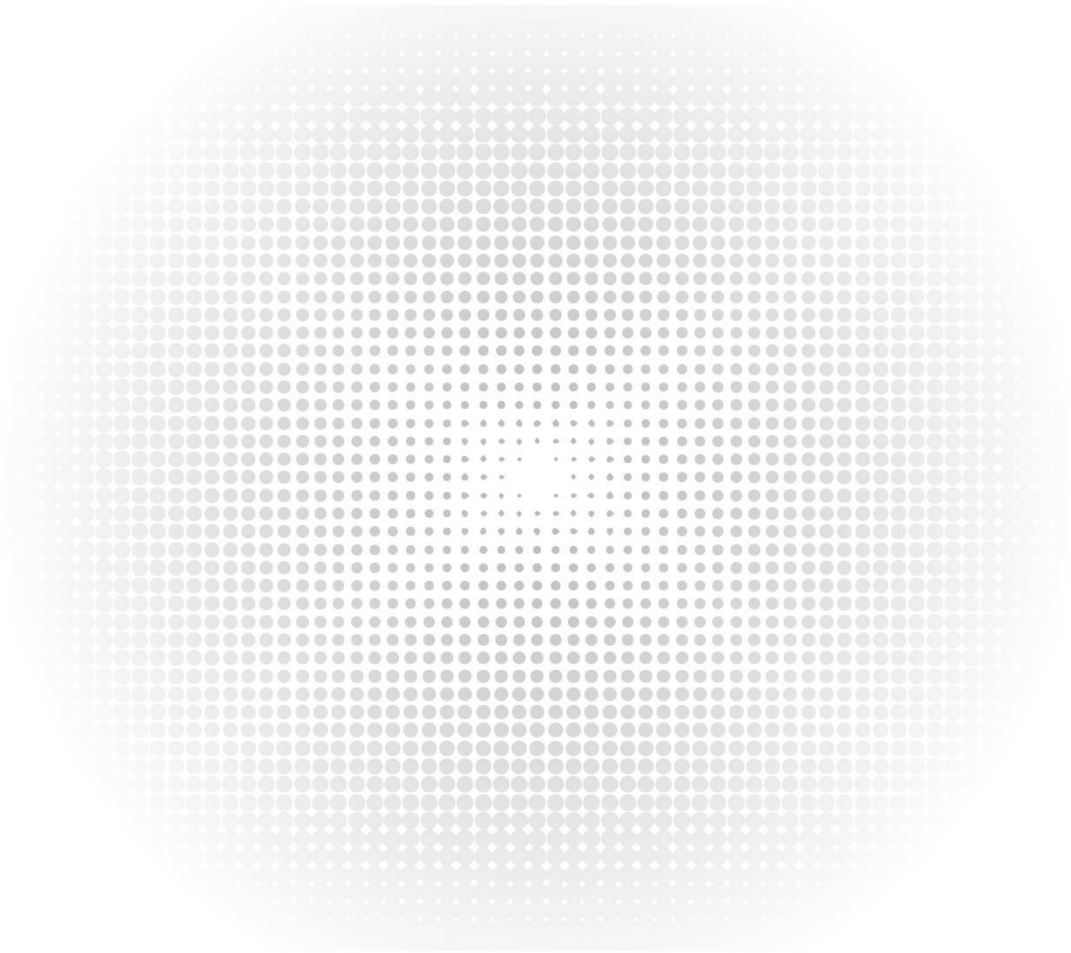
S5300-12S Switch Configuration Guide

Models: S5300-12S



CONFIGURATION GUIDE

Contents

Chapter 1 Configuration Preparation 1

1.1 Port Number of the Switch 1

1.2 Preparation Before Switch Startup 1

1.3 Acquiring Help 1

1.4 Command Modes 2

1.5 Canceling a Command 3

1.6 Saving Configuration 3

Chapter 2 System Management Configuration 4

2.1 File Management Configuration 4

2.1.1 Managing the file system 4

2.1.2 Commands for the file system 4

2.1.3 Starting up from a file manually 4

2.1.4 Updating software 5

2.1.5 Updating configuration 5

2.1.6 Using ftp to perform the update of software and configuration 6

2.2 Basic System Management Configuration 7

2.2.1 Configuring Ethernet IP address 7

2.2.2 Configuring default route 7

2.2.3 Using ping to test network connection state 8

Chapter 3 Terminal Configuration 9

3.1 VTY Configuration Introduction 9

3.2 Configuration Task 9

3.2.1 Relationship between line and interface 9

3.3 Monitor and Maintenance 9

3.4 VTY Configuration Example 9

CHAPTER 4 SSH Configuration Commands 10

4.1 Introduction 10

4.1.1 SSH server 10

4.1.2 SSH client 10

4.1.3 Function 10

4.2 Configuration Tasks 10

4.2.1 Configuring the authentication method list....10
4.2.2 Configuring the access control list....10
4.2.3 Configuring the authentication timeout value....10
4.2.4 Configuring the times of authentication retrying....11
4.2.5 Configuring the login silence period....11
4.2.6 Configuring ssh server Version....11
4.2.7 Configuring encryption algorithms for ssh server....11
4.2.8 Configuring exchange algorithms for ssh server....12
4.2.9 Configuring message authentication code (MAC) algorithms for ssh server....12
4.2.10 Enabling sftp....12
4.2.11 Enabling sshd....12
4.2.12 Enabling SSH server....13
4.3 SSH server Configuration Example....13
4.3.1 Access control list....13
4.3.2 Global configuration....13
Chapter 5 Network Management Configuration....14
5.1 Configuring SNMP....14
5.1.1 Introduction....14
5.1.2 SNMP Configuration Tasks....15
5.1.3 Configuration Example....22
5.2 RMON Configuration....22
5.2.1 RMON Configuration Task....22
Chapter 6 AAA Configuration....26
6.1 AAA Overview....26
6.1.1 AAA Security Service....26
6.1.2 Benefits of Using AAA....27
6.1.3 AAA Principles....27
6.1.4 AAA Method List....27
6.1.5 AAA Configuration Process....28
6.2 Authentication Configuration....28
6.2.1 AAA Authentication Configuration Task List....28
6.2.2 AAA Authentication Configuration Task....28
6.2.3 AAA Authentication Configuration Example....33

6.3 Authorization Configuration 33
6.3.1 AAA Authorization Configuration Task List 33
6.3.2 AAA Authorization Configuration Task 33
6.3.3 AAA Authorization Examples 34
6.4 AAA Accounting Configuration 35
6.4.1 AAA Accounting Configuration Task List 35
6.4.2 AAA Accounting Configuration Task 36
6.5 Local Account Policy Configuration 38
6.5.1 Local Account Policy Configuration Task List 38
6.5.2 Local Account Policy Configuration Task 38
6.5.3 Local Account Policy Example 39
Chapter 7 Configuring RADIUS 41
7.1 Overview 41
7.1.1 RADIUS Overview 41
7.1.2 RADIUS Operation 41
7.2 RADIUS Configuration Steps 42
7.3 RADIUS Configuration Task List 42
7.4 RADIUS Configuration Task 42
7.4.1 Configuring Switch to RADIUS Server Communication 42
7.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes 43
7.4.3 Specifying RADIUS Authentication 43
7.4.4 Specifying RADIUS Authorization 43
7.4.5 Specifying RADIUS Accounting 44
7.5 RADIUS Configuration Examples 44
7.5.1 RADIUS Authentication Example 44
7.5.2 RADIUS Application in AAA 44
Chapter 8 TACACS+ Configuration 45
8.1 TACACS+ Overview 45
8.1.1 The Operation of TACACS+ Protocol 45
8.2 TACACS+ Configuration Process 46
8.3 TACACS+ Configuration Task List 46
8.4 TACACS+ Configuration Task 46
8.4.1 Assigning TACACS+ Server 46

8.4.2 Setting up TACACS+ Encrypted Secret Key 47
8.4.3 Assigning to Use TACACS+ for Authentication 47
8.4.4 Assigning to Use TACACS+ for Authorization 47
8.4.5 Assigning to Use TACACS+ for Accounting 47
8.5 TACACS+ Configuration Example 48
8.5.1 TACACS+ Authentication Examples 48
8.5.2 TACACS+ Authorization Examples 48
8.5.3 TACACS+ Accounting Examples 49
Chapter 9 HTTP Switch Configuration 50
9.1 HTTP Configuration 50
9.1.1 Choosing the Prompt Language 50
9.1.2 Setting the HTTP Port 50
9.1.3 Enabling the HTTP Service 50
9.1.4 Setting the HTTP Access Mode 50
9.1.5 Setting the Maximum Number of VLAN Entries on Web Page 50
9.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page 51
9.2 HTTPS Configuration 51
9.2.1 Setting the HTTP Access Mode 51
9.2.2 It is used to set the HTTPS port 51
Chapter 10 Accessing the Switch 52
10.1 Accessing the Switch Through HTTP 52
10.1.1 Initially Accessing the Switch 52
10.1.2 Upgrading to the Web-Supported Version 52
10.2 Accessing a Switch through Secure Links 53
10.3 Introduction of Web Interface 53
10.3.1 Top Control Bar 53
10.3.2 Navigation Bar 54
10.3.3 Configuration Information Area 55
10.3.4 Configuration Area 55
Chapter 11 Basic Configuration 56
11.1 Hostname Configuration 56
11.2 Time Management 56

Chapter 12 Configuration of the Physical Interface 58

12.1 Configuring Port Description 58

12.2 Configuring the Attributes of the Port 58

12.3 Rate control 59

12.4 Port mirroring 59

12.5 Loopback Detection 59

12.6 Port security 60

12.6.1 IP Binding Configuration 60

12.6.2 MAC Binding Configuration 60

12.6.3 Setting the Static MAC Filtration Mode 60

12.6.4 Static MAC Filtration Entries 61

12.6.5 Setting the Dynamic MAC Filtration Mode 61

12.7 Storm control 61

12.7.1 Broadcast Storm Control 61

12.7.2 Multicast Storm Control 62

12.7.3 Unknown Unicast Storm Control 62

12.8 Port Protect Group Configuration 62

12.8.1 4.8.1 Port Protect Group List 62

12.8.2 4.8.2 Port Protect Group Interface Configuration 63

12.9 POE Management 63

12.9.1 POE Global Configuration 63

12.9.2 POE Global Real-time Information 63

12.9.3 POE Port List 64

12.9.4 POE Ports' Policy Power-up 64

12.9.5 POE Ports' Power Real-time Information 65

12.9.6 POE Ports' Other Real-time Information 65

Chapter 13 Layer-2 Configuration 66

13.1 VLAN Settings 66

13.1.1 VLAN List 66

13.1.2 VLAN Settings 67

13.2 GVRP Configuration 67

13.2.1 GVRP Global Attribute Configuration 67

13.2.2 Global Interface Attribute Configuration 68

13.3 STP Configuration **68**
13.3.1 STP Status Information 68
13.3.2 Configuring the Attributes of the STP Port 68
13.4 IGMP-Snooping Configuration **69**
13.4.1 IGMP-Snooping Configuration 69
13.4.2 IGMP-Snooping VLAN List 69
13.4.3 Static Multicast Address 70
13.4.4 Multicast List 71
13.5 Setting Static ARP **71**
13.6 Static MAC Address Configuration **72**
13.7 LLDP Configuration **72**
13.7.1 Configuring the Global Attributes of LLDP 72
13.7.2 LLDP Port Attribute Configuration 73
13.8 DDM Configuration **73**
13.9 Port Aggregation Configuration **73**
13.9.1 Port Aggregation Configuration 73
13.9.2 5.9.2 Port Channel Group Loading Balance Configuration 74
13.10 Ring Protection Configuration **75**
13.10.1 EAPS Ring List 75
13.10.2 EAPS Ring Configuration 75
13.11 MEAPS Configuration **76**
13.11.1 MEAPS Ring Network List 76
13.11.2 EAPS Ring Network Configuration 76
13.12 Backup Link Protocol Configuration **77**
13.12.1 Backup Link Protocol Global Configuration 77
13.12.2 Backup Link Protocol Interface Configuration 77
13.13 MTU Configuration **78**
13.14 PDP Configuration **78**
13.14.1 Configuring the Global Attributes of PDP 78
13.14.2 PDP Interface Attribute Configuration 79

Chapter 14 Layer-3 Configuration **80**

14.1 Configuring the VLAN Interface **80**
14.2 Static Routing Configuration **81**

Chapter 15 Advanced Configuration 83

15.1 QoS Configuration **83**

15.1.1 Configuring QoS Port 83

15.1.2 Global QoS Configuration 84

15.2 IP Access Control List **84**

15.2.1 Setting the Name of the IP Access Control List 84

15.2.2 Setting the Rules of the IP Access Control List 85

15.2.3 Applying the IP Access Control List 86

15.3 MAC Access Control List **86**

15.3.1 Setting the Name of the MAC Access Control List 86

15.3.2 Setting the Rules of the MAC Access Control List 87

15.3.3 Applying the MAC Access Control List 87

Chapter 16 Network Management Configuration 89

16.1 SNMP Configuration **89**

16.1.1 SNMP Community Management 89

16.1.2 SNMP Host Management 90

16.2 RMON **90**

16.2.1 RMON Statistic Information Configuration 90

16.2.2 RMON History Information Configuration 91

16.2.3 RMON Alarm Information Configuration 91

16.2.4 RMON Event Configuration 92

Chapter 17 Diagnosis Tools 94

17.1 Ping **94**

17.1.1 Ping 94

Chapter 18 System Management 96

18.1 User Management **96**

18.1.1 User List 96

18.1.2 Establishing a New User 97

18.1.3 User Group Management 97

18.1.4 Password Group Management 98

18.1.5 Authentication Group Configuration 99

18.1.6 Authorization Group Management 99

18.2 Log Management **100**
18.3 Managing the Configuration Files **100**
18.3.1 Exporting the Configuration Information 100
18.3.2 Importing the Configuration Information 101
18.4 Software Management **101**
18.4.1 Backing up the IOS Software 101
18.4.2 Upgrading the IOS Software 102
18.5 Rebooting the Device **102**
Chapter 19 Interface Configuration **103**
19.1 Introduction **103**
19.1.1 Supported Interface Types 103
19.1.2 Interface Configuration Introduction 103
19.2 Configuring Interface Common Attribute **104**
19.2.1 Adding Description 104
19.2.2 Configuring Bandwidth 105
19.2.3 Configuring Time Delay 105
19.3 Monitoring and Maintaining Interface **105**
19.3.1 Checking Interface State 105
19.3.2 Initializing and Deleting Interface 106
19.3.3 Shutting down and Enabling Interface 106
19.4 Setting the Ethernet Interface **106**
19.4.1 Choosing an Ethernet Interface 106
19.4.2 Configuring the Rate 107
19.4.3 Configuring the Duplex Mode of an Interface 107
19.4.4 Configuring Flow Control on an Interface 107
19.5 Configuring Logistical Interface **107**
19.5.1 Configuring Aggregation Interface 108
19.5.2 Configuring VLAN Interface 108
Chapter 20 Interface Configuration Example **109**
20.1 Configuring Public Attribute of Interface **109**
20.1.1 Interface Description Example 109
20.1.2 Interface Shutdown Example 109
Chapter 21 Interface Range Configuration **110**

21.1 Interface Range Configuration Task 110
21.1.1 Understanding Interface Range 110
21.1.2 Entering Interface Range Mode 110
21.1.3 Configuration Example 110
Chapter 22 Port Physical Characteristics Configuration 111
22.1 Configuring the Ethernet Interface 111
22.1.1 Configuring Rate 111
22.1.2 Configuring the Duplex Mode of an Interface 111
22.1.3 Configuring Flow Control on the Interface 111
Chapter 23 Port's Additional Features Configuration 112
23.1 Port Isolation 112
23.2 Storm Control 112
23.3 Port's Rate Limitation 113
23.4 Port Loop Detection 114
23.5 Port MAC-address learning 114
23.6 Port's Security 115
23.7 Interface's binding 115
23.8 SVL/IVL 116
23.9 Configuring Link Scan 117
23.9.1 Overview 117
23.9.2 Link scan Configuration Task 117
23.9.3 Configuration Example 117
23.10 Configuring Port Enhanced Link Status Check 117
23.10.1 Overview 117
23.10.2 Configuration Task 117
23.10.3 Configuration Example 117
23.11 Configuring system mtu 118
23.11.1 Overview 118
23.11.2 Configuration Task 118
23.11.3 Configuration Example 118
Chapter 24 Configuring Port Mirroring 119
24.1 Configuring Port Mirroring Task List 119
24.2 Configuring Port Mirroring Task 119

24.2.1 Configuring Port Mirroring 119
24.2.2 Displaying Port Mirroring Information 120
24.3 Remote Mirroring Configuration Example 120
Chapter 25 Configuring MAC Address Attribute 123
25.1 MAC Address Configuration Task List 123
25.2 MAC address Configuration Task 123
25.2.1 Configuring Static Mac Address 123
25.2.2 Configuring MAC Address Aging Time 123
25.2.3 Displaying blackhole Mac Address 124
25.2.4 Displaying MAC Address Table 124
25.2.5 Clearing Dynamic MAC Address 124
Chapter 26 MAC Access-List Configuration 126
26.1 Creating MAC Access-List 126
26.2 Configuring Items of MAC Access-List 126
26.3 Applying MAC Access-List 127
Chapter 27 Configuring 802.1x 128
27.1 802.1x Configuration Task List 128
27.2 802.1x Configuration Task 128
27.2.1 Configuring 802.1x Port Authentication 128
27.2.2 Configuring 802.1x Multiple Port Authentication 129
27.2.3 Configuring 802.1x Re-authentication 129
27.2.4 Configuring 802.1x Re-authentication times 130
27.2.5 Configuring 802.1x Transmission Frequency 130
27.2.6 Configuring 802.1x User Binding 130
27.2.7 Configuring Authentication Method for 802.1x Port 130
27.2.8 Selecting Authentication Type for 802.1x Port 131
27.2.9 Configuring MAB Authentication on the Port 131
27.2.10 Configuring 802.1x Accounting 132
27.2.11 Configuring 802.1x guest-vlan 132
27.2.12 Forbidding Supplicant With Multiple Network Cards 133
27.2.13 Resuming Default 802.1x Configuration 133
27.2.14 Monitoring 802.1x Authentication Configuration and State 133
27.3 802.1x Configuration Example 134

Chapter 28 Configuring GVRP 136

28.1 Overview 136

28.2 Configuring Task List 136

28.2.1 GVRP Configuration Task List 136

28.3 GVRP Configuration Task 136

28.3.1 Enabling/Disabling GVRP Globally 136

28.3.2 Dynamic VLAN to Validate only on a Registered Port 136

28.3.3 Enabling/Disabling GVRP on the Interface 136

28.3.4 Monitoring and Maintenance of GVRP 137

28.4 Configuration Example 137

Chapter 29 VLAN Configuration 139

29.1 VLAN Introduction 139

29.2 Dot1Q Tunnel Overview 139

29.2.1 Preface 139

29.2.2 Dot1Q Tunnel Realization Mode 139

29.3 VLAN Configuration Task List 140

29.4 VLAN Configuration Task 141

29.4.1 Adding/Deleting VLAN 141

29.4.2 Configuring Switch Port 141

29.4.3 Creating/Deleting VLAN Interface 142

29.4.4 Enable Dual VLAN Tagging functionality 142

29.4.5 Monitoring Configuration and State of VLAN 142

29.4.6 Enabling/disabling global Dot1Q Tunnel 143

29.4.7 Configuring MAC-based VLAN 143

29.5 Dot1Q Tunnel Configuration Examples 143

29.5.1 Dot1Q Tunnel configuration examples 143

Chapter 30 Private VLAN Settings 146

30.1 Overview of Private VLAN 146

30.2 Private VLAN Type and Port Type in Private VLAN 146

30.2.1 Having One Primary VLAN Type 146

30.2.2 Having Two Secondary VLAN Types 146

30.2.3 Port Types Under the Private VLAN Port 146

30.2.4 Modifying the Fields in VLAN TAG 146

30.3 Private VLAN Configuration Task List....146
30.4 Private VLAN Configuration Tasks....147
30.4.1 Configuring Private VLAN....147
30.4.2 Configuring the Association of Private VLAN Domains....147
30.4.3 Configuring the L2 Port of Private VLAN to Be the Host Port....148
30.4.4 Configuring the L2 Port of Private VLAN to Be the Promiscuous Port....148
30.4.5 Modifying Related Fields of Egress Packets in Private VLAN....148
30.4.6 Displaying the Configuration Information of Private VLAN....149
30.5 Configuration Example....149
Chapter 31 Configuring STP....152
31.1 STP Introduction....152
31.2 SSTP Configuration Task List....152
31.3 SSTP Configuration Task....153
31.3.1 Selecting STP Mode....153
31.3.2 Disabling/Enabling STP....153
31.3.3 Forbidding/Enable Port's STP....153
31.3.4 Configuring the Switch Priority....154
31.3.5 Configuring the Hello Time....154
31.3.6 Configuring the Max-Age Time....154
31.3.7 Configuring the Forward Delay Time....154
31.3.8 Configuring the Port Priority....155
31.3.9 Configuring the Path Cost....155
31.3.10 Monitoring STP State....155
31.3.11 Configuring SNMP Trap....155
31.4 Configuring VLAN spanning-tree....156
31.4.1 Overview....156
31.4.2 VLAN STP Configuration Task....156
Chapter 32 Configuring RSTP....158
32.1 RSTP Configuration Task List....158
32.2 RSTP Configuration Task....158
32.2.1 Enabling/Disabling Switch RSTP....158
32.2.2 Configuring the Switch Priority....158
32.2.3 Configuring the Forward Delay Time....158

32.2.4 Configuring the Hello Time....159
32.2.5 Configuring the Max-Age....159
32.2.6 Configuring the Path Cost....160
32.2.7 Configuring the Port Priority....160
32.2.8 Configuring edge port....161
32.2.9 Configuring port's connection type....161
32.2.10 Restarting the check of protocol conversion....161
Chapter 33 Configuring MTSP....163
33.1 MSTP Overview....163
33.1.1 Introduction....163
33.1.2 MST Domain....163
33.1.3 IST, CST, CIST and MSTI....163
33.1.4 Port Role....164
33.1.5 MSTP BPDU....167
33.1.6 Stable State....169
33.1.7 Hop Count....169
33.1.8 STP Compatibility....169
33.2 MSTP Configuration Task List....170
33.3 MSTP Configuration Task....170
33.3.1 Default MSTP Configuration....170
33.3.2 Enabling and Disabling MSTP....171
33.3.3 Configuring MST Area....171
33.3.4 Configuring Network Root....172
33.3.5 Configuring Secondary Root....173
33.3.6 Configuring Bridge Priority....174
33.3.7 Configuring STP Time Parameters....174
33.3.8 Configuring Network Diameter....175
33.3.9 Configuring Maximum Hop Count....175
33.3.10 Configuring Port Priority....176
33.3.11 Configuring Path Cost of the Port....176
33.3.12 Configuring Edge Port....177
33.3.13 Configuring Port Connection Type....177
33.3.14 Activating MST-Compatible Mode....177
33.3.15 Restarting Protocol Conversion Check....178

33.3.16 Configuring Port's Role Restriction....179
33.3.17 Configuring Port's TCN Restriction....179
33.3.18 Checking MSTP Information....179

Chapter 34 Configuring STP Optional Characteristic....181

34.1 STP Optional Characteristic Introduction....181
34.1.1 Port Fast....181
34.1.2 BPDU Guard....182
34.1.3 BPDU Filter....182
34.1.4 Uplink Fast....183
34.1.5 Backbone Fast....184
34.1.6 Root Guard....185
34.1.7 Loop Guard....186
34.2 Configuring STP Optional Characteristic....186
34.2.1 STP Optional Characteristic Configuration Task....186
34.2.2 Configuring Port Fast....187
34.2.3 Configuring BPDU Guard....187
34.2.4 Configuring BPDU Filter....188
34.2.5 Configuring Uplink Fast....188
34.2.6 Configuring Backbone Fast....189
34.2.7 Configuring Root Guard....189
34.2.8 Configuring Loop Guard....189
34.2.9 Configuring Loop Fast....190
34.2.10 Configuring Address Table Aging Protection....191
34.2.11 Configuring FDB-Flush....191
34.2.12 Configuring BPDU Terminal....192

Chapter 35 Configuring Port Aggregation....193

35.1 Overview....193
35.2 Port Aggregation Configuration Task List....193
35.3 Port Aggregation Configuration Task....193
35.3.1 Configuring Logical Channel Used to Aggregation....193
35.3.2 Aggregation of Physical Port....193
35.3.3 Selecting Load Balance Method After Port Aggregation....194
35.3.4 Monitoring the Concrete Conditions of Port Aggregation....195

Chapter 36 PDP Overview 196

36.1 Overview **196**

36.2 PDP Configuration Tasks **196**

36.2.1 Default PDP Configuration 196

36.2.2 Setting the PDP Clock and Information Storage 196

36.2.3 Setting the PDP Version 196

36.2.4 Starting PDP on a Switch 197

36.2.5 Starting PDP on a Port 197

36.2.6 PDP Monitoring and Management 197

36.3 PDP Configuration Example **197**

Chapter 37 LLDP Overview 199

37.1 LLDP Overview **199**

37.1.1 Initializing the Protocol 199

37.1.2 Initializing LLDP Transmit Mode 199

37.1.3 Initializing LLDP Receive Mode 199

37.1.4 LLDP PDU Packet Structure Description 200

37.2 LLDP Configuration Task List **201**

37.3 LLDP Configuration Tasks **201**

37.3.1 Disabling/enabling LLDP 201

37.3.2 Configuring Holdtime 202

37.3.3 You can configure the switch priority and make it more likely that a standalone switch or a switch in the stack will be chosen as the root switch. 202

37.3.4 imer 202

37.3.5 Configuring Reinit 203

37.3.6 Configuring the To-Be-Sent TLV 203

37.3.7 Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV 205

37.3.8 Configuring the Transmission or Reception Mode 207

37.3.9 Specifying the Management IP Address of a Port 208

37.3.10 Sending Trap Notification to mib Database 208

37.3.11 Configuring the Location Information 208

37.3.12 Specifying a Port to Set the Location Information 211

37.3.13 Configuring Show-Relative Commands 211

37.3.14 Configuring the Deletion Commands 212

37.4 Configuration Examples 212
37.4.1 Network Environment Requirements 212
37.4.2 Network Topology 212
37.4.3 Configuration Steps 212

Chapter 38 Introduction of Backup Link 221

38.1 Overview 221
38.2 BackupLink Port Backup 221
38.2.1 Configuring Backup Port 221
38.2.2 Status Control of the Port 222
38.2.3 Port Roles and Status 222
38.2.4 Link Status Change Processing 222
38.2.5 Pre-emption of Backup Port 222
Delay Preemption 223
38.3 VLAN Load Balancing 223
38.3.1 Configuration of Load balancing 223
38.3.2 Port status Control in Traffic Sharing 223
38.4 MAC Address Aging Operation 224
38.4.1 Normal Work Mechanism of the Link 224
38.4.2 Downlink Fault Handling Mechanism 225
38.4.3 Uplink Fault Handling Mechanism 225
38.4.4 Link Recovery Processing Mechanism 227

Chapter 39 BackupLink Configuration 228

39.1 Guidance Notes for BackupLink Configuration 228
39.2 BackupLink Configuration Tasks 228
39.3 BackupLink Configuration 228
39.3.1 Configuring BackupLink Group 228
39.3.2 Configuring the Preemption Feature for BackupLink Group 229
39.3.3 Configuring Load Balancing for VLAN 229
39.3.4 Configuring the MMU Feature for BackupLink Group 230
39.3.5 Configuring MonitorLink Group 230

Chapter 40 Introduction of Fast Ethernet Ring Protection 231

40.1 Overview 231
40.2 Related Concepts of Fast Ether-Ring Protection 231

40.2.1 Roles of Ring's Nodes 231
40.2.2 Role of the Ring's Port 232
40.2.3 Control VLAN and Data VLAN 232
40.2.4 Aging of the MAC Address Table 232
40.2.5 Symbol of a Complete Ring Network 232
40.3 Types of EAPS Packets 233
40.4 Fast Ethernet Ring Protection Mechanism 233
40.4.1 Ring Detection and Control of Master Node 233
40.4.2 Notification of Invalid Link of Transit Node 233
40.4.3 Resuming the Link of the Transit Node 234
Chapter 41 Fast Ethernet Ring Protection Configuration 235
41.1 Default EAPS Settings 235
41.2 Requisites before Configuration 235
41.3 MEAPS Configuration Tasks 235
41.4 Fast Ethernet Ring Protection Configuration 236
41.4.1 Configuring the Master Node 236
41.4.2 Configuring the Transit Node 236
41.4.3 Configuring the Ring Port 237
41.4.4 Browsing the State of the Ring Protection Protocol 237
41.5 MEAPS configuration 238
41.5.1 Configuration Example 238
Chapter 42 MEAPS Introduction 240
42.1 MEAPS Overview 240
42.2 Basic Concepts of MEAPS 240
42.2.1 Domain 240
42.2.2 Ring 241
42.2.3 Major Ring 241
42.2.4 Sub Ring 241
42.2.5 Control VLAN 241
42.2.6 Data VLAN 242
42.2.7 Master Node 242
42.2.8 Transit Node 242
42.2.9 Edge Node and Assistant Node 242

42.2.10 Primary Port and Secondary Port 243
42.2.11 Transit Port 243
42.2.12 Common Port and Edge Port 243
42.2.13 Aging of the MAC Address Table (FLUSH MAC FDB) 244
42.2.14 Complete Flag of Ring 244
42.3 Types of EAPS Packets 244
42.4 Fast Ethernet Ring Protection Mechanism 245
42.4.1 Polling mechanism 245
42.4.2 Notification of Invalid Link of Transit Node 245
42.4.3 Channel Status Checkup Mechanism of the Sub-Ring Protocol Packet on the Major ring 247
Chapter 43 Fast Ethernet Ring Protection Configuration 252
43.1 Requisites before Configuration 252
43.2 MEAPS Configuration Tasks 252
43.3 Fast Ethernet Ring Protection Configuration 253
43.3.1 Configuring the Master Node 253
43.3.2 Configuring the Transit Node 254
43.3.3 Configuring the Edge Node and the Assistant Node 254
43.3.4 Configuring Sub-ring Networking Mode 255
43.3.5 Configuring the Ring Port 256
43.3.6 Browsing the State of the Ring Protection Protocol 256
Chapter 44 Appendix of MEAPS Configuration 257
44.1 Working Procedure of MEAPS 257
44.1.1 Complete State 257
44.1.2 Link-Down 257
44.1.3 Recovery 259
44.2 MEAPS Configuration Examples 260
44.2.1 Configuration Examples 260
44.3 Unfinished Configurations (to be continued) 268
Chapter 45 Unidirectional Link Detection (UDLD) 269
45.1 UDLD Overview 269
45.1.1 UDLD Mode 269
45.1.2 Running Mechanism 269
45.1.3 State of the Port 270

45.1.4 Maintaining the Cache of the Neighbor....270
45.1.5 Echo Detection....270
45.2 UDLD Configuration Task List....270
45.3 UDLD Configuration Tasks....271
45.3.1 Globally Enabling or Disabling UDLD....271
45.3.2 Enabling or Disabling the UDLD Interface....271
45.3.3 Setting the Message Interval of the Aggressive Mode....272
45.3.4 Restarting the Interface Shut Down by UDLD....272
45.3.5 Displaying the UDLD State....272
45.4 Configuration Example....274
45.4.1 Network Environment Requirements....274
45.4.2 Network Topology....274
45.4.3 Configuration Procedure....274
Chapter 46 IGMP-snooping Configuration....277
46.1 IGMP-snooping Configuration Task....277
46.1.1 Enabling/Disabling IGMP-Snooping of VLAN....277
46.1.2 Adding/Deleting Static Multicast Address of VLAN....278
46.1.3 Configuring immediate-leave of VLAN....278
46.1.4 Configuring immediate-leave of port....278
46.1.5 Configuring Static Routing Interface of VLAN....279
46.1.6 Configuring IPACL of Generating Multicast Forward Table....279
46.1.7 Configuring the Function to Filter Multicast Message Without Registered Destination Addresss....279
46.1.8 Configuring Router Age Timer of IGMP-snooping....280
46.1.9 Configuring Response Time Timer of IGMP-Snooping....280
46.1.10 Configuring Querier of IGMP-Snooping....280
46.1.11 Configuring IGMP-snooping's Querier Time Timer....281
46.1.12 Configuring data forwarding of IGMP-snooping's forward-l3-to-mrouter to router port....281
46.1.13 Configuring sensitive mode and value for IGMP-snooping....282
46.1.14 Configuring IGMP-snooping's v3-leave-check function....282
46.1.15 Configuring IGMP-snooping's forward-wrongiif-within-vlan function....282
46.1.16 Configuring IGMP-snooping's IPACL function at port....283
46.1.17 Configuring IGMP-snooping's multicast filtering in VLAN....283
46.1.18 Configuring maximum multicast IP address quantity function at IGMP-snooping's port....283
46.1.19 Configuring IGMP-snooping's report-suppression function....284

46.1.20 Configuring IGMP-snooping's proxy-leave function....284
46.1.21 Monitoring and Maintaining IGMP-Snooping....284
46.1.22 IGMP-Snooping Configuration Example....287
Chapter 47 IGMP-Proxy Configuration....289
47.1 IGMP-proxy Configuration Tasks....289
47.1.1 Enabling/Disabling IGMP-Proxy....289
47.1.2 Adding/Deleting VLAN Agent Relationship....289
47.1.3 Monitoring and Maintaining IGMP-Proxy....290
47.1.4 IGMP-Proxy Configuration Example....290
Chapter 48 MLD-Snooping Configuration....291
48.1 IPv6 Multicast Overview....291
48.2 MLD-Snooping Multicast Configuration Tasks....291
48.2.1 Enabling/Disabling MLD-Snooping Multicast....291
48.2.2 Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group....291
48.2.3 Adding/Canceling the Static Multicast Address of VLAN....292
48.2.4 Setting Router Age Timer of MLD-Snooping....292
48.2.5 Setting Response Time Timer of MLD-Snooping....292
48.2.6 Setting Querier of MLD-Snooping....293
48.2.7 Setting the Port of the Static Multicast Router....293
48.2.8 Enabling/Disabling Immediate Leave....293
48.2.9 Monitoring and Maintaining MLD-Snooping Multicast....294
Chapter 49 OAM Configuration....296
49.1 OAM Overview....296
49.1.1 OAM Protocol's Attributes....296
49.1.2 OAM Mode....297
49.1.3 Components of the OAM Packet....298
49.2 OAM Configuration Task List....299
49.3 OAM Configuration Tasks....299
49.3.1 Enabling OAM on an Interface....299
49.3.2 Configuring OAM Link Monitoring....299
49.3.3 Configuring the Trouble Notification from Remote OAM Entity....301
49.3.4 Displaying the Information about OAM Protocol....302
49.4 Configuration Example....302

49.4.1 Network Environment Requirements....302
49.4.2 Network Topology....303
49.4.3 Configuration Procedure....303
Chapter 50 Overview of CFM and Y1731 Configuration....306
50.1 Stipulations....306
50.1.1 Format Stipulation in the Command Line....306
Chapter 51 CFM Configuration....307
51.1 CFM Configuration Task List....307
51.2 CFM Maintenance Task List....307
51.3 CFM Configuration....307
51.3.1 Adding the Maintenance Domain....307
51.3.2 Adding the Maintenance Association....307
51.3.3 Adding MIP (Maintenance domain Intermediate Point)....307
51.3.4 Adding MEP (Maintenance association End Point)....308
51.3.5 Starting CFM....308
51.4 CFM Maintenance....308
51.4.1 Using the Loopback Function....308
51.4.2 Using the Linktrace Function....308
51.5 Configuration Example....309
Chapter 52 Y1731 Configuration....310
52.1 Configuration Task List....310
52.1.1 Enable frame delay measurement function....310
52.1.2 Displaying the Y1731 Protocol Information....310
52.1.3 Deleting Y1731 Configuration or Statistics Information....311
52.2 Configuration example....311
Chapter 53 DHCP-Snooping Configuration....315
53.1 IGMP-Snooping Configuration Tasks....315
53.1.1 Enabling/Disabling DHCP-Snooping....315
53.1.2 Enabling DHCP-Snooping in a VLAN....315
53.1.3 Enabling DHCP anti-attack in a VLAN....316
53.1.4 Setting an Interface to a DHCP-Trusting Interface....316
53.1.5 Enabling/Disabling binding table fast update function....316

53.1.6 Enabling DAI in a VLAN 317
53.1.7 Setting an Interface to an ARP-Trusting Interface 317
53.1.8 Enabling Source IP Address Monitoring in a VLAN 317
53.1.9 Setting an Interface to the One Which is Trusted by IP Source Address Monitoring 318
53.1.10 Setting DHCP-Snooping Option 82 318
53.1.11 Setting the Policy of DHCP-Snooping Option82 Packets 319
53.1.12 Configuring the TFTP Server for Backing up Interface Binding 320
53.1.13 Configuring a File Name for Interface Binding Backup 320
53.1.14 Configuring the Interval for Checking Interface Binding Backup 321
53.1.15 Configuring Interface Binding Manually 321
53.1.16 Monitoring and Maintaining DHCP-Snooping 321
53.1.17 DHCP-Snooping Configuration Example 322

Chapter 54 MACFF Configuration 325

54.1 MACFF Configuration Tasks 325
54.1.1 Enabling or Disabling MACFF 325
54.1.2 Enabling MACFF in VLAN 325
54.1.3 Configuring the Default AR of MACFF in VLAN 326
54.1.4 Configuring other ARs of MACFF in VLAN 326
54.1.5 Specifying a Physical Port to Shut down MACFF 326
54.1.6 Enabling MACFF Debugging 326
54.1.7 MACFF Configuration Example 327

Chapter 55 Layer-2 (L2) Tunnel Protocol Configuration 329

55.1 Overview 329
55.2 Layer-2 (L2) Tunnel Protocol Configuration 329
55.3 L2 Protocol Tunnel Configuration Example 329

Chapter 56 QoS Configuration 331

56.1 QoS Overview 331
56.1.1 QoS Concept 331
56.1.2 Terminal-To-Terminal QoS Model 331
56.1.3 Queue Algorithm of QoS 332
56.1.4 Weighted Random Early Detection 332
56.2 QoS Configuration Task List 333
56.3 QoS Configuration Tasks 334

56.3.1 Setting the Global cos Priority Queue 334
56.3.2 Setting the Bandwidth of the CoS Priority Queue 334
56.3.3 Setting the Schedule Policy of the CoS Priority Queue 335
56.3.4 Setting the Default CoS Value of a Port 335
56.3.5 Setting the CoS Priority Queue of a Port 336
56.3.6 Setting the Bandwidth of a Port CoS Priority Queue 336
56.3.7 Setting the Schedule Policy of a Port CoS Priority Queue 337
56.3.8 Setting the CoS Priority Queue Based on DSCP 337
56.3.9 Establishing the QoS Policy Mapping 337
56.3.10 Setting the Description of the QoS Policy Mapping 338
56.3.11 Setting the Matchup Data Flow of the QoS Policy Mapping 338
56.3.12 Setting the Actions of the Matchup Data Flow of the QoS Policy Mapping 339
56.3.13 Applying the QoS Policy on a Port 341
56.3.14 Applying the QoS Policy Globally 341
56.3.15 Configuring Trust Mode 341
56.3.16 Displaying the QoS Policy Mapping Table 342
56.4 QoS Configuration Example 342
56.4.1 Example for Applying the QoS Policy on a Port 342

Chapter 57 DoS Attack Prevention Configuration 343

57.1 DoS Attack Overview 343
57.1.1 Concept of DoS Attack 343
57.1.2 DoS Attack Type 343
57.2 DoS Attack Prevention Configuration Task List 344
57.3 DoS Attack Prevention Configuration Tasks 344
57.3.1 Configuring Global Dos Attack Prevention 344
57.3.2 Configuring Dos Attack Prevention 345
57.4 DoS Attack Prevention Configuration Example 345

Chapter 58 Attack Prevention Introduction 346

58.1 Overview of Filter 346
58.2 he Mode of Filter 346

Chapter 59 Attack Prevention Configuration 347

59.1 Attack Prevention Configuration Tasks 347
59.2 Attack Prevention Configuration 347

59.2.1 Configuring the Attack Filter Parameters....347
59.2.2 Configuring the Attack Prevention Type....347
59.2.3 Enabling the Attack Prevention....348
59.2.4 Checking the State of Attack Prevention....349
Chapter 60 Attack Prevention Configuration Example....350
60.1 Using Filter ARP to Protect the LAN....350
60.2 Using Filter IP to Protect Layer-3 Network....350
Chapter 61 Configuring IP Addressing....352
61.1 IP Introduction....352
61.1.1 IP....352
61.2 Configuring IP Address Task List....352
61.3 Configuring IP Address....352
61.3.1 Configuring IP Address at the Network Interface....352
61.3.2 Configuring multiple IP addresses at the network interface....353
61.3.3 Configuring Address Resolution....354
61.3.4 Detecting and maintaining IP addressing....356
61.4 IP Addressing Example....356
Chapter 62 Configuring DHCP....357
62.1 Overview....357
62.1.1 DHCP Application....357
62.1.2 Advantages of DHCP....357
62.1.3 DHCP Terms....357
62.2 Configuring DHCP Client....357
62.2.1 Configuration Task List of DHCP Client....357
62.2.2 DHCP Client Configuration Tasks....358
62.2.3 DHCP Client Configuration Example....359
Chapter 63 IP Service Configuration....360
63.1 Configuring IP Service....360
63.1.1 Managing IP connection....360
63.1.2 Configuring performance parameters....362
63.1.3 Detecting and Maintaining IP Network....362
63.2 Configuring Access List....364

63.2.1 Filtering IP Packet....364
63.2.2 Creating Standard and Extensible IP Access List....364
63.2.3 Apply the Access List to the Interface....365
63.2.4 Extensible Access List Example....366
63.3 Configuring IP Access List Based on Physical Port....366
63.3.1 Filtering IP Packet....366
63.3.2 Creating Standard and Extensible IP Access List....367
63.3.3 Applying ACL on Ports....368
63.3.4 Extensible Access List Example....368
Chapter 64 IP ACL Application Configuration....369
64.1 Applying the IP Access Control List....369
64.1.1 Applying ACL on Ports....369
Chapter 65 Routing Protocol Overview....370
65.1 IP Routing Protocol....370
65.2 Choosing Routing Protocol....370
65.2.1 Interior Gateway Router Protocol....370
65.2.2 Exterior Gateway Routing Protocol....370
Chapter 66 Configuring VRF....372
66.1 Overview....372
66.2 VRF Configuration Task List....372
66.3 Configuration Task....372
66.3.1 Creating VRF Table....372
66.3.2 Relating the interface to VRF....372
66.3.3 Configuring the Target VPN Expansion Attribute of VRF....373
66.3.4 Configuring Description of VRF....373
66.3.5 Configuring Static Route of VRF....373
66.3.6 Monitoring VRF....373
66.3.7 Maintaining VRF....374
66.4 Example of the VRF Configuration....374
Chapter 67 Static routing Configuration....377
67.1 Overview....377
67.2 Static Routing Configuration Task List....377

67.3 Static Routing Configuration Task 377
67.3.1 Configure the Static Routing 377
67.4 Example of the Static Routing Configuration 377
Chapter 68 Configuring RIP 378
68.1 Overview 378
68.2 RIP Configuration Task List 378
68.3 RIP Configuration Task 378
68.3.1 Starting the RIP 378
68.3.2 Generating the RIP instance interface 379
68.3.3 Allowing the mono-broadcasting updtaed and grouped by RIP Router 379
68.3.4 Using the Offsets on the Route metric 379
68.3.5 Regulating the Timer 380
68.3.6 Appointing the RIP Version Number 380
68.3.7 Activating the 'Passive' and 'Deaf' of the Interface 381
68.3.8 Activating RIP Authentication 381
68.3.9 Prohibitting the Route summary 382
68.3.10 Prohibitting the Authentication of Source IP Address and Zero-domain 383
68.3.11 Maximum Number of Equivalent Routes 383
68.3.12 Activating or Prohibit the Horizontal Split 383
68.3.13 Monitoring and Maintainance of RIP 384
68.4 Example of the RIP Configuration 385
Chapter 69 BEIGRP Dynamic Routing Protocol Configuration 386
69.1 Overview 386
69.2 BEIGRP Configuration Task List 386
69.2.1 Activating BEIGRP Protocol 386
69.2.2 Configuring the Sharable Percentage of Bandwidth 387
69.2.3 Adjusting the Arithmetic Coefficient of BEIGRP Composite Distance 387
69.2.4 Using "Offset" to Adjust the Composite Distance of the Router 387
69.2.5 Turning off Auto-Summary 388
69.2.6 Redistributing Other Routes into the BEIGRP Process 388
69.2.7 Configuring Other Parameters of BEIGRP 388
69.2.8 Monitoring and Maintaining BEIGRP 390
69.3 Examples of BEIGRP configuration 390

Chapter 70 Configuring OSPF 391

70.1 Overview **391**

70.2 OSPF Configuration Tast List **391**

70.3 OSPF Configuration Task **392**

70.3.1 Starting OSPF 392

70.3.2 Configuring the Interface Parameter of OSPF 392

70.3.3 Configuring OSPF Network Type 393

70.3.4 Configuring One-to-Multiple Broadcast Network 394

70.3.5 Configuring Non-Broadcasting Network 394

70.3.6 Configure OSPF domain 395

70.3.7 Configuring the NSSA Area of OSPF 395

70.3.8 Configuring Route Summary Within OSPF Domain 396

70.3.9 Configuring the Gathering of a Forwarding Router 396

70.3.10 Creating Default Route 396

70.3.11 Selecting Router ID Through Loopback Interface 397

70.3.12 Configuring the Management Distance of OSPF 397

70.3.13 Configuring the Route Calculation Timer 397

70.3.14 Configuring the On-Demand Link 398

70.3.15 Monitoring and Maintaining OSPF 398

70.4 Examples of OSPF Configuration **399**

70.4.1 Examples of OSPF point to multipoints, non-broadcasting configuration 399

70.4.2 Configuring example of variable-length subnet mask 400

70.4.3 Examples of the configuration of OSPF route and route distribution 400

Chapter 71 Configure BGP 406

71.1 Overview **406**

71.1.1 The BGP implementation of the router 406

71.1.2 How does BGP select the path 406

71.2 BGP Configuration Task List **407**

71.2.1 Basic configuration task list of BGP 407

71.2.2 Advanced BGP configuration tasks list 407

71.3 BGP Configuration Task **408**

71.3.1 Configuring Basic BGP Features 408

71.3.2 Configuring advanced BGP features 412

71.4 Monitoring and Maintaining BGP....417
71.4.1 Deleting the BGP Routing Table and the BGP Database....417
71.4.2 Displaying the Routing Table and the System Statistics Information....418
71.4.3 Tracking the BGP Information....419
71.5 Examples of BGP configuration....419
71.5.1 Example of BGP route-map....419
71.5.2 Example of neighbour configuration....420
71.5.3 Example of BGP route filtration based on the neighbor....421
71.5.4 Examples of BGP route filtration based on the interface....421
71.5.5 Examples of using prefix list to configure route filtration....421
71.5.6 Example of BGP route aggregation....422
71.5.7 Example of BGP route reflector....423
71.5.8 Example of BGP confederation....425
71.5.9 Example of route map with BGP group attribute....427
Chapter 72 Congiuring PBR....429
72.1 Overview....429
72.2 PBR Configuration Task List....429
72.3 PBR Configuration Task....429
72.3.1 Create standard access-list....429
72.3.2 Create route-map....429
72.3.3 Apply route-map on interface....430
72.3.4 Maintaining PBR....430
72.4 PBR configution example....430
Chapter 73 Switch Routing Protocol Highpriority Configuration....432
73.1 Overview....432
73.2 Configuration task list....432
73.3 Configuration task....432
73.3.1 Enable priority improving of the routing packets forwarding to CPU....432
Chapter 74 IP Hardware Subnet Routing Configuration....433
74.1 IP Hardware Subnet Configuration Task....433
74.1.1 Overview....433
74.1.2 Configuring IP Hardware Subnet Routing....433
74.2 Configuration Example....433

Chapter 75 IP-PBR Configuration....434
75.1 IP-PBR Configuration....434
75.1.1 Enabling or Disabling IP-PBR Globally....434
75.1.2 ISIS Configuration Task List....434
75.1.3 Monitoring and Maintaining MVC....435
75.1.4 IP-PBR Configuration Example....436
Chapter 76 Multi-VRF CE Intro....438
76.1 Overview....438
76.1.1 Establishing Routes with CE....438
76.1.2 Establishing Routes with PE....438
Chapter 77 Multi-VRF CE Configuration....440
77.1 Default VRF Configuration....440
77.2 MCE Configuration Tasks....440
77.3 MCE Configuration....440
77.3.1 Configuring VRF....440
77.3.2 Configuring VPN Route....441
77.3.3 Configuring the BGP Route between PE and CE....442
77.3.4 Testifying the VRF Connectivity between PE and CE....442
Chapter 78 MCE Configuration Example....443
78.1 Configuring S11....443
78.2 Configuring MCE-S1....444
78.3 Configuring PE....446
78.4 Configuring MCE-S2....448
78.5 Setting S22....450
78.6 TestifyingVRF Connectivity....451
Chapter 79 VRRP Configuration....452
79.1 Overview....452
79.2 VRRP Configuration Task List....452
79.3 VRRP Configuration Task....452
79.3.1 Configuring VRRP Virtual IP Address....452
79.3.2 Configuring VRRP Authentication Mode....452
79.3.3 Configuring VRRP Description....453

79.3.4 Configuring VRRP Priority Preemption 453
79.3.5 Configuring VRRP Protocol Packet MAC Address 453
79.3.6 Configuring VRRP Priority 454
79.3.7 Configuring VRRP Clock Value 454
79.3.8 Configuring VRRP Monitoring Object 454
79.3.9 Monitoring and Maintaining VRRP 455
79.3.10 VRRP Configuration Example 456

Chapter 80 Multicast Overview 458

80.1 Multicast Routing Realization 458
80.2 Multicast Routing Configuration Task List 459
80.2.1 Basic Multicast Configuration Task List 459
80.2.2 IGMP Configuration Task List 459
80.2.3 PIM-DM Configuration Task List 459
80.2.4 PIM-SM Configuration Task List 459

Chapter 81 Basic Multicast Routing Configuration 460

81.1 Starting up Multicast Routing 460
81.2 Starting up the Multicast Function on the Port 460
81.2.1 Starting up PIM-DM 460
81.2.2 Starting up PIM-SM 460
81.3 Configuring TTL Threshold 460
81.4 Configuring IP Multicast Boundary 461
81.5 Configuring IP Multicast Helper 461
81.6 Configuring Stub Multicast Route 463
81.7 Monitoring and Maintaining Multicast Route 463

Chapter 82 IGMP Configuration 465

82.1 Overview 465
82.2 IGMP Configuration 465
82.2.1 Changing Current IGMP Version 465
82.2.2 Configuring IGMP Query Interval 466
82.2.3 Configuring IGMP Querier Interval 466
82.2.4 Configuring Maximum IGMP Response Time 466
82.2.5 Configuring IGMP Query Interval for the Last Group Member 467
82.2.6 Static IGMP Configuration 467

82.2.7 Configuring the IGMP Immediate-leave List....468
82.3 IGMP Characteristic Configuration Example....468
82.3.1 Example for changing the IGMP version....468
82.3.2 IGMP query interval configuration example....469
82.3.3 IGMP Querier interval configuration example....469
82.3.4 Maximum IGMP response time example....469
82.3.5 Example for configuring IGMP query interval for the last group member....469
82.3.6 Static IGMP configuration example....470
82.3.7 IGMP Immediate-leave list configuration example....470
Chapter 83 PIM-DM Configuration....471
83.1 PIM-DM Introduction....471
83.2 Configuring PIM-DM....471
83.2.1 Modifying Timer....471
83.2.2 Designating the Version Number....472
83.2.3 Configuring State-Refresh....472
83.2.4 Configuring Filtration List....472
83.2.5 Setting DR Priority....473
83.2.6 Clearing Item (S,G)....473
83.3 PIM-DM State-Refresh Configuration Example....473
Chapter 84 Configuring PIM-SM....474
84.1 PIM-SM Introduction....474
84.2 PIM-SM Configuration List....474
84.2.1 Enabling Global Multicast....474
84.2.2 Starting up PIM-SM....475
84.2.3 Configuring Neighbor Filter List....475
84.2.4 DR Election....476
84.2.5 Configuring Candidate RP....477
84.2.6 Configuring Candidate BSR....478
84.2.7 Configuring SPT-threshhold....479
84.2.8 Configuring SSM....479
84.2.9 Configuring Management Domain sz....480
84.2.10 Configuring Source Address of Registered Packets....481
84.2.11 Configuring anycast-rp....481

84.2.12 Displaying pim-sm Local Routing Entries....481
84.2.13 Clearing pim-sm Routing Entries....482
84.2.14 Tracking pim-sm Debugging Information....483
84.3 Configuration Example....484
84.3.1 pim-sm Common Topology Configuration Examples....485
84.3.2 Mixing of Multi-Protocol Multicast....487
Chapter 85 IPv6 Protocol Configuration....488
85.1 IPv6 Protocol Configuration....488
85.2 Enabling IPv6....488
85.2.1 Setting the IPv6 Address....488
Chapter 86 Setting the IPv6 Services....489
86.1 Setting the IPv6 Services....489
86.1.1 Managing the IPv6 Link....489
Chapter 87 ND Configuration....491
87.1 ND Overview....491
87.1.1 Address Resolution....491
Chapter 88 OSPFv3 Configuration....492
88.1 Overview....492
88.2 OSPFv3 Configuration Task List....492
88.3 OSPFv3 Configuration Tasks....493
88.3.1 Enabling OSPFv3....493
88.3.2 Setting the Parameters of the OSPFv3 Interface....493
88.3.3 Setting OSPFv3 on Different Physical Networks....494
88.3.4 Setting the OSPF Network Type....494
88.3.5 Setting the Parameters of the OSPFv3 Domain....494
88.3.6 Setting the Route Summary in the OSPFv3 Domain....495
88.3.7 Setting the Summary of the Forwarded Routes....495
88.3.8 Generating a Default Route....496
88.3.9 Choosing the Route ID on the Loopback Interface....496
88.3.10 Setting the Management Distance of OSPFv3....496
88.3.11 Setting the Timer of Routing Algorithm....496
88.3.12 Monitoring and Maintaining OSPFv3....497

88.4 OSPFv3 Configuration Example **498**
88.4.1 Example for OSPFv3 Route Learning Settings 498
Chapter 89 Overview of NTP Configuration **506**
89.1 Stipulation **506**
89.1.1 Format Stipulation in the Command Line 506
Chapter 90 NTP Configuration **507**
90.1 Overview **507**
90.2 NTP Configuration **507**
90.2.1 Configuring the Equipment As an NTP Server 507
90.2.2 Configuring NTP Authentication Function 507
90.2.3 Configuring NTP Association 508
90.2.4 Configuring time zone 508
90.2.5 Configuring Summer Time 508
Chapter 91 IPv6 ACL Configuration **509**
91.1 IPv6 ACL Configuration **509**
91.1.1 Filtering IPv6 Packets 509
91.1.2 Setting up IPv6 ACL 509
91.1.3 Applying ACL to the Ports 510
91.1.4 Examples of IPv6 ACL 510
Chapter 92 IP-Attack Prevention Configuration **511**
92.1 Overview **511**
92.2 IP-Attack Prevention Configuration Task List **511**
92.3 IP-Attack Prevention Configuration **511**
92.3.1 Configuring IP attack detection parameters 511
92.3.2 Configuring the IP attack detection type 511
92.3.3 Enabling IP-Attack Prevention function 512
92.4 Examples of IP-Attack Prevention Configuration **512**
Chapter 93 IP Attacks Prevention against Direct Network Segment Scanning **513**
93.1 Overview **513**
93.2 Configuration task list of IP Attacks Prevention against Direct Network Segment Scanning **513**
93.3 Configuring IP Attacks Prevention against Direct Network Segment Scanning **513**

93.3.1 Configuring detection parameters of IP attacks prevention against direct network segment scanning 513
93.3.2 Configure detection types of IP anti-direct network segment scanning detection types 513
93.3.3 Enable IP Attacks Prevention against Direct Network Segment Scanning 514
93.4 Examples of IP Attacks Prevention against Direct Network Segment Scanning 514
93.5 Detection Results of IP Attacks Prevention against Direct Network Segment Scanning 514
Chapter 94 Configuring Time Range 515
94.1 Time Range Introduction 515
94.1.1 Overview 515
94.1.2 Absolute Time Range 515
94.1.3 Periodic Time Range 515
94.1.4 Isolating Time Range 515
94.1.5 From-to Time Range 515
94.1.6 Activating Time Range 515
94.2 Time Range Configuration Task List 516
94.3 Time Range Configuration Task 516
94.3.1 Adding/Deleting Time Range 516
94.3.2 Adding/Deleting Absolute Time Range 516
94.3.3 Adding/Deleting Periodic Time Range 517
94.3.4 Applying Time Range 517
94.3.5 Monitoring the configuration and state of Time Range 517
94.4 Configuration Example 518
Chapter 95 uRPF Configuration 519
95.1 Overview of uRPF 519
95.1.1 uRPF (Unicast Reverse Path Forwarding) 519
95.2 uRPF Configuration 519
95.2.1 Enabling uRPF in the Global Configuration Mode 519
95.2.2 Configuring uRPF Check Mode on the VLAN Interface 519
Chapter 96 Cable Diagnostic Configuration 520
96.1 Enable the Ethernet interface cable diagnostic 520
Chapter 97 Optical Port Additional Function Configuration 521
97.1 Enable Optical Port DDM Function 521
97.2 Optical Port Single-fiber Transceiver Function 521

97.3 Optical Port Adaptive Optical Module Function 522

Chapter 98 Power over Ethernet 523

98.1 POE Overview 523

98.1.1 Introduction to POE Power Supply 523

98.1.2 Power-Up Procedure of PoE 524

98.2 POE Configuration Task List 525

98.3 POE Configuration Tasks 525

98.3.1 Displaying the information about POE-related systems. 525

98.3.2 Enabling the Power Supply of a Port 526

98.3.3 Setting the Maximum Power of a Port 527

98.3.4 Setting the Power Supply Priority for a Port 527

98.3.5 Configuring the Port Description (usually for PD) 527

98.3.6 Configuring the Forced Power Supply 528

98.3.7 Configuring port high inrush power-on function 528

98.3.8 Configuring the extra power of the device 529

98.3.9 Configuring the hot restart function 529

98.3.10 Configuring power supply detection mode 530

Chapter 99 Configuring Virtualization 531

99.1 Overview 531

99.2 Virtualization Configuration Task List 531

99.3 Virtualization Configuration Task 531

99.3.1 Configuring virtualized ports for interconnection 531

99.3.2 Configuring parameters of virtualization 531

99.3.3 Enabling Virtualization 532

99.3.4 Saving Virtualization Configuration 532

99.3.5 Showing virtualization configuration 532

Chapter 100 Introduction of Fast Ethernet Ring Network Protection 534

100.1 Overview 534

100.2 ERPS-Related Concepts 534

100.2.1 Ring Network Level 535

100.2.2 Ring Network Node Role 535

100.2.3 Ring Network Port Role 535

100.2.4 ERPS & CFM 535

100.2.5 Ring Network Interconnection Mode Using R-APS Virtual Channel 536
100.2.6 R-APS Transmission VLAN 536
100.2.7 Revertive Mode 537
100.3 Type of ERPS Packets 537
100.4 ERPS Ring Network Protection Mechanism 538
100.4.1 Stable State 538
100.4.2 Local Link Failure Processing 538
100.4.3 Local Link Recovery Processing 538
100.4.4 Protection Switching - Link Recovery 538
100.4.5 Protection Switching - Manual Switching 539
100.4.6 Protection Switching - Forced Switching 540
100.4.7 Switching Recovery Processing 540

Chapter 101 ERPS Configuration 542

101.1 ERPS Configuration Instructions 542
101.2 ERPS Configuration Tasks 542
101.2.1 Configuring the Ring Network Nodes 542
101.2.2 Configuring the Ring Network Ports 544
101.2.3 Ring Network Control Commands 544
101.2.4 Checking Ring Network Protection Protocol Status 545
101.3 ERPS Configuration Instance 545
101.3.1 Configuration example 1-ERPS single ring configuration 545
101.3.2 Configuration example 2-ERPS multi-ring configuration 550

Chapter 102 Loopback Detection Configuration 556

102.1 Introduction to Loopback Detection 556
102.1.1 Format of Loopback Detection Packet 556
102.2 Loopback Detection Configuration Task List 556
102.3 Loopback Detection Configuration 557
102.3.1 Configuring the global loopback detection 557
102.3.2 Configuring the loopback detection of the port 557
102.3.3 Configuring the loopback detection for certain VLANs 557
102.3.4 Configure Loopback Detection Time 557
102.3.5 Configuring the loopback-detection control 558
102.3.6 Configuring the Upper Limit of Port Loop Detection Frames 559

102.3.7 Configuring the frame number detection function of the port 559
102.3.8 Configuring Loopback Detection Destination MAC....559
102.3.9 Configuring loopback detection existence....559
102.3.10 Configuring to prohibit forwarding of looped packets on port....560
102.3.11 Configuring Isolated VLAN Recovery on port 560
102.3.12 Showing loopback detection global configuration information....560
102.3.13 Showing loopback detection interface....560
102.4 Configuration Example 561

Chapter 103 MAD Configuration 563

103.1 MAD Overview....563
103.2 MAD Configuration Task List....563
103.3 MAD Configuration Task....563
103.3.1 LACP MAD Configuration....563

Chapter 104 RNP Configuration....564

104.1 RNP Overview....564
104.2 RNP Configuration Task List....564
104.3 RNP Configuration Tasks....564
104.3.1 Configuring the timeout of the RNP old master device....564
104.3.2 Monitoring RNP State....564
104.4 Configuration Example 564

Chapter 105 SGNP Configuration 566

105.1 SGNP Overview....566
105.2 SGNP Configuration Task List....566
105.3 SGNP Configuration Tasks....566
105.3.1 Configuring the timeout period of SGNP neighbors....566
105.3.2 Monitoring SGNP configuration and status....566
105.4 Configuration Example 566

Chapter 1 Configuration Preparation

The chapter mainly describes the following preparatory works before you configure the switch at the first time:

- Port number of the switch
- Preparation before switch startup
- How to get help
- Command mode
- Cancelling a command
- Saving configuration

1.1 Port Number of the Switch

The physical port of the switch is numbered in the **<type><slot>/<port>** form. THE type-to-name table is shown as follows:

Interface Type	Name	Simplified Name
10M Ethernet	Ethernet	e
100M fast Ethernet	FastEthernet	f
1000M Ethernet	GigaEthernet	g

The expansion slot number to mark and set ports must be the number **0**. Other expansion slots are numbered from left to right, starting from **1**.

The ports in the same expansion slot are numbered according to the order from bottom to top and the order from left to right, starting from **1**. If only one port exists, the port number is **1**.

NOTE: Ports in each kind of modulars must be numbered sequently bottom from to top and from left to right.

1.2 Preparation Before Switch Startup

Do the following preparatory works before the switch is configured:

1. Set the switch's hardware according to the requirements of the manual.
2. Configure a PC terminal simulation program.
3. Determine the IP address layout for the IP network protocols.

1.3 Acquiring Help

Use the question mark (?) and the direction mark to help you enter commands:

- Enter a question mark. The currently available command list is displayed.

  Switch> ?

- Enter several familiar characters and press the space key. The available command list starting with the entered familiar characters is displayed.

  Switch> s?

- Enter a command, press the space key and enter the question mark. The command parameter list is displayed.

  Switch> show ?

- Press the “up” key and the commands entered before can be displayed. Continue to press the “up” key and more commands are to be displayed. After that, press the “down” key and the next command to be entered is displayed under the current command.

1.4 Command Modes

The command line interfaces for the switch can be classified into several modes. Each command mode enables you to configure different groupware. The command that can be used currently is up to the command mode where you are. You can enter the question mark in different command modes to obtain the available command list. Common command modes are listed in the following table:

Command Mode	Login Mode	Prompt	Exit Mode
System monitoring mode	Enter **Ctrl-p** after the power is on.	monitor#	Run **quit**.
User mode	Log in.	Switch>	Run **exit** or **quit**.
Management mode	Enter **enter** or **enable** in user mode.	Switch#	Run **exit** or **quit**.
Office configuration mode	Enter **config** in management mode.	Switch_config#	Run **exit** or **quit** or **Ctrl-z** to directly back to the management mode.
Port configuration mode	Enter the **interface** command in office configuration mode, such as **interface f0/1**.	Switch_config_f0/1#	Run **exit** or **quit** or **Ctrl-z** to directly back to the management mode.

Each command mode is unsuitable to subsets of some commands. If problem occurs when you enter commands, check the prompt and enter the question mark to obtain the available command list. Problem may occur when you run in incorrect command mode or you misspelled the command.

Pay attention to the changes of the interface prompt and the relative command mode in the following case:

Switch> enter

Password: <enter password>

Switch# config

Switch_config# interface f0/1

Switch_config_f0/1# quit

Switch_config# quit

Switch#

1.5 Canceling a Command

To cancel a command or resume its default properties, add the keyword “no” before most commands. An example is given as follows:

no ip routing

1.6 Saving Configuration

You need to save configuration in case the system is restarted or the power is suddenly off. Saving configuration can quickly recover the original configuration. You can run write to save configuration in management mode or office configuration mode.

Chapter 2 System Management Configuration

2.1 File Management Configuration

2.1.1 Managing the file system

The filename in flash is no more than 20 characters and filenames are case insensitive.

2.1.2 Commands for the file system

The boldfaces in all commands are keywords. Others are parameters. The content in the square brakcet "[ ]" is optional.

Command	Description
format	Formats the file system and delete all data.
dir [filename]	Displays files and directory names. The file name in the symbol "[]" means to display files starting with several letters. The file is displayed in the following format: Index number file name <FILE> lengthestablished time
delete filename	Deletes a file. The system will prompt if the file does not exist.
md dirname	Creates a directory.
rd dirname	Deletes a directory. The system will prompt if the directory is not existed.
more filename	Displays the content of a file. If the file content cannot be displayed by one page, it will be displayed by pages.
cd	Changes the path of the current file system.
pwd	Displays the current path.

2.1.3 Starting up from a file manually

monitor#boot flash *<local_filename>*

The previous command is to start a switch software in the flash, which may contain multiple switch software.

Parameter

Parameter	Description
Flash	A file stored in the flash memory.
local_filename	A file name stored in the flash memory Users must enter the file name.

Example

monitor#boot flash switch.bin

2.1.4 Updating software

User can use this command to download switch system software locally or remotely to obtain version update or the custom-made function version (like data encryption and so on).

There are two ways of software update in monitor mode.

1) Through TFTP

monitor#copy tftp flash: [ip_addr]

The previous commad is to copy file from the tftp server to the flash in the system. After you enter the command, the system will prompt you to enter the remote server name and the remote filename.

Parameter

Parameter	Description
flash	Store device in the flash memory.
ip_addr	IP address of the tftp server If there is no specified IP address, the system will prompt you to enter the IP address after the **copy** command is run.

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin.**

monitor#copy tftp flash

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

please wait ...

##

##

##

##

##

##

TFTP:successfully receive 3377 blocks ,1728902 bytes

monitor#

2.1.5 Updating configuration

The switch configuration is saved as a file, the filename is startup-config. You can use commands similar to software update to update the configuration.

1) Through TFTP

monitor#copy tftp flash startup-config

2.1.6 Using ftp to perform the update of software and configuration

switch #copy ftp {flash|cf} [ip_addr|option]

Use ftp to perform the update of software and configuration in formal program management. Use the **copy** command to download a file from ftp server to switch, also to upload a file from file system of the switch to ftp server. After you enter the command, the system will prompt you to enter the remote server name and remote filename.

copy{**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}|{**flash**<:filename>}

{{**flash**<:filename>}|**ftp**:[[[//login-name: [login-password]@]location] /directory]/filename} <blksize>〈mode〉〈type〉

Parameter

Parameter	Description
login-nam	Username of the ftp server If there is no specified username, the system will prompt you to enter the username after the **copy** command is run.
login-password	Password of the ftp server If there is no specified password, the system will prompt you to enter the password after the **copy** command is run.
nchecksize	The size of the file is not checked on the server.
blksize	Size of the data transmission block Default value: 512
ip_addr	IP address of the ftp server If there is no specified IP address, the system will prompt you to enter the IP address after executing the **copy** command.
active	Means to connect the ftp server in active mode.
passive	Means to connect the ftp server in passive mode.
type	Set the data transmission mode (ascii or binary)

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin**.

config#copy ftp flash

Prompt: ftp user name[anonymous]? login-nam

Prompt: ftp user password[anonymous]? login-password

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

or

config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin

##

##

FTP:successfully receive 3377 blocks ,1728902 bytes

config#

NOTE:

1) When the ftp server is out of service, the wait time is long. If this problem is caused by the tcp timeout time (the default value is 75s), you can configure the global command ip tcp synwait-time to modify the tcp connection time. However, it is not recommended to use it.

2) When you use ftp in some networking conditions, the rate of data transmission might be relatively slow. You can properly adjust the size of the transmission block to obtain the best effect. The default size is 512 characters, which guarantee a relatively high operation rate in most of the networks.

2.2 Basic System Management Configuration

2.2.1 Configuring Ethernet IP address

monitor#ip address <*ip_addr*> <*net_mask*>

This command is to configure the IP address of the Ethernet. The default IP address is 192.168.0.1, and the network mask is 255.255.255.0.

Parameter

Parameter	Description
ip_addr	IP address of the Ethernet
net_mask	Mask of the Ethernet

Example

monitor#ip address 192.168.1.1 255.255.255.0

2.2.2 Configuring default route

monitor#ip route default <*ip_addr*>

This command is used to configure the default route. You can configure only one default route.

Parameter

Parameter	Description
ip_addr	IP address of the gateway

Example

monitor#ip route default 192.168.1.1

2.2.3 Using ping to test network connection state

monitor#ping <*ip_address*>

This command is to test network connection state.

Parameter

Parameter	Description
ip_address	Destination IP address

Example

monitor#ping 192.168.20.100

PING 192.168.20.100: 56 data bytes

64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms

----192.168.20.100 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

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

Chapter 3 Terminal Configuration

3.1 VTY Configuration Introduction

The system uses the **line** command to configure terminal parameters. Through the command, you can configure the width and height that the terminal displays.

3.2 Configuration Task

The system has four types of lines: console, aid, asynchronous and virtual terminal. Different systems have different numbers of lines of these types. Refer to the following software and hardware configuration guide for the proper configuration.

Line Type	Interface	Description	Numbering
CON(CTY)	Console	To log in to the system for configuration.	0
VTY	Virtual and asynchronous	To connect Telnet, X.25 PAD, HTTP and Rlogin of synchronous ports (such as Ethernet and serial port) on the system	32 numbers starting from 1

3.2.1 Relationship between line and interface

1. Relationship between synchronous interface and VTY line

The virtual terminal line provides a synchronous interface to access to the system. When you connect to the system through VTY line, you actually connect to a virtual port on an interface. For each synchronous interface, there can be many virtual ports.

For example, if several Telnets are connecting to an interface (Ethernet or serial interface), you need to do the following steps for the VTY configuration:

1. Log in to the line configuration mode.
2. Configure the terminal parameters.

For VTY configuration, refer to Part 3.4 "VTY configuration example".

3.3 Monitor and Maintenance

Run **showline** to chek the VTY configuration.

3.4 VTY Configuration Example

It shows how to cancel the limit of the line number per screen for all VTYs without **more** prompt:

Switch_config# line vty 0 31

Switch_config_line# length 0

CHAPTER 4 SSH Configuration Commands

4.1 Introduction

4.1.1 SSH server

A scure and encrypted communication connection can be created between SSH client and the device through SSH server. The connection has telnet-like functions. SSH server supports the encryption algorithms including des, 3des and blowfish.

4.1.2 SSH client

SSH client is an application running under the ssh protocol. SSH client can provide authentication and encryption, so SSH client gurantees secure communication between communication devices or devices supporting SSH server even if these devices run in unsafe network conditions. SSH client supports the encryption algorithms including des, 3des and blowfish.

4.1.3 Function

SSH server and SSH client supports version 1.5. Both of them only support the shell application.

4.2 Configuration Tasks

4.2.1 Configuring the authentication method list

SSH server adopts the login authentication mode. SSH server uses the **default** authentication method list by default.
Run the following command in global configuration command mode to configure the authentication method list:

Command	Purpose
Ip sshd auth_method STRING	Configures the authentication method list. The length of the authentication method name is no more than 20 characters.

4.2.2 Configuring the access control list

To control the access to the device's SSH server, you need to configure the access control list for SSH server.
Run the following command in global configuration mode to configure the access control list:

Command	Purpose
Ip sshd access-class STRING	Configures the access control list. The length of the access control list name is no more than 19 characters.

4.2.3 Configuring the authentication timeout value

After a connection is established between client and server, server cuts off the connection if authentication cannot be approved within the set time.
Run the following command in global configuration mode to configure the configuration timeout value:

Command	Purpose
Ip sshd timeout <60-65535>	Configures the authentication timeout value.

4.2.4 Configuring the times of authentication retrying

If the times for failed authentications exceed the maximum times, SSH server will not allow you to retry authentication unless a new connction is established. The maximum times for retrying authentication is 6 by default.
Run the following command in global configuration mode to configure the maximum times for retrying authentication:

Command	Purpose
Ip sshd auth-retries <0-65535>	Configures the maximum times for retrying authentication.

4.2.5 Configuring the login silence period

When the failure login times exceed the threshold, the device enters the login silence period. The silence period is 60s.
Run the following command to configure the login silence period in the global configuration mode:

Command	Purpose
ip sshd silence-period <0-3600>	Configures the login silence period.

4.2.6 Configuring ssh server Version

By default, the SSH server supports login using both version 1 and version 2. It can be configured to only allow version 2 login and disable version 1 login.
Run the following command to configure the ssh server version in the global configuration mode:

Command	Purpose
ip sshd version 2	Configures the SSH server to only support version 2 login and prohibit version 1 login

4.2.7 Configuring encryption algorithms for ssh server

By default, the SSH server supports the following encryption algorithms:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr. This command will configure the SSH server to support the specified encryption algorithms.
To configure the SSH server's supported encryption algorithms, use the following command in global configuration mode:

Command	Purpose
ip sshd Ciphers STRING	Configures supported encryption algorithms for ssh server..

4.2.8 Configuring exchange algorithms for ssh server

By default, the SSH server supports the following key exchange algorithms.
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha256. This command will configure the SSH server to support the specified key exchange algorithms.
To configure the SSH server's supported key exchange algorithms, use the following command in global configuration mode:

Command	Purpose
ip sshd KexAlgorithms STRING	Configures key exchange algorithms for ssh server.

4.2.9 Configuring message authentication code (MAC) algorithms for ssh server

By default, the SSH server supports the following message authentication code (MAC) algorithms:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96,hmac-sha2-256.
This command will configure the SSH server to support the specified message authentication code (MAC) algorithms.
To configure the SSH server's supported message authentication code (MAC) algorithms, use the following command in global configuration mode:

Command	Purpose
ip sshd MACs STRING	Configures message authentication code (MAC) algorithms for ssh server.

4.2.10 Enabling sftp

Stp is a security file transmission system based on the ssh protocol whose authentication and data transmission are encrypted. Though its transmition rate is slow, it has a strong network security.
Sftp is diabled by default. Run the following command to enable sftp in the global configuration mode:

Command	Purpose
ip sshd sftp	Enables sftp.

4.2.11 Enabling sshd

It takes one to two minutes to calculate the initial password when enabling ssh server. The initial password will be saved in **flash** when enabling the function. The device will read the encryption key from **flash** when reenabling ssh server. Thus, the start time is shortened.
The sshd (encryption key saving) is disabled by default. Run the following command to enable sshd (encryption key saving) in the global configuration mode:

Command	Purpose
ip sshd save	Enables sshd

4.2.12 Enabling SSH server

SSH server is disabled by default. When SSH server is enabled, the device will generate a rsa password pair, and then listen connection requests from the client. The process takes one or two minutes.
Run the following command in global configuration mode to enable SSH server:

Command	Purpose
Ip sshd enable	Enables SSH server. The digit of the password is 1024.

4.3 SSH server Configuration Example

The following configuration only allows the host whose IP address is 192.168.20.40 to access SSH server. The local user database is used to distinguish user ID.

4.3.1 Access control list

ip access-list standard ssh-acl

permit 192.168.20.40

4.3.2 Global configuration

aaa authentication login ssh-auth local

ip sshd auth-method ssh-auth

ip sshd access-class ssh-acl

ip sshd enable

Chapter 5 Network Management Configuration

5.1 Configuring SNMP

5.1.1 Introduction

The SNMP system includes the following parts:

- SNMP management side (NMS)
- SNMP agent (AGENT)
- Management information base (MIB)

SNMP is a protocol working on the application layer. It provides the packet format between SNMP management side and agent.

SNMP management side can be part of the network management system (NMS, like CiscoWorks). Agent and MIB are stored on the system. You need to define the relationship between network management side and agent before configuring SNMP on the system.

SNMP agent contains MIB variables. SNMP management side can check or modify value of these variables. The management side can get the variable value from agent or stores the variable value to agent. The agent collects data from MIB. MIB is the database of device parameter and network data. The agent also can respond to the loading of the management side or the request to configure data. SNMP agent can send trap to the management side. Trap sends alarm information to NMS indicating a certain condition of the network. Trap can point out improper user authentication, restart, link layer state (enable or disable), close of TCP connection, lose of the connection to adjacent systems or other important events.

1. SNMP notification

When some special events occur, the system will send 'inform' to SNMP management side. For example, when the agent system detects an abnormal condition, it will send information to the management side.

SNMP notification can be treated as trap or inform request to send. Since the receiving side doesn't send any reply when receiving a trap, this leads to the receiving side cannot be sure that the trap has been received. Therefore the trap is not reliable. In comparison, SNMP management side that receives "inform request" uses PDU that SNMP echoes as the reply for this information. If no "inform request" is received on the management side, no echo will be sent. If the receiving side doesn't send any reply, then you can resend the "inform request". Then notifications can reach their destination.

Since inform requests are more reliable, they consume more resources of the system and network. The trap will be discarded when it is sent. The "inform request" has to be stored in the memory until the echo is received or the request timeouts. In addition, the trap is sent only once, while the "inform request" can be resent for many times. Resending "inform request" adds to network communications and causes more load on network. Therefore, trap and inform request provide balance between reliability and resource. If SNMP management side needs receiving every notification greatly, then the "inform request" can be used. If you give priority to the communication amount of the network and there is no need to receive every notification, then trap can be used.

This switch only supports trap, but we provide the extension for "inform request".

2. SNMP version

System of our company supports the following SNMP versions:

- SNMPv1---simple network management protocol, a complete Internet standard, which is defined in RFC1157.
- SNMPv2C--- Group-based Management framework of SNMPv2, Internet test protocol, which is defined in RFC1901.

Layer 3 switch of our company also supports the following NMP:

- SNMPv3--- a simple network management protocol version 3, which is defined in RFC3410.

SNMPv1 uses group-based security format. Use IP address access control list and password to define the management side group that can access to agent MIB.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- Message integrity — Ensuring that a packet has not been tampered with in-transit.
- Authentication — Determining the message is from a valid source.
- Encryption — Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available, that is, authentication and encryption, authentication and no encryption, no authentication.

You need to configure SNMP agent to the SNMP version that the management working station supports. The agent can communicate with many management sides.

3. Supported MIB

SNMP of our system supports all MIBII variables (which will be discussed in RFC 1213) and SNMP traps (which will be discussed in RFC 1215).

Our system provides its own MIB extension for each system.

5.1.2 SNMP Configuration Tasks

SNMP configuration commands include:

- Configuring SNMP view
- Creating or modifying the access control for SNMP community
- Configuring the contact method of system administrator and the system's location
- Defining the maximum length of SNMP agent data packet
- Monitoring SNMP state
- Configuring SNMP local engine
- Configuring SNMP trap
- Configuring SNMPv3 group
- Configuring SNMPv3 user
- Configuring snmp-server encryption
- Configuring snmp-server trap-source
- Configuring snmp-server trap-timeout
- Configuring snmp-server trap-add-hostname
- Configuring snmp-server trap-logs
- Configuring snmp -dos-max retry times
- Configuring keep-alive times

- Configuring snmp-server necode
- Configuring snmp-server event-id
- Configuring snmp-server getbulk-timeout
- Configuring snmp-server getbulk-delay
- Showing snmp running information
- Showing snmp debug information

1. Configuring SNMP view

The SNMP view is to regulate the access rights (include or exclude) for MIB. Use the following command to configure the SNMP view.

Command	Purpose
snmp-server view *name oid* [excluded | included]	Adds the subtree or table of OID-specified MIB to the name of the SNMP view, and specifies the access right of the object identifier in the name of the SNMB view.

The subsets that can be accessed in the SNMP view are the remaining objects that "include" MIB objects are divided by "exclude" objects. The objects that are not configured are not accessible by default.
After configuring the SNMP view, you can implement SNMP view to the configuration of the SNMP group name, limiting the subsets of the objects that the group name can access.

2. Creating or modifying the access control for SNMP community

You can use the SNMP community character string to define the relationship between SNMP management side and agent. The community character string is similar to the password that enables the access system to log in to the agent. You can specify one or multiple properties relevant with the community character string. These properties are optional:
Allowing to use the community character string to obtain the access list of the IP address at the SNMP management side
Defining MIB views of all MIB object subsets that can access the specified community
Specifying the community with the right to read and write the accessible MIB objects
Configure the community character string in global configuration mode using the following command:

Command	Purpose
snmp-server community [0|7] string [**view** *view-name*] [**ro | rw**] [*word*]	Defines the group access character string.

You can configure one or multiple group character strings. Run command "no snmp-server community" to remove the specified community character string.
For how to configure the community character string, refer to the part "SNMP Commands".

3. Configuring the contact method of system administrator and the system's location

SysContact and sysLocation are the management variables in the MIB's system group, respectively defining the linkman's

identifer and actual location of the controlled node. These information can be accessed through config. files. You can use the following commands in global configuration mode.

Command	Purpose
snmp-server contact *text*	Sets the character string for the linkman of the node.
snmp-server location *text*	Sets the character string for the node location.

4. Defining the maximum length of SNMP agent data packet

When SNMP agent receives requests or sends response, you can configure the maximum length of the data packet. Use the following command in global configuration mode:

Command	Purpose
snmp-server packetsize *byte-count*	Sets the maximum length of the data packet.

5. Monitoring SNMP state

You can run the following command in global configuration mode to monitor SNMP output/input statistics, including illegal community character string items, number of mistakes and request variables.

Command	Purpose
show snmp	Monitor the SNMP state.

6. Configuring SNMP local engine

Use the following command to configure the system to send the SNMP local engine:

Command	Purpose
snmp-server engineID local *engineID*	Configuring SNMP local engine

7. Configuring SNMP trap

Use the following command to configure the system to send the SNMP traps (the second task is optional):

- Configuring the system to send trap

Run the following commands in global configuration mode to configure the system to send trap to a host.

Command	Purpose
snmp-server host|hostv6 host community-string [trap-type]	Specifies the receiver of the trap message.

snmp-server host|hostv6 *host* [vrf *word*] [udp-port *port-num*] [permit|deny *event- id*] {{version [v1 | v2c | v3]} | {[informs | traps] | [auth **|noauth]}}** community-string/user [authentication| configure| snmp]	Specifies the receiver, version number and username of the trap message.

When the system is started, the SNMP agent will automatically run. All types of traps are activated. You can use the command snmp-server host to specify which host will receive which kind of trap.

Some traps need to be controlled through other commands. For example, if you want SNMP link traps to be sent when an interface is opened or closed, you need to run snmp trap link- status in interface configuration mode to activate link traps. To close these traps, run the interface configuration command snmp trap link-stat.

You have to configure the command snmp-server host for the host to receive the traps.

- Modifying the running parameter of the trap

As an optional item, it can specify the source interface where traps originate, queue length of message or value of resending interval for each host.

To modify the running parameters of traps, you can run the following optional commands in global configuration mode.

Command	Purpose
snmp-server trap-source *interface*	Specifies the source interface where traps originate and sets the source IP address for the message.
snmp-server queue-length *length*	Creates the queue length of the message for each host that has traps. Default value: 10
snmp-server trap-timeout *seconds*	Defines the frequency to resend traps in the resending queue. Default value: 30 seconds

8. Configuring the SNMP binding source address

Run the following command in the global configuration mode to set the source address for the SNMP message.

Command	Purpose
snmp source-addr *ipaddress*	Set the source address for the SNMP message.

9. Configuring snmp-server udp-port

Run the following command in the global mode to configure snmp-server udp-port.

Command	Purpose
snmp-server udp-port *portnum*	Set SNMP server udp-port number

10. Configuring SNMPv3 group

Run the following command to configure a group.

Command	Purpose
snmp-server group [*groupname* { **v3** [**auth	noauth	priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]	Configure a SNMPv3 group. You can only read all items in the subtree of the Internet by default.

11. Configuring SNMPv3 user

You can run the following command to configure a local user. When an administrator logs in to a device, he has to user the username and password that are configured on the device. The security level of a user must be higher than or equals to that of the group which the user belongs to. Otherwise, the user cannot pass authentication.

Command	Purpose
snmp-server user *username groupname* {v3 [encrypted|auth] [md5|sha] *auth-password*}	Configures a local SNMPv3 user.

12. Configuring snmp-server encryption

You can run the following command in global configuration mode to configure snmp-server encryption. Use ciphertext to show SHA password and MD5 password. The command is one-off and it cannot be cancelled with command “NO”.

Command	Purpose
snmp-server encryption	Use ciphertext to show SHA password and MD5 password.

13. Configuring snmp-server trap-source

You can run the following command in global configuration mode to configure snmp-server trap-source. Use command “no” to delete such an interface.

Command	Purpose
snmp-servertrap-source interface	Any SNMP server is with a trap address no matter from which interface SNMP server sends the SNMP trap.

14. Configuring snmp-server trap-timeout

You can run the following command in global configuration mode to configure snmp-server trap-timeout.

Command	Purpose
snmp-server trap-timeout *seconds*	Before sending the trap, the switch software will find the route of the destination address. If there is no route, the trap will be saved into the retransmission queue. The command “server trap-timeout” determines the retransmission interval.

15. Configuring snmp-server trap-add-hostname

Run the following command to configure snmp-server trap-add-hostname.

Command	Purpose
snmp-server trap-add-hostname	In a specific time, the network management host needs to locate which host the trap comes from.

16. Configuring snmp-server trap-logs

Using the following command to configure snmp-server trap-logs.

Command	Purpose
snmp-server trap-logs	Enable snmp-servertrap-logs to record the forwarding record of trap as logs.

17. Configuring snmp -dos-max retry times

Set password retry times for logging in snmp in five minutes.

Command	Purpose
snmp-server set-snmp-dos-max *retry times*	Setpasswordretrytimesfor logging in snmp in five minutes.

It should be used cooperatively with snmp-server host.

18. Configuring keep-alive times

You can run the following command in global configuration mode to configure snmp-server keep-alive times.

Command	Purpose
snmp-server keep-alive *times*	Send keep-alive times regularly to the trap host.

19. Configuring snmp-server encode

You can run the following command in global configuration mode to configure snmp-server encode information (This is the only tag of the device.). Use command “no” to remove the tag information.

Command	Purpose
snmp-server necode *text*	Corresponds to snmp private MIB variables.

20. Configuring snmp-server event-id

You can run the following command in global configuration mode to configure snmp-server event-id. Use Command "no" to delete the configuration.

Command	Purpose
snmp-server event-id *number* trap-oid *oid*	It is used in host configuration and for filtering in forwarding trap.

21. Configuring snmp-server getbulk-timeout

You can run the following command in global configuration mode to configure snmp-server getbulk-timeout. If it is timeout, all request from getbulk will not be deal with. Use command "no" to delete the configuration.

Command	Purpose
snmp-servergetbulk-timeout seconds	Set getbulk-timeout. If it is timeout, all request from getbulk will not be deal with.

22. Configuring snmp-server getbulk-delay

You can run the following command in global configuration mode to configure snmp-server getbulk-delay. Unit is centisecond. Use the no form of the command to delete.

Command	Purpose
snmp-servergetbulk-delay ticks	To avoid snmp occupies excessive CPU,set snmp- server getbulk-delay ticks. Unit: centisecond.

23. Showing snmp running information

Use the show snmp command to monitor SNMP input and output statistics, including illegal community string entries, errors, and the number of request variables. Use the show snmp engineID command to display SNMP engine information. Use the show snmp host command to display SNMP trap host information. Use the show snmp view command to display SNMP view information. Use the show snmp mibs command to display mib registration information. Use the show snmp group command to display SNMP group information. Use the show snmp user command to display SNMP user information.

Command	Purpose
show snmp engineID	Show SNMP trap local engine information.
show snmp *host*	Show SNMP trap host information.
show snmp *view*	Show snmp view information.
show snmp *mibs*	Show snmp mibs registration information.
show snmp *group*	Show snmp group information
show snmp *user*	Show snmp user information.

24. Showing snmp debug information

Showing information about SNMP error, snmp event and snmp packet.

Command	Purpose
debug snmp *error*	Enable the debug switch of SNMP error.
debug snmp *event*	Enable the debug switch of snmp event.
debug snmp *packet*	Enable the debug switch of snmp packet

5.1.3 Configuration Example

1. Example 1

snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.10.2 public

The above example shows:

How to set the community string public that can only read all MIB variables. How to set the community string private that can read and write all MIB variables. The above command specifies the community string public to send traps to 192.168.10.2 when a system requires to send traps. For example, when a port of a system is in the down state, the system will send a linkdown trap information to 192.168.10.2.

2. Example 2

snmp-server group getter v3 auth

snmp-server group setter v3 priv write v-write

snmp-server user get-user getter v3 auth sha 12345678

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

snmp-server view v-write internet included

The above example shows how to use SNMPv3 to manage devices. Group **getter** can browse device information, while group **setter** can set devices. User **get-user** belongs to group **getter** while user **set-user** belongs to group **setter**. For user get-user, its security level is authenticate but not encrypt, its password is 12345678, and it uses the **sha** arithmetic to summarize the password. For user set-user, its security level is authenticate and encrypt, its password is 12345678, and it uses the **md5** arithmetic to summarize the password.

5.2 RMON Configuration

5.2.1 RMON Configuration Task

RMON configuration tasks include:

- Configuring the rMon alarm function for the switch
- Configuring the rMon event function for the switch
- Configuring the rMon statistics function for the switch
- Configuring the rMon history function for the switch

- Displaying the rMon configuration of the switch

1. Configuring rMon alarm for switch

You can configure the rMon alarm function through the command line or SNMP NMS. If you configure through SNMP NMS, you need to configure the SNMP of the switch. After the alarm function is configured, the device can monitor some statistic value in the system. The following table shows how to set the rMon alarm function:

Command	Purpose
config	Enter the global configuration mode.
rmon alarm index variable *interval* {absolute | delta} rising-threshold *value* [*eventnumber*] falling-threshold *value* [*eventnumber*] [owner *string*] [repeat]	Add an rMon alarm item. **index** is the index of the alarm item. Its effective range is from 1 to 65535. **variable** is the object in the monitored MIB. It must be an effective MIB object in the system. Only objects in the Integer, Counter, Gauge or Time Ticks type can be detected. **interval** is the time section for sampling. Its unit is second.Its effectivevalue is from 1to 2147483647. **absolute** is used to directly monitor the value of MIB object. **Delta** is used to monitor the value change of the MIB objects between two sampling. **value** is the threshold value when an alarm is generated. **Event number** is the index of an event that is generated when a threshold is reached. Event number is optional. **Owner string** is to describe the information about the alarm. **Repeat** is to repeat trigger event.
exit	Enter the management mode again.
write	Save the configuration.

After a rMon alarm item is configured, the device will obtain the value of variable-specified oid after an interval. The obtained value will be compared with the previous value according to the alrm type (absolute or delta). If the obtained value is bigger than the previous value and surpasses the threshold value specified by rising-threshold, an event whose index is eventnumber (If the value of eventnumber is 0 or the event whose index is eventnumber does not exist in the event table, the event will not occur). If the variable-specified oid cannot be obtained, the state of the alarm item in this line is set to invalid. If you run rmon alarm many times to configure alarm items with the same index, only the last configuration is effective. You can run no rmon alarm index to cancel alarm items whose indexes are index.

2. Configuring rMon event for switch

The steps to configure the rMon event are shown in the following table:

Step	Command	Purpose
1.	config	Enter the global configuration mode.
2.	rmon event index [description *string*] [log] [owner *string*] [trap community] [ifctrl *interface*]	Add a rMon event item. **index** means the index of the event item. Its effective range is from 1 to 65535. **description** means the information about the event. **log** means to add a piece of information to the log table when a event is triggered. **trap** means a trap message is generated when the event is triggered.

		community means the name of a community. **ifctrl interface** is the interface controlling event shutdown. **owner string** is to describe the information about the alarm.
3.	exit	Enter the management mode again.
4.	write	Save the configuration.

After a rMon event is configured, you must set the domain eventLastTimeSent of the rMon event item to sysUpTime when a rMon alarm is triggered. If the log attribute is set to the rMon event, a message is added to the log table. If the trap attribute is set to the rMon event, a trap message is sent out in name of community. If you run rmon event many times to configure event items with the same index, only the last configuration is effective. You can run no rmon event index to cancel event items whose indexes are index.

3. Configuring rMon statistics for switch

The rMon statistics group is used to monitor the statistics information on every port of the device.
The steps to configure the rMon statistics are as follows:

Step	Command	Purpose
1.	config	Enter the global configuration mode.
2.	interface iftype ifid	Enter the port mode. iftype means the type of the port. ifid means the ID of the interface.
3.	rmon collection stats index [owner *string*]	Enable the statistics function on the port. **index** means the index of the statistics. **owner string** is to describe the information about the statistics.
4.	exit	Enter the global office mode.
5.	exit	Enter the management mode again.
6.	write	Save the configuration.

If you run rmon collection stat many times to configure statistics items with the same index, only the last configuration is effective. You can run no rmon collection stats index to cancel statistics items whose indexes are index.

4. Configuring rMon history for switch

The rMon history group is used to collect statistics information of different time sections on a port in a device. The rMon statistics function is configured as follows:

Step	Command	Purpose
1.	config	Enter the global configuration command.
2.	interface iftype ifid	Enter the port mode. **iftype** means the type of the port. **ifid** means the ID of the interface.

3.	rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]	Enable the history function on the port. **index** means the index of the history item. Among all data collected by history item, the latest bucket-number items need to be saved. You can browse the history item of the Ethernet to obtain these statistics values. The default value is 50 items. **second** means the interval to obtain the statistics data every other time. The default value is 1800 seconds. **owner string** is used to describe some information about the history item.
4.	exit	Enter the global office mode again.
5.	exit	Enter the management mode again.
6.	write	Save the configuration.

After a rMon history item is added, the device will obtain statistics values from the specified port every second seconds. The statistics value will be added to the history item as a piece of information. If you run rmon collection history index many times to configure history items with the same index, only the last configuration is effective. You can run no rmon history index to cancel history items whose indexes are index.

NOTE: Too much system sources will be occupied in the case the value of bucket-number is too big or the value of interval second is too small.

5. Displaying rMon configuration of switch

Run show to display the rMon configuration of the switch.

Command	Purpose
show rmon [alarm] [event] [statistics] [history]	Displays the rmon configuration information. **alarm** means to display the configuration of the alarm item. **event** means to show the configuration of the event item and to show the items that are generated by the occurrence of events and are contained in the log table. **statistics** means to display the configuration of the statistics item and statistics values that the device collects from the port. **history** means to display the configuration of the history item and statistics values that the device collects in the latest specified intervals from the port.

Chapter 6 AAA Configuration

6.1 AAA Overview

Access control is used to control the users to access OLT or NAS and to limit their service types. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your OLT or access server.

6.1.1 AAA Security Service

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- Authentication: It is a method of identifying users, including username/password inquiry and encryption according to the chosen security protocol.

  Authentication is a method to distinguish the user's identity before users access the network and enjoy network services. AAA authentication can be configured through the definition of an authentication method list and then application of this method list on all interfaces. This method list defines the authentication type and the execution order; any defined authentication method list must be applied on a specific interface before it is executed. The only exception is the default authentication method list (which is named default). If there are no other authentication method lists, the default one will be applied on all interfaces automatically. If anyone is defined, it will replace the default one. For how to configure all authentications, see "Authentication Configuration".

- Authorization: it is a remote access control method to limit user's permissions.

  AAA authorization takes effect through a group of features in which a user is authorized with some permissions. Firstly, the features in this group will be compared with the information about a specific user in the database, then the comparison result will be returned to AAA to confirm the actual permissions of this user. This database can be at the accessed local server or OLT, or remote Radius/TACACS+ server. The Radius or TACACS+ server conducts user authorization through a user-related attribute-value peer. The attribute value (AV) defines the allowably authorized permissions. All authorization methods are defined through AAA. Like authentication, an authorization method list will be first defined and then this list will be applied on all kinds of interfaces. For how to carry on the authorization configuration, see "Authorization Configuration".

- Accounting: it is a method to collect user's information and send the information to the security server. The collected information can be used to open an account sheet, make auditing and form report lists, such as the user ID, start/end time, execution commands, and the number of packets or bytes.

  The accounting function can track the services that users access, and at the same time track the service-consumed network resource number. When AAA accounting is activated, the access server can report user's activities to the TACACS+ or Radius server in way of accounting. Each account contains an AV peer, which is stored on the security server. The data can be used for network management, client's accounting analysis or audit. Like authentication and authorization, an accounting method list must be first defined and then applied on different interfaces. For how to carry on the accounting configuration, see "Accounting Configuration".

6.1.2 Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS, TACACS+
- Multiple backup systems

6.1.3 AAA Principles

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

6.1.4 AAA Method List

To configure AAA, define a named method list first and then apply it to the concrete service or interface. This method list defines the running AAA type and their running sequence. Any defined method list must be applied to a concrete interface or service before running. The only exception is the default method list. The default method list is automatically applied to all interfaces or services. Unless the interface applies other method list explicitly, the method list will replace the default method list.

A method list is a sequential list that defines the authentication methods used to authenticate a user. In AAA method list you can specify one or more security protocols. Thus, it provides with a backup authentication system, in case the initial method is failed. Our switch software uses the first method listed to authenticate users; if that method does not respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

It is important to notice that the switch software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local user name database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

The following figures shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. Take the authentication as an example to demonstrate the relation between AAA service and AAA method list.

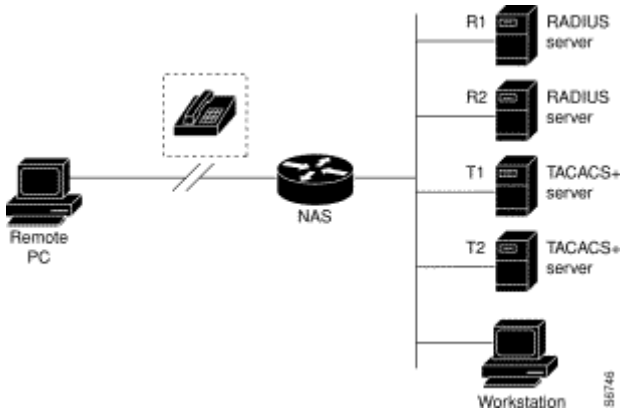


Figure 6-1 Typical AAA Network Configuration

In this example, default is the name of the method list, including the protocol in the method list and the request sequence of the method list follows the name. The default method list is automatically applied to all interfaces.

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Suppose the system administrator wants to apply the method list to a certain or a specific port. In such case, the system administrator should create a non-default method list and then apply the list of this name to an appropriate port.

6.1.5 AAA Configuration Process

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack. Before you configure AAA, you need know the basic configuration procedure. To do AAA security configuration on XXCOM OLT or access servers, perform the following steps:

- If you decide to use a security server, configure security protocol parameters first, such as RADIUS, TACACS+.
- Define the method lists for authentication by using an AAA authentication command.
- Apply the method lists to a particular interface or line, if required.
- (Optional) Configure authorization using the AAA authorization command.
- (Optional) Configure accounting using the AAA accounting command.

6.2 Authentication Configuration

6.2.1 AAA Authentication Configuration Task List

- Configuring Login Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- Modifying the Notification Character String for Username Input
- Modifying AAA authentication password-prompt
- Creating local user name authentication database

6.2.2 AAA Authentication Configuration Task

General configuration process of AAA authentication

To configure AAA authentication, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+.

Refer to the relevant section for the concrete configuration methods.

(2) Configuring Authentication Method List Using aaa authentication

(3) If necessary, apply the accounting method list to a specific interface or line.

1. Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the aaa authentication login command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the aaa authentication login command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command. After the authentication method lists are configured, you can apply these lists by running login authentication. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	Enables AAA globally.
line { **console** | **vty** } line-number [ending-line-number]	Enter the configuration mode of a line.
login authentication {default | *list-name*}	Applies the authentication list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The key word method specifies the actual method of the authentication method. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

aaa authentication login default group radius

NOTE: Because the keyword none enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

If you cannot find the authentication method list, you can only login through the console port. Any other way of login is in accessible.

The following table lists the supported login authentication methods:

Keyword	Notes:
enable	Uses the enable password for authentication.
group *name*	Uses named server group for authentication.

group radius	Uses RADIUS for authentication.
group tacacs+	Uses group tacacs+ for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
localgroup	Uses the local strategy group username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Passes the authentication unconditionally.

(1) Login Authentication Using Enable Password

Use the aaa authentication login command with the enable method keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default enable

(2) Login Authentication Using Line Password

Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default line

Before you can use a line password as the login authentication method, you need to define a line password.

3. Login Authentication Using Local Password

Use the aaa authentication login command with the local method keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default local

For information about adding users into the local username database, refer to the section "Establishing Username Authentication" in this chapter.

4. Login Authentication Using Group RADIUS

Use the aaa authentication login command with the group radius method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default group radius

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter "Configuring RADIUS."

2. Enabling Password Protection at the Privileged Level

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line. Use the following command in global configuration mode:

Command	Purpose
aaa authentication enable default method1 [method2...]	Enables user ID and password checking for users requesting privileged EXEC level.

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered. The following table lists the supported enable authentication methods:

Keyword	Notes
enable	Uses the enable password for authentication.
group group-name	Uses named server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses tacacs+ for authentication.
line	Uses the line password for authentication.
none	Passes the authentication unconditionally.

When configuring enable authentication method as the remote authentication, use RADIUS for authentication. Do as follows:

(1) Uses RADIUS for enable authentication:

The user name for authentication is $ENABLE*level*$; level is the privileged level the user enters, that is, the number of the privileged level after enable command. For instance, if the user wants to enter the privileged level 7, enter command enable 7; if configuring RADIUS for authentication, the user name presenting to Radius-server host is $ENABLE7$; the privileged level of enable is 15 by default, that is, the user name presenting to Radius-server host in using RADIUS for authentication is $ENABLE15$. The user name and the password need to configure on Radius-server host in advance. The point is that in user database of Radius-server host, the Service-Type of the user specifying the privileged authentication is 6, that is, Admin-User.

3. Configuring Message Banners for AAA Authentication

The banner of configurable, personal logon or failed logon is supported. When AAA authentication fails during system login, the configured message banner will be displayed no matter what the reason of the failed authentication is.

- Configuring the registration banner

Run the following command in global configuration mode.

Command	Purpose
aaa authentication banner delimiter text-string delimiter	Configures a personal logon registration banner.

- Configuring the banner of failed logon

Run the following command in global configuration mode.

Command	Purpose
aaa authentication fail-message *delimiter text-string delimiter*	Configures a personal banner about failed logon.

- Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is ended.

4. Modifying the Notification Character String for Username Input

To modify the default text of the username input prompt, run aaa authentication username-prompt. You can run no aaa authentication username-prompt to resume the password input prompt.

username:

The aaa authentication username-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command in global configuration mode:

Command	Purpose
aaa authentication username-prompt *text-string*	Modifies the default text of the username input prompt.

5. Modifying AAA authentication password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt command. To return to the default password prompt text, use the no form of this command. You can run no aaa authentication username-prompt to resume the password input prompt.

password:

The aaa authentication password-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command in global configuration mode:

Command	Purpose
aaa authentication password-prompt *text-string*	String of text that will be displayed when the user is prompted to enter a password.

6. Creating the Authentication Database with the Local Privilege

To create the enable password database with the local privilege level, run **enable password** in global configuration mode. To cancel the enable password database, run **no enable password.**

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

no enable password [level *level*]

6.2.3 AAA Authentication Configuration Example

1. RADIUS Authentication Example

The following example shows how to configure the OLT to authenticate and authorize using RADIUS:

aaa authentication login radius-login group radius local

aaa authorization network radius-network group radius

line vty 3

login authentication radius-login

The meaning of each command line is shown below:

- The aaa authentication login radius-login group radius local command configures the OLT to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The aaa authorization network radius-network group radius command queries RADIUS for network authorization, address assignment, and other access lists.
- The login authentication radius-login command enables the radius-login method list for line 3.

6.3 Authorization Configuration

6.3.1 AAA Authorization Configuration Task List

- Configuring EXEC authorization through AAA

6.3.2 AAA Authorization Configuration Task

General configuration process of AAA authorization

To configure AAA authorization, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

5. Run aaa authorization to define the authorization method list. The authorization service is not provided by default.

6. If necessary, apply the accounting method list to a specific interface or line.

1. Configuring EXEC authorization through AAA

To enable AAA authorization, run aaa authorization. The aaa authorization exec command can create one or several authorization method lists and enable the EXEC authorization to decide whether the EXEC hull program is run by the users or not, or decide whether the users are authorized with the privilege when entering the EXEC hull program. After the

authorization method lists are configured, you can apply these lists by running login authorization. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authorization exec {**default** | *list-name*}*method1* [*method2*...]	Creates the global authorization list.
line [**console** | **vty**] line-number [ending-line-number]	Enter the configuration mode of a line.
login authorization {default | *list-name*}	Applies the authorization list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the authorization process. Only when the previously-used method returns the authorization error can other authorization methods be used. If the authorization fails because of the previous method, other authorization methods will not be used. If you requires the EXEC shell to be entered even when all authorization methods returns the authorization errors, designate none as the last authorization method in the command line.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, you can run the following command to designate RADIUS as the default authorization method of EXEC:

aaa authorization exec default group radius

NOTE:

If the authorization method list cannot be found during authorization, the authorization will be directly passed without the authorization service conducted.

The following table lists currently-supported EXEC authorization methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct authorization.
group radius	Uses RADIUS authorization.
group tacacs+	Uses tacacs+ authorization.
local	Uses the local database to perform authorization.
if-authenticated	Automatically authorizes the authencated user with all required functions.
none	Passes the authorization unconditionally.

6.3.3 AAA Authorization Examples

1. Example of Local EXEC Authorization

The following example shows how to perform the local authorization and local authorization by configuring the OLT:

aaa authentication login default local

aaa authorization exec default local

!

localauthor a1

exec privilege default 15

!

local author-group a1

username exec1 password 0 abc

username exec2 password 0 abc author-group a1

username exec3 password 0 abc maxlinks 10

username exec4 password 0 abc autocommand telnet 172.16.20.1

!

The following shows the meaning of each command line:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.
- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- Command localauthor al defines a local authority policy named al. Command exec privilege default 15 means the privileged level of exec login user is 15 by default.
- Command local author-group a1 means apply the local authorization policy a1 to global configuration (the default local policy group).
- Command username exec1 password 0 abc defines an account exec1 with password abc in the global configuration mode.
- Command username exec2 password 0 abc author-group a1 defines an account exec 2 with password abc in the global configuration mode. The account is applied to the local authorization policy a1.
- Command username exec3 password 0 abc maxlinks 10 defines an account exec 3 with password abc in the global configuration mode. The account makes 10 users available simultaneously.
- Command username exec4 password 0 abc autocommand telnet 172.16.20.1 defines an account exec4 with password abc. telnet 172.16.20.1 is automatically run when the user login the account.

6.4 AAA Accounting Configuration

6.4.1 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA
- Configuring Accounting Update using AAA
- Accounting Suppress Null-username

6.4.2 AAA Accounting Configuration Task

General configuration process of AAA accounting

To configure AAA accounting, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

7. Apply the method lists to a particular interface or line, if required. The accounting service is not provided by default.

8. If necessary, apply the accounting method list to a specific interface or line.

1. Configuring Connection Accounting Using AAA

To enable AAA accounting, run command aaa accounting. To create a or multiple method list(s) to provide accounting information about all outbound connections made from the OLT, use the aaa accounting connection command. The outbound connections include Telnet, PAD, H323 and rlogin. Only H323 is supported currently. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting connection {default | *list-name*} {{{start-stop | stop-only} group *groupname*} | none}	Establishes the global accounting list.

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the accounting process.

The following table lists currently-supported connection accounting methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct accounting.
group radius	Uses the RADIUS for accounting.
group tacacs+	Uses the TACACS+ for accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

2. Configuring Network Accounting using AAA

To enable AAA accounting, run command aaa accounting. The aaa accounting network command can be used to establish one or multiple accounting method lists. The network accounting is enabled to provide information to all PPP/SLIP sessions, these information including packets, bytes and time accounting. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting network {default | *list-name*} {{{start-stop | stop-only} group *groupname}* | none}	Establishes the global accounting list.

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the accounting process.

The following table lists currently-supported network accounting methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct accounting.
group radius	Uses the RADIUS for accounting.
group tacacs+	Uses the TACACS+ for accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

3. Configuring Accounting Update through AAA

To activate the AAA accounting update function for AAA to send the temporary accounting record to all users in the system, run the following command: You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting update [newinfo] [periodic *number*]	Enables AAA accounting update.

If the newinfo keyword is used, the temporary accounting record will be sent to the accounting server when there is new accounting information to be reported. For example, after IPCP negotiates with the IP address of the remote terminal, the temporary accounting record, including the IP address of the remote terminal, will be sent to the accounting server.

When the periodic keyword is used, the temporary accounting record will be sent periodically. The period is defined by the number parameter. The temporary accounting record includes all accounting information occurred before the accounting record is sent.

The two keywords are contradictable, that is, the previously-configured parameter will replace the latter-configured one. For example, if aaa accounting update periodic and then aaa accounting update new info are configured, all currently-registered users will generate temporary accounting records periodically. All new users have accounting records generated according to the new info algorithm.

4. Limiting User Accounting Without Username

To prevent the AAA system from sending the accounting record to the users whose username character string is null, run the following command in global configuration mode:

aaa accounting suppress null-username

6.5 Local Account Policy Configuration

6.5.1 Local Account Policy Configuration Task List

- Local authentication policy configuration
- Local authorization policy configuration
- Local password policy configuration
- Local policy group configuration

6.5.2 Local Account Policy Configuration Task

1. Local authentication policy configuration

To enter local authentication configuration, run command localauthen WORD in global configuration mode.

(1) The max login tries within a certain time

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

The configured local authentication policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

2. Local authorization policy configuration

To enter local authorization configuration, run command localauthor *WORD* in global configuration mode.

(1) To authorize priority for login users.

exec privilege {default | console | ssh | telnet} *<1-15>*

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

3. Local password policy configuration

To enter local authorization configuration, run command localpass *WORD* in global configuration mode.

(1) The password cannot be the same with the user name

non-user

(2) The history password check (The new password cannot be the same with the history password. The history password record is 20.)

non-history

(3) Specify the components of the password (complicate the password)

element [number] [lower-letter] [upper-letter] [special-character]

(4) Specify the components of the password (complicate the password)

min-length *<1-127>*

(5) password validity period (the validity of the password)

validity 1d2h3m4s

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

4. Local policy group configuration

To configure the local group policy, use the **localgroup WORD** command in global configuration mode. (The global configuration mode is considered as the default local policy configuration mode).

(1) local authentication configuration: apply the configured local authentication policy to the policy group

local authen-group *WORD*

(2) local authorization configuration: apply the configured local authorization policy to the policy group

local author-group *WORD*

(3) local password configuration: apply the configured local password policy to the policy group

local pass-group *WORD*

(4) local account configuration: set the max links and freeze for the policy group

local user {{maxlinks *<1-255>*} | { freeze *WORD* }}

(5) account configuration: set the account for the policy group and establish the local database

username *username* [password ***password*** | {**encryption-type** ***encrypted-password***}] [maxlinks *number*] [authen-group *WORD*] [author-group *WORD*] [pass-group *WORD*] [autocommand *command*]

The configured local policy group can be used in local authentication and authorization. Local method is applicable to the default policy group and localgroup word is to a local policy group.

6.5.3 Local Account Policy Example

This section provides one sample configuration using local account policy. The following example shows how to configure the local authentication and local authorization.

```
aaa authentication login default local
aaa authorization exec default local
!
localpass a3
 non-user
 non-history
 element number lower-letter upper-letter special-character
 min-length 10
 validity 2d
!
localauthen a1
 login max-tries 4 try-duration 2m
!
localauthor a2
```

exec privilege default 15

!

local pass-group a3

local authen-group a1

local author-group a2

!

The meaning of each command line is shown below:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.
- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- The command localpass a3 defines the password policy named a3.
- The command localauthen a1 defines the authentication policy named a1.
- The command localauthor a2 defines the authorization policy named a2.
- The command local pass-group a3 applies the password policy named a3 to the default policy group.
- The command localauthen a1 applies the authentication policy named a1 to the default policy group.
- The command localauthor a2 applies the authorization policy named a2 to the default policy group.

Chapter 7 Configuring RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The "RADIUS Configuration Task List" section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set. The last section in this chapter-RADIUS Configuration Examples- provides with two examples. Refer to RADIUS Configuration Commands for more details of RADIUS command.

7.1 Overview

7.1.1 RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on OLTs and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.

RADIUS is not suitable in the following network security situations:

- RADIUS does not support the following protocols::

  AppleTalk Remote Access (ARA)

  NetBIOS Frame Control Protocol (NBFCP)
- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD connections
- Conditions of OLT to other switching devices. RADIUS does not provide two-way authentication. On the OLT only incoming call authentication is available when running RADIUS. The outbound call is impossible.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

7.1.2 RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

(1)The user is prompted for and enters a username and password.

(2)The username and encrypted password are sent over the network to the RADIUS server.

(3)The user receives one of the following responses from the RADIUS server:

ACCEPT: The user is authenticated.

REJECT: The user is not authenticated and is prompted to reenter the username and password, or access is denied.

CHALLENGE: A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

a. Services that the user can access, including Telnet or rlogin.

b. Connection parameters, including the host or client IP address, access list, and user timeouts.

7.2 RADIUS Configuration Steps

To configure RADIUS on your OLT or access server, you must perform the following tasks:

- Use the aaa authentication global configuration command to define method lists for RADIUS authentication. For more information about using the aaa authentication command, refer to the "Configuring Authentication" chapter.
- Use line and interface commands to enable the defined method lists to be used. For more information, refer to the "Configuring Authentication" chapter.

The following configuration tasks are optional:

- If necessary, run aaa authorization in global configuration mode to authorize the user's service request. For more information about using the aaa authorization command, refer to the "Configuring Autorization" chapter.
- If necessary, run aaa accounting in global configuration mode to record the whole service procedure. For more information about running aaa accounting, see Record Configuration.

7.3 RADIUS Configuration Task List

- Configuring OLT to RADIUS Server Communication
- Configuring OLT to Use Vendor-Specific RADIUS Attributes
- Specifying RADIUS Authentication
- Specifying RADIUS Authorization
- Specifying RADIUS Accounting

7.4 RADIUS Configuration Task

7.4.1 Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider. A RADIUS server and a switch use a shared secret text string to encrypt passwords and exchange responses. Use the **radius-server host** command to specify RADIUS server, Use the **radius-server key** command to specify a shared secret text (key) string.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

Command	Purpose
radius-server host *ip-address* [**auth-port** *port-number*][**acct-port** *portnumber*]	Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers.
radius-server key *string*	Specifies the shared secret text string used between the

	router and a RADIUS server.

To configure global communication settings between the router and a RADIUS server, use the following radius-server commands in global configuration mode:

Command	Purpose
radius-server retransmit *retries*	Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is 2).
radius-server timeout *seconds*	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
radius-server deadtime *minutes*	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

7.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS). To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

Command	Purpose
radius-server vsa send [authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

7.4.3 Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the aaa authentication command, specifying RADIUS as the authentication method. For more information, refer to the chapter "Configuring Authentication."

7.4.4 Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you must issue the aaa authorization command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

7.4.5 Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the aaa accounting command, specifying RADIUS as the accounting method. For more information, refer to the chapter "Configuring Accounting."

7.5 RADIUS Configuration Examples

7.5.1 RADIUS Authentication Example

The following example shows how to configure the switch to authenticate and authorize using RADIUS:

aaa authentication login use-radius group radius local

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

aaa authentication login use-radius radius local configures the OLT to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, use-radius is the name of the method list, which specifies RADIUS and then local authentication.

7.5.2 RADIUS Application in AAA

The following example shows a general configuration using RADIUS with the AAA command set:

radius-server host 1.2.3.4

radius-server key myRaDiUSpassWoRd

username root password AlongPassword

aaa authentication login admins group radius local

line vty 1 16

login authentication admins

The meaning of each command line is shown below:

radius-server host is used to define the IP address of the RADIUS server.

radius-server key is used to define the shared key between network access server and RADIUS server.

aaa authentication login admins group radius local command defines the authentication method list "admins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.

login authentication admins is used to designate to apply the admins method list during login.

Chapter 8 TACACS+ Configuration

8.1 TACACS+ Overview

As an access security control protocol, TACACS+ provides the centralized verification of acquiring the network access server's access right for users. . The communication's safety is guaranteed because the information exchange between network access server and TACACS+ service program is encrypted

Before using TACACS+ configured on network access server, TACACS+'s server has to be accessed and configured. TACACS+ provides independent modularized authentication, authorization and accounting.

Authentication—supporting multiple authentication ways (ASCII, PAP, CHAP and etc), provides the ability of processing any conversation with users (for example, bringing forward probing questions like family address, service type, ID number and etc. after providing login username and password). Moreover, TACACS+ authentication service supports sending information to user's screen, like sending information to notify user that their password has to be changed because of the company's password aging policy.

Authorization—detailed controlling of user's service limitation during service time, including setting up automatic commands, access control, dialog continuing time and etc. It can also limit the command enforcement which user might execute.

Accounting—collecting and sending the information of creating bills, auditing, or counting the usage status of network resources. Network manager can use accounting ability to track user's activities for security auditing or provide information for user's bills. The accounting function keeps track of user authentication, beginning and starting time, executed commands, packets' quantity and bytes' quantities, and etc.

8.1.1 The Operation of TACACS+ Protocol

1. Authentication in ASCII Form

When user logs in network access server which uses TACACS+, and asking for simple authentication in ASCII form, the following process might happen under typical circumstances:

When the connection is built up, network access server communicates with TACACS+ service program to acquire username prompt, and then gives it to user. User enters username, and network access server communicates with TACACS+ service program again to acquire password prompt. It shows password prompt to user. User enters password and then the password is sent to TACACS+ service program.

NOTE: TACACS+ allows any dialogues between server's program and user until it collects enough information to identify user. Normally it is accomplished by the combination of prompting username and password, but it can also include other items, like ID number. All of these are under the control of TACACS+ server's program.

Network access server finally gets one of the following responses from TACACS+ server:

ACCEPT	User passes authentication, and service begins. If network access server is configured as requiring service authorization, authorization begins at this moment.
REJECT	User does not pass authentication. User might be rejected for further access or prompted to access again. It depends on the treatment of TACACS+ server.
ERROR	Error happens during authentication, and the cause might be at server. It also

	might happen at the network connection between server and network access server. If ERROR response is received, normally network access tries another way to identify user.
CONTINUE	It prompts user to enter additional authentication information.

2. Authentication in PAP and CHAP Ways

PAP login is similar with ASCII login, but the difference is that username and password of network access server is in PAP message not entered by user, thus it would not prompt user to enter relative information. CHAP login is similar in the main parts. After authentication, user need to enter authorization stage if network access server asks for the authorization for user. But before TACACS+ authorization is handled, TACACS+ authentication has to be finished.

If TACACS+ authorization needs to be processed, it needs to contact with TACACS+ server program again and go back to the authorization response of ACCEPT or REJECT. If back to ACCEPT, AV (attribute-value) for data, which is used for specifying the user's EXEC or NETWORK dialogue and confirming services which user can access, might be included.

8.2 TACACS+ Configuration Process

In order to configure as supporting TACACS+, the following tasks must be processed:

Using command **tacacs-server** to assign one or multiple IP addresses of TACACS+ server. Using command tacacs key to assign encrypted secret key for all the exchanged information between network access server and TACACS+ server. The same secret key has to be configured in TACACS+ server program.

Use the global configuration command aaa authentication to define the method table which uses TACACS+ to do authentication. More information about command aaa authentication, please refer to "Authentication Configuration".

Use commands line and interface to apply the defined method table on interfaces or lines. More relative information, please refer to "Authentication Configuration".

8.3 TACACS+ Configuration Task List

- Assigning TACACS+ server
- Setting up TACACS+ encrypted secret key
- Assigning to use TACACS+ for authentication
- Assigning to use TACACS+ for authorization
- Assigning to use TACACS+ for accounting

8.4 TACACS+ Configuration Task

8.4.1 Assigning TACACS+ Server

Command **Tacacs-server** could help to assign the IP address of TACACSC+ server. Because TACACS+ searching host in the configured order, this characteristic is useful for servers which configured with different priorities. In order to assign TACACS+ host, use the following commands under global configuration mode:

Command	Purpose
tacacs-server host *ip-address*	To assign the IP address of TACACS+ server and

[single-connection| multi-connection] [port *integer*] [timeout *integer*] [key *string*]	relative features.

Use command tacacs-server to configure the following as well:

- Use single-connection key word to assign the adoption of single connection. This would allow server program to deal with more TACACS+ operations and be more efficient. multi-connection means the adoption of multiple TCP connection.
- Use parameter port to assign TCP interface number which is used by TACACS+ server program. The default interface number is 49.
- Use parameter timeout to assign the time's upper limit (taken second as the unit) for OLT's waiting response from server.
- Use parameter key to assign the encrypted and decrypted secret keys for messages.

NOTE: Connect host after using tacacs-server, and connect the timeout value defined by command timeout to cover the global timeout value configured by command tacacs-server timeout. Use the encrypted secret key assigned by tacacs-server to cover the default secret key configured by global configuration command tacacs-server key. Therefore, this command could be used to configure the unique TACACS+ connection to enhance the network security.

8.4.2 Setting up TACACS+ Encrypted Secret Key

In order to set up the encrypted secret key of TACACS+ message, use the following command under the global configuration mode:

Command	Purpose
tacacs-server key *keystring*	To set up the encrypted secret key matched with the encrypted secret key used by TACACS+ server.

NOTE: In order to encrypt successfully, the same secret key should also be configured for TACACS+ server program.

8.4.3 Assigning to Use TACACS+ for Authentication

After having marked the TACACS+ server and defined its related encrypted secret key, method table need to be defined for TACACS+ authentication. Because TACACS+ authentication is by AAA, command aaa authentication should be assigned as TACACS+'s authentication way. More information, please refer to "Authentication Configuration".

8.4.4 Assigning to Use TACACS+ for Authorization

AAA authorization could help to set up parameter to confine user's network access limitation. TACACS+ authorization could be applied to services like command, network connection, EXEC dialogue and etc. Because TACACS+ authorization is by AAA, command aaa authorization should be assigned as TACACS+'s authentication way. More information, please refer to "Authorization Configuration".

8.4.5 Assigning to Use TACACS+ for Accounting

AAA accounting is able to track user's current service and their consumed network resources' quantity. Because TACACS+

authorization is by AAA, command aaa accounting should be assigned as TACACS+'s accounting way. More information, please refer to "Accounting Configuration".

8.5 TACACS+ Configuration Example

This chapter includes the following TACACS+ configuration example.

8.5.1 TACACS+ Authentication Examples

The following configuring login authentication is accomplished by TACACS+:

aaa authentication login test group tacacs+ local

tacacs-server host 1.2.3.4

tacacs-server key testkey

line vty 0

login authentication test

In this example:

Command **aaa authentication** defines the authentication method table test used on vty0. Key word tacacs+ means the authentication is processed by TACACS+, and if TACACS+ does not respond during authentication, key word local indicates to use the local database on the network access server to do authentication.

Command **tacacs-server host** marks TACACS+ server's IP address as 1.2.3.4. command tacacs-server key defines the shared encrypted secret key as testkey.

The following example is the security protocol used when configuring TACACS+ as login authentication, with the usage of method table default not test:

aaa authentication login default group tacacs+ local

tacacs-server host 1.2.3.4

tacacs-server key goaway

In this example:

Command **aaa authentication** defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command **tacacs-server host** marks TACACS+ server program's IP address as 1.2.3.4. Command **tacacs-server key** defines the shared encrypted secret key as goaway.

8.5.2 TACACS+ Authorization Examples

aaa authentication login default group tacacs+ local

aaa authorization exec default group tacacs+

tacacs-server host 10.1.2.3

tacacs-server key goaway

In this example:

Command aaa authentication defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command aaa authorization does network service authorization by TACACS+.

Command tacacs-server host marks TACACS+ server's IP as 10.1.2.3. Command tacacs-server key defines the shared encrypted secret key as goaway.

8.5.3 TACACS+ Accounting Examples

The following configuration of login authentication's method table uses TACACS+ as one of the methods to configure the accounting by TACACS+:

aaa authentication login default group tacacs+ local

aaa accounting exec default start-stop group tacacs+

tacacs-server host 10.1.2.3

tacacs-server key goaway

In this example:

Command **aaa authentication** defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command **aaa accounting** does accounting of network service by TACACS+. In this example, the relative information of starting and beginning time is accounted and sent to TACACS+ server.

Command **tacacs-server host** marks TACACS+ server's IP address as 10.1.2.3. Command **tacacs-server key** defines the shared encrypted secret key as goaway.

Chapter 9 HTTP Switch Configuration

9.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and SNMP but also through Web browser. The switches support the HTTP configuration, the abnormal packet timeout configuration, and so on.

9.1.1 Choosing the Prompt Language

Up to now, switches support two languages, that is, English and Chinese, and the two languages can be switched over through the following command.

Command	Purpose
[no] ip http language { english}	Sets the prompt language of Web configuration to **English**.

9.1.2 Setting the HTTP Port

Generally, the HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support users to change the service port and after the service port is changed you have to use the IP address and the changed port to access switches. For example, if you set the IP address and the service port to **192.168.1.3** and **1234** respectively, the HTTP access address should be changed to **http:// 192.168.1.3:1234**. You'd better not use other common protocols' ports so that access collision should not happen. Because the ports used by a lot of protocols are hard to remember, you'd better use port IDs following port 1024.

Command	Purpose
ip http port { *portNumber* }	Sets the HTTP port.

9.1.3 Enabling the HTTP Service

Switches support to control the HTTP access. Only when the HTTP service is enabled can HTTP exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops.

Command	Purpose
ip http server	Enables the HTTP service.

9.1.4 Setting the HTTP Access Mode

You can access a switch through two access modes: HTTP access and HTTPS access, and you can use the following command to set the access mode to **HTTP**.

Command	Purpose
ip http http-access enable	Sets the HTTP access mode.

9.1.5 Setting the Maximum Number of VLAN Entries on Web Page

A switch supports at most 4094 VLANs and in most cases Web only displays parts of VLANs, that is, those VLANs users want

to see. You can use the following command to set the maximum number of VLANs. The default maximum number of VLANs is 100.

Command	Purpose
ip http web max-vlan { *max-vlan* }	Sets the maximum number of VLAN entries displayed in a web page.

9.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page

A switch supports at most 100 multicast entries. You can run the following command to set the maximum number of multicast entries and Web then shows these multicast entries. The default maximum number of multicast entries is 15.

Command	Purpose
ip http web igmp-groups { *igmp-groups* }	Sets the maximum number of multicast entries displayed in a web page.

9.2 HTTPS Configuration

In order to improve the security of communications, switches support not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

9.2.1 Setting the HTTP Access Mode

You can run the following command to set the access mode to **HTTPS.**

Command	Purpose
ip http ssl-access enable	Sets the HTTPS access mode.

9.2.2 It is used to set the HTTPS port.

As the HTTP port, HTTPS has its default service port, port 443, and you also can run the following command to change its service port. It is recommended to use those ports following port 1024 so as to avoid collision with other protocols' ports.

Command	Purpose
ip http secure-port {*portNumber*}	Sets the HTTPS port.

Chapter 10 Accessing the Switch

10.1 Accessing the Switch Through HTTP

When accessing the switch through Web, please make sure that the applied browser complies with the following requirements:

- HTML of version 4.0
- HTTP of version 1.1
- JavaScript™ of version 1.5

What's more, please ensure that the main program file, running on a switch, supports Web access and your computer has already connected the network in which the switch is located.

10.1.1 Initially Accessing the Switch

When the switch is initially used, you can use the Web access without any extra settings:

1. Modify the IP address of the network adapter and subnet mask of your computer to 192.168.0.2 and 255.255.255.0 respectively.

2. Open the Web browser and enter **192.168.0.1** in the address bar. It is noted that **192.168.0.1** is the default management address of the switch.

3、If the Internet Explorer browser is used, you can see the dialog box in figure 1. Both the original username and the password are “admin”, which is capital sensitive.



Figure 10-1: ID checkup of WEB login

4. After successful authentication, the systematic information about the switch will appear on the IE browser.

10.1.2 Upgrading to the Web-Supported Version

If your switch is upgraded to the Web-supported version during its operation and the switch has already stored its configuration files, the Web visit cannot be directly applied on the switch. Perform the following steps one by one to

enable the Web visit on the switch:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Switch_config#".
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
4. Enter the **ip http server** command in global configuration mode and start the Web service.
5. Run **username** to set the username and password of the switch. For how to use this command, refer to the "Security Configuration" section in the user manual.

After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.

6. Enter **write** to store the current configuration to the configuration file.

10.2 Accessing a Switch through Secure Links

The data between the WEB browser and the switch will not be encrypted if you access a switch through common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to access the switch.

To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Switch_config#".
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
4. Enter the **ip http server** command in global configuration mode and start the Web service.
5. Run **username** to set the username and password of the switch. For how to use this command, refer to the "Security Configuration" section in the user manual.
6. Run **ip http ssl-access enable to enable the secure link access of the switch.**
7. Run **no ip http http-access enable to forbid to access the switch through insecure links.**
8. Enter **write** to store the current configuration to the configuration file.
9. Open the WEB browser on the PC that the switch connects, enter **https://192.168.0.1** on the address bar (**192.168.0.1** stands for the management IP address of the switch) and then press the Enter key. Then the switch can be accessed through the secure links.

10.3 Introduction of Web Interface

The homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

10.3.1 Top Control Bar



Figure 10-2: Top control bar

Save All	Write the current settings to the configuration file of the device. It is equivalent to the execution of the **write** command. The configuration that is made through Web will not be promptly written to the configuration file after validation. If you click “Save All”, the unsaved configuration will be lost after rebooting.
English	The interface will turn into the English version.
Chinese	The interface will turn into the Chinese version.
Logout	Exit from the current login state. After you click "logout", you have to enter the username and the password again if you want to continue the Web function.
Port Panel	Displays the simple port panel.
About	Displays vendor information and sets automatic refresh.

After you configure the device, the result of the previous step will appear on the left side of the top control bar. If error occurs, please check your configuration and retry it later.

10.3.2 Navigation Bar



Figure 10-3 Navigation bar

The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at “Runtime Info”. If a certain item need be configured, please click the group name and then the sub-item. For example, to browse the flux of the current port, you have to click “Interface State" and then “Interface Flow”.

NOTE: The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web with limited user’s permissions, only “Interface State” will appear.

10.3.3 Configuration Information Area

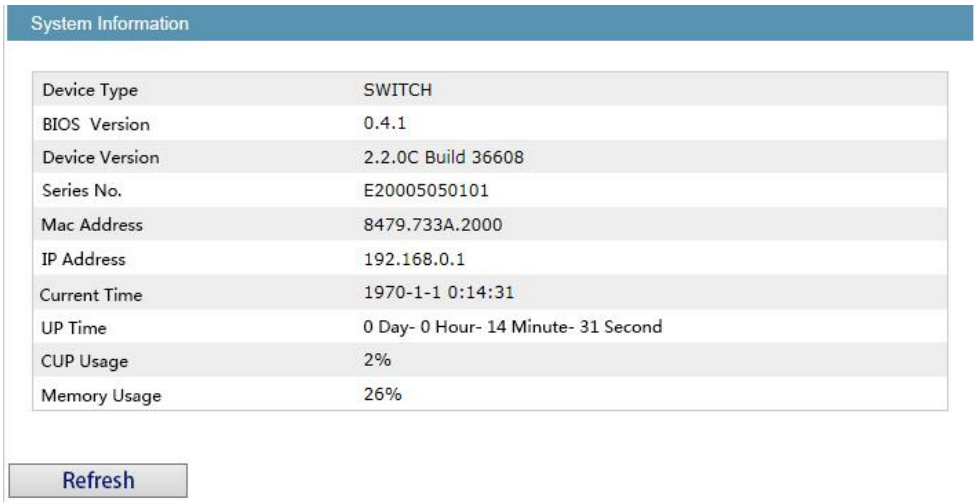


Figure 10-4 Configuration Area

The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

10.3.4 Configuration Area

The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to the device. The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click "Save All" on the top control bar.
Reset	Means discarding the modification of the sheet. The content of the sheet will be reset.
New	Creates a list item. For example, you can create a VLAN item or a new user.
Delete	Deletes an item in the list.
Back	Go back to the previous-level configuration page.

Chapter 11 Basic Configuration



Figure 11-1 A list of basic configuration

11.1 Hostname Configuration

If you click **Basic Config** -> **Hostname Config** in the navigation bar, the **Hostname Configuration** page appears, as shown in figure 2.

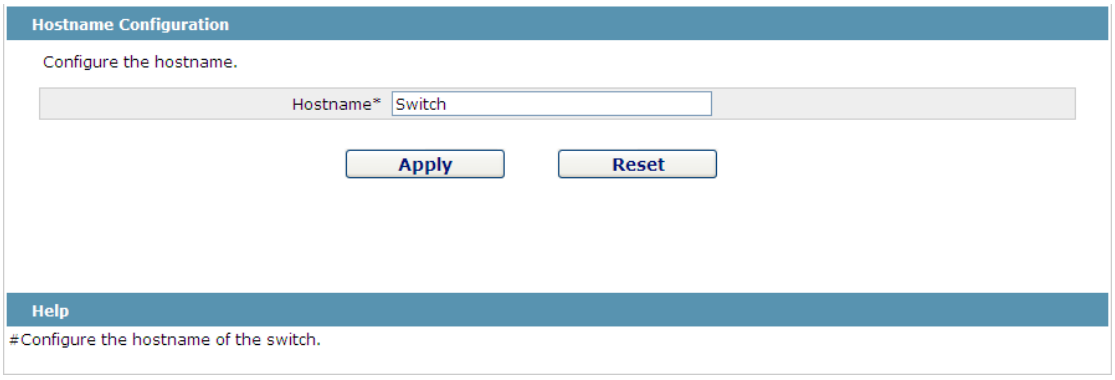


Figure 11-2 Hostname configuration

The hostname will be displayed in the login dialog box.

The default name of the device is "Switch". You can enter the new hostname in the text box shown in figure 3 and then click "Apply".

11.2 Time Management

If you click System Manage -> Time Manage, the Time Setting page appears.

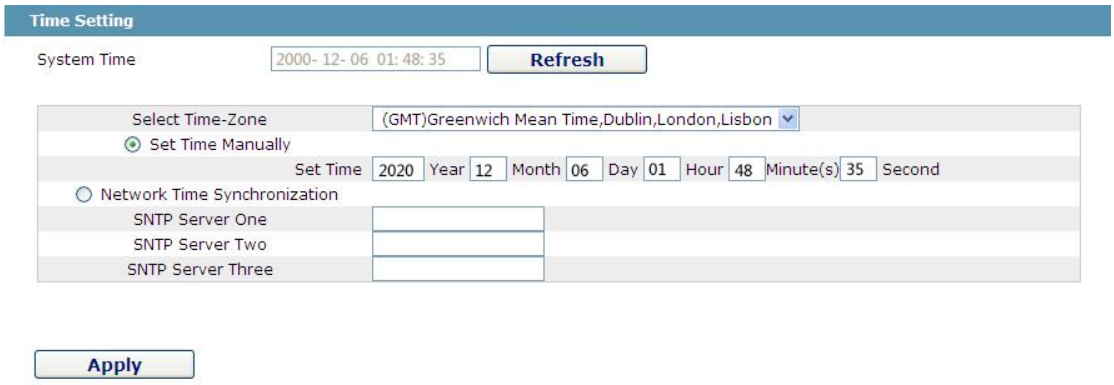


Figure 11-3 Clock management

To refresh the clock of the displayed device, click "Refresh".

In the "Select Time-Zone" dropdown box select the time zone where the device is located. When you select "Set Time Manually", you can set the time of the device manually. When you select "Network Time Synchronization", you can designate 3 SNTP servers for the device.

Chapter 12 Configuration of the Physical Interface

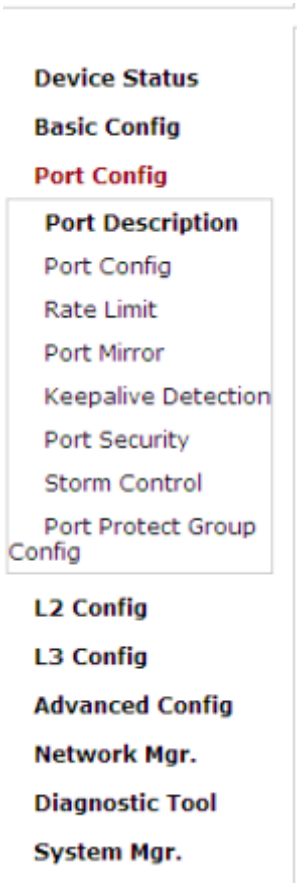


Figure 12-1: Physical port configuration list

12.1 Configuring Port Description

If you click **Physical port config -> Port description Config** in the navigation bar, the **Port description Configuration** page appears, as shown in figure 2.

Port	Port Description
G0/1	

Figure 12-2: Port description configuration

You can modify the port description on this page and enter up to 120 characters. The description of the VLAN port cannot be set at present.

12.2 Configuring the Attributes of the Port

If you click **Physical port config -> Port attribute Config** in the navigation bar, the **Port Attribute Configuration** page appears, as shown in figure 3.

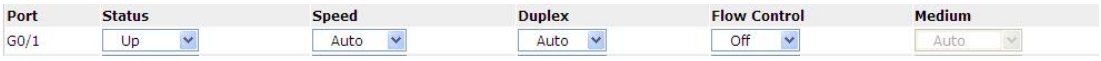


Figure 12-3 Configuring the port attributes

On this page you can modify the on/off status, rate, duplex mode, flow control status and medium type of a port.

NOTE: After the speed or duplex mode of a port is modified, the link state of the port may be switched over and the network communication may be impaired.

12.3 Rate control

If you click **Physical port Config -> Port rate-limit Config** in the navigation bar, the **Port rate limit** page appears, as shown in figure 4.



Figure 12-4 Port's rate limit

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited. The receiving and sending rates can be configured either by percentage or by specific units of the switch.

12.4 Port mirroring

If you click **Physical port Config -> Port Mirror** in the navigation bar, the **Port Mirror Config** page appears, as shown in figure 4-5.

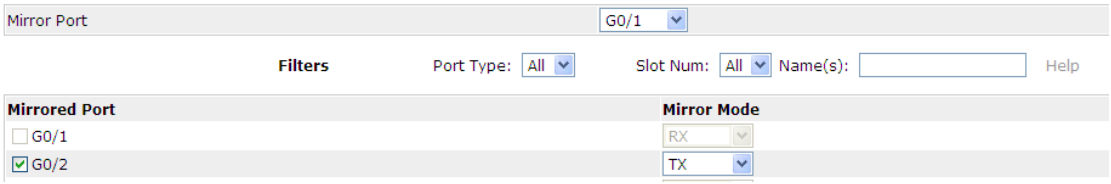


Figure 12-5 Port mirror configuration

Click the dropdown list on the right side of "Mirror Port" and select a port to be the destination port of mirror.

Click a checkbox and select a source port of mirror, that is, a mirrored port.

RX	The received packets will be mirrored to the destination port.
TX	The transmitted packets will be mirrored to a destination port.
RX & TX	The received and transmitted packets will be mirrored simultaneously.

12.5 Loopback Detection

If you click **Physical port Config -> Port loopback detection** in the navigation bar, the **Setting the port loopback detection page** appears, as shown in figure 4-6.



Figure 12-6: Port loopback detection

You can set the loopback detection cycle on the **Loopback Detection** page.

12.6 Port security

12.6.1 IP Binding Configuration

If you click **Physical port Config -> Port Security -> IP bind** in the navigation bar, the **Configure the IP-Binding Info** page appears, as shown in figure 4-7.



Figure 12-7 IP binding configuration

Click "Detail" and then you can conduct the binding of the source IP address for each physical port. In this way, the IP address that is allowed to visit the port will be limited.



Figure 12-8 Setting the binding of the source IP address

12.6.2 MAC Binding Configuration

If you click **Physical port Config -> Port Security -> MAC bind** in the navigation bar, the **Configure the MAC-Binding Info** page appears, as shown in figure 4-10.



Figure 12-9 MAC binding configuration

Click "Detail" and then you can conduct the binding of the source MAC address for each physical port. In this way, the MAC address that is allowed to visit the port will be limited.



Figure 12-10 Setting the binding of the source MAC address

12.6.3 Setting the Static MAC Filtration Mode

If you click Physical port Config -> Port Security -> Static MAC filtration mode in the navigation bar, the Configure the static MAC filtration mode page appears, as shown in figure 4-11.

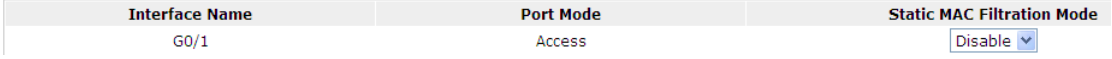


Figure 12-11: Setting the static MAC filtration mode

On this page you can set the static MAC filtration mode. By default, the static MAC filter is disabled. Also, the static MAC filter mode cannot be set on ports in trunk mode.

12.6.4 Static MAC Filtration Entries

If you click Physical port Config -> Port security -> Static MAC filtration entries in the navigation bar, the Setting the static MAC filtration entries page appears.

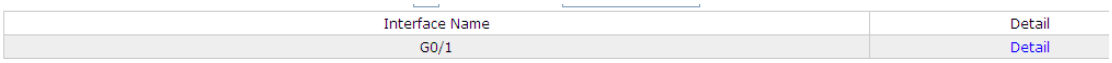


Figure 12-12: Static MAC filtration entry list

If you click "Detail", you can conduct the binding of the source MAC address for each physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.

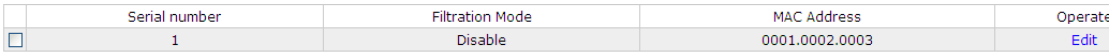


Figure 12-13: Setting static MAC filtration entries

12.6.5 Setting the Dynamic MAC Filtration Mode

If you click Physical port Config -> Port Security -> Dynamic MAC filtration mode in the navigation bar, the Configure the dynamic MAC filtration mode page appears, as shown in figure 4-14.

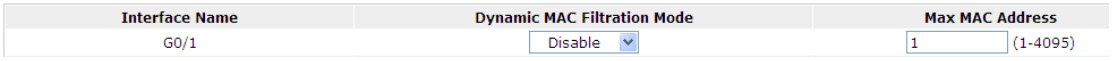


Figure 12-14: Setting the dynamic MAC filtration mode

You can set the dynamic MAC filtration mode and the allowable maximum number of addresses on this page. By default, the dynamic MAC filtration mode is disabled and the maximum number of addresses is 1.

12.7 Storm control

In the navigation bar, click **Physical port Config -> Storm control**. The system then enters the page, on which the broadcast/multicast/unknown unicast storm control can be set.

12.7.1 Broadcast Storm Control



Figure 12-15 Broadcast storm control

Through the dropdown boxes in the **Status** column, you can decide whether to enable broadcast storm control on a port. In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

12.7.2 Multicast Storm Control



Figure 12-16 Setting the broadcast storm control

Through the dropdown boxes in the **Status** column, you can decide whether to enable multicast storm control on a port. In the **Threshold** column you can enter the threshold of the multicast packets. The legal threshold range for each port is given behind the threshold.

12.7.3 Unknown Unicast Storm Control



Figure 12-17 Unknown unicast storm control

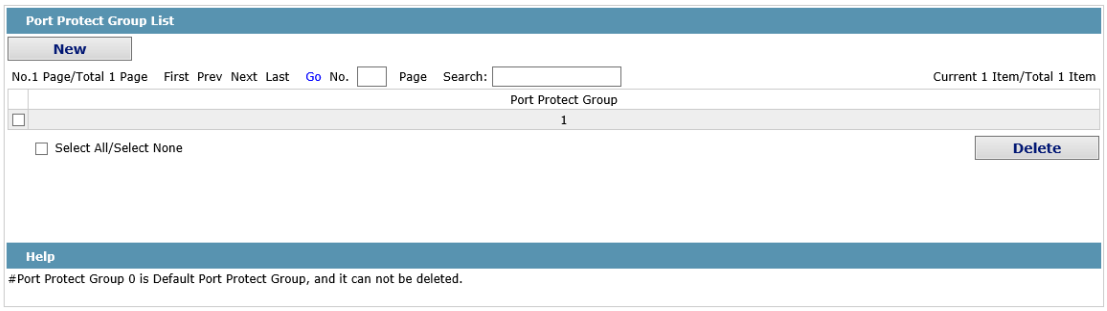
In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

12.8 Port Protect Group Configuration

Click "Port Config" -> "Port Protect Group Config" in the navigation bar, and enter the configuration page of Port Protect Group List and Port Protect Group Interface Config.

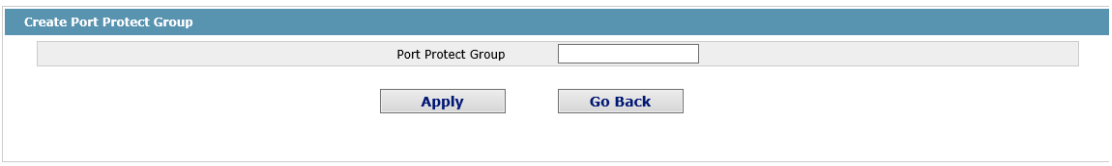
12.8.1 4.8.1 Port Protect Group List

Click "Port Config" -> "Port Protect Group Config" -> "Port Protect Group List" in the navigation bar, and enter the configuration page of "Port Protect Group List".



Click "New" to create a new port protect group, as shown in the above figure.

Tick one port protect group and delete it. The port protect group is 0 by default, which cannot be deleted.



12.8.2 4.8.2 Port Protect Group Interface Configuration

Click "Port Config" -> "Port Protect Group Config" -> "Port Protect Group Interface Config" in the navigation bar, and enter the configuration page of "Port Protect Group Interface Config".

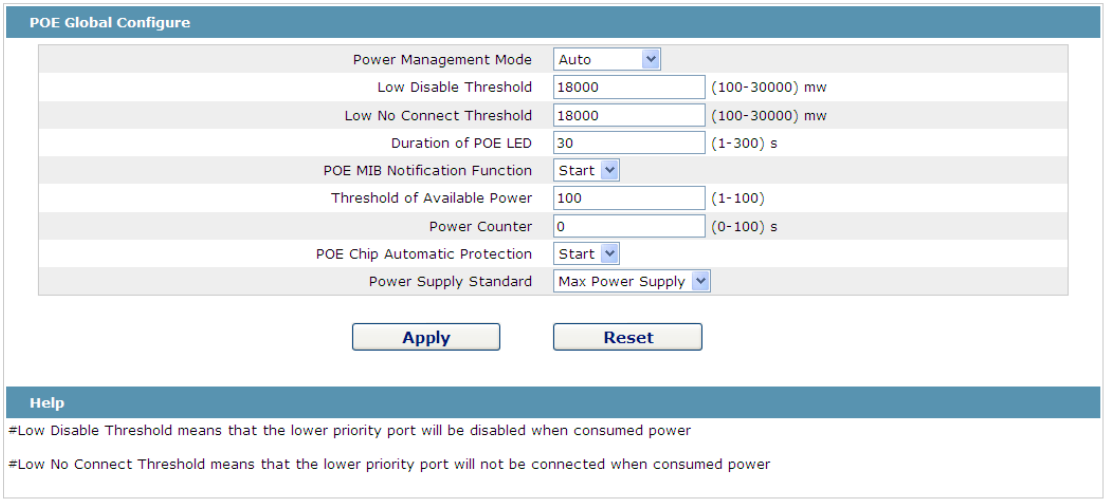
Port	Port Protect Group
g0/1	

The port protect group must be a created group. If one port has configured the default protect group, other ports can only be configured with the default protect group.

12.9 POE Management

12.9.1 POE Global Configuration

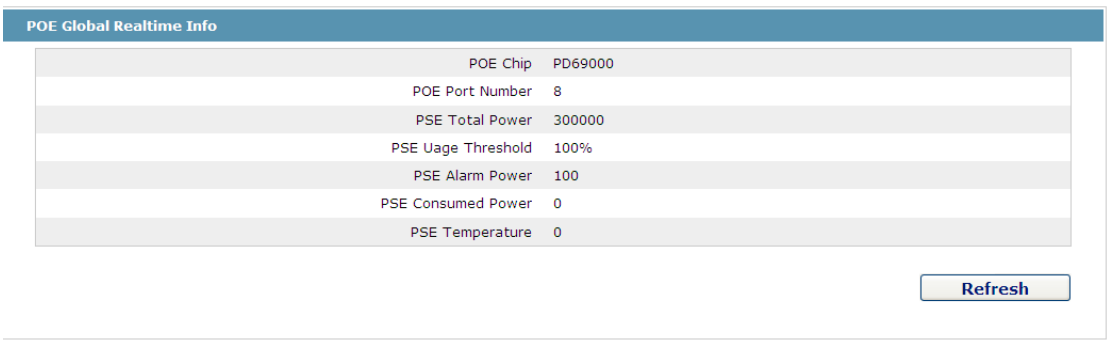
Click "physical port configuration" and "POE management" in turn to enter POE global configuration page.



On this page, POE can be configured as power management mode, low disable threshold, and enable/ disable POE MIB notification function and other global POE properties.

12.9.2 POE Global Real-time Information

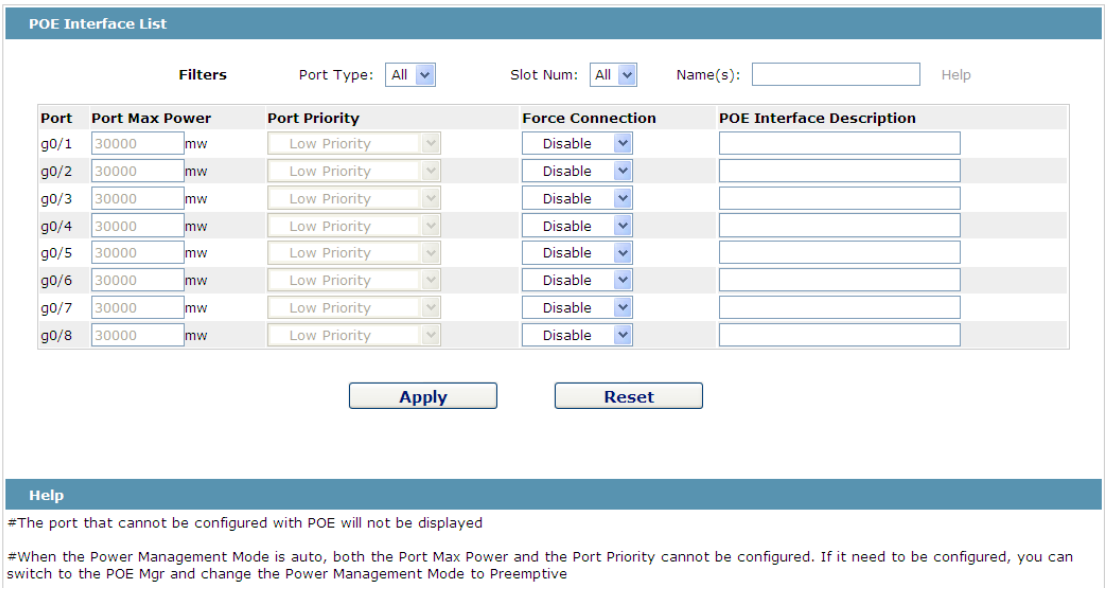
Click "physical port configuration", "POE management" and "POE global real-time information" in turn on the navigation bar to enter POE global real-time information page.



Check POE port quantity, POE power, POE temperature and other information as above on this page.

12.9.3 POE Port List

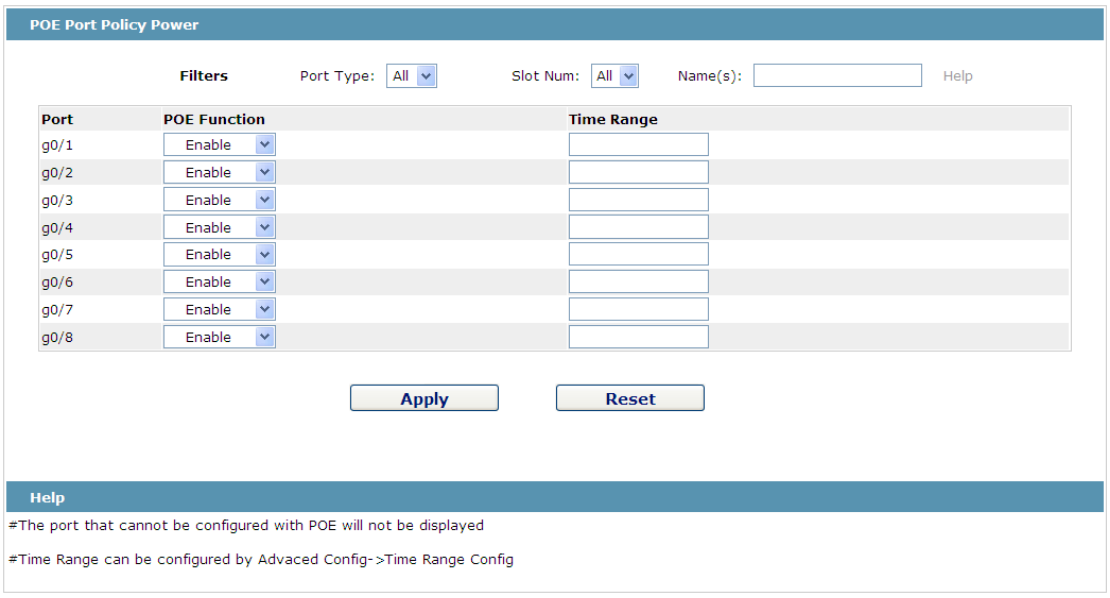
Click "physical port configuration", "POE management" and "POE port list" on navigation bar in turn to enter POE port list page.



Each of POE port's maximum power, priority and mandatory power-up could be configured at this page; illustrative information could also be added on the port at this page.

12.9.4 POE Ports' Policy Power-up

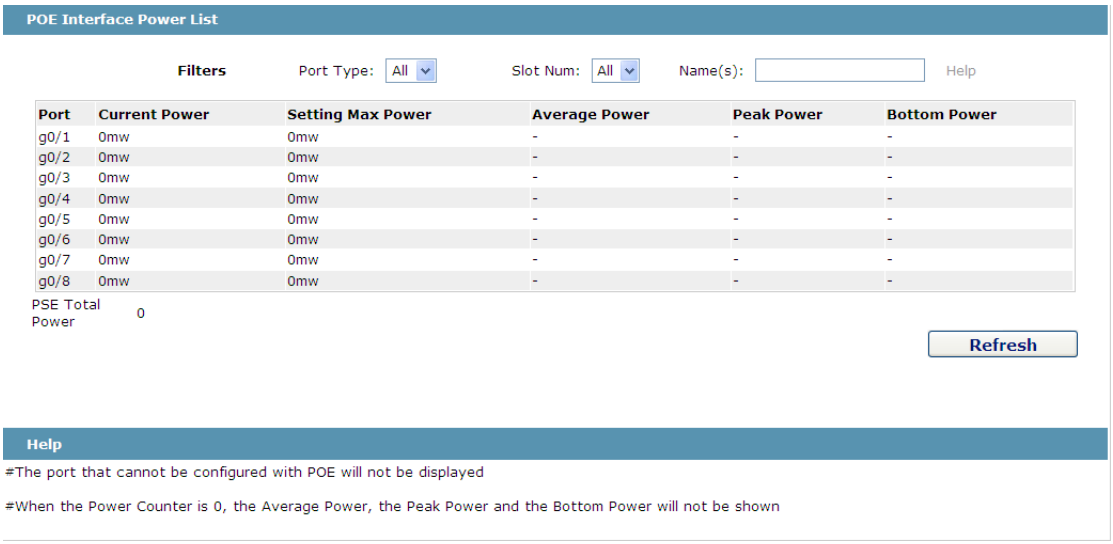
Click "physical port configuration", "POE management" and "POE ports' policy power-up" in turn on navigation bar to enter POE ports' policy power-up management page.



Two controlling methods of ports' power-up can be configured at this page. One is to open and shut down POE function directly; the other is configure Time Range to set the POE operating time of the port.

12.9.5 POE Ports' Power Real-time Information

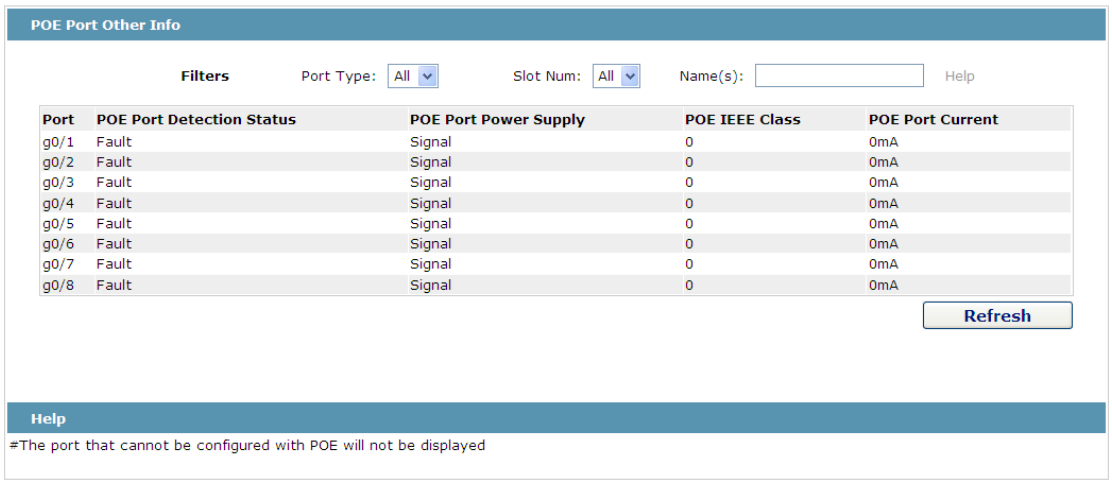
Click "physical port configuration", "POE management" and "POE ports power real-time information" in turn on navigation bar to enter POE ports' power real-time information.



At this page, you could check POE ports' current power, set real time information like the maximum power, average power, peak power, valley power and etc.

12.9.6 POE Ports' Other Real-time Information

Click "physical port configuration", "POE management" and "POE port other real-time information" in turn on navigation bar to enter POE ports' other real-time information page.



POE port detection status, POE port power-up status could be checked at this page.

Chapter 13 Layer-2 Configuration



Figure 13-1 Layer-2 configuration list

13.1 VLAN Settings

13.1.1 VLAN List

If you click **Layer-2 Config** -> **VLAN Config** in the navigation bar, the **VLAN Config** page appears, as shown in figure 2.

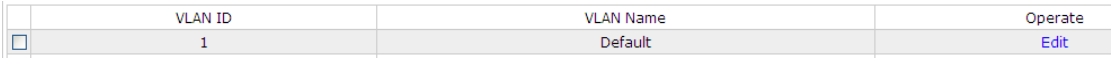


Figure 13-2 VLAN configuration

The VLAN list will display VLAN items that exist in the current device according to the ascending order. In case of lots of items, you can look for the to-be-configured VLAN through the buttons like “Prev”, “Next” and “Search”.

You can click “New” to create a new VLAN.

You can also click “Edit” at the end of a VLAN item to modify the VLAN name and the port’s attributes in the VLAN.

If you select the checkbox before a VLAN and then click “Delete”, the selected VLAN will be deleted.

NOTE: By default, a VLAN list can display up to 100 VLAN items. If you want to configure more VLANs through Web, please log on to the switch through the Console port or Telnet, enter the global configuration mode and then run the “**ip http web max-vlan**” command to modify the maximum number of VLANs that will be displayed.

13.1.2 VLAN Settings

If you click "New" or “Edit” in the VLAN list, the VLAN configuration page appears, on which new VLANs can be created or the attributes of an existent VLAN can be modified.

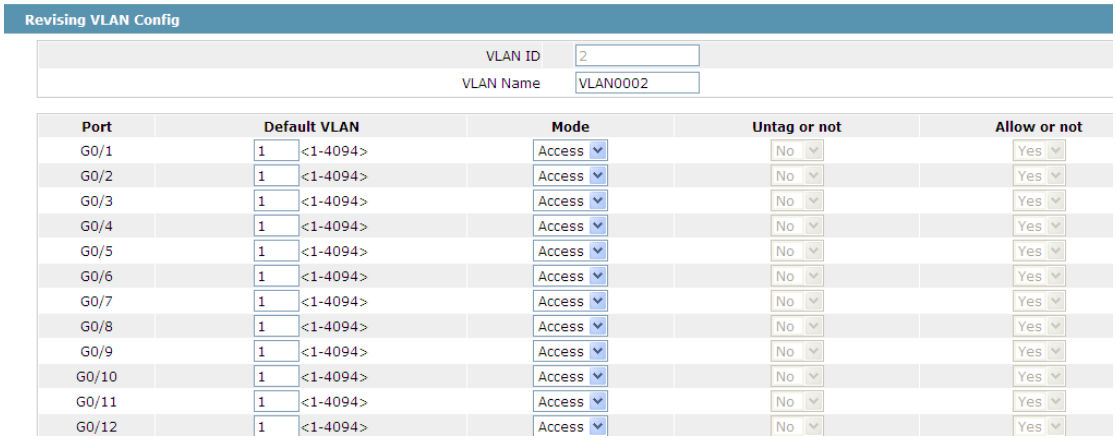


Figure 13-3 Revising VLAN configuration

If you want to create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be null.

Through the port list, you can set for each port the default VLAN , the VLAN mode (Trunk or Access), whether to allow the entrance of current VLAN packets and whether to execute the untagging of the current VLAN when the port works as the egress port.

NOTE: When a port in Trunk mode serves as an egress port, it will untag the default VLAN by default.

13.2 GVRP Configuration

13.2.1 GVRP Global Attribute Configuration

If you click **Layer-2 Config -> GVRP Config -> GVRP Global Config** in the navigation bar, the **GVRP Global Config** page appears, as shown the following Figure.

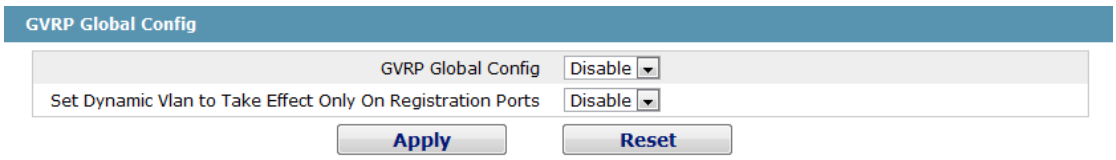


Figure 13-4 GVRP Global Configuration

You can enable or disable the global GVRP protocol and sets whether the dynamic vlan is only effective on the registration interface.

13.2.2 Global Interface Attribute Configuration

If you click **Layer-2 Config -> GVRP Config -> GVRP Interface Config** in the navigation bar, the **GVRP Interface Config** page appears, as shown the following Figure.



Figure 13-5 Global Interface Attribute Configuration

To enable or disable GVRP protocol on the GVRP interface configuration.

13.3 STP Configuration

13.3.1 STP Status Information

If you click **Layer-2 Config -> STP Config** in the navigation bar, the **STP Config** page appears, as shown in figure 10.

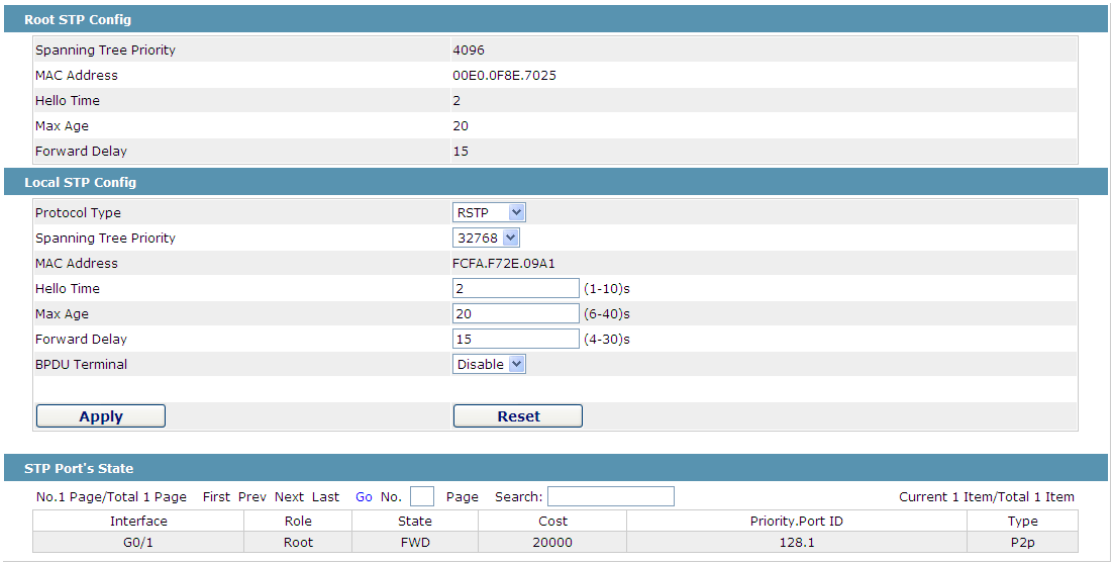


Figure 13-6 Configuring the global attributes of STP

The root STP configuration information and the STP port's status are only-read.

On the local STP configuration page, you can modify the running STP mode by clicking the Protocol type dropdown box.

The STP modes include STP, RSTP and disabled STP.

The priority and the time need be configured for different modes.

NOTE: The change of the STP mode may lead to the interruption of the network.

13.3.2 Configuring the Attributes of the STP Port

If you click the "Configure RSTP Port" option, the "Configure RSTP Port" page appears.

Port	Protocol Status	Priority(0~240)	Path-Cost(0~200000000)	Edge Port Property
G0/1	Enable	128	0	Auto
G0/2	Enable	128	0	Auto
G0/3	Enable	128	0	Auto
G0/4	Enable	128	0	Auto
G0/5	Enable	128	0	Auto
G0/6	Enable	128	0	Auto
G0/7	Enable	128	0	Auto
G0/8	Enable	128	0	Auto

Figure 13-7 Configuring the attributes of RSTP

The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to "Disable" and the STP mode is also changed, the port will not run the protocol in the new mode.

The default value of the path cost of the port is 0, meaning the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

13.4 IGMP-Snooping Configuration

13.4.1 IGMP-Snooping Configuration

If you click **Layer-2 Config -> IGMP snooping**, the IGMP-Snooping configuration page appears.

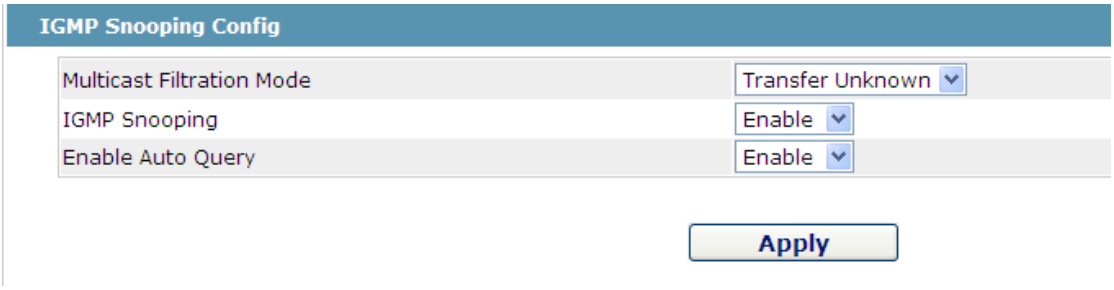


Figure 13-8 IGMP-snooping configuration

On this page you can set whether to make a switch to forward unknown multicasts, whether to enable IGMP snooping, and whether to configure the switch as the querier of IGMP.

13.4.2 IGMP-Snooping VLAN List

If you click Layer-2 Config -> IGMP snooping vlan list, the IGMP-Snooping VLAN list page appears.

	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router's Port	Operate
☐	1	Running	Disable	SWITCH(querier);	Edit

Figure 13-9: IGMP-snooping VLAN list

If you click **New**, IGMP-snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP snooping VLAN. If you click **Cancel**, a selected IGMP-Snooping VLAN can be deleted; if you click **Edit**, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.

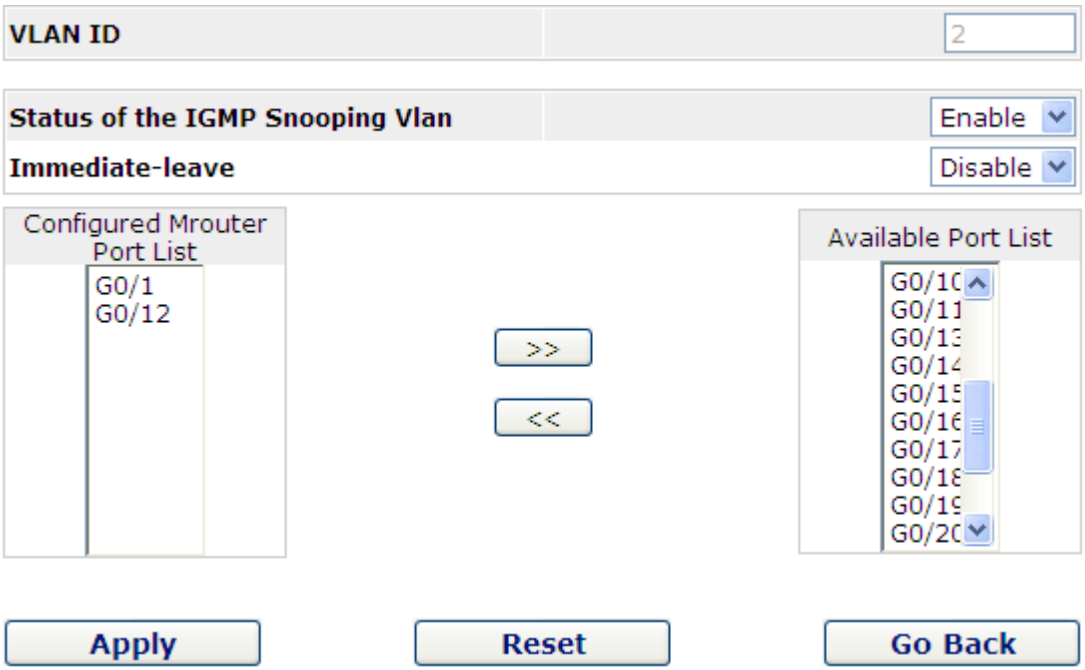


Figure 13-10: Static routing port of IGMP VLAN

When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click ">>" and "<<" to delete and add a routing port.

13.4.3 Static Multicast Address

If you click Static multicast address, the Setting the static multicast address page appears.

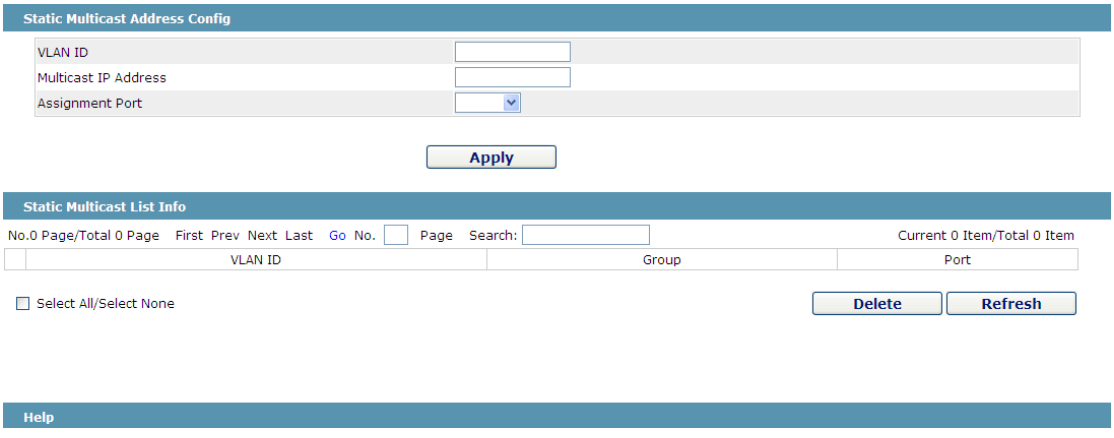


Figure 13-11 Multicast List

On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

Click "Refresh" to refresh the contents in the list.

13.4.4 Multicast List

Click the **Multicast List Info** option on the top of the page and the **Multicast List Info** page appears.



Figure 13-12 Multicast List

On this page the multicat groups, which are existent in the current network and are in the statistics of IGMP snooping, as well as port sets which members in each group belong to are dislayed.

Click "Refresh" to refresh the contents in the list.

NOTE:

By default, a multicast list can display up to 15 VLAN items. You can modify the number of multicast items by running **ip http web igmp-groups** after you log on to the device through the Console port or Telnet.

13.5 Setting Static ARP

If you click **Layer-2 Config -> Static ARP Config**, the static ARP configuration page appears.

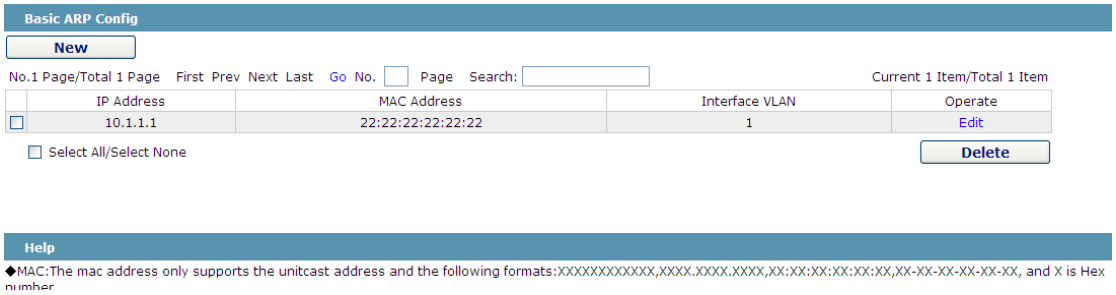


Figure 13-13 Displaying static ARP

You can click **New** to add an ARP entry. If the **Alias** column is selected, it means to answer the ARP request of the designated IP address.

If you click Edit, you can modify the current ARP entry.

If you click Cancel, you can cancel the chosen ARP entry.

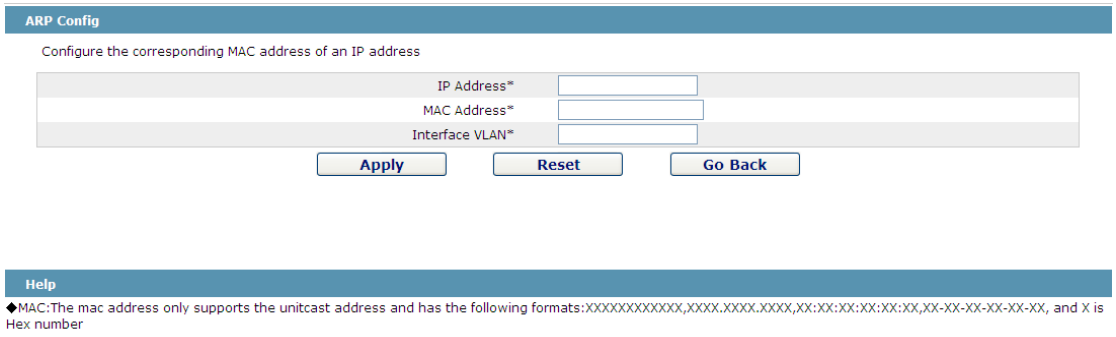


Figure 13-14 Setting static ARP

13.6 Static MAC Address Configuration

If you click Layer-2 Config -> Static MAC Config -> Static MAC List, the Static MAC Address List Info page appears.

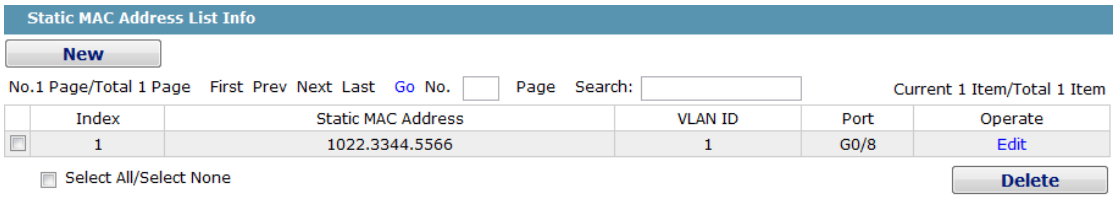


Figure 13-15 Setting Static MAC Address List Info

Click **New** to designate static MAC address and VLAN. The unicast MAC address can only configure one interface. Multiple MAC addresses can configure multiple interfaces.

Click **Edit** to modify the static MAC address.

Click **Delete** to delete the selected MAC address table.

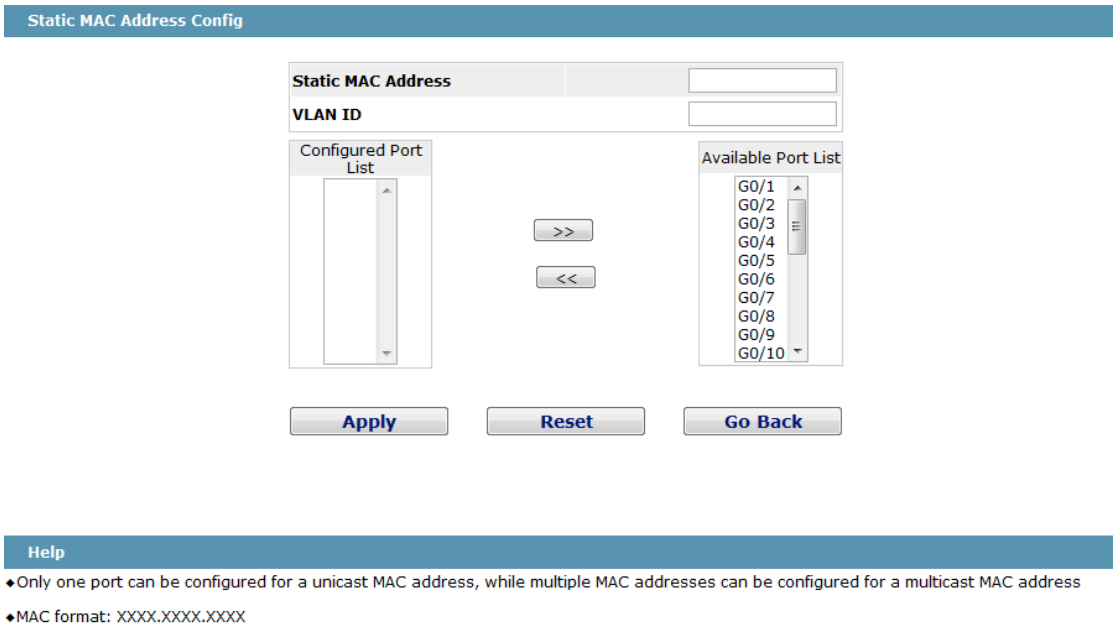


Figure 13-16 Static MAC Address Config

13.7 LLDP Configuration

13.7.1 Configuring the Global Attributes of LLDP

If you click **Layer-2 Config** -> **LLDP Config** -> **LLDP Global Config** in the navigation bar, the **Basic Config of LLDP Protocol** page appears, as shown in the following Figure.

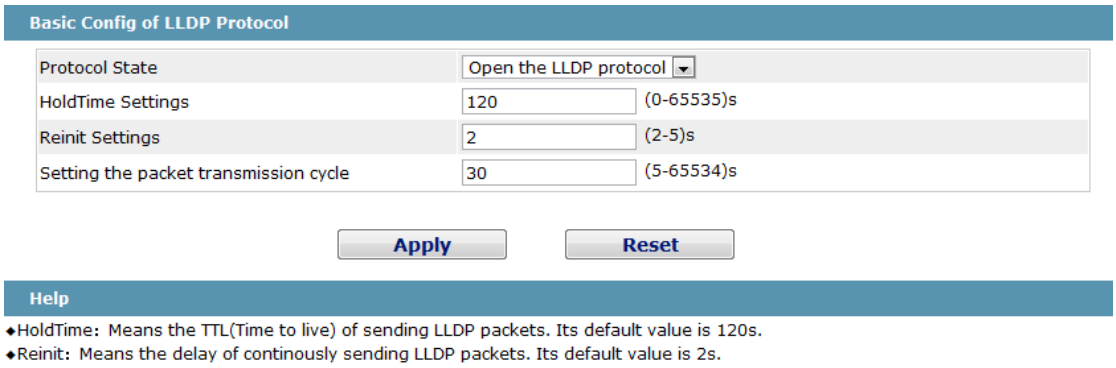


Figure 13-17 Configuring the Global Attributes of LLDP

You can choose to enable LLDP or disable it. When you choose to disable LLDP, you cannot configure LLDP.

The "HoldTime" parameter means the ttl value of the packet that is transmitted by LLDP. Its default value is 120s.

The "Reinit" parameter means the delay of successive packet transmission of LLDP. Its default value is 2s.

13.7.2 LLDP Port Attribute Configuration

If you click Layer-2 Config -> LLDP Config -> LLDP Interface Config in the navigation bar, the LLDP Port Config page appears.

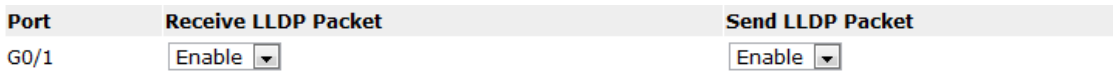


Figure 13-18 Configuring the LLDP port

After the LLDP port is configured, you can enable or disable LLDP on this port.

13.8 DDM Configuration

If you click **L2 Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 5-21.

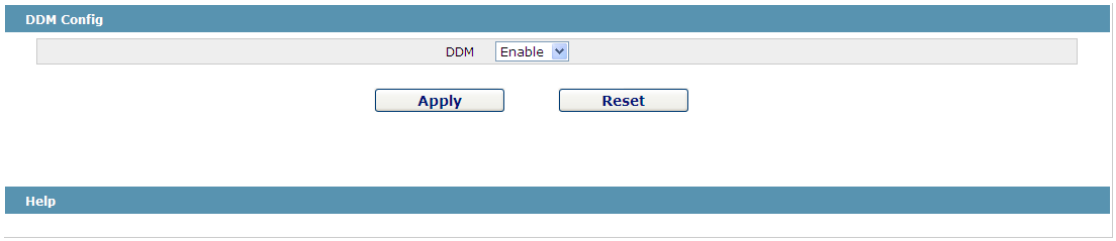


Figure 13-19: DDM configuration

13.9 Port Aggregation Configuration

13.9.1 Port Aggregation Configuration

If you click Layer-2 Config -> Port Channel-> Port Channel, the Port Aggregation Config page appears.

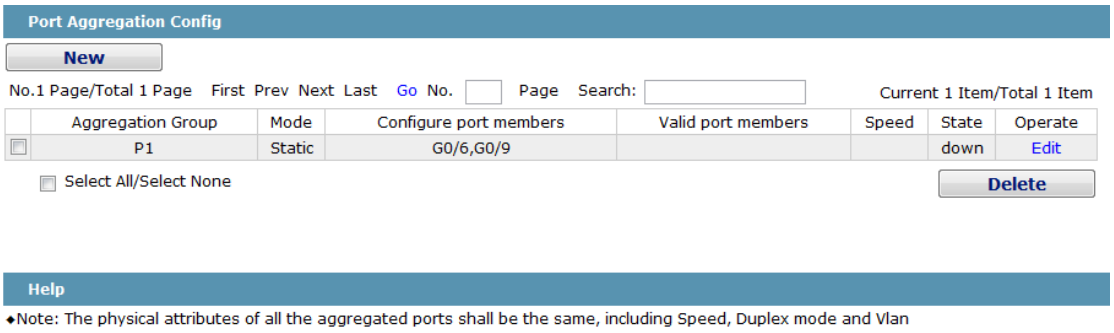


Figure 13-20 Port Aggregation Information

Click **New** to create an aggregation group. It can configure 32 aggregation groups in maximum and each group is with 8 physical ports into aggregation. Click **Delete** to delete the selected aggregation group. Click "**Reset**" to modify the setting.

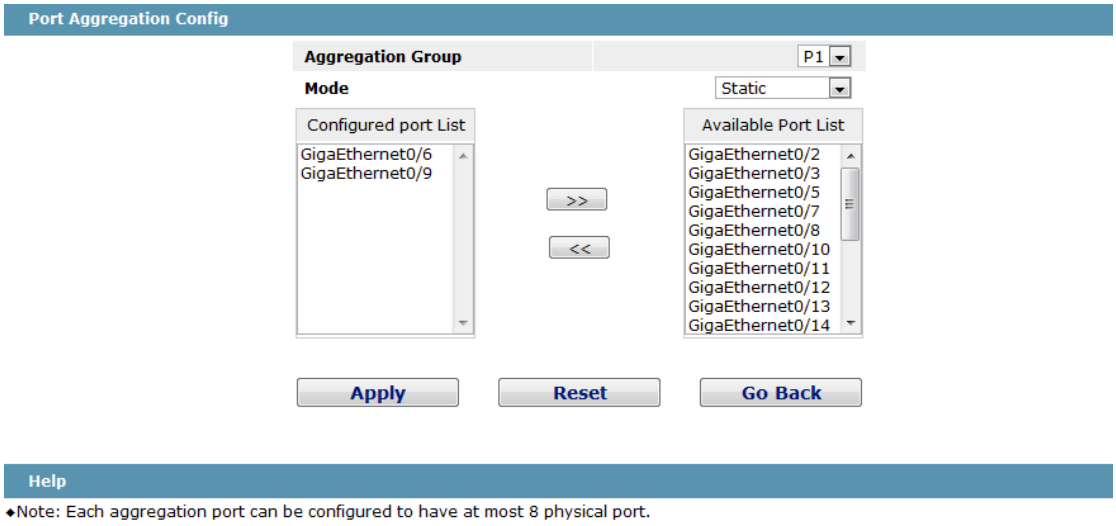


Figure 13-21 Port Aggregation Configuration

If you create an aggregation group, it is optional; if you modify the aggregation group, it is not optional.

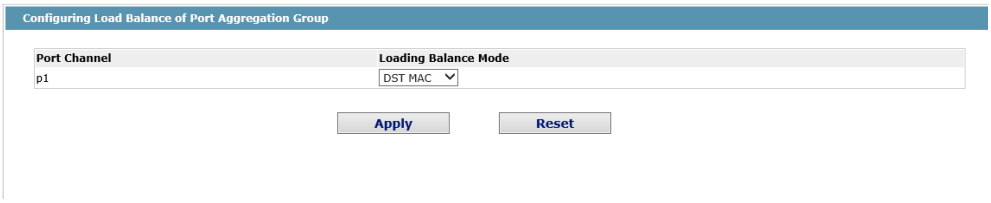
When the aggregation port has a member port, the user can select the aggregation mode: static, LACP Active and LACP Passive.

You can click ">>" and "<<" to delete and add an aggregation member port.

13.9.2 5.9.2 Port Channel Group Loading Balance Configuration

Some models support link aggregation load balancing configuration and others not, but they can be configured in the global configuration mode.

3928 supports the aggregation group based load balancing configuration:



The Aggregation Group Based Load Balancing Configuration

You can use different aggregation groups to set different aggregation modes.

13.10 Ring Protection Configuration

13.10.1 EAPS Ring List

If you click Layer-2 Config -> Ring protection Config, the EAPS ring list page appears.

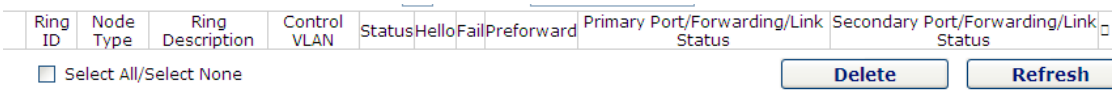


Figure 13-22 EAPS Ring List

In the list shows the currently configured EAPS ring, including the status of the ring, the forwarding status of the port and the status of the link.

Click "New" to create a new EAPS ring.

Click the "Operate" option to configure the "Time" parameter of the ring.

NOTE:

1. The system can support 8 EAPS rings.
2. After a ring is configured, its port, node type and control Vlan cannot be modified. If the port of the ring, the node type or the control Vlan need be adjusted, please delete the ring and then establish a new one.

13.10.2 EAPS Ring Configuration

If you click "New" on the EAPS ring list, or "Operate" on the right side of a ring item, the "Configure EAPS" page appears.

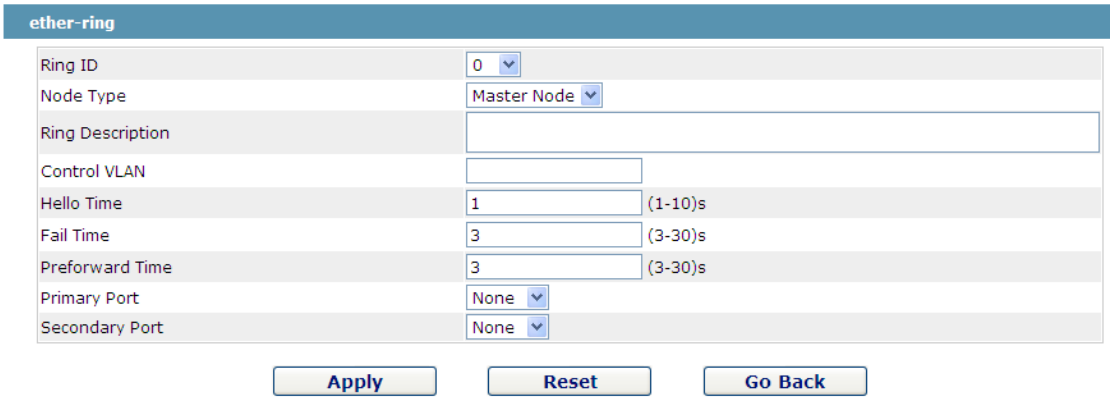


Figure 13-23 EAPS ring configuration

NOTE: If you want to modify a ring, on this page the node type, the control VLAN, the primary port and the secondary port cannot be modified.

In the dropdown box on the right of "Ring ID", select an ID as a ring ID. The ring IDs of all devices on the same ring must be the same.

The dropdown box on the right of "Node Type" is used to select the type of the node. Please note that only one master node can be configured on a ring.

Enter a value between 1 and 4094 in the text box on the right of "Control VLAN" as the control VLAN ID. When a ring is

established, the control VLAN will be automatically established too. Please note that if the designated control VLAN is 1 and the VLAN of the control device is also 1 the control device cannot access the control VLAN. Additionally, please do not enter a control VLAN ID that is same as that of another ring.

In the text boxes of “Primary Port” and “Secondary Port”, select a port as the ring port respectively. If "Node Type" is selected as “Transit-Node”, the two ports will be automatically set to transit ports.

Click “Apply” to finish EAPS ring configuration, click “Reset” to resume the initial values of the configuration, or click “Return” to go back to the EAPS list page.

13.11 MEAPS Configuration

13.11.1 MEAPS Ring Network List

Click “L2 Config” -> “Multiple Ring Protection” in the navigation bar, and enter the multiple ring protection configuration page.

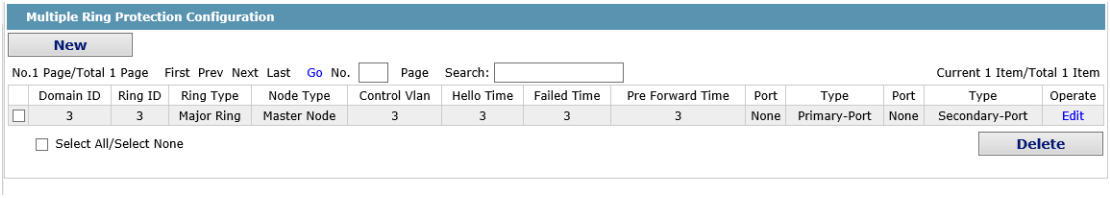


Figure 13-24 MEAPS Network List

The list displays the currently configured MEAPS ring, including the domain ID, the ring ID, the ring type, the node type, control VLAN, Hello Time, Fail Time, Pre Forward Time and the primary and secondary port on the ring.

Click “New” to create MEAPS ring network.

Click “Modify” right of the entry to configure the time parameter, and the primary and secondary port of the ring network.

NOTE:

1. MEAPS domain numbers the system supported is 4 (0-3).
2. The ring numbers supported in the domain is 8 (0-7).
3. Once one MEAPS has configured, its ID, ring ID, ring type, node type and control Vlan cannot be configured. If these parameters need to be configured, please delete the net ring and re-create it.

13.11.2 EAPS Ring Network Configuration

Click “New” in the EAPS ring list or “Modify” right of the ring entry, and enter EAPS ring network configuration page.

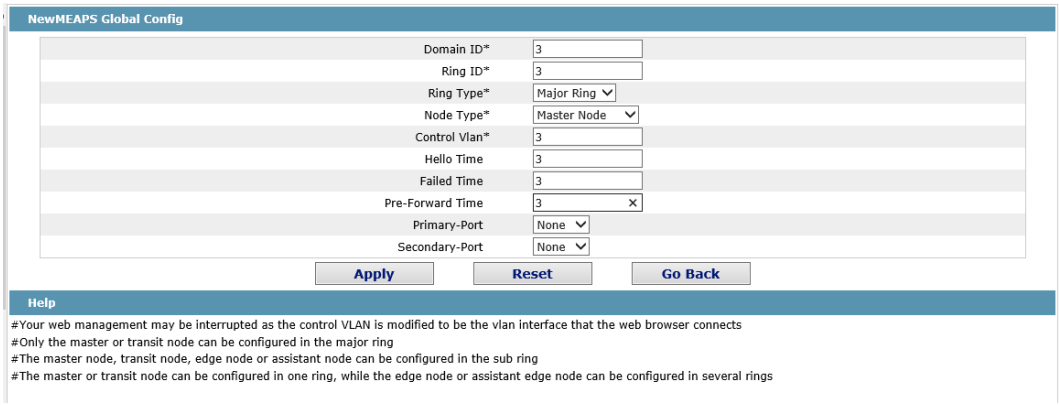


Figure 13-25 MEAPS Configuration

NOTE: Once one MEAPS has configured, its ID, ring ID, ring type, node type and control Vlan cannot be configured.

The primary ring can only configure the master node and the transit node.

The secondary ring can configure the primary node, the transit node, the edge node

The primary node and the transit node can only exit in one ring, and the edge node and the assistant edge node can exist in many rings simultaneously.

In the text boxes of "Primary Port" and "Secondary Port", select a port as the ring port respectively or select "None".

13.12 Backup Link Protocol Configuration

13.12.1 Backup Link Protocol Global Configuration

If you click Layer-2 Config ->Backup Link Config ->Backup Link Protocol Global Config on the navigation bar, the Backup Link Protocol Global Config page appears.

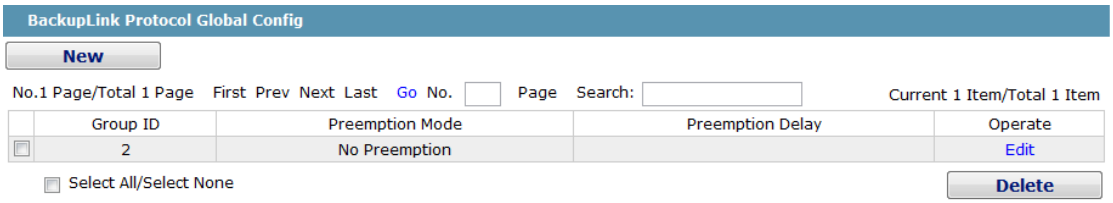


Figure 13-26 Backup Link Protocol Global Configuration

On the page, the current configured backup link groups are shown, including Preemption Mode and Preemption Delay.

Click **New** to create a new link backup group.

Click **Edit** on the right to configure Preemption Mode and Preemption Delay.

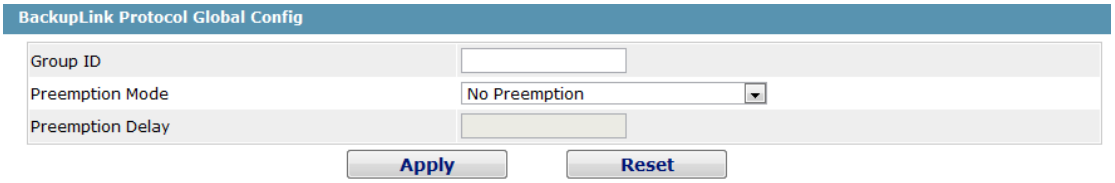


Figure 13-27 Backup Link Protocol Global Configuration

NOTE:

1. The system supports 8 link backup groups.
2. The Preemption mode determines the policy the primary port and the backup port forward packets.

13.12.2 Backup Link Protocol Interface Configuration

If you click Layer-2 Config -> Backup Link Protocol Config -> Backup Link Protocol Interface Config on the navigation bar, the Backup Link Protocol Global Config page appears.

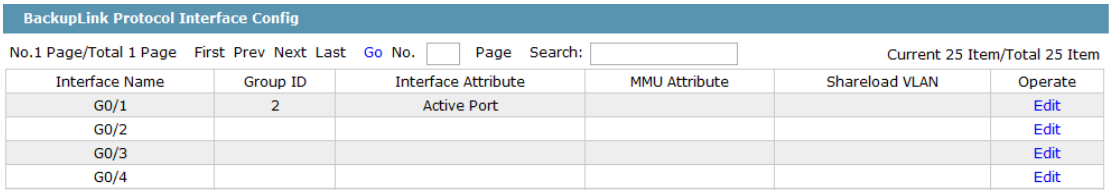


Figure 13-28 Backup Link Protocol Interface Configuration

This page shows the backup link group's member ports, Interface Attribute, MMU Attribute, Shareload Vlan, etc.

Click **Edit** on the right to configure the Backup Link Protocol.

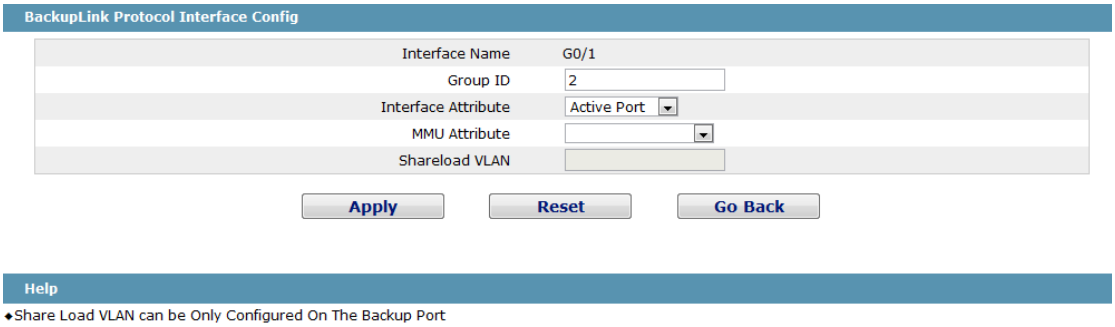


Figure 13-29 Backup Link Protocol Interface Configuration

The backup link group which has configured the primary port cannot take other ports as its primary port. Likewise, the backup link group which has configured the backup port cannot take other ports as its backup port.

13.13 MTU Configuration

If you click **Layer-2 Config -> MTU Config** on the navigation bar, the **MTU Config** page appears.

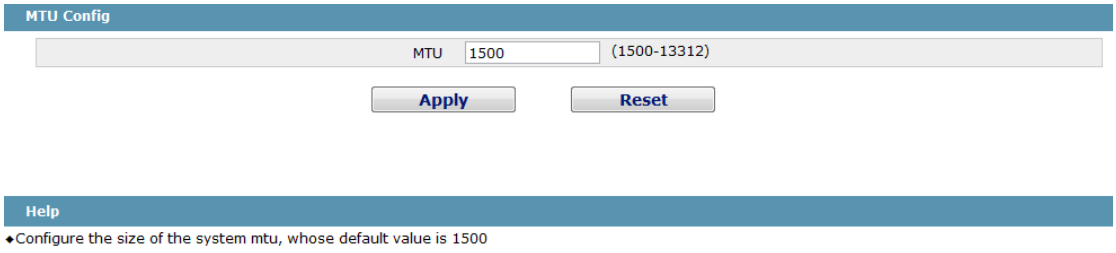


Figure 13-30 MTU Configuration

You can set the size of the maximum transmission unit (MTU).

13.14 PDP Configuration

13.14.1 Configuring the Global Attributes of PDP

If you click Layer-2 Config -> PDP Config -> PDP Global Config in the navigation bar, the Basic Config of PDP Protocol page appears.

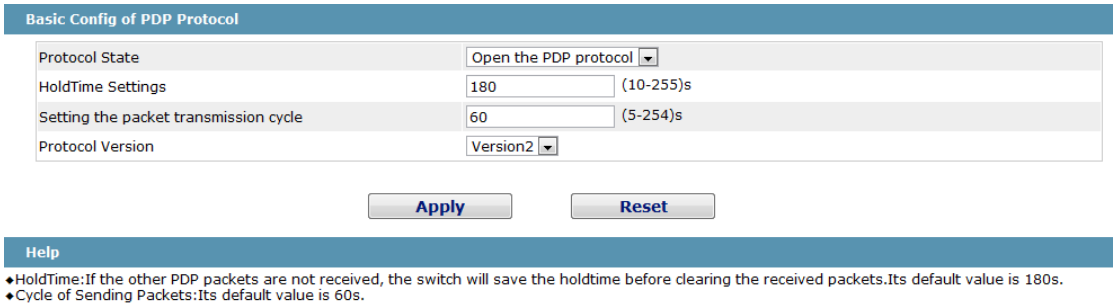


Figure 13-31 Basic Config of PDP Protocol

You can choose to enable PDP or disable it. When you choose to disable PDP, you cannot configure PDP.

The "**Hold Time**" parameter means the time to be saved before the router discards the received information if other PDP packets are not received.

13.14.2 PDP Interface Attribute Configuration

If you click Layer-2 Config -> PDP Config-> PDP Interface Config in the navigation bar, the Protocol Port Config page appears.



Figure 13-32 PDP Interface Attribute Configuration

After the PDP port is configured, you can enable or disable PDP on this port.

Chapter 14 Layer-3 Configuration



Figure 14-1: Layer-3 configuration list

14.1 Configuring the VLAN Interface

If you click Layer-3 Config -> VLAN interface and IP address Config, the Configuring the VLAN interface page appears.

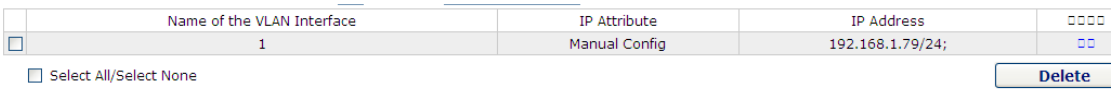


Figure 14-2: Configuring the VLAN interface

Click **New** to add a new VLAN interface. Click **Cancel** to delete a VLAN interface. Click **Modify** to modify the settings of a corresponding VLAN interface.

When you click **New**, the name of the corresponding VLAN interface can be modified; but if you click **Modify**, the name of the corresponding VLAN interface cannot be modified.

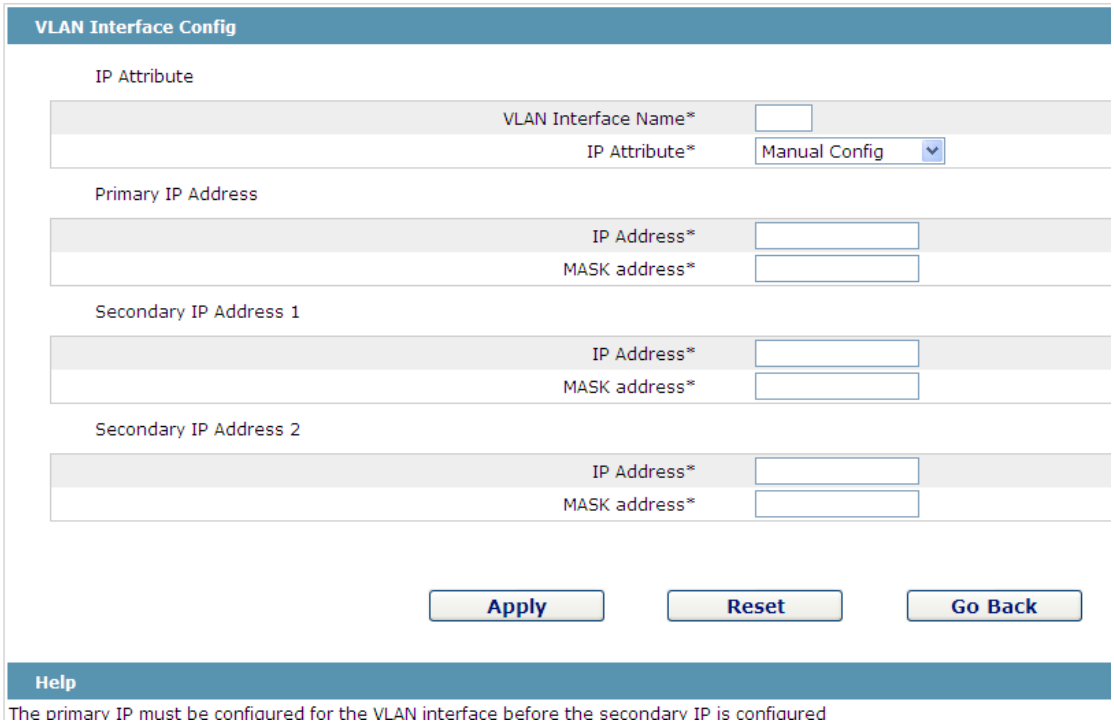


Figure 14-3: VLAN interface configuration

NOTE: Before the accessory IP of a VLAN interface is set, you have to set the main IP.

14.2 Static Routing Configuration

If you click Layer-3 Config -> Static Routing, the Configuring the static routing table page appears.

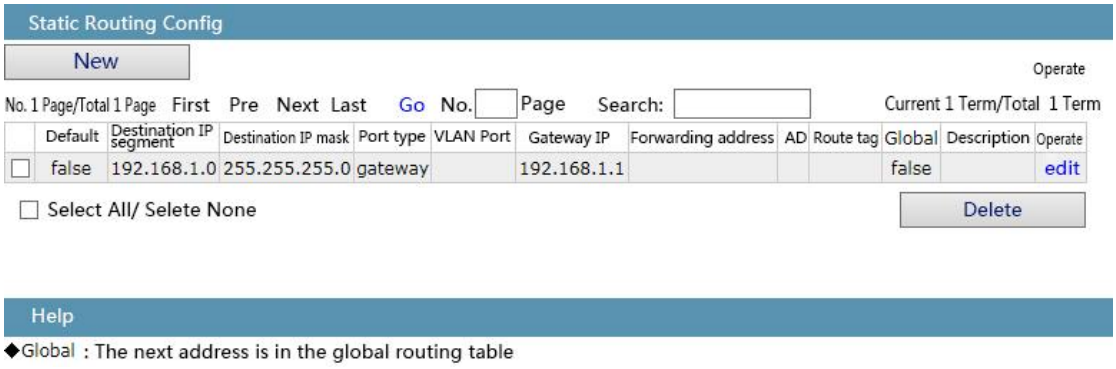


Figure 14-4: configure Static Routing

Click **New** to add a new static routing table.

Click **Modify** to modify the settings of a corresponding static routing table.

Click **Cancel** to delete a static routing table.

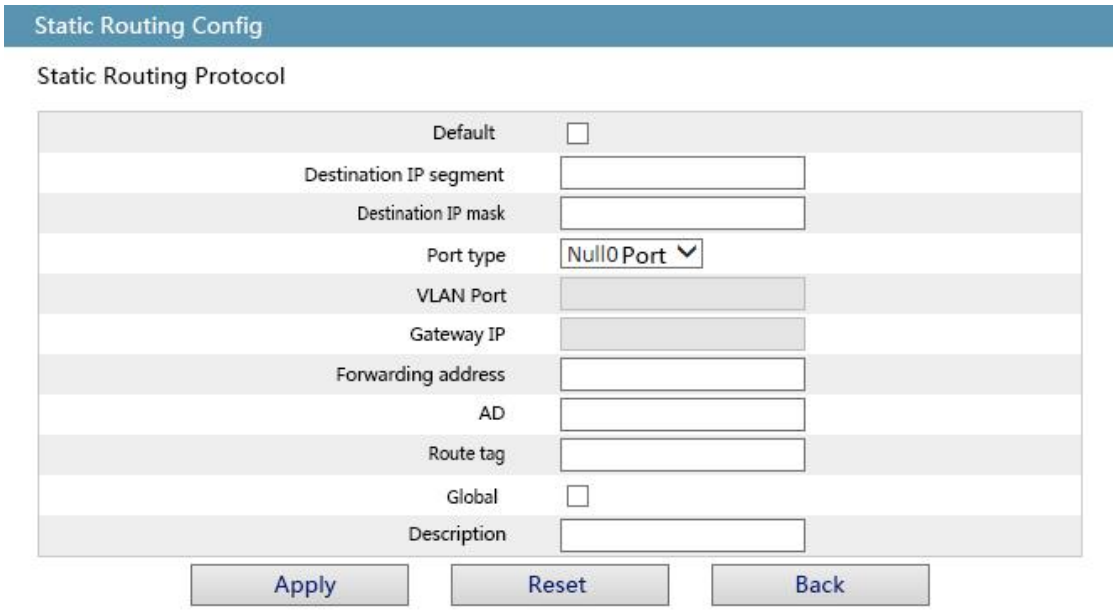


Figure 14-5: Static Routing configuration

Chapter 15 Advanced Configuration



Figure 15-1 A list of advanced configuration

15.1 QoS Configuration

15.1.1 Configuring QoS Port

If you click Advanced Config -> QoS -> Configure QoS Port, the Port Priority Config page appears.

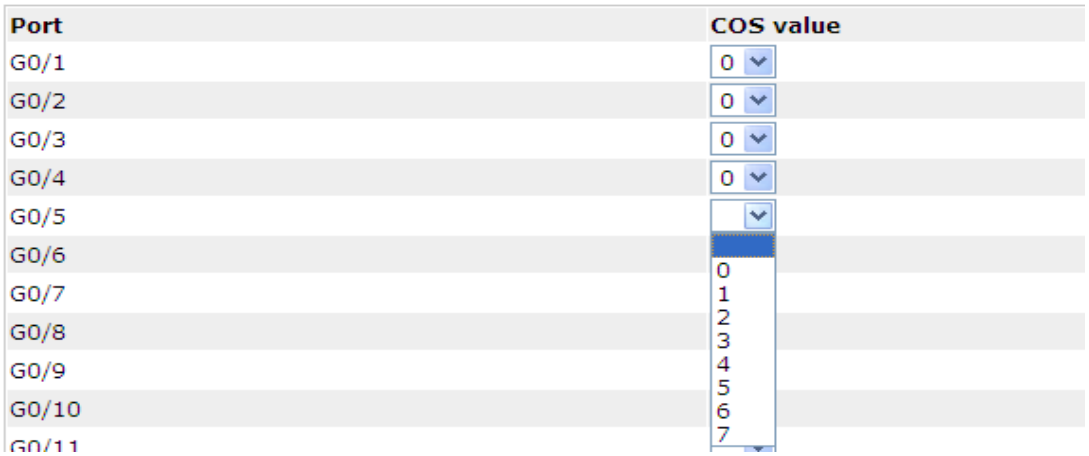


Figure 15-2 Configuring the QoS Port

You can set the CoS value by clicking the dropdown box on the right of each port and selecting a value. The default CoS value of a port is 0, meaning the lowest priority. If the CoS value is 7, it means that the priority is the highest.

15.1.2 Global QoS Configuration

If you click Advanced Config -> QoS Config -> Global QoS Config, the Port's QoS parameter configuration page appears.

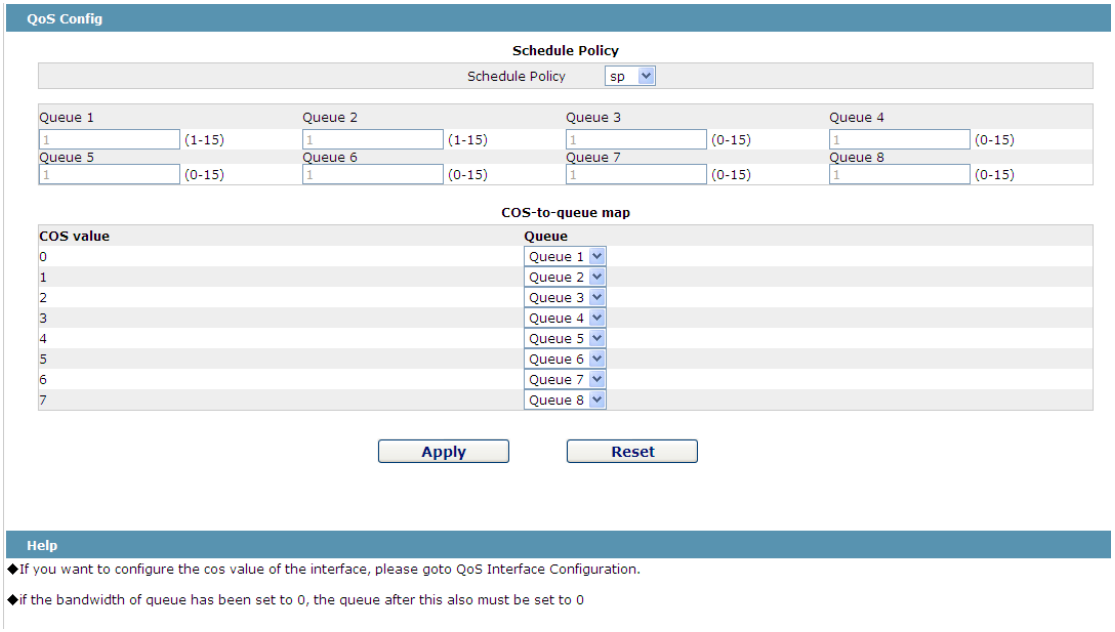


Figure 15-3 Configuring global QoS attributes

In WRR schedule mode, you can set the weights of the QoS queues. There are 4 queues, among which queue 1 has the lowest priority and queue 4 has the highest priority.

15.2 IP Access Control List

15.2.1 Setting the Name of the IP Access Control List

If you click Advanced Config -> IP access control list -> IP access control list Config, the IP ACL configuration page appears.

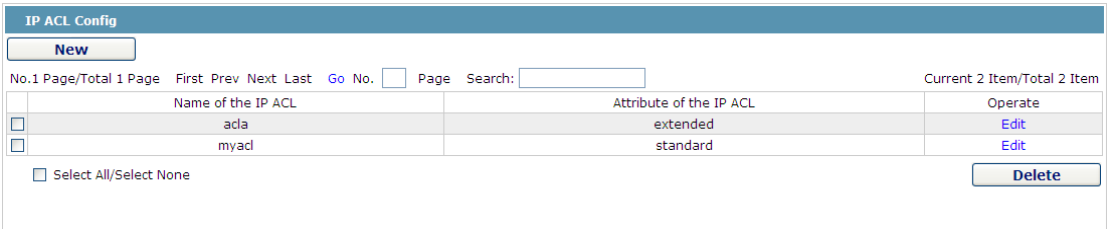


Figure 15-4: IP access control list configuration

Click **New** to add a name of the IP access control list. Click **Cancel** to delete an IP access control list.

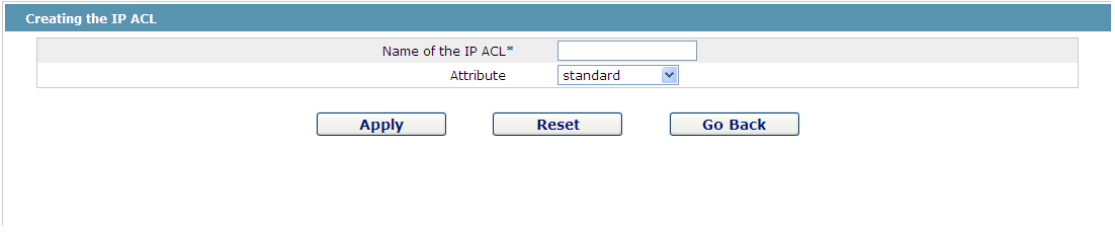


Figure 15-5: Creating a name of the IP access control list

If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

15.2.2 Setting the Rules of the IP Access Control List

Standard IP access control list

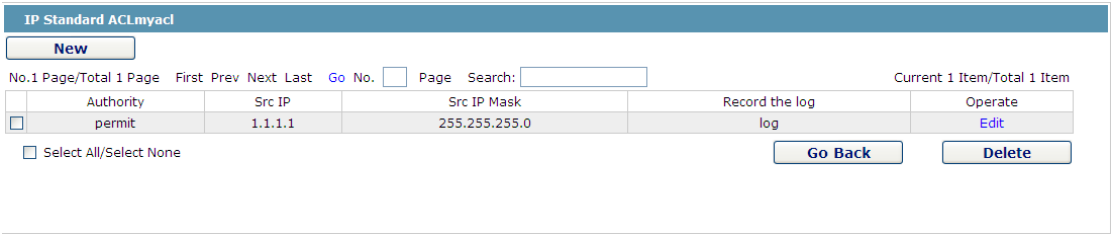


Figure 15-6: Standard IP access control list

Click **New** to add a rule of the IP access control list. Click **Cancel** to delete a rule of the IP access control list. If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

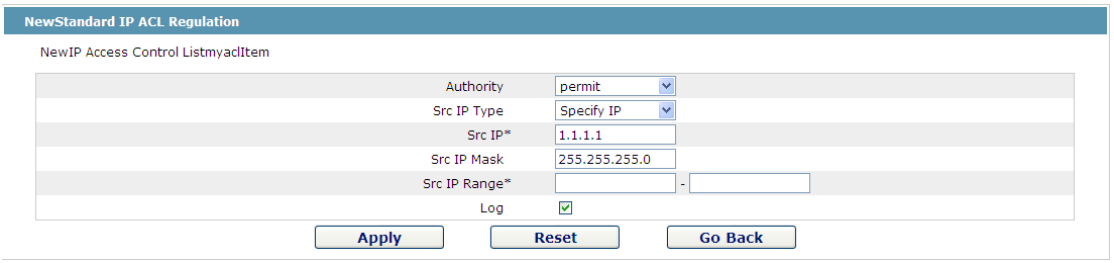


Figure 15-7: Setting the Rules of the standard IP access control list

Extended IP access control list

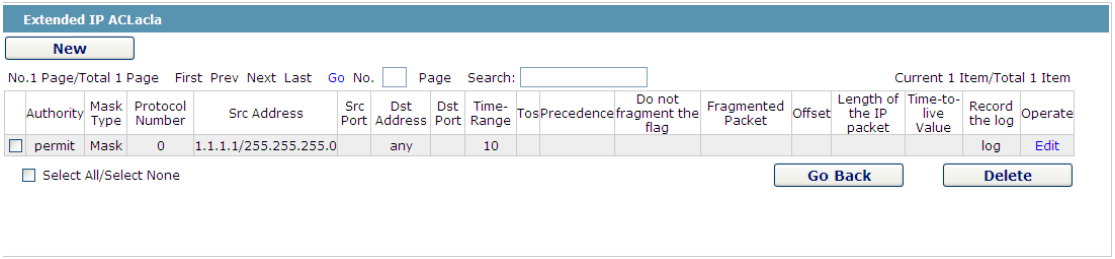


Figure 15-8: Extended IP access control list

Click **New** to add a rule of the IPaccess control list. Click **Cancel** to delete a rule of the IP access control list. If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

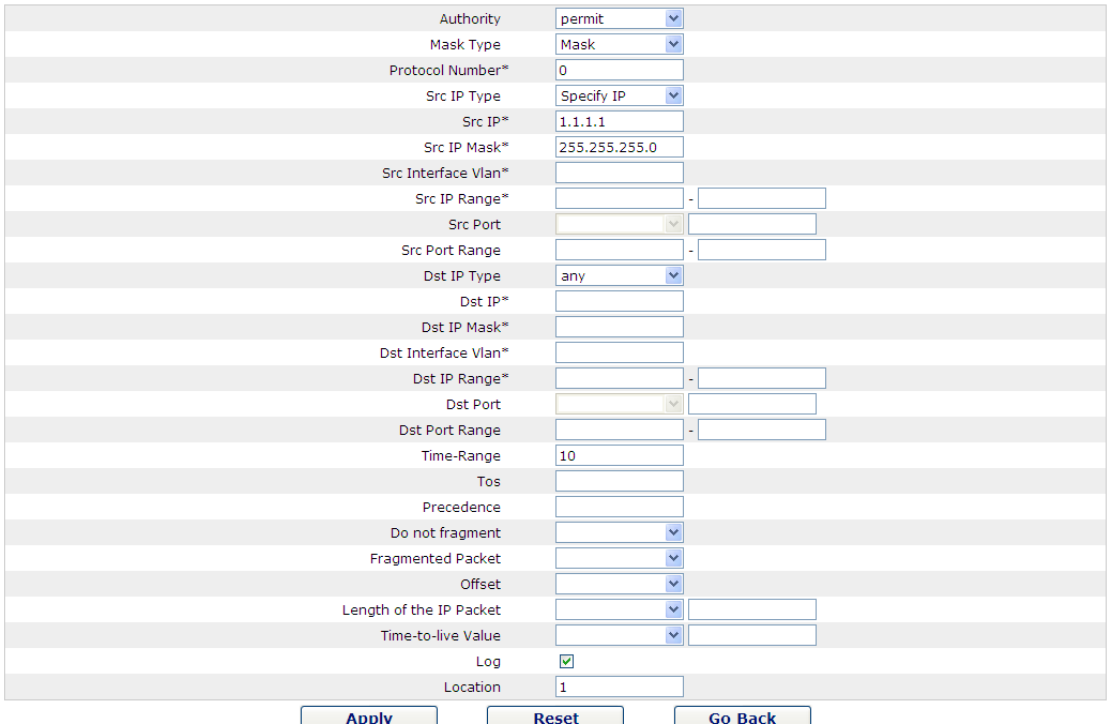


Figure 15-9: Setting the Rules of the extended IP access control list

15.2.3 Applying the IP Access Control List

If you click Advanced Config -> IP access control list -> Applying the IP access control list, the Applying the IP access control list page appears.

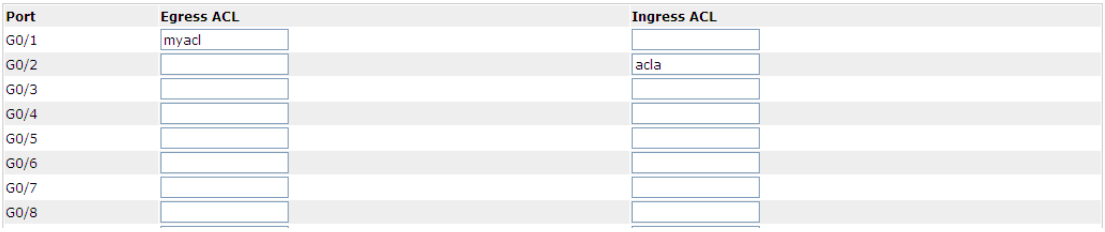


Figure 15-10: Applying the IP access control list

15.3 MAC Access Control List

15.3.1 Setting the Name of the MAC Access Control List

If you click Advanced Config -> MAC access control list -> MAC access control list Config, the MAC ACL configuration page appears.

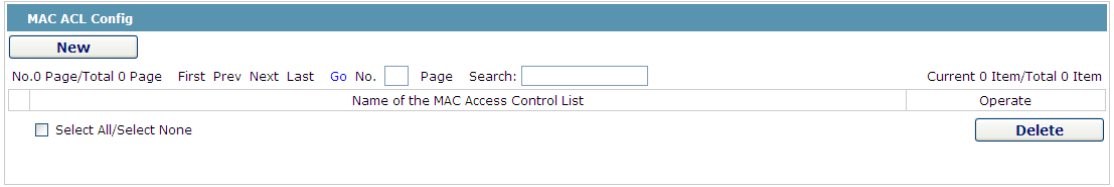


Figure 15-11: MAC access control list configuration

Click **New** to add a name of the MAC access control list. Click **Cancel** to delete a MAC access control list.



Figure 15-12: Setting the name of MAC access control list

15.3.2 Setting the Rules of the MAC Access Control List

If you click **Modify**, the corresponding MAC access control list appears and you can set the corresponding rules for the MAC access control list.

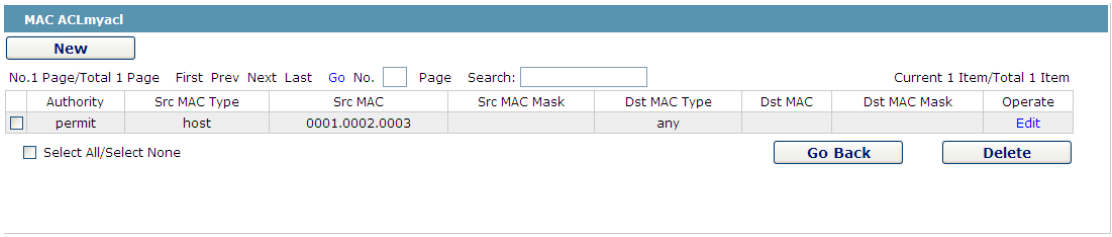


Figure 15-13: Specific MAC access control list configuration

Click **New** to add a rule of the MAC access control list. Click **Cancel** to delete a rule of the MAC access control list.

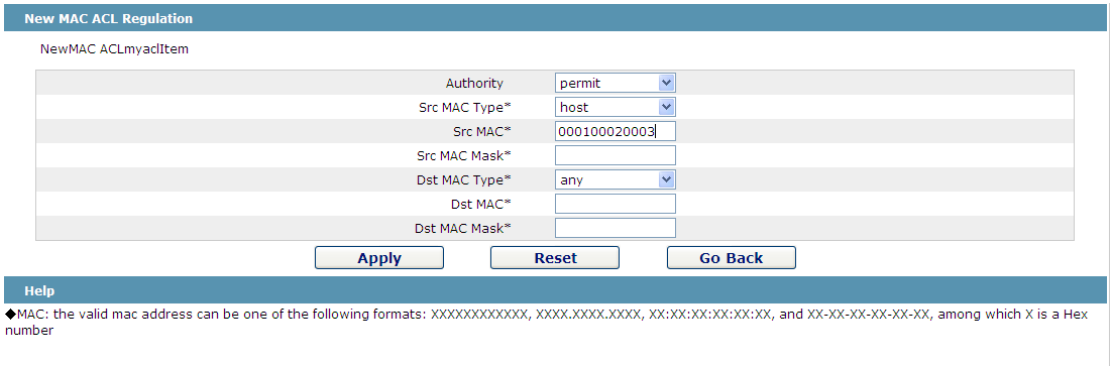


Figure 15-14: Setting the Rules of the MAC Access Control List

15.3.3 Applying the MAC Access Control List

If you click Advanced Config -> MAC access control list -> Applying the MAC access control list, the Applying the MAC access control list page appears.

Port	Egress ACL	Ingress ACL
G0/1		
G0/2		
G0/3		
G0/4		
G0/5		
G0/6		
G0/7		

Figure 15-15: Applying the MAC access control list

Chapter 16 Network Management Configuration

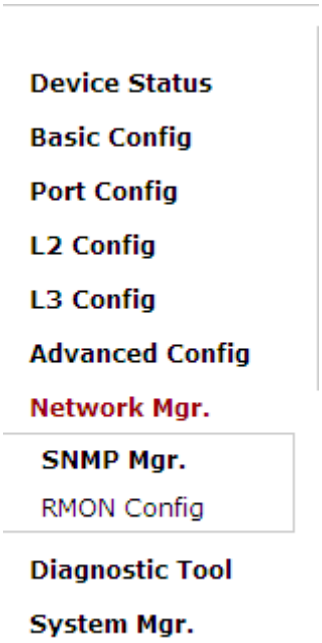


Figure 16-1 Network management configuration list

16.1 SNMP Configuration

If you click **Network management Config** -> **SNMP management** in the navigation bar, the **SNMP management** page appears, as shown in figure 2.

16.1.1 SNMP Community Management

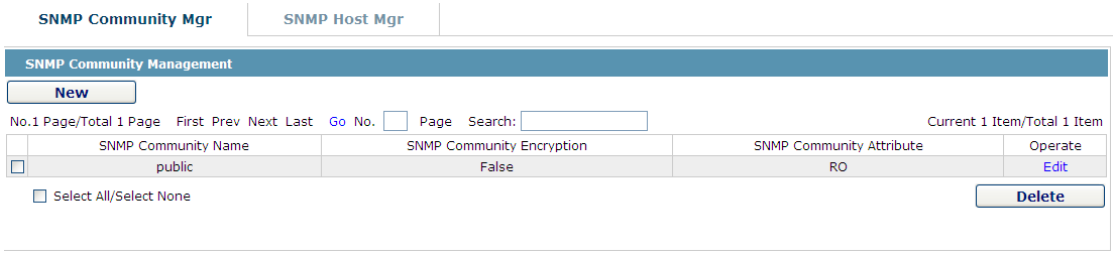


Figure 16-2 SNMP community management

On the SNMP community management page, you can know the related configuration information about SNMP community.

You can create, modify or cancel the SNMP community information, and if you click **New** or **Edit**, you can switch to the configuration page of SNMP community.

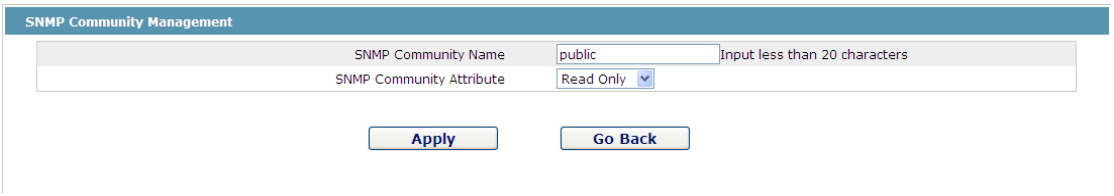


Figure 16-3 SNMP community management settings

On the SNMP community management page you can enter the SNMP community name, select the attributes of SNMP community, which include Read only and Read-Write.

16.1.2 SNMP Host Management

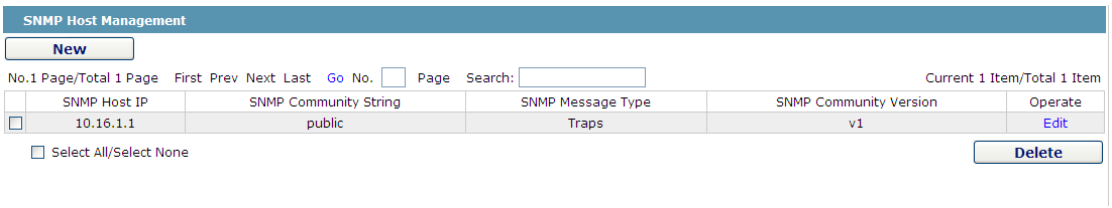


Figure 16-4 SNMP host management

On the SNMP community host page, you can know the related configuration information about SNMP host.

You can create, modify or cancel the SNMP host information, and if you click **New** or **Edit**, you can switch to the configuration page of SNMP host.

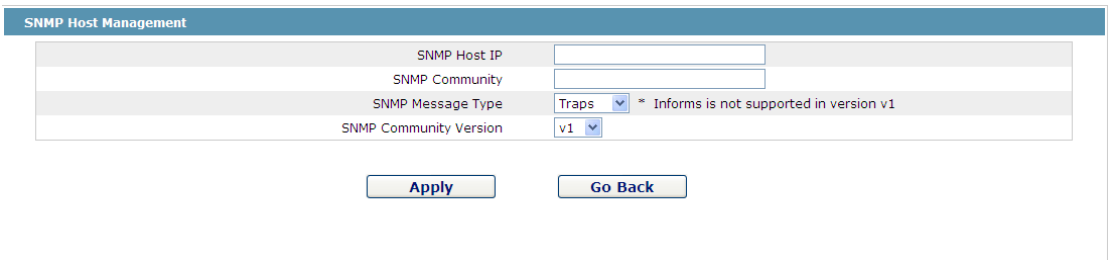


Figure 16-5 SNMP host management settings

On the SNMP host configuration page, you can enter SNMP Host IP, SNMP Community, SNMP Message Type and SNMP Community Version. SNMP Message Type includes Traps and Informs, and as to version 1, SNMP Message Type does not support Informs.

16.2 RMON

16.2.1 RMON Statistic Information Configuration

If you click Network Management Config -> RMON -> RMON Statistics -> New, the RMON Statistics page appears.

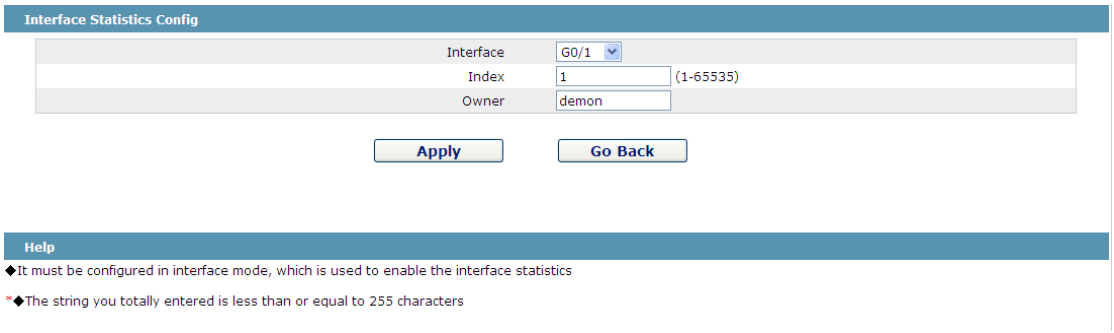


Figure 16-6 Configuring the RMON statistic information

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

At present, the monitor statistic information can be obtained through the command line "show rmon statistics", but the Web does not support this function.

16.2.2 RMON History Information Configuration

If you click Network Management Config -> RMON -> RMON history -> New, the RMON history page appears.

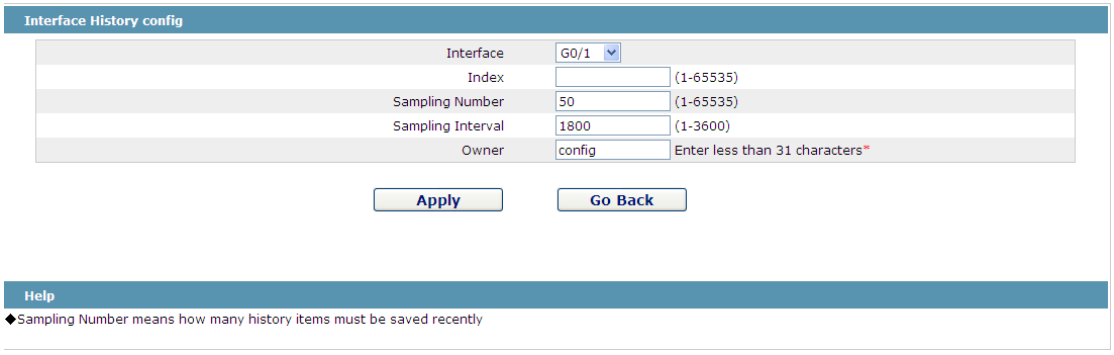


Figure 16-7 Configuring the RMON history information

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

The sampling number means the items that need be reserved, whose default value is 50.

The sampling interval means the time between two data collection, whose default value is 1800s.

At present, the monitor statistic information can be obtained through the command line "show rmon history", but the Web does not support this function.

16.2.3 RMON Alarm Information Configuration

If you click Network Management Config -> RMON -> RMON Alarm -> New, the RMON Alarm page appears.

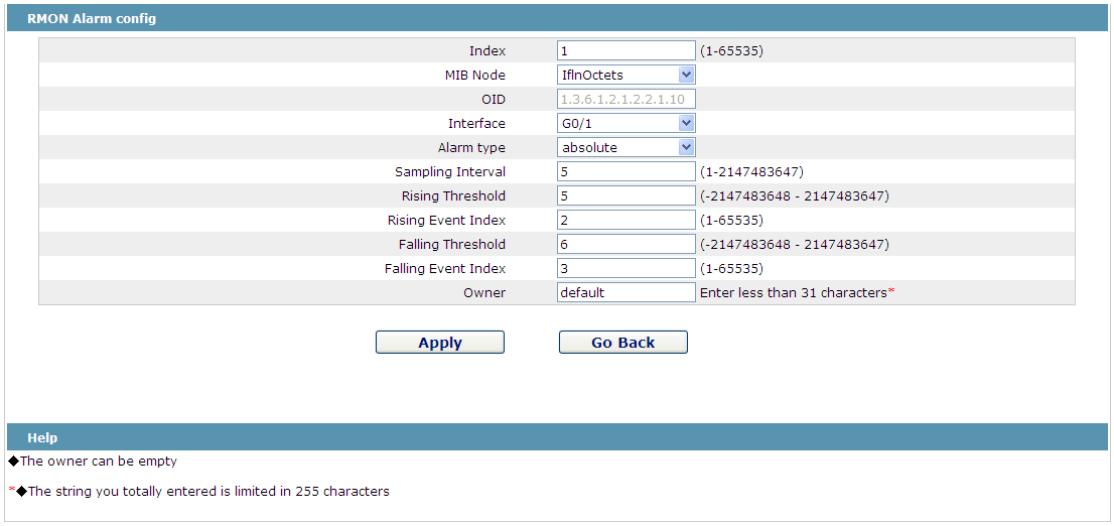


Figure 16-8 Configuring the RMON alarm information

The index is used to identify a specific alarm information; if the index is same to the previously applied index, it will replace the previous one.

The MIB node corresponds to OID.

If the alarm type is **absolute**, the value of the MIB object will be directly minitored; if the alarm type is **delta**, the change of the value of the MIB object in two sampling will be monitored.

When the monitored MIB object reaches or exceeds the rising threshold, the event corresponding to the index of the rising event will be triggered.

When the monitored MIB object reaches or exceeds the falling threshold, the event corresponding to the index of the falling event will be triggered.

16.2.4 RMON Event Configuration

If you click Network Management Config -> RMON -> RMON Event -> New, the RMON event page appears.

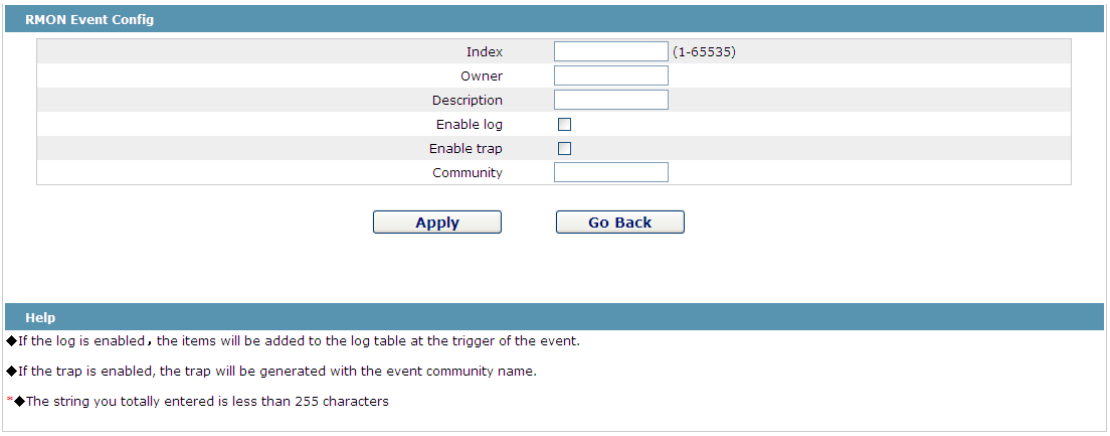


Figure 16-9 RMON event configuration

The index corresponds to the rising event index and the falling event index that have already been configured on the **RMON alarm config** page.

The owner is used to describe the descriptive information of an event.

"Enable log" means to add an item of information in the log table when the event is triggered.

“Enable trap” means a trap will be generated if the event is triggered.

Chapter 17 Diagnosis Tools



Figure 17-1 Diagnosis tool list

17.1 Ping

17.1.1 Ping

If you click **Diagnosis Tools** -> **Ping**, the **Ping** page appears.

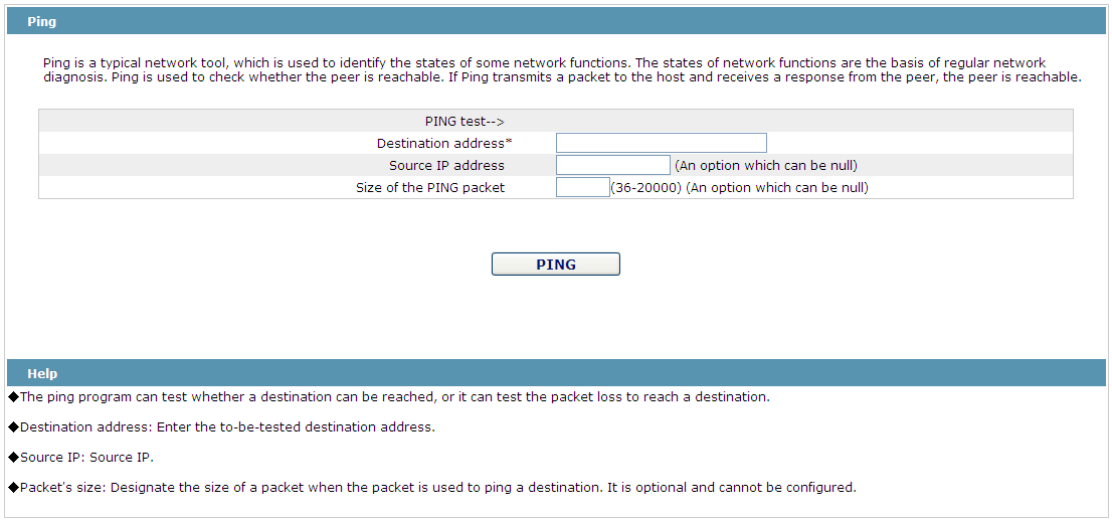


Figure 17-2 Ping

Ping is used to test whether the switch connects other devices.

If a Ping test need be conducted, please enter an IP address in the “Destination address” textbox, such as the IP address of your PC, and then click the “PING” button. If the switch connects your entered address, the device can promptly return a test result to you; if not, the device will take a little more time to return the test result.

"Source IP address" is used to set the source IP address which is carried in the Ping packet.

"Size of the PING packet" is used to set the length of the Ping packet which is transmitted by the device.

Chapter 18 System Management



Figure 18-1 Navigation list of system management

18.1 User Management

18.1.1 User List

If you click System Manage -> User Manage, the User Management page appears.

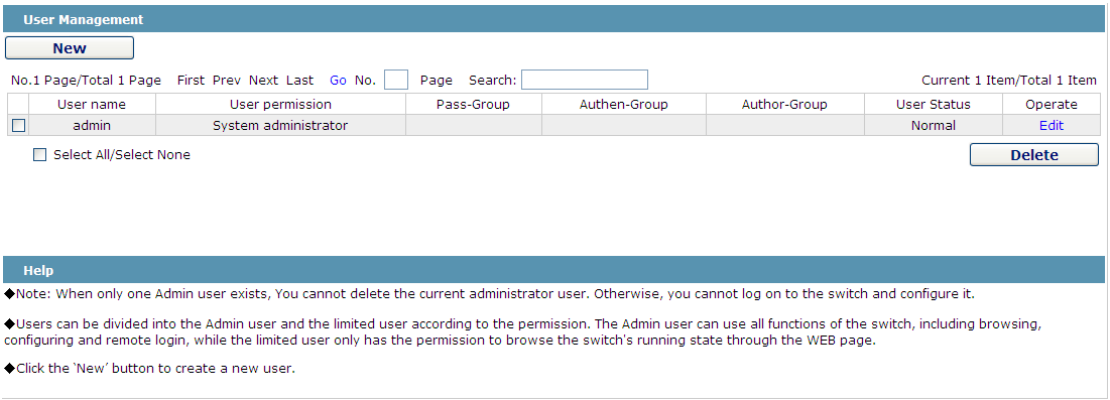


Figure 18-2 User list

You can click "New" to create a new user.

To modify the permission or the login password, click "Edit" on the right of the user list.

NOTE:

1. Please make sure that at least one system administrator exists in the system, so that you can manage the devices through Web.
2. The limited user can only browse the status of the device.

18.1.2 Establishing a New User

If you click "New" on the **User Management** page, the **Creating User** page appears.

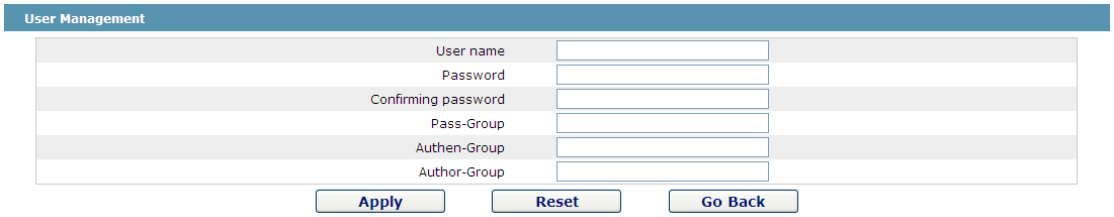


Figure 18-3 Creating new users

In the "User name" text box, enter a name, which contains letters, numbers and symbols except "?", "\", "&", "#" and the "Space" symbol. \ " & # and characters other than spaces.

In the "Password" textbox enter a login password, and in the "Confirming password" textbox enter this login password again.

In the "User permission" dropdown box set the user's permission. The "System administrator" user can browse the status of the device and conduct relevant settings, while the limited user can only browse the status of the device.

18.1.3 User Group Management

If you click **New** on the **User Mgr.** page, the **User Group Management** page appears.

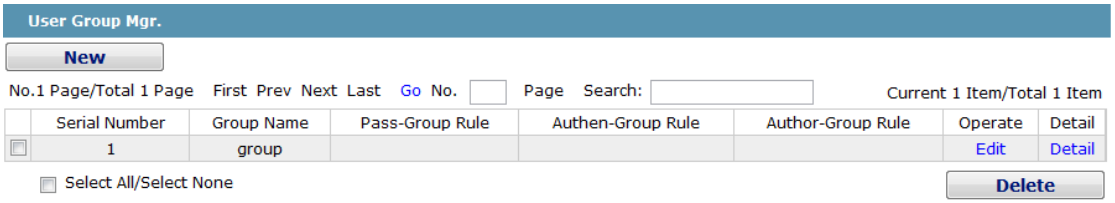


Figure 18-4 User group list

Click **New** to create a new user group.

Click **Delete** to delete the user group.

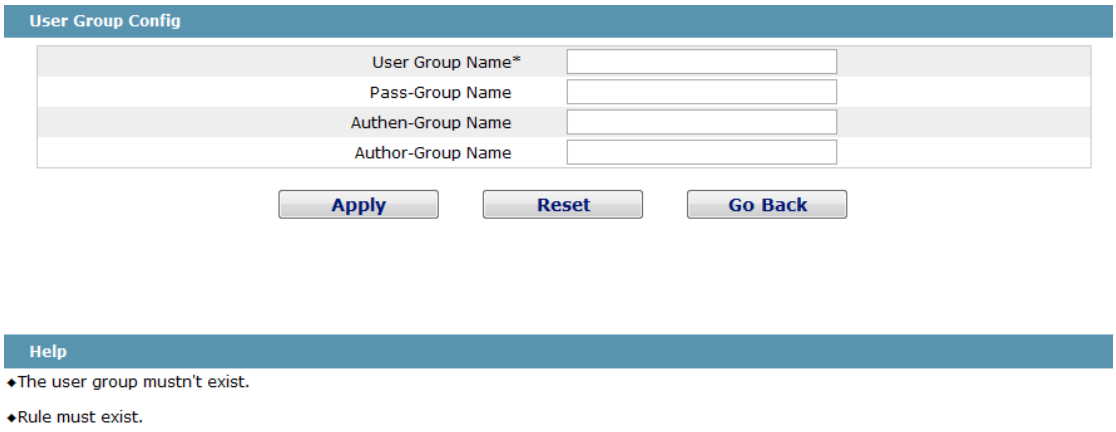


Figure 18-5 User group configuration

The User Group Name must be different with the existing group names. The user group cannot be created until the Pass-Group name, Authen-Group Name and Author-Group Name are specified. Configuring the Pass-Group name, Authen-Group Name and Author-Group Name in another 3 pages.

18.1.4 Password Group Management

Click Pass-Group Mgr. and the Pass-Group Mgr. page appears.

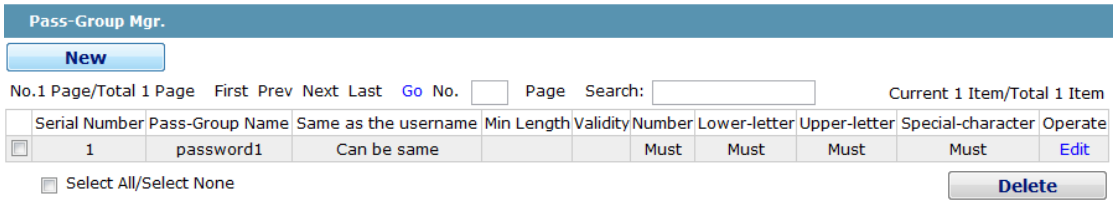
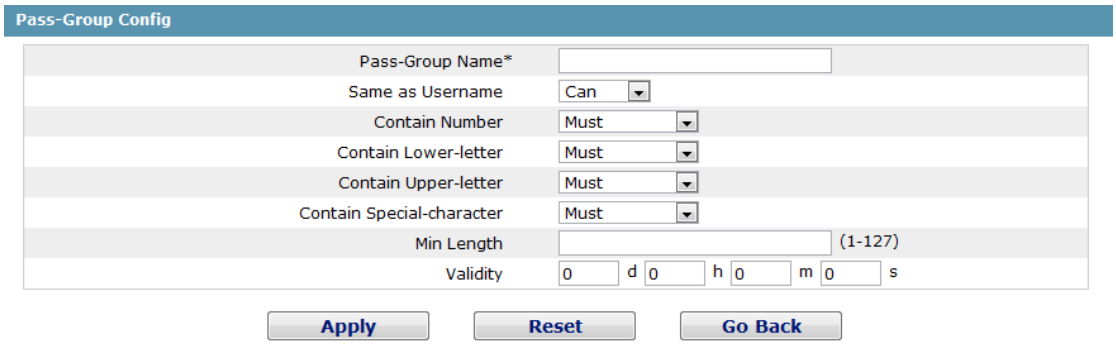


Figure 18-6 Password Group Management

Click **New** to create a new password rule.

Click **Delete** to delete the password rule.



In the Pass-Group Configuration, the password can be set whether to be same as Username, Contain Number, Contain Lower-letter, Contain Upper-letter, Contain Special-character, Min Length and validity.

The rule can be applied to the user management. The password is valid only when it conforms to the rule.

18.1.5 Authentication Group Configuration

Click **Authen-Group Mgr.** on the navigation bar, and **Authen-Group Mgr.** appears.

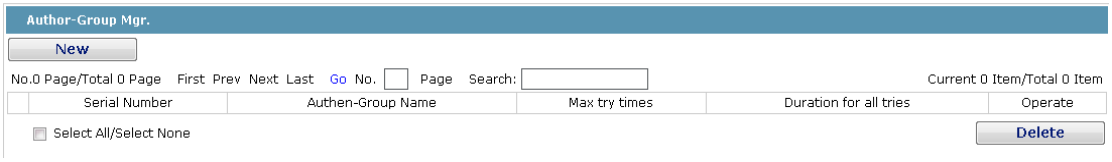
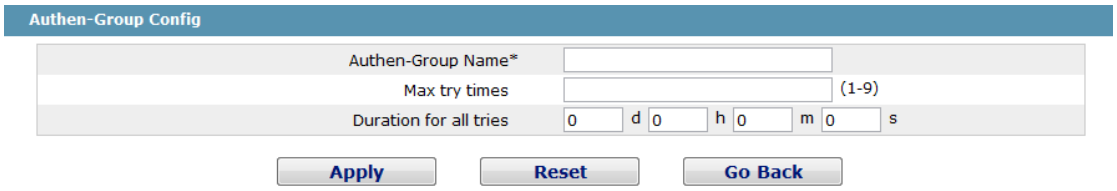
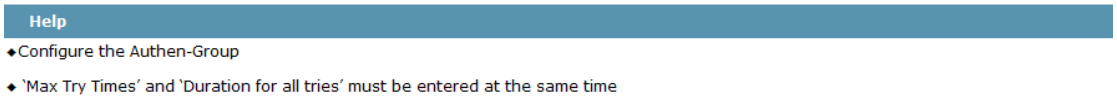


Figure 18-7 Pass Group Configuration

Click **New** to create a new authorization rule.

Click **Delete** to delete the authorization rule.





The **Max try times** and **Duration of all tries** can be configured or not. But they must be adjusted simultaneously.

18.1.6 Authorization Group Management

If you click **Author-Group Mgr.** and the **Author-Group Mgr.** page appears.

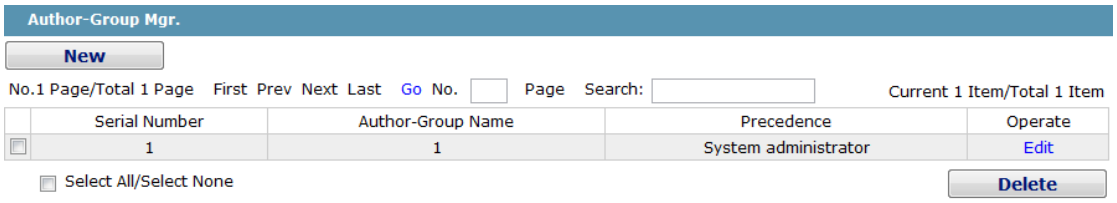


Figure 18-8 Author Group Management

Click **New** to create a new authorization rule.

Click **Delete** to delete the new authorization rule.

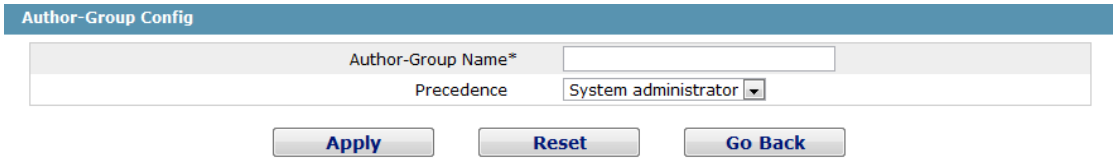


Figure 18-7 Author Group Configuration

The authorization rule determines the user's access: Administrator or Limited user. The **Administrator** has full access to the configuration and the **Limited user** only has access to check the configuration.

18.2 Log Management

If you click System Manage -> Log Manage, the Log Management page appears.

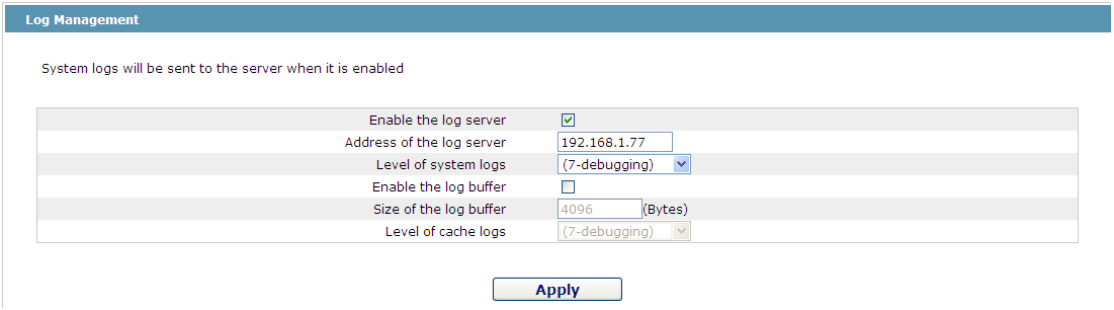


Figure 18-8 Log management

If "Enabling the log server" is selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the "Address of the system log server" textbox and select the log's grade in the "Grade of the system log information" dropdown box.

If "Enabling the log buffer" is selected, the device will record the log information to the memory. By logging on to the device through the Console port or Telnet, you can run the command "show log" to browse the logs which are saved on the device. The log information which is saved in the memory will be lost after rebooting. Please enter the size of the buffer area in the "Size of the system log buffer" textbox and select the grade of the cached log in the "Grade of the cache log information" dropdown box.

18.3 Managing the Configuration Files

If you click System Manage -> Configuration file, the Configuration file page appears.

18.3.1 Exporting the Configuration Information

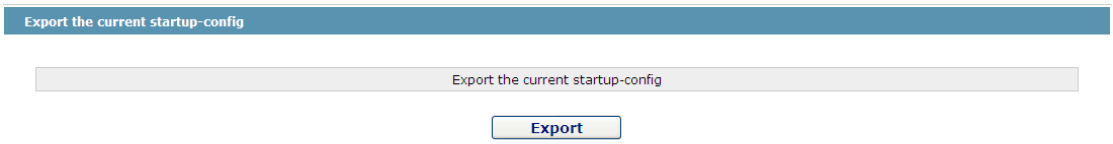


Figure 18-9 Exporting the configuration file

The current configuration file can be exported, saved in the disk of PC or in the mobile storage device as the backup file.

To export the configuration file, please click the "Export" button and then select the "Save" option in the pop-up download dialog box.

The default name of the configuration file is "startup-config", but you are suggested to set it to an easily memorable name.

18.3.2 Importing the Configuration Information

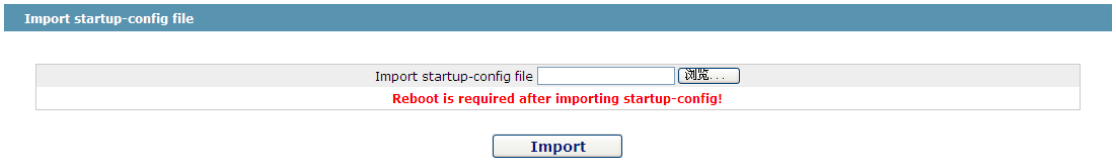


Figure 18-10 Importing the configuration files

You can import the configuration files from PC to the device and replace the configuration file that is currently being used. For example, by importing the backup configuration files, you can resume the device to its configuration of a previous moment.

NOTE:

1. Please make sure that the imported configuration file has the legal format for the configuration file with illegal format cannot lead to the normal startup of the device.
2. If error occurs during the process of importation, please try it later again, or click the "Save All" button to make the device re-establish the configuration file with the current configuration, avoiding the incomplete file and the abnormality of the device.
3. After the configuration file is imported, if you want to use the imported configuration file immediately, do not click "Save All", but reboot the device directly.

18.4 Software Management

If you click **System Manage -> Software Upgrade**, the software management page appears.

18.4.1 Backing up the IOS Software

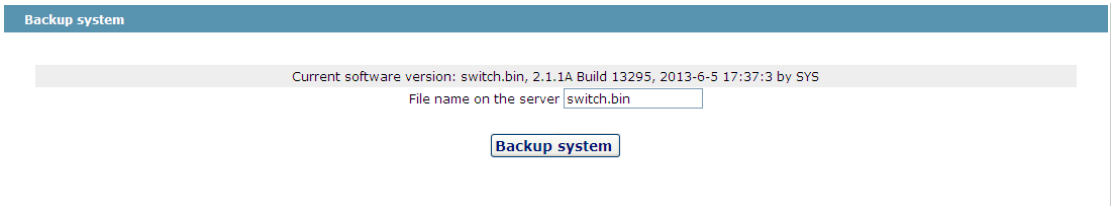


Figure 18-11 Backing up IOS

On this page the currently running software version is displayed. If you want to backup IOS, please click "Backuping IOS"; then on the browser the file download dialog box appears; click "Save" to store the IOS file to the disk of the PC, mobile storage device or other network location.

NOTE:

The default name of IOS document is "Switch.bin". It is suggested to modify it as a name which is detectable and searchable when its backup is created.

18.4.2 Upgrading the IOS Software

NOTE:

1. Please make sure that your upgraded IOS matches the device type, because the matchable IOS will not lead to the normal startup of the device.
2. The upgrade of IOS probabely takes one to two minutes; when the "updating" button is clicked, the IOS files will be uploaded to the device.
3. If errors occur during upgrade, please do not restart the device or cut off the power of the device, or the device cannot be started. Please try the upgrade again.
4. After the upgrade please save the configuration and then restart the device to run the new IOS.

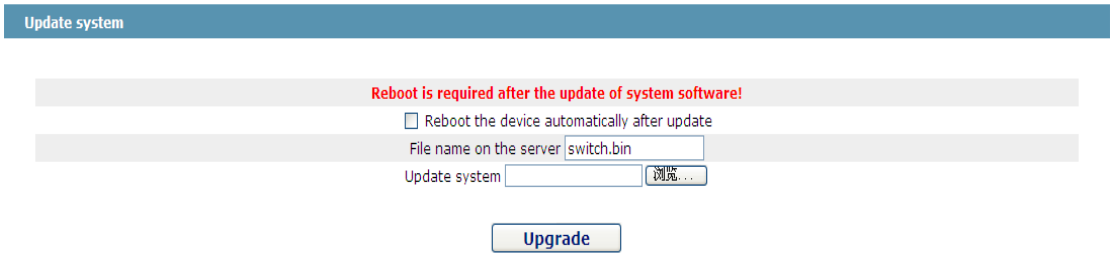


Figure 18-12 Upgrading the IOS software

The upgraded IOS is always used to solve the already known problems or to perfect a specific function. If you device run normally, do not upgrade your IOS software frequently.

If IOS need be upgraded, please first enter the complete path of the new IOS files in the textbox on the right of "Upgrading IOS", or click the "Browsing" button and select the new IOS files on your computer, and then click "Updating".

18.5 Rebooting the Device

If you click System Manage -> Reboot Device, the Rebooting page appears.

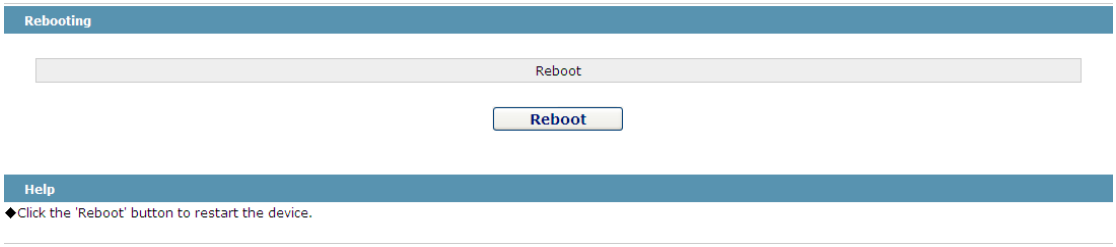


Figure 18-13 Rebooting the device

If the device need be rebooted, please first make sure that the modified configuration of the device has already been saved, and then click the "Reboot" button.

Chapter 19 Interface Configuration

19.1 Introduction

This section helps user to learn various kinds of interface that our switch supports and consult configuration information about different interface types.

For detailed description of all interface commands used in this section, refer to *Interface configuration command*. For files of other commands appeared in this section, refer to other parts of the manual.

The introduction includes communication information that can be applied to all interface types.

19.1.1 Supported Interface Types

For information about interface types, please refer to the following table.

Interface Type	Task	Reference
Ethernet interface	Configures fast Ethernet interface. Configures gigabit Ethernet interface.	Configuring Ethernet Interface
Logical Interface	Aggregation interface VLAN interface	Configuring Logistical Interface

The two supported kinds of interface: Ethernet interface and logical interface. The Ethernet interface type depends on one device depends on the standard communication interface and the interface card or interfaced module installed on the switch. The logical interface is the interface without the corresponding physical device, which is established by user manually.

The supported Ethernet interfaces of our switch include:

- Fast Ethernet interface
- Gigabit Ethernet interface

The supported logical interface of our switch include:

- aggregation interface
- VLAN interface

19.1.2 Interface Configuration Introduction

The following description applies to the configuration process of all interfaces. Take the following steps to perform interface configuration in global configuration mode.

(1) Run the **interface** command to enter the interface configuration mode and start configuring interface. At this time, the switch prompt becomes 'config_' plus the shortened form of the interface to be configured. Use these interfaces in terms of their numbers. Numbers are assigned during installation(exworks) or when an interface card are added to the system. Run the **show interface** command to display these interfaces. Each interface that the device supports provides its own state as follows:

```
Switch_config#show interface g0/2
GigaEthernet0/2 is administratively down, line protocol is down
```

Hardware is Giga-Combo-FX, address is 00e0.0f8d.e0e1 (bia 00e0.0f8d.e0e1)
MTU 1500 bytes, BW 10000 kbit, DLY 10 usec
Encapsulation ARPA
port info 1 0 2 1
Auto-duplex, Auto-speed
flow-control off
Received 0 packets, 0 bytes
0 broadcasts, 0 multicasts
0 discard, 0 error, 0 PAUSE
0 align, 0 FCS, 0 symbol
0 jabber, 0 oversize, 0 undersize
0 carriersense, 0 collision, 0 fragment
0 L3 packets, 0 discards, 0 Header errors
Transmited 0 packets, 0 bytes
0 broadcasts, 0 multicasts
0 discard, 0 error, 0 PAUSE
0 sqettest, 0 deferred
0 single, 0 multiple, 0 excessive, 0 late
0 L3 forwards

NOTE: There is no need to add blank between interface type and interface number. For example, in the above line, g0/2 or g 0/2 is both right.

(1) You can configure the interface configuration commands in interface configuration mode. Various commands define protocols and application programs to be executed on the interface. These commands will stay until user exits the interface configuration mode or switches to another interface.

(2) Once the interface configuration has been completed, use the show command in the following chapter 'Monitoring and Maintaining Interface' to test the interface state.

19.2 Configuring Interface Common Attribute

The following content describes the command that can be executed on an interface of any type and configures common attributes of interface. The common attributes of interface that can be configured include: interface description, bandwidth and delay and so on.

19.2.1 Adding Description

Adding description about the related interface helps to memorize content attached to the interface. This description only serves as the interface note to help identify uses of the interface and has no effect on any feature of the interface. This description will appear in the output of the following commands: **show running-config** and **show interface**. Use the following command in interface configuration mode if user wants to add a description to any interface.

Command	Description
description *string*	Adds description to the currently-configured interface.

For examples relevant to adding interface description, please refer to the following section 'Interface Description Example'.

19.2.2 Configuring Bandwidth

The upper protocol uses bandwidth information to perform operation decision. Use the following command to configure bandwidth for the interface:

Command	Description
bandwidth *kilobps*	Configures bandwidth for the currently configured interface.

The bandwidth is just a routing parameter, which doesn't influence the communication rate of the actual physical interface.

19.2.3 Configuring Time Delay

The upper protocol uses time delay information to perform operation decision. Use the following command to configure time delay for the interface in the interface configuration mode.

Command	Description
delay tensofmicroseconds	Configures time delay for the currently configured interface.

The configuration of time delay is just an information parameter. Use this command cannnot adjust the actual time delay of an interface.

19.3 Monitoring and Maintaining Interface

The following tasks can monitor and maintain interface:

- Checking interface state
- Initializing and deleting interface
- Shutting down and enabling interface

19.3.1 Checking Interface State

Our switch supports displaying several commands related to interface information, including version number of software and hardware, interface state. The following table lists a portion of interface monitor commands. For the description of these commands, please refer to 'Interface configuration command'.
Use the following commands:

Command	Description
show interface [type [slot|port]]	Displays interface state.
show running-config	Displays current configuration.

show version	Displays memory configuration, software version, start-up image and so on.

19.3.2 Initializing and Deleting Interface

You can dynamically establish and delete logical interfaces. This also applies to the sub interface and channalized interface. Use the following command to initialize and delete interface in global configuration mode:

Command	Description
no interface [type [slot|port]]	Initializes physical interface or deletes virtual interface.

19.3.3 Shutting down and Enabling Interface

When an interface is shut down, all features of this interface are disabled, and also this interface is marked as unavailable interface in all monitor command displays. This information can be transmitted to other switches via dynamic routing protocol.
Use the following command to shutdown or enable an interface in the interface configuration mode:

Command	Description
shutdown	Shuts down an interface.
no shutdown	Enables an interface.

You can use the **show interface** command and the **show running-config** command to check whether an interface has been shut down. An interface that has been shut down is displayed as 'administratively down' in the **show interface** command display. For more details, please refer to the following example in 'Interface Shutdown Example'.

19.4 Setting the Ethernet Interface

In this section the procedure of setting the Enthernet interface will be described. The detailed configuration includes the following steps, among which step 1 is obligatory while other steps are optional.

19.4.1 Choosing an Ethernet Interface

Run the following command in global configuration mode to enter the Ethernet interface configuration mode:

Command	Purpose
interface gigaethernet [*slot*|*port*]	Enters the gigabit-Ethernet interface configuration mode.

The **show interface gigaethernet** [*slot*|*port*] command can be used to show the state of the gigabit-Ethernet interface.

19.4.2 Configuring the Rate

The Ethernet rate can be realized not only through auto-negotiation but also through interface configuration.

Command	Purpose
show interface gigaethernet [*slot*|*port*]	Sets the rate of fast Ethernet to 10M, 100M, 1000M or auto-negotiation.
show interface gigaethernet [*slot*|*port*]	Resumes the default settings. The rate is auto-negotiation

NOTE: The speed of the optical interface varies according to the model. For example, the speed of GE-FX is 1000M, but it can also be specified as 100M through configuration. The speed of FE-FX is 100M. If there is auto parameter after the speed command of the optical interface, the interface can enable the automatic negotiation function. Otherwise, The speed of the optical interface is fixed and cannot negotiate. The gigabit port can support 10,100,1000 mode in auto mode.The specific configuration is subject to the prompt from each port.

19.4.3 Configuring the Duplex Mode of an Interface

By default, Ethernet interfaces can automatically negotiate whether to be half duplex or full duplex. The duplex mode for the gigbit interface is always auto.

Command	Purpose
duplex {full|half|auto}	Sets the duplex mode of an Ethernet interface.
No duplex	Resumes the default settings. The duplex mode is auto-negotiation.

19.4.4 Configuring Flow Control on an Interface

When an interface is in full duplex mode, flow control is realized through the 802.3X-defined PAUSE frame. In half duplex mode, it is implemented by back pressure.

Command	Purpose
flow-control *on/off /auto*	Enables or disables flow control on an interface.
no flow-control	Resumes the default settings, that is, there is no flow control on an interface.

19.5 Configuring Logistical Interface

This section describes how to configure a logical interface. The contents are as follows:

- Configuring aggregation interface
- Configuring VLAN interface

19.5.1 Configuring Aggregation Interface

The inadequate bandwidth of a single Ethernet interface gives rise to the birth of the aggregation interface. It can bind several full-duplex interface with the same rate together, greatly improving the bandwidth.
Run the following command to define the aggregation interface:

Command	Description
Interface port-aggregator *number*	Configures the aggregation interface

19.5.2 Configuring VLAN Interface

V VLAN interface is the routing interface in switch. The VLAN command in global configuration mode only adds layer 2 VLAN to system without defining how to deal with the IP packet whose destination address is itself in the VLAN. If there is no VLAN interface, this kind of packets will be dropped.
Run the following command to define VLAN interface:

Command	Description
Interface vlan *number*	Configures VLAN interface.

Chapter 20 Interface Configuration Example

20.1 Configuring Public Attribute of Interface

20.1.1 Interface Description Example

The following example shows how to add description related to an interface. This description appears in the configuration file and interface command display.

interface vlan 1

ip address 192.168.1.23 255.255.255.0

20.1.2 Interface Shutdown Example

The following example shows how to shut down the Ethernet interface 0/1:

interface GigaEthernet0/1

shutdown

The following example shows how to enable the interface:

interface GigaEthernet0/1

no shutdown

Chapter 21 Interface Range Configuration

21.1 Interface Range Configuration Task

21.1.1 Understanding Interface Range

In the process of configuring interface tasks, there are cases when you have to configure the same attribute on ports of the same type. In order to avoid repeated configuration on each port, we provide the **interface range** configuration mode. You can configure ports of the same type and slot number with the same configuration parameters. This reduces the workload.

Note:

when entering the **interface range** mode, all interfaces included in this mode must have been established.

21.1.2 Entering Interface Range Mode

Run the following command to enter the **interface range** mode.

Step	Command	Description
1	**interface range** type slot/<port1-port2 | port3>[, <port1-port2|port3>]	Enters the range mode. All ports included in this mode accord to the following conditions: (1) The slot number is set to **slot**. (2) The port numbers before/after the hyphen must range between port1 and port2, or equal to port3. (3) Port 2 must be less than port 1 (4) There must be no space before/after the hyphen or the comma.

21.1.3 Configuration Example

Enter the interface configuration mode via the following commands, including slot 0 and fast Ethernet 1,2,3,4:

switch_config# interface range gigaEthernet 0/1-4

switch_config_if_range#

Chapter 22 Port Physical Characteristics Configuration

22.1 Configuring the Ethernet Interface

22.1.1 Configuring Rate

The Ethernet rate can be realized through auto-negotiation or configuration on the interface.
Run the following command to configure the Ethernet rate:

Command	Purpose
Speed {**10**|**100**|**auto**} (T port)	Set the rate of fast Ethernet to 10M, 100M, 1000M or auto-negotiation.
No speed	Resume the default settings—auto-negotiation.

NOTE: The speed of the optical interface is fixed. For example, the rate of GBIC and GE-FX is 1000M; the rate of FE-FX is 100M. If the auto parameter is behind the speed command, it means that you can enable the auto-negotiation function on the optical interface. Otherwise, you cannot enable the auto-negotiation function on the optical interface.

22.1.2 Configuring the Duplex Mode of an Interface

By default, the Ethernet interface can be auto, half duplex or full duplex. The gigabit combo SFP/TX ports does not support speed 1000 and compulsory duplex mode simultaneously.

Command	Purpose
duplex {full | half | auto}	Sets the duplex mode of the Ethernet.
No duplex	Resumes the default setting. The duplex mode is auto-negotiation.

22.1.3 Configuring Flow Control on the Interface

When the interface is in full-duplex mode, the flow control is achieved through the PAUSE frame defined by 802.3X. When the interface is in half-duplex mode, the flow control is achieved through back pressure.

Command	Purpose
flow-control {on | off | auto}	Enable or disable the flow control on the interface.
no flow-control	Resume the default settings. The default settings have no flow control.

NOTE: The difference between “flow-control auto” and “flow-control on” is that the flow control frame is compulsory received. The flow control frame is forwarded when the peer negotiation is successful in “auto” mode.

Chapter 23 Port's Additional Features Configuration

23.1 Port Isolation

Under normal condition, data packet could be forwarded among different ports of switches. Under some circumstances, flows among ports need to be forbidden, and port isolation function is the one to provide this kind of control. For isolation which is not based on group, data communication could not work between isolated ports, but data packets among non-isolated ports and isolated and non-isolated ports could be forwarded normally. For isolation based on group, isolated ports in group cannot do data communication, but they can do data communication with any ports outside group. To be noticed, port isolation function works for layer 2 messages, but it does not support isolation based on group.

Isolation based on non-group:

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] switchport protected	Enable/cancel port isolation function
exit	Back to global configuration mode
exit	Back to management configuration mode

Isolation based on group:

Command	Purpose
config	Entering global configuration mode.
[no] port-protected *group-id*	Create and enable the isolation group mode. *group-id* means to configure the the isolation group ID.
[no] description *word*	Description of the group. *Word* stand for the character string of the group.
exit	Back to global configuration mode.
interface g0/1	Entering the interface which to be configured
[no] switchport protected *group-id*	Add/remove isolation group. *group-id stand for* the isolation group ID that is configured.
exit	Back to global configuration mode.
exit	Back to management configuration mode.

23.2 Storm Control

Switch's ports could be attacked by constant abnormal unicast (MAC address locating failure), multicast or broadcast messages. It might cause switch's ports and even the whole switch's failure. Therefore, a mechanism has be provided to restrain this phenomenon. Storm control function could set different rates at the ingress for different kinds of messages which are allowed to enter switch.

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] **storm-control {broadcast | multicast | unicast} threshold** *count*	Configuring port's storm control function. **Unicast** means it works for unknown unicast. **Multicast** means it works for multicast. **Broadcast** means it works for broadcast. **Count** means the threshold which is to be configured.
[no] **storm-control mode { kbps | pps }**	Setting the unit for port storm control threshold. mode unit kbps or pps
[no] **storm-control { broadcast | multicast } action { shutdown | block | resume }**	Configuring the storm control action for a port. **shutdown:** The port will be shut down when the traffic reaches the storm control threshold. **block:** The port will be blocked when the traffic reaches the storm control threshold. **resume:** The port will resume normal operation after being blocked or shut down due to storm control.
[no] **storm-control { broadcast | multicast } auto-resume [** *second* **]**	Configuring the storm control auto-resume time for a port. Unit: second, default value: 60s
[no] **storm-control notify { log | trap }**	Configuring storm control alarm reporting for a port. **log:** Storm control alarms will be logged and printed through syslog output. **trap:** Storm control alarms will be sent as SNMP traps.
exit	Back to global configuration mode
exit	Back to management configuration mode

23.3 Port's Rate Limitation

Port's rate limitation is used for limiting the rate of flow which comes in and goes out of ports. Use the following commands to limit port's flow rate after entering management mode:

Command	Purpose
config	Entering global configuration mode

interface g0/1	Entering the interface which to be configured
[no] switchport rate-limit {*band* | Bandwidth *percent* } { ingress | egress}	Configuring the flow rate limitation for port. Band is the limited flow rate. *Percent* is the limited flow percentage. **Ingress** means it works for ingress; **Egress** means it works for egress.
exit	Back to global configuration mode
exit	Back to management configuration mode

23.4 Port Loop Detection

Port loop detection function is used for detecting whether port has loop. Time interval of loop detection messages sent by port could be configured. Use the following command to set time interval of loop detection messages sent by port after entering management mode.

Command	Purpose
config	Entering global configuration mode
Interface g0/1	Entering the interface which to be configured
[no] keepalive [*second*]	Configuring time interval of loop detection messages sent by port. *Second* is the time interval of sending messages.
exit	Back to global configuration mode
exit	Back to management configuration mode

23.5 Port MAC-address learning

Port MAC address learning is used to enable/disable port MAC address learning. The configuration method is as follows:

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] switchport disable-learning	Configure port MAC address learning. Enable/disable port MAC address learning function.
exit	Back to global configuration mode

exit	Back to management configuration mode

23.6 Port's Security

Port's security does controlling by accessing port according to MAC address. Port's security has three kinds of modes: dynamic security mode, static accepting mode, and static rejecting mode. Under dynamic security mode, maximum MAC address quantity which is allowed to be learnt by ports can be configured. When the maximum mac quantity has been learnt from some port by switch, mac address would not be learnt; at the meantime, switch drops all the DLF messages. Under static security mode, static security MAC address can be configured at port. Under static accepting mode, only messages which source MAC is safe MAC address are allowed to get in, and others would be dropped. Under static rejecting mode, messages which source MAC is safe MAC address would be dropped, and other messages would be allowed to get in.

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] switchport port-security mode {dynamic | static *accept*|*reject* | sticky}	Configuring port's security mode. **Dynamic** means dynamic security mode. **static** *accept* means static accepting mode **static** *reject* means static rejecting mode
[no] switchport port-security dynamic maximum *num*	Configuring maximum learnable MAC address quantity
[no] switchport port-security static mac-address *H.H.H*	Configuring static security address
[no] switchport port-security sticky {maximum *sticky_number* | mac-address *H.H.H* | aging-time *aging_time*}	Configuring port MAC address sticky. **maximum** *sticky_number* means maximum sticky MAC address quantity. **mac-address** *H.H.H* means to configure sticky MAC address manually. **aging-time** *aging_time* means to configure aging time of sticky MAC address manually.
exit	Back to global configuration mode
exit	Back to management configuration mode

23.7 Interface's binding

This switch could be bind with IP address and MAC address on interface at the same time, or be bind with only IP address or MAC address. It works for IP and ARP messages.

Use the following commands to do configuration after entering management mode:

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] switchport port-security bind|block {ip|arp| both-arp-ip A.B.C.D | mac H.H.H }	Configuring interface's binding function. Bind only allows messages which conform to binding requirements to pass, and other messages would not be allowed to pass. Block only reject messages which conform to binding requirements, and others would be allowed to pass. Ip means it would only work for IP messages which conform to binding requirements; Arp means it would only work for arp messages which conform to binding requirements; both-arp-ip means it would work for ip and arp messages conforming to binding requirements.
exit	Back to global configuration mode
exit	Back to management configuration mode

23.8 SVL/IVL

This switch can be configured with Shared (SVL)/independent (IVL) vlan learning mode. By default, the ports are all in IVL mode.

This switch could be bind with IP address and MAC address on interface at the same time, or be bind with only IP address or MAC address. It works for IP and ARP messages.

Use the following commands to do configuration after entering management mode:

Command	Purpose
config	Entering global configuration mode
[no]vlan shared-learning	Configuring SVL/IVL
exit	Back to management configuration mode

23.9 Configuring Link Scan

23.9.1 Overview

Configuring port's scanning time interval is to scan port's up/down status quickly.

23.9.2 Link scan Configuration Task

- Configuring port's scanning time interval.

1. Setting up port's scanning time interval

When setting up port's scanning time interval, use the following command under global configuration mode:

Command	Purpose
[no] Link scan {normal *interval* | fast *interval*}	Mode means to choose optical port's scanning mode. **Normal** means standard link scanning mode. **Fast** means quick link scanning mode. Fast mode mainly applies to service protocol, like rstp. **Interval** means configuring port's scanning time interval.

23.9.3 Configuration Example

Configuring standard scanning interval as 20 millisecond

link scan normal 20

23.10 Configuring Port Enhanced Link Status Check

23.10.1 Overview

Configuring port's enhanced link status check is to scan port's link status quickly.

23.10.2 Configuration Task

- Enable/disable port's enhanced link status check.

1. Enable/disable port's enhanced link status check

When enable/disable port's enhanced link status check, use the following command under interface configuration mode:

Command	Purpose
[no] switchport enhanced-link	Enable/disable port's enhanced link status check.

23.10.3 Configuration Example

Enable enhanced link status check of interface g0/1.

Switch_config#interface g0/1

Switch_config_g0/1#switchport enhanced-link

23.11 Configuring system mtu

23.11.1 Overview

Configuring system mtu

23.11.2 Configuration Task

- Configuring system mtu

1. Setting up mtu

Use the following command under global configuration mode:

Command	Purpose
[no] system mtu *mtu*	Configuring system mtu value

23.11.3 Configuration Example

Configuring system mtu 2000 bytes

Switch_config#system mtu 2000

Chapter 24 Configuring Port Mirroring

24.1 Configuring Port Mirroring Task List

- Configuring port mirroring
- Displaying port mirroring information

24.2 Configuring Port Mirroring Task

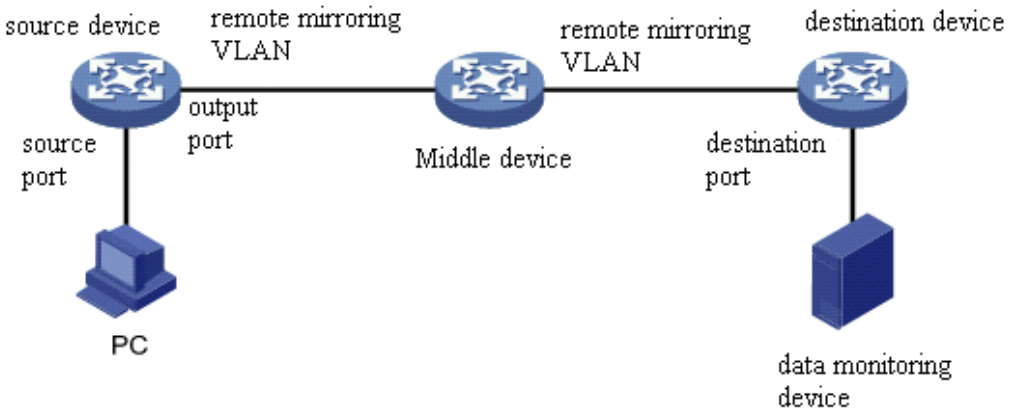
24.2.1 Configuring Port Mirroring

In order to make switch management easy, you can set port mirror and use a port of the switch to observe the flux that runs through a group of ports.

Port mirroring could be divided like local mirroring and remote mirroring. Local mirroring means copying message to this device's port, and remote mirroring function means transferring message to remote device across multiple network devices. Port mirroring is configured by the way of mirroring group, and relative concepts include port, destination port, remote mirroring VLAN, remote mirroring TPID, VLAN DISABLE-LEARNING and etc.

In the remote mirroring, the local device would add a vlan tag in the mirroring message. Messages from different mirroring's remote groups are detected by setting the tag's vid (remote mirroring vlan) and tpid. In order to achieve remote mirroring function, it is required that the middle device could transfer messages within remote mirroring's vlan to remote device.

Remote mirroring's schemetic plot is like following:



Configuring remote mirroring function on source device, and mirroring source port's message to the output port while adding configuring RSPAN TAG on the message. Vlan id in this tag is the remote mirroring VLAN. Middle device transfer mirroring message to the destination port by broadcasting. The destination device transfer message from destination port to data monitoring device by configuration. If the destination device supports port mirroring function, the message could be transferred from destination port to data monitoring device by configuring local mirroring. If the destination device supports the configuration of mac address learning based on vlan, the message could be transferred to data monitoring device by shutting down remote mirroring vlan address learning. If the destination device's qos policy mapping supports the matching of vlan, the message could be transferred to monitoring device by qos policy mapping.

Enter the EXEC mode and perform the following steps to configure port mirroring:

Command	Description
config	Enters the global configuration mode.
mirror session *session_number* {**destination** {**interface** *interface-id*} { **rspan** *vid tpid*} | **source** {**interface** *interface-id* [, | -] rx | tx | both] }	Configures port mirroring. **session-number** is the number of the port mirroring. **destination** is the destination port of the mirroring. Vid of the remote mirroring tag. tpid of the remote mirroring tag. **source** is the source port of mirroring. **rx** means the input data of mirroring. Tx means the output data of mirroring. Both means the input and output data of mirroring.
exit	Enters the management mode again.
write	Saves the configuration.

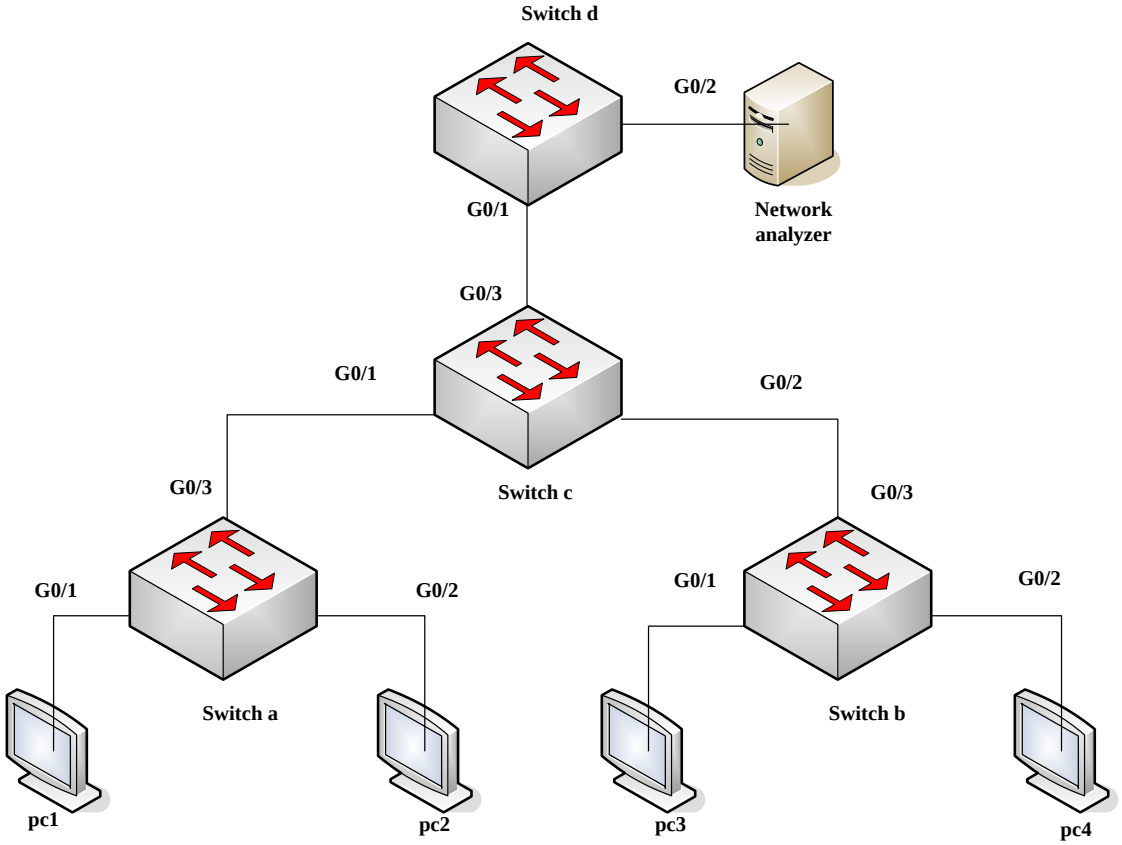
24.2.2 Displaying Port Mirroring Information

Run show to display the configuration information of port mirroring.

Command	Description
show mirror [session *session_number]*	Displays the configuration information about port mirroring. **session-number** is the number of the port mirroring.

24.3 Remote Mirroring Configuration Example

The network environment is as shown in following figure:



Users need to monitor the flow of the g0/1 port in switch a and the g0/1 port in switch b at the network analyzer, which can be realize through remote mirroring. The configuration is as follows:

switch a:

mirror session 1 destination interface g0/3 rspan 100 0x8100

mirror session 1 source interface g0/1 both

switch b:

mirror session 1 destination interface g0/3 rspan 1000 0x8100

mirror session 1 source interface g0/1 both

switch c:

```
interface GigaEthernet0/1
 switchport mode trunk
!
interface GigaEthernet0/2
 switchport mode trunk
!
interface GigaEthernet0/3
 switchport mode trunk
!
!
vlan 1,100,1000
```

!

switch d:

mirror session 1 destination interface g0/2

mirror session 1 source interface g0/1 both

Chapter 25 Configuring MAC Address Attribute

25.1 MAC Address Configuration Task List

- Configuring Static Mac Address
- Configuring Mac Address Aging Time
- Configuring blackhole Mac Address
- Displaying Mac Address Table
- Clearing Dynamic Mac Address

25.2 MAC address Configuration Task

25.2.1 Configuring Static Mac Address

Static MAC address entries are MAC address entries that do not age by the switch and can only be deleted manually. According to the actual requirements during the operation process, you can add and delete a static MAC address. Use the following command in privileged level to add and delete a static MAC address.

Command	Purpose
configure	Enters the global configuration mode.
[no] mac address-table static *mac-addr* vlan *vlan-id* interface *interface-id*	Adds/deletes a static MAC address entry. **Mac-addr** indicates the MAC address. **Vlan-id** indicates the VLAN number. Valid value is from 1~4094. **Interface-id** indicates the interface name.
exit	Returns to EXEC mode.
write	Saves configuration.

25.2.2 Configuring MAC Address Aging Time

When a dynamic MAC address is not used during the specified aging time, the switch will delete this MAC address from the MAC address table. The aging time of the switch MAC address can be configured in terms of needs. The default aging time is 300 seconds.

Configure the aging time of MAC address in the privileged mode as follows:

Command	Purpose
configure	Enters the global configuration mode
mac address-table aging-time [0 | 10-1000000]	Configures the aging time of MAC address. **0** indicates no-age of the MAC address. Valid value is from 10 to 1000000 in seconds.
exit	Returns to the management mode.

write	Saves configuration.

25.2.3 Displaying blackhole Mac Address

Blackhole MAC address table entries refer to those entries that are not allowed to communicate and can only be manually deleted. Blackhole MAC addresses can be added and removed according to the actual needs of the use of the switch. Configure the following commands to add and remove a blackhole MAC address:

Command	Purpose
config	Enters the global configuration mode
[no] mac address-table blackhole*mac-addr* vlan *vlan-id*	Adds/deletes a blackhole MAC address entry. **mac-addr** indicates the MAC address. **Vlan-id** indicates the VLAN number. Valid value is from 1~4094.
exit	Returns to the management mode.
write	Saves configuration.

25.2.4 Displaying MAC Address Table

Since debugging and management are required in operation process, we want to know content of the switch MAC address table. Use the show command to display content of the switch MAC address table.

Command	Purpose
show mac address-table [dynamic [interface *interface-id* | vlan *vlan-id*] | static | brief | multicast | interface *interface-id* | vlan *vlan-id* | H.H.H | blackhole]	**Dynamic** indicates the MAC address that acquires dynamically. **Interface-id** indicates the interface name. **Vlan-id** indicates the VLAN number. Valid value is from 1 to 4094. **Static** indicates the static MAC address table. **Brief** indicates the brief information of the MAC address. **Multicast** indicates multicast MAC address table. **Interface** indicates interface MAC address table. **Vlan** indicates MAC address table in VLAN. **H.H.H** indicates specific address. **Blackhole** indicates BLACKHOLE MAC address table.

25.2.5 Clearing Dynamic MAC Address

The acquired MAC addresses need to be cleared in some circumstances.

Use the following command to delete a dynamic MAC address in privileged mode:

Command	Purpose
clear mac address-table dynamic [address *mac-addr* | interface *interface-id* | vlan *vlan-id*]	Deletes a dynamic MAC address entry. **Dynamic** indicates the MAC address that dynamically acquires. **Mac-addr** is the MAC address. **Interface-id** indicates the interface name. **Vlan-id** indicates the VLAN number. Valid value is from 1 to 4094.

Chapter 26 MAC Access-List Configuration

Access-list configuration includes:

- Creating MAC access-list
- Configuring items of MAC access-list
- Applying MAC access-list

26.1 Creating MAC Access-List

A MAC access-list must be created first before applying it on the port. When a MAC access-list has been created, it enters MAC access-list configuration mode, under which items of MAC access-list can be configured.

Enter privilege mode and use the following steps to add or delete a MAC access-list.

Command	Purpose
config	Enters the global configuration mode.
[no] mac access-list *name*	To add or cancel a MAC access list, run the previous command. **name** stands for the name of theMACaccess list.

26.2 Configuring Items of MAC Access-List

In MAC access-list configuration mode, specify to permit or deny any source MAC address or a specific host source MAC address and any destination MAC address. The same items can be configured in a MAC access list only once.

Enter MAC access list configuration mode and use the following steps to set MAC access list entry.

Command	Purpose
[**no**] {**permit	deny**} {**any**	**host** src-mac-addr	src-mac-addr src-mac-mask } {**any**	**host** dst-mac-addr	dst-mac-addr dst-mac-mask}[**arp** [{any	src-ip-addr} {any	dst-ip-addr }]	ethertype |cos value]	To add/delete a MAC access list entry, run the previous command. You can repeat this command to add/delete multiple MAC access list entry. **any** means match with any MAC address; **src-mac-addr** stands for source MAC address; **src-mac-mask** stands for source mac mask; **dst-mac-addr** stands for the destination MAC address; ***dst-mac-mask*** stands for destination mac mask; **arp** stands for matched arp packet **src-ip-addr** stands for source ip address **dst-ip-addr** stands for the destination IP address **ethertype** stands for type of the matched Ethernet packet **cos value** stands for packet header marking.

exit	Log out from the MAC list configuration mode and enter the global configuration mode again.
exit	Goes back to the EXEC mode.
write	Saves the settings.

MAC list configuration example

Switch_config#mac access-list 1

Switch-config-macl#permit host 1.1.1 any

Switch-config-macl#permit host 2.2.2 any

The above configuration is to compare the source MAC address, so the mask is the same. The configuration is successful.

26.3 Applying MAC Access-List

The created MAC list can be applied on any physical port. Only one MAC list can be applied to a port. The same MAC list can be applied to multiple ports. Enter the privilege mode and perform the following operation to configure the MAC list. Enter the privilege mode and perform the following operation to configure the MAC list.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] mac access-group *name*	Apply the created MAC list to the port or delete the applied MAC list from the port. NameMAC: Name of the MAC access list
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Chapter 27 Configuring 802.1x

27.1 802.1x Configuration Task List

- Configuring 802.1x port authentication
- Configuring 802.1x multiple port authentication
- Configuring 802.1x re-authentication
- Configuring 802.1x re-authentication times
- Configuring 802.1x transmission frequency
- Configuring 802.1x user binding
- Configuring authentication method for 802.1x port
- Selecting authentication type for 802.1x port
- Configuring port mab authentication
- Configuring 802.1x accounting
- Configuring 802.1x guest-vlan
- Forbidding Supplicant with multiple network cards
- Resuming default 802.1x configuration
- Monitoring 802.1x authentication configuration and state

27.2 802.1x Configuration Task

27.2.1 Configuring 802.1x Port Authentication

802.1x defines three control methods for the port: mandatory authentication approval, mandatory authentication disapproval and 802.1x authentication startup.

Mandatory authentication approval means the port has already passed authentication. The port does not need any authentication any more, and all users can perform dara access control through the port. The authentication method is defaulted by the port. Mandatory authentication disapproval means the port authentication does not get passed no matter what kind of method is applied. No user can perform the data access control through the port.

802.1x authentication startup means the port is to run 802.1x authentication protocol. 802.1x authentication will be applied to users who access the port. Only users who pass the authentication can perform data access control through the port. After the 802.1x authentication is started up, the AAA authentication method must be configured.

Run the following command to enable the 802.1x function before configuring 802.1x:

Command	Purpose
dot1x enable	Enable the 802.1x function.

Run the following command to start up the 802.1x authentication:

Command	Purpose
dot1x port-control auto	Configure the 802.1x protocol control method on the port.

aaa authentication dot1x {default |list name} method1 [method2...]	Configure the AAA authentication of 802.1x.

Run one of the following commands in port configuration mode to select 802.1x control method:

Command	Purpose
dot1x port-control auto	Enables the 802.1x authentication method on the port.
dot1x port-control force-authorized	Approve the mandatory port authentication.
dot1x port-control force-unauthorized	Disapprove the mandatory port authentication.
dot1x port-control misc-mab	Enables 802.1x hybrid authentication.

27.2.2 Configuring 802.1x Multiple Port Authentication

802.1x authentication is for the authentication of single host user. In this case, the switch allows only one user to perform authentication and access control. Other users cannot be authenticated and access unless the previous user exits authentication and access. In the case the port connects multiple hosts through switch devices, such as 1108 switch, that do not support 802.1x, you can start up the multiple port access function to make sure that all host users can access.

The multi-auth has two modes: one is multiple-host mode and the other is multiple-auth mode. In **multiple-hosts** mode, the port will be set to **up** if one of the users passes the authentication. Thus, other users can access the device by the port without authentication. In **multiple-auth** mode, the swich will authenticate each user separately. The port will be set to **up** if one user has been successfully authenticated. The port is set to down if all users are failed to authenticate. Thus, the failure of one user will not affect other users' access to the device.

Note: **Multi-auth** mode cannot be configured simultaneously with **guest vlan** or **mab authentication**. If an interface is in multi-auth mode, all users on the interface will be authenticated again.

Run the following command in interface configuration mode to activate 802.1x multiple host authentication:

Command	Purpose
dot1x authentication multiple-hosts	Set the 802.1x multiple port authentication. The port is set to **up** only if one user passes the authentication.
dot1x authentication multiple-auth	Set the 802.1x multiple port authentication. Each user is non-related in authentication.

27.2.3 Configuring 802.1x Re-authentication

After the authentication is passed, the authentication to the client will still be conducted every interval to ensure the legality of the client's authentication.

In this case, you need to enable the re-authentication function. After the re-authentication is started, the authentication

request will be periodically sent to the host.

Run the following commands to configure the re-authentication function.

Command	To
dot1x re-authentication	Enables the re-authentication function.
dot1x timeout re-authperiod *time*	Configures the period of the re-authentication function.

27.2.4 Configuring 802.1x Re-authentication times

After the authentication fails, the switch will re-send request/ID packet to enable the authentication. When the re-authentication times exceeds the certain number and there is still no respond, the authentication will be suspended.

Run the following command in interface configuration command to set the maximum times for of re- authentication:

Command	Purpose
dot1x reauth-max *time*	Set the maximum times of re- authentication.

27.2.5 Configuring 802.1x Transmission Frequency

In the process of 802.1x authentication, data texts will be sent to the host. The data transmission can be adjusted by controlling 802.1x transmission frequency so that the host response is successful.

Run the following command to configure the transmission frequency:

Command	Purpose
dot1x timeout tx-period *time*	Set the message transmission frequency of 802.1x.

27.2.6 Configuring 802.1x User Binding

When 802.1x authentication is performed, you can bind a user to a certain port to ensure the security of port access. Run the following command in interface configuration mode to start up 802.1x user binding.

Command	Purpose
dot1x user-permit *xxxz*	Configure a user that is bound to a port.

27.2.7 Configuring Authentication Method for 802.1x Port

The 802.1x authentication can be performed in different methods at different ports. In the default configuration, the 802.1x authentication adopts the **default** method.

Run the following command in interface configuration mode to configure the method of the 802.1x authentication:

Command	Purpose
dot1x authentication method *yyy*	Configure the method of the 802.1x authentication.

27.2.8 Selecting Authentication Type for 802.1x Port

You can select the type for the 802.1x authentication. The 802.1x authentication type determines whether AAA uses Chap authentication or Eap authentication. Eap authentication supports the md5-challenge mode and the eap-tls mode. Challenge required by MD5 is generated locally when the Chap authentication is adopted, while challenge is generated at the authentication server when the eap authentication is adopted. Each port adopts only one authentication type. The authentication type of global configuration is adopted by default. Once a port is set to an authentication type, the port will use the authentication type unless you run the **No** command to resume the default value.

Eap-tls takes the electronic certificate as the authentication warrant and complies with the handshake rules in Translation Layer Security (tls). Therefore, high security is guaranteed.

Run the following command in global configuration mode to configure the authentication type:

Command	Purpose
dot1x authen-type {chap|eap}	Select chap or eap.

Also run the following command in interface configuration mode:

Command	Purpose
dot1x authentication type {chap|eap}	Select chap or eap or the configured authentication type in global mode.

27.2.9 Configuring MAB Authentication on the Port

When a peer device cannot run the 802.1x client software, the switch will adopt the MAB authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication.

Note: You can run the dot1x mabformat command on a switch to specify the accounting ID and the password's format so that you make it sure that they are same with those on the radius server.

When MAB is enabled and the peer device, however, neither sends the eapol_start packet nor responds to the request_identity packet and exceeds the timeout threshold, the switch regards the peer device not to support the 802.1x authentication client and then turns to the MAB authentication.

NOTE: The MAB authentication mode cannot coexist with the multi-auth mode.

When the MAB authentication is enabled, you can set the format of the MAC address to the Radius server through this command.

Command	Purpose
dot1x mab	Enables the MAB authentication on a port.

To set the format of the MAC address, you can run the following command in global configuration mode:

Command	Purpose
dot1x mabformat{1|2|3|4|5|6}	Chooses one MAC address' format from six formats from format 1 to format 6. The default format is 1.

27.2.10 Configuring 802.1x Accounting

The 802.1x authentication and 802.1x accounting can be performed at the same time. It working mechanism is: after the dot1x authentication is approved, judge whether the accounting function is enabled on the authentication interface; if the accounting function is enabled, send the accounting request through the AAA interface; when the AAA module returns successful request response message, the AAA interface can forward texts.

The accounting can adopt various accounting methods configured in the AAA module. For details, refer to AAA configuration.

After the beginning of accounting, dot1x periodically sends **update** message to the server through the AAA interface for obtaining correct accounting information. According to different AAA configuration, the AAA module decides whether to send the **update** message.

At the same time, You are required to enable the dot1x re-authentication function so that the switch can know when supplicant is abnormal.

Run the following commands in interface configuration mode to enable the dot1x accounting and to configure the accounting method:

Command	Purpose
dot1x accounting enable	Enable the dot1x accounting.
dot1x accounting method {*method name*}	Configure the accounting method. Its default value is **default**.

27.2.11 Configuring 802.1x guest-vlan

Guest-vlan gives releavant ports some access rights (such as downloading client software) when the client does not respond. Guest-vlan can be any configured vlan in the system. If the configured guest-vlan does not meet the conditions, ports cannot run in the guest-vlan.

Note: There is no access right if the authentication fails.

Run the following command in the global mode to enable the guest-vlan:

Command	Purpose
Dot1x guest-vlan	Enable the guest-vlan at all ports.

When there is no **guest-vlan id** originally configured at each port, guest-vlan cannot function even if guest-vlan is enabled in global mode. Only when **guest-vlan id** is configured in port configuration mode, guest-vlan can function.

Run the following command in port configuration mode to configure **guest-vlan id**:

Command	Purpose
Dot1x guest-vlan {id(1-4094)}	Enable the vlan id of guest-vlan at all ports.

27.2.12 Forbidding Supplicant With Multiple Network Cards

Forbid the Supplicant with multiple network adapters to prevent agents. Run the following command in port configuration mode:

Command	Purpose
dot1x forbid multi-network-adapter	Forbid the Supplicant with multiple network adapters.

27.2.13 Resuming Default 802.1x Configuration

Run the following command to resume all global configuration to default configuration:

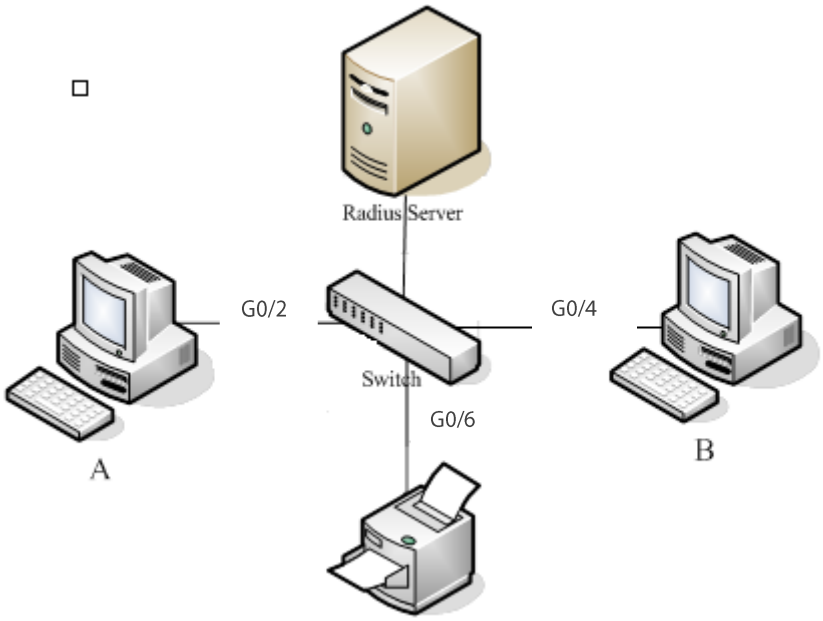
Command	Purpose
dot1x default	Resume all global configuration to default configuration.

27.2.14 Monitoring 802.1x Authentication Configuration and State

To monitor the configuration and state of 802.1x Authentication and decide which 802.1x parameter needs to be adjusted, run the following command in management mode:

Command	Purpose
show dot1x { interface|statistics|misc-mab-db }	Monitor the configuration and state of 802.1x authentication.

27.3 802.1x Configuration Example



Host A connects port G0/2 of the switch. Host B connects port G0/4. Host C connects with port G0/6. The IP address of the radius-server host is 192.168.20.2. The key of radius is TST. Port G0/2 adopts remote radius authentication, user binding and re-authentication. Port G0/4 adopts local authentication of eap type, and enables multi-host and guest-vlan. Port G0/6 adopts mab authentication and the mac address format is AA:BB:CC:DD:EE:FF.

Global configuration

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-G0/2 group radius
aaa authentication dot1x TST-G0/4 local
aaa authentication dot1x TST-G0/6 group radius
aaa accounting network dot1x_acc start-stop group radius
dot1x enable
dot1x re-authentication
dot1x timeout re-authperiod 10
dot1x mabformat 2
dot1x guest-vlan
interface VLAN1
ip address 192.168.20.24 255.255.255.0
!
vlan 1-2
```

radius-server host 192.168.20.2 auth-port 1812 acct-port 1813

radius-server key TST

Configuring port G0/2

interface GigaEthernet0/2

dot1x port-control auto

dot1x authentication method TST-G0/2

dot1x user-permit radius-TST

dot1x accounting enable

dot1x accounting method dot1x_acc

Configuring port G0/4

Interface GigaEthernet0/4

dot1x authentication multiple-hosts

dot1x port-control auto

dot1x authentication method TST-G0/4

dot1x guest-vlan 2

Configuring port G0/6

interface GigaEthernet0/6

dot1x mab

dot1x authentication method TST-G0/6

Chapter 28 Configuring GVRP

28.1 Overview

GVRP (GARP VLAN Registration Protocol GARP VLAN) is a GARP (GARP VLAN Registration Protocol GARP VLAN) application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange the VLAN configuration information with the other GVRP switches, prune the unnecessary broadcast and unknown unicast traffic, and dynamically create and manage the VLANs on the switches that are connected through the 802.1Q trunk ports.

28.2 Configuring Task List

28.2.1 GVRP Configuration Task List

- Enabling/Disabling GVRP Globally
- Enabling/Disabling GVRP on the Interface
- Monitoring and Maintenance of GVRP

28.3 GVRP Configuration Task

28.3.1 Enabling/Disabling GVRP Globally

Perform the following configuration in global configuration mode.

Command	Description
[no] gvrp	Enables/disables GVRP globally.

It is disabled by default.

28.3.2 Dynamic VLAN to Validate only on a Registered Port

Run the following commands in global configuration mode:

Command	Description
[no] gvrp dynamic-vlan-pruning	Enable/disable VLAN to validate only on a registered port.

After this function is enabled, dynamic VLAN takes effect only on the ports on which this dynamic VLAN is registered. After this command is enabled and if a port has not registered a dynamic VLAN, this port will not belong to the dynamic VLAN even though this port is a trunk port and it allows the dynamic VLAN to pass through.
The function is disabled by default.

28.3.3 Enabling/Disabling GVRP on the Interface

Perform the following configuration in interface configuration mode:

Command	Description
[no] gvrp	Enables/disables interface GVRP.

In order for the port to become an active GVRP participant, you must enable GVRP globally first and the port must be an 802.1Q trunk port,
It is enabled by default.

28.3.4 Monitoring and Maintenance of GVRP

Perform the following operations in EXEC mode:

Command	Description
show gvrp statistics [interface port_list]	Displays GVRP statistics.
show gvrp status	Displays GVRP global state information.
[no] debug gvrp [packet | event]	Enables/disables GVRP data packet and event debug switches. All debug switches will be enabled/disabled if not specified the concrete switch.

Display GVRP statistics:

switch#show gvrp statistics interface Tthernet0/1

GVRP statistics on port Ethernet0/1

GVRP Status: Enabled

GVRP Failed Registrations: 0

GVRP Last Pdu Origin: 0000.0000.0000

GVRP Registration Type: Normal

Display GVRP global state information:

Switch#show gvrp status

GVRP is enabled

28.4 Configuration Example

The network connection is as follows. In order to make the VLAN configuration information of Switch A and Switch B identical, you can enable GVRP on Switch A and Switch B. The configuration is as follows:



1) Configure the interface 1 that Switch A connects to Switch B to trunk:

Switch_config_g0/1# switchport mode trunk

2) Enable global GVRP of switch A:

Switch_config#gvrp

3) Enable GVRP of interface 1 of Switch A:

Switch_config_g0/1#gvrp

4) Configure VLAN 10, Vlan 20 and Vlan30 on Switch A

Switch_config#vlan 10,20,30

5) Configure the interface 2 that Switch A connects to Switch B to trunk:

Switch_config_g0/2# switchport mode trunk

6) Enable global GVRP of switch B:

Switch_config#gvrp

7) Enable GVRP of interface 2 of Switch B

Switch_config_g0/2#gvrp

8) Configure VLAN 40, Vlan 50 and Vlan60 on Switch B

Switch_config#vlan 40,50,60

After completing the configuration, the VLAN configuration information will be displayed respectively on Switch A and Switch B, that is, VLAN10, VLAN20,VLAN30, VLAN40, VLAN50 and VLAN60 on both switches.

Chapter 29 VLAN Configuration

29.1 VLAN Introduction

VLAN(Virtual Local Area Network) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. In 1999 IEEE established IEEE 802.1Q Protocol Standard Draft used to standardize VLAN realization project. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.

There are the following types of Virtual LANs:

- Port-Based VLAN: each physical switch port is configured with an access list specifying membership in a set of VLANs.
- 802.1Q trunk mode is supported on the interface.
- Access mode interface is supported.
- Port-Based Vlan is to ascribe port to one subset of vlan that the switch supports. If this vlan subset has only one vlan, then this port is access port. If this vlan subset has multiple vlan, then this port is trunk port. There is one default vlan among the multiple vlan, and the vlan id is the port vlan id (PVID).
- Vlan-allowed range is supported on the interface.

Vlan-allowed parameter is used to control vlan range that the port belongs. Vlan-untagged parameter is used to configure port to send packets without vlan tag to the corresponding vlan.

VLAN can be classified based on MAC address, IP subnetwork, the protocol and the port.

29.2 Dot1Q Tunnel Overview

29.2.1 Preface

Dot1Q Tunnel is a lively name of the tunnel protocol based on 802.1Q encapsulation, which is defined in IEEE 802.1ad. Its core idea is to encapsulate the VLAN tag of the private network to that of the public network, and the packets with two layers of tags traverse the backbone network of ISP and finally a relatively simple L2 VPN tunnel is provided to users. The Dot1Q Tunnel protocol is a simple and manageable protocol, which is realized through static configuration without signaling support and widely applied to enterprise networks, which mainly consist of OLTs, or small-scale MAN.

The Dot1Q Tunnel attribute of XXCOM switches just meets this requirement. As a cheap and compact L2 VPN solution, it is increasingly popular among more and more small-scale users when VPN network is required. At the inside of carrier's network, P device need not support the Dot1Q Tunnel function. That is, traditional L3 switches can meet the requirements fully and protect the investment of the carrier greatly.

- Enables Dot1Q Tunnel globally.
- Supports the inter-translation between customer VLAN and SPVLAN on the downlink port, including translation in Flat mode and in QinQ mode.
- Supports the configuration of the uplink port.

29.2.2 Dot1Q Tunnel Realization Mode

There are two modes to realize Dot1Q Tunnel: port-based Dot1Q Tunnel and Dot1Q Tunnel based on inner CVLAN tag classification.

1) Port-based Dot1Q Tunnel:

When a port of this device receives packets, no matter whether packets have the VLAN tag, the switch will add the VLAN tag of the default VLAN on this port to these packets. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port.
The packet with a single VLAN tag has the following structure, as shown in table 1:

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Table 29-1 The packet with a single VLAN tag

The packet with double VLAN tags has the following structure, as shown in table 2:

DA (6B)	SA (6B)	**ETYPE(8100) (2B)**	**SPVLAN Tag (2B)**	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Table 29-2 Packet with double VLAN tags

2) Dot1Q Tunnel based on the inner CVLAN Tag:

The service is distributed according to the CVLAN ID zone of the inner CVLAN tag of Dot1Q Tunnel. The CVLAN zone can be translated into SPVLAN ID and there are two translation modes: Flat VLAN translation and QinQ VLAN translation. In QinQ VLAN translation mode, when a same user uses different services by using different CVLAN IDs, the services can be distributed according to CVLAN ID. For example, the CVLAN ID of bandwidth service ranges between 101 and 200. The CVLAN ID of VOIP service ranges between 201 and 300. The CVLAN ID of IPTV service ranges between 301 and 400. According to the CVLAN ID range, when the PE device receives the user data, add SPVLAN Tag whose SPVLAN ID is 1000 to the bandwidth service and whose SPVLAN ID is 3000 to the IPTV service. The difference between Flat VLAN translation mode and QinQ VLAN translation mode is SPVLAN Tag in the Flat VLAN translation mode is not add to the outside layer of CVLAN Tag, but replace CVLAN Tag directly.

29.3 VLAN Configuration Task List

- Adding/Deleting VLAN
- Configuring switch port
- Creating/Deleting VLAN interface
- Monitoring configuration and state of VLAN
- Enabling/disabling global Dot1Q Tunnel

29.4 VLAN Configuration Task

29.4.1 Adding/Deleting VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. A VLAN may have multiple ports and all unicast, multicast and broadcast message can only be forwarded from the same VLAN to the terminal. Each VLAN is a logistical network. If the data wants to reach another VLAN, it must be forwarded by router or bridge.

Run the following command to configure VLAN

Command	Purpose
vlan vlan-id	Enter the VLAN configuration mode.
name str	Name in the vlan configuration mode.
Exit	Exit vlan configuration mode, and establish vlan.
vlan vlan-range	Establish multiple VLANs at the same time.
no vlan vlan-id | vlan-range	Delete one or multiple VLANs.

Vlan can perform dynamic addtion and deletion via vlan management protocol GVRP.

29.4.2 Configuring Switch Port

The switch's port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

- The access mode indicates that this port is only subordinate to one vlan and only sends and receives untagged ethernet frame.
- The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.
- The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.
- The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. The SPVLAN should be set when packets are forwarded out of the port. If the packets are in the untagged range, all these packets are forwarded out without any change. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

Each port has one default vlan and pvid,and all the data without vlan tag received on the port belong to the data packets

of the vlan.

Trunk mode can ascribe port to multiple vlan and also can configure which kind of packet to forward and the number of vlan that belongs, that is, the packet sent on the port is tagged or untagged, and the vlan list that the port belongs.

Run the following command to configure the switch port:

Run…	To…
switchport pvid *vlan-id*	Configure pvid of switch port.
switchport mode {access | trunk | dot1q-translating-tunnel | dot1q-tunnel-uplink }	Configure port mode of the switch.
switchport trunk vlan-allowed …	Configure vlan-allowed range of switch port.
switchport trunk vlan-untagged …	Configure vlan-untagged range of switch port.

29.4.3 Creating/Deleting VLAN Interface

Vlan interface can be established to realize network management or layer 3 routing feature. The vlan interface can be used to specify ip address and mask. Run the following command to configure vlan interface:

Run…	To…
[no] interface vlan *vlan-id*	Create/Delete a VLAN interface.

29.4.4 Enable Dual VLAN Tagging functionality

To enable management of remote devices and add an outer VLAN to the management VLAN, you can configure Dual VLAN Tagging functionality. After configuring this feature, when receiving Dual VLAN Tagged packets, the outer VLAN Tag is removed, and the packet is processed based on the inner VLAN Tag. When sending Layer 3 packets through the inner VLAN interface, the configured outer VLAN Tag is added to the packet.

Run…	To…
[no] ethernet double-vlan-tag [inner-vlan innerVlanId **outer-vlan** outerVlanId**]**	Enables/Disables Dual VLAN Tagging functionality or configures Dual VLAN Tag entries.

29.4.5 Monitoring Configuration and State of VLAN

Run the following commands in EXEC mode to monitor configuration and state of VLAN:

Run…	To…
show vlan [id *x* | interface *intf* | dot1q-tunnel [interface *intf*]|mac-vlan | subnet |protocol-vlan |dot1q-translating-tunnel]	Display configuration and state of VLAN or Dot1Q Tunnel.

show interface vlan *x*	Display the states of vlan ports or supervlan port.

29.4.6 Enabling/disabling global Dot1Q Tunnel

After Dot1Q Tunnel is enabled globally, their ports can be defaulted as the downlink ports of Dot1Q Tunnel, and the SPVLAN tag will be added to incoming packets.

The command to enable dot1q-tunnel is shown in the following table:

Run…	To…
dot1q-tunnel	Configures the global dot1q-tunnel on a switch.

29.4.7 Configuring MAC-based VLAN

MAC-Based VLAN is a VLAN classification method based on the source MAC address of a packet. When a port receives an untagged packet, the device uses the source MAC address as the matching key and looks up the MAC VLAN table to determine the VLAN to which the packet belongs.

Configuration of MAC-Based VLAN includes adding/removing MAC VLAN entries and enabling/disabling MAC VLAN functionality on ports.

To add/remove MAC VLAN entries in global configuration mode, use the following commands:

Run…	To…
mac-vlan mac-address ***mac-addr*** **vlan** ***vlan-id [priority]***	Adds a MAC-based VLAN entry
no mac-vlan mac-address ***mac-addr***	Removes a MAC-based VLAN entry

MAC-Based VLAN functionality only takes effect on ports where it is enabled. In port configuration mode, use the following commands to enable/disable MAC VLAN functionality on a port:

Run…	To…
[no] switchport mac-vlan	Enables/disables MAC-based VLAN functionality on a port

Note: In access port mode, if an incoming packet matches a VLAN in the MAC VLAN table that is different from the port's PVID (Port VLAN ID), the packet will be discarded. Therefore, unless necessary, do not configure a port with MAC VLAN functionality enabled as an access port mode.

29.5 Dot1Q Tunnel Configuration Examples

29.5.1 Dot1Q Tunnel configuration examples

The following typical solutions show how to apply Dot1Q tunnel.

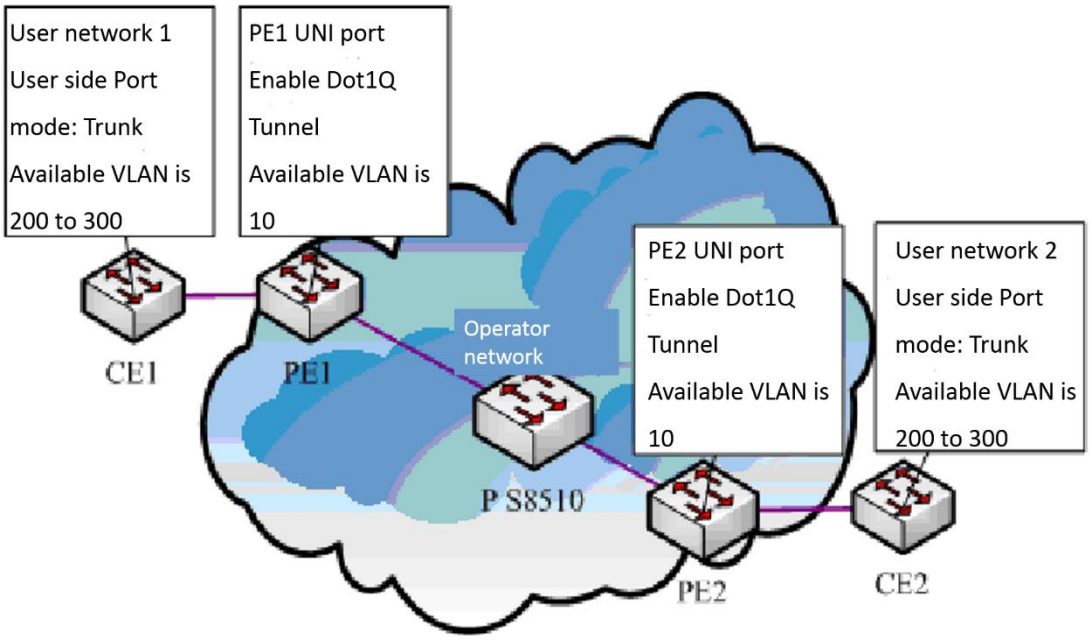


Figure 3 Configuration of Dot1Q Tunnel

As shown in the figure above, port F0/1 of CE1 connects port F0/1 (or port G0/1) of PE1; PE1 connects S8510 on port F0/2 (or port G0/2); PE2 connects S8510 on port F0/2 (or port G0/2); and port F0/1 (or port G0/1) of PE2 connects port F0/1 of CE1.

The ports of PE are set to be the access port of VLAN 10 and on them Dot1Q Tunnel is enabled. However, the ports of CE still need Trunk VLAN 200-300, enabling the link between CE and PE to be an asymmetrical link. In this case, the public network only needs to distribute users a VLAN ID, 10. No matter how many VLAN IDs of private network are planned in the user's network, the newly distributed VLAN ID of the public network will be mandatorily inserted into the tagged packets when these packets enter the backbone network of ISP. These packets then pass through the backbone network through the VLAN ID of the public network, reach the other side of the backbone network, that is, the PE devices, get rid of the VLAN tag of the public network, resume the user's packets and at last are transmitted to the CE devices of the users. Therefore, the packets that are forwarded in the backbone network have two layers of 802.1Q tag headers, one being the tag of the public network and the other being the tag of the private network. The detailed flow of packet forwarding is shown as follows:

1) Because the egress port of CE1 is a Trunk port, all the packets that are transmitted by users to PE1 have carried the VLAN tag of the private network (ranging from 200 to 300). One of these packets is shown in figure 4.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 4 Structure of a packet from CE1

2) After the packets enter PE1, PE1, for the ingress port is the access port of Dot1Q tunnel, ignores the VLAN tag of the private network but inserts the default VLAN 10's tag into these packets, as shown in figure 5.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	SPVLAN Tag (2B)	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 5 Structure of a packet going into PE1

3) In the backbone network, packets are transmitted along the port of trunk VLAN 10. The tag of the private network is kept in transparent state until these packets reach PE2.

4) PE2 discovers that the port where it connects CE2 is the access port of VLAN 10, removes the tag header of VLAN 10 according to 802.1Q, resumes the initial packets of users, and transmit the initial packets to CE2, as shown in figure 6.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 6 Structure of a packet from PE2

Seen from the forwarding flow, Dot1Q Tunnel is very concise for the signaling is not required to maintain the establishment of the tunnel, which can be realized through static configuration.

As to the typical configuration figure of Dot1Q Tunnel, XXCOM's products of different models are configured as follows when they run as PE (PE1 has the same configuration as PE2).

1) Dot1Q Tunnel Configuration of the switch:

Switch_config#dot1q-tunnel

Switch_config_g0/1#switchport pvid 10

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#switchport trunk vlan-untagged 1-9,11-4094

Appendix Abbreviations

English abbreviation	English full name
VPN	Virtual Private Network
TPID	Tag Protocol Identifier
QoS	Quality of Service
P	provider bridged network core
PE	provider bridged network edge
CE	customer network edge
UNI	user-network interface
NNI	network-network interface
CVLAN	Customer VLAN
SPVLAN	Service provider VLAN

Chapter 30 Private VLAN Settings

30.1 Overview of Private VLAN

Private VLAN has settled the VLAN application problems facing ISPs: If ISP provides each user with a VLAN, the support by each device of 4094 VLANs will restrict the total of ISP-supported users.

30.2 Private VLAN Type and Port Type in Private VLAN

Private VLAN subdivides the L2 broadcast domain of a VLAN into multiple sub-domains, each of which consists of a private VLAN pair: a primary VLAN and a secondary VLAN. One private VLAN domain may have multiple private VLAN pairs and each private VLAN pair stands for a sub-domain. There is only one primary VLAN in a private VLAN domain and all private VLAN pairs share the same primary VLAN. The IDs of secondary VLANs in each sub-domain differ with each other.

30.2.1 Having One Primary VLAN Type

- Primary VLAN: It is relevant to a promiscuous port and only one primary VLAN exists in the private VLAN. Each port in the primary VLAN is a member in the primary VLAN.

30.2.2 Having Two Secondary VLAN Types

- Isolated VLAN: No layer-2 communication can be conducted between two ports in the same isolated VLAN. Also, there is only one isolated VLAN in a private VLAN. The isolated VLAN must be related with the primary VLAN.
- Community VLAN: Layer-2 communication can be conducted between two ports in the same VLAN, but they have no communication with the ports in another community VLAN. One private VLAN may contain multiple community VLANs. The community VLAN must be related with the primary VLAN.

30.2.3 Port Types Under the Private VLAN Port

- Promiscuous port: it belongs to the primary VLAN. It can communicate with all other ports, including the isolated port and community port of a secondary VLAN in the same private VLAN.
- Isolated port: It is the host port in the isolated VLAN. In the same private VLAN, the isolated port is totally L2 isolated from other ports except the promiscuous port, so the flows received from the isolated port can only be forwarded to the promiscuous port.
- Community port: It is the host port in the community VLAN. In a private VLAN, the community ports of the same community VLAN can conduct L2 communication each other or with the promiscuous port, but not with the community port of other VLANs and the isolated ports in the isolated VLANs.

30.2.4 Modifying the Fields in VLAN TAG

This functionality supports to modify the VLAN ID and priority in VLAN tag and decides whether the egress packets of private VLAN carry the tag or not.

30.3 Private VLAN Configuration Task List

- Configuring Private VLAN

- Configuring the association of private VLAN domains
- Configuring the L2 port of private VLAN to be the host port
- Configuring the L2 port of private VLAN to be the promiscuous port
- Modifying related fields of egress packets in private VLAN
- Displaying the configuration information of private VLAN

30.4 Private VLAN Configuration Tasks

The conditions for a private VLAN peer to take effect are listed below:

1. Having the primary VLAN
2. Having the secondary VLAN
3. Having the association between primary VLAN and secondary VLAN
4. Having the promiscuous port in primary VLAN

30.4.1 Configuring Private VLAN

Use the following commands to set VLAN to be a private VLAN.

Command	Purpose
vlan *vlan-id*	Enters the VLAN mode.
private-vlan {primary|community|isolated}	Configures the features of private VLAN.
no private-vlan {primary|community|isolated}	Deletes the features of private VLAN.
show vlan private-vlan	Displays the configuration of private VLAN.
exit	Exits from Vlan configuration mode.

30.4.2 Configuring the Association of Private VLAN Domains

Run the following commands to associate the primary VLAN and the secondary VLAN.

Command	Purpose
vlan vlan-id	Enters the primary VLAN configuration mode.
private-vlan association {svlist | **add** svlist | **remove** svlist}	Sets the to-be-associated secondary VLAN.
no private-vlan association	Clears all associations between the current primary VLAN and all secondary VLANs.
exit	Exits the VLAN configuration mode.

30.4.3 Configuring the L2 Port of Private VLAN to Be the Host Port

Run the following commands to set the L2 port of private VLAN to be the host port:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport mode private-vlan host	Sets the layer-2 port to be in host's port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan host-association *p_vid s_vid*	Associates the L2 host port with private VLAN.
no switchport private-vlan host-association	Deletes the association between L2 host port and private VLAN.
exit	Exits from the interface configuration mode.

30.4.4 Configuring the L2 Port of Private VLAN to Be the Promiscuous Port

Run the following commands to set the L2 port of private VLAN to be the promiscuous port:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport mode private-vlan promiscuous	Sets the layer-2 port to be in promiscuous port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan mapping p_vid{svlist | add svlist | **remove** svlist}	Associates the L2 promiscuous port with private VLAN.
no switchport private-vlan mapping	Deletes the association between L2 promiscuous port and private VLAN.
exit	Exits from the interface configuration mode.

30.4.5 Modifying Related Fields of Egress Packets in Private VLAN

Run the following commands to modify related fields of the egress packets in private VLAN:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport private-vlan tag-pvid *vlan-id*	Sets the VLAN ID field in the tag of egress packet.
switchport private-vlan tag-pri *pri*	Sets the priority field in the tag of egress packet.

[no] switchport private-vlan untagged	Sets whether the egress packets have the tag or not.
exit	Exits from interface configuration mode.

30.4.6 Displaying the Configuration Information of Private VLAN

Run the following commands in global, interface or VLAN configuration mode to display the private VLAN configuration information of private VLAN and L2 port:

Command	Purpose
show vlan private-vlan	Displays the configuration of private VLAN.
show vlan private-vlan interface *interface*	Displays the configuration of the L2 port in the private VLAN.

30.5 Configuration Example

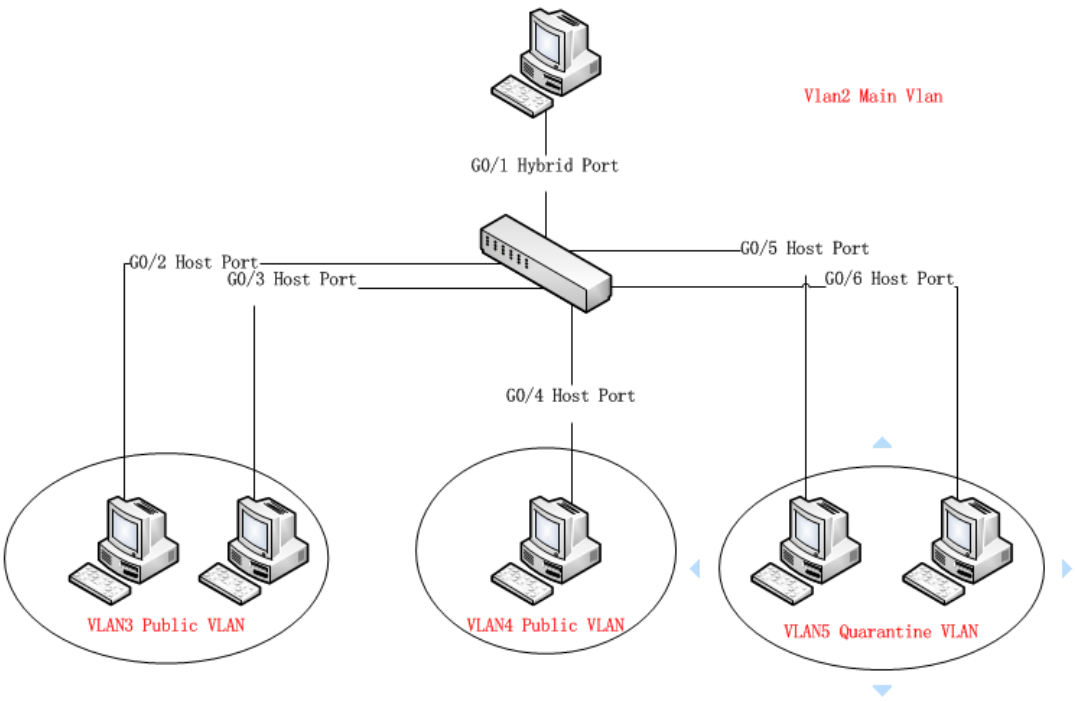


Figure 30-1: Typical Configuration of Private VLAN

As shown in figure 1, port G0/1 is the promiscuous port in primary VLAN 2 and ports G0/2-G0/6 are host ports, among which ports G0/2 and G0/3 are host ports (public ports) of Community VLAN 3, port G0/4 is that of Community VLAN 4, and ports G0/5 and G0/6 are host ports of Isolated VLAN 5.

According to the definition of private VLAN, L2 communication can be conducted between promiscuous port G0/1 and host ports of all sub-VLAN domains, so it is between host ports G0/2 and G0/3 of community VLAN 3, but they cannot conduct L2 communication with other host ports of secondary VLANs. L2 communication cannot go on between ports G0/5 and G0/6 in Isolated VLAN 5, but the two ports can conduct L2 communication with promiscuous port G0/1.

The commands requiring to be entered in a switch are shown below:

```
Switch_config#interface GigaEthernet0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous
Switch_config_g0/1#switchport private-vlan mapping 2 3-5
Switch_config_g0/1#switchport pvid 2

Switch_config#interface GigaEthernet0/2
Switch_config_g0/2#switchport mode private-vlan host
Switch_config_g0/2#switchport private-vlan host-association 2 3
Switch_config_g0/2#switchport pvid 3

Switch_config#interface GigaEthernet0/3
Switch_config_g0/3#switchport mode private-vlan host
Switch_config_g0/3#switchport private-vlan host-association 2 3
Switch_config_g0/3#switchport pvid 3

Switch_config#interface GigaEthernet0/4
Switch_config_g0/4#switchport mode private-vlan host
Switch_config_g0/4#switchport private-vlan host-association 2 4
Switch_config_g0/4# switchport pvid 4

Switch_config#interface GigaEthernet0/5
Switch_config_g0/5#switchport mode private-vlan host
Switch_config_g0/5#switchport private-vlan host-association 2 5
Switch_config_g0/5#switchport pvid 5

Switch_config#interface GigaEthernet0/6
Switch_config_g0/5#switchport mode private-vlan host
Switch_config_g0/5#switchport private-vlan host-association 2 5
Switch_config_g0/5#switchport pvid 5

Switch_config#vlan 2
Switch_config_vlan2#private-vlan primary
Switch_config_vlan2#private-vlan association 3-5

Switch_config#vlan 3
Switch_config_vlan3#private-vlan community

Switch_config#vlan 4
Switch_config_vlan4#private-vlan community

Switch_config#vlan 5
Switch_config_vlan5#private-vlan isolated
```

```
Switch_config#show vlan private-vlan
Primary  Secondary  Type         Ports
-------  ---------  -----------  ------------------------------------------
2        3          community    g0/1, g0/2, g0/3
2        4          community    g0/1, g0/4
2        5          isolated     g0/1, g0/5, g0/6
```

Chapter 31 Configuring STP

31.1 STP Introduction

The standard Spanning-Tree Protocol (STP) is defined in IEEE 802.1D. It simplifies the LAN topology comprising several bridges to a sole spinning tree, preventing network loop from occurring and ensuring stable work of the network.

The algorithm of STP and its protocol configure the random bridging LAN to an active topology with simple connections. In the active topology, some bridging ports can forward frames; some ports are in the congestion state and cannot transmit frames. Ports in the congestion state may be concluded in the active topology. When the device is ineffective, added to or removed from the network, the ports may be changed to the transmitting state.

In the STP topology, a bridge can be viewed as root. For every LAN section, a bridging port will forward data from the network section to the root. The port is viewed as the designated port of the network section. The bridge where the port is located is viewed as the designated bridge of the LAN. The root is the designated bridge of all network sections that the root connects. In ports of each bridge, the port which is nearest to the root is the root port of the bridge. Only the root port and the designated port (if available) is in the transmitting state. Ports of another type are not shut down but they are not the root port or the designated port. We call these ports are standby ports.

The following parameters decides the structure of the stabilized active topology:

(1) Identifier of each bridge

(2) Path cost of each port

(3) Port identifier for each port of the bridge

The bridge with highest priority (the identifier value is the smallest) is selected as the root. Ports of each bridge has the attribute **Root Path Cost**, that is, the minimum of path cost summation of all ports from the root to the bridge. The designated port of each network segment refers to the port connecting to the network segment and having the minimum path cost.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Our switch standard supports two modes of spanning tree protocol 802.1D STP and 802.1w RSTP. Some models of the switch support distributing STP mode according to VLAN and MSTP spanning tree protocol. For more details, please refer to 'Configuring RSTP' in chapter 2.

This chapter describes how to configure the standard spanning tree protocol that switch supports.

NOTE: 802.1D STP and 802.1w RSTP are abbreviated to SSTP and RSTP in this article. SSTP means Single Spanning-tree.

31.2 SSTP Configuration Task List

- Selecting STP Mode
- Disabling/Enabling STP
- Forbidding/Enable Port's STP
- Configuring the Switch Priority
- Configuring the Hello Time
- Configuring the Max-Age Time
- Configuring the Forward Delay Time
- Configuring the Port Priority

- Configuring the Path Cost
- Monitoring STP State
- Configuring SNMP Trap

31.3 SSTP Configuration Task

31.3.1 Selecting STP Mode

Run the following command to configure the STP mode:

Command	Purpose
spanning-tree mode {sstp | pvst | rstp | mstp}	Select the STP configuration.

31.3.2 Disabling/Enabling STP

Spanning tree is enabled by default. Disable spanning tree only if you are sure there are no loops in the network topology. Follow these steps to disable spanning-tree:

Command	Purpose
no spanning-tree	Disables STP.

To enable spanning-tree, use the following command:

Command	Purpose
spanning-tree	Enables default mode stp (sstp).
spanning-tree mode {sstp | pvst | rstp | mstp}	Enables a certain mode stp.

31.3.3 Forbidding/Enable Port's STP

Under default circumstances, STP protocol operates on all switching ports (physical ports and aggregation ports). STP operation is forbidden under port configuration mode by the following command:

Command	Purpose
no spanning-tree	Forbidding port to operate STP.

After STP operation is forbidden on port, port would keep assigning ports and forwarding status, and would not send BPDU. But all STP mode would still do type checking and counting on BPDU received by port. Boundary information and topology information would also be updated.

NOTE: When processing "no spanning-tree", if port has already have roles like "RootPort", "AlternatePort", "MasterPort" or "BackupPort, under RSTP/MSTP mode, protocol information received by port would be aged and turned into "DesignatedPort". Under SSTP/PVST mode, port would stay as the former role for some time, and information would be

aging after timer is over time.

NOTE: Every STP mode supports BpduGuard function on "no spanning-tree" port.

31.3.4 Configuring the Switch Priority

You can configure the switch priority and make it more likely that a standalone switch or a switch in the stack will be chosen as the root switch.
Follow these steps to configure the switch priority:

Command	Purpose
spanning-tree sstp priority *value*	Modifies SSTP priority value.
no spanning-tree sstp priority	Returns SSTP priority to default value (32768).

31.3.5 Configuring the Hello Time

User can configure the interval between STP data units sent by the root switch through changing the hello time.
Use the following command to configure Hello Time of SSTP:

Command	Purpose
spanning-tree sstp hello-time *value*	Configures SSTP Hello Time.
no spanning-tree sstp hello-time	Returns SSTP Hello Time to default value (2s).

31.3.6 Configuring the Max-Age Time

Use the sstp max age to configure the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.
Follow these steps to configure the maximum-aging time:

Command	Purpose
spanning-tree sstp max-age *value*	Configures the SSTP max-age time.
no spanning-tree sstp max-age	Returns the max-age time to default value (20s).

31.3.7 Configuring the Forward Delay Time

Configure sstp forward delay to determine the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.
Use the following command to configure sstp forward delay:

Command	Purpose
spanning-tree sstp forward-time *value*	Configures SSTP Forward time.

no spanning-tree sstp forward-time	Returns forward time to default value (15s).

31.3.8 Configuring the Port Priority

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
Follow these steps to configure the port priority of an interface:

Command	Purpose
spanning-tree port-priority *value*	Configures the port priority for an interface.
spanning-tree sstp port-priority *value*	Modifies SSTP port priority.
no spanning-tree sstp port-priority	Returns port priority to default value (128).

31.3.9 Configuring the Path Cost

Follow these steps to configure the cost of an interface:

Command	Purpose
spanning-tree cost *value*	Configures the cost for an interface.
spanning-tree sstp cost *value*	Modifies SSTP path cost.
no spanning-tree sstp cost	Returns path cost to default value.

31.3.10 Monitoring STP State

To monitor the STP configuration and state, use the following command in management mode:

Command	Purpose
show spanning-tree	Displays spanning-tree information on active interfaces only.
show spanning-tree detail	Displays a detailed summary of interface information.
show spanning-tree interface	Displays spanning-tree information for the specified interface.

31.3.11 Configuring SNMP Trap

You can monitor the change of STP in a switch remotely from the network management software of the host by configuring the trap function of STP.
STP protocols support two types of traps: newRoot and topologyChange. When the switch changes from the non-root

type to the newRoot type, the switch sends newRoot Trap message; when the switch detects the topology change, such as a non-edge port changes from the state of non-forward to forward, the switch sends topologyChange Trap message.

NOTE: It needs to use network management software which supports Trap to receive STP trap. Network management software need to be import Bridge-MIB set, and OID is 1.3.6.1.2.1.17.

Use the following commands to intiate STP Trap under global configuration mode:

Command	Purpose
spanning-tree management trap [newroot | topologychange]	Initiating STP Trap. If Trap type is not defined, two kinds of TRAP would be initiated at the mean time.
no spanning-tree management trap	Shut down STP Trap.

31.4 Configuring VLAN spanning-tree

31.4.1 Overview

In SSTP mode, there is only one spanning tree instance for the entire network, and the state of the switch port in the spanning tree determines its state in VLAN. In the case of multiple vlans in the network, the isolation between the single spanning tree protocol and the VLAN topology may cause the normal communication of part of the network to be blocked. The switch supports running independent SSTP on a certain number of vlans, ensuring that ports can have different states in different vlans. At the same time, the traffic balance between VLANs can be realized.

It is important to note that the number of VLANs that can run the spanning tree protocol independently depends on the actual version, and other VLAN topologies that exceed the number limit will not be controlled by STP.

31.4.2 VLAN STP Configuration Task

Follow these commands to configure the properties of SSTP in the VLAN in the global configuration mode:

Command	Purpose
spanning-tree mode pvst	Start the mode of allocating STP by VLAN.
spanning-tree vlan *vlan-list*	Assign a STP Instance to the specified VLAN. vlan-list: VLAN list (same below).
no spanning-tree vlan *vlan-list*	Remove a spanning-tree Instance from the specified VLAN.
spanning-tree vlan *vlan-list* priority *value*	Configure the priority level of the spanning tree in the specified VLAN.
no spanning-tree *vlan-list* priority	Reset the spanning tree priority in VLAN to default.
spanning-tree vlan *vlan-list* forward-time *value*	Configure the Forward Delay of the specified VLAN.

no spanning-tree vlan *vlan-list* forward-time	Reset the Forward Delay of the specified VLAN to default.
spanning-tree vlan *vlan-list* max-age *value*	Configure the Max-age of the specified VLAN.
no spanning-tree vlan *vlan-list* max-age	Reset the Max-age of the specified VLAN to default.
spanning-tree vlan *vlan-list* hello-time *value*	Configure the Hello-time of the specified VLAN.
no spanning-tree vlan *vlan-list* hello-time	Reset the Hello-time of the specified VLAN to default.

Follow these commands to configure the properties of the port in the interface configuration mode:

Command	Purpose
spanning-tree vlan *vlan-list* cost	Configure the port path cost in the specified VLAN.
no spanning-tree vlan *vlan-list* cost	Reset the port path cost in the specified VLAN to default.
spanning-tree vlan *vlan-list* port-priority	Configure the port-priority in the specified VLAN.
no spanning-tree vlan *vlan-list* port-priority	Reset the port-priority in the specified VLAN to default.

Follow these commands to check the state of spanning-tree at specified VLAN in the management configuration mode:

Command	Purpose
show spanning-tree vlan *vlan-list*	Check the spanning-tree state in VLAN.
show spanning-tree pvst instance-list	Check the relationship between PVST instance and the VLAN.

Chapter 32 Configuring RSTP

32.1 RSTP Configuration Task List

- Enabling/Disabling Switch RSTP
- Configuring the Switch Priority
- Configuring the Forward Delay Time
- Configuring the Hello Time
- Configuring the Max-Age
- Configuring the Path Cost
- Configuring the Port Priority
- Configuring edge port
- Configuring port's connection type
- Restarting the check of protocol conversion

32.2 RSTP Configuration Task

32.2.1 Enabling/Disabling Switch RSTP

Follow these configurations in the global configuration mode:

Command	Purpose
spanning-tree mode rstp	Enables RSTP
no spanning-tree mode	Returns STP to default mode (SSTP)

32.2.2 Configuring the Switch Priority

You can configure the switch priority and make it more likely that a standalone switch or a switch in the stack will be chosen as the root switch.

Follow these configurations in the global configuration mode:

Command	Purpose
spanning-tree rstp priority *value*	Modifies rstp priority value.
no spanning-tree rstp priority	Returns rstp priority to default value.

Note: If the priority of all bridges in the whole switch network uses the same value, then the bridge with the least MAC address will be chosen as the root bridge. In the situation when the RSTP protocol is enabled, if the bridge priority value is modified, it will cause the recalculation of spanning tree.

The bridge priority is configured to 32768 by default.

32.2.3 Configuring the Forward Delay Time

Link failures may cause network to recalculate the spanning tree structure. But the latest configuration message can no be conveyed to the whole network. If the newly selected root port and the specified port immediately start forwarding data,

this may cause temporary path loop. Therefore the protocol adopts a kind of state migration mechanism. There is an intermediate state before root port and the specified port starting data forwarding, after the intermediate state passing the Forward Delay Time, the forward state begins. This delay time ensures the newly configured message has been conveyed to the whole network. The Forward Delay characteristic of the bridge is related to the network diameter of the switch network. Generally, the grater the network diameter, the longer the Forward Delay Time should be configured.
Follow these configurations in the global configuration mode:

Command	purpose
spanning-tree rstp forward-time *value*	Configures Forward Delay
no spanning-tree rstp forward-time	Returns Forward Delay Time to default value (15s).

Note: If you configure the Forward Delay Time to a relatively small value, it may leads to a temporary verbose path. If you configure the Forward Delay Time to a relatively big value, the system may not resume connecting for a long time. We recommend user to use the default value.
The Forward Delay Time of the bridge is 15 seconds.

32.2.4 Configuring the Hello Time

The proper hello time value can ensure that the bridge detect link failures in the network without occupying too much network resources.
Follow these configurations in the global configuration mode:

command	purpose
spanning-tree rstp hello-time *value*	Configures Hello Time
no spanning-tree rstp hello-time	Returns Hello Time to default value.

To be noticed is that too-long Hello Time value would cause network bridge cannot receive Hello message because of link's packet loss. Therefore network bridge would consider link is broken and recalculate spanning tree. If Hello Time value is too short, it would cause that network bridge sends configuration message frequently and the network bandwidth is occupied. It adds burden on network and CPU. It is suggested that user uses default value.
Note: We recommend user to use the default value.
The default Hello Time is 2 seconds.

32.2.5 Configuring the Max-Age

The ma-age is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.
Follow these configurations in the global configuration mode:

Command	Purpose
spanning-tree rstp max-age *value*	Configures the max-age value.
no spanning-tree rstp max-age	Returns the max-age time to default value (20s).

We recommend user to use the default value. Note: if you configure the Max Age to a relatively small value, then the calculation of the spanning tree will be relatively frequent, and the system may regard the network block as link failure. If you configure the Max Age to a relatively big value, then the link status will go unnoticed in time.
The Max Age of bridge is 20 seconds by default.

32.2.6 Configuring the Path Cost

The spanning-tree path cost default value is derived from the media speed of an interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values to interfaces that you want selected last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
Beginning in interface configuration mode, follow these steps to configure the cost of an interface:

Command	Purpose
spanning-tree rstp cost *value*	Configures the cost for an interface.
no spanning-tree rstp cost	Returns path cost to default value.

Note: The modification of the priority of the Ethernet port will arise the recalculation of the spanning tree. We recommend user to use the default value and let RSTP protocol calculate the path cost of the current Ethernet interface.
When the port speed is 10Mbps, the path cost of the Ethernet interface is 2000000. When the port speed is 100Mbps, the path cost of the Ethernet interface is 200000.

32.2.7 Configuring the Port Priority

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first, and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
Follow these configurations in the interface configuration mode:

Command	Purpose
spanning-tree rstp port-priority *value*	Configures the port priority for an interface.
no spanning-tree rstp port-priority	Returns the port priority to the default value.

NOTE: The modification of the priority of the Ethernet interface will arise the recalculation of the spanning tree.
The default Ethernet interface priority is 128.

32.2.8 Configuring edge port

The edge port means this port connects with terminal device on network. A mandatory edge port would be at forwarding status instantly after being linked up. Use the following command to configure RSTP's edge port under port configuration mode:

Command	Purpose
spanning-tree rstp edge	Configuring port as edge port.

Under automatic detection of protocol mode, if port does not receive BPDU at some time, the port is considered as edge port.

32.2.9 Configuring port's connection type

It the switches which operate RSTP protocol connect with each other by point to point, they could establish topology quickly by handshake mechanism.

Under default condition, the protocol determines whether the port uses point-to-point connection according to port's duplex property. If port works under duplex mode, the protocol would consider its connection is point to point. If port works under half duplex mode, the protocol would consider its connection as shared.

If it is confirmed that the switch connected with port runs on RSTP or MSTP protocol, the port's connection type could be configured as point-to-point to guarantee the processing of quick handshake.

Under port configuration mode, use the following command to configure port's connection type:

Command	Purpose
spanning-tree rstp point-to-point [force-true | force-false | auto]	Configuring point-to-point port. force-true: forcing to point-to-point type. force-false: forcing to none point-to-point type. Auto: protocol automatically detects port's type.

32.2.10 Restarting the check of protocol conversion

RSTP protocol allows switch to cooperatively work with traditional 802.1D STP switch by a protocol conversion mechanism. If switch's one port receives STP's configuration information, this port would change to send STP messages only.

After a port is at STP compatible status, this port would recover to RSTP status even if this port does not receive 802.1D STP BPDU any longer. At the meantime, use command **spanning-tree rstp migration-check** to start port's check of protocol conversion and recover port to RSTP mode.

Use the following command to restart the check of RSTP protocol conversion under global configuration mode:

Command	Purpose
spanning-tree rstp migration-check	Restarting all ports' check process of protocol conversion

Use the following command to do check of port's protocol conversion under switch's port configuration mode:

Command	Purpose
spanning-tree rstp migration-check	Restarting the check of current port's protocol conversion process

Chapter 33 Configuring MTSP

33.1 MSTP Overview

33.1.1 Introduction

Multiple Spanning Tree Protocol (MSTP) is used to create simple complete topology in the bridging LAN. MSTP can be compatible with the earlier Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

Both STP and RSTP only can create sole STP topology. All VLAN messages are forwarded through the only STP. STP converges too slow, so RSTP ensures a rapid and stable network topology through the handshake mechanism.

MSTP inherits the rapid handshake mechanism of RSTP. At the same time, MST allows different VLAN to be distributed to different STPs, creating multiple topologies in the network. In networks created by MSTP, frames of different VLANs can be forwarded through different paths, realizing the load balance of the VLAN data.

Different from the mechanism that VLAN distributes STP, MSTP allows multiple VLANs to be distributed to one STP topology, effectively reducing STPs required to support lots of VLANs.

33.1.2 MST Domain

In MSTP, the relationship between VLAN and STP is described through the MSTP configuration table. MSTP configuration table, configuration name and configuration edit number makes up of the MST configuration identifier.

In the network, interconnected bridges with same MST configuration identifier are considered in the same MST region. Bridges in the same MST region always have the same VLAN configuration, ensuring VLAN frames are sent in the MST region.

33.1.3 IST, CST, CIST and MSTI

Figure 33.1 shows an MSTP network, including three MST regions and a switch running 802.1D STP.

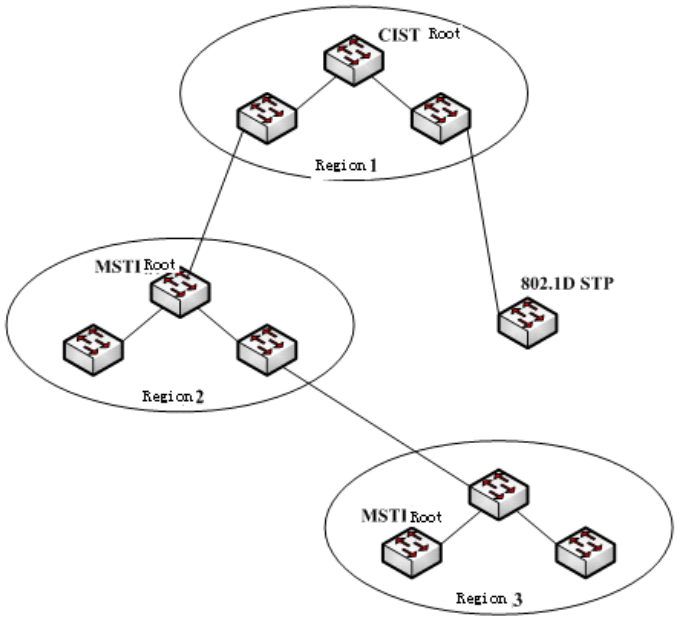


Figure 33-1 MSTP topology

1. CIST

Common and Internal Spanning Tree (CIST) means the spanning tree comprised by all single switches and interconnected LAN. These switches may belong to different MST regions. They may be switches running traditional STP or RSTP. Switches running STP or RSTP in the MST regions are considered to be in their own regions.

After the network topology is stable, the whole CIST chooses a CIST root bridge. An internal CIST root bridge will be selected in each region, which is the shortest path from the heart of the region to CIST root.

2. CST

If each MST region is viewed as a single switch, Common Spanning Tree (CST) is the spanning tree connecting all "single switches". As shown in Figure 2.1, region 1, 2 and 3 and STP switches make up of the network CST.

3. IST

Internal Spanning Tree (IST) refers to part of CIST that is in an MST region, that is, IST and CST make up of the CIST.

4. MSTI

The MSTP protocol allows different VLANs to be distributed to different spanning trees. Multiple spanning tree instances are then created. Normally, No.0 spanning tree instance refers to CIST, which can be expanded to the whole network. Every spanning tree instance starting from No.1 is in a certain region. Each spanning tree instance can be distributed with multiple VLANs. In original state, all VLANs are distributed in CIST.

MSTI in the MST region is independent. They can choose different switches as their own roots.

33.1.4 Port Role

Ports in MSTP can function as different roles, similar to ports in RSTP.

1. Root port

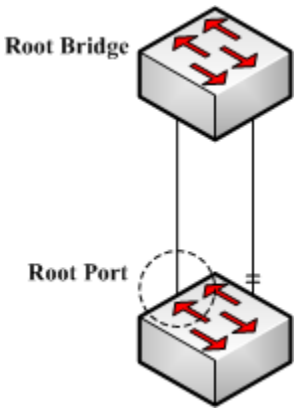


Figure 33-2 Root port

Root port stands for the path between the current switch and the root bridge, which has minimum root path cost.

2. Alternate port

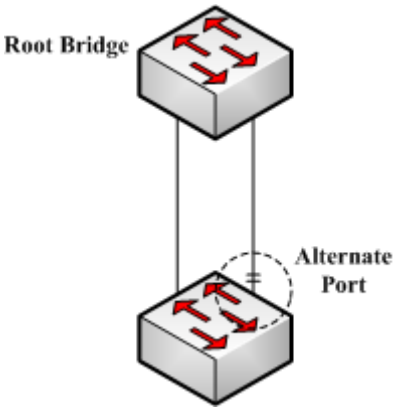


Figure 33-3 Alternate port

The alternate port is a backup path between the current switch and the root bridge. When the connection of root port is out of effect, the alternate port can promptly turn into a new root port without work interruption.

3. Designated port

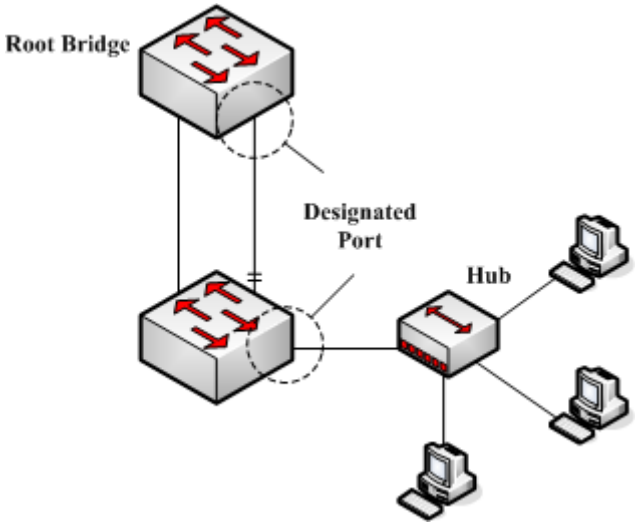


Figure 33-4 Designated port

The designated port can connect switches or LAN in the next region. It is the path between the current LAN and root bridge.

4. Backup port

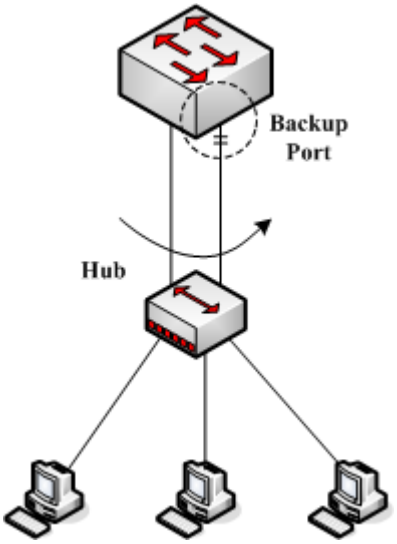


Figure 33-5 Backup port

When two switch ports directly connect or both connect to the same LAN, the port with lower priority is to be the backup port, the other port is to be the designated port. If the designated port breaks down, the backup port becomes the designated port to continue working.

5. Master port

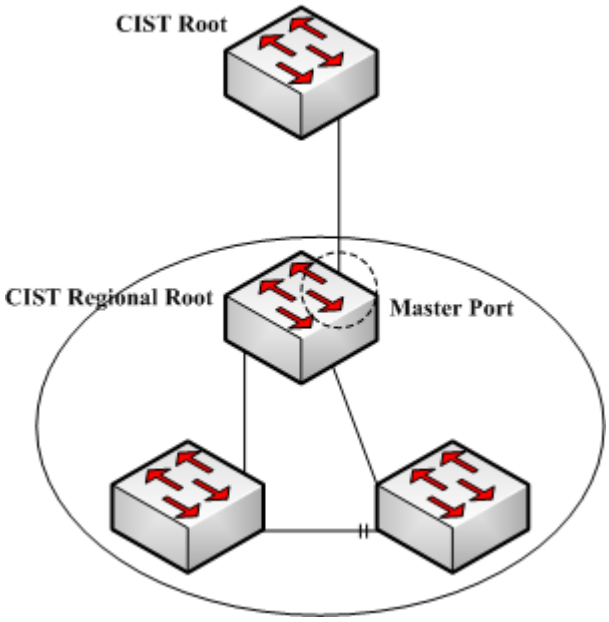


Figure 33-6 Master port

The Master port is the shortest path between MST region and CIST root bridge. Master port is the root port of the root bridge in the CIST region.

6. Boundary port

The concept of boundary port in CIST is a little different from that in each MSTI. In MSTI, the role of the boundary port means that the spanning tree instance does not expand on the port.

7. Edge port

In the RSTP protocol or MSTP protocol, edge port means the port directly connecting the network host. These ports can directly enter the forwarding state without causing any loop in the network.

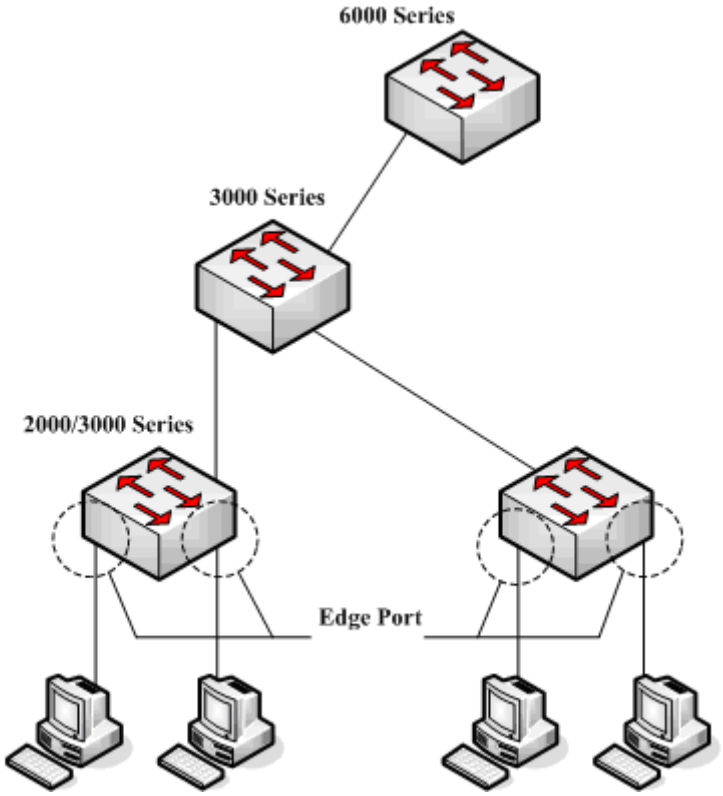


Figure 33-7 Edge port

In original state, MTSP and RSTP do not take all ports as edge ports, ensuring the network topology can be rapidly created. In this case, if a port receives BPDU from other switches, the port is resumed from the edge state to the normal state. If the port receives 802.1D STP BPDU, the port has to wait for double Forward Delay time and then enter the forwarding state.

33.1.5 MSTP BPDU

Similar to STP and RSTP, switches running MSTP can communicate with each other through Bridge Protocol Data Unit (BPDU). All configuration information about the CIST and MSTI can be carried by BPDU. Table 2.1 and Table 2.2 list the structure of BPDU used by the MSTP.

Field Name	Byte Number
Protocol Identifier	1 - 2
Protocol Version Identifier	3
BPDU Type	4
CIST Flags	5
CIST Root Identifier	6 - 13
CIST External Root Path Cost	14 - 17
CIST Regional Root Identifier	18 - 25
CIST Port Identifier	26 - 27
Message Age	28 - 29
Max Age	30 - 31
Hello Time	32 - 33
Forward Delay	34 - 35
Version 1 Length	36
Version 3 Length	37 - 38
Format Selector	39
Configuration Name	40 - 71
Revision	72 - 73
Configuration Digest	74 - 89
CIST Internal Root Path Cost	90 - 93
CIST Bridge Identifier	94 - 101
CIST Remaining Hops	102
MSTI Configuration Messages	103 ~

Table 33-1 MSTP BPDU

Field Name	Byte Number
MSTI FLAGS	1
MSTI Regional Root Identifier	2 - 9
MSTI Internal Root Path Cost	10 - 13
MSTI Bridge Priority	14

MSTI Port Priority	15
MSTI Remaining Hops	16

Table 33-2 MST configuration information

33.1.6 Stable State

The MSTP switch performs calculation and compares operations according to the received BPDU, and finally ensures that:

1. switch is selected as the CIST root of the whole network.
2. Each switch and LAN segment can decide the minimum cost path to the CIST root, ensuring a complete connection and prevent loops.
3. Each region has a switch as the CIST regional root. The switch has the minimum cost path to the CIST root.
4. Each MSTI can independently choose a switch as the MSTI regional root.
5. Each switch in the region and the LAN segment can decide the minimum cost path to the MSTI root.
6. The root port of CIST provides the minimum-cost path between the CIST regional root and the CIST root.
7. The designated port of the CIST provided its LAN with the minimum-cost path to the CIST root.
8. The Alternate port and the Backup port provides connection when the switch, port or the LAN does not work or is removed.
9. The MSTI root port provides the minimum cost path to the MSTI regional root.
10. The designated port of MSTI provides the minimum cost path to the MSTI regional root.
11. A master port provides the connection between the region and the CIST root. In the region, the CIST root port of the CIST regional root functions as the master port of all MSTI in the region.

33.1.7 Hop Count

Different from STP and RSTP, the MSTP protocol does not use Message Age and Max Age in the BPDU configuration message to calculate the network topology. MSTP uses Hop Count to calculate the network topology.

To prevent information from looping, MSTP relates the transmitted information to the attribute of hop count in each spanning tree. The attribute of hop count for BPDU is designated by the CIST regional root or the MSTI regional root and reduced in each receiving port. If the hop count becomes 0 in the port, the information will be dropped and then the port turns to be a designated port.

33.1.8 STP Compatibility

MSTP allows the switch to work with the traditional STP switch through protocol conversion mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message. At the same time, the port that receives the STP information is then considered as a boundary port.

NOTE: When a port is in the STP-compatible state, the port will not automatically resume to the MSTP state even if the port does not receive the STP message any more. In this case, you can run spanning-tree mstp migration-check to clear the STP message that the port learned, and make the port to return to the MSTP state.

The switch that runs the RSTP protocol can identify and handle the MSTP message. Therefore, the MSTP switch does not require protocol conversion when it works with the RSTP switch.

33.2 MSTP Configuration Task List

- Default MSTP configuration
- Enabling and disabling MSTP
- Configuring MSTP Area
- Configuring Network Root
- Configuring Secondary Root
- Configuring Bridge Priority
- Configuring STP Time Parameters
- Configuring Network Diameter
- Configuring Maximum Hop Count
- Configuring Port Priority
- Configuring Path Cost for the Port
- Configuring Edge Port
- Configuring Port Connection Type
- Activating MST-Compatible Mode
- Restarting Protocol Conversion Check
- Configuring Port's Role Restriction
- Configuring Port's TCN Restriction
- Checking MSTP Information

33.3 MSTP Configuration Task

33.3.1 Default MSTP Configuration

Attribute	Default Settings
STP mode	SSTP (PVST, RSTP and MSTP is not started)
Area name	Character string of MAC address
Area edit level	0
MST configuration list	All VLANs are mapped in CIST (MST00).
Spanning-tree priority (CIST and all MSTI)	32768
Spanning-tree port priority (CIST and all MSTI)	128
Path cost of the spanning-tree port (CIST and all MSTI)	1000 Mbps: 20000 100 Mbps: 200000 10 Mbps: 2000000
Hello Time	2 seconds
Forward Delay	15 seconds
Maximum-aging Time	20 seconds
Maximum hop count	20

33.3.2 Enabling and Disabling MSTP

The STP protocol can be started in PVST or SSTP mode by default. You can stop it running when the spanning-tree is not required.

Run the following command to set the STP to the MSTP mode:

Command	Purpose
spanning-tree	Enables STP in default mode.
spanning-tree mode mstp	Enables MSTP.

Run the following command to disable STP:

Command	Purpose
no spanning-tree	Disable the STP.

33.3.3 Configuring MST Area

The MST area where the switch resides is decided by three attributes: configuration name, edit number, the mapping relation between VLAN and MSTI. You can configure them through area configuration commands. Note that the change of any of the three attributes will cause the change of the area where the switch resides.

In original state, the MST configuration name is the character string of the MAC address of the switch. The edit number is 0 and all VLANs are mapped in the CIST (MST00). Because different switch has different MAC address, switches that run MSTP are in different areas in original state. You can run **spanning-tree mstp instance *instance-id* vlan *vlan-list*** to create a new MSTI and map the designated VLAN to it. If the MSTI is deleted, all these VLANs are mapped to the CIST again.

Run the following command to set the MST area information:

Command	Purpose
spanning-tree mstp name *string*	Configures the MST configuration name. **string** means the character string of the configuration name. It contains up to 32 characters, capital sensitive. The default value is the character string of the MAC address.
no spanning-tree mstp name	Sets the MST configuration name to the default value.
spanning-tree mstp revision *value*	Sets the MST edit number. **value** represents the edit number, ranging from 0 to 65535. The default value is 0.
no spanning-tree mstp revision	Sets the MST edit number to the default value.
spanning-tree mstp instance *instance-id* vlan *vlan-list*	Maps VLAN to MSTI. **instance-id** represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 15.

	vlan-list means the VLAN list that is mapped to the spanning tree. It ranges from 1 to 4094. **instance-id** is an independent value representing a spanning tree instance. **vlan-list** can represent a group of VLANs, such as "1,2,3", "1-5" and "1,2,5-10".
no spanning-tree mstp instance *instance-id*	Cancels the VLAN mapping of MSTI and disables the spanning tree instance. instance-id represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 15.

Run the following command to check the configuration of the MSTP area:

Command	Purpose
show spanning-tree mstp region	Displays the configuration of the MSTP area.

33.3.4 Configuring Network Root

In MSTP, each spanning tree instance has a bridge ID, containing the priority value and MAC address of the switch. During the establishment of spanning tree topology, the switch with comparatively small bridge ID is selected as the network root. MSTP can set the switch to the network switch through configuration. You can run the command **Spanning-tree mstp Spanning-tree mstp *instance-id* rootroot** to modify the priority value of the switch in a spanning tree instance from the default value to a sufficiently small value, ensuring the switch turns to be the root in the spanning tree instance.

In general, after the previous command is executed, the protocol automatically check the bridge ID of the current network root and then sets the priority field of the bridge ID to **24576** when the value **24576** ensures that the current switch becomes the root of the spanning tree.

If the network root's priority value is smaller than the value **24576**, MSTP automatically sets the spanning tree's priority of the current bridge to a value that is 4096 smaller than the priority value of the root. Note that the number **4096** is a step length of network priority value.

When setting the root, you can run the **diameter** subcommand to the network diameter of the spanning tree network. The keyword is effective only when the spanning tree instance ID is 0. After the network diameter is set, MSTP automatically calculates proper STP time parameters to ensure the stability of network convergence. Time parameters include Hello Time, Forward Delay and Maximum Age. The subcommand Hello-time can be used to set a new hello time to replace the default settings.

Run the following command to set the switch to the network root:

Command	Purpose
spanning-tree mstp *instance-id* root primary [**diameter** *net-diameter* [**hello-time** *seconds*]]	Sets the switch to the root in the designated spanning tree instance. **instance-id** represents the number of the spanning tree instance, ranging from 0 to 15. **net-diameter** represents the network diameter, which is an

	optional parameter. It is effective when **instance-id** is 0. It ranges from 2 to 7. **seconds** represents the unit of the hello time, ranging from 1 to 10.
no spanning-tree mstp *instance-id* root	Cancels the root configuration of the switch in the spanning tree. **instance-id** means the number of the spanning tree instance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
show spanning-tree mstp [**instance** *instance-id*]	Checks the MSTP message.

33.3.5 Configuring Secondary Root

After the network root is configured, you can run **spanning-tree mstp *instance-id* root secondary** to set one or multiple switches to the secondary roots or the backup roots. If the root does not function for certain reasons, the secondary roots will become the network root.

Different from the primary root configuration, after the command to configure the primary root is run, MSTP sets the spanning tree priority of the switch to **28672**. In the case that the priority value of other switches is the default value **32768**, the current switch can be the secondary root.

When configuring the secondary root, you can run the subcommands **diameter** and **hello-time** to update the STP time parameters. When the secondary root becomes the primary root and starts working, all these parameters starts functioning.

Run the following command to set the switch to the secondary root of the network:

Command	Purpose
spanning-tree mstp *instance-id* root secondary [**diameter** *net-diameter* [**hello-time** *seconds*]]	Sets the switch to the secondary root in the designated spanning tree instance. **instance-id** represents the number of the spanning tree instance, ranging from 0 to 15. **net-diameter** represents the network diameter, which is an optional parameter. It is effective when **instance-id** is 0. It ranges from 2 to 7. **seconds** represents the unit of the hello time, ranging from 1 to 10.
no spanning-tree mstp *instance-id* root	Cancels the root configuration of the switch in the spanning tree. **instance-id** means the number of the spanning tree instance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
show spanning-tree mstp [**instance** *instance-id*]	Check the message about the MST instance.

33.3.6 Configuring Bridge Priority

In some cases, you can directly set the switch to the network root by configuring the bridge priority. It means that you can set the switch to the network root without running the subcommand **root**. The priority value of the switch is independent in each spanning tree instance. Therefore, the priority of the switch can be set independently.

Run the following command to configure the priority of the spanning tree:

Command	Purpose
spanning-tree mstp *instance-id* priority *value*	Sets the priority of the switch. instance-id represents the number of the spanning tree instance, ranging from 0 to 15. **value** represents the priority of the bridge. It can be one of the following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
no spanning-tree mstp *instance-id* priority	Resumes the bridge priority of the switch to the default value. **instance-id** means the number of the spanning tree instance, ranging from 0 to 15.

33.3.7 Configuring STP Time Parameters

The following are STP time parameters:

- Hello Time:
  The interval to send the configuration message to the designated port when the switch functions as the network root.
- Forward Delay:
  Time that the port needs when it changes from the **Blocking** state to the **learning** state and to the **forwarding** state in STP mode.
- Max Age:
  The maximum live period of the configuration information about the spanning tree.

To reduce the shock of the network topology, the following requirements for the time parameters must be satisfied:

- 2 x (fwd_delay - 1.0) >= max_age
- max_age >= (hello_time + 1) x 2

Run the following command to configure the time parameter of the multiple spanning tree protocol:

Command	Purpose
spanning-tree mstp hello-time *seconds*	Sets the parameter **Hello Time**. The parameter **seconds** is the unit of **Hello Time**, ranging from 1 to 10 seconds. Its default value is two seconds.
no spanning-tree mstp hello-time	Resumes **Hello Time** to the default value.
spanning-tree mstp forward-time *seconds*	Sets the parameter **Forward Delay**. The parameter **seconds** is the unit of **Forward Delay**, ranging from 4 to 30 seconds. Its default value is 15 seconds.
no spanning-tree mstp forward-time	Resumes **Forward Delay** to the default value.
spanning-tree mstp max-age *seconds*	Sets the parameter **Max Age**. The parameter **seconds** is the unit of **Max Age**, ranging from 6 to 40 seconds. Its default value is 20 seconds.
no spanning-tree mstp max-age	Resumes **Max Age** to the default value.

It is recommended to modify STP time parameters by setting root or network diameter, which ensures correct modification of time parameters.

The newly-set time parameters are valid even if they do not comply with the previous formula's requirements. Pay attention to the notification on the console when you perform configuration.

33.3.8 Configuring Network Diameter

Network diameter stands for the maximum number of switches between two hosts in the network, representing the scale of the network.

You can set the MSTP network diameter by running the command **spanning-tree mstp diameter *net-diameter***. The parameter **net-diameter** is valid only to CIST. After configuration, three STP time parameters is automatically updated to comparatively better values.

Run the following command to configure **net-diameter**:

Command	Purpose
spanning-tree mstp diameter *net-diameter*	Configure net-diameter. The parameter **net-diameter** ranges from 2 to 7. The default value is 7.
no spanning-tree mstp diameter	Resumes **net-diameter** to the default value.

The parameter **net-diameter** is not saved as an independent setup in the switch. Only when modified by setting the network diameter can the time parameter be saved.

33.3.9 Configuring Maximum Hop Count

Run the following command to configure the maximum hop count.

Command	Purpose
spanning-tree mstp max-hops *hop-count*	Set the maximum hops. **hop-count** ranges from 1 to 40. Its default value is 20.
no spanning-tree mstp *hop-count*	Resume the maximum hop count to the default value.

33.3.10 Configuring Port Priority

If a loop occurs between two ports of the switch, the port with higher priority will enter the forwarding state and the port with lower priority is blocked. If all ports have the same priority, the port with smaller port number will first enter the forwarding state.

In port configuration mode, run the following command to set the priority of the STP port:

Command	Purpose
spanning-tree mstp *instance-id* port-priority *priority*	Sets the priority of the STP port. **instance-id** stands for the number of the spanning tree instance, ranging from 0 to 15. **priority** stands for the port priority. It can be one of the following values: 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240
spanning-tree port-priority *value*	Sets the port priority in all spanning tree instances. **value** stands for the port priority. It can be one of the following values: 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240
no spanning-tree mstp *instance-id* port-priority	Resumes the port priority to the default value.
no spanning-tree port-priority	Resumes the port priority to the default value in all spanning tree instances.

33.3.11 Configuring Path Cost of the Port

In MSTP, the default value of the port's path cost is based on the connection rate. If a loop occurs between two switches, the port with less path cost will enter the forwarding state. The less the path cost is, the higher rate the port is. If all ports have the same path cost, the port with smaller port number will first enter the forwarding state.

In port configuration mode, run the following command to set the path cost of the port:

Command	Purpose
spanning-tree mstp *instance-id* cost *cost*	Sets the path cost of the port. **instance-id** stands for the number of the spanning tree instance, ranging from 0 to 15.

	cost stands for the path cost of the port, which ranges from 1 to 200000000.
spanning-tree cost *value*	Sets the path cost of the port in all spanning tree instances. **Value** stands for the path cost of the port, which ranges from 1 to 200000000.
no spanning-tree mstp *instance-id* cost	Resumes the path cost of the port to the default value.
no spanning-tree cost	Resumes the path cost of the port to the default value in all spanning tree instances.

33.3.12 Configuring Edge Port

Edge port means this port connects with terminal device on network. A mandatory edge port would be at forwarding status instantly after Link Up. Use the following command to configure MSTP's edge port under port configuration mode:

Command	Purpose
spanning-tree mstp edge	Configuring port as edge port
no spanning-tree mstp edge	Recovering the default automatic check edge port

33.3.13 Configuring Port Connection Type

If the connection between MSTP-supported switches is the point-to-point direct connection, the switches can rapidly establish connection through handshake mechanism. When you configure the port connection type, set the port connection to the point-to-point type.

The protocol decides whether to use the point-to-point connection or not according to the duplex attribute. If the port works in full-duplex mode, the protocol considers the connection is a point-to-point one. If the port works in the half-duplex mode, the protocol considers the connection is a shared one.

If the switch that the port connects run the RSTP protocol or the MSTP protocol, you can set the port connection type to **point-to-point**, ensuring that a handshake is rapidly established.

In port configuration mode, run the following command to set the port connection type.

Command	Purpose
spanning-tree mstp point-to-point force-true	Sets the port connection type to **point-to-point**.
spanning-tree mstp point-to-point force-false	Sets the port connection type to **shared**.
spanning-tree mstp point-to-point auto	Automatically checks the port connection type.
no spanning-tree mstp point-to-point	Resumes the port connection type to the default settings.

33.3.14 Activating MST-Compatible Mode

The MSTP protocol that our switches support is based on IEEE 802.1s. In order to be compatible with other MSTPs, especially MSTP that the Cisco switches support, the MSTP protocol can work in MST-compatible mode. Switches running

in MSTP-compatible mode can identify the message structure of other MSTPs, check the contained MST regional identifier and establish the MST region.

The MST-compatible mode and the STP-compatible mode are based on MSTP protocol conversion mechanism. If one port of the switch receives BPDU in compatible mode, the port automatically changes to the mode and sends BPDU in compatible mode. To resume the port to standard MST mode, you can run **spanning-tree mstp migration-check**.

In global configuration mode, run the following commands to enable or disable the MST-compatible mode:

Command	Purpose
spanning-tree mstp mst-compatible	Enable the MST-compatible mode of the switch.
no spanning-tree mstp mst-compatible	Disable the MST-compatible mode of the switch.

NOTE:

1. The main function of the compatible mode is to create the MST area for switches and other MSTP-running switches. In actual networking, make sure that the switch has the same configuration name and the same edit number. It is recommended to configure switches running other MSTP protocols to the CIST root, ensuring that the switch enters the compatible mode by receiving message.
2. If the MST-compatible mode is not activated, the switch will not resolve the whole BPDU-compatible content and take the content as the common RSTP BPDU. In this way, the switch cannot be in the same area with the MST-compatible switch that it connects.
3. A port in compatible mode cannot automatically resumes to send standard MST BPDU even if the compatible mode is shut down in global configuration mode. In this case, run migration-check.

33.3.15 Restarting Protocol Conversion Check

MSTP allows the switch to work with the traditional STP switch through protocol conversion mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message. At the same time, the port that receives the STP information is then considered as a boundary port.

NOTE: When a port is in the STP-compatible state, the port will not automatically resume to the MSTP state even if the port does not receive the STP message any more. In this case, you can run **spanning-tree mstp migration-check** to clear the STP message that the port learned, and make the port to return to the MSTP state.

The switch that runs the RSTP protocol can identify and handle the MSTP message. Therefore, the MSTP switch does not require protocol conversion when it works with the RSTP switch.

In global configuration mode, run the following command to clear all STP information that is detected by all ports of the switch:

Command	Purpose
spanning-tree mstp migration-check	Clears all STP information that is detected by all ports of the switch.

In port configuration mode, run the following command to clear STP information detected by the port.

Command	Purpose
spanning-tree mstp migration-check	Clears STP information detected by the port.

33.3.16 Configuring Port's Role Restriction

The function of configuring port's role restriction could make the port not be selected as root port.
Use the following command to configure port's role restriction under port configuration mode:

Command	Purpose
spanning-tree mstp restricted-role	Making the port not be selected as root port

33.3.17 Configuring Port's TCN Restriction

The configuration of port's TCN restriction could make port do not spread topology change to other ports.
Use the following command to configure port's TCN restriction under port configuration mode:

Command	Purpose
spanning-tree mstp restricted-tcn	Making port do not spread topology change to other ports.

33.3.18 Checking MSTP Information

In monitor command, global configuration command or port configuration command, run the following command to check all information about MSTP.

Command	Purpose
show spanning-tree	Checks MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree detail	Checks the details of MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree interface *interface-id*	Checks the STP interface information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree mstp	Checks all MST instances.
show spanning-tree mstp region	Checks the MST area configuration.
show spanning-tree mstp instance *instance-id*	Checks information about a MST instance.
show spanning-tree mstp detail	Checks detailed MST information.
show spanning-tree mstp interface *interface-id*	Checks MST port configuration.

show spanning-tree mstp protocol-migration	Checks the protocol conversion state of the port.

Chapter 34 Configuring STP Optional Characteristic

34.1 STP Optional Characteristic Introduction

The spanning tree protocol module of the switch supports seven additional features (the so-called optional features). These features are not configured by default. The supported condition of various spanning tree protocol modes towards the optional characteristics is as follows:

Optional Characteristic	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	Yes	Yes
BPDU Filter	Yes	Yes	No	No
Uplink Fast	Yes	Yes	No	No
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	Yes	Yes
Loop Guard	Yes	Yes	Yes	Yes

34.1.1 Port Fast

Port Fast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. You can use Port Fast on interfaces connected to a single workstation or server, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An interface with Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted. If Port Fast is configured on a Port connected to a switch, it is possible to create a loop.

The Port Fast feature can be set in either global or Port configuration mode. If configured in global mode, all ports will be considered as Port Fast ports and will quickly enter the Forwarding state. It's also easier to create loops. To prevent network loops from being created by configuring the Port Fast function, you can use the BPDU Guard or BPDU Filter features to protect the ports.

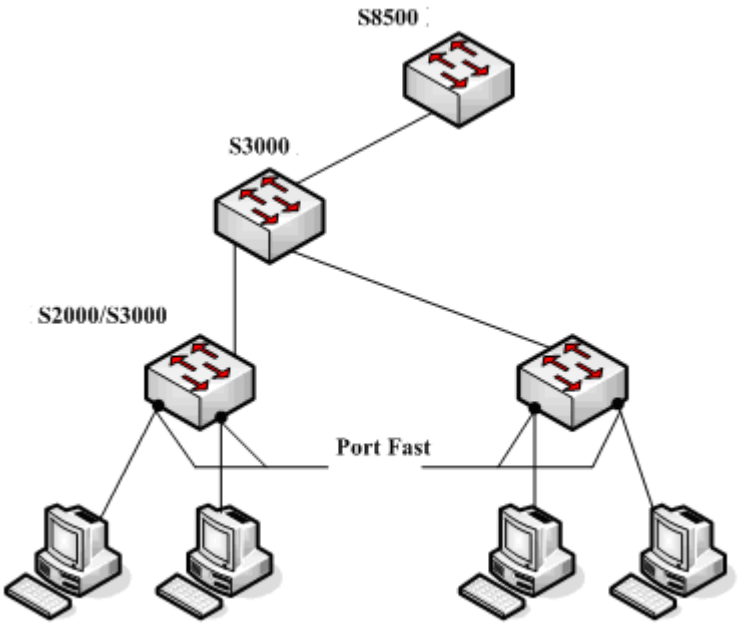


Figure 34-1 Port Fast

NOTE:

For the rapid convergent spanning tree protocol, RSTP and MSTP, can immediately bring an interface to the forwarding state, and therefore there is no need to use Port Fast feature.

34.1.2 BPDU Guard

If a Port Fast-enabled port receives a BPDU, it can be attributed to a bad network configuration. The BPDU Guard feature passively protects the port after it receives a BPDU.

BPDU Guard behaves differently under different spanning tree protocols. In SSTP/PVST mode, a Port Fast-enabled port that is also configured with the BPDU Guard is forced to shutdown once receiving the BPDU, after which the user can only manually configure it to recover. In RSTP/MSTP mode, a normal port configured with BPDU Guard will be set to a Blocking state for a period of time if it receives a BPDU.

The BPDU Guard feature can be configured independently without Port Fast. In all spanning tree protocol modes, a port configured with the BPDU Guard feature will still send the BPDU, and also receive and process the BPDU. In RSTP/MSTP mode, configuring the BPDU Guard on the port can prevent these devices connected to the switch from receiving BPDU.

The BPDU Guard feature can be configured in global or port mode. In global mode, using the **spanning tree portfast bpduguard** command will not prevent a port from sending BPDU. It is important to note that in a more complex network, improper use of the BPDU Guard function can result in loops.

34.1.3 BPDU Filter

The BPDU filtering feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

In SSTP/PVST mode, if a **Port Fast** port with BPDU filter configured receives the BPDU, the features BPDU Filter and Port Fast at the port will be automatically disabled, resuming the port as a normal port. Before entering the **Forwarding** state,

the port must be in the **Listening** state and **Learning** state.

The BPDU Filter feature can be configured in global configuration mode or in port configuration mode. In global configuration mode, run the command **spanning-tree portfast bpdufilter** to block all ports to send BPDU out. The port, however, can still receive and process BPDU.

34.1.4 Uplink Fast

The feature **Uplink Fast** enables new root ports to rapidly enter the **Forwarding** state when the connection between the switch and the root bridge is disconnected.

A complex network always contains multiple layers of devices, as shown in figure 34.2. Both aggregation layer and the access layer of the switch have redundancy connections with the upper layer. These redundancy connections are normally blocked by the STP to avoid loops.

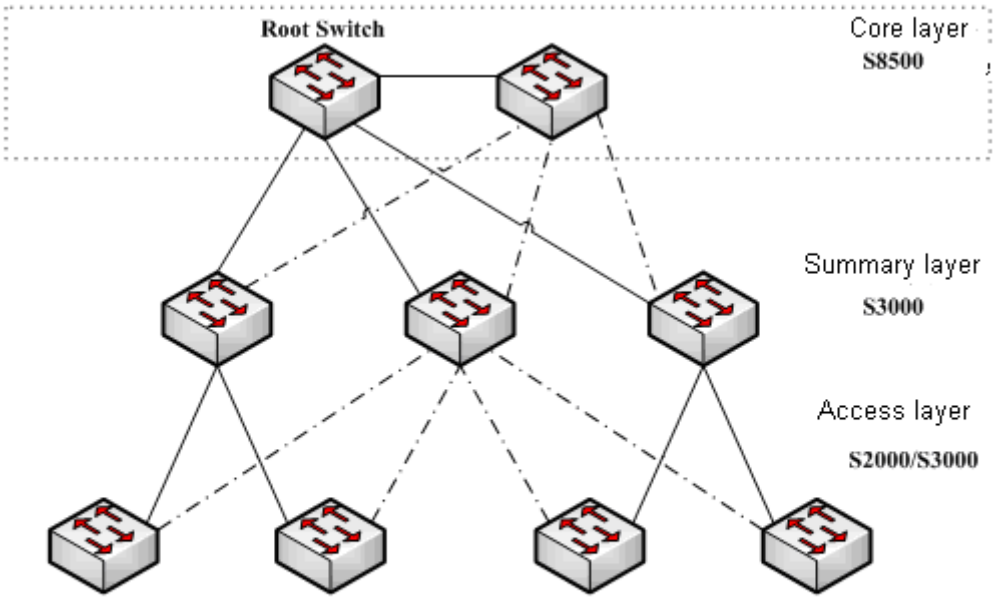


Figure 34-2 Switching network topology

Suppose the connection between a switch and the upper layer is disconnected (called as Direct Link Failure), the STP chooses the Alternate port on the redundancy line as the root port. Before entering the **Forwarding** state, the Alternate port must be in the **Listening** state and **Learning** state. If the **Uplink Fast** feature is configured by running the command **spanning-tree uplinkfast** in global configuration mode, new root port can directly enter the forwarding state, resuming the connection between the switch and the upper layer.

Figure 34.3 shows the working principle of the **Uplink Fast** feature. The port for switch C to connect switch B is the standby port when the port is in the original state. When the connection between switch C and root switch A is disconnected, the previous **Alternate** port is selected as new root port and immediately starts forwarding.

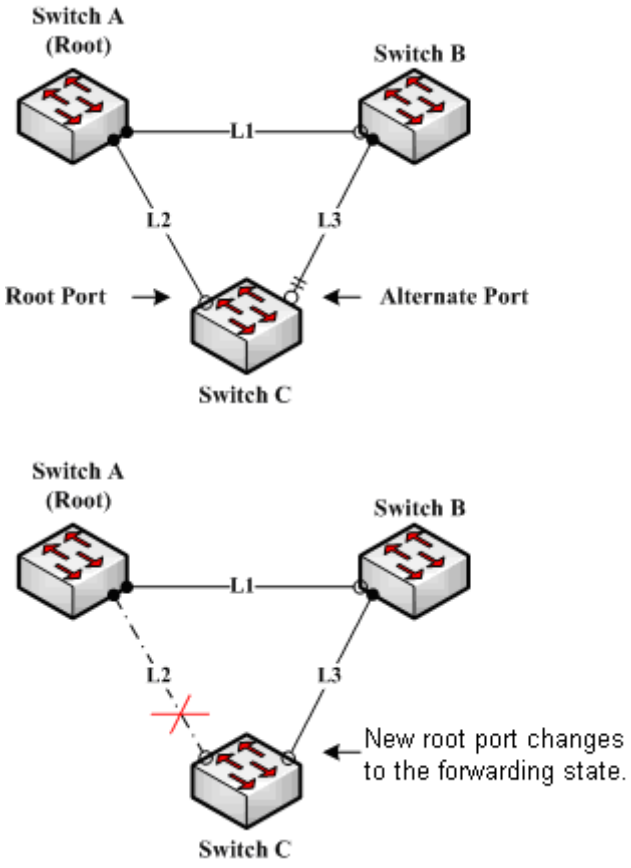


Figure 34-3 Uplink Fast

NOTE:

The Uplink Fast feature adjusts to the slowly convergent SSTP and PVST. In RSTP and MSTP mode, new root port can rapidly enter the Forwarding state without the Uplink Fast function.

34.1.5 Backbone Fast

The **Backbone Fast** feature is a supplement of the **Uplink Fast** technology. The **Uplink Fast** technology makes the redundancy line rapidly work in case the direct connection to the designated switch is disconnected, while the **Backbone Fast** technology detects the indirect-link network blackout in the upper-layer network and boosts the change of the port state.

In figure 34.3, Connection L2 between switch C and switch A is called as the direct link between switch C and root switch A. If the connection is disconnected, the **Uplink Fast** function can solve the problem. Connection L1 between switches A and B is called as the indirect link of switch C. The disconnected indirect link is called as indirect failure, which is handled by the **Backbone Fast** function.

The working principle of the Backbone Fast function is shown in Figure 34.4.

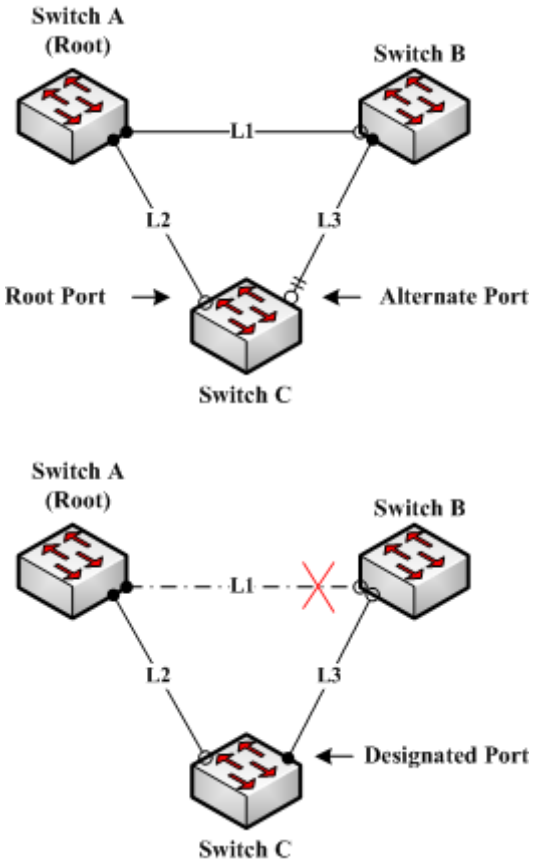


Figure 34-4 Backbone Fast

Suppose the bridge priority of switch C is higher than that of switch B. When L1 is disconnected, switch B is selected to send BPDU to switch C because the bridge priority is used as root priority. To switch C, the information contained by BPDU is not prior to information contained by its own. When Backbone Fast is not enabled, the port between switch C and switch B ages when awaiting the bridge information and then turns to be the designated port. The aging normally takes a few seconds. After the function is configured in global configuration mode by running the command **spanning-tree backbonefast**, when the Alternate port of switch C receives a BPDU with lower priority, switch C thinks that an indirect-link and root-switch-reachable connection on the port is disconnected. Switch C then promptly update the port as the designated port without waiting the aging information.

After the Backbone Fast function is enabled, if BPDU with low priority is received at different ports, the switch will perform different actions. If the Alternate port receives the message, the port is updated to the designated port. If the root port receives the low-priority message and there is no other standby port, the switch turns to be the root switch.

Note that the Backbone Fast feature just omits the time of information aging. New designated port still needs to follow the state change order: the listening state, then the learning state and finally the forwarding state.

NOTE: Similar to Uplink Fast, the Backbone Fast feature is effective in SSTP and PVST modes.

34.1.6 Root Guard

The Root Guard feature prevents a port from turning into a root port because of receiving high-priority BPDU.

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch, as shown in

Figure 17-8. You can avoid this situation by enabling root guard on SP switch interfaces that connect to switches in your customer's network. If spanning-tree calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface in the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root.

If a switch outside the SP network becomes the root switch, the interface is blocked (root-inconsistent state), and spanning tree selects a new root switch. The customer's switch does not become the root switch and is not in the path to the root.

If the switch is operating in multiple spanning-tree (MST) modes, root guard forces the interface to be a designated port. If a boundary port is blocked in an internal spanning-tree (IST) instance because of root guard, the interface also is blocked in all MST instances. A boundary port is an interface that connects to a LAN, the designated switch of which is either an IEEE 802.1D switch or a switch with a different MST region configuration.

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. VLANs can be grouped and mapped to an MST instance.

You can enable this feature by using the spanning-tree guard root interface configuration command.

NOTE: Root Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won't be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

34.1.7 Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is enabled on the entire switched network. Loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

You can enable this feature by using the **spanning-tree loopguard default** global configuration command.

When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if loop guard in all MST instances blocks the interface. On a boundary port, loop guard blocks the interface in all MST instances.

NOTE:

Loop Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, the designated port is always be blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. Loop Guard will not block a port, which is provided with the designated role due to receiving the lower level BPDU.

34.2 Configuring STP Optional Characteristic

34.2.1 STP Optional Characteristic Configuration Task

- Configuring Port Fast
- Configuring BPDU Guard
- Configuring BPDU Filter
- Configuring Uplink Fast
- Configuring Backbone Fast
- Configuring Root Guard
- Configuring Loop Guard

- Configuring Port Fast
- Configuring Address Table Aging Protection
- Configuring Port Fast
- Configuring Port FastBPDU Terminal

34.2.2 Configuring Port Fast

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting for the standard forward-time delay. This function is not valid in other spanning tree modes.
Use the following command to configure the port fast feature in the global configuration mode:

Command	Purpose
spanning-tree port fast default	Globally enables port fast feature. It is valid to all interfaces.
no spanning-tree portfast default	Globally disables port fast feature. It has no effect on the interface configuration.

NOTE:
The port fast feature only applies to the interface that connects to the host. The BPDU Guard or BPDU Filter must be configured at the same time when the port fast feature is configured globally.
Use the following command to configure the port fast feature in the interface configuration mode:

Command	Purpose
spanning-tree portfast	Enables port fast feature on the interface.
no spanning-tree portfast	Disables port fast feature on the interface. It has no effect on the global configuration.

34.2.3 Configuring BPDU Guard

The BPDU Guard feature passively protects the port after it receives a BPDU, and the port still send BPDU.
BPDU Guard behaves differently under different spanning tree protocols. In SSTP/PVST mode, a Port Fast-enabled port that is also configured with the BPDU Guard is forced to shut down once receiving the BPDU, after which the user can only manually configure it to recover. In RSTP/MSTP mode, a normal port configured with BPDU Guard will be set to a Blocking state for a period of time if it receives a BPDU.
Follow these steps to globally enable the BPDU guard feature:

Command	Purpose
spanning-tree portfast bpduguard	Globally enables bpdu guard feature. It is valid to all interfaces.
no spanning-tree portfast bpduguard	Globally disables bpdu guard feature.

Instruction: Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Follow these steps to enable the BPDU guard feature in interface configuration mode:

Command	Purpose
spanning-tree bpduguard enable	Enables bpdu guard feature on the interface.
spanning-tree bpduguard disable	Disables bpdu guard feature on the interface. It has no effect on the global configuration.
no spanning-tree bpduguard	Disables bpdu guard feature on the interface. It has no effect on the global configuration.

34.2.4 Configuring BPDU Filter

You should enable BPDU filtering in SSTP/PVST mode so that the interface do not send BPDUs, which is also another protection method for the Port Fast port.

Follow these steps to globally enable the BPDU filter feature.:

Command	Purpose
spanning-tree portfast bpdufilter	Globally enables bpdu filter feature. It is valid to all interfaces.
no spanning-tree portfast bpdufilter	Globally disables bpdu filter feature.

Instruction: Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Follow these steps to enable the BPDU filter feature in the interface configuration mode :

Command	Purpose
spanning-tree bpdufilter enable	Enables bpdu filter feature on the interface.
spanning-tree bpdufilter disable	Disables bpdu filter feature. It has no effect on the global configuration.
no spanning-tree bpdufilter	Disables bpdu filter feature. It has no influence on the global configuration.

34.2.5 Configuring Uplink Fast

The Uplink Fast feature enables the new root port to quickly enter the Forwarding state when the connection between the switch and the network root bridge is interrupted.

Uplink Fast feature is only valid in SSTP/PVST mode.

Follow these steps to globally enable UplinkFast.:

Command	Purpose
spanning-tree uplinkfast	Enables uplink fast feature.
no spanning-tree uplinkfast	Disables uplink fast feature.

34.2.6 Configuring Backbone Fast

Backbone Fast feature is complementary to Uplink Fast technology. Uplink Fast enables redundant lines to start working quickly when the direct connection to the designated switch is interrupted. Backbone Fast can detect non-directly-connected network interruptions in the upper-layer network and speed up port status changes

Backbone fast feature is only valid in SSTP/PVST mode.

Follow these steps to globally enable BackboneFast.:

Command	Purpose
spanning-tree backbonefast	Enables backbone fast feature.
no spanning-tree backbonefast	Disables backbone fast feature.

34.2.7 Configuring Root Guard

Root Guard feature can prevent a port with a high-priority BPDU from becoming a Root port.

Root Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won't be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

Follow these steps to enable root guard on an interface:

Command	Purpose
spanning-tree guard root	Enables root guard feature on the interface.
no spanning-tree guard	Disables root guard and loop guard features on the interface.
spanning-tree guard none	Disables root guard and loop guard features on the interface.

34.2.8 Configuring Loop Guard

The Loop Guard feature protects a Root Port or Alternate Port after it becomes a Designated Port. It prevents the port from loops caused by not receiving BPDUs.

Loop Guard feature acts differently somehow in SSTP/PVST. In SSTP/PVST mode, the designated port is always blocked by Loop Guard. In RSTP/MSTP, the designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. A port which is provided with the designated role due to receiving the lower level BPDU will not be blocked by Loop Guard.

Follow these steps to enable loop guard in global configuration mode:

Command	Purpose
spanning-tree loopguard default	Globally enables loop guard feature. It is valid to all interfaces.
no spanning-tree loopguard default	Globally disables loop guard.

Follow these steps to enable loop guard in the interface configuration mode:

Command	Purpose
spanning-tree guard loop	Enables loop guard feature on the interface.
no spanning-tree guard	Disables root guard and loop guard feature on the interface.
spanning-tree guard none	Disables root guard and loop guard on the interface.

34.2.9 Configuring Loop Fast

NOTE: Please use this chapter's configuration command under the technical engineer's instruction.

Loop Fast feature is applied to improve network's convergence performance limitedly under special network environment. For example, this feature is enabled on every port which composes the ring network which is made up of dozens of switches.

Use the following command to configure Loop Fast on all ports under global configuration mode:

Command	Purpose
spanning-tree loopfast	Enabling Loop Fast feature for all ports under global configuration mode
no spanning-tree loopfast	Shutting down Loop Fast under global configuration mode

Use the following commands to configure Loop Fast under port configuration mode:

Command	Purpose
spanning-tree loopfast	Enabling port's Loop Fast Feature
no spanning-tree loopfast	Cancelling all port's Loop Fast Configuration. If configuring global Loop Fast, the feature is still valid on ports.
spanning-tree loopfast disable	Disabling port's Loop Fast

34.2.10 Configuring Address Table Aging Protection

Under the condition of network topology's frequent change, configuring address table aging protection could avoid communication impacted because spanning tree protocol updates MAC address table frequently.
Spanning tree protocol with Fast convergence, like RSTP and MSTP, when detects the change of spanning tree's topology, would do elimination operation on switch's MAC address table, which is deleting old MAC address and accelerating MAC address's update to guarantee the communication could recover rapidly. Under default configuration, XXCOM switch finishes elimination operation by the way of MAC address table's fast aging. For most models of switches, address table's fast aging could finish in one second and have rare effect on CPU's function.
After address table's aging protection function is enabled, STP protocol would initiate timer protection after the first aging. Before timer is overtime (default is 15 seconds), aging would not be processed. If network topology changes within 15 seconds, the protocol would operate the second aging after timer is overtime.

NOTE: STP protocol executive address's aging could be disabled completely by the command **no spanning-tree fast-aging.** Before operating this configuration, please confirm network does not have loop. Otherwise, after network topology changes, terminal devices might need 5 minutes or longer time to regain communication with each other.

Use the following commands to configure address table's aging protection function under global configuration mode:

Command	Purpose
spanning-tree fast-aging	Enabling/disabling address table's aging function.
spanning-tree fast-aging protection	Enabling/disabling address table's aging protection function.
spanning-tree fast-aging protection time	Configuring address table's aging protection time. Within the time, spanning tree can only execute one time of address table's aging. The default is 15 seconds.

Adding no on the above commands can disable the relative configuration.

34.2.11 Configuring FDB-Flush

NOTE: Please use this chapter's configuration command under XXCOM technical engineer's instruction.

XXCOM Switch's rapid spanning tree protocol (RSTP and MSTP) eliminates old MAC address by using the address table's fast aging method not FDB-Flush way under default configuration.
Use the following commands to configure FDB-Flush under global configuration mode:

Command	Purpose
spanning-tree fast-aging flush-fdb	Enabling FDB-Flush
no spanning-tree fast-aging flush-fdb	Disabling FDB-Flush

To be noticed is that FDB-Flush is independent with fast aging function. FDB-Flush could be configured when configuring **no spanning-tree fast-aging.** But fast aging protection function is not valid for FDB-Flush.

34.2.12 Configuring BPDU Terminal

By default, XXCOM's switch will forward the BPDU received when no spanning tree is running. The BPDU Terminal function can disable the forwarding of BPDU when no spanning tree is running.
Use the following commands to configure BPDU Terminal under global configuration mode:

Command	Purpose
spanning-tree bpdu-terminal	Enabling BPDU Terminal.
no spanning-tree bpdu-terminal	Disabling BPDU Terminal.

Chapter 35 Configuring Port Aggregation

The port aggregation configuration task in this chapter describes how to configure port aggregation for the switch.

35.1 Overview

Port aggregation means that several physical ports with the same attributes are bound together to form a logical channel. The port aggregation method can be to statically aggregate several physical ports together regardless of whether the ports connected to these physical ports meet the conditions for aggregation. When using LACP for aggregation, after the port aggregation negotiate with the port and the opposite port, the port can be aggregated into a logical channel.

Supported Features:

- Static aggregation control is supported

Bind a physical port to a logical port, regardless whether they can actually bind to a logical port.

- Aggregation control of LACP dynamic negotiation is supported

When a physical port is configured to bind to a logical port, the physical port with LACP negotiation can be bound to a logical port. Other ports cannot be bound to the logical port.

- Flow balance of port aggregation is supported.

After port aggregation, the data flow of the aggregation port will be distributed to each aggregated physical port.

35.2 Port Aggregation Configuration Task List

- Configuring logical channel used for aggregation
- Aggregation of physical port
- Selecting load balance mode after port aggregation
- Monitoring the concrete condition of port aggregation

35.3 Port Aggregation Configuration Task

35.3.1 Configuring Logical Channel Used to Aggregation

You should establish a logical port before binding all the physical ports together. The logical port is used to control the channel formed by these binding physical ports.

Use the following command to configure the logical channel:

Command	Description
interface port-aggregator id	Configures aggregated logical channel.

35.3.2 Aggregation of Physical Port

To aggregate multiple physical ports into a logical channel, you can use static aggregation or LACP protocol for negotiation.

In the case when the static aggregation is used, it is required that the link of the physical port should be up, and the VLAN attribute of aggregation port and physical port should be identical, and then this port will be aggregated to the logical channel, regardless of whether the current port accords with the conditions of port aggregation and whether the port that connects with the physical port accords with the aggregation conditions.

With the LACP protocol, port aggregation must be performed after the peer connected to the port and the port have been negotiated through. The link of the port must be up and the port should be negotiated to full-duplex mode. The speed of all physical ports should be same during aggregation process, that is, if there is one physical port that has been aggregated successfully, then the speed of the second physical port must be the same as the first configured one. Also the vlan attributes of all physical ports must be identical to the aggregated port.

LACP provides two aggregation methods, one is Active and the other is Passive. In Active mode, the switch actively initiates the aggregation negotiation process, while In Passive mode, The switch passively accepts the aggregation negotiation process. If both ports use Passive method, then the aggregation fails. This is because both sides will wait for the other side to launch aggregation negotiation process.

VALN attributes: PVID, Trunk attribute, vlan-allowed range and vlan-untagged range.

Use the following command to perform aggregation on the physical ports:

Command	Description
aggregator-group *agg-id* mode { lacp | static }	Configures aggregation option of the physical port.

35.3.3 Selecting Load Balance Method After Port Aggregation

You can select the load share method to ensure that all ports can share the data traffic after the aggregation of all physical ports. The switch can provides up to six load balance strategy:

- src-mac

It is to share the data traffic according to the source MAC address, that is, the message with same MAC address attributes is to get through a physical port.

- dst-mac

It is to share the data traffic according to the destination MAC address, that is, the message with same MAC address attributes is to get through a physical port.

- both-mac

It is to share the data traffic according to source and destination MAC addresses, that is, the message with same MAC address attributes is to get through a physical port.

- src-ip

It is to share the data traffic according to the source IP address, that is, the message with same IP address attributes is to get through a physical port.

- dst-ip

It is to share the data traffic according to the destination IP address, that is, the message with same IP address attributes is to get through a physical port.

- both-ip

It is to share the data traffic according to the destination and source IP addresses, that is, the message with same IP address attributes is to get through a physical port.

Use the following command to configure load balance method:

Command	Description
aggregator-group load-balance	Configures load balance method.

35.3.4 Monitoring the Concrete Conditions of Port Aggregation

Use the following command to monitor port aggregation state in EXEC mode:

Command	Description
show aggregator-group [id] {detail|brief|summary}	Displays port aggregation state.

Chapter 36 PDP Overview

36.1 Overview

PDP is specially used to discover network equipment, that is, it is used to find all neighbors of a known device. Through PDP, the network management program can use SNMP to query neighboring devices to acquire network topology.
Our company's switches can discover the neighboring devices but they do not accept SNMP queries. Therefore, switches only run at the edge of network, or they cannot acquire a complete network topology.
PDP can be set on all SNAPs (e.g. Ethernet).

36.2 PDP Configuration Tasks

- Default PDP Configuration
- Setting the PDP Clock and Information Storage
- Setting the PDP Version
- Starting PDP on a Switch
- Starting PDP on a Port
- PDP Monitoring and Management

36.2.1 Default PDP Configuration

Function	Default Settings
Global configuration mode	This function is not enabled by default.
Interface configuration mode	Starts up.
PDP clock (packet transmission frequency)	60 seconds
PDP information storage	180 seconds
PDP version	2

36.2.2 Setting the PDP Clock and Information Storage

To set the PDP packet transmission frequency and the PDP information storage time, you can run the following commands in global configuration mode.

Command	Purpose
pdp timer seconds	Sets the transmission frequency of the PDP packets.
pdp holdtime seconds	Sets the PDP information storage time.

36.2.3 Setting the PDP Version

To set the PDP version, you can run the following command in global configuration mode.

Command	Purpose
pdp version {1|2}	Setts the PDP version.

36.2.4 Starting PDP on a Switch

To enable PDP, you can run the following commands in global configuration mode.

Command	Purpose
pdp run	Starts PDP on a switch.

36.2.5 Starting PDP on a Port

To enable PDP on a port by default, you can run the following command in port configuration mode.

Command	Purpose
pdp enable	Starts PDP on a port of a switch.

36.2.6 PDP Monitoring and Management

To monitor the PDP, run the following commands in EXEC mode:

Command	Purpose
show pdp traffic	Displays the counts of received and transmitted PDP packets.
show pdp neighbor [detail]	Displays neighbors that PDP discovers.

36.3 PDP Configuration Example

Example 1: Starting PDP

Switch_config# pdp raun

Switch_config# int g0/1

Switch_config_g0/1#pdp enable

Example 2: Setting the PDP clock and information storage

Switch_config#pdp timer 30

Switch_config#pdp holdtime 90

Example 3: Setting the PDP version

Switch_config#pdp version 1

Example 4: Monitoring PDP

Switch_config#show pdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Gig0/1	169	Gig0/1	COM, RISC	R S

Chapter 37 LLDP Overview

37.1 LLDP Overview

The link layer discovery protocol (LLDP) at 802.1AB helps to detect network troubles easily and maintain the network topology. It enables neighboring devices to send notifications of their status information to other devices, and each port of all devices stores its own defined information. If necessary, it can also send updated information to neighboring devices directly connected to them. The device will store the information in standard SNMP MIBs. The network management system can query the current connection status of the second layer from the MIB. LLDP does not configure or control network elements or traffic, it just reports the configuration of the second layer.

Simply, LLDP is a neighbor discovery protocol. It sets a standard method for the Ethernet network device, such as switches, routers and WAPs. It enables the Ethernet device notify its existence to other nodes and save the discovery information of neighboring devices. For instance, all information including the device configuration and the device identification can be notified through the protocol. Specifically, LLDP defines a universal notification information set, a transmission notification protocol and a method of storing all notification information. The device need to notify the notification information can transmit many notifications in a LAN data packet. The transmission type is TLV.

TLV has three compulsory types: Chassis ID TLV, Port ID TLV and Time To Live TLV; five optional types: Port Description, System Name, System Description, System Capabilities and Management Address; and three extension TLVs: DOT1 (Port Vlan ID, Protocol Vlan ID, Vlan Name, Protocol Identity); DOT3 (MAC/PHY Configuration/Status, Power Via MDI, Link Aggregation, Max Frame Size); MED (MED Capability, Network Policy, Location Identification, Extended Power-via-MDI, Inventory (Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Mode Name, Assert ID).

LLDP is a unidirectional protocol. One LLDP agent transmits its state information and functions through its connected MSAP, or receives the current state information or function information about the neighbor. However, the LLDP agent cannot request any information from the peer through the protocol. During message exchange, message transmission and reception do not affect each other. You can configure only message transmission or reception or both.

37.1.1 Initializing the Protocol

LLDP can work under three modes: transmit-only, receive-only and transmit-and-receive. The default mode is transmit-and-receive.

37.1.2 Initializing LLDP Transmit Mode

Set LLDP to transmit-only in the interface mode. In transmit-only mode, the interface transmits LLDP packets when the state or value of one or more information elements (management object) of the local system change or the transmission timer is timeout. The interface will not transmit LLDP packets when disabling the function.

37.1.3 Initializing LLDP Receive Mode

Set LLDP to receive-only in the interface mode. In receive-only mode, the interface can receive LLDP packets from the neighbors and save tlv into the remote MIB. The interface will drop LLDP packets when disabling the function.

37.1.4 LLDP PDU Packet Structure Description

In accordance with the order, LLDP PDU includes three compulsory TLVs in the front, one or more optional TLV in the middle and LLDPUD TLV in the end. As shown in figure 37-1:

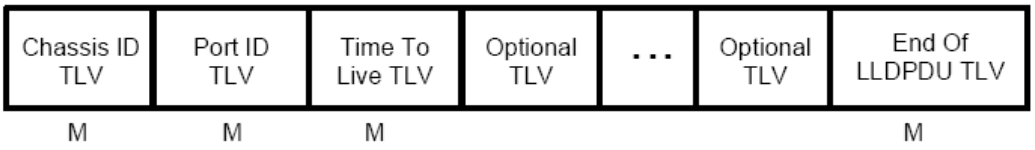


Figure 37-1 LLDP PDU Format

NOTE: M must include TLV.

- Three compulsory TLVs should be listed in sequence at the beginning of LLDP PDU:

1. Chassis ID TLV
2. Port ID TLV
3. Time To Live TLV

- Optional TLV selected by the network management can be listed randomly.

4. Port Description
5. System Name
6. System Description
7. System Capabilities
8. Management Address

Three extensions (including DOT1):

9. Port Vlan ID
10. Protocol Vlan ID
11. Vlan Name
12. Protocol Identity

DOT3:

13. MAC/PHY Configuration/Status
14. Power Via MDI
15. Link Aggregation
16. Max Frame Size

MED (TLV of MED is not transmitted by default. LLDP packets with MED TLV will be transmitted only when LLDP packets with MED TLV are received.)

17. MED Capability (TLV is compulsory if MED TLV is added.)
18. Network Policy
19. Location Identification
20. Extended Power-via-MDI
21. Inventory (including Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Mode Name or Assert ID)

- The end TLV should be the last one in LLDP PDU.

37.2 LLDP Configuration Task List

- Disabling/enabling LLDP
- Configuring Holdtime

You can configure the switch priority and make it more likely that a standalone switch or a switch in the stack will be chosen as the root switch.

Follow these steps to configure the switch priority:

Command	Purpose
spanning-tree sstp priority *value*	Modifies SSTP priority value.
no spanning-tree sstp priority	Returns SSTP priority to default value (32768).

- imer
- Configuring Reinit
- Configuring the To-Be-Sent TLV
- Configuring the Transmission or Reception Mode
- Specifying the Management IP Address of a Port
- Sending Trap Notification to mib Database
- Configuring Show-Relative Commands
- Configuring the Deletion Commands

37.3 LLDP Configuration Tasks

37.3.1 Disabling/enabling LLDP

When the LLDP is enabled, the local port periodically sends the LLDP frame out to inform the opposite end about the information of the local.

Run the following command in global configuration mode to enable LLDP:

Step	Command	Purpose
Step 1	config	Enters the global configuration mode.
Step 2	lldp run	Enables LLDP

Run the following command to disable LLDP:

Step	Command	Purpose
Step 1	config	Enters the global configuration mode.
Step 2	no lldp run	Disables LLDP

NOTE: Only when the LLDP function is enabled can the received LLDP message be processed, otherwise the LLDP frame will be forwarded directly.

37.3.2 Configuring Holdtime

Normally, the remote information stored in the MIB will be updated before aging. But the information in the MIB will also be aging because the update frame may be lost in the process of sending. To prevent this, you can set the TTL value so that update LLDP frames are sent multiple times during the aging time. You can control the timeout time of transmitting the LLDP message through modifying **holdtime**:

Run the following command in global configuration mode to configure **holdtime** of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp holdtime time	Configures the timeout time of LLDP. Range from: 0 to 65535, default 120s.

Run the following command to resume the timeout time to default:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp holdtime	Resumes the default timeout time, that is, 120 seconds.

NOTE: To ensure the former neighbor information is not lost owing to aging when receiving next LLDP frame, the timeout time should be longer than the LLDP packet transmit interval.

37.3.3 You can configure the switch priority and make it more likely that a standalone switch or a switch in the stack will be chosen as the root switch.

Follow these steps to configure the switch priority:

Command	Purpose
spanning-tree sstp priority *value*	Modifies SSTP priority value.
no spanning-tree sstp priority	Returns SSTP priority to default value (32768).

37.3.4 imer

You can control the interval of the switch to transmit message by configuring the timer of LLDP.

Run the following command in global configuration mode to configure timer of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.

Step2	lldp timer time	Configures the interval of message transmission of LLDP. The value ranges from 5 to 65534. The default time is 30 seconds.

Run the following command to resume the default interval:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp timer	Resumes the default interval, that is, 30 seconds.

37.3.5 Configuring Reinit

LLDP information is automatically sent when the status or value of one or more information elements (managed objects) in the local system changes and the transmission timer expires. Since a single information change requires the transmission of LLDP frames, a continuous series of information changes may trigger the transmission of many LLDP frames. Because only one change is reported in each frame. To avoid this situation, network management defines waiting time between two consecutive transmissions of LLDP frames. You can control the interval of the switch to continuously transmit two messages by configuring reinit of LLDP.

Run the following command in global configuration mode to configure reinit of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp reinit time	Resumes the default interval of continuously transmitting message. The value ranges from 2 to 5. The default interval value is two seconds.

Run the following command to resume the default reinit:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp reinit	Resumes the default interval of continuously transmit message, that is, 2 seconds.

37.3.6 Configuring the To-Be-Sent TLV

You can choose TLV which requires to be sent by configuring tlv-select of LLDP. By default, all TLVs are transmitted.

Run the following commands in global configuration mode to add or delete tlv of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp tlv-select management-address	Optional. Transmits the management address tlv. The management address is usually layer-3 IP address which should be easy to use.
Step3	lldp tlv-select port-description	Optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	lldp tlv-select system-capabilities	Optional. Transmits the system performance tlv. The system performance refers to the system of transmitting packets such as the switch or router.
Step5	lldp tlv-select system-description	Optional. Transmits system description tlv. The system description is consist of texts including numbers and letters. The system description should include the full name of the system, the hardware version, the software system and the network software.
Step6	lldp tlv-select system-name	Optional. Transmits system name tlv. The name of the system should be the name of the system manager, i.e. the name of the switch.

Run the following command to delete the to be transmitted tlv in the global configuration mode:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp tlv-select management-address	Optional. Transmits the management address tlv. The management address is usually layer-3 IP address which should be easy to use.
Step3	no lldp tlv-select port-description	Optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	no lldp tlv-select system-capabilities	Optional. Transmits the system performance tlv. The system performance refers to the system of transmitting packets such as the switch or router.
Step5	no lldp tlv-select system-description	Optional. Transmits the port description tlv. The port description uses number or letters for description.
Step6	no lldp tlv-select system-name	Optional. Transmits system name tlv. The name of the system should be the name of the system manager, i.e. the name of the switch.

37.3.7 Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV

Through the configuration of dot1-tlv-select/ dot3-tlv-select/ med-tlv-select of LLDP on a port, you can select expanded TLV to be sent. By default, TLV of both DOT1 and DOT3 will be transmitted while TLV of MED will not be transmitted. Run the following commands in port configuration mode to add the to-be-sent TLV:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp dot1-tlv-select port-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PVID of a port.
Step4	lldp dot1-tlv-select protocol-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	lldp dot1-tlv-select vlan-name	Optional. Sends the 802.1-defined TLV and notifies the VLAN name of a port.
Step6	Lldp dot3-tlv-select macphy-confg	Optional. Sends the 802.3-defined TLV: a) The bit rate and the communication mode (duplex) on the physical layer; b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;
Step7	lldp dot3-tlv-select power	Optional. Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.
Step8	lldp dot3-tlv-select link-aggregation	Optional. Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	lldp dot3-tlv-select max-frame-size	Optional. Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port.
Step10	lldp med-tlv-select network-policy	Optional. Sends the MED-defined TLV and the interface can effectively discover and diagnose VLAN configured error-matching flow and the attribute of layer-2 and layer-3.
Step11	lldp med-tlv-select location	Optional. Sends the MED-defined TLV and specifies the address: a) coordinate-based LCI, which is defined in IETF 3825[6];

		b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	lldp med-tlv-select power-management	Optional. Sends the MED-defined TLV and shows the information of power supply.
Step13	lldp med-tlv-select inventory	Optional. Sends the MED-defined TLV and shows the attribute of detailed inventory.
Step14	lldp dot1-tlv-select protocol-identity	Optional. Sends the 802.1-defined TLV and notifies the Protocol-identity of a port.

Run the following commands in global configuration mode to delete to-be-sent TLV:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no lldp dot1-tlv-select port-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PVID of a port.
Step4	no lldp dot1-tlv-select protocol-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	no lldp dot1-tlv-select vlan-name	Optional. Sends the 802.1-defined TLV and notifies the vlan name of a port.
Step6	no lldp dot3-tlv-select macphy-confg	Optional. Sends the 802.3-defined TLV: a) The bit rate and the communication mode (duplex) on the physical layer; b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;
Step7	no lldp dot3-tlv-select power	Optional. Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.
Step8	No lldp dot3-tlv-select link-aggregation	Optional. Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	no lldp dot3-tlv-select max-frame-size	Optional. Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port.
Step10	no lldp med-tlv-select network-policy	Optional. Sends the MED-defined TLV and the interface can effectively discover and diagnose

		VLAN configured error-matching flow and the attribute of layer-2 and layer-3.
Step11	no lldp med-tlv-select location	Optional. Sends the MED-defined TLV and specifies the address: a) coordinate-based LCI, which is defined in IETF 3825[6]; b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	no lldp med-tlv-select power-management	Optional. Sends the MED-defined TLV and shows the information of power supply.
Step13	no lldp med-tlv-select inventory	Optional. Sends the MED-defined TLV and shows the attribute of detailed inventory.
Step14	no lldp dot1-tlv-select protocol-identity	Optional. Sends the 802.1-defined TLV and cancel to notify the Protocol-identity of a port.

37.3.8 Configuring the Transmission or Reception Mode

LLDP can work under three modes: transmit-only, receive-only and transmit-and-receive.

By default, LLDP works under the transmit-and-receive mode. You can modify the working mode of LLDP through the following commands.

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no lldp transmit	Disables the transmit-only mode of the port.
Step4	no lldp receive	Disables the receive-only mode of the port.

Run the following commands in the interface configuration mode and set lldp to the transmit-and-receive mode.

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	Lldp transmit	Enables the transmit mode of the port.
Step4	Lldp receive	Enables the receive mode of the port.

NOTE: Except the above mode, the interface can also be configured to the transmit-only mode or the receive-only mode.

37.3.9 Specifying the Management IP Address of a Port

In port configuration state, you can randomly configure the management address of the port, from which the LLDP packets are transmitted. This management address should be an IP address related with this port, and only in this way the normal communication of this port can be guaranteed.
Run the following commands in port configuration mode to set the management IP address:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp management-ip A.B.C.D	Sets the management IP address of a port.

Note: Both the no lldp management-ip command can be used to resume the default management address of the port and the default management address is the IP address of the VLAN interface that corresponds to the PVID port. When the corresponding VLAN interface does not exist, the management address is 0.0.0.0.

37.3.10 Sending Trap Notification to mib Database

Run the following commands in the global configuration mode to sending trap notification to lldp mib database or ptopo mib database.

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp trap-send lldp-mib	Sends trap notification to lldp mib database.
Step3	lldp trap-send ptopo-mib	Sends trap notification to ptopo mib database.

NOTE: Both the no lldp command and the management-ip command can be used to resume the default management address of the port and the default management address is the IP address of the VLAN interface that corresponds to the PVID port. When the corresponding VLAN interface does not exist, the management address is 0.0.0.0.

37.3.11 Configuring the Location Information

The location configuration is used to determine the address of the local machine.
Run the following commands in global configuration mode to configure the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	location elin identifier id WORD	Sets the location elin information, in which id is the elin identifier number and WORD stands for the elin information, which ranges from 10 to 25 bytes.

Step3	location civic identifier id	Enters the location configuration mode.
Step4	language WORD	Sets the language
Step5	state WORD	Sets the state's (provincial) name, such as shanghai.
Step6	county WORD	Sets the name of a county.
Step7	city WORD	Sets the name of a city.
Step8	division WORD	Sets the name of a division.
Step9	neighborhood WORD	Sets the name of neighborhood.
Step10	street WORD	Sets the name of a street.
Step11	leading-street-dir WORD	Sets the direction of a main street, such as N (north).
Step12	trailing-street-suffix WORD	Sets the suffix of a small street, such as SW.
Step13	street-suffix WORD	Sets the suffix of a street, such as platz.
Step14	number WORD	Sets the street number, such as number 123.
Step15	street-number-suffix WORD	Sets the suffix of the street number, such as number 1/2 of A road.
Step16	landmark WORD	Sets the landmark, such as Colombia University.
Step17	additional-location WORD	Sets the additional location.
Step18	name WORD	Sets the information about a resident, such as Joe's haircut shop.
Step19	postal-code WORD	Sets the postal code.
Step20	building WORD	Sets the information about a building.
Step21	unit WORD	Sets the information about a unit.
Step22	floor WORD	Sets the information about a floor.
Step23	room WORD	Sets the information about a room.
Step24	type-of-place WORD	Sets the type of a place, such as office.
Step25	postal-community WORD	Sets the name of a postal office.
Step26	post-office-box WORD	Sets the name of a postal box, such as 12345.
Step27	additional-code WORD	Sets the additional code.
Step28	country WORD	Sets the name of a country.
Step29	script WORD	Sets the script.

Run the following commands in global configuration mode to delete the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no location elin identifier id	Deletes the location enlin information of elin identifier.
Step3	no location civic identifier id	Deletes the location enlin information of id, which is the number of civic identifier.
Step4	location civic identifier id	Enters the location configuration mode.
Step5	no language	Deletes the language.
Step6	no state	Deletes the state's (provincial) name, such as shanghai.
Step7	no county	Deletes the name of a county.
Step8	no city	Deletes the name of a city.
Step9	no division	Deletes the name of a division.
Step10	no neighborhood	Deletes the name of neighborhood.
Step11	no street	Deletes the name of a street.
Step12	no leading-street-dir	Deletes the direction of a main street, such as N (north).
Step13	no trailing-street-suffix	Deletes the suffix of a small street, such as SW.
Step14	no street-suffix	Deletes the suffix of a street, such as platz.
Step15	no number	Deletes the street number, such as number 123.
Step16	no street-number-suffix	Deletes the suffix of the street number, such as number 1/2 of A road.
Step17	no landmark	Deletes the landmark, such as Colombia University.
Step18	no additional-location	Deletes the additional location.
Step19	no name	Deletes the information about a resident, such as Joe's haircut shop.
Step20	no postal-code	Deletes the name of a postal office.
Step21	no building	Deletes the information about a building.
Step22	no unit	Deletes the information about a unit.
Step23	no floor	Deletes the information about a floor.
Step24	no room	Deletes the information about a room.

Step25	no type-of-place	Deletes the type of a place, such as office.
Step26	no postal-community	Deletes the name of a postal office.
Step27	no post-office-box	Deletes the name of a postal box, such as 12345.
Step28	no additional-code	Deletes the additional code.
Step29	no country	Deletes the name of a country.
Step30	no script	Deletes the script.

37.3.12 Specifying a Port to Set the Location Information

The following commands can be used to set the location information for a port and bear the location information in TLV.
Run the following commands in port configuration mode to set the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	location civic id	Sets the location information of civic id.
Step4	location elin id	Sets the location information of elin id.

Run the following commands in port configuration mode to delete the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no location civic	Deletes the location information of civic id.
Step4	no location elin	Deletes the location information of elin id.

37.3.13 Configuring Show-Relative Commands

You can observe the information about the neighbor, statistics or port state received by the LLDP module by running show-relative commands.
Run the following commands in EXEC or global configuration mode:

Command	Purpose
Show lldp errors	Displays the error information about the LLDP module.

Show lldp interface *interface-name*	Displays the information about port state, that is, the transmission mode and the reception mode.
Show lldp neighbors	Displays the abstract information about the neighbor.
Show lldp neighbors detail	Displays the detailed information about the neighbor.
Show lldp traffic	Displays all received and transmitted statistics information.
Show location elin	Displays the information of location elin.
Show location civic	Displays the information of location civic.

37.3.14 Configuring the Deletion Commands

You can delete the received neighbor lists and all statistics information by running the following command in EXEC mode. Run the following commands in EXEC mode:

Command	Purpose
clear lldp counters	Deletes all statistics data.
clear lldp table	Deletes all received neighbor information.

37.4 Configuration Examples

37.4.1 Network Environment Requirements

Configure LLDP protocol on the port connecting two switches.

37.4.2 Network Topology

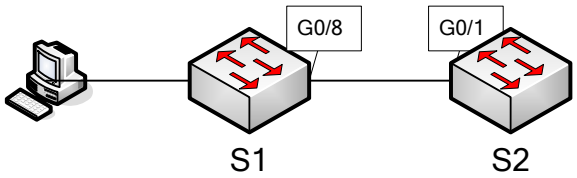


Figure 2 Network Topology

37.4.3 Configuration Steps

1. Basic Configuration

Configuring switch S1:

Switch_config#lldp run

Switch_config#

Configuring switch S2:

Switch_config#lldp run

Switch_config#

The information of Neighbor B will be displayed on Switch A about 1 minute later. MED-TLV information is not sent by default.

S1:

Switch_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gig0/8	99	Gig0/1	B

Total entries displayed: 1

Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 96

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID: 1

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Maximum frame size: 1500

Total entries displayed: 1

2. TLV Configuration

Configuring Switch S1:

Switch_config#lldp run

Switch_config#

Configuring Switch S2:

Switch_config#lldp run

Switch_config# no lldp tlv-select system-name

Switch_config#int g0/8

Switch_config_g0/8#no lldp dot1-tlv-select port-vlan-id

Switch_config_g0/8#no lldp dot3-tlv-select max-frame-size

Switch_config_g0/8#

The information of Neighbor B will be displayed on Switch A about 1 minute later, which is highlighted in red. To differentiate, the information displayed in the basic configuration of 1.4.3.1 is highlighted in blue.

S1:

Switch_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID Local-Intf Hldtme Port-ID Capability

Switch Gas0/8 92 Gig0/1 R B

Total entries displayed: 1

Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: -- not advertised

system description: XXCOM(tm) SWITCH Software, Version 4.1.0B

Serial: S24090103

Copyright by Shanghai Baud Data Communication CO. LTD.

Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 95

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID -- not advertised

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Total entries displayed: 1

3. Location Configuration

Configuring switch S1:

Switch_config#lldp run

Switch_config#

Configuring switch S2:

Switch_config#lldp run

Switch_config#location elin identifier 1 1234567890// Configure elin information

Switch_config#location civic identifier 1 // Enter location configuration mode

Switch_config_civic#language English

Switch_config_civic#city Shanghai

Switch_config_civic#street Curie

Switch_config_civic#script EN// Above configuring civic information

Switch_config_civic#quit

Switch_config#int g0/8

Switch_config_g0/8#location elin 1 //Specify elin id for the port

Switch_config_g0/8#location civic 1 // Specify civic id for the port

Switch_config_g0/8#show location elin //Display elin configuration information

elin information:

elin 1: 1234567890

total: 1

Switch_config_g0/8#show location civic // Display civic configuration information

civic address information:

identifier: 1

City: Shanghai

Language: English

Script: EN

Street: Curie

---

total: 1

Switch_config_g0/8#

The information of Neighbor B will be displayed on Switch A about 1 minute later. S1:

Switch_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gig0/8	115	Gig0/1	B

Total entries displayed: 1

Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 109

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID: 1

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

MED Information:

MED Codes:

(CA)Capabilities, (NP)Network Policy, (LI)Location Identification

(PS)Power via MDI ¨CPSE, (PD)Power via MDI ¨CPD, (IN)Inventory

Hardware Revision: 0.4.0

Software Revision: 4.1.0B

Serial Number: S24090103

Manufacturer Name:

Model Name: SWITCH

Asset ID: S24090103

Capabilities: CA,NP,LI,PS,IN

Device type: Network Connectivity

Network Policy: Voice

Policy: Unknown

Power requirements:

Type: PSE Device

Source: Unknown

Priority: Low

Value: 150(0.1 Watts)

Civic address location:

Language: English

City: Shanghai

Street: Curie

Script: EN

ELIN location:

ELIN: 1234567890

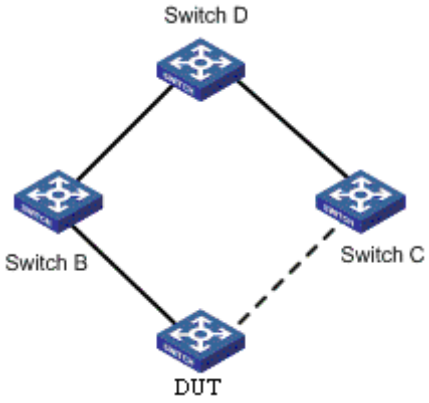
Total entries displayed: 1

Switch_config#

Chapter 38 Introduction of Backup Link

38.1 Overview

Dual-uplink networking is a common form of networking. As is shown below, DUT goes upstream to Switch D dually through Switch B and Switch C.



Dual-Uplink Networking

Although the dual-uplink networking can provide link backup, the loops in the network will cause the broadcast storms; therefore, it is necessary to take measures to avoid loops. In general, the loops can be eliminated by STP; but as the STP convergence consumes longer time, more traffic will be lost. So, STP does not apply to networking environment with higher demands for convergence time.

BackupLink provides link backup through a pair of link-layer interfaces while solving the STP problem of slow convergence. In one group of BackupLink ports, one is configured as primary port and the other as the alternate port. These ports can be exchange ports or aggregate ports. In the case that the user does not use STP protocol, BackupLink can ensure the redundancy and backup of link.

38.2 BackupLink Port Backup

38.2.1 Configuring Backup Port

For BackupLink, its basic function is to configure another switch port for one switch port as the backup; meanwhile, in two backup ports, only one port is in the forwarding state. Two backup ports can be connected with the same device or different devices.

NOTE:

1. Two ports which can backup each other may be two physical ports, two aggregate ports or one physical port and one aggregate port;
2. The backup port cannot be configured on the ports which have been configured with link aggregation, port security or EAPS or other network protections;
3. If one port has already been configured with backup, it can no longer become the backup of other ports;
4. The port which has been configured with backup cannot be configured with link aggregation, port security or EAPS or other network protection;
5. On the port which has been configured with BackupLink, the link status detection optimization of the physical layer can be enabled in order to improve the convergence performance.

38.2.2 Status Control of the Port

The ports which are configured with backup function must deleted from STP module; BackupLink is responsible for setting the status of port in all VLANs [1-4094]; these VLANs can belong to different MST (STG).

38.2.3 Port Roles and Status

Configuration commands must be able to specify the default role for two ports which backup each other: Active and Backup.

NOTE:

1. In the initial case, if the link status of Active and Backup ports is Linkup, the Active port is in the forwarding state, the Backup port is in the blocking state;
2. In the initial case, if one port is in the link status of Linkdown, the other port enters the forwarding state regardless of whether it is the Active role;
3. At one moment, the Backup port is in the forwarding state, the Active port is in the blocking state; if the backup port configuration is repeated on the port, it is necessary to force the Backup port to be in the blocking state and recover the forwarding status of Active port.

38.2.4 Link Status Change Processing

In basic port backup functions, link status changes processing must meet the following requirements:

- If the Active port is in the state of Linkdown and the Backup port is in the state of Linkdown, the link breaks, which is unable to forward the data frame;
- If the Active port is in the state of Linkdown and the Backup port is in the state of Linkup but not in the forwarding state, the Backup port enters the forwarding state;
- If the Active port is in the state of Linkup and the Backup port is in the link status of Linkdown, the Active port enters the forwarding state;
- If the Active port is in the state of Linkup and the Backup port is in the state of Linkup and in the forwarding state, the Active port is still in blocking state and the data frame is forwarded from the Backup port without enabling the preemption mode.
- If the Active port is in the state of Linkup and the Backup port is in the state of Linkup and in the forwarding state, the forwarded port and blocked port will be decided according to different strategies in the case of enabling the preemption mode. See 1.2.5.

38.2.5 Pre-emption of Backup Port

BackupLink needs to support port preemption: A and B are a pair of backup ports; Port A is in the forwarding state, Port B recovers from LinkDown state and is in blocking state; if Port B meets the conditions of preemption, Port B enters the forwarding state instead of Port A.

The port preemption must be enabled through the command; by default, the preemption is disabled.

Port preemption must be configured independently for each pair of backup ports; different backup port groups can use different preemptive modes:

- Preemption based on port role. Preemption is based on the roles specified at the time of configuring backup ports; if the Backup port in the forwarding state and the Active port is in the link status of UP, the Backup port is blocked

and the Active port is set as the forwarding state.

- Preemption based on port bandwidth. Backup ports must support the preemption of the forwarding state based on the bandwidth; the port with small bandwidth is always blocked.

NOTE:

The preemption configuration on the same group of backup ports must meet the following requirements:

1. The preemption function takes effect after it is configured on any port in the backup group; but if this configuration is deleted, the function is invalid;
2. The preemption function can be configured on two ports in the backup group, but the preemption mode and delay parameters must be consistent;
3. Two ports which are inconsistent in the preemption parameters cannot be configured as the backup ports.

Delay Preemption

For port preemption, the delay-time preemption is required: If Port B can preempt the forwarding state of Port A, the preemption is completed after the delay-time.

The delay-time preemption must be configured through the command; "0" needs to be taken as the legitimate delay-time preemption, indicating immediate preemption.

38.3 VLAN Load Balancing

BackupLink VLAN load balancing enables two ports on the BackupLink port group to simultaneously forward traffic for different VLANs. For example, the BackupLink port group is configured with the forwarding traffic of VLAN 1 ~ 100, where one port forwards the traffic of VLAN1 ~ VLAN50 while the other port forwards the traffic of VLAN51 ~ VLAN100. If one port is in the state of Linkdown, then the other port will forward all the traffic.

38.3.1 Configuration of Load balancing

VLAN load balancing is only configured on the backup port; the user specifies a set of VLAN through the command, and the backup port has the priority to enter the forwarding state in this VLAN group. Therefore, VLAN traffic sharing takes effect only after the backup function is configured on the port.

NOTE:

For different BackupLink groups, the same group VLAN can be configured, or they have overlapping VLAN segments. But for the overlapping VLAN segments, the system will assign them to different MSTs (STG); therefore, when the port of some group is operated, its states in all MSTs (STG) will take change. So, typically, when the load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

38.3.2 Port status Control in Traffic Sharing

- Create the new MST (STG) for the designated VLAN

In order to achieve the differentiated setting of port status in different VLANs, it is necessary to assign the VLAN specified by the user in the traffic sharing command to a new MST (STG).

BackupLink must check the user-specified VLAN through the interface provided by L2 module; if the specified VLAN has already been used by other protocol modules (for example, in MSTP, it is assigned to some MST, or it is configured as control VLAN of EAPS), this VLAN can no longer be used as VLAN traffic sharing. Such case needs to be handled as the user configuration error.

- The same VLAN is used by multiple backup port groups.

BackupLink must be able to handle the case that different backup port groups are configured with the same VLAN. For example: P1 and P2 are mutually backuped, and the VLAN v traffic sharing is configured on P2; P3 and P4 are mutually backuped, and VLAN v is configured on P4. At this time:

1. In the process of loading the configuration, only need to make a distribution operation of the MST in the VLAN v;
2. After the VLAN v traffic sharing is deleted from all the backup port groups, VLAN v needs to be restored to the default MST.

- Refresh port status after MST is created

The modification of the MST of VLAN may cause incorrect status of some ports in the system STG table; at this time:

1. L2 is responsible for notifying the protocol module except BackupLink of refreshing port status setting;
2. For each set of backup ports in BackupLink module, the module actively refreshes their status in all VLANs.

- Port status setting

After configuring the VLAN traffic sharing, the status setting of backup ports must comply with the following rules:

1. If two ports which are mutually backuped are in the link status of DOWN, their status in all VLANs [1-4094] is set as Blocking;
2. If only one of two ports is in the state of UP, the status of this port in all VLANs is set as Forwarding;
3. If two ports are both in the state of UP, the port which is selected as Active role is set as the Blocking state in traffic sharing VLAN and the Forwarding state in other VLANs; the port which is selected as Backup role is set as the Forwarding state in traffic sharing VLAN and the Blocking state in other VLANs.

38.4 MAC Address Aging Operation

BackupLink must support the topology change notifications for the uplink to deal with the case that loops exist in the uplink network, as is shown below:

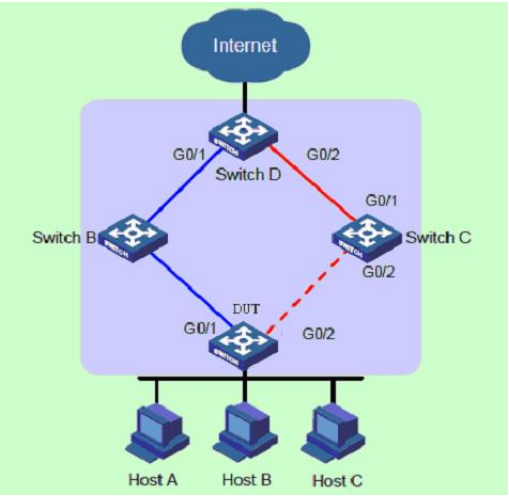


Diagram of BackupLink Address Aging Mechanism

38.4.1 Normal Work Mechanism of the Link

As is shown above, DUT port "GigaEthernet0/1" is the primary; Port "GigaEthernet0/2" is a backup port. When dual uplinks are in normal work condition, the primary port is in the forwarding state and its link is the primary link; the secondary port is blocked and its link is the secondary link. The data are transmitted along the link represented by blue line; no loop exists in the network to avoid broadcast storm.

38.4.2 Downlink Fault Handling Mechanism

When the DUT's primary link fails, the primary port "GigaEthernet0/1" is switched to the standby state, the secondary port "GigaEthernet0/2" is switched to the forwarding state. At this time, MAC address forwarding table entries and ARP table entries on the devices in the network may have been wrong, so it is necessary to provide a mechanism for MAC and ARP updating to complete the quick switch of traffic, avoiding traffic loss. Currently, there are two kinds of updating mechanism:

- Notify the device of updating table entries through the link updating packet MMU.

In this way, the upstream device (such as Switch D, Switch B and Switch C (optional) in the above figure) can support the MMU function of BackupLink and identify the situation of MMU packet. To achieve fast link switch, it is necessary to enable the MMU packet sending function on the DUT and enable MMU packet receiving and processing function on the port of upstream device on the dual uplink network.

After the DUT link switch occurs, the MMU packet will be sent from new primary link, that is, from Port "MMU GigaEthernet0/2". When the upstream device receives the MMU packet, it will judge whether the sending control VLAN of this MMU packet is in the receiving control VLAN list configured by the port receiving the packet. If it is not in the receiving control VLAN list, the device will directly forward the MMU packet without processing; if it is in the receiving control VLAN list, the device will extract the VLAN Bitmap data in the MMU packet and the MAC and ARP entries learned by the device in these VLANs are deleted.

Thereafter, if Switch D receives the data packet of DUT as the destination device, for the packet requiring the layer-2 forwarding, Switch D will forward it in the way of Layer-2 broadcasting; for the packet requiring the layer-3 forwarding, the device will first update ARP entries through using the ARP detection method and then forward the packet out. Thus, the data traffic can be transmitted correctly.

- Automatically update entries through traffic

This approach applies to the case of butting with the devices not supporting BackupLink (including other vendors' devices) under the premise that the upstream traffic is triggered.

If there is no upstream traffic from the DUT to trigger the updating of MAC and ARP entries of Switch D, when Switch D receives the data packet of DUT as the destination device, it will still forward it via the port "GigaEthernet0/1"; but the packet cannot reach the DUT, the traffic breaks until its MAC or ARP entries age automatically.

In the case that the DUT has upstream traffic to send, because MAC and ARP entries of the DUT are also wrong, the traffic will not be sent out until their entries automatically age and re-learn. When the upstream traffic reaches the device "Switch D" through the port "GigaEthernet0/2", Switch D will update its own MAC and ARP entries; then when Switch D receives the data packet of the DUT as the destination device again, Switch D will forward it out through Port "GigaEthernet0/2", and the packet can reach DUT via Switch C.

NOTE:

For the updating of the mechanism which notifies the device of updating through MMU packet, there is no need to wait until the entries age; the time of entry updating can be dramatically reduced.

38.4.3 Uplink Fault Handling Mechanism

In the networking environment shown in the above figure, the BackupLink function is used for the link redundancy backup on the DUT; GigaEthernet0/1 is the primary port; GigaEthernet0/2 is the secondary port. When the primary link where the port "GigaEthernet0/1" is faulty, the traffic is switched to the the secondary link where the port "GigaEthernet0/2" is in the period of milliseconds, achieving the efficient and reliable link backup and fast convergence performance.

However, when the link where the uplink port "GigaEthernet0/1" of Switch B is fails, for the device "DUT" configuring the

BackupLink group, as the link where its primary port GigaEthernet0/1 is is not faulty, the link switch in the BackupLink group will not occur at this time. But in fact, the traffic on the DUT cannot uplink to Switch D through the link of the port "GigaEthernet0/1", so the traffic is interrupted. To solve this problem, BackupLink must support the "MonitorLink" mechanism which changes the local link based on the uplink topology changes. "MonitorLink" is used to monitor the uplink to achieve the purpose of making the downlink synchronize with the uplink, improving the backup role of BackupLink.

- Introduction of MonitorLink Concepts

MonitorLink group is composed of one or more upstream and downstream ports. The status of downstream port varies with the change of uplink port status.

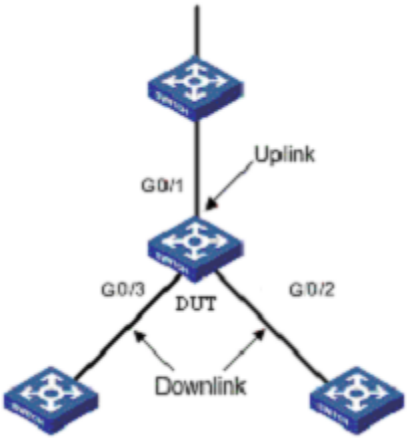


Diagram of MonitorLink Group Concepts Introduction

As is shown above, three ports of DUT (GigaEthernet0/1, GigaEthernet0/2 and GigaEthernet0/3) form a MonitorLink group.

"Uplink Port" is a monitored object in MonitorLink group, which is a port role of the MonitorLink group specified through the command line. The Uplink port of MonitorLink group can be an Ethernet port (electrical or optical), or aggregate interface. As is shown in Figure 3.3, GigaEthernet 1/ 1, a port of the DUT, is the uplink port of MonitorLink group configured on the device. When the uplink port of MonitorLink group fails, the MonitorLink group is in the status of DOWN and all the downlink ports will be closed. When the uplink port of MonitorLink group is not specified, then it is considered that the uplink port fails and that all the downlink ports will be closed.

"Downlink Port" is a monitor in MonitorLink group, which is another port role of the MonitorLink group specified through the command line. The downlink port of MonitorLink group can be an Ethernet port (electrical or optical), or aggregate interface. As is shown in the above figure, two ports of the DUT, GigaEthernet0/2 and GigaEthernet0/3, are two downlink ports of MonitorLink group configured on the device.

- MonitorLink operating mechanism

In the networking environment shown below, BackupLink group is configured on the DUT in order to achieve reliable access to the Internet from the host. GigaEthernet0/1 as the primary port is in the forwarding state; GigaEthernet0/2 is the secondary port.

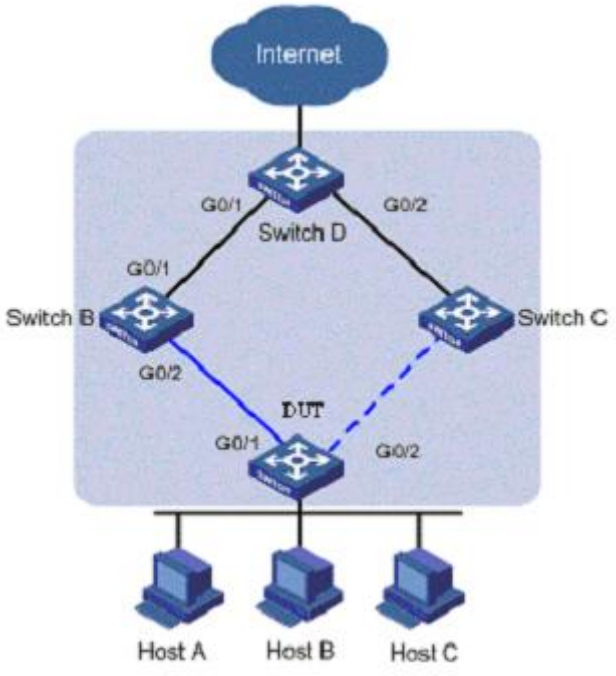


Diagram of MonitorLink operating mechanism

In order to prevent the phenomenon that DUT traffic cannot uplink because of the failure of the link where the port of Switch B, "GigaEthernet 1/ 1", is, MonitorLink group is configured on Switch B, and the port "GigaEthernet0/1" is specified as the uplink port and "GigaEthernet0/2" is specified as downlink port.

When the link where the uplink port of Switch B, GigaEthernet0/1, is fails, MonitorLink group will forcibly shut down this group's downlink port "GigaEthernet0/2", triggering the link switch of BackupLink group on the DUT.

When the link where the uplink port of Switch B, GigaEthernet0/1, is recovers from the failure, the downlink port "GigaEthernet0/2" will also be enabled; if BackupLink group on the DUT is configured as role preemption mode, similarly, the link switch of BackupLink group on the DUT will be triggered; otherwise, it is necessary to wait for the next link switch. Thus, the combination of MonitorLink technology with BackupLink technology enables efficient and reliable link backup and fast convergence performance.

38.4.4 Link Recovery Processing Mechanism

BackupLink group supports two modes: non-role preemption mode and role preemption mode. Link recovery mechanism is different in different modes. For the non-role preemption mode, please see 38.2.4; for the role preemption mode, please see 38.2.5.

Chapter 39 BackupLink Configuration

39.1 Guidance Notes for BackupLink Configuration

Before configuring BackupLink protocol, please read the following guidance notes:

- Primary port (Ethernet port or aggregate port) can be configured with a BackupLink backup port; moreover, this backup port and primary port cannot be the same port;
- A port can only belong to one BackupLink group; a backup port can only taken as the backup port of one primary port; one primary port can not belong to other BackupLink groups;
- Any port within the BackupLink group cannot be a member of the aggregate ports. Aggregate port and physical port, physical port and physical ports, aggregate port and aggregate port can become the members of BackupLink group.
- BackupLink primary port and backup port may be different in type; they may be Fast Ethernet ports, Gigabit ports or aggregate ports, but both must have similar features. Thus, When the primary port fails, the backup port can forward its data traffic in similar way;
- VLAN load balancing and BackupLink preemption functions cannot be used simultaneously.

39.2 BackupLink Configuration Tasks

- Configuring BackupLink group
- Configuring the preemption feature for BackupLink group
- Configuring load balancing for VLAN
- Configuring the MMU feature for BackupLink group
- Configuring MonitorLink group

39.3 BackupLink Configuration

39.3.1 Configuring BackupLink Group

Configure BackupLink group according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**backup-link-group** *id*	Configure backuplink group. *Id*: backuplink group instance number.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/1#**backup-link-group** *id* **active[backup]**	Configure backuplink group port role. *Id*: backuplink group instance number.
Switch_config_g1/1#**exit**	Exit from the port configuration mode.
Switch_config#	

NOTE: Use the "no backup-link-group id" command to delete backuplink group configuration and backuplink group port configuration.

NOTE: If the backuplink group is directly configured for the port in the case that it is not established, the system will automatically create the backuplink group.

39.3.2 Configuring the Preemption Feature for BackupLink Group

Configure the preemption feature for BackupLink group according to the following steps.

Command	Purpose
Switch#config	Enter switch configuration mode.
Switch_config#**backup-link-group** *id* {**preemption-mode [forced | bandwidth] {delay** *value*}}	Configure the preemption feature for BackupLink group. *Id*: backuplink group instance number; *value*: delay-time.
Switch_config#	

NOTE: Use the "**backup-link-group** id {**preemption-mode [forced | bandwidth] {delay** value}}" command to directly create BackupLink group.

39.3.3 Configuring Load Balancing for VLAN

Configure load balancing for VLAN according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/2#**share-load vlan** *vlanmap*	Configure load balancing for VLAN. *Vlanmap*: vlan value
Switch_config_g1/2#**exit**	Exit from the port configuration mode.
Switch_config#	

NOTE: The "share-load vlan vlanmap" command is only used for backup port, that is, before the vlan load balancing, the port must be configured as a backup port.

NOTE: For different BackupLink groups, the same group VLAN can be configured, or they have overlapping VLAN segments. But after the overlapping VLAN segments are configured, the system will assign them to different MSTs (STG); therefore, when the port of some group is operated, its status in all MSTs (STG) will take change. So, typically, when the load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

39.3.4 Configuring the MMU Feature for BackupLink Group

Configure the MMU feature for BackupLink group according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/2#**backup-link-group mmu transmit [receive]**	Configure MMU sending (receiving) function.
Switch_config_g1/2#**exit**	Exit from the port configuration mode.
Switch_config#	

NOTE: The port configured as "transmit" must be the port of backuplink group, that is, it must be first configured as "active" or "backup". In the case of configuring the port with "receive" function, it is not necessary to configure the port for backuplink group.

39.3.5 Configuring MonitorLink Group

Configure MonitorLink group according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**monitor-link-group** *id*	Configure MonitorLink group. *Id*: MonitorLink group instance number.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/1#**monitor-link-group** *id* **uplink[downlink]**	Configure MonitorLink group port role. *Id*: MonitorLink group instance number.
Switch_config_g1/1#**exit**	Exit from the port configuration mode.
Switch_config#	

NOTE: Use the "no monitor-link-group id" command to delete MonitorLink group configuration and MonitorLink group port configuration.

NOTE: If the MonitorLink group port role is directly configured for the port in the case that the MonitorLink group is not established, the system will automatically create the MonitorLink group .

Chapter 40 Introduction of Fast Ethernet Ring Protection

40.1 Overview

MY COMPANYEthernet ring protection protocol is a special type of link-layer protocol specially designed for constructing the ring Ethernet topology. The Ethernet protection protocol can shut down one link in a complete ring topology, preventing the data loop from forming the broadcast storm. If a link is broken, the protocol immediately resumes the link that is previously shut down. In this way, the nodes among the ring network can communicate with each other.

The ring protection protocol and STP are both used for topology control on the link layer. STP is suitable for all kinds of complicated networks, which transmits the change of network topology hop by hop. The ring protection protocol is used for ring topology and adopts the pervasion mechanism to transmit the change of network topology. Therefore, the convergence of the ring protection protocol in the ring network is better than STP. In a sound network, the ring protection protocol can resume network communication within less than 50ms.

NOTE: EAPS supports to set a switch to be a node of multiple physical ring to construct complicated topology.

40.2 Related Concepts of Fast Ether-Ring Protection

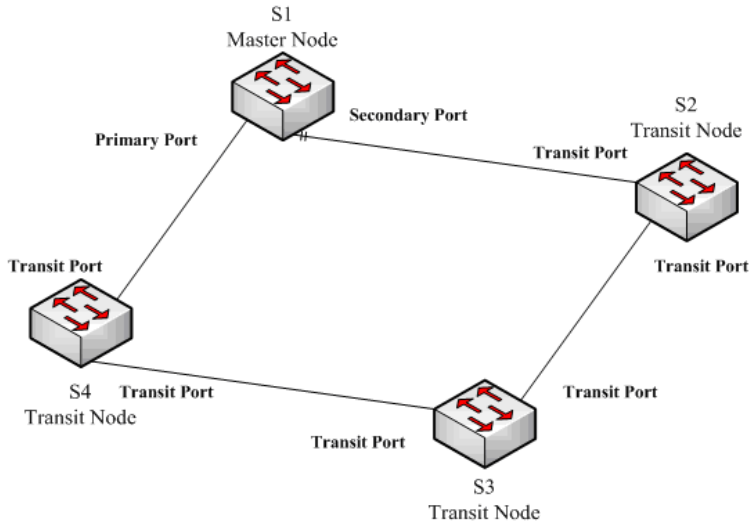


Figure 40.1 EAPS Ethernet ring

40.2.1 Roles of Ring's Nodes

Each switch on an Ethernet ring is a ring node. The ring nodes are classified into master nodes and transit nodes. Only one switch on the Ethernet ring can serve as a mere master node and other switches are worked as transit nodes.

Master node: It positively knows whether the ring's topology is complete, removes loopback, control other switches to update topology information.

Transit node: It only checks the state of the local port of the ring, and notifies the master node of the invalid link.

The role of each node can be specified by user through configuration. The thing is that each switch in the same ring can be set to only one kind of node. In figure 40.1, switch S1 is the master node of ring network, while switches S2, S3 and S4 are transit nodes.

40.2.2 Role of the Ring's Port

EAPS demands each switch has two ports to connect the ring network. Each port of the ring network also needs to be specified through configuration and the protocol supports the following kinds of port roles:

Primary port: the primary port can be configured only on the master node. The master node transmits the ring detection packets through the primary port.

Secondary port: the secondary port can be configured only on the master node. The master node receives the ring detection packets from the secondary port and judges whether the topology of the ring network is complete. In complete topology, the master node blocks the data packets on the secondary port, and prevents loopback from occurring; after a link on the ring network is interrupted, the master node will open the secondary port to forwarding the data packets.

Transit port: the transmit port can only be configured on the transit node. Both ports through which the transit node connects the ring network are all transit ports.

Each port of the ring network can be configured as only one port role after the node's role of the switch and the control VLAN are configured. As shown in figure 40.1, the port through which master node S1 connects transit node S4 is a primary port, the port through which S1 connects S2 is a secondary port, and the ports through which other switches connect the ring network are all transit ports.

NOTE: To configure a same switch to belong to multiple rings, the switch must connect different rings through different physical ports.

40.2.3 Control VLAN and Data VLAN

A private control VLAN is used between master node and transit node to transmit protocol packets. This control VLAN is specified by user through configuration and ring's ports are added also by user to the control VLAN, which guarantees that the protocol packets can be normally forwarded. In general, each port of the ring network is in the forwarding state in the control VLAN and the ports which do not belong to the ring network cannot forward the packets of control VLAN.

NOTE: You can specify different control VLAN for each ring on a switch. The control VLAN is only used to forward the control packets of the ring network, not for L2/L3 communication. For example, if the VLAN port that corresponds to the control VLAN is established, the IP address of the VLAN port cannot be pinged through other devices.

The VLANs except the control VLAN are all data VLANs, which are used to transmit the packets of normal services or the management packets.

NOTE: The data VLAN can be used for normal L2/L3 communication. For example, you can establish a VLAN port corresponding to data VLAN and configure dynamic routing protocols.

40.2.4 Aging of the MAC Address Table

The Ethernet ring protection protocol can transmit data packets to the correct link by controlling the aging of the switch's MAC address table when the topology changes. In general, the time for a MAC address to age in the MAC address table is 300 seconds. The ring protection protocol can control the aging of the MAC address table in a short time.

40.2.5 Symbol of a Complete Ring Network

Both the master node and the transit node can show whether the current ring network is complete through the state symbol "COMPLETE". On the master node, only when all links of the ring network are normal, the primary port is in forwarding state and the secondary port is in blocking state can the "COMPLETE" symbol be real; on the transit node, only when its two transit ports are in forwarding state can the "COMPLETE" symbol be true.

The state symbol of the ring network helps user to judge the topology state of the current network.

40.3 Types of EAPS Packets

The EAPS packets can be classified into the following types, as shown in table 40.1.

Type of the packet	Remarks
Loopback detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
RING-DOWN-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is detected and the packets show the MAC address aging table of the transit node.
RING-UP-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is resumed and the packets show the MAC address aging table of the transit node.

Table 40.1 Types of EAPS packets

40.4 Fast Ethernet Ring Protection Mechanism

40.4.1 Ring Detection and Control of Master Node

The master node transmits the HEALTH packets to the control VLAN through the primary port in a configurable period. In normal case, the HEALTH packets will pass through all other nodes of the ring network and finally arrive at the secondary port of the master node.

The secondary port blocks all data VLANs in primitive condition. When receiving the HEALTH packets continuously, the secondary port keeps blocking data VLANs and blocking the loop. If the secondary port does not receive the HEALTH packets from the primary port in a certain time (which can be configured), it will regard the ring network is out of effect. Then the master node removes the blocking of data VLANs on the secondary port, ages the local MAC address table, and transmits the RING-DOWN-FLUSH-FDB packets to notify other nodes.

If the master node receives the HEALTH packets at the secondary port that is open to data VLANs, the ring network is resumed. In this case, the master node immediately blocks data VLANs on the secondary port, updates the local topology information and reports other nodes to age the MAC address table through RING-UP-FLUSH-FDB packets.

You can configure related commands on the Hello-time node and the Fail-time node to modify the interval for the primary port to transmit the HEALTH packets and the time limit for the secondary port to wait for the HEALTH packets.

40.4.2 Notification of Invalid Link of Transit Node

After the transit port of the transit node is out of effect, the LINK-DOWN packet will be immediately transmitted by the other transit port to notify other nodes. In normal case, the packet passes through other transit nodes and finally arrives at one port of the master node.

After the master node receives the LINK-DOWN packet, it thinks that the ring network is invalid. In this case, the master node removes the blocking of data VLANs on its secondary port, ages the local MAC address table, transmits the RING-

DOWN-FLUSH-FDB packet and notifies other nodes.

40.4.3 Resuming the Link of the Transit Node

After the transit port is resumed, it does not immediately transmit the packets of data VLANs, but enters the Pre-Forwarding state. A transit port in pre-forwarding state only transmits and receives the control packets from the control VLAN.

If there is only one transit port invalid in the ring network and when the port enters the pre-forwarding state, the secondary port of the master node can receive the HEALTH packet from the primary port again. In this case, the master node blocks data VLANs on the secondary port again and transmits the notification of ageing address table outside. After the node with a transit port in pre-forwarding state receives the notification of aging address table, the node will first modify the pre-forwarding port to the forwarding port and then ages the local MAC address table.

If a transit mode does not receives the notification of aging address table from the master node, it thinks that the link to the master node is already out of effect, the transit node will automatically set the pre-forwarding port to be a forwarding one.

You can configure the related commands through the pre-forward-time node to modify the time for the transit port to keep the pre-forwarding state.

Chapter 41 Fast Ethernet Ring Protection Configuration

41.1 Default EAPS Settings

NOTE: The fast Ethernet protection protocol cannot be set together with STP.
After STP is disabled, you are recommended to run **spanning-tree bpdu-terminal** to keep the ring node from forwarding BPDU, which leads to the storm.

See the following table:

Spanning tree protocol	spanning-tree mode rstp
Fast Ethernet Ring Protection	There is no configuration.

Table 2.1 Default settings of the Ethernet ring protection protocol and STP.

41.2 Requisites before Configuration

Before configuring MEAPS, please read the following items carefully:

- One of important functions of the ring protection protocol is to stop the broadcast storm, so please make sure that before the ring link is reconnected all ring nodes are configured. If the ring network is connected in the case that the configuration is not finished, the broadcast storm may easily occur.
- EAPS is well compatible with STP, but the port under the control of EAPS is not subject to STP.
- The ring protection protocol supports a switch to configure multiple ring networks.
- Configuring ring control VLAN will lead to the automatic establishment of corresponding system VLAN.
- The port of each ring can forward the packets from the control VLAN of the ring, while other ports, even in the Trunk mode, cannot forward the packets from the control VLAN.
- By default, Fail-time of the master node is triple longer than Hello-time, so that packet delay is avoided from shocking the ring protection protocol. After Hello-time is modified, Fail-time need be modified accordingly.
- By default, Pre-Forward-Time of the transit node is triple longer than Hello-time of the master node so that it is ensured that the master node can detect the recovery of the ring network before the transit port enters the pre-forwarding state. If Hello-time configured on the master node is longer than Fre-Forward-Time of the transit node, loopback is easily generated and broadcast storm is then triggered.
- The physical interface, the fast-Ethernet interface, the gigabit-Ethernet interface and the aggregation interface can all be set to be the ring's interfaces. If link aggregation, 802.1X or port security has been already configured on a physical interface, the physical interface cannot be set to be a ring's interface any more. Note: The versions of MY COMPANY switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

41.3 MEAPS Configuration Tasks

- Configuring the Master Node
- Configuring the Transit Node
- Configuring the Ring Port
- Browsing the State of the Ring Protection Protocol

41.4 Fast Ethernet Ring Protection Configuration

41.4.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch#config	Enters the switch configuration mode.
Switch_config#ether-ring *id*	Sets a node and enters the node configuration mode. id: Instance ID
Switch_config_ring#control-vlan *vlan-id*	Configures the control VLAN. Vlan-id: ID of the control VLAN
Switch_config_ring#master-node	Configures the node type to be a master node.
Switch_config_ring#hello-time *value*	This step is optional. Configures the cycle for the master node to transmit the HEALTH packets. Value: It is a time value ranging from 1 to 10 seconds and the default value is 1 second.
Switch_config_ring#fail-time *value*	This step is optional. Configures the time for the secondary port to wait for the HEALTH packets. Value: It is a time value ranging from 3 to 30 seconds and the default value is 3 second.
Switch_config_ring#exit	Saves the current settings and exits the node configuration mode.

NOTE: The **no ether-ring *id*** command is used to delete the node settings and port settings of the Ethernet ring.

41.4.2 Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	Purpose
Switch#config	Enters the switch configuration mode.
Switch_config#ether-ring *id*	Sets a node and enters the node configuration mode. id: Instance ID
Switch_config_ring#control-vlan *vlan-id*	Configures the control VLAN. Vlan-id: ID of the control VLAN
Switch_config_ring#transit-node	Configures the node type to be a transit node.

Switch_config_ring#pre-forward-time *value*	This step is optional. Configures the time of maintaining the pre-forward state on the transit port. Value: It is a time value ranging from 3 to 30 seconds and the default value is 3 second.
Switch_config_ring#exit	Saves the current settings and exits the node configuration mode.

41.4.3 Configuring the Ring Port

Configure a port of a switch to be the port of Ethernet ring according to the following steps:

Command	Purpose
Switch#config	Enters the switch configuration mode.
Switch_config#interface *intf-name*	Enters the interface configuration mode. intf-name: Stands for the name of an interface.
Switch_config_intf#ether-ring *id* **{primary-port | secondary-port | transit-port }**	Configures the type of the port of Ethernet ring. ID of the node of Ethernet ring
Switch_config_intf#exit	Exits from interface configuration mode.

REMARK:

The **no ether-ring** *id* {**primary-port** | **secondary-port** | **transit-port** } command can be used to cancel the port settings of Ethernet ring.

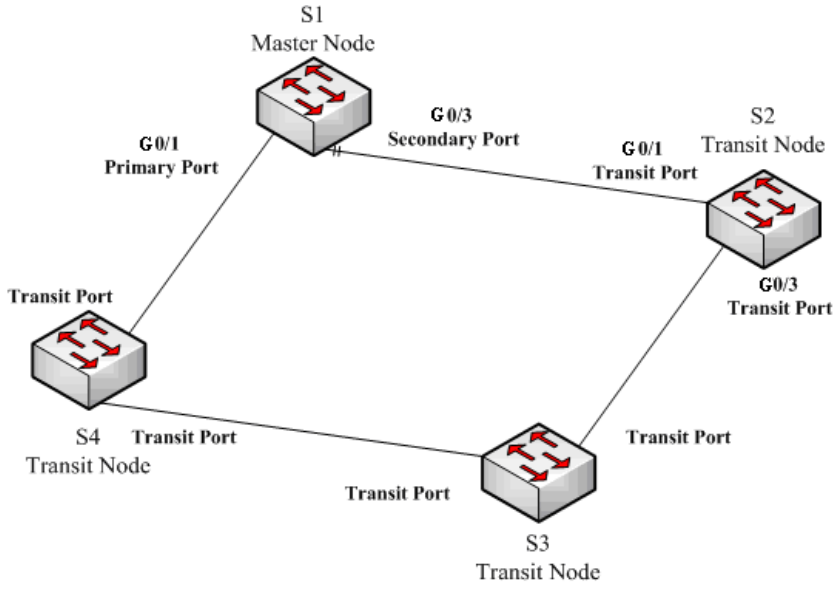
41.4.4 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show ether-ring *id*	Browses the summary information about the ring protection protocol and the port of Ethernet ring. id: ID of Ethernet ring
show ether-ring *id* **detail**	Browses the detailed information about the ring protection protocol and the port of Ethernet ring.
show ether-ring *id* **interface** *intf-name*	Browses the state of the Ether-ring port or that of the common port.

41.5 MEAPS configuration

41.5.1 Configuration Example



MEAPS configuration

As shown in figure 2.1, master node S1 and transit node S2 are configured as follows. As to the settings of other nodes, they are same to S2's settings.

Configuring switch S1:

Shuts down STP and configures the Ether-ring node:

S1_config#no spanning-tree

S1_config#ether-ring 1

S1_config_ring1#control-vlan 2

S1_config_ring1#master-node

The following commands are used to set the time related parameters:

S1_config_ring1#hello-time 2

S1_config_ring1#fail-time 6

Exits from the node configuration mode:

S1_config_ring1#exit

Configures the primary port and the secondary port:

S1_config#interface gigaEthernet 0/1

S1_config_g0/1#ether-ring 1 primary-port

S1_config_g0/1#exit

S1_config#interface gigaEthernet 0/3

S1_config_g0/3#ether-ring 1 secondary-port

S1_config_g0/3#exit

Establishes the control VLAN:

S1_config#vlan 2

S1_config_vlan2#exit

S1_config#interface range g0/1 , 3

S1_config_if_range#switchport mode trunk

S1_config_if_range#exit

Configuring switch S2:

S1_config#no spanning-tree

S1_config#ether-ring 1

S1_config_ring1#control-vlan 2

S1_config_ring1#transit-node

S1_config_ring1#pre-forward-time 8

S1_config_ring1#exit

S1_config#interface gigaEthernet 0/1

S1_config_g0/1#ether-ring 1 transit-port

S1_config_g0/1#exit

S1_config#interface gigaEthernet 0/3

S1_config_g0/3#ether-ring 1 transit-port

S1_config_g0/3#exit

S1_config#vlan 2

S1_config_vlan2#exit

S1_config#interface range gigaEthernet 0/1 , 3

S1_config_if_range#switchport mode trunk

S1_config_if_range#exit

Chapter 42 MEAPS Introduction

42.1 MEAPS Overview

EAPS is a protocol specially applied on the link layer of the Ethernet ring. When the Ethernet ring is complete, you should prevent the broadcast storm from occurring on the data loopback. But when a link of an Ethernet ring is broken, you should enable the backup link rapidly to resume the communication of different nodes in the ring. The role of switch is specified by you through configuration.

MEAPS, an expansion on the basis of EAPS, can support not only the single ring but also the level-2 multi-ring structure. The later structure consists of the aggregation layer in the middle, constructed by aggregation equipment through the Ethernet ring for fast switching, and the access layer at the outside, connected by the access equipment. Different levels of rings are connected through the tangency or intersection mode. See the specific topology in the following figure:

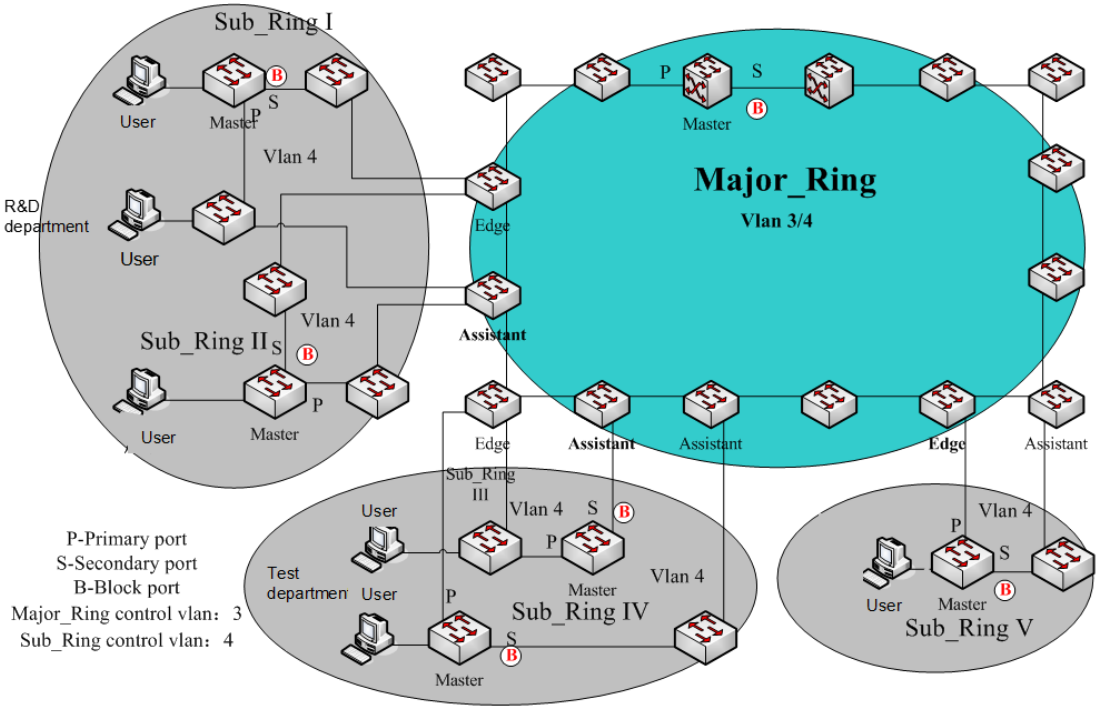


Figure 1 MEAPS Structure

The ring protection protocol and STP are both used for topology control on the link layer. STP is suitable for all kinds of complicated networks, which transmits the change of network topology hop by hop. The ring protection protocol is used for ring topology and adopts the pervasion mechanism to transmit the change of network topology. Therefore, the convergence of the ring protection protocol in the ring network is better than STP. In a sound network, the ring protection protocol can resume network communication within less than 50ms.

42.2 Basic Concepts of MEAPS

42.2.1 Domain

The domain specifies the protection range of the Ethernet loopback protection protocol and is marked by ID, which consists of integers; A group of switches that support the same protection data and have the same control VLAN can form

a domain after they are connected with each other. One domain may include only one ring or multiple rings that intersect each other. See Figure-2.

One MEAPS domain has the following factors: MEAPS ring, control VLAN, master node, transit node, edge node and assistant edge node.

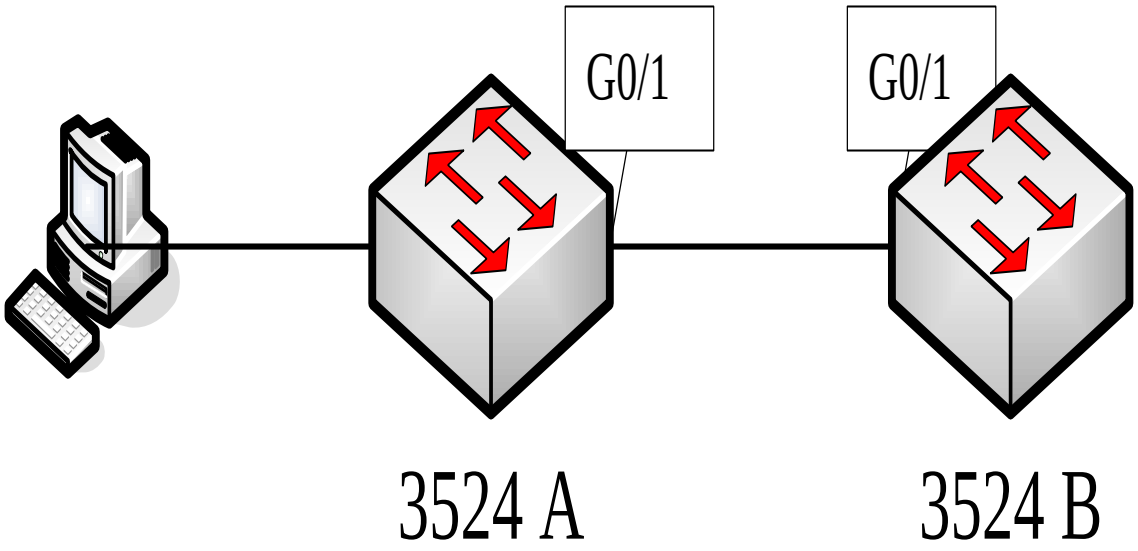


Figure-2 Simple MEAPS model

42.2.2 Ring

One ring corresponds to a ring Ethernet topology physically, which is a group of switches that are connected each other into a ring. One MEAPS domain may include only one MEAPS ring or multiple rings that intersect each other.

42.2.3 Major Ring

When a domain includes many rings, the included rings except the major ring are called as sub rings. The primary and secondary ports of each node on the major ring should be added into the main control VLAN and the sub control VLAN at the same time. See Figure-2.

42.2.4 Sub Ring

When a domain includes many rings, you should choose one ring from them as a major ring. The primary and secondary ports of each node on the sub ring should be added into the sub control VLAN. See Figure-2.

42.2.5 Control VLAN

The control VLAN is a concept against the data VLAN, and in MEAPS, the control VLAN is just used to transmit the MEAPS packets. Each MEAPS has two control VLANs, that is, the main control VLAN and the sub control VLAN.

You need to specify the main control VLAN when configuring the major ring or the sub ring. During configuration you just need to specify the main control VLAN and take the VLAN which is 1 more than the ID of the main control VLAN as the sub

control VLAN. The major ring will be added to the main control VLAN and the sub control VLAN at the same time, while the sub ring will only be added to the sub control VLAN. See number 3 and number 4 beside each port on the following figure.

The main-ring protocol packets are transmitted in the main control VLAN, while the sub-ring protocol packets are transmitted in the sub control VLAN. The sub control VLAN on the major ring is the data VLAN of the major ring. The ports of a switch that access the Ethernet ring belong to the control VLAN, and only those ports that access the Ethernet ring can be added into the control VLAN.

NOTE: The MEAPS port of the major ring should belong to both the main control VLAN and the sub control VLAN; the MEAPS port of the sub ring only belongs to the sub control VLAN. The major ring is regarded as a logical node of the sub ring and the packets of the sub ring are transparently transmitted through the major ring; the packets of the major ring are transmitted only in the major ring.

42.2.6 Data VLAN

Appearing against the control VLAN, the data VLAN is used to transmit data packets. The data VLAN can also include the MEAPS port and the non-MEAPS port. Each domain protects one or multiple data VLANs. The topology that is calculated by the ring protection protocol in a domain is effective only to the data VLAN in this domain.

Whether the data VLAN is created or not has no influence on the work of the ring state machine, where the MEAPS port is controlled by the MEAPS module and the non-MEAPS port is controlled by the STP module.

NOTE: The processing methods which are similar to that of the MSTP module can be used, that is, the status of a port in the default STP instance is decided by the link status of the port, no matter what the VLAN configuration of a port is.

42.2.7 Master Node

The master node works as policy making and control of a ring. Each ring must possess only one master node. The master node takes active attitude to know whether the ring's topology is complete, removes loopback, control other switches to update topology information. See the following figure, where S3 is the master node of the sub ring and S4 is the master node of the major ring.

42.2.8 Transit Node

All switches on the Ethernet except the master node can be called as the transit nodes. The transit node only checks the state of the local port of the ring, and notifies the master node of the invalid link. See the following figure, in which S1, S2, S5 and S6 are all transit nodes.

42.2.9 Edge Node and Assistant Node

When the sub ring and the major ring are intersected, there are two intersection points, two switches beside which are called as the edge node for one and the assistant node for the other. The two nodes are both the nodes of the sub ring. There are no special requirements as to which switch will be set to be the edge node or the assistant node if their configurations can distinguish themselves. However, one of them must be set as the edge node and the other must be set as the assistant node. The edge node or the assistant node is a role that a switch takes on the sub ring, but the switch takes a role of the transit node or the master node when it is on the major ring. See the following figure, in which S2 is the assistant node and S5 is the edge node.

42.2.10 Primary Port and Secondary Port

The two ports through which the master node accesses the Ethernet ring are called as the primary port and the secondary port. The roles of the two ports are decided by the clients.

The primary port is in forwarding state when it is up. Its function is to forward the packets of the data VLAN on the master node and to receive and forward the control packets on the control VLAN. The master node will transmit the loopback detection packets from the primary port to the control VLAN. If the link of the primary port is resumed from the invalid status, the master node requires to send the address aging notification to the control VLAN promptly and then starts to transmit the loopback detection packets from the primary port.

The secondary port is in forwarding or blocking state when it is up. The master node receives the ring detection packets from the secondary port and judges whether the topology of the ring network is complete. In complete topology, the master node blocks the data packets on the secondary port, and prevents loopback from occurring; after a link on the ring network is interrupted, the master node will open the secondary port to forwarding the data packets.

NOTE: A port can be set as the primary port or the secondary port of a node and it cannot be set to be both the primary port and the secondary port.

42.2.11 Transit Port

The two ports for the transit node to access the Ethernet ring are both transit ports. Users can decide the role of the two ports through configuration.

The transit port is in forwarding or preforwarding state when it is up. A transit port receives the control packets from the control VLAN and at the same time forwards these packets to other ports in the control VLAN. After the transit port resumes from the invalid state, it first enters the pre-forwarding state, receives and forwards only the control packets, and blocks the data VLAN. After the transit node receives the notification of the aging address table, it enters the forwarding state.

NOTE: A port can be set as the primary port or the transit port of a node and it cannot be reset.

42.2.12 Common Port and Edge Port

The edge node and the assistant node are the places where the sub ring and the major ring intersect. As to the two ports that access the Ethernet, one is a common port, which is the public port of the sub ring and the major ring; the other is the edge port in the sub ring. The roles of the two ports are decided by users through configuration.

The common port is on the main-ring port and so its state is decided by the state of the main-ring port. The common port itself has no operations or notifications. When the link, connecting the common port, changes, the sub-ring node where the common port lies will not be notified. The existence of the common port just guarantees the completeness of the ring.

The edge port of the edge node is in forwarding or preforwarding state when it is up. Its basic characteristics are consistent with those of the transit port except one function. The exceptional function is that when the edge port is up and its corresponding main-ring port is also up, it will transmit the edge-hello packets from the main-ring port to detect the completeness of the major ring.

The edge port of the assistant node is in forwarding, preforwarding or EdgePreforwarding state when it is up. Besides the same characteristics of the transit port, it also has one more state, the Edge Preforwarding state. If the edge port is in

forwarding state and the main-ring port that the edge port corresponds to has not received the edge-hello packets, the state of the edge port is changed into the EdgePreforwarding state, and it only receives and forwards the control packets and blocks the data VLAN until the corresponding main-ring port receives the Edge-hello packets again.

The edge port of the edge node and the assistant node is to help detect the completeness of the major ring. For more details, see the channel status checkup mechanism of the sub-ring protocol packets on the major ring in the following chapter.

NOTE: Each port can be set as the only edge port of a node and it cannot be configured again; the common port can be borne only on a port of the major ring and it cannot be configured on a port without a corresponding main-ring port.

42.2.13 Aging of the MAC Address Table (FLUSH MAC FDB)

The Ethernet ring protection protocol can transmit data packets to the correct link by controlling the aging of the switch's MAC address table when the topology changes. In general, the time for a MAC address to age in the MAC address table is 300 seconds. The ring protection protocol can control the aging of the MAC address table in a short time.

42.2.14 Complete Flag of Ring

Both the master node and the transit node can show whether the current ring network is complete through the state symbol "COMPLETE". On the master node, only when all links of the ring network are normal, the primary port is in forwarding state and the secondary port is in blocking state can the "COMPLETE" symbol be real; on the transit node, only when its two transit ports are in forwarding state can the "COMPLETE" symbol be true. On the master node, only when all links of the ring network are normal, the primary port is in forwarding state and the secondary port is in blocking state can the "COMPLETE" symbol be real; on the transit node, only when its two transit ports are in forwarding state can the "COMPLETE" symbol be true.

The state symbol of the ring network helps user to judge the topology state of the current network.

42.3 Types of EAPS Packets

Type of the packet	Description
Ring Detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
link interruption (LINK-DOWN)	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
MAC address aging table of the transit node (RING-DOWN-FLUSH-FDB)	It is transmitted by the master node after interruption of the ring network is detected and the packets show the MAC address aging table of the transit node.
Ring resume aging address table (RING-UP-FLUSH-FDB)	It is transmitted by the master node after interruption of the ring network is resumed and the packets show the MAC address aging table of the transit node.
Ring completeness detection (EDGE-HELLO)	It is decided by the edge port of the edge node, transmitted by the main-ring port that the edge node corresponds to, and detects whether the major ring is complete.

Table 1.1 Types of EAPS packets

42.4 Fast Ethernet Ring Protection Mechanism

42.4.1 Polling mechanism

The primary port transmits the HEALTH packets to the control VLAN. In normal case, the HEALTH packets will pass through all other nodes of the ring and finally arrive at the secondary port of the master node.

The secondary port blocks all data VLANs in primitive condition. When receiving the HEALTH packets continuously, the secondary port keeps blocking data VLANs and blocking the loop. If the secondary port does not receive the HEALTH packets from the primary port in a certain time (which can be configured), it will regard the ring network is out of effect. Then the master node removes the blocking of data VLANs on the secondary port, ages the local MAC address table, and transmits the RING-DOWN-FLUSH-FDB packets to notify other nodes.

If the master node receives the HEALTH packets at the secondary port that is open to data VLANs, the ring network is resumed. In this case, the master node immediately blocks data VLANs on the secondary port, updates the local topology information and reports other nodes to age the MAC address table through RING-UP-FLUSH-FDB packets.

As shown in the following figure, the master node, S4, transmits the HELLO packets periodically. If the loopback has no troubles, the HELLO packets will arrive at the secondary port of the master node, and the master node will block data forwarding of the data VLAN that the secondary port belongs to, preventing the loopback from happening.

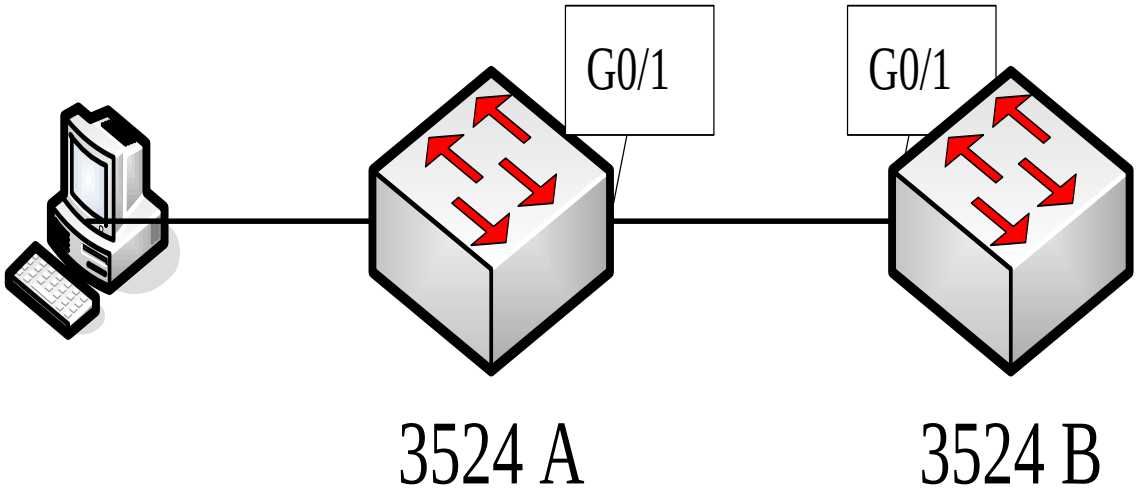


Figure 3 Polling mechanism

Note: You can configure related commands on the Hello-time node and the Fail-time node to modify the interval for the primary port to transmit the HEALTH packets and the time limit for the secondary port to wait for the HEALTH packets.

42.4.2 Notification of Invalid Link of Transit Node

The link state change notification mechanism provides a faster processing mechanism for ring network topology changes than the polling mechanism:

After the transit port of the transit node is out of effect, the LINK-DOWN packet will be immediately transmitted by the other transit port to notify other nodes. In normal case, the packet passes through other transit nodes and finally arrives at one port of the master node.

After the master node receives the LINK-DOWN packet, it thinks that the ring network is invalid. In this case, the master node removes the blocking of data VLANs on its secondary port, ages the local MAC address table, transmits the RING-DOWN-FLUSH-FDB packet and notifies other nodes. As shown in the following figure, trouble occurs on the link between node S3 and node S6. After node S3 and node S6 detect that trouble has already occurred on the link, they block the ports that the troubled link corresponds to and transmit the LINK-DOWN packets respectively from the other port; when the master node receives the LINK-DOWN packets, holds that the trouble occurs on the loopback, and decides not to wait for the fail-time any more.

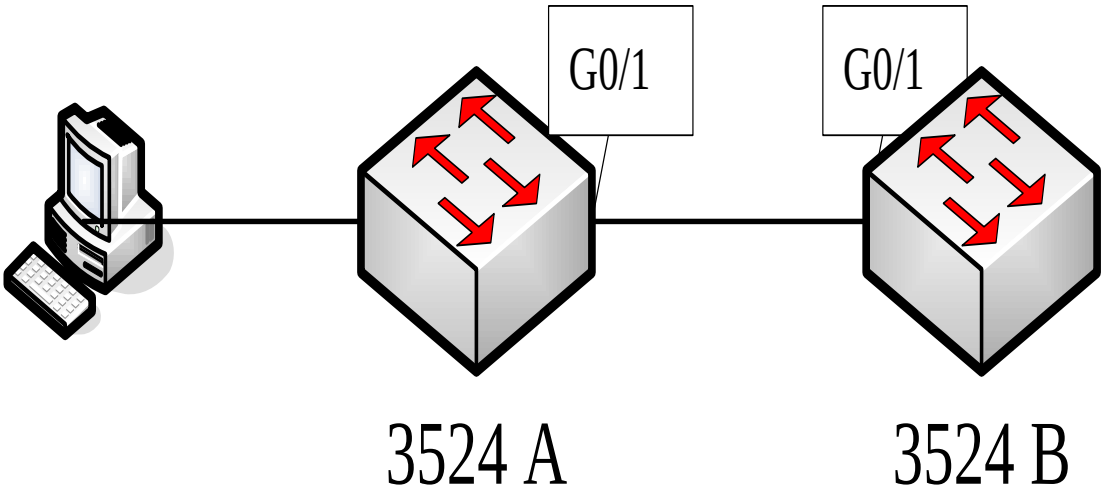


Figure 4 Link status change's notification

After the transit port is resumed, it does not immediately transmit the packets of data VLANs, but enters the Pre-Forwarding state. A transit port in pre-forwarding state only transmits and receives the control packets from the control VLAN.

If there is only one transit port invalid in the ring network and when the port enters the pre-forwarding state, the secondary port of the master node can receive the HEALTH packet from the primary port again. In this case, the master node blocks data VLANs on the secondary port again and transmits the notification of ageing address table outside. After the node with a transit port in pre-forwarding state receives the notification of aging address table, the node will first modify the pre-forwarding port to the forwarding port and then ages the local MAC address table.

If a transit mode does not receives the notification of aging address table from the master node, it thinks that the link connecting the master node is already out of effect, and the transit node will automatically set the pre-forwarding port to be a forwarding one.

NOTE: You can configure the related commands through the pre-forward-time node to modify the time for the transit port to keep the pre-forwarding state.

42.4.3 Channel Status Checkup Mechanism of the Sub-Ring Protocol Packet on the Major ring

The ports on the major ring are simultaneously added to the control VLAN of the major ring and the control VLAN of the sub ring. Hence, the protocol packets of the sub ring should be broadcast among the edge ports of the edge node and the assistant node through the channel, provided by the major ring. In this case, the whole major ring is just like a node of the sub ring (similar as a virtual transit node), as shown in the following figure:

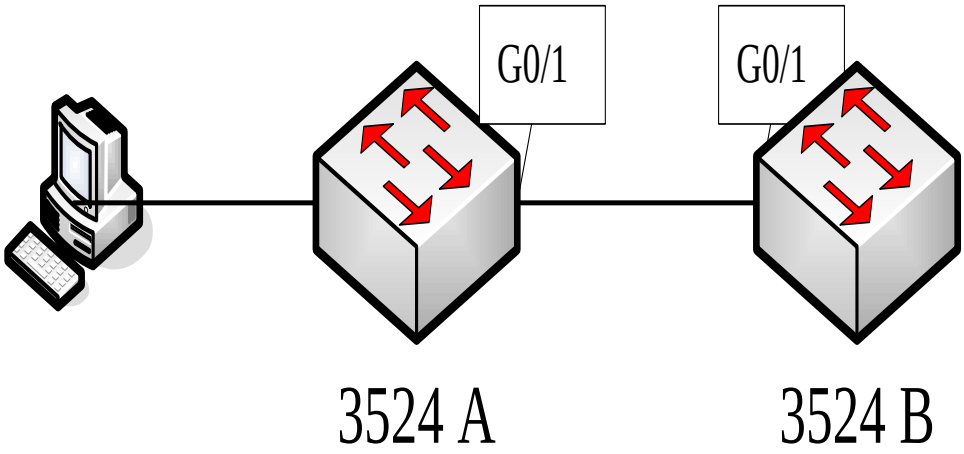


Figure 5 Intersection of the major ring and the sub ring

When trouble occurs on the link of the major ring, and when the channel of the sub-ring protocol packets between the edge node and the assistant node are interrupted, the master node of the sub ring cannot receive the HELLO packets that the master node itself transmits. In this case, the Fail Time times out, and the master node of the sub ring changes to the Failed state and opens its secondary port.

The above-mentioned processes have an effective protection towards general networking, guaranteeing not only the prevention of the broadcast loopback but also the corresponding functions of the backup link. The dual homing networking mode is always used in actual networking, as shown in the following figure. The two sub rings in the dual homing networking, sub ring I and sub ring II, interconnect through the edge node and assistant node, and forms a big ring. When the major ring has troubles, the secondary ports of the master nodes of all sub rings open and forms the broadcast loop (marked by the arrow) in the big ring.

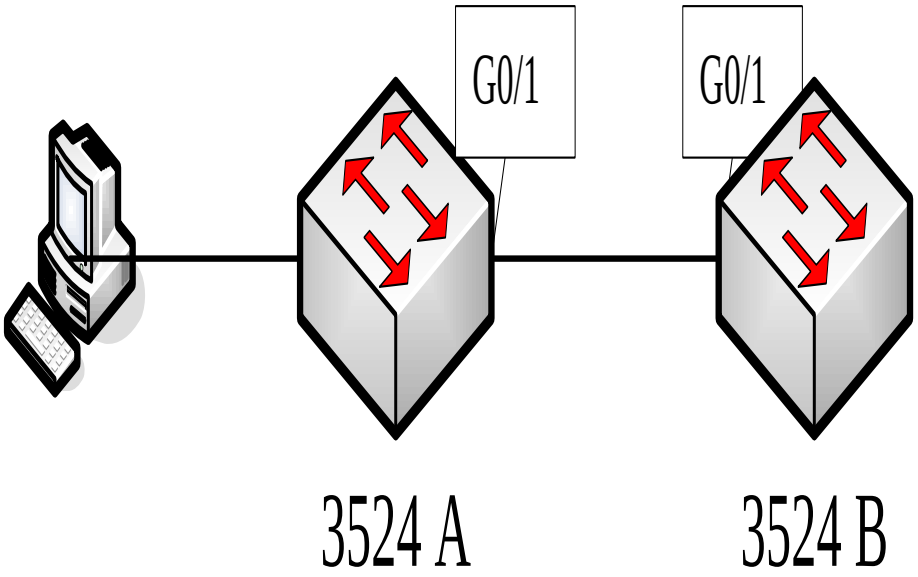


Figure 6 Broadcast storm triggered by the dual homing networking mode

The channel status checkup mechanism of the sub-ring protocol packet on the major ring is introduced to solve the problem about the dual homing ring. This mechanism is to monitor the status of the channel link on the major ring between the edge node and the assistant node, which requires the help of the edge node and the assistant node. The purpose of this mechanism is to keep the data loop from happening by blocking the edge port of the edge node before the secondary port of the master node on the sub ring opens. The edge node is the trigger of the mechanism, while the assistant node is the listener and decider of this mechanism. Once the notification message from the edge node cannot be received, the edge node will instantly be in blocked state until this notification message is received again. The results of the mechanism, which bring about after the troubles on the major ring, are shown in the following figure:

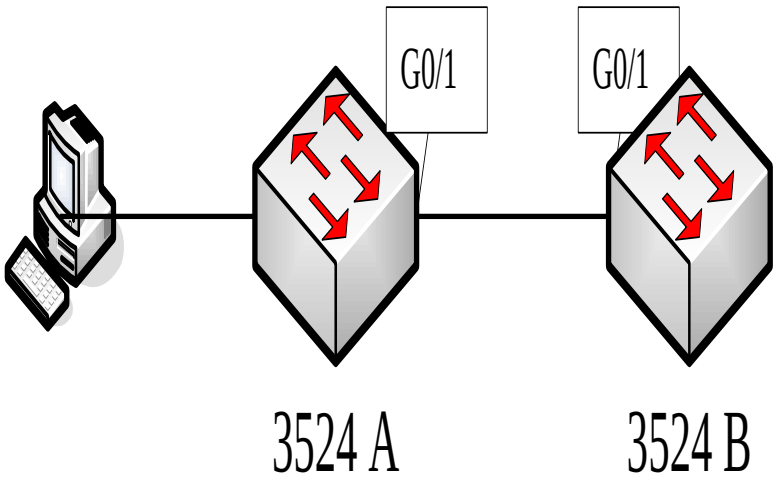


Figure 7 Results of the channel status checkup mechanism

But you should pay special attention to this point that the edge port of the assistant node must be blocked before the secondary port of the master node on the sub ring opens. Otherwise, the broadcast storm will happen.

The whole procedure of this mechanism is described as follows:

1. Check the channel status on the major ring between the edge node and the assistant node.

The edge node of the sub ring periodically transmits the Edge-Hello packets to the major ring through the two ports of the major ring, and these packets pass through all nodes on the major ring in sequence and finally arrive the assistant node, as shown in the following figure. If the assistant node can receive the edge-hello packet in the regulated time, it indicates that the channel of this packet is normal; if not, it indicates that the channel is interrupted. The edge-hello packet is the control packet of the sub ring, but is transmitted and received by the ports on the major ring and is transferred to the sub ring for processing.

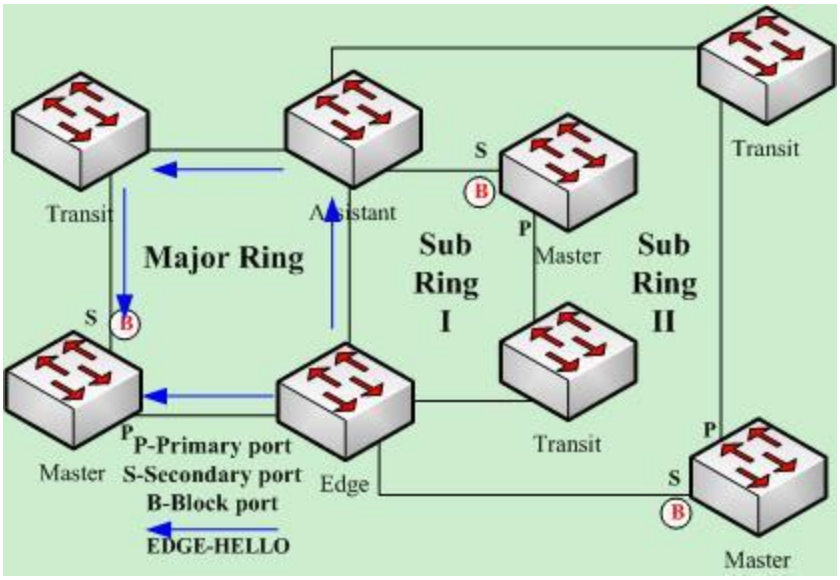


Figure 8 Checking the channel status on the major ring between the edge node and the assistant node

2. The edge node blocks the edge port at the interruption of the channel.

If the assistant node cannot receive the edge-hello packet during Edge Fail Time, the assistant holds that the channel of the sub-ring protocol packet - the edge-hello packet - is interrupted, changes its edge port's status into the Edge-Preforwarding status instantly, blocks the forwarding of the data packets (though still receives and forwards the control packet), and immediately transmits the LINK-DOWN packet to the master node for the master node to open the secondary port to avoid communication interruption among all nodes on the ring.

NOTE: In order to guarantee that the edge port first changes into the edge-preforwarding status and then the master node opens the secondary port, you shall be sure that the cycle for the edge node to transmit the edge-hello packet, Edge Hello Time, is smaller than the cycle for the master node to transmit the Hello packet, Hello Time; similarly, the Edge Fail Time of the assistant node should be smaller than Fail Time. At the same time, Fail Time is generally the triple of Hello Time, and Edge Fail Time is also the triple of Edge Hello Time.

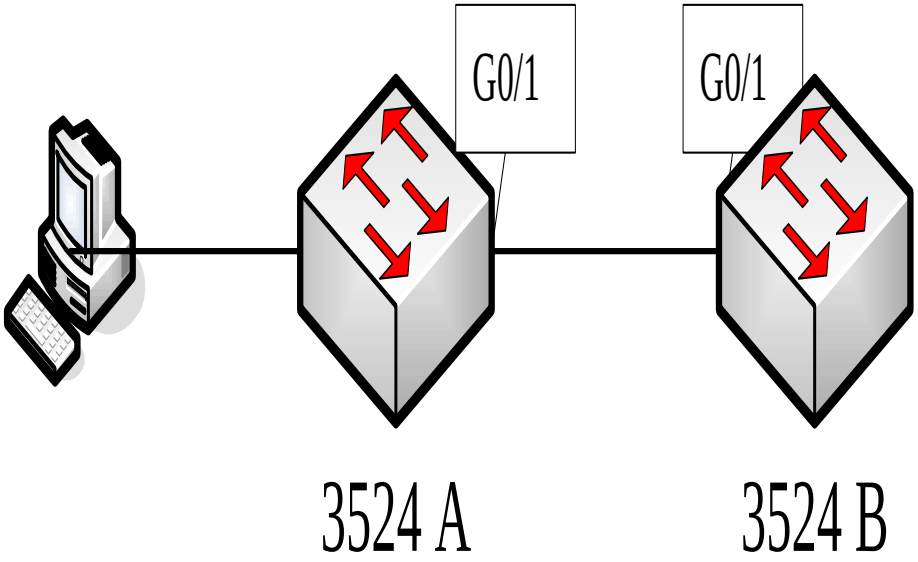


Figure 9 The edge port being blocked by the edge node at the interruption of the channel

3. Channel recovery

When the link of the major ring and the communication between the edge node and the assistant node resumes, the channel of the sub-ring protocol packet resumes to the normal function. In this case, the master node of the sub ring receives the Hello packet again, which is transmitted by the master node itself, and therefore it switches to the Complete status, blocks the secondary port and transmits the RING-UP-FLUSH-FDB packet to the ring. At the same time, the status of the edge port of the assistant node changes from Edge-Preforwarding to Forwarding, guaranteeing a smooth communication among all nodes on the ring. The following figure shows that the channel is resumed and then the communication on the ring is also resumed.

NOTE: Before the edge node opens the blocked edge port, the secondary port of the master node on the sub ring should be blocked to prevent the broadcast storm from happening.

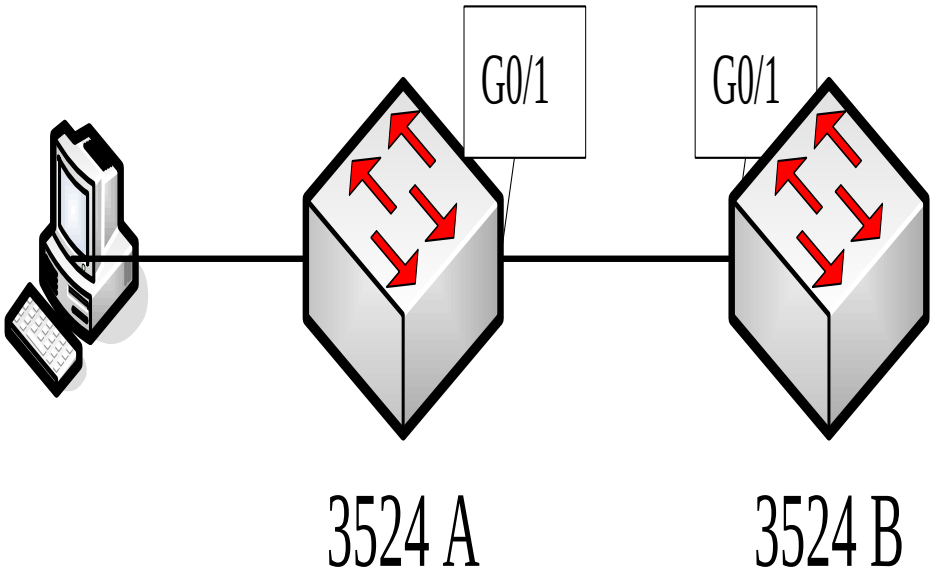


Figure 10 Channel recovery

Chapter 43 Fast Ethernet Ring Protection Configuration

43.1 Requisites before Configuration

Before configuring MEAPS, please read the following items carefully:

- One of important functions of the ring protection protocol is to stop the broadcast storm, so please make sure that before the ring link is reconnected all ring nodes are configured. For example, when EAPS is configured, after the master node and all transit nodes are configured, connect the network cable and the secondary port of the master node; when configuring ERPS, please keep at least one link disconnected until all ring nodes are configured.
- Enable the ring protection protocol to be compatible with the STP of a switch through relative configurations. The users are allowed to set "no spanning-tree", SSTP, RSTP PVST or MSTP mode.
- After an instance of the ring's node is set, users are forbidden to change the basic information of the node (excluding the time parameters) unless the current ring's node is deleted and then reset.
- If you run show to browse the configured node and find its **state** is **init**, it shows that the node's configuration is unfinished and therefore the node cannot be started. In this case, you are required to change or add basic information to complete the configuration of the node.
- The ring protection protocol supports a switch to configure multiple ring networks.
- The configuration of the control VLAN of the ring automatically leads to the establishment of the corresponding VLAN without requiring users' manual configuration.
- The port of each ring can forward the packets from the control VLAN of the ring, while other ports, even in the Trunk mode, cannot forward the packets from the control VLAN.
- By default, Fail-time of the master node is triple longer than Hello-time, so that packet delay is avoided from shocking the ring protection protocol. After Hello-time is modified, Fail-time need be modified accordingly.
- By default, Pre-Forward-Time of the transit node is triple longer than Hello-time of the master node so that it is ensured that the master node can detect the recovery of the ring network before the transit port enters the pre-forwarding state. If Hello-time configured on the master node is longer than Fre-Forward-Time of the transit node, loopback is easily generated and broadcast storm is then triggered.
- Users cannot set Edge Hello Time and Edge Fail Time, and their default values are decided by Hello Time and Fail Time respectively for their values are 1/3 of Hello Time and Fail Time respectively.
- The physical interface, the fast-Ethernet interface, the gigabit-Ethernet interface and the aggregation interface can all be set to be the ring's interfaces. If link aggregation, 802.1X or port security has been already configured on a physical interface, the physical interface cannot be set to be a ring's interface any more.
- This protocol is similar with the original EAPS in functions, but its ring's topology has more expansibility and flexibility. Hence, MEAPS and EAPS are partially compatible, and the intersection configuration can be done on the MEAPS ring and the EAPS ring.

43.2 MEAPS Configuration Tasks

- Configuring the Master Node
- Configuring the Transit Node
- Configuring the Edge Node and the Assistant Node
- Configuring the Ring Port
- Browsing the State of the Ring Protection Protocol

43.3 Fast Ethernet Ring Protection Configuration

43.3.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch#**config**	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1#**master-node**	Compulsory. Configures the node type to be a master node.
Switch_config_ring1#**major-ring[sub-ring]**	Compulsory. Sets the node's level to be one of the major or sub ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". *vlan-id*: control vlan ID
Switch_config_ring1#**hello-time** *value*	Optional. Configures the cycle for the master node to transmit the HEALTH packets. *Value:* It is a time value ranging from 1 to 10 seconds and the default value is 3 seconds.
Switch_config_ring1#**fail-time** *value*	Optional. Configures the time for the secondary port to wait for the HEALTH packets. *Value*: It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring1#**exit**	Saves the current settings and exits the node configuration mode.
Switch_config#	

NOTE:

The *no mether-ring id domain id2* command is used to delete the node settings and the node's port settings of the ring.

NOTE:

The major ring and the sub-ring must configure with the same vlan- the major ring control vlan. After configuration, the major ring control vlan and the sub-ring control vlan will be established on the major ring simultaneously. The sub-ring control vlan will be created on the sub-ring and forbid the major ring to control vlan.

43.3.2 Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. *id1*: ID of the node; id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1# **transit -node**	Compulsory. Configures the node type to be a transit node.
Switch_config_ring1#**major-ring[sub-ring]**	Compulsory. Sets the node's level to be one of the major or sub ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". *vlan-id:* control vlan ID
Switch_config_ring1#**pre-forward-time** *value*	Optional. Configures the time of maintaining the pre-forward state on the transit port. Value: It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring#exit	Saves the current settings and exits the node configuration mode.
Switch_config#	

43.3.3 Configuring the Edge Node and the Assistant Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# **config**	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1#**edge-node[assistant-node]**	Compulsory. Sets the node type to be an edge node.
Switch_config_ring1#**sub-ring**	This step can be omitted. The edge node must be the sub-ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1"

	vlan-id: control vlan ID.
Switch_config_ring1#**pre-forward-time** *value*	Optional. Configures the time of maintaining the pre-forwarding state of the edge port. *Value:* It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring1#**exit**	Saves the current settings and exits the node configuration mode.
Switch_config#	

43.3.4 Configuring Sub-ring Networking Mode

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# **config**	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1#**edge-node[assistant-node]**	Compulsory. Sets the node type to be an edge node.
Switch_config_ring1#**sub-ring**	This step can be omitted.The edge node must be the sub-ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". *vlan-id*: control vlan ID
Switch _config_ring2#**single-subring-mode**	Compulsory. The ring configuration can be finished without configuring the command, but the sub-ring networking mode is not available. In the sub-ring networking mode, the sub-ring protocol packet channel detection mechanism cannot work on the major ring and there must no dual homing networking. The command is effective only for the edge node and the assistant node.
Switch_config_ring1#**pre-forward-time** *value*	Optional. Configures the time of maintaining the pre-forwarding state of the edge port. Value: It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring1#**exit**	Saves the current settings and exits the node configuration mode.
Switch_config#	

43.3.5 Configuring the Ring Port

Configure a port of a switch to be the port of Ethernet ring according to the following steps:

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config#interface *intf-name*	Enters the interface configuration mode.
Switch_config_intf#mether-ring *id1* **domain** *id2* **primary-port [secondary-port | transit-port | common-port | edge-port]**	Configures the type of the port of Ethernet ring. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_intf#exit	Exits from interface configuration mode.

NOTE: Run **no mether-ring** *id1* **domain** *id2* **primary-port [secondary-port | transit-port | common-port | edge-port] to delete the ring port configuration.**

43.3.6 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show mether-ring	Browses the summary information about the ring protection protocol and the ports of ring.
show mether-ring *id1* **domain** *id2*	Browses the summary information about the designated ring protection protocol and the ports of ring. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
show mether-ring *id1* **domain** *id2* **detail**	Browses the detailed information about the designated ring protection protocol and the port of Ethernet ring.
show mether-ring *id1* **domain** *id2* **interface** *intf-name*	Browses the states of the designated ring ports or those of the designated common ports.

Chapter 44 Appendix of MEAPS Configuration

44.1 Working Procedure of MEAPS

MEAPS adopts three protection mechanisms to support the single-ring or level-2 multi-ring structure. The following sections shows, from the complete state to the link-down state, then to recovery and finally to the complete state again, the details of MEAPS running and the change of the MEAPS topology by typical examples.

44.1.1 Complete State

The complete state of the ring, which is advocated for only one ring, is monitored and maintained by the polling mechanism. In complete status, all links on the whole ring are in UP state, which finds expression in the state of the master node. In order to prevent the broadcast storm from occurring, the master node will block its secondary port. At the same time, the master node will periodically transmit the Hello packets from its primary port. These hello packets will pass through the transit node in sequence and finally return to the master node from its secondary port. The ring in complete state is shown in the following figure. The major ring and two sub rings are all in complete state. The hello packet of the major ring is only broadcast in the major ring, while the hello packet of the sub ring can be transparently transmitted through the major ring, then return to the sub ring, and finally get the secondary port of the master node on the sub ring.

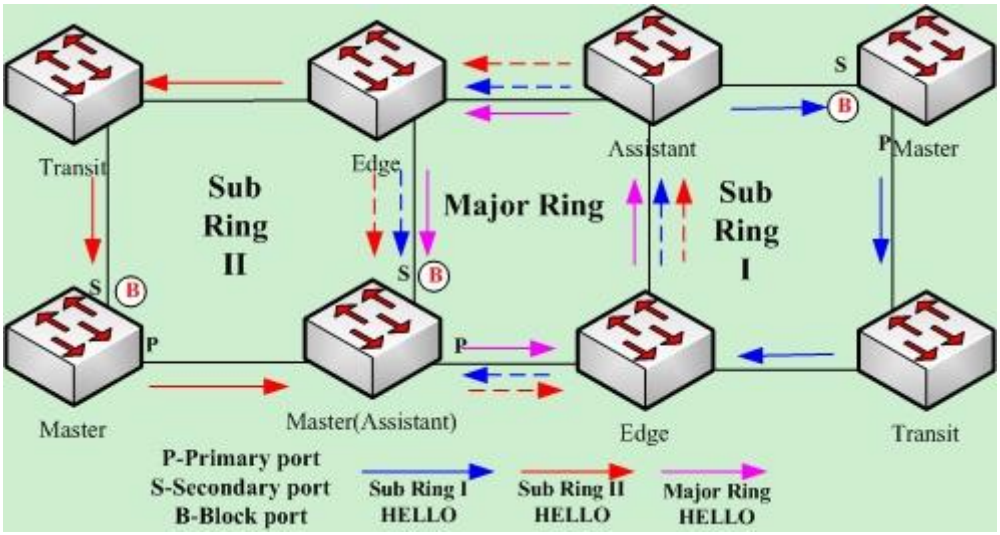


Figure 11 Complete state

44.1.2 Link-Down

The link-down state of the ring is decided by the polling mechanism, the notification of the link state change and the channel status checkup mechanism of the sub-ring protocol packet. Surely the link-down state of the ring is also advocated as to only one ring. When some link in the ring is in link-down state, the ring changes from the compete state to the troubled state, that is, the link-down state.

If link-down occurs on a link, the polling mechanism and the link status change notification mechanism will both function. The transit node, on which link-down occurs, will transmit the link-down packet to the master node through the Up port at its other side; at the same time, the polling mechanism will monitor and change promptly the state of the ring through Fail Time. When a trouble occurs on the sub-ring protocol channel, the trouble will be handled by the channel status checkup mechanism of the sub-ring protocol packet on the major ring. As shown in the following figure, the trouble notification

message on the link of the major ring and on the common link is only transmitted on the major ring and finally transmitted to the master node; the trouble notification message on the link of sub ring 2 will be transmitted to the master node of the sub ring, which can be transparently transmitted through the major ring.

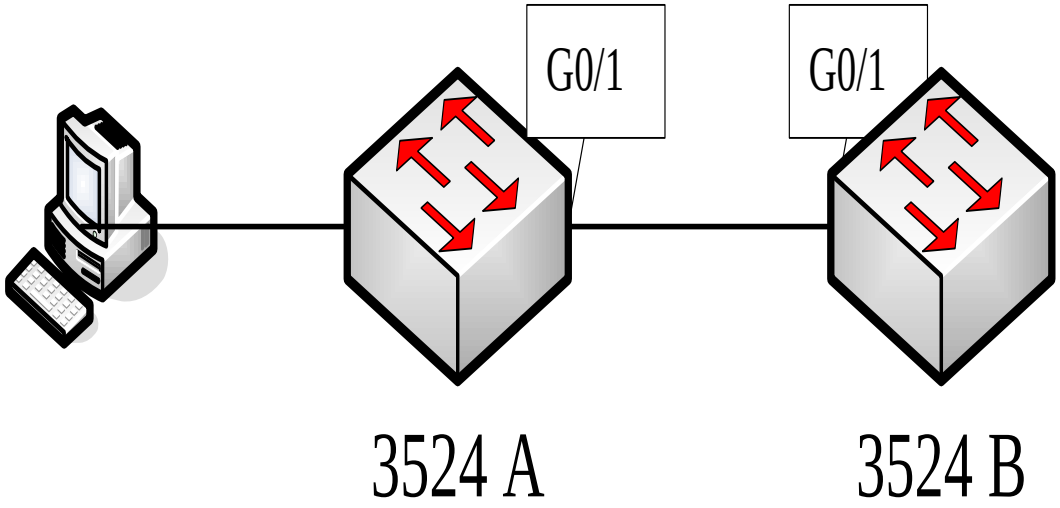


Figure 12 Ring transmitting the trouble and notifying the master node

After the master node receives the link-down packet, its state will be changed to the Failed state and at the same time the secondary port will be opened, the FDB table will be refreshed, and the RING-DOWN-FLUSH-FDB packets will be transmitted from two ports for notifying all nodes. As shown in the following figure, the master node on the major ring notifies the transit node on the major ring of refreshing FDB; sub ring 1 has troubles on its channel, so the edge port of the assistant node will be blocked; the master node of sub ring 2 notifies the transit nodes on the sub ring to refresh FDB and then the transparent transmission will be conducted on the major ring.

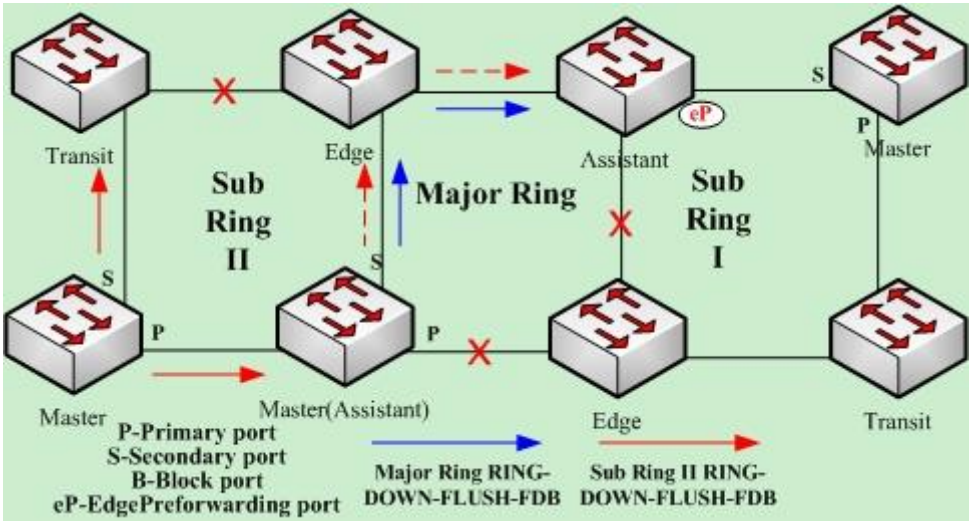


Figure 13 Ring transmitting troubles and refreshing FDB

44.1.3 Recovery

When the port on the transit node is recovered, the transit node will shift to its Preforwarding state. The processing procedure when the port of the transit node is recovered is shown in the following figure. The link of the major ring will recover, while the transit node, which connects the link of the major ring, changes into the Preforwarding state, blocks the data packets but allows the Hello packets of the control packet to pass through; similarly, the transit node on sub ring 2 also changes into the Preforwarding state; when the hello packet on sub ring 1 arrives the edge node, due to the fact that the resumed transit node only allows the control packet of the major to pass through and that the hell packet of sub ring 1 is just like the data packet of the major ring, the hello packet cannot be forwarded.

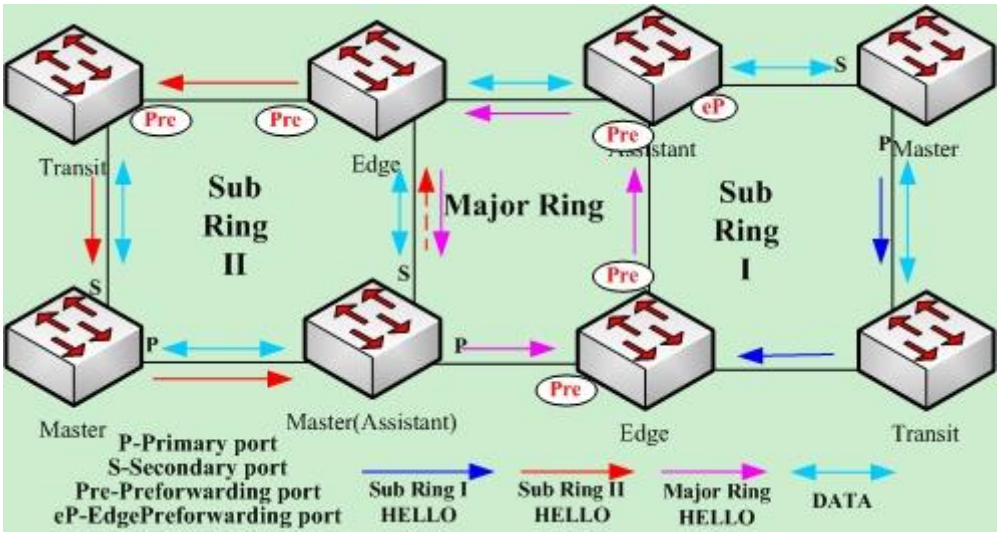


Figure 14 Recovery of the ring's link and the shift of the transit node to preforwarding

The transit port can transmit the control packet in preforwarding state, so the secondary port of the master node can receive the hello packet from the primary port. Hence, the master node shifts its state to Complete, blocks the secondary port and transmits the RING-UP-FLUSH-FDB packet from the primary port. After the transit node receives the RING-UP-FLUSH-FDB packet, the transit node will shift back to the Link-Up state, open the blocked port and refresh the FDB table. The procedure of ring recovery is shown in the following figure. The master node on the major ring changes into the complete state, blocks the secondary port, transmits the RING-UP-FLUSH-FDB packet to all transit nodes on the major ring and makes these transit nodes to shift back to their link-up state, to open the blocked port and to refresh the FDB table; similarly, the transit node and the master node on sub ring 2 also take on the corresponding change; due to the sub-ring protocol packet's channel recovery on sub ring 1, the secondary port of the master node can receive the hello packet from the primary port, and the master node shifts its state back to the complete state, blocks the secondary port, transmits the RING-UP-FLUSH-FDB packet and makes the assistant node open the edge port and sub ring 1 resume to its complete state.

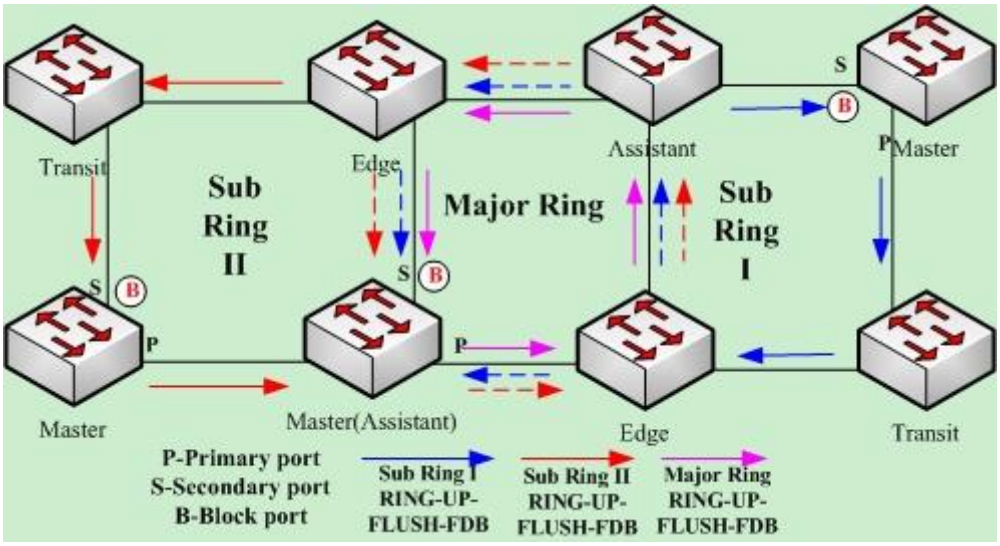


Figure 15 Recovery of the ring

Of course, if the transit node in Preforwarding state does not receive the RING-UP-FLUSH-FDB packet and Fail Time also exceeds, the transit node will open the blocked transit port and resume data communication.

44.2 MEAPS Configuration Examples

44.2.1 Configuration Examples

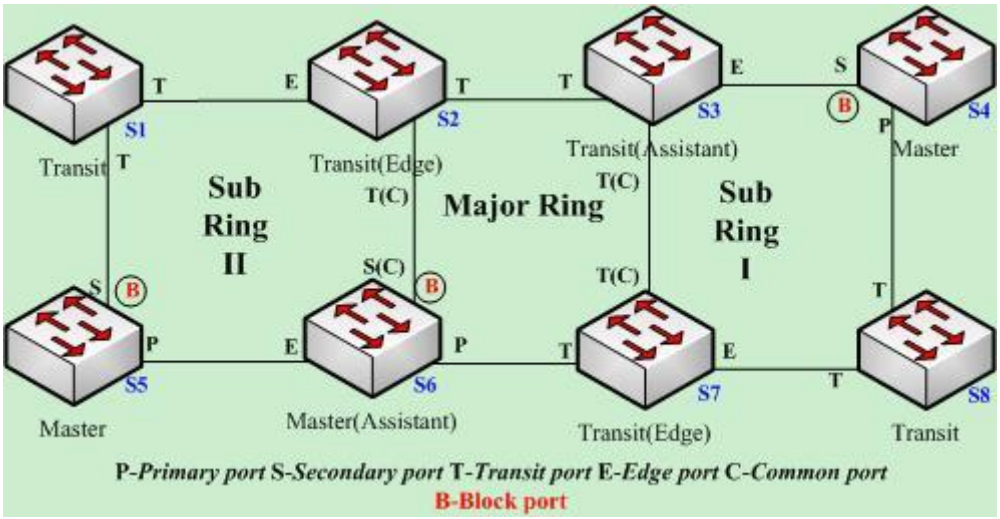


Figure 2.1 MEAPS Configuration Examples

As shown in figure 2.1, master node S1 and transit node S2 are configured as follows. As to the settings of other nodes, they are same to S2's settings.

Configuring switch S1:

The following commands are used to set the sub-ring transit node, node 2:

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#transit-node

Switch_config_ring2#sub-ring

Switch_config_ring2#control-vlan 2

The following commands are used to set the time parameter:

Switch_config_ring2#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring2#quit

The following commands are used to set the transit port of node 2:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 2 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

Configuring switch S2:

The following commands are used to set the major-ring transit node, node 1:

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring1#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring1#quit

The following commands are used to set the transit port of node 1:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

The following commands are used to set the sub-ring edge node, node 2:

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#edge-node

Switch_config_ring2#sub-ring *(This step can be omitted.)*

Switch_config_ring2#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring2#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring2#quit

The following commands are used to set the common port and edge port of node 2:

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 2 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S3:

The following commands are used to set the transit port of node 1:

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring1#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring1#quit

The following commands are used to set the transit port of node 1:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

The following commands are used to set the sub-ring assistant node, node 4:

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#assistant-node

Switch_config_ring4#sub-ring *(This step can be omitted.)*

Switch_config_ring4#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring4#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring4#quit

The following commands are used to set the common port and edge port of node 2:

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 4 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S4:

The following commands are used to set the sub-ring master node, node 4:

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#master-node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring4#hello-time 4

Switch_config_ring4#fail-time 12

Exits from the node configuration mode:

Switch_config_ring4#quit

The following commands are used to set the primary port and secondary port of node 4:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 4 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

Configuring switch S5:

The following commands are used to set the sub-ring master node, node 2:

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#master-node

Switch_config_ring2#sub-ring

Switch_config_ring2#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring2#hello-time 4

Switch_config_ring2#fail-time 12

Exits from the node configuration mode:

Switch_config_ring2#quit

The following commands are used to set the primary port and secondary port of node 2:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 2 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

Configuring switch S6:

The following commands are used to set the major-ring master node, node 1:

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#master-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring1#hello-time 4

Switch_config_ring1#fail-time 12

Exits from the node configuration mode:

Switch_config_ring1#quit

The following commands are used to set the transit port of node 1:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

The following commands are used to set the sub-ring assistant node, node 2:

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#assistant-node

Switch_config_ring2#sub-ring *(This step can be omitted.)*

Switch_config_ring2#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring2#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring2#quit

The following commands are used to set the common port and edge port of node 2:

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 2 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S7:

The following commands are used to set the major-ring transit node, node 1:

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring1#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring1#quit

The following commands are used to set the transit port of node 1:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

The following commands are used to set the secondary port of node 4:

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#edge-node

Switch_config_ring4#sub-ring *(This step can be omitted.)*

Switch_config_ring4#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring4#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring4#quit

The following commands are used to set the common port and edge port of node 2:

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 4 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

Configuring switch S8:

The following commands are used to set the sub-ring transit node, node 4:

Switch_config#mether-ring 4 domain 1

Switch_config_ring4# transit -node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

The following commands are used to set the time related parameters:

Switch_config_ring4#pre-forward-time 12

Exits from the node configuration mode:

Switch_config_ring4#quit

The following commands are used to set the transit port of node 4:

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 4 domain 1 transit -port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 transit -port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

44.3 Unfinished Configurations (to be continued)

- Unfinished basic information configuration: there is one of the ring's role, the ring's grade and the control VLAN unset. One exceptional case is that when a node's role has configured to be the edge node or assistant node, the default ring's grade is sub-ring.
- Contradiction of basic information: When a node's role is edge-node or assistant-node, the default ring's grade is sub-ring; when the ring's grade is major-ring, prompt information will appear.
- Sub ring having no corresponding major-ring node: When a node's role is edge-node or assistant-node, this node is borne on the major-ring node; if there is no corresponding major-ring node to compulsorily create the sub-ring edge node or sub-ring assistant node, prompt information will appear (in this case, you can use the show command to browse the MEAPS state; if you find the basic information is complete but the state is init, it indicates that the configuration of the ring's node has not finished).
- Conflicts arising during control VLAN configuration: If the control VLAN, which is configured by a node, conflicts with other configured nodes, prompt information will appear (in this case, you can use the show command to browse the MEAPS state; if you find the basic information is complete but the state is init, it indicates that the configuration of the ring's node has not finished).
- When configuring the sub-ring node according to the major ring node, the id of the sub-ring node must be greater than the ID of the major ring node. Otherwise, here pops up a prompt.

Chapter 45 Unidirectional Link Detection (UDLD)

45.1 UDLD Overview

UDLD is a L2 protocol that monitors the physical location of the cable through the devices which are connected by optical cable or twisted-pair, and detects whether the unidirectional link exists. Only when the connected device supports UDLD can the unidirectional link be detected and shut down. The unidirectional link can cause a lot of problems, including the STP topology ring. Hence, when detecting a unidirectional link, UDLD will shut down the affected interface and notify uses. UDLD works with the physical-layer protocol mechanism to judge the status if the physical link. On the physical layer, the physical signals and incorrect detections are automatically negotiated and processed, while UDLD processes other matters, such as detecting the ID of a neighbor and shutting down the incorrect connection port. If you enable automatic negotiation and UDLD, the detection at layer 1 and layer 2 can prevent physical/logical links and other protocols' problems.

45.1.1 UDLD Mode

UDLD supports two modes, the normal mode (default) and the aggressive mode. In normal mode, UDLD can detect the existence of a unidirectional link according to the unidirectional services of the link. In aggressive mode, UDLD can detect not only the existence of a unidirectional link as in the previous mode but also connection interruption which cannot be detected by L1 detection protocols.

In **normal** mode, if UDLD determines that the connection is gone, UDLD will set the state of the port to **undetermined**, not to **down**. In **aggressive** mode, if UDLD determines that the link is gone and the link cannot be reconnected, it is thought that interrupted communication is a severe network problem and UDLD will set the state of the protocol to **linkdown** and the port is in **errdisable** state. No matter in what mode, if UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

In **aggressive** mode, UDLD can detect the following cases of the unidirectional link:

- On the optical fiber or the twisted pair, an interface cannot receive or transmit services.
- On the optical fiber or the twisted pair, the interface of one terminal is down and the interface of the other terminal is up.
- One line in the optical cable is broken, and therefore the data can only be transmitted or only be received.

In previous cases, UDLD will shut down the affected interface.

45.1.2 Running Mechanism

UDLD is a L2 protocol running on the LLC layer, which uses 01-00-0c-cc-cc-cc as its destination MAC address. SNAP HDLC is similar to 0x0111. When it runs with layer-1 FEFI and automatic negotiation, the completeness of a link in the physical layer and the logical link layer can be checked.

UDLD can provide some functions that FEFI and automatic negotiation cannot conduct, such as checking and caching the neighbor information, shutting down any mis-configured port and checking the faults and invalidation on the logical ports except the point-to-point logical ports.

UDLD adopts two basic mechanisms: learn the information about neighbors and save it in the local cache. When a new neighbor is detected or a neighbor applies for synchronizing the cache again, a series of UDLD probe/echo (hello) packets will be transmitted.

UDLD transmits the probe/echo packets on all ports and, when a UDLD echo information is received on the ports, a detection phase and an authentication process are triggered. If all effective conditions are satisfied (port is connected in

two directions and the cable is correctly connected), this port will be up. Otherwise, the port will be down.
Once a link is established and labeled as bidirectional, UDLD will transmit a probe/echo message every 15 seconds.

45.1.3 State of the Port

The UDLD interface may be in one of the following states:

Port state	Remark
Detection	Means that the interface is in detection state.
Unknown	Means that the interface is in unknown state, that is, it may be in detection state or it has not conducted detection.
Unidirectional	Means that the unidirectional connection has been detected.
Bidirectional	Means that the bidirectional connection has been detected.

45.1.4 Maintaining the Cache of the Neighbor

UDLD transmits the Probe/Echo packets regularly on each active interface to maintain the completeness of the neighbor's cache. Once a Hello message is received, it will be saved in the memory temporally and an interval that is defined by hold-time will also be saved. If the hold-time times out, the corresponding cache is fully cleared. If a new Hello message is received in the hold-time, the new Hello message will replace the old one and the timer will be reset to zero.
Once a UDLD-running interface is disabled or the device on the interface is restarted, all the caches on the interface will be removed to maintain the completeness of the UDLD cache. UDLD transmits at least one message to notify the neighbor to remove the corresponding cache items.

45.1.5 Echo Detection

The echo mechanism is the basis of the detection algorithm. Once a UDLD device learns a new neighbor or another synchronization request from an asynchronous neighbor, it will start or restart the detection window of the local terminal and transmit an echo message for full agreement. Because all neighbors are demanded a corresponding action, the echo sender expects an **echos** message. If the checkup window is over before a legal echo is received, this link is thought to be a unidirectional one. In this case, link reconnection will be triggered or the **link down** process on the port is enabled.

45.2 UDLD Configuration Task List

- Globally Enabling or Disabling UDLD
- Enabling or Disabling the UDLD Interface
- Setting the Message Interval of the Aggressive Mode
- Restarting the Interface Shut Down by UDLD
- Displaying the UDLD State

45.3 UDLD Configuration Tasks

45.3.1 Globally Enabling or Disabling UDLD

In global configuration mode, run the following command to enable the UDLD function of all interfaces.

Command	Purpose
udld [enable | aggressive]	Enables the UDLD modules of all interfaces in some mode.

In global configuration mode, run the following command to disable the UDLD function of all interfaces.

Command	Purpose
no udld [enable | aggressive]	Shuts down the UDLD modules of all interfaces.

Note: If you enable or disable the UDLD function in global configuration mode, the UDLD function will be performed on all interfaces.

UDLD of the Aggressive mode is a variation of UDLD, which can provide extra benefits. When UDLD is in aggressive mode and the port stops transmitting the UDLD packets, UDLD will try to establish a link with its neighbor again. If the times of tries exceed a certain number, the state of the port is changed into the Error-Disable state and the link of the port is down. When UDLD is running, the ports at both terminals should run in the same mode, or the expecting result cannot be obtained.

45.3.2 Enabling or Disabling the UDLD Interface

In interface configuration mode, run the following command to enable the UDLD function of an interface.

Command	Purpose
udld port [aggressive]	Enables the UDLD module of an interfaces in some mode. If the **aggressive** parameter is not entered, the UDLD function of the interface is enabled in **normal** mode; if the **aggressive** parameter is entered, the UDLD function of the interface is enabled in **aggressive** mode.

In interface configuration mode, run the following command to disable the UDLD function of an interface.

Command	Purpose
no udld port [aggressive]	Disables the UDLD module of the interface by entering the corresponding command in some mode.

NOTE:

When UDLD is running, the ports at both terminals should run in the same mode, or the expecting result cannot be obtained.

45.3.3 Setting the Message Interval of the Aggressive Mode

In global configuration mode, run the following command to set the message interval of the aggressive mode.

Command	Purpose
udld message *time*	Sets the message interval of the aggressive mode.

45.3.4 Restarting the Interface Shut Down by UDLD

In the EXEC mode, run the following command to restart the interface that is shut down by the UDLD module.

Command	Purpose
udld reset	Restarts the interface shut down by UDLD.

45.3.5 Displaying the UDLD State

Run the following command to display the states of the UDLD modules of all current interfaces.

Command	Purpose
show udld	Displays the states of the UDLD modules of all current interfaces.

Run the following command to display the state of the UDLD module of the specified interface.

Command	Purpose
show udld *interface*	Displays the state of the UDLD module of the specified interface.

The UDLD displaying command is used to browse the state and the mode of UDLD, the current detection state, the state of the current link and some information about the neighbors.

It is used to display the running states of the UDLD modules of the current interfaces.

```
Switch#show udld

Interface FastEthernet0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
```

```
Current bidirectional state: Bidirectional
Current operational state: Advertisment
Message interval: 15
Time out interval: 5
Entry 1
---
Expiration time: 42
Cache Device index: 1
Device ID: CAT0611Z0L9
Port ID: FastEthernet0/1
Neighbor echo 1 device: S35000202
Neighbor echo 1 port: FastEthernet0/1

Message interval: 15
Time out interval: 5
UDLD Device name: Switch

Interface FastEthernet0/2
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface FastEthernet0/3
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

.....
```

It is used to display the operational state of the UDLD module of the current interface.

```
Switch#show udld interface f0/1
Interface FastEthernet0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisment
Message interval: 15
Time out interval: 5
Entry 1
---
Expiration time: 42
Cache Device index: 1
Device ID: CAT0611Z0L9
Port ID: FastEthernet0/1
Neighbor echo 1 device: S35000202
Neighbor echo 1 port: FastEthernet0/1

Message interval: 15
Time out interval: 5
```

UDLD Device name: Switch

45.4 Configuration Example

45.4.1 Network Environment Requirements

Configure the UDLD protocol on the ports that connect two MY COMPANY S3524 switches.

45.4.2 Network Topology

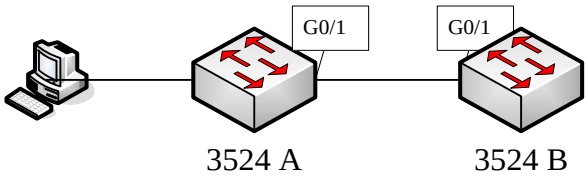


Figure 2 Network topology

45.4.3 Configuration Procedure

Configuring Switch A:
Switch_config#udld enable
Switch_config#interface g0/1
Switch_config_g0/1#udld port
Switch_config_g0/1#quit
Configuring Switch B:
Switch_config#udld enable
Switch_config#interface g0/1
Switch_config_g0/1#udld port
Switch_config_g0/1#quit

Entering the **show** command on Switch A:
Switch_config#show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Detection
Message interval: 15
Time out interval: 1
Entry 1

Expiration time: 44

Cache Device index: 1
Device ID: S35043000
Port ID: GigaEthernet0/1
Neighbor echo 1 device: S32030079
Neighbor echo 1 port: GigaEthernet0/1

Message interval: 15
Time out interval: 1
UDLD Device name: SwitchB
Switch_config#
Switch_config#show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Advertisment
Message interval: 15
Time out interval: 7
Entry 1

Expiration time: 43
Cache Device index: 1
Device ID: S35043000
Port ID: GigaEthernet0/1
Neighbor echo 1 device: S32030079
Neighbor echo 1 port: GigaEthernet0/1

Message interval: 15
Time out interval: 7
UDLD Device name: SwitchB
Switch_config#
Switch_config#show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisment
Message interval: 15
Time out interval: 15

Entry 1

Expiration time: 36

Cache Device index: 1

Device ID: S35043000

Port ID: GigaEthernet0/1

Neighbor echo 1 device: S32030079

Neighbor echo 1 port: GigaEthernet0/1

Message interval: 15

Time out interval: 15

UDLD Device name: SwitchB

Switch_config#

From the information above, you can find the three phases of the link state which UDLD detects:

- Detection phase: In this phase, the UDLD packets are transmitted every other second.
- Unknown phase: In this phase, the UDLD packets are transmitted every eight seconds.
- Known bidirectional/unidirectional connection phase: Once a link is established and labeled as bidirectional, UDLD will transmit a probe/echo message every 16 seconds.

Chapter 46 IGMP-snooping Configuration

46.1 IGMP-snooping Configuration Task

The task of IGMP-snooping is to maintain the relationships between VLAN and group address and to update simultaneously with the multicast changes, enabling switches to forward data according to the topology structure of the multicast group.

The main functions of IGMP-snooping are shown as follows:

1. Listening IGMP message;
2. Maintaining the relationship table between VLAN and group address;
3. Keeping the IGMP entity of host and the IGMP entity of router in the same state to prevent flooding from occurring.

Note:

Because igmp-snooping realizes the above functions by listening the **query** message and **report** message of igmp, igmp-snooping can function properly only when it works on the multicast router, that is, the switch must periodically receive the igmp **query** information from the router. The **router age** timer of igmp-snooping must be set to a time value that is bigger than the group query period of the multicast router connecting igmp-snooping. You can check the multicast router information in each VLAN by running **show ip igmp-snooping**.

- Enabling/Disabling IGMP-snooping of VLAN
- Adding/Deleting static multicast address of VLAN
- Configuring immediate-leave of VLAN
- Configuring Static Routing Interface of VLAN
- Configuring IPACL of Generating Multicast Forward Table
- Configuring the function to filter multicast message without registered destination address
- Configuring the Router Age timer of IGMP-snooping
- Configuring the Response Time timer of IGMP-snooping
- Configuring IGMP Querier of IGMP-snooping
- Configuring IGMP-snooping's Querier Time Timer
- Configuring data forwarding of IGMP-snooping's forward-l3-to-mrouter to router port
- Configuring sensitive mode and value for IGMP-snooping
- Configuring IGMP-snooping's v3-leave-check function
- Configuring IGMP-snooping's forward-wrongiif-within-vlan function
- Configuring IPACL function at IGMP-snooping's port
- Configuring maximum multicast IP address quantity function at IGMP-snooping's port
- Monitoring and maintaining IGMP-snooping
- IGMP-snooping configuration example

46.1.1 Enabling/Disabling IGMP-Snooping of VLAN

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping [vlan *vlan_id*]	Enables IGMP-snooping of VLAN.
no ip igmp-snooping [vlan *vlan_id*]	Resumes the default configuration.

If vlan is not specified, all vlans in the system, including vlans created later, can be enabled or disabled.

In the default configuration, IGMP-snooping of all VLANs is enabled, just as the **ip igmp-snooping** command is configured.

Note: IGMP-snooping can run on up to 16 VLANs.

To enable IGMP-snooping on VLAN3, you must first run **no ip IGMP-snooping** to disable IGMP-snooping of all VLANs, then configure **ip IGMP-snooping VLAN 3** and save configuration.

46.1.2 Adding/Deleting Static Multicast Address of VLAN

Hosts that do not support IGMP can receive corresponding multicast message by configuring the static multicast address.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* static *A.B.C.D* interface *intf*	Adds static multicast address of VLAN.
no ip igmp-snooping vlan *vlan_id* static *A.B.C.D* interface *intf*	Deletes static multicast address of VLAN.

46.1.3 Configuring immediate-leave of VLAN

When the characteristic immediate-leave is configured, the switch can delete the port from the port list of the multicast group after the switch receives the **leave** message. The switch, therefore, does not need to enable the timer to wait for other hosts to join the multicast. If other hosts in the same port belongs to the same group and their users do not want to leave the group, the multicast communication of these users may be affected. In this case, the **immediate-leave** function should not be enabled.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* immediate-leave	Configures the **immediate-leave** function of the VLAN.
no ip igmp-snooping vlan *vlan_id* immediate-leave	Sets immediate-leave of VLAN to its default value.

The **immediate-leave** characteristic of VLAN is disabled by default.

46.1.4 Configuring immediate-leave of port

When the characteristic immediate-leave is configured on a port, the switch can delete the port from the port list of the multicast group after the switch receives the **leave** message. The switch, therefore, does not need to enable the timer to wait for other hosts to join the multicast. If other hosts in the same port belongs to the same group and their users do not want to leave the group, the multicast communication of these users may be affected. In this case, the **immediate-leave** function should not be enabled.

The immediate-leave configuration of the port and the immediate-leave configuration of the VLAN work simultaneously.

Perform the following configuration in interface configuration mode:

Command	Description
ip igmp-snooping immediate-leave	Configures the **immediate-leave** function of the port.
no ip igmp-snooping immediate-leave	Sets immediate-leave of the port to its default value.

By default, the immediate-leave feature of a port is disabled.

46.1.5 Configuring Static Routing Interface of VLAN

Configure the static routing interface and send the multicast packet to the routing port. The switch will send the multicast report packets to all routing ports in vlan.
Run following commands in the global configuration mode:

Command	Purpose
ip igmp-snooping vlan *vlan_id* mrouter interface *intf*	Add the static routing port of VLAN.
no ip igmp-snooping vlan *vlan_id* mrouter interface *intf*	Delete the static routing port of VLAN.

46.1.6 Configuring IPACL of Generating Multicast Forward Table

Run following commands in global configuration mode to configure IPACl. Thus, The rules and limitations of generating the multicast forwarding table after receiving packets of igmp report can be set.

Command	Purpose
ip igmp-snooping policy *word*	Adds IPACL in generating multicast forwarding table.
no ip igmp-snooping policy	Deletes IPACL in generating multicast forwarding table.

46.1.7 Configuring the Function to Filter Multicast Message Without Registered Destination Addresss

When multicast message target fails to be found (DLF, the destination address is not registered in the switch chip through igmp-snooping), the default process method is to send message on all ports of VLAN.Through configuration, you can change the process method and all multicast messages whose destination addresses are not registered to any port will be dropped.

Command	Description
ip igmp-snooping dlf-drop	Drops multicast message whose destination fails to be found.
no ip igmp-snooping dlf-drop	Resumes the fault configuration (forward).

NOTE:

1. The attribute is configured for all VLANs.
2. The default method for the switch to handle this type of message is forward (message of this type will be broadcasted within VLAN).

46.1.8 Configuring Router Age Timer of IGMP-snooping

The **Router Age** timer is used to monitor whether the IGMP inquirer exists. IGMP inquirers maintains multicast addresses by sending **query** message. IGMP-snooping works through communication between IGMP inquier and host.
Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer router-age *timer_value*	Configures the value of Router Age of IGMP-snooping.
no ip igmp-snooping timer router-age	Resumes the default value of Router Age of IGMP-snooping.

NOTE:
For how to configure the timer, refer to the query period setup of IGMP inquirer. The timer cannot be set to be smaller than query period. It is recommended that the timer is set to three times of the query period.
The default value of Router Age of IGMP-snooping is 260 seconds.

46.1.9 Configuring Response Time Timer of IGMP-Snooping.

The **response time** timer is the upper limit time that the host reports the multicast after IGMP inquirer sends the **query** message. If the **report** message is not received after the timer ages, the switch will delete the multicast address.
Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer response-time timer_value	Configures the value of Response Time of IGMP-snooping.
no ip igmp-snooping timer response-time	Resumes the default value of Response Time of IGMP-snooping.

NOTE:
The timer value cannot be too small. Otherwise, the multicast communication will be unstable.
The value of Response Time of IGMP-snooping is set to 15 seconds.

46.1.10 Configuring Querier of IGMP-Snooping

If the multicast router does not exist in VLAN where IGMP-snooping is activated, the **querier** function of IGMP-snooping can be used to imitate the multicast router to regularly send IGMP **query** message. (The function is global, that is, it can be enabled or disabled in VLAN where IGMP-snooping is globally enabled)

When the multicast router does not exist in LAN and multicast flow does not need routing, the automatic query function of the switch can be activated through IGMP snooping, enabling IGMP snooping to work properly.
Perform the following configuration in global configuration mode:

Command	Description
[no] ip igmp-snooping querier [address *[ip_addr*]	Configures the querier of IGMP-snooping. The optional parameter **address** is the source IP address of **query** message.

The **IGMP-snooping querier** function is disabled by default. The source IP address of fake **query** message is 10.0.0.200 by default.

NOTE:

If the querier function is enabled, the function is disabled when the multicast router exists in VLAN; the function can be automatically activated when the multicast router times out.

46.1.11 Configuring IGMP-snooping's Querier Time Timer

Querier Time Timer is the time interval when switch as local IGMP querier sends messages. Timer broadcasts query message within VLAN after aging.
Configure as following under global configuration mode:

Command	Operation
ip igmp-snooping querier querier-timer *timer_value*	Configuring the value of IGMP-snooping's Querier Time
no ip igmp-snooping querier querier-timer	Recovering IGMP-snooping's Querier Time as default

By default IGMP-snooping querier is shut down. The default time interval of Query messages is 200 seconds.

NOTE:

If Querier function is initiated, querier-timer should not be set as too long. In subnet if there are other switches with querier initiated, long querier-timer (longer than other switch's router-age) would lead to the instablization of querier selection in subnet.

46.1.12 Configuring data forwarding of IGMP-snooping's forward-l3-to-mrouter to router port

If L3 multicast feature is initiated and igmp-snooping does not join messages to downstream port, only downstream vlan port can be learnt by multicast route. If forward-l3-to-mrouter function is intiated, all the downstream router ports can be learnt. Data messages could be sent to multicast router pot registered by PIM-SM message not broadcasting messages to all downstream physical port. The command is mainly used under the following conditions.
When multiple switches initiate L3 multicast cascadingly, the upstream device can only learn downstream vlan ports by multicast router protocol. The upstream and downstream devices do not have interactive igmp messages, therefore, the upstream devices' snooping cannot learn the specific physical ports connected with downstream devices. When upstream devices forward multicast flows, they would send them to all physical port in vlan. When this function is initiated, messages could be forwarded to physical ports which connect with downstream devices, and messages would not be

broadcasted in downstream vlan.

Configure as following under global configuration mode:

Command	Operation
[no] ip igmp-snooping forward-l3-to-mrouter	Configuring IGMP-snooping's forward-l3-to-mrouter function.

Under default condition, IGMP-snooping forward-l3-to-mrouter is shut down

NOTE:

This command could forward data messages to multicast router port, but switching chip has restraining function on source data port. Therefore, messages would not be forwarded to source data port, but only to downstream router port registered by PIM-SM.

46.1.13 Configuring sensitive mode and value for IGMP-snooping

If IGMP-snooping's sensitive mode is enabled, when port at trunk mode is shut down, set router-age time of mrouter at active status as sensitive value, and send out query message quickly.

Configure as following under global configuration mode:

Command	Operation
[no] ip igmp-snooping sensitive [value [3-30]]	Configuring IGMP-snooping's sensitive and value could be router-age time of currently active mrouter.

By default IGMP-snooping sensitive is disabled.

NOTE:

When it is sensitive mode, sensitive value is used to update router-age aiming at current one time period. Next time, route-age is recovered as configured time router-age time.

46.1.14 Configuring IGMP-snooping's v3-leave-check function

If IGMP-snooping's v3-leave-check feature is enabled, send special query message after receiving v3's leave message. Otherwise, no operation is processed.

Configure as following under global configuration mode:

Command	Operation
[no] ip igmp-snooping v3-leave-check	Configuring IGMP-snooping's v3-leave-check. Send special query message after receiving v3 leave message.

46.1.15 Configuring IGMP-snooping's forward-wrongiif-within-vlan function

If IGMP-snooping's forward-wrongiif-within-vlan function is enabled, do L2 forwarding of the multicast data message received from wrong vlan interface port within source vlan. Forward messages to the group member ports in the vlan. Otherwise, drop messages.

Configure as following under global configuration mode:

Command	Operation
[no] ip igmp-snooping forward-wrongiif-within-vlan	Configuring IGMP-snooping's forward-wrongiif-within-vlan and forwarding relative group member ports within the vlan

By default IGMP-snooping forward-wrongiif-within-vlan is enabled.

NOTE:

Command ip igmp-snooping forward-wrongiif-within-vlan is only meaningful when L3 multicast is enabled.

46.1.16 Configuring IGMP-snooping's IPACL function at port

If IGMP-snooping's IPACL function at port is enabled, use IPACL at port to assign whether messages of some multicast IP address need to be dealt with or ignored.

Configure as following under physical port configuration mode:

Command	Purpose
ip igmp-snooping policy *word*	Adding multicast message's IPACL which need to be dealt with port.
no ip igmp-snooping policy	Deleteding multicast message's IPACL which need to be dealt with port.

46.1.17 Configuring IGMP-snooping's multicast filtering in VLAN

If IGMP-snooping multicast filtering in the VLAN is enabled, only the multicast group report request in the filtering list will be accepted and added to the group in the VLAN, otherwise it will be discarded and no group will be added.

Configure as following in global configuration mode:

Command	Purpose
ip igmp-snooping vlan *value* filter *vlanid-list*	Configure IGMP-snooping's multicast filtering in VLAN. The parameter vlanid-list is VLAN ID list connected with "," and "-". Note that "," and "-" must be followed by at least one space.
ip igmp-snooping vlan *value* filter *vlanid-list*	Remove multicast filtering in VLAN

46.1.18 Configuring maximum multicast IP address quantity function at IGMP-snooping's port

If configuring the maximum multicast IP address quantity at IGMP-snooping port, the quantity of applied groups at the port would be judged whether it is beyond the configured maximum quantity when IGMP-snooping generates forwarding entry. If it is beyond the maximum quantity, the port's entry would not be generated.

Configure as following under physical port configuration mode:

Command	Operation
[no] ip igmp-snooping limit [value [1-2048]]	configuring the maximum multicast IP address quantity at IGMP-snooping port

By default the maximum quantity is 2048 at IGMP-snooping.

46.1.19 Configuring IGMP-snooping's report-suppression function

If the report-suppression function of IGMP-snooping is configured, in the same VLAN, regardless of whether the client initiates the request in the initial state or responds to the query, the switch forwards limited number to the mrouter port. The number of forwarding is determined by the parameter after **max-number**, and the range is 1-5. If the max-number keyword is omitted, the number of forwarding is 1 by default.

When the IGMP Snooping function is normal, this configuration can reduce the processing cost of the local switch and the upstream switch, and save the bandwidth for forwarding report packets.

Configure as following in global configuration mode:

Command	Operation
[no] ip igmp-snooping report-suppression [max-number value [1-5]]	Configure the IGMP-snooping report-suppression and its report maximum forwarding number.

By default, IGMP-snooping report-suppression function is disabled

If **ip igmp-snooping report-suppression** is configured without keyword max-number, the number of report forwards is 1 by default.

46.1.20 Configuring IGMP-snooping's proxy-leave function

If the IGMP-snooping proxy-leave function is configured, in the same VLAN, the switch sends the leave message of the multicast group to the upstream device only after all members of a multicast group have truly left the group.

When the IGMP Snooping function is normal, this configuration can reduce the processing cost of the local switch and the upstream switch, and save the bandwidth for forwarding leave packets.

Configure as following in global configuration mode:

Command	Operation
[no] ip igmp-snooping proxy-leave	Configure IGMP-snooping's proxy-leave function

By default, IGMP-snooping proxy-leave function is disabled.

46.1.21 Monitoring and Maintaining IGMP-Snooping

Perform the following operations in management mode:

Command	Description
show ip igmp-snooping	Displays IGMP-snooping configuration information.
show ip igmp-snooping timer	Displays the clock information of IGMP-snooping.

show ip igmp-snooping group	Displays information about the multicast group of IGMP-snooping.
show ip igmp-snooping group interface	Displays information about the multicast group of IGMP-snooping in port.
show ip igmp-snooping statistics [message|packet|hardware|vlan *vlanid*]	Displays statistics information about IGMP-snooping.
show ip igmp-snooping vlan	Displays vlan information of IGMP-snooping.
[no] debug ip igmp-snooping [packet | timer | event | error]	Enables and disables packet/clock debug/event/mistake print switch of IGMP-snooping. If the debug switch is not specified, all debug switches will be enabled or disabled.

Display VLAN information about IGMP-snooping running:

```
switch # show ip igmp-snooping
Global IGMP snooping configuration:
---------------------------------
Globally enable     : Enabled
VLAN nodes          : 1,50,100,200,400,500
Dlf-frames filtering : Disabled
Sensitive           : Disabled
Querier             : Enabled
Querier address     : 10.0.0.200
Querier interval    : 140 s
Router age          : 260 s
Response time       : 15 s

vlan_id   Immediate-leave   Ports   Router Ports
-----------------------------------------------------------------
   1       Disabled       5-10    SWITCH(querier);
   50      Disabled       1-4     SWITCH(querier);
100        Disabled       NULL    SWITCH(querier);G0/1(static);
   200     Disabled       NULL    SWITCH(querier);
   400     Disabled       NULL    SWITCH(querier);
   500     Disabled       NULL    SWITCH(querier);
```

Display information about the multicast group of IGMP-snooping:

```
switch# show ip igmp-snooping group
The total number of groups      2

Vlan Group      Type Port(s)
---- ---------- ---- ------------------------------------------------------
   1 226.1.1.1      IGMP G0/1G0/3
   1 225.1.1.16     IGMP G0/1G0/3
```

Display the IGMP-snooping multicast group information added on the port:

```
Switch#show ip igmp-snooping group interface g0/4

Number of joined groups: 1
```

```
Vlan Group          Mode    Source Num
---- --------------- ------- ----------
2 230.1.1.1       Exclude   0
```

Display IGMP-snooping timer:

```
switch#show ip igmp-snooping timers
vlan 1 router age : 251 Indicating the timeout time of the router age timer
vlan 1 multicast address 0100.5e00.0809 response time : 1  Indicating the period from when the last multicast group query message is received to the current time; if no host on the port respond when the timer times out, the port will be deleted..
```

Display IGMP-snooping statistics:

```
Switch_config#show ip igmp-s statistics

IGMP Snooping Message Statistics
-----------------------------------
L2 main messages sent OK    : 75
L2 main messages sent failed  : 0
L2 packets received          : 72
L2 packets sent              : 72
L2 packets sent failed        : 0
L2 link-status messages       : 3
IGMP Snooping messages received: 79
IGMP packet messages received  : 72

IGMP Snooping Packet Statistics
----------------------------------------
Received packets               : 72
IGMP packets                   : 29
M-routing protocol packets         : 0
Other packets                  : 43
Received IGMP general queries     : 0
Received IGMPv2 specific queries   : 0
Received IGMPv3 g specific queries  : 0
Received IGMPv3 gs specific queries: 0
Received IGMPv1 reports          : 0
Received IGMPv2 reports          : 0
Received IGMP leaves             : 0
Received IGMPv3 reports          : 29
Flooded queries                : 0
Forwarded and proxy-sent reports   : 0
Forwarded and proxy-sent leaves    : 0

IGMP Snooping Hardware Operation Statistics
-----------------------------------------
Total              : 0   Total number of hardware operations
Succeeded          : 0   Number of successful hardware operations
Failed             : 0   Number of failed hardware operations
Report/leave processing: 0    Number of hardware operations processing report and leave
Response timer expiring: 0    Number of hardware operations in response to timer aging
Group creating/updating: 0  Number of hardware operations resulting from creating and updating groups
```

```
Group deleting       : 0  Number of hardware operations caused by deleting a group
```

Display VLAN information of IGMP-snooping:

```
Switch_config#show ip igmp-snooping vlan
vlan_id   Immediate-leave   Ports   Router Ports
-----------------------------------------------------------------
    1       Disabled        7-30
    2       Disabled        NULL
```

Debug the message timer of IGMP-snooping:

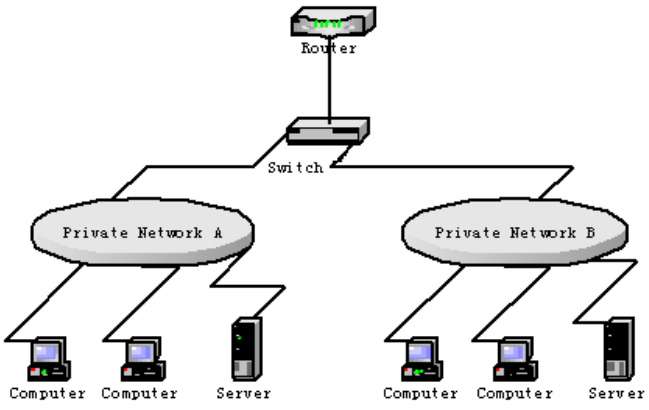
```
switch#debug ip igmp-snooping packet
Jan  1 02:22:28 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:28 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:29 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:29 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:38 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:38 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:39 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:39 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:11 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:11 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:12 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:12 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
```

Debug the message timer of IGMP-snooping:

```
switch#debug ip igmp-snooping timer
Jan  1 02:30:36 IGMP-snooping: Vlan 1 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 100 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 200 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 400 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 500 router on interface (null) expiry. Inquerying the response timer
expiry
```

46.1.22 IGMP-Snooping Configuration Example

Figure 1 shows network connection of the example.



Configuring Switch

1. Enable IGMP-snooping of VLAN 1 connecting Private Network A.
   Switch_config#ip igmp-snooping vlan 1
2. Enable IGMP-snooping of VLAN 2 connecting Private Network B.
   Switch_config#ip igmp-snooping vlan 2

Chapter 47 IGMP-Proxy Configuration

47.1 IGMP-proxy Configuration Tasks

The IGMP Proxy allows the VLAN where the multicast user is located to receive the multicast source from other VLANs. The IGMP Proxy runs on layer 2 independently without other multicast routing protocols. IGMP proxy will be transmitted by the IGMP packets of the proxied VLAN to the proxying VLAN and maintain the hardware forward table of the multicast user of the agent VLAN according to these IGMP packets. IGMP proxy divides different VLANs into two kinds: proxied VLANs and proxying VLANs. The downstream multicast VLANs can be set to the proxied VLANs, while the upstream multicast VLANs can be set to the proxying VLANs.

Although IGMP proxy is based on IGMP snooping, two are independent in application; IGMP Snooping will not be affected when IGMP proxy is enabled or disabled, while IGMP proxy can run only when IGMP Snooping is enabled.

IGMP proxy cannot be used unless the following conditions are met:

1. L3 switch
2. Avoiding to enable IP multicast routing at the same time
3. Preventing a vlan to act as downstream vlan and also upstream vlan

- Enabling/Disabling IGMP-Proxy
- Adding/deleting VLAN agent relationship
- Adding/deleting static multicast source entries
- Monitoring and Maintaining IGMP-Proxy
- Setting the Example of IGMP Proxy

47.1.1 Enabling/Disabling IGMP-Proxy

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-proxy enable	Enables IGMP proxy.
no ip igmp-proxy enable	Resumes the default settings.

NOTE:

IGMP-proxy cannot be enabled after IP multicast-routing is enabled. The previously enabled IGMP proxy is automatically shut down if IP multicast routing is enabled. The shutdown of ip multicast-routing will not lead to the automatic enablement of IGMP proxy.

47.1.2 Adding/Deleting VLAN Agent Relationship

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-proxy agent-vlan a*vlan_map* client-vlan map c*vlan_map*	Adds the agent VLAN (avlan_map) to manage the represented vlan (cvlan_map).

no ip igmp-proxy agent-vlan a*vlan_map* client-vlan map c*vlan_map*	Deletes the agent relationship.

NOTE:

1. The represented VLAN cannot be configured before vlan is designated by avlan_map; also, the agent VLAN cannot be configured before cvlan_map.
2. The represented and agent VLANs must accept the control of IGMP-Snooping.

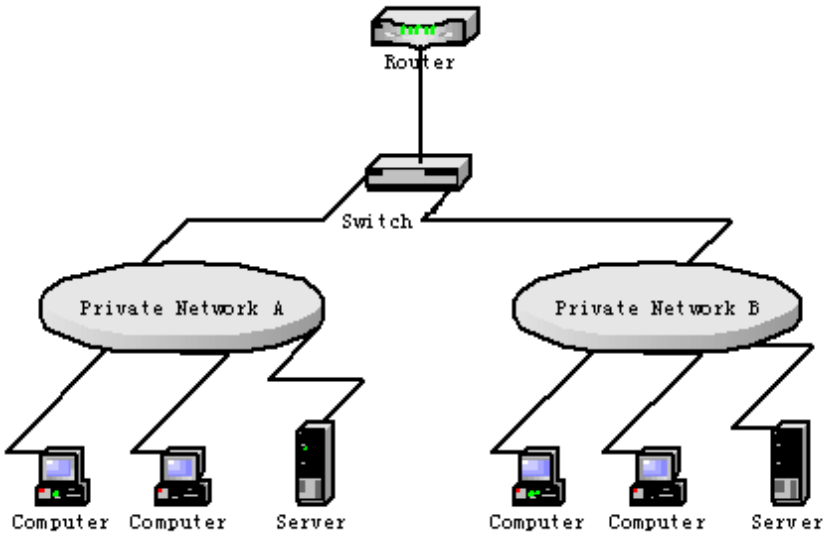
47.1.3 Monitoring and Maintaining IGMP-Proxy

Run the following commands in EXEC mode:

Command	Operation
show ip igmp-proxy	Displays the information about IGMP proxy.
[**no**] **debug ip igmp-proxy** *[error | event | packet]*	Enables or disables the IGMP-proxy debug switch.

47.1.4 IGMP-Proxy Configuration Example

The network topology is shown in figure 1.



Switch configuration:

1. Enable IGMP snooping and IGMP proxy.

   Switch_config#ip igmp-snooping

   Switch_config#ip igmp-proxy enable

2. Add VLAN 2 (in Private Network A) as the agent VLAN of the represented VLAN 3 (in Private Network B).

   Switch_config#ip igmp-proxy agent-vlan 2 client-vlan map 3

Chapter 48 MLD-Snooping Configuration

48.1 IPv6 Multicast Overview

The task of MLD snooping is to maintain the forwarding relationship of IPv6 group addresses in VLAN and synchronize with the change of the multicast group, enabling the data to be forwarded according to the topology of the multicast group. Its functions include monitoring MLD-snooping packets, maintaining the table between group address and VLAN, keep the MLD-snooping host the same with the MLD-snooping router and solve the flooding problems.

When a L2 device has not got MLD snooping run, the multicast data will be broadcast at the second layer; when the L2 device gets MLD snooping run, the multicast data of the known multicast group will not be broadcast at the second layer but be sent to the designated receiver, and the unknown multicast data will be dropped.

NOTE:

Because MLD-snooping solves the above-mentioned problems by monitoring the Query or Report packets of MLD-Snooping, MLD snooping can work normally only when there exists the multicast router, which means the switch must periodically receive the MLD-Snooping query message from the router. Therefore, the router age timer setting of MLD-Snooping must be larger than the group query period of the multicast router connected to it. You can see the multicast router information in each vlan, using the **show ipv6 mdl-snooping** command.

48.2 MLD-Snooping Multicast Configuration Tasks

- Enabling/Disabling MLD-Snooping
- Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group
- Adding/Deleting the Static Multicast Address of VLAN
- Setting Router Age Timer of MLD-Snooping
- Setting Response Time Timer of MLD-Snooping
- Setting the Port of the Static Multicast Router
- Setting the Immediate Leave Function
- Monitoring and Maintaining MLD-Snooping

48.2.1 Enabling/Disabling MLD-Snooping Multicast

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping	Enables MLD snooping multicast.
no ipv6 mld-snooping	Disables MLD snooping.

NOTE:

After MLD-Snooping is enabled and the multicast packets fail to be found, the multicast packets whose destination addresses are not registered are dropped.

48.2.2 Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping solicitation	Enables the solicitation of hardware forward of multicast group.
no ipv6 mld-snooping solicitation	Disables the solicitation of hardware forward of multicast group.

48.2.3 Adding/Canceling the Static Multicast Address of VLAN

The static multicast address configuration allows some hosts that do not support the MLD-Snooping protocol to receive the corresponding group packets.

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping vlan *vlan_id* static *X:X:X:X::X* interface *intf_name*	Adds the static multicast address of VLAN.
no ipv6 mld-snooping vlan *vlan_id* static *X:X:X:X::X* interface *intf_name*	Removes the static multicast address of VLAN.

48.2.4 Setting Router Age Timer of MLD-Snooping

The Router Age timer is used to monitor the existence of an MLD-Snooping querying party. The MLD-Snooping querying party maintains and manages the multicast address by sending query packets. MLD-Snooping relies on the communication between the MLD-Snooping querying party and the host.

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping timer router-age *timer_value*	Sets the router age of MLD-Snooping.
no ipv6 mld-snooping timer router-age	Resumes the default router age of MLD-Snooping.

NOTE: The settings of this timer shall refer to the query period settings of MLD-Snooping and be larger than the query period. It is recommended to set the router age timer to be triple of the query period.

The default router age of MLD snooping is 260 seconds.

48.2.5 Setting Response Time Timer of MLD-Snooping

Response Time timer is the latest Time for the host to report multicast after the MLD-Snooping interrogator sends the query packet. If the report message has not been received any packet after the timer aging, the switch will delete the multicast address.

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping timer response-time *timer_value*	Sets the response time of MLD-Snooping.
no ipv6 mld-snooping timer response-time	Resumes the default response time of MLD-Snooping.

NOTE:

The value of the timer cannot be set too small, or the multicast communication may be unstable.

The default response time of MLD snooping is 10 seconds.

48.2.6 Setting Querier of MLD-Snooping

If there is no multicast router in enabling VLAN with MLD-snooping, enable Querier of MLD-snooping module (which acts as a virtualized multicast router) to forward IGMP group query packets regularly. (The function can only be enabled or disabled when all VLANs enable MLD-snooping)

When there is no multicast router in the LAN and the multicast flow has no need for routing, run **MLD-snooping querier** command to activate the self-query of the switch.

Run following command in global configuration mode:

Command	Purpose
[no] ipv6 mld-snooping querier [address *[ip_addr]*]	Sets Querier of MLD-snooping. Selects the address of the optional parameter as the source IP of the Query packet.

IGMP-snooping querier is disabled by default. The source IP address of the fake Query packet is FE80::3FF:FEFE:FD00:1.

NOTE:

Enable Querier, if there is a multicast router in the VLAN, the function becomes invalid automatically; if the multicast router is timeout, the function become valid automatically.

48.2.7 Setting the Port of the Static Multicast Router

Once a port is configured as a static multicast router port, all MLD-Snooping report and done messages received are forwarded to that port.

Run the following commands in global configuration mode.

Command	Operation
ipv6 mld-snooping vlan *WORD* mrouter interface *inft_name*	Sets the static multicast router's port of MLD snooping in Vlan **word**.
no ipv6 mld-snooping vlan *WORD* mrouter interface *inft_name*	Deletes the static multicast router's port of MLD snooping in Vlan **word**.

48.2.8 Enabling/Disabling Immediate Leave

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping vlan *WORD* immediate-leave	Enables the immediate-leave functionality.
no ipv6 mld-snooping vlan *WORD* immediate-leave	Resumes the default settings.

48.2.9 Monitoring and Maintaining MLD-Snooping Multicast

Run the following commands in EXEC mode:

Command	Operation
show ipv6 mld-snooping	Displays the configuration of MLD-Snooping.
show ipv6 mld-snooping timer	Displays the clock of MLD-Snooping.
show ipv6 mld -snooping groups	Displays the multicast group of MLD-Snooping.
show ipv6 mld-snooping statistics	Displays the statistics information of MLD-Snooping.
show ipv6 mld-snooping vlan	Displays the configuration of MLD-Snooping in VLAN.
show ipv6 mld-snooping mac	Displays the multicast MAC addresses recorded by MLD snooping.

The MLD-Snooping information is displayed below:

```
#show ipv6 mld-snooping

Global MLD snooping configuration:
------------------------------------
Globally enable     : Enabled
Querier             : Enabled
Querier address     : FE80::3FF:FEFE:FD00:1
Router age          : 260 s
Response time       : 10 s
Handle Solicitation  : Disabled

Vlan 1:
----------
Running
Routers: SWITCH(querier);
```

The multicast group of MLD-Snooping is displayed blow:

```
#show ipv6 mld--snooping groups

Vlan Group          Type Port(s)
---- --------------- ---- -----------------------------------
1 FF02::1:FF32:1B9B MLD  G2/23
1 FF02::1:FF00:2  MLD  G2/23
1 FF02::1:FF00:12 MLD  G2/23
```

```
1 FF02::1:FF13:647D MLD  G2/23
2 FF02::1:FF00:2  MLD  G2/22
2 FF02::1:FF61:9901 MLD  G2/22
```

The timer of MLD-Snooping is displayed blow:

```
Switch#show ipv6 mld-snooping timer

vlan 1 Querier on port 0 : 251
#
```

Querier on port 0: 251 meaning the router age timer times out.

vlan 2 multicast address 3333.0000.0005 response time : This shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

The MLD-snooping statistics information is displayed below:

```
#show ipv6 mld-snooping statistics
vlan 1
------------
v1_packets:0       quantity of v1 packets
v2_packets:6       quantity of v2 packets
v3_packets:0       quantity of v3 packets
general_query_packets:5    Quantity of general query packets
special_query_packets:0    Quantity of special query packets
listener_packets:6     Quantity of Report packets
done_packets:0    Quantity of Leave packets
err_packets:0     Quantity of error packets
```

The MLD-Snooping proxying is displayed below:

```
#show ipv6 mld-snooping mac
Vlan Mac              Ref Flags
---- ---------------- ---- ------
1 3333:0000:0001    1   2
2 3333:ff61:9901    1   0
   FF02::1:FF61:9901
1 3333:0000:0002    1   2
1 3333:ff00:0002    1   0
   FF02::1:FF00:2
1 3333:ff00:0012    1   0
   FF02::1:FF00:12
1 3333:ff13:647d    1   0
   FF02::1:FF13:647D
1 3333:ff32:1b9b    1   0
   FF02::1:FF32:1B9B
2 3333:ff00:0002    1   0
   FF02::1:FF00:2
1 3333:ff00:0001    1   2
1 3333:ff8e:7000    1   2
```

Chapter 49 OAM Configuration

49.1 OAM Overview

EFM OAM of IEEE 802.3ah provides point-to-point link trouble/performance detection on the single link. However, EFM OAM cannot be applied to EVC and so terminal-to-terminal Ethernet monitoring cannot be realized. OAM PDU cannot be forwarded to other interfaces. Ethernet OAM regulated by IEEE 802.3ah is a relatively slow protocol. The maximum transmission rate is 10 frames per second and the minimum transmission rate is 1 frame per second.

49.1.1 OAM Protocol's Attributes

- Supporting Ethernet OAM devices and OAM attributes

The Ethernet OAM connection process is called as the Discovery phase when the OAM entity finds the OAM entity of the remote device and a stable session will be established. During the phase, the connected Ethernet OAM entities report their OAM mode, Ethernet OAM configuration information and local-node-supported Ethernet OAM capacity to each other by interacting the information OAM PDU. If the loopback configuration, unidirectional link detection configuration and link-event configuration have been passed on the Ethernet OAM of the two terminals, the Ethernet OAM protocol will start working on the link layer.

- Link monitoring

The Ethernet OAM conducts the link monitoring through Event Notification OAM PDU. If the link has troubles and the local link monitors the troubles, the local link will transmits Event Notification OAM PDU to the peer Ethernet OAM to report the normal link event. The administrator can dynamically know the network conditions through link monitoring. The definition of a normal link event is shown in table 1.

Normal Link Event	Definition
Period event of error signal	Specifies the signal number *N* as the period. The number of error signals exceeds the defined threshold when *N* signals are received.
Error frame event	The number of error frames exceeds the defined threshold during the unit time.
Period event of error frame	Specifies the frame number *N* as the period. The number of error frames exceeds the defined threshold when *N* frames are received.
Second frame of error frame	Specifies that the number of seconds of the error frame exceeds the defined threshold in the designated *M* second.

Table 1 Definition of the normal link event

- Remote trouble indication

It is difficult to check troubles in the Ethernet, especially the case that the network performance slows down while physical network communication continues. OAM PDU defines a flag domain to allow Ethernet OAM entity to transmit the trouble information to the peer. The flag can stand for the following emergent link events:

- Link Fault: The physical layer detects that the reception direction of the local DTE has no effect. If troubles occur, some devices at the physical layer support unidirectional operations and allows trouble notification from remote OAM.
- Dying Gasp: If an irrecoverable local error occurs, such as OAM shutdown, the interface enters the error-disabled state and then is shut down.
- Critical Event: Uncertain critical events occur (critical events are specified by the manufacturer).

Information OAM PDU is continuously transmitted during Ethernet OAM connection. The local OAM entity can report local

critical link events to remote OAM entity through Information OAM PDU. The administrator thus can dynamically know the link's state and handle corresponding errors in time.

- Remote loopback

OAM provides an optional link-layer-level loopback mode and conducts error location and link performance testing through non-OAM-PDU loopback. The remote loopback realizes only after OAM connection is created. After the OAM connection is created, the OAM entity in active mode triggers the remote loopback command and the peer entity responses the command. If the remote terminal is in loopback mode, all packets except OAM PDU packets and Pause packets will be sent back through the previous paths. Error location and link performance testing thus can be conducted. When remote DTE is in remote loopback mode, the local or remote statistics data can be queried and compared randomly. The query operation can be conducted before, when or after the loopback frame is transmitted to the remote DTE. Regular loopback check can promptly detect network errors, while segmental loopback check can help locating these network errors and then remove these errors.

- Round query of any MIB variables described in chapter 30 of *802.3*.

49.1.2 OAM Mode

The device can conduct the OAM connection through two modes: active mode and passive mode. The device capacity in different mode is compared in table 2. Only OAM entity in active mode can trigger the connection process, while the OAM entity in passive mode has to wait for the connection request from the peer OAM entity. After the remote OAM discovery process is done, the local entity in active mode can transmit any OAM PDU packet if the remote entity is in active mode, while the local entity's operation in active mode will be limited if the remote entity is in passive mode. This is because the device in active mode does not react on remote loopback commands and variable requests transmitted by the passive remote entity.

Capacity	Active Mode	Passive Mode
Initializing the Ethernet OAM discovery process	Yes	No
Responding to the OAM discovery initialization process	Yes	Yes
Transmitting the Information OAM PDU packet	Yes	Yes
Permitting to transmit the Event Notification OAM PDU packet	Yes	Yes
Allowing to transmit the Variable Request OAM PDU packet	Yes	No
Allowing to transmit Variable Response OAM PDU packet	Yes	Yes
Allowing to transmit the Loopback Control OAM PDU packet	Yes	No
Responding to Loopback Control OAM PDU	Yes, but the peer terminal must be in active mode.	Yes
Allowing to transmit specified OAM PDU	Yes	Yes

Table 2 Comparing device capacity in active and passive modes

After the Ethernet OAM connection is established, the OAM entities at two terminals maintain connection by transmitting the Information OAM PDU packets. If the Information OAM PDU packet from the peer OAM entity is not received in five seconds, the connection times out and a new OAM connection then requires to be established.

49.1.3 Components of the OAM Packet

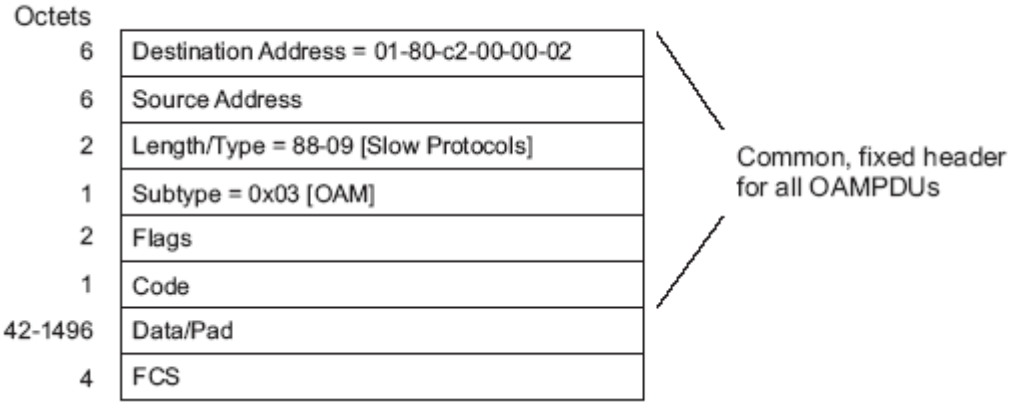


Figure 1 Components of the OAM packet

The following are the meanings of the fields of the OAM packet:

- Destination address: means the destination MAC address of the Ethernet OAM packet.
- Source address: means the source MAC address of the Ethernet OAM packet. It is the MAC address of the transmitter terminal's port and also a unicast MAC address.
- Length/Type: Always adopts the Type encoding. The protocol type of the Ethernet OAM packet is 0x8809.
- Subtype： The subtype of the protocol for Ethernet OAM packets is 0x03.
- Flags: a domain where the state of Ethernet OAM entity is shown
- Code: a domain where the type of the OAMPDU packet is shown
- Data/Pad: a domain including the OAMPDU data and pad values
- FCS: checksum of the frame

CODE	OAMPDU
00	Information
01	Event Notification
02	Variable Request
03	Variable Response
04	Loopback Control
05-FD	Reserved
FE	Organization Specific
FF	Reserved

Table 3 Type of the CODE domain

The Information OAM PDU packet is used to transmit the information about the state of the OAM entity to the remote OAM entity to maintain the OAM connection.

The Event Notification OAMPDU packet is used to monitor the link and report the troubles occurred on the link between the local and remote OAM entities.

The Loopback control OAMPDU packet is mainly used to control the remote loopback, including the state of the OAM loopback from the remote device. The packet contains the information to enable or disable the loopback function. You can open or shut down the remote loopback according to the contained information.

49.2 OAM Configuration Task List

- Enabling OAM on an interface
- Enabling remote OAM loopback
- Configuring OAM link monitoring
- Configuring the trouble notification from remote OAM entity
- Displaying the information about OAM protocol

49.3 OAM Configuration Tasks

49.3.1 Enabling OAM on an Interface

Run the following command to enable OAM:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	ethernet oam	Enables Ethernet OAM on an interface.
Step4	ethernet oam [max-rate oampdus | min-rate seconds | mode {active | passive} | timeout seconds]	Configures optional OAM parameters: ● The **max-rate** parameter is used to configure the maximum number of OAMPDUs transmitted per second. It ranges between 1 and 10 and its default value is 10. ● The **min-rate** parameter is used to configure the minimum transmission rate of OAMPDU. Its unit is second. It ranges between 1 and 10 and its default value is 1. ● The **mode {active | passive}** parameter is used to set the mode of OAM. The OAM connection can be established between two interfaces only when at least one interface is in active mode. ● The **timeout** parameter is used to set the timeout time of the OAM connection. It ranges between 1 and 30 seconds and its default value is 1 second.

You can run **no Ethernet oam** to shut down the OAM function.

The remote OAM loopback cannot be enabled on the physical interface that belongs to the aggregation interface.

49.3.2 Configuring OAM Link Monitoring

You can configure the low threshold and the high threshold of OAM link monitoring.

The procedure to configure the OAM link monitoring on an interface is shown in the following table:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	ethernet oam link-monitor negotiation-supported	Enables link monitoring on an interface. The link monitoring is supported by default.
Step4	ethernet oam link-monitor symbol-period {threshold {high { symbols |none} | low {symbols}} | window symbols}	Sets the high and low threshold of the periodical event of the error signal, which triggers the error link events. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. The unit of the window size is the number of the 100M signal. The window size ranges between 10 and 600 on a 1000M Ethernet interface and its default value is 10 in this case, while the window size ranges between 1 and 60 on a 100M Ethernet interface and its default value is 1 in this case.
Step5	ethernet oam link-monitor frame {threshold {high { symbols |none} | low {symbols}} | window symbols}	Sets the high and low thresholds of the error frame event, which triggers the link events of error frame. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. Its unit is second. It ranges between 1 and 60 and its default value is 1.
Step6	ethernet oam link-monitor frame-period {threshold {high { symbols |none} | low {symbols}} | window symbols}	Sets the high and low thresholds of the period event of error frame, which triggers the link events of error frame period. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. The unit of the window size is the number of the 14881 frames. The window size ranges between 100 and 6000 on a 1000M Ethernet interface and its default value is 100 in this case, while the window size ranges between 10 and 600 on a 100M Ethernet interface and its default value is 10 in this case.
Step7	ethernet oam link-monitor frame-	Sets the high and low thresholds of the second event of

	seconds {threshold {high { symbols |none} | low {symbols}} | window symbols}	error frame, which triggers the link events of error frame's second. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 900 and its default value is **none**. The **threshold low** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 900 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. Its unit is second. It ranges between 10 and 900 and its default value is 60.
Step8	ethernet oam link-monitor receive-crc {threshold {high { symbols |none} | low {symbols}} | window symbols}	Sets the high and low thresholds of the error CRC frame event, which triggers the link events of CRC checksum error. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. Its unit is second. It ranges between 1 and 180 and its default value is 10.

49.3.3 Configuring the Trouble Notification from Remote OAM Entity

You can configure an **error-disable** action on an interface. The local interface will enter the **errdisabled** state in the following cases:

1. The high threshold of a normal link event on a local interface is exceeded.
2. The remote interface which connects the local interface enters the **errdisabled** state.
3. The OAM function on the remote interface which connects the local interface is shut down by the administrator.

The procedure to configure the remote OAM trouble indication on an interface is shown in the following table:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface	Configures the trigger action of a remote OAM trouble on an interface: ● The **critical-event** parameter is used to enable an interface to enter the **errdisabled** state when an undesignated critical event occurs. ● The **dying-gasp** parameter is used to enable the local interface to enter the **errdisabled** state if the high threshold of a normal link event on a local interface is exceeded or if the remote interface

which connects the local interface enters the **errdisabled** state or if the OAM function on the remote interface which connects the local interface is shut down by the administrator.

- The **link-fault** parameter is used to enable an interface to enter the **errdisabled** state when the receiver detects signal loss.

Our switch cannot generate the LINK FAULT packets and the Critical Event packets. However, these packets will be handled if they are received from the remote terminal. Our router can transmit and receive the Dying Gasp packet. When the local port enters the **errdisabled** state or is closed by the administrator or the OAM function of the local port is closed by the manager, the Dying Gasp packet will be transmitted to the remote terminal that connects the local port.

49.3.4 Displaying the Information about OAM Protocol

Command	Purpose
show ethernet oam discovery interface [intf-type intf-id]	Displays the OAM discovery information on all interfaces or a designated interface.
show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id]	Displays the OAM statistics information on all interfaces or a designated interface. ● The **pdu** parameter is used to classify and count the OAM packets according to the code-domain value of the OAM packet. ● The **link-monitor** parameter is used to display the detailed statistics information of normal link events. ● The **remote-failure** parameter is to display the detailed statistics information about the remote trouble.
show ethernet oam configuration interface [intf-type intf-id]	Displays the OAM configuration information on all interfaces or a designated interface.
show ethernet oam runtime interface [intf-type intf-id]	Displays the OAM running information on all interfaces or a designated interface.

Table 4 Displaying the information about OAM protocol

49.4 Configuration Example

49.4.1 Network Environment Requirements

You need configure the OAM protocol on the interface where two switches connect for capturing the information about the switch receiving error frames on user access side.

49.4.2 Network Topology

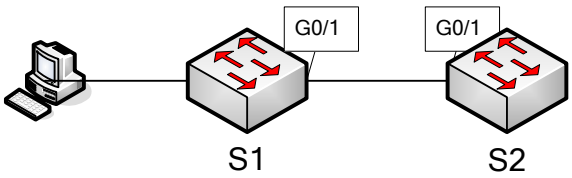


Figure 2 Network topology

49.4.3 Configuration Procedure

Configuring switch S1:

Switch_config_g0/1#ethernet oam

Switch_config_g0/1#ethernet oam mode passive

Switch_config_g0/1#ethernet oam link-monitor frame threshold low 10

Switch_config_g0/1#ethernet oam link-monitor frame window 30

Switch_config_g0/1#show ethernet oam configuration int g0/1

GigaEthernet0/1

General

Admin state : enabled

Mode : passive

PDU max rate : 10 packets/second

PDU min rate : 1 seconds/packet

Link timeout : 1 seconds

High threshold action: no action

Remote Failure

Link fault action : no action

Dying gasp action : no action

Critical event action: no action

Remote Loopback

Is supported : not supported

Loopback timeout : 2

Link Monitoring

Negotiation : supported

Status : on

Errored Symbol Period Event

Window : 10 * 100M symbols

Low threshold : 1 error symbol(s)

High threshold : none

Errored Frame Event

Window : 30 seconds

Low threshold : 10 error frame(s)

High threshold : none

Errored Frame Period Event

Window : 100 * 14881 frames

Low threshold : 1 error frame(s)

High threshold : none

Errored Frame Seconds Summary Event

Window : 60 seconds

Low threshold : 1 error second(s)

High threshold : none

Errored CRC Frames Event

Window : 1 seconds

Low threshold : 10 error frame(s)

High threshold : none

Configuring switch S2: Switch_config_g0/1#ethernet oam

Switch_config_g0/1#show ethernet oam statistics link-monitor int g0/1

GigaEthernet0/1

Local Link Events:

Errored Symbol Period Event:

No errored symbol period event happened yet.

Errored Frame Event:

No errored frame event happened yet.

Errored Frame Period Event:

No errored frame period event happened yet.

Errored Frame Seconds Summary Event:

No errored frame seconds summary event happened yet.

Errored CRC Frames Event:

No errored CRC frame event happened yet.

Remote Link Events:

Errored Symbol Period Event:

No errored symbol period event happened yet.

Errored Frame Event:

No errored frame event happened yet.

Errored Frame Period Event:

No errored frame period event happened yet.

Errored Frame Seconds Summary Event:

No errored frame seconds summary event happened yet.

Errored CRC Frames Event:

No errored CRC frame event happened yet.

Chapter 50 Overview of CFM and Y1731 Configuration

50.1 Stipulations

50.1.1 Format Stipulation in the Command Line

Syntax	Meaning
Bold	Stands for the keyword in the command line, which stays unchanged and must be entered without any modification. It is presented as a bold in the command line.
{italic}	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the brace.
<italic>	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the point bracket.
[ ]	Stands for the optional parameter, which is in the square bracket.
{ x | y | ... }	Means that you can choose one option from two or more options.
[x | y | ...]	Means that you can choose one option or none from two or more options.
{ x | y | ... } *	Means that you has to choose at least one option from two or more options, or even choose all options.
[x | y | ...] *	Means that you can choose multiple options or none from two or more options.
&<1-n>	Means that the parameter before the “&” symbol can be entered 1~n times.
#	Means that the line starting with the “#” symbol is an explanation line.

Chapter 51 CFM Configuration

51.1 CFM Configuration Task List

- Adding the Maintenance Domain
- Adding the Maintenance Association
- Adding MIP (Maintenance domain Intermediate Point)
- Adding MEP (Maintenance association End Point)
- Starting CFM

51.2 CFM Maintenance Task List

- Using the Loopback Function
- Using the Linktrace Function

51.3 CFM Configuration

51.3.1 Adding the Maintenance Domain

Configuration mode: Global

Command	Purpose
ethernet cfm md mdnf {string} <char_string> [**level** <0-7> | **creation** <MHF_creation_type> | **sit** <sender_id_type> | **ip** <IP_address>]	Adds a maintenance domain whose name is char_string. Note: 【1】 The system enters the maintenance domain configuration mode after the maintenance domain is added.

51.3.2 Adding the Maintenance Association

Configuration mode: maintenance domain

Command	Purpose
ma manf {string} <char_string> **ci** {100ms | 1s | 10s | 1min | 10min} **meps** <mepids> [**vlan** <1-4094> | **creation** <MHF_creation_type> | **sit** <sender_id_type> | **ip** <IP_address>]	Adds a maintenance association whose name is char_string.

51.3.3 Adding MIP (Maintenance domain Intermediate Point)

Configuration mode: physical interface

Command	Purpose
ethernet cfm mip add level *<0-7>* [vlan *<1-4094>*]	Adds a designated VLAN and hierarchical MIP to the designated physical interface.

51.3.4 Adding MEP (Maintenance association End Point)

Configuration mode: physical interface

Command	Purpose
ethernet cfm mep add mdnf *{string} <char_string>* **manf** *{string} <char_string>* **mepid** *<1-8191>* **mepid** *<1-8191>* [**direction** *{up | down}* **| ip** *<ip_address>* **| lap** *{all | mac | rCCM | eCCM | xcon | none}* **|fat** *<250 - 1000>* **| frt** *<250 - 1000>*]	Adds a designated maintenance domain and an MEP to the designated physical interface.

51.3.5 Starting CFM

Configuration mode: Global

Command	Purpose
ethernet cfm *{enable}*	Starts CFM.

51.4 CFM Maintenance

51.4.1 Using the Loopback Function

Configuration mode: EXEC

Command	Purpose
ethernet cfm loopback mdnf {string} <char_string> **manf** {string} <char_string> **mepid** <1-8191> **mac** <AA:BB:CC:DD:EE:FF> **number** <1-64>	Uses a designated MEP to conduct loopback towards itself.

51.4.2 Using the Linktrace Function

Configuration mode: EXEC

Command	Purpose
ethernet cfm linktrace mdnf *{string}*	Uses a designated MEP to conduct loopback

<char_string> **manf** *{string} <char_string>* **mepid** *<1-8191>* **mac** *<AA:BB:CC:DD:EE:FF>* [**ttl** *{1-255}* | **fdb-only** *{yes}*] *<char_string>* **manf** *{string} <char_string>* **mepid** *<1-8191>* **mac** *<AA:BB:CC:DD:EE:FF>* **ttl** *<1-255>*	towards itself.

51.5 Configuration Example

You want to add a maintenance domain whose name is customer and hierarchy is 5, set a customer1 maintenance association for vlan1, configure the transmission interval of CCM of the maintenance association to 1s and add an MEP whose MEPID is 2009 to physical port1, specify its remote MEP as 2008:

Switch_config#ethernet cfm md mdnf string customer level 5

Switch_config_cfm#ma manf string customer1 vlan 1 ci 1s meps 1-2,2009

Switch_config_cfm#interface g0/1

Switch_config_g0/1#ethernet cfm mep add mdnf string customer manf string customer1 mepid 2009 rmep 2008 direction down lap all

Switch_config_g0/1#exit

Switch_config#ethernet cfm enable

Chapter 52 Y1731 Configuration

52.1 Configuration Task List

- Enabling Frame Delay Measurement
- Displaying the Information About OAM Protocol

52.1.1 Enable frame delay measurement function

Run the following command to enable the frame delay measurement function:

Command	Purpose
config	Enter the global configuration mode.
ethernet y1731 delay-measurement [-n *number***]*** *MEGID* **{ aimmep** *MEPID*| *macaddr* **} [one-way]**	Enable the frame delay measurement function. **-n** (optional) set the number of packets to send, the default value is 5 (only valid for bidirectional detection). **MEGID** is the name of the MEG to perform the loopback function. (The name is concatenated from md and ma. For example, the name of md is test, the name of ma is aa, so the name of MEG is testaa) **aimmep** is the target mep to perform the frame delay measurement function. The mac address of the destination mep must be learned through the cc function. **macaddr** The MAC address of the destination MEP that performs the frame delay measurement function, no need to learn the mac address. **one-way** means to implement the one-way frame delay measurement function, and will continuously send one-way delay measurement messages after it is enabled.
[no]ethernet y1731 delay-measurement info	Enable/disable the information display function of one-way frame delay measurement, which is used to observe the frame delay and delay variation of each received one-way delay measurement message.

52.1.2 Displaying the Y1731 Protocol Information

Run show to browse Y1731 configuration:

Command	Purpose
show ethernet y1731 delay-measurement *MEGID*	The command is used to display the detection information about the continuous check of MEG, including whether continuity is lost or whether other faults occur. MEGID is the name of MEG. MEPID is the symbol of to-be-displayed MEP

show ethernet y1731 traffic	The command is used to display some statistics information about the Y.1731 module, including statistics of the received and transmitted OAM packets and the system error.

52.1.3 Deleting Y1731 Configuration or Statistics Information

Run **clear** to browse Y1731 configuration and statistics information:

Command	Purpose
clear ethernet y1731 counters	The command is used to delete the transmission statistics information about the OAM packets and the system error information.

52.2 Configuration example

Topology:
DUT1 and DUT2 are directly connected to GigaEthernet0/8 through port GigaEthernet0/25

DUT1 Configuration:
ethernet cfm ENABLE
ethernet cfm md mdnf STRING test
ma manf STRING aa meps 1-2
!
interface GigaEthernet0/25
switchport mode trunk
ethernet cfm ENABLE
ethernet cfm mep add mdnf STRING test manf STRING aa mepid 1 rmepid 2
!

DUT2 Configuration:
ethernet cfm ENABLE
ethernet cfm md mdnf STRING test
ma manf STRING aa meps 1-2
!
interface GigaEthernet0/8
switchport mode trunk
ethernet cfm ENABLE
ethernet cfm mep add mdnf STRING test manf STRING aa mepid 2 rmepid 1
!

1). When the one-way mode is enabled, the device will send a 1DM message to the peer device.
Local (DUT1) device:
DUT1#ethernet y1731 delay-measurement testaa 1234.5678.9abc one-way

DUT1#

Send 5 packets, One-way ETH-DM Terminate.

DUT1_config#show ethernet y1731 traffic

ETH-OAM traffic/errors:

Total output CCM frames: 0

Total output LBM frames: 0

Total output LTM frames: 0

Total output AIS frames: 0

Total output 1DM frames: 5

Total output DMM frames: 0

Total input CCM frames: 0

Total input LBM frames: 0

Total input LBR frames: 0

Total input LTM frames: 0

Total input LTR frames: 0

Total input AIS frames: 0

Total input 1DM frames: 0

Total input DMM frames: 0

Total input DMR frames: 0

Total memory allocation failures: 0

Total system failures: 0

Peer (DUT2) device:

DUT2_config#Jan 1 00:02:37 %ETHOAM-6-1DM_DELAY: MEG testaa MEP 1 receive 1DM frame, FD = 1708540ms, FDV = 0ms

Jan 1 00:02:38 %ETHOAM-6-1DM_DELAY: MEG testaa MEP 1 receive 1DM frame, FD = 1708540ms, FDV = 0ms

Jan 1 00:02:39 %ETHOAM-6-1DM_DELAY: MEG testaa MEP 1 receive 1DM frame, FD = 1708540ms, FDV = 0ms

Jan 1 00:02:40 %ETHOAM-6-1DM_DELAY: MEG testaa MEP 1 receive 1DM frame, FD = 1708540ms, FDV = 0ms

Jan 1 00:02:41 %ETHOAM-6-1DM_DELAY: MEG testaa MEP 1 receive 1DM frame, FD = 1708520ms, FDV = 20ms

DUT2_config#show ethernet y1731 traffic

(View packet statistics)

ETH-OAM traffic/errors:

Total output CCM frames: 0

Total output LBM frames: 0

Total output LTM frames: 0

Total output AIS frames: 0

Total output 1DM frames: 0

Total output DMM frames: 0

Total input CCM frames: 0

Total input LBM frames: 0

Total input LBR frames: 0

Total input LTM frames: 0

Total input LTR frames: 0

Total input AIS frames: 0
Total input 1DM frames: 5
Total input DMM frames: 0
Total input DMR frames: 0
Total memory allocation failures: 0
Total system failures: 0

DUT2_config#show ethernet y1731 delay-measurement testaa
(See the results of the delay measurement)
MEG testaa one way delay measurement :
FD min: 1708520ms
FD max: 1708540ms
Average FD: 1708530ms
FDV current: 20ms
FDV min: 0ms
FDV max: 20ms

2). When the two-way mode is enabled, the device will send a DMM message to the peer device, and the peer device will reply with a DMR message.
Local (DUT1) device:
DUT1#ethernet y1731 delay-measurement testaa 1234.5678.9abc
Two-way delay measurement MEG: testaa Local MEP: 1 Aimaddress: 1234.5678.9ABC
-- delay measurement statistics--
Packets: send = 5, Received = 5, Lost = 0(0/5 loss)
-- Approximate round trip times in milli-seconds:
MINFD = -2545510ms, MAXFD = -2545440ms, Average = 856447987ms
MINFDV = 0ms, MAXFDV = 20ms

DUT1#show ethernet y1731 traffic
(View packet statistics)
ETH-OAM traffic/errors:
Total output CCM frames: 0
Total output LBM frames: 0
Total output LTM frames: 0
Total output AIS frames: 0
Total output 1DM frames: 0
Total output DMM frames: 5
Total input CCM frames: 0
Total input LBM frames: 0
Total input LBR frames: 0
Total input LTM frames: 0
Total input LTR frames: 0
Total input AIS frames: 0

Total input 1DM frames: 0
Total input DMM frames: 0
Total input DMR frames: 5
Total memory allocation failures: 0
Total system failures: 0

Peer (DUT2) device:
DUT2#show ethernet y1731 traffic
(View packet statistics)
ETH-OAM traffic/errors:
Total output CCM frames: 0
Total output LBM frames: 0
Total output LTM frames: 0
Total output AIS frames: 0
Total output 1DM frames: 0
Total output DMM frames: 0
Total input CCM frames: 0
Total input LBM frames: 0
Total input LBR frames: 0
Total input LTM frames: 0
Total input LTR frames: 0
Total input AIS frames: 0
Total input 1DM frames: 0
Total input DMM frames: 5
Total input DMR frames: 0
Total memory allocation failures: 0
Total system failures: 0

3). Command to clear statistics:
DUT1#clear ethernet y1731 delay-measurement testaa
DUT1#clear ethernet y1731 counters

Chapter 53 DHCP-Snooping Configuration

53.1 IGMP-Snooping Configuration Tasks

DHCP-Snooping is to prevent the fake DHCP server from providing the DHCP service by judging the DHCP packets, maintaining the binding relationship between MAC address and IP address. The L2 switch can conduct the DAI function and the IP source guard function according to the binding relationship between MAC address and IP address. The DHCP-snooping is mainly to monitor the DHCP packets and dynamically maintain the MAC-IP binding list. The L2 switch filters the packets, which do not meet the MAC-IP binding relationship, to prevent the network attack from illegal users.

- Enabling/Disabling DHCP-snooping function
- Enabling DHCP-Snooping in a VLAN
- Setting an Interface to a DHCP-Trusting Interface
- Enabling DAI in a VLAN
- Setting an Interface to an ARP-Trusting Interface
- Enabling Source IP Address Monitoring in a VLAN
- Setting A Trust Interface for Monitoring Source IP Address
- Binding DHCP Snooping to a Standby TFTP Server
- Configuring a file name for DHCP-snooping binding backup
- Configuring an interval for DHCP-snooping binding backup
- Configuring or adding the binding relationship manually
- Mointoringandmaintaining DHCP-snooping
- DHCP-snooping Example

53.1.1 Enabling/Disabling DHCP-Snooping

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping	Enables DHCP-snooping.
no ip dhcp-relay snooping	Resumes the default settings.

This command is used to enable DHCP snooping in global configuration mode. After this command is run, the switch is to monitor all DHCP packets and form the corresponding binding relationship.

NOTE: If the client obtains the address of a switch before this command is run, the switch cannot add the corresponding binding relationship.

53.1.2 Enabling DHCP-Snooping in a VLAN

If DHCP snooping is enabled in a VLAN, the DHCP packets which are received from all distrusted physical ports in a VLAN will be legally checked. The DHCP response packets which are received from distrusted physical ports in a VLAN will then be dropped, preventing the faked or mis-configured DHCP server from providing address distribution services. For the DHCP request packet from distrusted ports, if the hardware address field in the DHCP request packet does not match the MAC address of this packet, the DHCP request packet is then thought as a fake packet which is used as the attack packet for DHCP DOS and then the switch will drop it.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping vlan *vlan_id*	Enables DHCP-snooping in a VLAN.
no ip dhcp-relay snooping vlan *vlan_id*	Disables DHCP-snooping in a VLAN.

53.1.3 Enabling DHCP anti-attack in a VLAN.

To enable attack prevention in a VLAN, you need to configure the allowable maximum DHCP clients in a specific VLAN and conduct the principle of "first come and first serve". When the number of users in the specific VLAN reaches the maximum number, new clients are not allowed to be distributed.
Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping vlan *vlan_id* max-client *number*	Enabling DHCP anti-attack in a VLAN.
no ip dhcp-relay snooping vlan *vlan_id* max-client	Disables DHCP anti-attack in a VLAN.

53.1.4 Setting an Interface to a DHCP-Trusting Interface

If an interface is set to be a DHCP-trusting interface, the DHCP packets received from this interface will not be checked.
Run the following commands in physical interface configuration mode.

Command	Operation
dhcp snooping trust	Setting an Interface to a DHCP-Trusting Interface
no dhcp snooping trust	Resumes an interface to a DHCP-distrusted interface.

The interface is a distrusted interface by default.

53.1.5 Enabling/Disabling binding table fast update function

This function is disabled by default. When this function is disabled and a port has been bound to client A, the DHCP request of the same MAC address on other ports will be regarded as a fake MAC attack even if client A is off line.
When this function is enabled, the above-mentioned case will not occur.
It is recommended to use this function in case that a client frequently changes its port and address lease, distributed by DHCP server, cannot be modified to a short period of time.

Command	Operation
ip dhcp-relay snooping rapid-refresh-bind	Enables the fast update function of the binding table.

no ip dhcp-relay snooping rapid-refresh-bind	Disables the fast update function of the binding table.

53.1.6 Enabling DAI in a VLAN

When dynamic ARP monitoring is conducted in all physical ports of a VLAN, a received ARP packet will be rejected if the source MAC address and the source IP address of this packet do not match up with the configured MAC-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all ARP packets.

Command	Operation
ip arp inspection vlan *vlanid*	Enables dynamic ARP monitoring on all distrusted ports in a VLAN.
no ip arp inspection vlan *vlanid*	Disables dynamic ARP monitoring on all distrusted ports in a VLAN.

53.1.7 Setting an Interface to an ARP-Trusting Interface

ARP monitoring is not enabled on those trusted interfaces. The interfaces are distrusted ones by default.
Run the following commands in interface configuration mode.

Command	Operation
arp inspection trust	Setting an Interface to an ARP-Trusting Interface
no arp inspection trust	Resumes an interface to an ARP-distrusting interface.

53.1.8 Enabling Source IP Address Monitoring in a VLAN

After source IP address monitoring is enabled in a VLAN, IP packets received from all physical ports in the VLAN will be rejected if their source MAC addresses and source IP addresses do not match up with the configured MAC-to-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all IP packets received from the physical interface.
Run the following commands in global configuration mode.

Command	Operation
ip verify source vlan *vlanid*	Enables source IP address checkup on all distrusted interfaces in a VLAN.
no ip verify source vlan *vlanid*	Disables source IP address checkup on all interfaces in a VLAN.

NOTE: If the DHCP packet (also the IP packet) is received, it will be forwarded because global snooping is configured.

53.1.9 Setting an Interface to the One Which is Trusted by IP Source Address Monitoring

The source address detection function will not be enabled for the IP source address trust interface.

Run the following commands in interface configuration mode.

Command	Operation
ip-source trust	Sets an interface to the one with a trusted source IP address.
no ip-source trust	Resumes an interface to the one with a distrusted source IP address.

53.1.10 Setting DHCP-Snooping Option 82

Option 82 brings the local information to a server and helps the server to distribute addresses to clients.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping information option	Sets that option82, which is in the default format, is carried when DHCP-snooping forwards the DHCP packets.
no ip dhcp-relay snooping information option	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

To specify the format of option82, conduct the following settings in global mode.

Command	Operation
ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type / cm-type/ [host]/hw-type}	Sets the format of option82 that the DHCP packets carry when they are forwarded by DHCP-Snooping.
no ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type /cm-type/[host]/hw-type}	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the circuit-id:

Command	Operation
dhcp snooping information circuit-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information circuit-id **hex** [*xx-xx-xx-xx-xx-xx*]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose

	content is the Hex system.. This command is set on the port that connects the client.
no dhcp snooping information circuit-id	Deletes the manually configured option82 circuit-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the remote-id:

Command	Operation
dhcp snooping information remote-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information remote-id **hex** [*xx-xx-xx-xx-xx-xx*]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no dhcp snooping information remote-id	Deletes the manually configured option82 remote-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the vendor-specific:

Command	Operation
dhcp snooping information vendor-specific string STRING	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information vendor-specific hex [*xx-xx-xx-xx-xx-xx*]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no dhcp snooping information vendor-specific	Deletes the manually configured option82 vendor-specific.

53.1.11 Setting the Policy of DHCP-Snooping Option82 Packets

You can set the policy for the DHCP request packets, which carry with option82, after these packets are received. The policies include the following ones:

"Drop" policy: Run the following command in port mode to drop the request packets with option82.

Command	Operation
dhcp snooping information drop	Drops the request packets that contain option82.

"Append" policy: Run the following command in port mode to add the request packets with option82.

Command	Operation
dhcp snooping information append	Enables the function to add option82 on a port.
dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* | vlanip | hostname }	Stands for the first parameter carried by option82 vendor-specific (suboption9).
dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* | vlanip | hostname }	Stands for the second parameter carried by option82 vendor-specific (suboption9).

53.1.12 Configuring the TFTP Server for Backing up Interface Binding

After the switch configuration is rebooted, the previously-configured interface binding will be lost. In this case, there is no binding relationship on this interface. After source IP address monitoring is enabled, the switch rejected forwarding all IP packets. After the TFTP server is configured for interface binding backup, the binding relationship will be backed up to the server through the TFTP protocol. After the switch is restarted, the switch automatically downloads the binding list from the TFTP server, securing the normal running of the network.
Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping database-agent *ip-address*	Configures the IP address of the TFTP server which is to back up interface binding.
no ip dhcp-relay snooping database-agent *ip-address*	Cancels the TFTP Server for backing up interface binding.

53.1.13 Configuring a File Name for Interface Binding Backup

When backing up the interface binding relationship, the corresponding file name will be saved on the TFTP server. In this way, different switches can back up their own interface binding relationships to the same TFTP server.
Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping db-file *name* [timestamp]	Configures a file name for interface binding backup.
no ip dhcp-relay snooping db-file	Cancels a file name for interface binding backup.

53.1.14 Configuring the Interval for Checking Interface Binding Backup

The MAC-to-IP binding relationship on an interface changes dynamically. Hence, you need check whether the binding relationship updates after a certain interval. If the binding relationship updates (adds or deletes binding entries), it need be backed up again. The default time interval is 30mins.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping write-immediately	Configures DHCP Snooping immediate backup when the binding information changes. no ip dhcp-relay snooping {write-time | write-immediately} Resumes the interval of checking interface binding backup to the default settings.
ip dhcp-relay snooping write-time *num*	Configures the interval for checking interface binding backup. The unit is min.
no ip dhcp-relay snooping write-time	Resumes the interval of checking interface binding backup to the default settings.

53.1.15 Configuring Interface Binding Manually

If a host does not obtain the address through DHCP, you can add the binding item on an interface of a switch to enable the host to access the network. You can run no ip source binding MAC IP to delete items from the corresponding binding list.

Note that the manually-configured binding items have higher priority than the dynamically-configured binding items. If the manually-configured binding item and the dynamically-configured binding item have the same MAC address, the manually-configured one updates the dynamically-configured one. The interface binding item takes the MAC address as the unique index.

Run the following commands in global configuration mode.

Command	Operation
ip source binding *MAC IP* interface *name vlan-id*	Configures Interface Binding Manually
no ip source binding *MAC IP vlan-id*	Cancels an interface binding item.

53.1.16 Monitoring and Maintaining DHCP-Snooping

Run the following commands in EXEC mode:

Command	Operation
show ip dhcp-relay snooping	Displays the information about DHCP-snooping configuration.
show ip dhcp-relay snooping binding	Displays the effective address binding items on an interface.

show ip dhcp-relay snooping binding all	Displays all binding items which are generated by DHCP snooping.
[**no**] **debug ip dhcp-relay** [snooping | binding | event | all]	Enables or disables the switch of DHCP relay snooping binding or event.

The following shows the information about the DHCP snooping configuration.

```
switch#show ip dhcp-relay snooping
ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
GigaEthernet0/1
ARP Inspect interface:
GigaEthernet0/11
```

The following shows the binding information about dhcp-relay snooping:

```
switch#show ip dhcp-relay snooping binding
Hardware Address   IP Address     remainder time Type        VLAN   interface

00:e0:0f:26:23:89  192.2.2.101    86400    DHCP_SN      3     GigaEthernet0/3
```

The following shows the binding information about dhcp-relay snooping:

```
switch#show ip dhcp-relay snooping binding all
Hardware Address   IP Address     remainder time Type        VLAN   interface

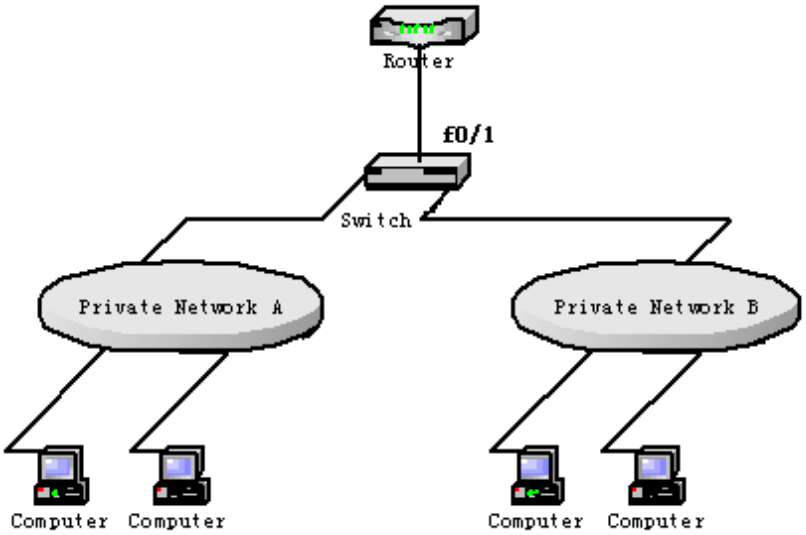
00:e0:0f:32:1c:59  192.2.2.1      infinite    MANUAL       1     GigaEthernet0/2
00:e0:0f:26:23:89  192.2.2.101    86400    DHCP_SN      3     GigaEthernet0/3
```

The following shows how to debug the information about dhcp-relay snooping.

```
switch#debug ip dhcp-relay all
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface GigaEthernet0/3
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 1
DHCPR: DHCP packet len 300
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 289
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 1
DHCPR: DHCP packet len 300
DHCPR: update binding on interface GigaEthernet0/3
DHCPR:  IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue
```

53.1.17 DHCP-Snooping Configuration Example

The network topology is shown in figure 1.



Configuring Switch

9. Enable DHCP snooping in VLAN 1 which connects private network A.

(1) Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

10. Enable DHCP snooping in VLAN 2 which connects private network B.

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 2

11. Sets the interface which connects the DHCP server to a DHCP-trusting interface.

Switch_config_g0/1#dhcp snooping trust

12. Configure option82 instance manually

```
interface GigaEthernet0/1
 dhcp snooping information circuit-id hex 00-01-00-05
 dhcp snooping information remote-id hex 00-e0-0f-13-1a-50
 dhcp snooping information vendor-specific hex 00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
 dhcp snooping information append
 dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
!
interface GigaEthernet0/2
 dhcp snooping trust
 arp inspection trust
 ip-source trust
!
!
!
ip dhcp-relay snooping
ip dhcp-relay snooping vlan  1-100
ip arp inspection vlan  1
```

ip verify source vlan 1

ip dhcp-relay snooping information option format manual

Chapter 54 MACFF Configuration

54.1 MACFF Configuration Tasks

MACFF is to isolate downlink ports of the same VLAN in a switch from exchanging inter-access packets, enabling these packets to be allocated to the default gateway of client through DHCP server and then to downlink ports. By capturing the ARP packets between downlink ports, MACFF can prevent downlink ports from learn ARPs; MACFF replies the gateway's MAC address, enabling all inter-access packets among all downlink ports to pass through the gateway.

Note: MACFF needs the support of DHCPR-snooping, so before enabling MACFF you have to make sure that DHCPR-snooping works normally. ICMP redirection on the gateway is disabled by default. The VLAN management address must be configured for MACFF-enabled switch.

- Enabling or Disabling MACFF
- Enabling MACFF in VLAN
- Configuring the Default AR of MACFF in VLAN
- Configuring other ARs of MACFF in VLAN
- Specifying a Physical Port to Shut down MACFF

54.1.1 Enabling or Disabling MACFF

Run the following commands in global configuration mode.

Command	Purpose
macff enable	Enables MACFF.
no macff enable	Resumes the default settings.

command is used to enable MACFF in global configuration mode. After this command is run, all ARP packets are listened by switch.

NOTE: You have to make sure that DHCP-Snooping is enabled before configuring this command. If the client obtains the address of a switch before this command is run, the switch cannot add the corresponding binding relationship.

54.1.2 Enabling MACFF in VLAN

If MACFF is enabled in a VLAN, the ARP packets received from all DHCP-snooping untrusted physical port of all VLAN will be monitored. If the destination IP address is the IP address of any DHCP client, on which the physical port that receives the ARP packets is located, these ARP packets will be dropped; if these are ARP response packets, these packets will also be dropped. If other DHCP client, default gateway or other service address requests from the port, their corresponding mac address will replay ARP request.

NOTE: The VLAN on which MACFF is enabled must be configured to have a management address. DHCP snooping shall also be enabled on this VLAN.

Run the following commands in global configuration mode.

Command	Purpose
macff vlan *vlan_id* enable	Enables MACFF in a VLAN.
no macff vlan *vlan_id* enable	Disables MACFF in a VLAN.

54.1.3 Configuring the Default AR of MACFF in VLAN

When you set the address on client manually (or DHCP server does not configure the default route option3, it is not recommended to use DHCP server in this way), the switch shall automatically enables default AR as the MACFF-specified default gateway. There is only one default AR.

Run the following commands in global configuration mode.

Command	Purpose
macff vlan *vlan_id* default-ar *A.B.C.D*	Sets the default AR of MACFF in VLAN.
no macff vlan *vlan_id* default-ar *A.B.C.D*	Deletes the default AR of MACFF in VLAN.

NOTE: Before configuring this command, you can run ip source binding xx-xx-xx-xx-xx-xx A.B.C.D interface name to add the client binding table on the switch. If you do not do this, MACFF will regard the manually configured client as illegal client and MACFF will not serve this client.

54.1.4 Configuring other ARs of MACFF in VLAN

After other ARs of MACFF are configured, MACFF allows DHCP client to access these ARs directly without forwarding packets via the default gateway allocated by DHCP server.

This function can be applied on some servers in the network segment of client or on other service addresses.

Run the following commands in global configuration mode.

Command	Purpose
macff vlan *vlan_id* **other_ar** *A.B.C.D*	Configures other ARs of MACFF in VLAN.
no macff vlan *vlan_id* other_ar *A.B.C.D*	Deletes other ARs of MACFF in VLAN.

54.1.5 Specifying a Physical Port to Shut down MACFF

If you specify a physical port to close MACFF, packets on this port will not be isolated and ARP packets will not be monitored.

Run the following commands in physical interface configuration mode.

Command	Purpose
macff disable	Specifies a physical port to shut down MACFF.
no macff disable	Specifies a physical port to enable MACFF (it is enabled by default).

In default settings, the ports are allowed to enable MACFF.

54.1.6 Enabling MACFF Debugging

Run the following commands in global configuration mode.

Command	Operation
debug macff	Enabling MACFF Debugging
no debug macff	Disabling MACFF Debugging

54.1.7 MACFF Configuration Example

The network topology is shown in figure 1.

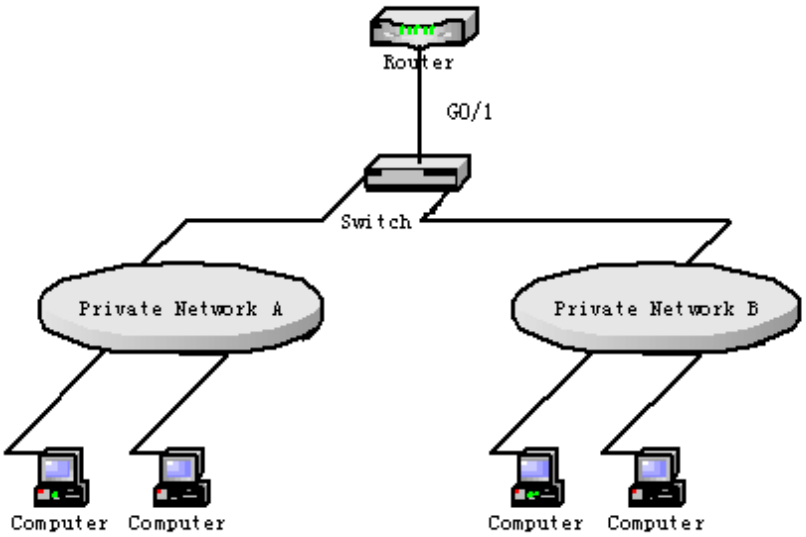


Figure 1

1. Enable MACFF in VLAN1, which connects private network A. The default gateway allocated by DHCP server is 192.168.2.1.

   Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1

   Switch_config#ip dhcp-relay snooping

   Switch_config#ip dhcp-relay snooping vlan 1

   Switch_config#macff enable

   Switch_config#macff vlan 1 enable

2. Enable MACFF in VLAN2, which connects private network B. The default gateway allocated by DHCP server is 192.168.2.2 (If necessary, the default gateway can also be 192.168.2.1).

   Switch_config#arp 192.168.2.2 00:e0:0f:ea:74:ee vlan 2

   Switch_config#ip dhcp-relay snooping vlan 2

   Switch_config#macff vlan 2 enable

3. Sets the ports that connect DHCP server, default gateway and other ARs respectively to be trusted.

   Switch_config_g0/1#dhcp snooping trust

4. If the downlink host A of VLAN 1 is manually configured IP and default gateway, the IP address is 192.168.2.102 and the MAC address is 6c-62-6d-59-18-b7. The default gateway, 192.168.2.1, enables MACFF to take effect. (If the client is not configured manually, this step will not be performed)

   Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1

   Switch_config#ip source binding 6c:62:6d:59:18:b7 192.168.2.102 interface GigaEthernet0/1

   Switch_config#macff vlan 1 default-ar 192.168.2.1

5. Specify a physical port in MACFF-enabled VLAN to shut down MACFF.

   Switch_config_g0/1#macff disable

6. Configures other ARs that are in the same network segment of client. MACFF allows the client to perform direct

access without the help of gateway. (The ports where other APs are should be set to trusted ports)

Switch_config_g0/1#macff disable

Chapter 55 Layer-2 (L2) Tunnel Protocol Configuration

55.1 Overview

The tunnel of layer-2 protocol allows users who connect the two terminals of a switch to transmit the designated layer-2 protocol packets transparently in their own networks through the switch without the affection of the corresponding layer-2 protocol module of this switch. The switch here is just a transparent transmission medium for users.

55.2 Layer-2 (L2) Tunnel Protocol Configuration

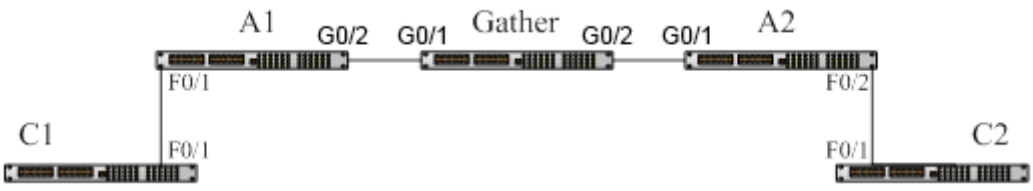
Run the following commands to set the L2 tunnel function on a L2 protocol:

Command	Usage Guidelines
config	Enters the global configuration mode.
interface <intf_name>	Enters the interface configuration mode of a switch port. Only the switch ports support the L2 tunnel (including physical ports and aggregation ports)
[no] l2protocol-tunnel *[stp]*	Sets the L2 protocol, which is used to enable the tunnel function, on this switch port. Currently only the tunnel function of the STP protocol is supported.
no spanning-tree	To disable the STP of a port, run the above-mentioned command.
exit	Goes back to the global mode.
write	Saves the settings.

NOTE: This command is used to disable STP on the port on which the tunnel function is enabled, preventing this port from influencing the devices that access the tunnel by sending the STP packets.

55.3 L2 Protocol Tunnel Configuration Example

The network topology is shown in the following figure:



A1/A2/Gather belongs to a core network. C1/C2 stands for two switches locating in two branches of a customer. The customer wants the two networks to be managed as an independent network, that is, the core network is just like a transparent transmission channel for this customer. To realize STP transparent transmission, the customer needs to make the following settings on each switch:

- Set port g0/2 of switch A1, port g0/1 of switch Gather and port g0/1 of switch A2 to the trunk mode respectively.

- Set port f0/1 of switch A1 and port f0/2 of switch A2 to access, disable STP, and then enable the tunnel function of the STP protocol on the two ports.

Chapter 56 QoS Configuration

If you care to use your bandwidth sufficiently and your network resources efficiently, you must pay attention to QoS configuration.

56.1 QoS Overview

56.1.1 QoS Concept

In general, the switch works in best-effort served mode in which the switch treats all flows equally and tries its best to deliver all flows. Thus if congestion occurs all flows have the same chance to be discarded. However in a real network different flows have different significances, and the QoS function of the switch can provide different services to different flows based on their own significances, in which the important flows will receive a better service.

As to classify the importance of flows, there are two main ways on the current network:

- The tag in the 802.1Q frame header has two bytes and 3 bits are used to present the priority of the packet. There are 8 priorities, among which 0 means the lowest priority and 7 means the highest priority.
- The DSCP field in IP header of the IP packet uses the bottom 6 bits in the TOS domain of the IP header.

In real network application the edge switch distributes different priorities to different flows based on their significance and then different services will be provided to different flows based on their priorities, which is the way to realize the terminal-to-terminal QoS.

Additionally, you can also configure a switch in a network, enabling the switch to process those packets with specific attributes (according to the MAC layer or the L3 information of packets) specially. This kind of behaviors are called as the one-leap behaviors.

The QoS function of the switch optimizes the usage of limited network bandwidth so that the entire performance of the network is greatly improved.

56.1.2 Terminal-To-Terminal QoS Model

The service model describes a group of terminal-to-terminal QoS abilities, that is, the abilities for a network to transmit specific network communication services from one terminal to another terminal. The QoS software supports two kinds of service models: Best-Effort service and Differentiated service.

1. Best-effort service

The best-effort service is a singular service model. In this service model, an application can send any amount of data at any necessary time without application of permits or aforehand network notification. As to the best-effort service, if allowed, the network can transmit data without any guarantee of reliability, delay or throughput. The QoS of the switch on which the best-effort service is realized is in nature this kind of service, that is, first come and first served (FCFS).

2. Differentiated service

As to the differentiated service, if a special service is to be transmitted in a network, each packet should be specified with a corresponding QoS tag. This designation can be embodied in different modes, such as, use IP priority status setting in IP data packet. The switch uses this QoS rule to conduct classification and complete the intelligent queuing. The QoS of the switch provides Strict Priority (SP), Weighted Round Robin (WRR), Deficit Round Robin (DRR) and First-Come-First-Served (FCFS).

56.1.3 Queue Algorithm of QoS

Each queue algorithm is the important basis to realize QoS. The QoS of the switch provides the following algorithms: Strict Priority (SP), Weighted Round Robin (WRR), Weighted Fair Queuing (WFQ) and First-Come-First-Served (FCFS).

1. Strict Priority

This algorithm means to first provide service to the flow with the highest priority and after the highest-priority flow comes the service for the next-to-highest flow. This algorithm provides a comparatively good service to those flows with relatively high priority, but its shortage is also explicit that the flows with low priority cannot get service and wait to die.

2. Weighted Round Robin

Weighted Round Robin (WRR) is an effective solution to the defect of Strict Priority (SP), in which the low-priority queues always die out. WRR is an algorithm that brings each priority queue a certain bandwidth and provides service to each priority queue according to the order from high priority to low priority. After the queue with highest priority has used up all its bandwidth, the system automatically provides service to those queues with next highest priority.

3. Weighted Fair Queuing

Weighted Fair Queuing (WFQ) classifies the packet according to the priority of the traffic. It sets the egress bandwidth based on the weight of each traffic. The bigger the weight, the greater the bandwidth. Thus, it guarantees the fairness of priority services and embodies the weight of different priority services.

4. First come first served

The First-Come-First-Served queue algorithm, which is shortened as FCFS, provides service to those packets according to their sequence of arriving at a switch, and the packet that first arrives at the switch will be served first.

56.1.4 Weighted Random Early Detection

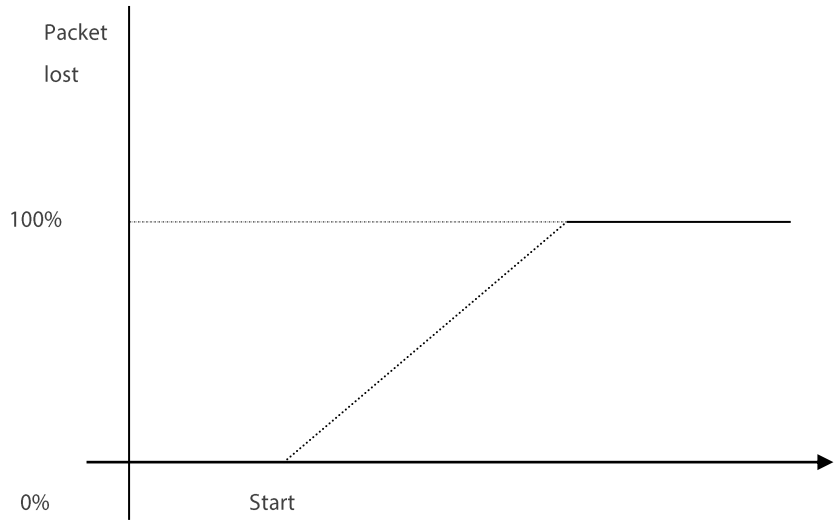
1. Congestion avoidance and traditional packet loss mechanism

Excessive congestion may inflict damage on network resources, so network congestion should be resolved through some measures. Congestion avoidance is a sort of flow control method of positively dropping packets and regulating network flows to solve network overload via network resource monitoring. The traditional way of resolving network congestion is to drop all incoming packets when the queue length reaches its threshold. But for TCP packets, heavy packet loss may cause TCP timeout and lead to slow TCP startup and congestion avoidance, which is called as TCP global synchronization.

2. WRED

The WRED algorithm is adopted to prevent TCP global synchronization. WRED helps users to set the queue threshold. When the queue length is less than the configured threshold, the packets will not be dropped; otherwise, the packets will be dropped randomly. Because WRED drops packets randomly, it is avoided for multiple TCP connections to slow down the transmission speed at the same time, which is the reason why TCP global synchronization is avoided. WRED enables other TCP connections to maintain a relatively high transmission speed when the packets of a certain TCP connection begin to be dropped and their transmission speed is slowed down. No matter what time it is, there are always some TCP connections to transmit packets with a high speed, which ensures effective bandwidth usability.

WRED cooperation is conducted when packets enter the outgoing queue and are checked for their size and packets in different ranges get different treatments. The key parameters include **Start**, **Slop** and **Drop priority.**



- When the queue length is less than start, packets will not be dropped.
- When the queue length is bigger than start, the incoming packets begin to be dropped randomly.The longer the queue is, the higher the dropping rate is.
- The rate for packet loss rises along with the increase of the queue length.

56.2 QoS Configuration Task List

In general, ONU will try its best to deliver each packet and when congestion occurs all packets have the same chance to be discarded. However, in reality different packets have different importance and the comparatively important packets should get the comparatively good service. QoS is a mechanism to provide different priority services to packets with different importance, in which the network can have its better performance and be used efficiently.

This chapter presents how to set QoS on ONU.

The following are QoS configuration tasks:

- Setting the Global cos Priority Queue
- Setting the Bandwidth of the cos Priority Queue
- Setting the Schedule Policy of the cos Priority Queue
- Setting the Default cos Value of a Port
- Setting the cos Priority Queue of a Port
- Setting the Bandwidth of the cos Priority Queue of a Port
- Setting the Schedule Policy of the cos Priority Queue f a Port
- Setting the CoS Priority Queue based on dscp
- Establishing the QoS Policy Mapping
- Setting the Description of the QoS Policy Mapping
- Setting the Matchup Data Flow of the QoS Policy Mapping
- Setting the Actions of the Matchup Data Flow of the QoS Policy Mapping

- Applying the QoS Policy on a Port
- Applying the QoS Policy on a global
- Configuring Trust Mode
- Displaying the QoS Policy Mapping Table

56.3 QoS Configuration Tasks

56.3.1 Setting the Global cos Priority Queue

The task to set the QoS priority queue is to map 8 CoS values, which are defined by IEEE802.1p, to the priority queues in a switch. This series of switch has 8 priority queues. According to different queues, the switch will take different schedule policies to realize QoS.

If a CoS priority queue is set in global mode, the mapping of CoS priority queue on all ports will be affected. When priority queues are set on a L2 port, the priority queues can only work on this L2 port.

Enter the following management mode and run the following commands one by one to set CoS priority queue.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **cos map** quid cos1..cosn	Sets the CoS priority queue. quid stands for the ID of a CoS priority queue. cos1…cosn stands for the IEEE802.1p-defined CoS value.
exit	Goes back to the EXEC mode.
write	Saves the settings.

56.3.2 Setting the Bandwidth of the CoS Priority Queue

The bandwidth of priority queue means the bandwidth distribution ratio of each priority queue, which is set when the schedule policy of the CoS priority queue is set to wrr or wfq. This series of switches has 8 priority queues in total.

If this command is run, the bandwidth of all priority queues on all interfaces are affected. This command validates only when the queue schedule mode is set to WRR/WFQ. This command decides the bandwidth weight value of the CoS priority queue when the WRR/WFQ schedule policy is used.

Run the following commands one by one to set the bandwidth of the CoS priority queue.

Command	Purpose
config	Enters the global configuration mode.
[no] scheduler weight bandwidth *weight1...weightn*	Sets the bandwidth of the CoS priority queue.. weight1…weightn stand for the weights of 8 CoS priority queues of WRR/DRR.
exit	Goes back to the EXEC mode.

write	Saves the settings.

56.3.3 Setting the Schedule Policy of the CoS Priority Queue

A switch has many output queues on each of its port. This series of switches has 8 priority queues. The output queues can adopt the following four schedule modes:

- SP (Sheer Priority): In this algorithm, only when the high-priority queue is null can the packets in the low-priority queue be forwarded, and if there are packets in the high-priority queue these packets will be unconditionally forwarded.
- WRR (Weighted Round Robin) is an algorithm that brings each priority queue a certain bandwidth and provides service to each priority queue according to the order from high priority to low priority.
- WFQ (Weighted Fair Queuing) is an algorithm that brings each priority queue a certain bandwidth according to the priority of the flow.
- The First-Come-First-Served queue algorithm, which is shortened as FCFS, provides service to those packets according to their sequence of arriving at a switch, and the packet that first arrives at the switch will be served first.

Enter the following configuration mode and set the schedule policy of CoS priority queue.

Command	Purpose
config	Enters the global configuration mode.
[no] scheduler policy { sp | wrr|wfq|fcfs }	Sets the schedule policy of the CoS priority queue. **sp** means to use the SP schedule policy. **wrr** means to use the WRR schedule policy. wfq means to use the WFQ schedule policy. **fcfs** means to use the FCFS schedule policy.
exit	Goes back to the EXEC mode.
write	Saves the settings.

56.3.4 Setting the Default CoS Value of a Port

If the port of a switch receives a data frame without tag, the switch will add a default CoS priority to it. Setting the default cos value of a port is to set the untagged default CoS value, which is received by the port, to a designated value.

Enter the management mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] cos default *cos*	Sets the CoS value of the received untagged frames.

	cos stands for the corresponding CoS value.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

56.3.5 Setting the CoS Priority Queue of a Port

When a priority queue is set on a L2 port, the priority queue will be used by the L2 port; otherwise, you should conduct the configuration of a global CoS priority queue.

Enter the management mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **cos map** quid cos1..cosn	Sets the CoS priority queue. quid stands for the ID of a CoS priority queue. cos1…cosn stands for the IEEE802.1p-defined CoS value.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

56.3.6 Setting the Bandwidth of a Port CoS Priority Queue

When a priority queue bandwidth is set on a L2 port, the priority queue bandwidth will be used by the L2 port; otherwise, you should conduct the configuration of a global priority queue bandwidth.

Enter the management mode and run the following commands one by one to set the CoS priority queue bandwidth of a port.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] scheduler weight bandwidth *weight1...weightn*	Sets the bandwidth of the CoS priority queue.. **weight1…weightn** stand for the weights of 8 CoS priority queues of WRR/DRR.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

write	Saves the settings.

56.3.7 Setting the Schedule Policy of a Port CoS Priority Queue

When a priority queue schedule policy is set on a L2 port, the priority queue schedule policy will be used by the L2 port; otherwise, you should conduct the configuration of a global priority queue schedule policy.
Enter the management mode and run the following commands one by one to set the CoS priority queue schedule policy of a port.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] scheduler policy { sp | wrr|wfq }	Sets the schedule policy of the CoS priority queue. **sp** means to use the SP schedule policy. **wrr** means to use the WRR schedule policy. **wfq** means to use the WFQ schedule policy. **drr** means to use the DRR schedule policy.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

56.3.8 Setting the CoS Priority Queue Based on DSCP

Based on the DSCP value, the COS queue is mapped again, the DSCP value is modified and the congestion bit is changed.
Enter the management mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
[**no**]**dscp map** *word* { **cos** *cos-value*} dscp	Word stands for the DSCP range table. Cos-value means to set the mapped priority CoS..
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

56.3.9 Establishing the QoS Policy Mapping

Flow classification means to identify a class of packets with certain attributes by applying a certain regulation and take

designated actions towards to these packets.

Do as follows to set up a QoS policy.

Enter the management mode and then run the following commands to establish a new QoS policy mapping.

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map *name*	Enters the configuration mode of the QoS policy map. name stands for the name of the policy.
exit	Exits from the global configuration mode.
exit	Goes back to the EXEC mode.

56.3.10 Setting the Description of the QoS Policy Mapping

Enter the management mode and run the following commands to set the description of a QoS policy mapping. This settings will replace the previous settings.

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map *name*	Enters the configuration mode of the QoS policy map. name stands for the name of the policy.
description description-text	Sets the description of the QoS policy. description-text stands for the text to describe the policy.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

56.3.11 Setting the Matchup Data Flow of the QoS Policy Mapping

The classification rule of the QoS data flow means the filtration rule configured by the administrator according to management requirements. It can be simple, for example, flows with different priorities can be identified by the ToS field of the IP packet's header, or complicated, for example, the packets can be classified according to the related information about the comprehensive link layer, the network layer and the transmission layer, such as the MAC address, the source address of IP, the destination address or the port ID of the application. In general, the classification standard is limited in the header of an encapsulated packet. It is rare to use the content of a packet as the classification standard.

Enter the management configuration mode, set the matchup data flow of policy and replace the previous settings with this data flow according to the following steps:

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map name	Enters the configuration mode of the QoS policy map. name stands for the name of the policy.
description description-text	Sets the description of the QoS policy. description-text stands for the text to describe the policy.
classify {**any** | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp** *dscp-value* | **tos** *tos-value* | **diffserv** *diffserv-value* | **ip** *ip-access-list* | **ipv6** *ipv6-access-list* | **mac** *mac-access-list*} no classify { cos | icos | vlan | ivlan | ethernet-type | precedence | dscp | tos | diffserv | ip | ipv6 | mac }	Matches up with any packet. Configures the matched COS value which ranges between 0 and 7. **icos** stands for the matched inner COS value which ranges between 0 and 7. **vlanid** stands for the matched VLAN, which ranges from 1 to 4094. **ivlanid** stands for the matched inner VLAN, which ranges from 1 to 4094. **ethernet-type** stands for the matched packet type, which is between 0x0600 and 0xFFFF. **precedence-value** stands for the priority field in tos of IP packet, which ranges from 0 to 7. **dscp-value** stands for the dscp field in tos of IP packet, which ranges from 0 to 63. **tos-value** stands for latency, throughput, reliability and cost fields in tos of IP packet, which ranges from 0 to 15. **diffserv-value** stands for the entire tos field. **Ip-access-list** stands for the name of the matched IP access list. The name has 1 to 20 characters. **Ipv6-access-list** stands for the name of the matched IPv6 access list. The name has 1 to 20 characters. Configures the name of the matched MAC access list. The name has 1 to -20 characters.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

56.3.12 Setting the Actions of the Matchup Data Flow of the QoS Policy Mapping

The actions to define the data flow mean to take corresponding actions to a data flow with compliance of the filtration rule, which include bandwidth limit, drop, update, etc.

Enter the management mode and run the following commands to set the action of a policy, matching up the data flow. The action will replace the previous settings.

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map *name*	Enters the configuration mode of the QoS policy map. name stands for the name of the policy.
action{bandwidth *max-band* |cos *cos* | drop | dscp *dscp-value* | precedence *precedence-value* | forward | icos *icos* | ivlanID { add *addivlanid* | *ivlanid*}| monitor *session-value* | quequ *quequ-value* | redirect *interface-id* | stat-packet | stat-byte | vlanID { add *addvlanid* | *vlanid*} | copy-to-cpu} no action {bandwidth | cos | drop | dscp | precedence | forward | | icos | ivlanID | monitor | quequ | redirect | stat-packet | stat-byte | vlanID | copy-to-cpu}	**max-band** stands for the occupied maximum bandwidth: 1-163840. Unit: 64Kbps Configures policing. **Cos:** Configures the matching flow COS value; the valid range is 0 to 7. **drop** means to drop the matched packets. **dscp-value:** Sets the matched DSCP field to dscp-value 0~63. **precedence-value** stands for the priority field in tos of IP packet (5-7 of tos), which ranges from 0 to 7. **Forward:** Conducts no operations to the matched packets. **Icos:** Sets the matched COS field to cos-value 0-7. **ivlanID** used to replace or add the inner vlan ID, which ranges from 1 to 4094. **session-value** is used to set mirroring, which ranges from 1 to 4. **queue-value** is used to set the mapping queue, which ranges from 1 to 8. **Interface-id:** Redirects the egress port of the matched flow. **stat-packet** stands for the number of packets under statistics. **stat-byte** means the number of bytes under statistics. **vlanID** is used to replace or add the outer vlan ID, which ranges from 1 to 4094. **copy-to-cpu** means to send message to CPU.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

56.3.13 Applying the QoS Policy on a Port

The QoS policy can be applied to a port; multiple QoS policies can be applied to the same port and the same QoS policy can also be applied to multiple ports. On the same port, the priorities of the policies which are earlier applied than those of the policies which are later applied. If a packet is set to have two policies and the actions are contradicted, the actions of the firstly matched policies. After a QoS policy is applied on a port, the switch adds a policy to this port by default to block other data flows, which are not allowed to pass through. When all policies on a port are deleted, the switch will automatically remove the default blockage policy from a port.

Enter the following management mode and run the following commands to apply the QoS policy.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] qos policy *name*{ ingress|egress}	Applies the QoS policy on a port. name stands for the name of QoS policy mapping. ingress means to exert an influence on the ingress. egress means to exert an influence on the egress.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

56.3.14 Applying the QoS Policy Globally

Enter the following management mode and run the following commands to apply the QoS policy.

Command	Purpose
config	Enters the global configuration mode.
[no] qos policy *name* ingress	Applies the QoS policy globally. name stands for the name of QoS policy mapping. ingress means to exert an influence on the ingress.
exit	Goes back to the EXEC mode.

56.3.15 Configuring Trust Mode

When configuring the trust mode under the global configuration mode, there are three options: cos, dscp or untrust. The data will be mapped to the queue in the option chosen above. If choosing the option: untrust, the priority of the packet

will be mapped to the queque by default.

Configuring the trust mode in EXEC mode as the following steps:

Command	Purpose
config	Enters the global configuration mode.
[**no**] **qos trust** { cos | dscp | untrust }	Configuring the trust mode in the global configuration mode. Untrust stand for not trust any modes.
exit	Goes back to the EXEC mode.

56.3.16 Displaying the QoS Policy Mapping Table

You can run the show command to display all or some designated QoS policy maps.

Run the following command in management mode to display the QoS policy mapping table.

Command	Purpose
show policy-map [policy-map-name | interface | global]	Displays all or some designated QoS policy maps. policy-map-name stands for the name of QoS mapping table. Interface stand for the QoS policy applied on a port. Global stand for the QoS policy for Global application.

56.4 QoS Configuration Example

56.4.1 Example for Applying the QoS Policy on a Port

The following example shows how to configure a QoS Policy that meet the IP access list on port g0/2:

ip access-list extended ipacl

permit ip 192.168.20.2 255.255.255.255 192.168.20.210 255.255.255.255

policy-map pmap

classify ip ipacl

action drop

interface g0/2

qos policy pmap ingress

Chapter 57 DoS Attack Prevention Configuration

57.1 DoS Attack Overview

57.1.1 Concept of DoS Attack

The DoS attack is also called the service rejection attack. Common DoS attacks include network bandwidth attacks and connectivity attacks. DoS attack is a frequent network attack mode triggered by hackers. Its ultimate purpose is to break down networks to stop providing legal users with normal network services.

DoS attack prevention requires a switch to provide many attack prevention methods to stop such attacks as Pingflood, SYNflood, Landattack, Teardrop, and illegal-flags-contained TCP. When a switch is under attack, it needs to judge which attack type it is and handles these attack packets specially, for example, sending them to CPU and drop them.

57.1.2 DoS Attack Type

Hackers will make different types of DoS attack packets to attack the servers. The following are common DoS attack packets:

1. Ping of Death

Ping of Death is the abnormal Ping packet, which claims its size exceeds the ICMP threshold and causes the breakdown of the TCP/IP stack and finally the breakdown of the receiving host.

2. Tear Drop

TearDrop uses the information, which is contained in the packet header in the trusted IP fragment in the TCP/IP stack, to realize the attack. IP fragment contains the information that indicates which part of the original packet is contained, and some TCP/IP stacks will break down when they receive the fake fragment that contains the overlapping offset.

3. SYN Flood

A standard TCP connection needs to experience three hand-shake processes. A client sends the SYN message to a server, the server returns the SYN-ACK message, and the client sends the ACK message to the server after receiving the SYN-ACK message. In this way, a TCP connection is established. SYN flood triggers the DoS attack when the TCP protocol stack initializes the hand-shake procedure between two hosts. After receiving SYN-ACK information, the request party adopts source address cheat causing the service party cannot receive ACK response. Subsequently, the service party will be in the phase of waiting ACK information. If there is continuous connection request from the attacker, TCP connection queue of this server will be blocked and the network bandwidth decreased rapidly, result in the network cannot provide normal service.

4. Land Attack

The attacker makes a special SYN message (the source address and the destinationaddress are the same service address). The SYN message causes the server to send the SYN-ACK message to the sever itself, hence this address also sends the ACK message and creates a null link. Each of this kinds of links will keep until the timeouttime, so the server will break down. Landattack can be classified into IPland andMACland.

57.2 DoS Attack Prevention Configuration Task List

As to global DoS attack prevention configuration, you configure related sub-functions and then the switch drops corresponding DoS attack packets. Hence, the bandwidth of the switch is guaranteed not to be used up.

DoS attack prevention configuration tasks are shown below:

- DoSATTACK PREVENTIONconfiguration tasks are shown below:
- Configuring DoS Attack Prevention Function

57.3 DoS Attack Prevention Configuration Tasks

57.3.1 Configuring Global Dos Attack Prevention

Configuring global DoS attack prevention means configuring DoS attack prevention sub-functions in global mode and each sub-function can prevent a different type of DoS attack packets. The DoS IP sub-function can prevent the LAND attacks, while the DoS ICMP sub-function can prevent Ping of Death. You can set the correspondingsub-function according to actual requirements.

Configure the DoS attack prevention function in EXEC mode.

Command	Purpose
config	Enters the global configuration mode.
[no] dos enable {all | icmp *icmp-value* | ip | l4port | mac | tcpflags | tcpfrag *tcpfrag-value* | tcpsmurf | icmpsmurf | ipsmurf }	Configures **all** to prevent all types of DoS attack packets. Configures **icmp** to prevent the ICMP packets which is longer than **icmp-value** from PING attack, among which the **icmp-value** meansthe maximum length of the ICMP packet, that is, 0-1023 bytes. Configures **ip** to prevent those IP packets whose source IPs are the same as the destination IPs. Configures **l4port** to prevent those TCP/UDPpackets whose source port IDs are destination port IDs. Configures **mac** to prevent the packet whose source MACs are the same as the destination MACs. Configures **tcpflags** to prevent those TCP packets containing illegal TCP flags. Configures **tcpfrag** to prevent the to-be-detected TCP packets whose minimum TCP header istcpfrag-value. Configures **tcpsmurf** to prevent those TCP packets whose destination addresses are boardcast addresses. Configures **icmpsmurf** to prevent those ICMP

	packets whose destination addresses are boardcast addresses. Configures **ipsmurf** to prevent those IP packets whose destination addresses are boardcast addresses.
exit	Goes back to the EXEC mode.
write	Saves the settings.

57.3.2 Configuring Dos Attack Prevention

You can display the Dos attack prevention configurations through the show command.

Run the following command in EXEC mode to display the configured DoS attackprevention functions.

Command	Purpose
show dos	Displays Dos attack prevention configuration.

57.4 DoS Attack Prevention Configuration Example

The following example shows how to configure to prevent the attacks of TCP packets, which have illegal flags, and then displays user's configuration.

config

dos enable tcpflags

show dos

The following example shows how to prevent the attacks of IP packets whose source IPs are destination IPs in global mode.

config

dos enable ip

Chapter 58 Attack Prevention Introduction

58.1 Overview of Filter

To guarantee the reasonable usage of network bandwidth, this switch series provides the function to prevent vicious traffic from occupying lots of network bandwidth.

Filter can identify the packets received by the interface of the switch and calculate them according to the packet type. In light of current attack modes, Filter can calculate the number of ARP, IGMP or IP message that a host sends in a time. Once the number exceeds the threshold, the switch will not provide any service to these hosts.

Filter limits the packet from a certain host by blocking the source address. For ARP attack, Filter blocks source MAC address; for IP attacks, such as Ping scan and TCP/UDP scan, Filter blocks source IP address.

58.2 he Mode of Filter

The mode of Filter determines how the switch specifies the attack source. There are two modes of Filter.

- Source Address Block Time (Raw)

In Raw mode, the switch will drop packets from the attack source in scheduled block-time since the attack source is determined. After block-time, the restriction on the attack source will be removed and a new calculation will be enabled.

In Raw mode, all the packets from the source address will be blocked. For instance, when the MAC address of the attack source is blocked, all packets whose source MAC address are the same with that of the attack source will be dropped, no matter it is ARP, ICMP, DHCP or other types.

- Source Address Block Polling (Hybrid)

After blocking the attack source, the switch will continue calculate the packets from the attack source and detect whether the packet number exceeds the threshold before the end of Polling Interval. If the packet number exceeds the threshold, the blocking state keeps. Otherwise, the blocking will be removed. In Hybrid Mode, the packet number when initially determining the attack source and the threshold of the packet number in Polling can be configured independently.

To realize continually calculate the packet, in the hybrid mode the packet type will be matched while the source address is blocked. For instance, if the MAC address of a host is blocked as it triggers ARP attack, IP packets from the host will be sent by the switch continually, unless the host is also identified with the existence of IP attack.

Please select the mode of Filter according to your application environment. If you want to set a strict limit on the attack source and reduce the burden of switch CPU, please use Raw mode; if you want to control the attack source flexibly and resume communication of the host as soon as possible after the end of the attack, please use Hybrid mode. Note that the Filter number a switch can support in Hybrid mode is limited. In condition of inadequate Filter number, Raw mode will be adopted automatically.

Chapter 59 Attack Prevention Configuration

59.1 Attack Prevention Configuration Tasks

When the number of IGMP, ARP or IP message that is sent by a host in a designated interval exceeds the threshold, we think that the host attack the network.

You can select the type of attack prevention (ARP, IGMP or IP), the attack prevention port and the attack detection parameter. You have the following configuration tasks:

- Configuring the attack filter parameters
- Configuring the attack prevention type
- Enables the attack prevention function
- Checking the State of Attack Prevention

59.2 Attack Prevention Configuration

59.2.1 Configuring the Attack Filter Parameters

In global configuration mode, run the following command to configure the parameters of Filter.

Command	Purpose
Switch# **config**	Enters the global configuration mode.
Switch_config# **filter period** *time*	Sets the attack filter period to time. Its unit is second.
Switch_config# filter threshold [arp | bpdu | dhcp | igmp | ip | icmp | icmpv6] *value*	Sets the attack filter threshold to value.
Switch_config# **filter block-time** *time*	Sets the out-of-service time (block-time) for the attack source when the attack source is detected. Its unit is second.
Switch_config# **filter polling period** *time*	Sets the filter polling period in Hybrid mode. Its unit is second.
Switch_config# **filter polling threshold [arp | bpdu | dhcp | igmp | ip | icmp | icmpv6]** *value*	Sets the filter polling threshod in Hybrid mode.
Switch_config# **filter polling auto-fit**	Sets the corresponding parameters of period and threshold of polling filter which adapts to the attack source filter. The command is efficient by default. The polling period equals with the attack filter period and the polling packet threshold equals to 3/4 of the attack filter packet threshold
Switch_config# **filter shutdown-action**	Shutdown the port when detecting the attack in a raw mode.

59.2.2 Configuring the Attack Prevention Type

In global and interface configuration mode, use the following command to configure the type of attack filter.

Command	Purpose
Switch# **config**	Enters the global configuration mode.
Switch_config# **filter dhcp**	Enables DHCP packet attack filter in the global configuration mode.
Switch_config# **filter icmp**	Enables ICMP packet attack filter.
Switch_config# **filter icmpv6**	Enables ICMPv6 packet attack filter.
Switch_config# **filter igmp**	Enables IGMP packet attack filter.
Switch_config# filter ip source-ip	Enables IP attack filter in the global configuration mode.
Switch_config# interface intf-name	Enters the interface configuration mode.
Switch_config_intf# **filter arp**	Enables ARP packet attack filter on the interface.
Switch_config_intf# **filter bpdu**	Enables BPDU packet attack filter on the interface.
Switch_config_intf# **filter dhcp**	Enables DHCP packet attack filter on the interface.
Switch_config_intf# **filter icmp**	Enables ICMP packet attack filter on the interface.
Switch_config_intf# **filter icmpv6**	Enables ICMPv6 packet attack filter on the interface.
Switch_config_intf# **filter ip source-ip**	Enables IP packet attack filter on the interface.

NOTE: ARP attack takes the combination "the host mac address + the source port" as an attack source. That is to say, packets with the same MAC address but coming from different ports, the count will not be accumulated. Both the IGMP attack and IP attack take the host's IP address and source port as the attack source.

NOTE:

1. The IGMP attack prevention and the IP attack prevention cannot be started up together.
2. IP, ICMP, ICMPv6 and DHCP filter take effect only in global and interface configuration mode.

59.2.3 Enabling the Attack Prevention

After all parameters for attack prevention are set, you can start up the attack prevention function. Note that small parts of processor source will be occupied when the attack prevention function is started.

Command	Purpose
Switch_config# **filter enable**	Enables the attack prevention function.
Switch_config# **filter mode** [**raw** | **hybrid**]	Sets the mode of Filter: Raw or Hybrid.

Use the no filter enable command to disable the attack prevention function and remove the block to all attack sources.

59.2.4 Checking the State of Attack Prevention

After attack prevention is started, you can run the following command to check the state of attack prevention:

Command	Purpose
show filter	After attack prevention is started, you can run the following command to check the state of attack prevention:
show filter summary	Checks the parameter configuration and summary information of Filter.

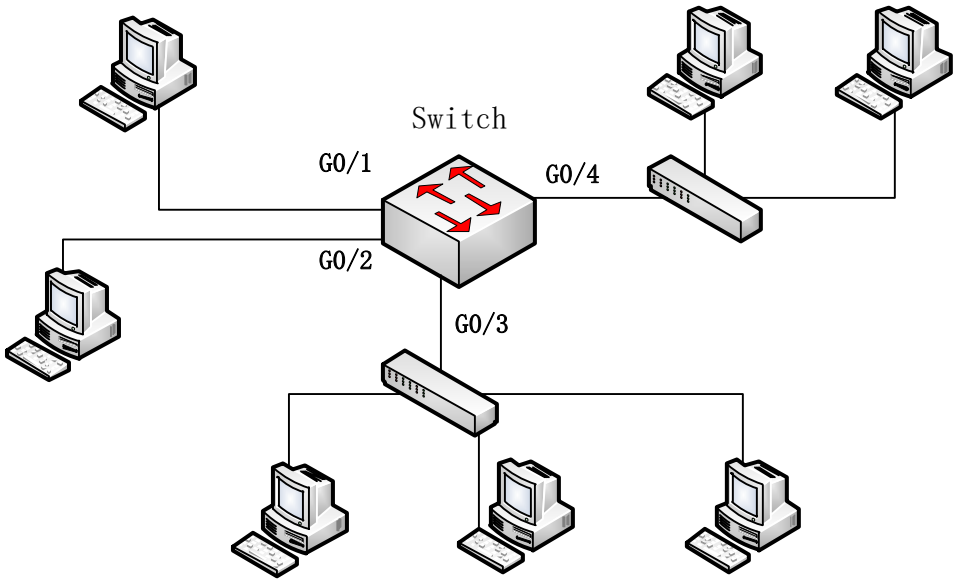
Chapter 60 Attack Prevention Configuration Example

NOTE:

The examples shown in this chapter is only a reference for Filter configuration. Please configure according to your actual network condition.

60.1 Using Filter ARP to Protect the LAN

As shown in the following figure, configure ARP attack Filter on Switch.



Sets the parameter of Filter. A host sending more than 100 ARP messages in 10s will be taken as an attack source.

Switch# config

Switch_config# filter period 10

Switch_config# filter threshold arp 100

Sets APR attack filter with 4 ports:

Switch_config# interface range g0/1 - 4

Switch_config_intf# filter arp

Sets Raw mode and enable Filter:

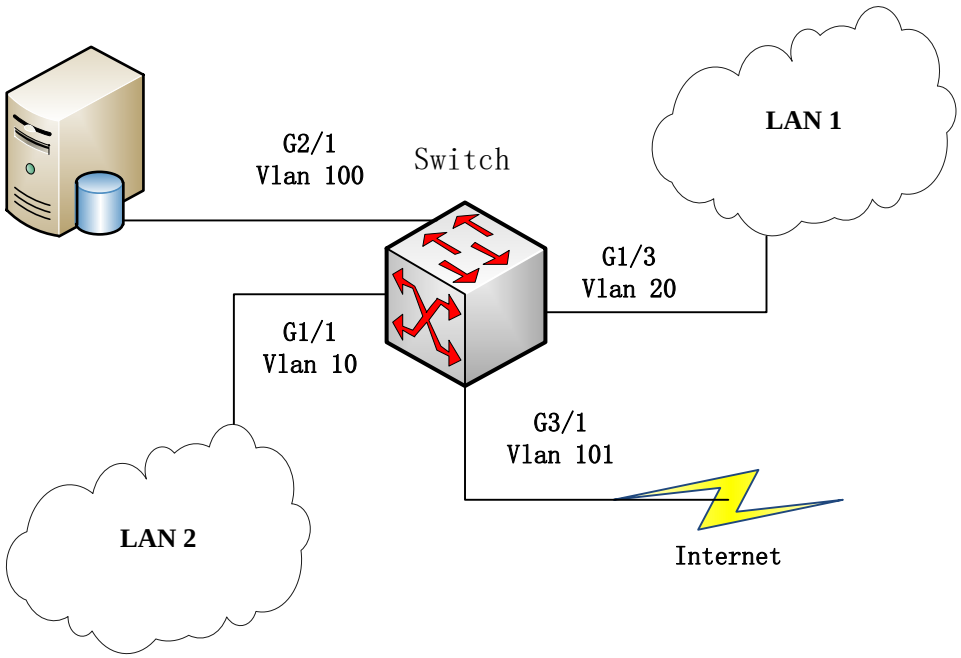
Switch_config_intf# exit

Switch_config# filter mode raw

Switch_config# filter enable

60.2 Using Filter IP to Protect Layer-3 Network

As shown in the following figure, Switch is connected to multiple LANs, servers and the internet. IP packet attack prevention can block IP scan of cross-subnet and large network connections triggered by BitTorrent in a short time.



Sets the parameter of Filter. A host sending more than 300 ARP messages in 1 minute will be taken as an attack source.

Switch# config

Switch_config# filter period 60

Switch_config# filter threshold ip 300

Enable IP packet filter in the global configuration mode and the interface mode. Note that the interface connecting the server and the external network is no need to configure:

Switch_config# filter ip source-ip

Switch_config# interface g1/1

Switch_config_g1/1# filter ip source-ip

Switch_config_g1/1# interface g1/3

Switch_config_g1/3# filter ip source-ip

Switch_config_g1/3# exit

Switch_config#

Enables Filter:

Switch_config# filter enable

Chapter 61 Configuring IP Addressing

61.1 IP Introduction

61.1.1 IP

Internet Protocol (IP) is a protocol in the network to exchange data in the text form. IP has the functions such as addressing, fragmenting, regrouping and multiplexing. Other IP protocols (IP protocol cluster) are based on IP. As a protocol working on the network layer, IP contains addressing information and control information which are used for routing.

Transmission Control Protocol (TCP) is also based on IP. TCP is a connection-oriented protocol which regulates the format of the data and information in data transmission. TCP also gives the method to acknowledge data is successfully reached. TCP allows multiple applications in a system to communicate simultaneously because it can send received data to each of the applications respectively.

The IP addressing, such as Address Resolution Protocol, are to be described in section "Configuring IP Addressing." IP services such as ICMP, HSRP, IP statistics and performance parameters are to be described in "Configuring IP Services."

61.2 Configuring IP Address Task List

An essential and mandatory requirement for IP configuration is to configure the IP address on the network interface of the routing switch. Only in this case can the network interface be activated, and the IP address can communicate with other systems. At the same time, you need to confirm the IP network mask.

To configure the IP addressing, you need to finish the following tasks, among which the first task is mandatory and others are optional. For creating IP addressing in the network, refer to section "IP Addressing Example."

IP address configuration task list:

- Configuring IP address at the network interface
- Configuring multiple IP addresses at the network interface
- Configuring Address Resolution
- Detecting and maintaining IP addressing

61.3 Configuring IP Address

61.3.1 Configuring IP Address at the Network Interface

The IP address determines the destination where the IP message is sent to. Some IP special addresses are reserved and they cannot be used as the host IP address or network address. Table 1 lists the range of IP addresses, reserved IP addresses and available IP addresses.

Type	Address or Range	State
A	0.0.0.0	Reserved
	1.0.0.0 to 126.0.0.0	Available
	127.0.0.0	Reserved
B	128.0.0.0 to 191.254.0.0	Available
	191.255.0.0	Reserved

C	192.0.0.0	Reserved
	192.0.1.0 to 223.255.254.0	Available
	223.255.255.0	Reserved
D	224.0.0.0 to 239.255.255.255	Multicast address
E	240.0.0.0 to 255.255.255.254	Reserved
	255.255.255.255	Broadcast

The official description of the IP address is in RFC 1166 "Internet Digit". You can contact the Internet service provider.
An interface has only one primary IP address. Run the following command in interface configuration mode to configure the primary IP address and network mask of the network interface:

Command	Purpose
ip address ip-address mask	Configure the main IP address of the interface.

The mask is a part of the IP address, representing the network.
NOTE: Our switches only support masks which are continuously set from the highest byte according to the network character order.

61.3.2 Configuring multiple IP addresses at the network interface

Each interface can possess multiple IP addresses, including a primary IP address and multiple subordinate IP addresses. You need to configure the subordinate IP addresses in the following two cases:
If IP addresses in a network segment are insufficient. For example, there are only 254 available IP addresses in a certain logical subnet, however, 300 hosts are needed to connect the physical network. In this case, you can configure the subordinate IP address on the switch or the server, enabling two logical subnets to use the same physical subnet.
Most of early-stage networks which are based on the layer-2 bridge are not divided into multiple subnets. You can divide the early-stage network into multiple route-based subnets by correctly using the subordinate IP addresses. Through the configured subordinate IP addresses, the routing switch in the network can know multiple subnets that connect the same physical network.
If two subnets in one network are physically separated by another network In this case, you can take the address of the network as the subordinate IP address. Therefore, two subnets in a logical network that are physically separated, therefore, are logically connected together.

NOTE: If you configure a subordinate IP address for a routing switch in a network segment, you need to do this for other routing switches in the same network segment.
Run the following command in interface configuration mode to configure multiple IP addresses on the network interface.

Command	Purpose
ip address *ip-address mask* secondary	Configure multiple IP addresses on the network interface.

NOTE: When the IP routing protocol is used to send the route update information, subordinate IP addresses may be treated in different ways.

61.3.3 Configuring Address Resolution

IP can realize functions such as IP address resolution control. The following sections show how to configure address resolution:

1. Creating address resolution

An IP device may have two addresses: local address (local network segment or device uniquely identified by LAN) and network address (representing the network where the device is located). The local address is the address of the link layer because the local address is contained in the message header at the link layer, and is read and used by devices at the link layer. The professionals always call it as the MAC address. This is because the MAC sub layer in the link layer is used to process addresses.

For example, if you want your host to communicate with a device on Ethernet, you must know the 48-bit MAC address of the device or the local address of the link layer. The process on how to obtain the local address of the link layer from the IP address is called as Address Resolution Protocol (ARP). The process on how to obtain the IP address from the local address of the link layer is called as Reverse Address Resolution (RARP).

Our system adopts address resolution in two types: ARP and proxy ARP. The ARP and proxy ARP are defined in RFC 860 and 1027 respectively.

ARP is used to map IP addresses to media or MAC address. When the IP address is known, ARP will find the corresponding MAC address. When the MAC address is known, the mapping relationship between IP address and MAC address is saved in ARP cache for rapid access. The IP message is then packaged in the message at the link layer and at last is sent to the network.

- Defining a static ARP cache

ARP and other address resolution protocols provide a dynamic mapping between IP address and MAC address. The static ARP cache item is generally not required because most hosts support dynamic address resolution. You can define it in global configuration mode if necessary. The system utilizes the static ARP cache item to translate the 32-bit IP address into a 48-bit MAC address. Additionally, you can specify the routing switch to respond to the ARP request for other hosts.

You can set the active period for the ARP entries if you do not want the ARP entry to exist permanently. The following two types show how to configure the mapping between the static IP address and the MAC address.

Run one of the following commands in global configuration mode:

Command	Purpose
arp ip-address hardware-address vlan	Globally map an IP address to a MAC address in the ARP cache.
arp ip-address hardware-address vlan **alias**	Specify the routing switch to respond to the ARP request of the designated IP address through the MAC address of the routing switch.

Run the following command in interface configuration mode:

Command	Purpose
arp timeout *seconds*	Set the timeout time of the ARP cache item in the ARP cache.
arp dynamic	Enables arp dynamic learning in the interface

Run show interfaces to display the ARP timeout time of the designated interface. Run the show arp to check the content of the ARP cache. Run clear arp-cache to delete all entries in the ARP cache.

- Configuring free ARP function

The switch can know whether the IP addresses of other devices collide with its IP address by sending free ARP message. The source IP address and the destination IP address contained by free ARP message are both the local address of the switch. The source MAC address of the message is the local MAC address.

The switch processes free ARP message by default. When the switch receives free ARP message from a device and finds that the IP address contained in the message collide with its own IP address, it will return an ARP answer to the device, informing the device that the IP addresses collide with each other. At the same time, the switch will inform users by logs that IP addresses collide.

The switch's function to send free ARP message is disabled by default. Run the following commands to configure the free ARP function on the port of the switch:

Command	Usage Guidelines
arp send-gratuitous	Start up free ARP message transmission on the interface.
arp send-gratuitous interval *value*	Set the interval for sending free ARP message on the interface. The default value is 120 seconds.

- Sets the maximum retransmissions of the Re-Detect packets.

The ARP entries (to be tagged with G), which the routing entry gateway depends on, require being re-detected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. The greater the retransmission times, the more likely to re-detect.

Command	Usage Guidelines
arp max-gw-retries *number*	Sets the maximum retransmissions of the Re-Detect packets. The default is 3.

- Sets re-detection when ARP entry is aging.

By default only ARP depends on routing entry has re-detection when aging. After enable this command, all ARP entries will adopt aging re-detection mechanism.

Command	Usage Guidelines
arp retry-allarp	Sets re-detection when the ARP entry is aging.

2. Mapping host name to IP addres

Any IP address can correspond to a host name. The system has saved a mapping (host name to address) cache which can be telneted or pinged.

To designate a mapping from host name to address, run the following commands in global mode:

Command	Purpose
ip host name address	Statically map the host name to the IP address.

61.3.4 Detecting and maintaining IP addressing

To detect and maintain the network, run the following command:

1. Clearing cache, list and database

You can clear all content in a cache, list or the database. When you think some content is ineffective, you can clear it.

Run the following command in management mode to clear the cache, list and database:

Command	Purpose
clear arp-cache	Clear the IP ARP cache.

2. Displaying statistics data about system and network

The system can display designated statistics data, such as IP routing table, cache and database. All such information helps you know the usage of the systematic resources and solve network problems. The system also can display the reachability of the port and the routes that the message takes when the message runs in the network.

All relative operations are listed in the following table. For how to use these commands, refer to Chapter "IP Addressing Commands". Run the following commands in management mode:

Command	Purpose
show arp	Display content in the ARP table.
show hosts	Display the cache table about hostname-to-IP mapping.
show ip interface [*type number*]	Displays the state of a port.
ping {host | address}	Test the reachability of the network node.

61.4 IP Addressing Example

The following case shows how to configure the IP address on interfaceVLAN11.

interface vlan 11

ip address 202.96.2.3 255.255.255.0

Chapter 62 Configuring DHCP

62.1 Overview

Dynamic Host Configuration Protocol (DHCP) is used to provide some network configuration parameters for the hosts on the Internet which is described in details in RFC 2131. One of the major functions of DHCP is to distribute IPs on an interface. DHCP supports the following three IP distribution mechanism:

- Automatic distribution

The DHCP server automatically distributes a permanent IP address to a client.

- Dynamic distribution

The DHCP server distributes an IP address for a client to use for a certain period of time or until the client does not use it.

- Manual distribution

The administrator of the DHCP server manually specifies an IP address and through the DHCP protocol sends it to the client.

62.1.1 DHCP Application

DHCP can be applied at the following cases: You can distribute IP address, network segment and related sources (such as relevant gateway) to an Ethernet interface by configuring the DHCP client.

- When a switch that can access DHCP connects multiple hosts, the switch can obtain an IP address
- From the DHCP server through the DHCP relay and then distribute the address to the hosts.

62.1.2 Advantages of DHCP

In current software version, the DHCP client or the DHCP client on the Ethernet interface is supported. DHCP has the following strong points:

- Fastening the settings;
- Reducing configuration errors;
- Controlling IP addresses of some device ports through the DHCP server

62.1.3 DHCP Terms

DHCP is based on the server/client mode. So the DHCP server and the DHCP client must exist at the same time:

- DHCP-Server

●It is a device to distribute and recycle the DHCP-related sources such as IP addresses and lease time.

- DHCP-Client

●It is a device to obtain information from the DHCP server for devices of the local system to use, such as IP address information.

In a word, there exists lease time during the process of dynamic DHCP distribution:

- Lease time

●It means the effective period of an IP, which starts from the distribution. After the lease time, the DHCP server withdraws the IP. To continue to use this IP, the DHCP client needs to apply it again.

62.2 Configuring DHCP Client

62.2.1 Configuration Task List of DHCP Client

- Obtaining an IP address

- Specifying an address for DHCP server
- Configuring DHCP parameters
- Monitoring DHCP

62.2.2 DHCP Client Configuration Tasks

1. Obtaining an IP address

Run the following command on the VLAN interface to obtain an IP address through the DHCP protocol for an interface.

Command	Function
ip address dhcp	Sets the IP address of an Ethernet interface through DHCP.

2. Specifying an address for DHCP server

If knowing the addresses of some DHCP servers, you can specify these servers' addresses on switch so as to reduce the time of protocol processing. You can run the following command in global mode:

Command	Function
ip dhcp-server *ip-address*	Specifies the IP address of the DHCP server.

The command is optional when you perform operations to "obtain an IP address".

3. Configuring DHCP parameters

To adjust the parameters of DHCP communication according to actual requirements, run the following commands in global mode:

Command	Function
ip dhcp client minlease *seconds*	Specifies the acceptable minimum lease time.
ip dhcp client retransmit *count*	Specifies the retransmission times for DHCP packet.
ip dhcp client select *seconds*	Specify the interval for SELECT.
ip dhcp client class_identifier *WORD*	Specify the classification code of the provider.
ip dhcp client client_identifier hrd_ether	Specify the client ID as the Ethernet type
ip dhcp client timeout_shut	Specify client timeout shutdown of the interface

The command is optional when you perform operations to "obtain an IP address".

4. Monitoring DHCP

To browse related information of the DHCP server, which is discovered by the switch currently, run the following

command in EXEC mode:

Command	Function
show dhcp server	Displays related information about the DHCP server, which is known by the switch.

To browse which IP address is currently used by the switch, run the following command in EXEC mode:

Command	Function
show dhcp lease	Displays IP resources, which are currently used by the switch, and related information.

Additionally, if you use DHCP to distribute an IP for an Ethernet interface, you can also run show interface to browse whether the IP address required by the Ethernet interface is successfully acquired.

62.2.3 DHCP Client Configuration Example

DHCP Client configuration example is shown below:

1. Obtaining an IP address

The following example shows interface vlan11 obtains an IP address through DHCP.

```
!
interface vlan 11
ip address dhcp
```

Chapter 63 IP Service Configuration

The section is to describe how to configure optional IP service. For the details of the IP service commands, refer to section "IP Service Commands".

63.1 Configuring IP Service

Optional IP service configuration tasks are listed as follows:

- Managing IP connection
- Configuring performance parameters
- Detecting and Maintaining IP Network

The above operations are not mandatory. You can perform the operations according to your requirements.

63.1.1 Managing IP connection

The IP protocol provides a series of services to control and manage IP connections. Most of these services are provided by ICMP. The ICMP message is sent to the host or other routing switches when the routing switch or the access server detects faults in the IP message header. ICMP is mainly defined in RFC 792.

Perform the following different operations according to different IP connection conditions:

1. Sending ICMP unreachable message

If the system receives a message and cannot send it to the destination, such as no routes, the system will send an ICMP-unreachable message to the source host. The function of the system is enabled by default.

If the function is disabled, you can run the following command in interface configuration mode to enable the function.

Command	Purpose
ip unreachables	Enable the function to send an ICMP-unreachable message.

2. Sending ICMP redirection message

Sometimes the host selects an unfavorable route. After a routing switch on the route receives a message from the host, it is to check the routing table and then forward the message through the message-receiving interface to another routing switch that is in the same network segment as the host. In this case, the routing switch notifies the source host of directly sending the message with the destination to another routing switch without winding itself. The redirection message requires the source host to discard the original route and take more direct route suggested in the message. Many host's operating system adds a host route to its routing table. However, the routing switch is more willing to trust information obtained through the routing protocol. Therefore, the routing switch would not add the host route according to the information.

The function is enabled by default. If the hot standby routing switch protocol is configured on the interface, the function is automatically disabled. However, the function will not be automatically enabled even if the hot standby routing switch protocol is canceled.

To enable the function, run the following command in interface configuration mode:

Command	Purpose
ip redirects	Permit sending the ICMP redirection messafge.

3. Sending ICMP mask response message

Sometimes the host must know the network mask. To get the information, the host can send the ICMP mask request message. If the routing switch can confirm the mask of the host, it will respond with the ICMP mask response message. By default, the routing switch can send the ICMP mask response message.

To send the ICMP mask request message, run the following command in interface configuration mode:

Command	Purpose
ip mask-reply	Send the ICMP mask reply message.

4. Supporting route MTU detection

The system supports the IP route MTU detection mechanism defined by RFC 1191. The IP route MTU detection mechanism enables the host to dynamically find and adjust to the maximum transmission unit (MTU) of different routes. Sometimes the routing switch detects that the received IP message length is larger than the MTU set on the message forwarding interface. The IP message needs to be segmented, but the "unsegmented" bit of the IP message is reset. The message, therefore, cannot be segmented. The message has to be dropped. In this case, the routing switch sends the ICMP message to notify the source host of the reason of failed forwarding, and the MTU on the forwarding interface. The source host then reduces the length of the message sent to the destination to adjust to the minimum MTU of the route.

If a link in the route is disconnected, the message is to take other routes. Its minimum MTU may be different from the original route. The routing switch then notifies the source host of the MTU of the new route. The IP message should be packaged with the minimum MTU of the route as much as possible. In this way, the segmentation is avoided and fewer message is sent, improving the communication efficiency.

Relevant hosts must support the IP route MTU detection. They then can adjust the length of IP message according to the MTU value notified by the routing switch, preventing segmentation during the forwarding process.

5. Setting IP maximum transmission unit (MTU)

All interfaces have a default IP maximum transmission unit (MTU), that is, the transmissible maximum IP message length. If the IP message length exceeds MTU, the routing switch segments the message.

Changing the MTU value of the interface is to affect the IP MTU value. If IP MTU equals to MTU, IP MTU will automatically adjust itself to be the same as new MTU as MTU changes. The change of IP MTU, however, does not affect MTU. IP MTU cannot be bigger than MTU configured on the current interface. Only when all devices connecting the same physical media must have the same MTU protocol can normal communication be created.

To set IP MTU on special interface, run the following command in interface configuration mode:

Command	Purpose
ip mtu *bytes*	Set IP MTU of the interface.

6. Authorizing IP source route

The routing switch checks the IP header of every message. The routing switch supports the IP header options defined by RFC 791: strict source route, relax source route, record route and time stamp. If the switch detects that an option is incorrectly selected, it will send message about the ICMP parameter problem to the source host and drop the message. If problems occur in the source route, the routing switch will send ICMP unreachable message (source route fails) to the source host.

IP permits the source host to specify the route of the IP network for the message. The specified route is called as the source route. You can specify it by selecting the source route in the IP header option. The routing switch has to forward the IP message according to the option, or drop the message according to security requirements. The routing switch then sends ICMP unreachable message to the source host. The routing switch supports the source route by default.

If the IP source route is disabled, run the following command in global configuration mode to authorize the IP source route:

Command	Usage Guidelines
ip source-route	Authorizing IP source route.

63.1.2 Configuring performance parameters

Run the following command to adjust IP performance.

1. Setting the wait time for TCP connection

When the routing switch performs TCP connection, it considers that the TCP connection fails if the TCP connection is not created during the wait time. The routing switch then notifies the upper-level program of the failed TCP connection. You can set the wait time for TCP connection. The default value of the system is 75 seconds. The previous configuration has no impact on TCP connections that the switch forwards. It only affects TCP connections that are created by the switch itself.

Run the following command in global configuration mode to set the wait time for TCP connections:

Command	Purpose
ip tcp synwait-time *seconds*	Set the wait time for TCP connection.

2. Setting the size of TCP windows

The default size of TCP windows is 2000 byte. Run the following command in global configuration mode to change the default window size:

Command	Purpose
ip tcp window-size *bytes*	Set the size of TCP windows.

63.1.3 Detecting and Maintaining IP Network

To detect and maintain the network, run the following command:

1. Clearing cache, list and database

You can clear all content in a cache, list or database. All incorrect data in a cache, list or database need be cleared.

Run the following command to clear incorrect data:

Command	Purpose
clear tcp statistics	To clear the statistics data about TCP, run the following command:

2. Clearing TCP connection

To disconnect a TCP connection, run the following command:

Command	Purpose
clear tcp {**local** host-name port **remote** host-name port | **tcb** address}	Clear the designated TCP connection. TCB refers to TCP control block.

3. Displaying statistics data about system and network

The system can display the content in the cache, list and database. These statistics data can help you know the usage of systematic sources and solve network problems.

Run the following commands in EXEC mode. For details, refer to "IP Service Command".

Command	Purpose
show ip access-lists *name*	Display the content of one or all access lists.
show ip sockets	Display all socket information about the routing switch.
show ip traffic	Display statistics data about IP protocol.
show tcp	Display information about all TCP connection states.
show tcp brief	Briefly display information about TCP connection states.
show tcp statistics	To display the statistics data about TCP, run the following command:
show tcp tcb	Display information about the designated TCP connection state.

4. Displaying debugging information

When problem occurs on the network, you can run debug to display the debugging information.

Run the following command in EXEC mode. For details, refer to "IP Service Command".

Command	Purpose
debug arp	Display the interaction information about ARP.
debug ip icmp	Display the interaction information about ICMP.
debug ip raw	Display the information about received/transmitted IP

	message.
debug ip packet	Display the interaction information about IP.
debug ip tcp	Display the interaction information about TCP.
debug ip udp	Display the interaction information about UDP.

63.2 Configuring Access List

63.2.1 Filtering IP Packet

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

- Controlling packet transmission on the interface
- Controlling virtual terminal line access
- Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the permit/forbid conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following steps:

1. Create the access list by designating the access list name and conditions.
2. Apply the access list to the interface.

63.2.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

NOTE: The standard access list and the extensible access list cannot have the same name.

Run the following command in global configuration mode to create a standard access list:

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.
deny {*source [source-mask]* | **any**}[**log | location**] or **permit** {*source [source-mask]* | **any**}[**log | location**]	Designate one or multiple permit/deny conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Command	Purpose
ip access-list extended *name*	Use a name to define an extensible IP access list.
{**deny | permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {**deny | permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**]	Designate one or multiple permit/deny conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. (precedence means the priority of the IP packet; TOS means Type of Service.)
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, you cannot add the command line to the designated access list. However, you can run no permit and no deny to delete items from the access list.

NOTE: When you create the access list, the end of the access list includes the implicit deny sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.
After the access list is created, the access list must be applied on the route or interface. For details, refer to section 3.2.3 "Applying the Access List to the Interface".

63.2.3 Apply the Access List to the Interface

After the access list is created, you can apply it to one or multiple interfaces including the in interfaces and out interfaces. Run the following command in interface configuration mode.

Command	Purpose
ip access-group *name* {in | out}	Apply the access list to the interface.

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the routing switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.
For the standard access list of the out interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the extensible access list, the routing switch also

checks the access list of the receiving side. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.
If the designated access control list does not exist, all packets are allowed to pass through.

63.2.4 Extensible Access List Example

In the following example, the first line allows any new TCP to connect the destination port after port 1023. The second line allows any new TCP to connect the SMTP port of host 130.2.1.2.

ip access-list extended aaa

permit tcp any 130.2.0.0 255.255.0.0 gt 1023

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in

Another example to apply the extensible access list is given. Suppose a network connects the Internet, you expect any host in the Ethernet can create TCP connection with the host in the Internet. However, you expect the host in the Internet cannot create TCP connection with the host in the Ethernet unless it connects the SMTP port of the mail host.
SMTP connects with TCP port in one end and the arbitrary port number in the other end. During the connection period, the same two port numbers are used. The mail packet from the Internet has a destination port, that is, port 25. The outgoing packet has a contrary port number. In fact, the security system behind the routing switch always receives mails from port 25. That is the exact reason why the incoming service and the outgoing service can be uniquely controlled. The access list can be configured as the outgoing service or the incoming service.
In the following case, the Ethernet is a B-type network with the address 130.20.0.0. The address of the mail host is 130.20.1.2. The keyword established is only used for the TCP protocol, meaning a connection is created. If TCP data has the ACK or RST digit to be set, the match occurs, meaning that the packet belongs to an existing connection.

ip access-list aaa

permit tcp any 130.20.0.0 255.255.0.0 established

permit tcp any 130.20.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in

63.3 Configuring IP Access List Based on Physical Port

63.3.1 Filtering IP Packet

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

- Controlling packet transmission on the interface
- Controlling virtual terminal line access
- Limiting route update content

The section describes how to create IP access lists and how to use them.
The IP access list is an orderly set of the permit/forbid conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS

accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following steps:

1. Create the access list by designating the access list name and conditions.
2. Applying ACL on a port

63.3.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

NOTE: The standard access list and the extensible access list cannot have the same name.

Run the following command in global configuration mode to create a standard access list:

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.
deny {*source [source-mask]* | **any**} [**log | location**] or **permit** {*source [source-mask]* | **any**} [**log | location**]	Designate one or multiple permit/deny conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Command	Purpose
ip access-list extended *name*	Use a name to define an extensible IP access list.
{**deny | permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {deny | permit} *protocol* any any [precedence *precedence*] [tos *tos*] [log] [time-range time-range] [location location] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [totallen eq|gt|lt lentgh] [ttl eq|gt|lt time] [offset-not-zero] [offset-zero]	Designate one or multiple permit/deny conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. precedence means the priority of the IP packet; TOS means Type of Service. If protocol is TCP/UDP, designate a single or 14 port number in a certain range. For more details, refer to Access List Configuration Example.
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, you cannot add the command line to the designated access list. However, you can run no permit and no deny to delete items from the access list.

NOTE: When you create the access list, the end of the access list includes the implicit deny sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

After ACL is established, it must be applied on the lines or ports. For details, refer to section "Applying the Access List to the Interface".

63.3.3 Applying ACL on Ports

When ACL is established, it will be applied on one or multiple ports, or on the ingress port or egress port.

Run the following command to apply IPv6 ACL on a port:

Command	Purpose
ip access-group *name*	Applying ACL on a port

After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the routing switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. If not permit, the system will discard the packet and returns an ICMP packet that host can reach.

If the designated access control list does not exist, all packets are allowed to pass through.

63.3.4 Extensible Access List Example

1. Port-based IP access list supporting TCP/UDP port filtration

The format is as follows:

{**deny | permit**} {tcp | udp}

source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt } port] }]

destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt } port] }]

[**precedence** *precedence*] [**tos** *tos*]

If you configure the access list by defining the port range, pay attention to the following:

(1) If you use the method of designating the port range to configure the access list at the source side and the destination side, some configuration may fail because of massive resource consumption. In this case, you need to use the fashion of designating the port range at one side, and use the fashion of designating the port at another side.

(2) When the port range filtration is performed, too many resources will be occupied. If the port range filtration is used too much, the access list cannot support other programs as well as before.

2. Port-based IP access list supporting TCP/UDP designated port filtration

In the following example, the first line allows any new TCP to connect the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface  g0/1
ip access-group aaa
```

Chapter 64 IP ACL Application Configuration

64.1 Applying the IP Access Control List

64.1.1 Applying ACL on Ports

After an ACL is established, it can be applied on one or many slots or globally.

Run the following command in port configuration mode:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] {ip | ipv6} access-group *name*	Applies the established IP access list to an interface or cancels the applied IP on the interface. Name IP: Name of the IP access list.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Run the following command in global configuration mode:

Command	Purpose
config	Enters the global configuration mode.
[no] {ip | ipv6} access-group *name* [vlan {*word* | add *word* | remove *word*}]	Applies the established IP access list on the global mode or cancels the applied IP on the global. **Egress** means that the ACL is applied in an outbound direction. **Vlan** means that the ACL is applied in an inbound VLAN. **Word** stands for the VLAN range table. **Add** means to add the VLAN range table. **Remove** means to delete the VLAN range table.
exit	Goes back to the EXEC mode.
write	Saves the settings.

NOTE: IP access list can be applied to VLAN in the global mode, but not to VLAN in port configuration mode.

Chapter 65 Routing Protocol Overview

65.1 IP Routing Protocol

The router of the Company implements multiple IP dynamic routing protocol. They will be introduced in the description of each potocol in this Chapter.

IP routing protocols are classified into two categories: interior gateway router protocol (IGP) and exterior gateway router protocol (EGP). The routers of our Company support RIP, OSPF, BGP and BEIGRP. RIP, OSPF, BGP and BEIGRP can be configured separately on real needs. The router of our company supports simultaneous configuration of multiple routing protocol, including unlimited OSPF (if memory is sufficient) processes, a BGP process, a RIP progress and unlimited BEIGRP processes. Command "redistribute" can be used to inject other router protocols into the database of current routing protocol so that the multiple routing protocols can be associated.

In order to configure IP dynamic routing protocol, the corresponding process shall be started and the corresponding network interfaces and the specific dynamic routing process should be associated, to indicate on which interfaces where the routing process run. To this end, the relevant steps for configuration shall be referred to in the corresponding document of configuration commands.

The routing device in this article refers to the switch.

65.2 Choosing Routing Protocol

The choice of routing protocol is a complicated process. When choosing a routing protocol, the following factors shall be taken into account:

- The size and complexity of the network
- Whether the support for VLSM is needed
- Network traffic
- Security requirement
- Reliability requirement
- Policy
- Others

The subject will not be detailed here. It is noted that the chosen routing protocol shall meet the real condition of network and comply with your requirements.

65.2.1 Interior Gateway Router Protocol

Interior Gateway Routing Protocol is used for the network in a single autonomous system. All the IP interior gateway routing protocol shall be associated with some specific networks (such as configuring: *network*) when it is launched. Each routing process listens to update messages from other routers on the network and broadcasts its own routing information on the network at the same time. The inside gateway router protocol supported by the router of the Company includes:

- RIP
- OSPF
- BEIGRP

65.2.2 Exterior Gateway Routing Protocol

Exterior gateway routing protocol is used for exchange routing information between different autonomous systems. It is usually required to configure the corresponding neighbors for exchanging routes, the reachable networks and local

autonomous system number. The exterior gateway routing protocol supported by the router of our company is BGP.

Chapter 66 Configuring VRF

66.1 Overview

One of the key of VPN is to keep safe and isolate data; it must be able to prevent communication of stations which belongs not to a same VPN. In order to differentiate VPN user route sent by which local interface on PE device, create virtual routes on PE device. Every virtual route has its own routing table and forwarding table. These routing tables and forwarding tables are called VRF (VPN Routing and Forwarding instances). One VRF includes the same station related routing table, interface (sub-interface), routing instances and routing policies. On PE, the physical port or the logic port with the same VPN corresponds to one VRF.

66.2 VRF Configuration Task List

If you would like to configure the VRF, the following tasks are necessary.

- Creating VRF Table
- Relating the interface to VRF
- Configuring the Target VPN Expansion Attribute of VRF
- Configuring Description of VRF
- Configuring Static Route of VRF
- Monitoring VRF
- Maintaining VRF
- Example of the VRF Configuration

66.3 Configuration Task

66.3.1 Creating VRF Table

To create VPN routing and forwarding table, do as follows in the global configuration mode:

Command	Purpose
PE_config#**ip vrf** ce	Enters VRF configuration mode, define VRF table.
PE_config_vrf_ce#**rd** ASN:nn or IP-address:nn	Designate the routing tag of VRF, create VRF routing and forwarding table
PE_config_vrf_ce#**route-target** [**export** | **import** | **both**] *ASN:nn or IP-address:nn*	Create input of VRF and output target VPN expansion attribute

66.3.2 Relating the interface to VRF

Relate the interface to VRF, do as follows:

Command	Purpose
PE_config#interface vlan 1	Enters the interface configuration mode
PE_config_v1#**ip vrf forwarding** *vrf-name*	Relate the interface to VRF
PE_config_v1#**ip address** *ip-address subnet-mask*	Configures the IP address of the interface.

66.3.3 Configuring the Target VPN Expansion Attribute of VRF

To configure the target VPN expansion attribute of VRF, do as follows:

Command	Purpose
PE_config#**ip vrf** ce	Enters the configuration mode of VRF
PE_config_vrf_ce#**rd** ASN:nn or IP-address:nn	Configures VRF routing tag and creates VRF table.
PE_config_vrf_ce#**route-target** [**export** | **import** | **both**]*ASN:nn or IP-address:nn*	Configures input of VRF and output target expansion attribute.
PE_config_vrf_ce#**import map** *WORD*	Configures route-map filter of the route adding to VRF routing table.
PE_config_vrf_ce#**export map** *WORD*	Add target VPN expansion attribute complying with route-map condition to the output target VPN expansion attribute of VRF.

Before publish the local route to other PE routing device, the entrance PE will add a route target attribute to every route learned from the direct station. The target value affiliated to the route is based on the VRF value configured in the output target expansion attribute.

Before installing the remote route published by other PE on the local VRF, every VRF on the entrance PE route device will be configured with one input target expansion attribute. The PE routing device can only be installed on a certain VRF until the routing target attribute borne by VPN-IPv4 matching with the VRF input target.

66.3.4 Configuring Description of VRF

To configure the description of VRF, do as follows:

Command	Purpose
PE_config#**ip vrf** ce	Enters VRF configuration mode.
PE_config_vrf_ce#**rd** ASN:nn or IP-address:nn	Configures VRF routing tag, and creates VRF table.
PE_config_vrf_ce# **description** LINE	Configures description of VRF.

66.3.5 Configuring Static Route of VRF

To configure the static route of VRF, do as follows:

Command	Purpose
PE_config#**ip vrf** ce	Enters VRF configuration mode.
PE_config_vrf_ce#**rd** ASN:nn or IP-address:nn	Configures VRF routing tag and creates VRF table.
PE_config_vrf_ce#**exit**	Exits from VRF configuration mode.
PE_config#**ip route** [**vrf** vrf-name] dest mask { type num | nexthop } [distance]	Configures VRF static route.

66.3.6 Monitoring VRF

To monitor VRF, show the statistics of VRF. To monitor, do as follows:

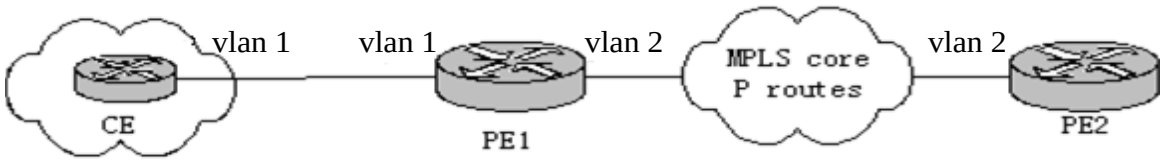
Command	Purpose
PE#show ip vrf	Shows VRF and its associated port information.
PE#show ip vrf [{brief | detail | **interfaces**}] *vrf-name*	Shows VRF configuration and its associated port information.
PE#**show ip route vrf** *vrf-name*[A.B.C.D | all | beigrp | bgp | ospf | rip | connect | static | summary]	Shows the routing information in VRF routing table.

66.3.7 Maintaining VRF

Maintain VRF, track the main routing table and change of VRF routing table and VRF configuration information in the management mode and do as follows:

Command	Purpose
PE#debug ip routing	Track the addition, deletion and change of the route in the main routing table
PE #debug ip routing message	Track information VRF received and sent
PE #debug ip routing vrf *vrf-name*	Track the change of designated VRF routing table including adding, deleting and changing.

66.4 Example of the VRF Configuration



The configuration of the routing device is as follows:

Routing device CE:

```
interface loopback 0
 ip address 22.1.1.1 255.255.255.0
!
interface vlan 1
ip address 170.168.20.152 255.255.255.0
!
router ospf 1
 network 170.168.20.0 255.255.255.0 area 0
 network 22.1.1.0 255.255.255.0 area 0
!
```

Routing device PE1:

```
ip vrf pe1
rd 1:1
route-target 1:1
!
interface vlan 1
```

```
ip vrf forwarding pe1
ip address 170.168.20.153 255.255.255.0
!
interface vlan 2
 ip address 176.168.20.152 255.255.255.0
!
router ospf 1 vrf pe1
 network 170.168.20.0 255.255.255.0 area 0
!
router bgp 1
neighbor 176.168.20.154 remote-as 2

address-family vpnv4
 neighbor 176.168.20.154 activate
 exit-address-family

 address-family ipv4 vrf pe1
 no synchronization
 redistribute ospf 1
 exit-address-family
```

Routing device PE2:

```
ip vrf pe2
rd 1:1
route-target 1:1
!
interface loopback 0
 ip vrf forwarding pe2
 ip address 44.1.1.1 255.255.255.0
!
interface vlan 2
 ip address 176.168.20.154 255.255.255.0
!
router bgp 2
neighbor 176.168.20.153 remote-as 1

address-family vpnv4
neighbor 176.168.20.153 activate
exit-address-family

address-family ipv4 vrf pe2
no synchronization
redistribute connected
```

exit-address-family

Chapter 67 Static routing Configuration

67.1 Overview

Static routing is a special routing configuration, and is configured by an administrator. In the network that structure is relatively simple, you only need to configure static routes on network interoperability. Properly setting up and using static routes can improve network performance and be guaranteed bandwidth for important network applications.

The shortcomings of the static route is: It cannot automatically adapt to changes in network topology. When network failure or topology change, the route may be unreachable, resulting in network outages. Then administrator must manually modify the configuration of static routes.

Default route is used when the router cannot find a matching routing table entry:

- If the packet's destination address cannot match any entries in the routing table, the packet will select the default routing;
- If there is no default route and destination of the packet is not in the routing table, the packet will be discarded.

Default route can be configured with static routes and appear in the route table as the form of network 0.0.0.0/0.

67.2 Static Routing Configuration Task List

If you would like to configure the static routing, the following tasks are necessary.

- configure the relevant physical parameters of the interface
- configure the link layer attributes of the related interface
- configure the IP address of the relevant interface

67.3 Static Routing Configuration Task

67.3.1 Configure the Static Routing

To activate the static routing, the following steps shall be carried out under the global configuration mode:

Command	Purpose
ip route *A.B.C.D mask* {next-hop | interface} [distance] [tag tag] [global] [description]	Configure the Static Routing

67.4 Example of the Static Routing Configuration

To assign tothenetwork segment 10.0.0.0/8 packets port is interface vlan 1, the configuration command is as follows:

ip route 10.0.0.0 255.0.0.0 vlan 1

Chapter 68 Configuring RIP

68.1 Overview

The Route Information Protocol (RIP) is a relatively old but still commonly used Interior Gateway Protocol (IGP), which is mainly used in the small-sized network of the same kind. And RIP is a traditional Distance Vector Routing Protocol, which occurs in the RFC 1058.

RIP exchanges Routing Information through broadcasting UDP Packets. In the Router, the update Route Information will be sent every 30 seconds. In case that no update information from the neighbor router has been received within 180 seconds, the Routes from that neighboring router in the Routing Table will then be labeled as “Unusable”. And if there is still no updated information received in the next 120 seconds, these Routes will be deleted from the Routing Table.

The Hop Count is taken by the RIP as a metric to measure different routes. And the Hop Count refers to the number of the passed routers of packets from the Source to the destination. The metric of the Route that is directly connected to the Network is “0”, the metric of the Route whose network is not able to reach is “16”. As the Route metric used by the RIP is in a relatively small range, it is not applicable to large-scale network.

If a router has a default route, RIP then will advertises the route to the false Network of 0.0.0.0. In fact, the 0.0.0.0 network does not exist, which is only used for realizing the function of default route in RIP. If the RIP has learned a default route, or the default gateway is configured in router and configured with default metric, the router will then announce the default network.

The RIP will send the updates to the interface of the appointed network. If the network of the very interface is not appointed, the network then will not be announced in any RIP updating.

The RIP-2 of our company's router supports Plaintext and MD5 Authentication, Route Summary, CIDR and VLSM.

68.2 RIP Configuration Task List

If you would like to configure the RIP, the following tasks are necessary. While you have to first activate the RIP, the other tasks are optional.

- Starting the RIP
- Enabling Unicasting of RIP route update messages.
- Applying the offset on the route metric
- Regulating the Timer
- Designating the RIP Version Number
- Activating the RIP Authentication
- Activating the ‘Passive’ and ‘Deaf’ of the Interface
- Prohibitting Route summary
- Prohibitting the Authentication on Source IP Address
- Activating or Prohibit the split-horizon
- Example of RIP Configuration

68.3 RIP Configuration Task

68.3.1 Starting the RIP

To activate the RIP, the following steps shall be carried out under the global configuration mode:

Command	Purpose

router rip process-id [**vrf** vrf-name]	Activate the RIP Routing Process and enter the router configuration mode.

68.3.2 Generating the RIP instance interface

After the RIP instance is enabled, only the interfaces associated with the instance can generate RIP network segments and use these interfaces to exchange routing information. Instances need to be associated with interfaces. In the interface configuration mode, configure as the following steps:

Command	Purpose
router rip *process-id* enalbe	Associates the interface to the process-id instance.

To make an interface an active RIP interface (generate a direct route to the interface, and the interface can send and receive RIP protocol packets), you need to meet the following: the interface is associated with a RIP instance, the interface has a legal IP address, and the interface status is up.

In addition, when a RIP instance is enabled on an interface, if the instance's vrf and the designated vrf on the interface are inconsistent, the interface cannot become the active RIP interface until the interface's vrf is revised.

When an interface is associated with an uncreated RIP instance, the RIP instance will be created with the vrf on the interface (if vrf is specified) and the enable process-id.

Each interface can only belong to one RIP instance.

68.3.3 Allowing the mono-broadcasting updtaed and grouped by RIP Router

The RIP is a broadcasting-Type Protocol. If you would like the updating of routes to to access to the non-broadcasting type network, the router shall be configured so as to enable information exchange. To this end, the following commands shall be used under router configuration mode:

Command	Purpose
neighbor ip-address	Define a neighbor router to exchange with it the Routing Information.

In addition, if you would like to control which interface(s) that can be used to exchange routing information, the command “ip rip passive” can be used to designate an interface or some interfaces prohibiting the sending of the update of routes. If necessary, please refer to the relevant discussion on the route filtration in the "Filtrating the Routing Information" in the Chapter of " Protocol-Independent Commands in Configuring IP Router”.

68.3.4 Using the Offsets on the Route metric

Offset List is taken to increase an offset on the Input and Output Routes, which have been learned with the RIP. On the other hand, you can use the Access List or the interface to limit the Offset List. In order to increase the Route metric, the following commands should be executed in the router configuration mode:

Command	Purpose
offset-list {interface-type number | *} {**in**|**out**} access-list-name offset	Increase an offset on the route metric.

68.3.5 Regulating the Timer

Routing protocols use several timers to determine the frequency for sending the updating of routes, how long the router will become invalid and other parameters. You can regulate these timers so as to make the performance of the Routing Protocols more suitable to the requirements of the network.

It is also possible to regulate the Route Protocol to accelerate the Convergence Time of all kinds of the IP Routing computation, to quickly backup to the redundant router so as to minimize the time of quick recovery. To regulate the Timer, the following commands should be used under router configuration model.

Command	Purpose
timers holddown *value*	Regulating the time (Unit: Second) it take to delete certain route from the Routing Table
timers expire *value*	Regulating the time (Unit: Second) that the router is announced to be invalid.
timers update *value*	Regulating the frequency for sending the updating of the Router (the time interval between sedning of the updating of routing, (unit: Second)
timers trigger *value*	Trigger update interval (unit: s)
timers peer *value*	peer timeout interval (unit: s)

68.3.6 Appointing the RIP Version Number

The RIP-2 of our company's router supports Authentication, Password Management, Route summary, CIDR and VLSM. Under the default circumstance, the router can receive the updates of RIPv1 and RIPv2, while it can only send the updates of RIP-1. By configuration, the router can be set to receive and send the updates of RIPv1 only, or receive and send the updates of RIPv2 only. For this purpose, the following commands should be taken in the router configuration mode:

Command	Purpose
version {1 | 2}	Configure the router to send and receive the updates of RIPv1 or RIPv2 only.

The above tasks are controlling the default behavior of the RIP. And you can also configure a certain interface to change this default behavior. In order to control the interface to send the RIP-1 updates or the RIP-2 updates, the following commands shall be used under interface configuration mode.

Command	Purpose
ip rip send version 1	Configure the interface to send the updates of RIP-1 only.

ip rip send version 2	Configure the interface to send the updates of RIP-2 only.
ip rip send version compatibility	Send by broadcasting the Updating of RIP-2.message.
ip rip v1demand	Send RIP-1 packets when request is sent.
ip rip v2demand	Send RIP-2 packets when request is sent.

At the same time, to control the interface to receive the updates of RIP-1 and RIP-2, the following commands shall be used under the interface configuration mode:

Command	Purpose
ip rip receive version 1	Configure the interface to receive the updates of RIP-1 only.
ip rip receive version 2	Configure the interface to receive the updates of RIP-2 only.
ip rip receive version 1 2	Configure the interface to receive the updates of RIP-1 and RIP-2.

68.3.7 Activating the 'Passive' and 'Deaf' of the Interface

By default the interface covered by RIP can forward and receive the routing update by flexibly applying the RIP protocol.
To configure the passive and deaf status of the interface in the interface configuration mode:

Command	Purpose
Ip rip passive	The interface will not forward the rip protocol grouping.
ip rip deaf	The interface does not receive rip protocol grouping.

68.3.8 Activating RIP Authentication

RIP-1 does not support authentication. If the grouping of RIP-2 is forwarding and receiving, the RIP authentication can be activated on the interface.
Multiple authentication modes are supported on RIP activated interface: plaintext authentication, MD5 authentication, dynamic authentication (md5 and sha1). Each RIP-2 grouping uses plaintext authentication by default.
Note:
If considering safety, do not use the plaintext authentication in RIP grouping, this is because the authentication key without encryption is forwarded to each RIP-2 grouping. If safety is not considered (for instance, the host with error configuration cannot participate in the route), the plaintext authentication is available.
To configure RIP plaintext authentication, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication simple	Configures the interface with the plaintext authentication.
ip rip password *string*	Configures the plaintext authentication key.

To configure MD5 authentication of RIP, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication md5	Configures the interface with MD5 authentication.
ip rip md5-key *key-ID* md5 *key*	Configures MD5 authentication key and authentication ID.

To configure the dynamic authentication of RIP, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication dynamic	Configures the interface with dynamic authentication (md5 and sha1).
ip rip dynamic-key *key-ID* { **md5 | sha1** } *key xxxx-xx-xx-xx:xx xx:xx*	Configures dynamic authentication key and authentication ID.

After configuring the RIP authentication configuration, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication commit	If the authentication cannot pass, age the opposite end peer and the route learned from the opposite end.

68.3.9 Prohibitting the Route summary

Under the default circumstance, the RIP-2 supports the automatic route summary, summarizing the RIP-2 Routes when crossing the boundary of the classified network. And the RIP-1 Automatic Route Gathering Function is always activated.
If there is a separated Sub-net, it is necessary to prohibit the Route summary to declare this Sub-net. If the Route Gathering is prohibited, when crossing the boundary of the classified network, the router will then send the route information of the sub-net and the host. Under the router configuration mode, the following command should be taken to prohibit the automatic gathering.

Command	Purpose
no auto-summary	Prohibit the Automatic summary

68.3.10 Prohibitting the Authentication of Source IP Address and Zero-domain

Under the default circumstance, the router will authenticate the Authenticable Source IP Address of the received route update. If this address is illegal, the router update will then be rejected.

If you have a router in hope to receive the updating from it, but you have not configured the corresponding "network" or "neighbor" on the receiver, the function should be therefore prohibited. However in the common practice, this command is not recommended to use. Under router configuration mode, the following commands will prohibit the default function of authenticating the source IP address in incoming route updates.

Under the default circumstance, the router will authenticate the zero-domain of the received route entry under version 1. If the corresponding field fails the authentication of the zero-domain, the routing entry will be discarded. If the configuration does not enable this authentication, it may cause the local to learn the wrong routing information from the peer.

Command	Purpose
no validate-update-source	Prohibit to authenticate the Source IP Address of the incoming RIP Router Updating.
no check-zero-domain	Prohibit to authenticate zero-domain of the incoming RIP Router Updating.

68.3.11 Maximum Number of Equivalent Routes

By default, the local RIP routing table can contain up to 4 equivalent routes. When learning routing information from multiple neighbors on one or some same network segments to generate equivalent routes, if the number of equivalent routes on a certain network segment is greater than the current maximum number of equivalent routes, it cannot be added to the RIP database.

Run the commands in the following table to configure the maximum number of the equivalent routes in the local RIP routing table in router configuration mode.

Command	Purpose
maximum-nexthop *number*	Configures the maximum number of equivalent routes for the RIP routing table.
No maximum-nexthop	Resumes the default maximum number of the routes in the RIP routing table.

68.3.12 Activating or Prohibit the Horizontal Split

Normally, the router, which is connected with IP Network and using the Distance Vector Routing Protocol, takes split-horizon to lower the possibility of route loops. The Split-Horizon prevents the announcements of route information to the receiving interface of this route information. In this way, communication within several routers (especially when the loop breaks) will be optimized. However, to Non-broadcasting Network (such as FR), things are not so easy. And maybe you have to prohibit the Horizontal Split.

If an interface has been configured with a supplementary IP Address and he Horizontal Split has been activated, the update-Source IP Address of the route update may not include every secondary IP address. The source IP address of one route update includes only one Network Number (unless the split-horizon is Prohibited).

In order to activate or prohibit the Horizontal Split, the following commands should be taken under interface configuration mode:

Command	Purpose
ip rip split-horizon {simple | poisoned}	Activate the Split- Horizon
no ip rip split-horizon {simple | poisoned}	Prohibit the Split- Horizon

Under the default circumstance, for the point to Point Interface, the Split-Horizon is activated; For Point-to multiple point Interface, the Split-Horizon is prohibited. The optional parameters **simple** and **poisoned** represent simple horizontal split and poisoned reversal horizontal split respectively.

Please refer to the specific example of using Split-Horizon in the "Examples of Split-Horizon" in Section of this Chapter.

NOTE: Commonly, it is suggested that the default state remain unchanged unless you are sure that your application can't declare the route correctly until you change its state. Always remember: if the Split-Horizon is prohibited on a serial interface (and the interface is connected with a Packet-switched Network), you have to prohibit Split-Horizon to all routers in any relevant Multicast Group on that Network.

68.3.13 Monitoring and Maintainance of RIP

With the RIP monitored and maintained, the Network Statistics can be displayed, such as: RIP protocol Parameter Configuration, Network utilization, Real-time Tracing of Network Communication and so on. Such information can help you judge the use of Network Resource and further solve the network problems and know the reachability of network nodes.

The following commands can be used to display the statistics information of all kinds of routes under management statistics:

Command	Purpose
show ip rip	Displays the present Status of all RIP.
Show ip rip *process-id*	Displays the present Status of designated RIP.
show ip rip *process-id* database	Displays all routes of RIP
show ip rip *process-id* protocol	Displays all the relevant information of RIP Protocol
Show ip rip *process-id* interface	Displays all interfaces and interface states of designated RIP.
show ip rip *process-id* peer	Displays all peers and states of designated RIP.

Under the management mode, the following commands shall be used to trace route protocol information.

Command	Purpose
debug ip rip database	Trace the procedure information of RIP Routing such as Insertion into the Routing Table, Deletion from the

	Routing Table, Changes of Routes and so on.
debug ip rip packet [send | receive]	Trace the RIP protocol messages.
debug ip rip message	Trace the RIP event, such as timer timeout.

68.4 Example of the RIP Configuration

Two switches A and B are configured as follows:

Router A

interface vlan1

ip address 192.168.20.81 255.255.255.0

ip rip 1 enable

!

interface loopback 0

ip address 10.1.1.1 255.0.0.0

ip rip 1 enable

!

router rip 1

!

Router B

interface vlan1

ip address 192.168.20.82 255.255.255.0

ip rip 1 enable

!

interface loopback 0

ip address 20.1.1.1 255.0.0.0

ip rip 1 enable

!

router rip 1

!

Chapter 69 BEIGRP Dynamic Routing Protocol Configuration

69.1 Overview

The technology used by BEIGRP is similar to distance vector routing protocol:

- The router only makes routing decisions with the information provided by directly connected neighbours;
- The router only provides the routing information it uses to the directly connected neighbors.

But, BEIGRP has some main differences with distance vector routing protocol, which entitles it to have more advantages:

- BEIGRP saves all routes from all neighbours in the topology table, not just the best routes so far;
- BEIGRP can make query to the neighbors when it is unable to access the destination and no alternative routes are available, so, the convergence speed of BEIGRP can compete with the best link-state protocol.

Diffused Update Algorithm (DUAL) is vital for BEIGRP's superiority to other traditional distance vector routing protocol. It always works actively and queries the neighbous when it is unable to access the destination and there is no alternative routes (feasible replacement). As the convergence process is active rather than negative (negatively waiting for the timeout of the routers), so the convergence speed of BEIGRP is very quick.

BEIGRP is a specific routing protocol designed to adapt to the requirements of EIGRP and is directly based on IP. It meets the following requirements of BEIGRP:

- Dynamically discover new neighbor and the disappearance of old neighbors through "Hello" message;
- So the transfer of data are all reliable;
- The transfer protocol permits unicast and multicast data transfer;
- The transfer protocol itself can adapt to the change of network condition and neighbor responding;
- BEIGRP can limit the percentage of its occupation of the bandwidth according to the requirements

69.2 BEIGRP Configuration Task List

To complete the configuration of BEIGRP the following tasks are required to be done, among them, the activation of BEIGRP is necessary while others can be decided according to the requirement.

- Activate BEIGRP protocol
- Configure the sharable percentage of bandwidth
- Adjust the arithmetic coefficient of BEIGRP composite distance
- Using "offset" to adjust the composite distance of the router
- Turn off auto-summary
- Redistributing other routes
- Customize route summary
- Configure other parameters of BEIGRP
- Disable horizontal separation
- The supervision and maintenance of BEIGRP

69.2.1 Activating BEIGRP Protocol

In order to create a BEIGRP process, it is required to execute the following commands:

Command	Purpose
router beigrp *as-number*	Add a BEIGRP process under global configuration mode
network network-number network-mask	Add addresses to this BEIGRP process under router configuration mode

After finishing the above configuration, BEIGRP will start to run on all interfaces belonging to this address, discoveres new neighbours through "Hello" and carryes out initial routing interaction through "update".

69.2.2 Configuring the Sharable Percentage of Bandwidth

Under default circumstances, BEIGRP can occupy 50% of the bandwidth at most. You may wish to change this default value in order to guarantee the normal interaction of other data, or wishes to adjust the actually usable bandwidth of BEIGRP through the command when the interface is configured with a bandwidth not fit for actual situation. Under these conditions, you can use the following commands under interface configuration mode:

Command	Purpose
ip beigrp bandwidth-percent *percent*	Configure the maximum percentage of BEIGRP messages' occupation of the bandwidth

69.2.3 Adjusting the Arithmetic Coefficient of BEIGRP Composite Distance

Under certain situations, the arithmetic co-efficient of BEIGRP composite distance may need to be adjusted, and finally influences the routing policy of the router. Although the default arithmetic co-efficient of BEIGRP can satisfy most networks, but it may still need to be adjusted under some particular conditions. But this adjust may bring great change to the whole network, so it must be performed by the most experienced engineers.
Use the following command under router configuration mode:

Command	Purpose
metric weights *k1 k2 k3 k4 k5*	Adjust the arithmetic co-efficient of BEIGRP composite distance.

69.2.4 Using "Offset" to Adjust the Composite Distance of the Router

We use offset list to purposely add all incoming and outcoming routes according to the requirement, or the composite distance of certain routes meeting the requirements. The aim of this approach is to finally influence the routing result of the router, and meets our expected result. During the process of configuration, the user can designate access list or application interface in the offset list selectively and according to your requirements, in order to more clearly notify which routes to carry out operations to increase offset. Looking at the following command:

Command	Purpose
offset{type number | *} {**in** | **out**} access-list-name offset	Apply an offset list.

69.2.5 Turning off Auto-Summary

The automatic summary of BEIGRP is turned off by default, and it is not currently supported:

Command	Purpose
no auto-summary	Turn off auto-summary.

69.2.6 Redistributing Other Routes into the BEIGRP Process

The **redistribute** operation follows the below rules:

- It isn't have to configure the command "default-metric" when redistribute the static routes and the connected routes. The related parameter (such as: bandwidth, delay, reliability, load and MTU) is attained from the related interface.
- It isn't necessary to configure the command "default-metric" when redistribute the routes of other BEIGRP process. The related parameter is attained from the BEIGRP process redistributed.
- It is necessary to configure the command "default-metric" when redistribute the routes of others protocol (such as: rip, OSPF). The related parameter is validated by the configuration of "default-metric". If we redistribute the routes of these types without the command "default-metric", the redistribution doesn't work.

In a router running the BEIGRP protocol and the RIP protocol, the following commands must be configured when we need obtain the routes from RIP protocol to BEIGRP protocol.

Command	Purpose
default-metric bandwidth delay reliability loading mtu	configure the default parameter of redistribute
redistribute *protocol [process]* [**route-map** *name*]	redistribute the routes to BEIGRP protocol.

69.2.7 Configuring Other Parameters of BEIGRP

In order to adapt to different network environments, and to make BEIGRP be more effectively and fully functions, we may need to adjust the following parameters:

- Adjust the time interval of BEIGRP to send “hello” messages and the timeout death time of the neighbours
- Turn off split-horizon

1. Adjusting the time interval of BEIGRP to send "hello" messages and the timeout death time of the neighbors

BEIGRP hello protocol archieves 3 objectives to enable correct BEIGRP operation:

- It discovers accessible new neighbors. The discovery is automatic and requires no manual configuration;
- It checks neighbors’ configuration and only permits communication with the neighbours configured with compatible mode.
- It continues to maintain the availability of the neighbors and detects the disappearance of the neighbors.

The router sends “hello” multicast packet on all interfaces running BEIGRP. All routers support BEIGRP receive these multicast groups, so that it can discover all neighbours.

“Hello” protocol uses two timers to detect the disappearance of the neighbours: hello interval defines the frequency of

sending BEIGRP hello messages on the interface of the router, while hold timer defines the interval of time the router has to wait for the communication data from the designated neighbor before the declaration of the neighbour's death. We ordered that every time it receives BEIGRP packet from the neighbour router, it resets the hold timer.

Different network type or network bandwidth will use different default value of hello timer:

Interface type encapsulation		Hello timer (second)	Hold timer (second)
LAN interface	Any	5	15
WAN interface	HDLC or PPP	5	15
	NBMA interface, bandwidth<=T1	60	180
	NBMA interface, bandwidth>T1	5	15
	The point-to-point sub-interface of NBMA interface	5	15

The difference of the default value of the timer in Hello protocol may induce the result that the BEIGRP neighbours connected to different IP sub-network use different hello and hold timer. To resolve the problem, the hello packet of every router designates its own hold timer, every BEIGRP router uses neighbour's the designated hold timer of the hello group to decide the timeout of this neighbour. Here, it can enable the appearance of different neighbour error detection timers in the different stands of the same WAN nephogram. But under some particular situation, the default value of the timer cannot be met, so if you want to adjust the time interval of sending hello messages, use the following command:

Command	Purpose
ip beigrp hello-interval *seconds*	Adjust the time interval of sending hello message from this interface

If you wish to adjust the timeout timer of the neighbour, use the following command:

Command	Purpose
ip beigrp hold-time *seconds*	Adjust the timeout death time of the neighbor

2. Shutting down the horizon split

Commonly, we wish to use split-horizon. It will prevent the routing information from one interface to be broadcasted back to the same interface, so as to avoid route loop. But under certain circumstances, this is not the optimized choice, and then we can use the following command to disable split-horizon:

Command	Purpose
no ip beigrp split-horizon	Turn off horizontal split

69.2.8 Monitoring and Maintaining BEIGRP

To clear the neighbourship with all neighbours, use the following command:

Command	Purpose
clear ip beigrp neighbors [*as-number*| *interface*]	To clear the neighborship with all neighbours

In order to show various statistics information of BEIGRP, execute the following commands:

Command	Purpose
show ip beigrp interface [*interface*] *[as-number*]	show interface information
show ip beigrp neighbors [*as-number*| *interface*]	show neighbor information
show ip beigrp topology [*as-number*| all-link | summary | active]	show topology information

69.3 Examples of BEIGRP configuration

None

Chapter 70 Configuring OSPF

70.1 Overview

OSPF is an IGP Route protocol developed by the OSPF Working Group of IETF. The OSPF, which is designed for the IP Network, supports the IP Sub-network and the External Route Information Label and at the same time allows the authentication of message and supports the IP Multicast.

The implementation of OSPF of our company complies with the OSPF V2 specification (Refers to RFC2328). Some key feathers in the implementation are listed in the following:

- Stub Area--Supporting the Stub Area
- Route redistribution--Any route, formed by and learned a routing protocol, can always be redistributed to the other route protocol Domain. Within the autonomous System, it means that OSPF can input the route learned by the RIP. And the routes learned by OSPF can also be redistributed to the RIP. Between autonomous Systems, OSPF can input the routes learned by BGP; and OSPF routes can also be injected to BGP.
- Authentication--The Plaintext and MD5 Authentications are supported between the neighboring routers within a area.
- Router Interface Parameters--The configurable Parameters include: Outgoing Cost, Retransmission Interval, Interface Transmission Delay, router Priority, Judgement on the router Switching-off Interval, the Interval of Hello Message and the Authentication Password.
- NSSA area--Refer to RFC 1587
- OSPF---RFC 1793 on the virtual circuit.

70.2 OSPF Configuration Tast List

OSPF requires to exchange routing data among all routers, ABR and ASBR in a area. In order to simplify the configuration, you may let them all work under default parameters without authentication, etc… but if you want to alter some parameters, you should guarantee the identity of the parameters on all routers.

In order to configure OSPF complete the following tasks. Besides the necessity of activating OSPF, other configurations are all optional.

- Start OSPF
- Configure the interface parameters of OSPF
- OSPF configuration on network type
- Configuring One-to-Multiple Broadcast Network
- Configuring Non-Broadcasting Network
- Configure OSPF domain
- Configuring the NSSA Area of OSPF
- Configure route summary within OSPF domain
- Configure the summary of a forward router
- Create default route
- Select router ID through LOOPBACK interface
- Configure the management distance of OSPF
- Configure the route calculating timer
- Enable the On-Demand link configuration
- The supervision and maintenance of OSPF

In addition to that, about configuring route redistribution, please refer to the related content about "Route Redistribution" of "Protocol-independent Feather Configurations of IP routing Protocol".

70.3 OSPF Configuration Task

70.3.1 Starting OSPF

Like other routing protocols, activating OSPF demands creating OSPF routing process, allocation of an IP address range related to the executing process, allocation of an area ID related to IP address range. Under the global configuration mode, use the following commands:

Command	Purpose
router ospf *process-id*	This command activates OSPF routing protocol, and enters router configuration mode.
network address mask **area** area-id	This command configures the interface(s) running OSPF and the area ID of the interface

70.3.2 Configuring the Interface Parameter of OSPF

During the implementation of OSPF, it is permitted to change the OSPF parameters related to interface according to the requirement. There is no need to change any parameter, but you should guarantee the identity of certain parameters on all routers on connected network.

Under interface configuration mode, use the following commands to configure interface parameters:

Command	Purpose
ip ospf authentication	Configures the authentication method for OSPF interface to send and receive packets.
ip ospf cost *cost*	Configures the metric of OSPF interface to forward packets.
ip ospf retransmit-interval *seconds*	The seconds taken to retransmit LSA between the neighbors belonging to the same OSPF interface.
ip ospf transmit-delay *seconds*	Configures the estimated time to transmit LSA on an OSPF interface (second as the unit).
ip ospf priority *number*	Configures the priority of router to become the DR router
ip ospf hello-interval *seconds*	Configures the time interval to send hello packet on OSPF interface.
ip ospf dead-interval *seconds*	If the router does not receive "hello" packet from the neighbor within the time interval defined, it considers the neighbor router to be turned off.
ip ospf password *key*	It is an authentication password of the adjacent router in an address, which uses simple password authentication of OSPF.

ip ospf message-digest-key *keyid* md5 *key*	Demand OSPF to use MD5 authentication.
ip ospf passive	Not send "hello" message on the interface.
ip ospf mtu-ignore	Do not check the mtu value in the packet on the port.

OSPF divides the physical media of the network into the following three categories:

- Broadcast network (Ethernet, Token Ring, FDDI)
- Non-broadcast, multi-access network (SMDS, Frame Relay, X.25)
- Point-to-point network (HDLC, PPP)

Can configure your network or broadcast network or non-broadcast multi-access network.

X.25 and Frame Relay networks provide optional broadcast capability. OSPF can be configured to work on broadcast networks through the map command. For the Map command, please refer to the description of the x.25 and Frame Relay map commands in the WAN Command Reference.

70.3.3 Configuring OSPF Network Type

No matter what the physical media type of the network is, you can configure your network to be broadcasting network or non-broadcasting, multi-access network. Using this feature, you can flexibly configure the network, you can configure the physical broadcasting network to be a non-broadcasting, multi-access network; you can also configure non-broadcasting network (X.25, Frame Relay, and SMDS) to be broadcasting network. This feature also reduces the configuration of the neighbors, for detailed information, please refer to the related content of non-broadcasting network's configuration of OSPF.

Configure non-broadcasting, multi-access network to be broadcasting network or non-broadcasting network, that is, to suppose there exists virtual links from every router to other routers, or suppose they consist of a full-mesh network. Because of the restriction of expenses, it is usually not practical; or a partially full-mesh network. Under this situation, you can configure a point-to-multiple point network. Routers not adjacent to each other can exchange routing information through virtual links.

OSPF point-to-multiple point interface can be defined as several point-to-point network interfaces, which creates multiple host routes. OSPF point-to-multiple point network has the following advantages over non-broadcasting, multi-access network and point-to-point network:

Point-to-multiple point network is easy to configure, it does not demand neighbor configuration command, it only uses one IP and will not produce DR.

Because it does not need to full-mesh network topology, it costs less.

It is more reliable. Even when virtual links fail, it can still maintain the connection.

Under interface configuration mode, configure OSPF network type with the following command:

Command	Purpose
ip ospf network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast] }}	This command configures the network type of OSPF.

At the end of this chapter, you can see an example of the configuration of OSPF point-to-multiple point network.

70.3.4 Configuring One-to-Multiple Broadcast Network

You do not need to describe the neighbor relations in point-to-multiple point network and broadcasting network. But you can use command "neighbor" to describe the priority of a certain neighbor.

Before using this command, some OSPF point-to-multiple point protocol traffic is multicast traffic. So for point-to-multiple point interface, command "neighbor" is not needed. Packet "hello", update packet and confirmation packet are all transmitted through broadcasting form, especially, multicast "hello" packet can dynamically discover all neighbors.

In point-to-multiple point network, the router supposes that all neighbors have the same metric. This value can be configured through command "ip ospf cost". In fact, the bandwidth of every neighbor is different, so the value should be different. This feature only applies to point-to-multiple point interface.

Using the following command to configure the interface to be point-to-multipoint interface and allocate a metric for each neighbor:

Command	Purpose
ip ospf network point-to-multipoint	On broadcasting media, configure the interface to be a point-to-multiple point network
exit	Return to global configuration mode
router ospf *process-id*	Configure an OSPF router process and enter into router configuration mode.
neighbor ip-address **cost** number	Designate a neighbor and allocate a metric for it. Repeat the above configuration command for each neighbor who wants to specify the weight. Otherwise, the weight of the neighbor uses the weight specified by the ip ospf cost command.

70.3.5 Configuring Non-Broadcasting Network

Because there are many routers in the OSPF network, so there must be one DR elected for the network. If the broadcasting ability is not configured, it is requested to perform parameter configuration for the selection process.

These parameters only carry out configuration on the routers that are eligible to become DR or BDR.

Under router configuration mode, use the following command to configure routers of non-broadcasting network which are mutually related:

Command	Purpose
neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Configure the router connected to the non-broadcasting network

You can designate the following parameters for a neighbor router:

- The precedence of neighbor router.
- Non-broadcasting poll interval.
- Interface accessible to the neighbor

In point to multiple point, non-broadcasting network, you can use command "neighbor" to designate neighbor relation.

Allocate an optional priority.

In the previous software versions, some users configure point to multipoint connections on non-broadcasting media (IP over ATM), so the router cannot dynamically discover its neighbor router. This feature permits the usage of command "neighbor" on point to multipoint interface.

In a point to multipoint network, the router supposes all neighbors have the same metric. This value can be configured through the command "ip ospf cost". In fact, as the bandwidth of each neighbor is different, the value should also be different. This feature only applies to point to multiple point interfaces.

Under interface configuration mode, use the following command to configure point to multiple point interfaces on media that do not support broadcasting.

Command	Purpose
ip ospf network point-to-multipoint non-broadcast	Configure point to multiple point interface on non-broadcasting media
exit	Enter into global configuration mode.
router ospf *process-id*	Create a OSPF routing process and enter into router configuration mode
neighbor ip-address [**cost** number]	Designate an OSPF neighbor and allocate a metric for it. Repeat the above configuration command for each neighbor who wants to specify the weight.

70.3.6 Configure OSPF domain

Configurable area parameters include: authentication, designating Stub area, designating metric for default summary route. Authentication adopts protection based on passwords.

Stub areas are those that don't distribute external routes in them. Instead, ABR generates a default external route to enter the stub area, enable it to enter the external network of the autonomous system. in order to utilize the features OSPF Stub support, you should use default route in the Stub area. In order to additionally reduce LSA number sent into the Stub area, you can prohibit gathering ABR to reduce the sending of summary LSA (type3) entered into the Stub area.

Under router configuration mode, use the following command to define the area parameter:

Command	Purpose
area *area-id* authentication simple	Activates OSPF area authentication
area *area-id* authentication message-digest	Enables OSPF to use MD5 for authentication
area *area-id* stub [no-summary]	Defines a Stub area
area *area-id* default-cost *cost*	Sets metric for default route in Stub area.

70.3.7 Configuring the NSSA Area of OSPF

The NSSA area is similar to the STUB area. However, the NSSA area allows external routes to be entered. The route summary and packet filtration are also supported during transmission. If ISP requires to use the remote network with different routing protocols, the NSSA can simplify management.

The enterprise-core boundary router cannot run in the STUB area of OSPF if NSSA is not applied. That's because the routes of the remote network cannot be forwarded to the STUB area. The simple routing protocols such as RIP can be advertised, but two kinds of routing protocols need be maintained. NSSA can put the center router and the remote router in the same NSSA area and OSPF thus be applied to the remote network.

When the NSSA area is used, note that the route generated by the ABR router can enter the NSSA area once NSSA is configured. Each router in the same area must admit that they are in the NSSA area, or different routers cannot communicate with each other. The displayed release must be used on ABR to avoid packet transmission confusement of the router.

Run the following command in router configuration mode to set the NSSA area of OSPF:

Command	Purpose
Area *area-id* nssa [no-redistribution][no-summary][default-information-originate] [translate-always]	Configures the OSPF NSSA area.

70.3.8 Configuring Route Summary Within OSPF Domain

This feature enables ABR to broadcast a summary route to other areas. In OSPF, ABR will broadcast every network to other areas. If the network number can be allocated according to a certain method, and be continuous, you can configure ABR to broadcast a summary route to other areas. A summary route can cover all networks within a certain range.

Under router configuration mode, use the following commands to define the address ranges:

Command	Purpose
area area-id **range** address mask	Define the address range for route summary.

70.3.9 Configuring the Gathering of a Forwarding Router

When distributing routes from other router areas to OSPF router area, each performs independent broadcasting in the form of external LSA. But you can configure the router to broadcast a route, which covers a certain address range. This method can reduce the size of OSPF link status database.

Under the router configuration mode, use the following command to configure gathering the router:

Command	Purpose
summary-address *prefix mask* [not advertise]	Describe the address and mask that cover the distribution route, only one gathering route is broadcasted.

70.3.10 Creating Default Route

You can demand ASBR to create a default route to enter into the OSPF route area. Whenever you configure a router distribute route to enter into OSPF domain, this router automatically changes into ASBR. But, ASBR does not create default route entering into OSPF route area by default.

Under router configuration mode, use the following command to force ASBR to create a default route:

Command	Purpose
default-information originate [always] [route-map *map-name*]	Force ASBR to create a default route entering into OSPF route area.

70.3.11 Selecting Router ID Through Loopback Interface

OSPF uses the biggest IP address configured on the interface as its router ID. If the interface connected to this IP address changes into DOWN state, or this IP address is deleted, OSPF process will restart to calculate new router ID and resend routing information from all interfaces.

If one loopback interface is configured with IP address, then the router uses that IP address as its router ID, since loopback interface will never become Down, and all these make the routing table more stable.

The router preferably uses LOOPBACK interface as the router ID, meanwhile selects the biggest IP address among all loopback interfaces as the router ID. If there is no loopback interface, then uses the biggest IP address of the router. You cannot designate OSPF to use any special interface.

Under global mode, use the following command, to configure IP Loopback interface.

Command	Purpose
interface loopback 0	Create a loopback interface and enter into interface configuration mode.
ip address ip-address mask	Allocate an IP address for the interface.

70.3.12 Configuring the Management Distance of OSPF

Management distance is defined as the reliability level of routing information source, such as a router or a group of routers. Generally speaking, management distance is an integer between 0-255, the higher the value is, the lower the reliability level it is. If the management distance is 255, then the route information source will not be trusted and should be neglected.

OSPF uses 3 different types of management distances: inter-domain, inner-domain and exterior. The route within an area is inner-domain; the route to other areas is inter-domain; the route distributed from other route protocol domains is exterior. The default value of every kind of route is 110.

Under router configuration mode, use the following command to configure the distance value of OSPF:

Command	Purpose
distance ospf [**intra-area** *dist1*] [inter-area *dist2*] [**external** *dist3*]	Change the management distance value of OSPF inner-domain, inter-domain and exterior route.

70.3.13 Configuring the Route Calculation Timer

You can configure the time delay between the time when OSPF receives topologic change information and when it starts to calculate SPF. You can also configure the interval between two consecutive calculations of SPF. Under router configuration mode, use the following command to configure:

Command	Purpose
timers delay *delaytime*	Set the time delay in the route calculation in a area.
timers hold *holdtime*	Set the minimum time interval of route calculation in a area.

70.3.14 Configuring the On-Demand Link

OSPF over on-demand circuits is an upgrade of OSPF, which enables the protocol more efficient in case of on-demand dialing network surfing. The OSPF protocol is to regularly exchange the HELLO packets and the link-state broadcast-refresh packets among the connected routers after the connection is first established or the information contained in the packet is changed, which means that the minimum spanning tree will be recalculated and the packet will be transmitted only when the topology is really changed.

If the point-to-point connection is among the routers, the configuration should be conducted on one terminal. Of course, the router on the other terminal must support this trait. If the point-to-multipoint connection is among the routers, the configuration must be conducted on the multipoint terminal.

It is recommended to configure the on-demand dialing in the STUB area. If this attribute is configured on each router in the STUB area, the routers outside the STUB area are allowed not to support the on-demand dialing. If on-demand dialing is configured in a standard area, other standard areas must support this trait, because the second kind of external link-state broadcast packets will be broadcast in all areas.

When the trait is configured on the broadcast-based network, the link-state broadcast packets can be restraint, while the HELLO packets cannot be restraint. That's because the HELLO packets are used to maintain the neighborhood relation and to select DR.

Run the following command in interface mode:

Command	Purpose
ip ospf demand-circuit	Configures OSPF on-demand dialing.

70.3.15 Monitoring and Maintaining OSPF

It can display the statistic information of the network, such as: the statistics about the content of IP routing Table, cache and database and etc… This information can help you to judge the utilization of the network resource, and solve the network problem. You can understand the availability of the network nodes, discover the route the network data packet goes through the network.

Use the following commands to display various routing statistics:

Command	Purpose
show ip ospf [*process-id*]	Display the general information about OSPF routing process.
show ip ospf [*process-id*] database[router| network| summary| asbr-summary| external| database-summary]{ *link-state-id*| self-originate| adv-router [*ip-address*]}	Display the related information about OSPF database.

show ip ospf border-routers	Display the internal routing table entry of ABR and ASBR.
show ip ospf interface	Display the information about OSPF interface.
show ip ospf neighbor	Display the OSPF neighbor information according to the interface.
debug ip ospf adj	Supervise the adjacency establishment of OSPF.
debug ip ospf events	Supervise the interface and neighbour events of OSPF.
debug ip ospf flood	Supervise the flooding process of OSPF database.
debug ip ospf lsa-generation	Supervise the LSA generation of OSPF.
debug ip ospf packet	Supervise the message of OSPF.
debug ip ospf retransmission	Supervise the message retransmission process of OSPF.
debug ip ospf spf [intra| external]	Supervise the SPF calculation route of OSPF.
debug ip ospf tree	Supervise the establishment of SPF tree of OSPF

70.4 Examples of OSPF Configuration

70.4.1 Examples of OSPF point to multipoints, non-broadcasting configuration

Switch A:

interface vlan 1

ip address 10.0.1.1 255.255.255.0

ip ospf network point-to-multipoint non-broadcast

!

router ospf 1

network 10.0.1.0 255.0.0.0 area 0

neighbor 10.0.1.3 cost 5

neighbor 10.0.1.4 cost 10

Switch B:

interface vlan 1

ip address 10.0.1.3 255.255.255.0

ip ospf network point-to-multipoint non-broadcast

!

router ospf 1

network 10.0.1.0 255.0.0.0 area 0

neighbor 10.0.1.1

neighbor 10.0.1.4 cost 14

Switch C:

interface vlan 1

ip address 10.0.1.4 255.255.255.0

ip ospf network point-to-multipoint non-broadcast

!

router ospf 1

network 10.0.1.0 255.0.0.0 area 0

neighbor 10.0.1.1

neighbor 10.0.1.3

70.4.2 Configuring example of variable-length subnet mask

OSPF and static routing support variable-length subnet masks (VLSMs). With VLSMs, you can use different masks for the same network number on different interfaces, which saves IP addresses and makes more efficient use of network address space.

In the following example, a 30-bit subnet mask is used, and a two-bit address space is reserved as the host address of the serial port. This is enough for a point-to-point serial link of two host addresses.

interface vlan 1

ip address 131.107.1.1 255.255.255.0

!

interface serial 1/1

ip address 131.107.254.1 255.255.255.252

!

router ospf 107

network 131.107.0.0 255.255.0.0 area 0.0.0.0

70.4.3 Examples of the configuration of OSPF route and route distribution

OSPF requires exchanging information among many internal routers, ABRs and ASBRs. Under minimum configuration, the routers based on OSPF can work under default parameters and have no requirement of authentication.

Here are three examples of configuration:

- The first example practices the basic OSPF command.
- The second example configures the configuration of internal router, ABR and ASBR in a single OSPF autonomous system.
- The third example illustrates a more complex example of configuration with various OSPF tools.

1. An example of basic OSPF configuration

The following example illustrates a simple OSPF configuration. Activate routing process 90, then connect the vlan 1 to area

0.0.0.0. Meanwhile, redistribute RIP to OSPF, OSPF to RIP.

```
interface vlan 1
ip address 130.130.1.1 255.255.255.0
!
router ospf 90
network 130.130.0.0 255.255.0.0 area 0
redistribute rip 1
!
router rip 1
redistribute ospf 90
```

2. An example of the basic configuration of inner router, ABR and ASBR

The following example allocates 4 areas ID for 4 IP address range. Firstly, routing process 109 is activated, the 4 areas are: 10.9.5.0, 2, 3, 0. The masks of area 10.9.50.0,2,3 designate the address range, but area 0 includes all the networks.

```
router ospf 109
network 131.108.20.0 255.255.255.0 area 10.9.50.0
network 131.108.0.0 255.255.0.0 area 2
network 131.109.10.0 255.255.255.0 area 3
network 0.0.0.0 0.0.0.0 area 0
redistribute static
!
interface vlan 1
ip address 131.108.20.5 255.255.255.0
!
interface vlan 2
ip address 131.108.1.5 255.255.255.0
!
interface vlan 3
ip address 131.108.2.5 255.255.255.0
!
interface vlan 4
ip address 131.109.10.5 255.255.255.0
!
interface vlan 5
ip address 131.109.1.1 255.255.255.0
!
interface vlan 6
ip address 10.1.0.1 255.255.0.0
```

!

ip route 44.0.0.0 255.0.0.0 VLAN1

!

The functions of network area configuration command are ordinal, so the order of the commands is important. The router matches the address/mask pair of each interface in order. For detailed information, please refer to the related content in the reference of related network protocol command in "OSPF command".

Let's return to the first network area in the above example. The area ID 10.9.50.0 is configured with an interface sub-network mask as 131.108.20.0. So vlan 1 matches. So vlan 1 only exists in area 10.0.50.0.

Then come to the second area. Except vlan 1, apply the same process on other interfaces, then vlan 2 matches. So vlan 2 connects to area2.

Continue the matching of other network areas. NOTICE that the last network area command is a special case, which means that the rest interfaces are all connected to network area 0.

3. An example of the virtual link.

Figure 5-2 is the network topology of the example:

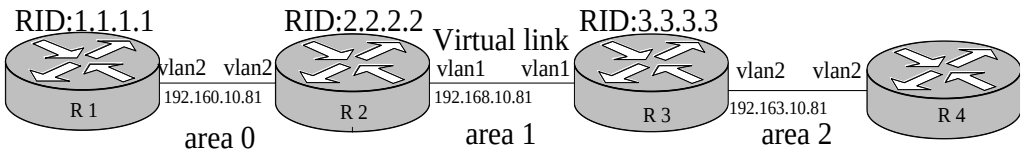


Figure 5-2 Network Topology of the Example

Configure the router according to the above Figure:

R1:

interface vlan 2

ip address 192.160.10.81 255.255.255.0

!

router ospf 1

router-id 1.1.1.1

network 192.160.10.81 255.255.255.0 area 0

!

R2:

interface vlan 1

ip address 192.168.10.81 255.255.255.0

!

interface vlan 2

ip address 192.160.10.82 255.255.255.0

!

router ospf 192

router-id 2.2.2.2

network 192.168.10.81 255.255.255.0 area 1

network 192.160.10.82 255.255.255.0 area 0

area 1 virtual-link 3.3.3.3

!

R3:

interface vlan 1

ip address 192.168.10.82 255.255.255.0

!

interface vlan 2

ip address 192.163.10.81 255.255.255.0

!

router ospf 192

router-id 3.3.3.3

network 192.168.10.82 255.255.255.0 area 1

network 192.163.10.81 255.255.255.0 area 2

area 1 virtual-link 2.2.2.2

!

4. An example of complex OSPF on ABR router configuration

The following example illustrates several tasks involved in configuring ABR. It can be divided into the following two directories:

- Basic OSPF configuration
- Route distribution

The tasks in this configuration are briefly described below.

Figure 5-3 illustrates the range and allocation of network addresses.

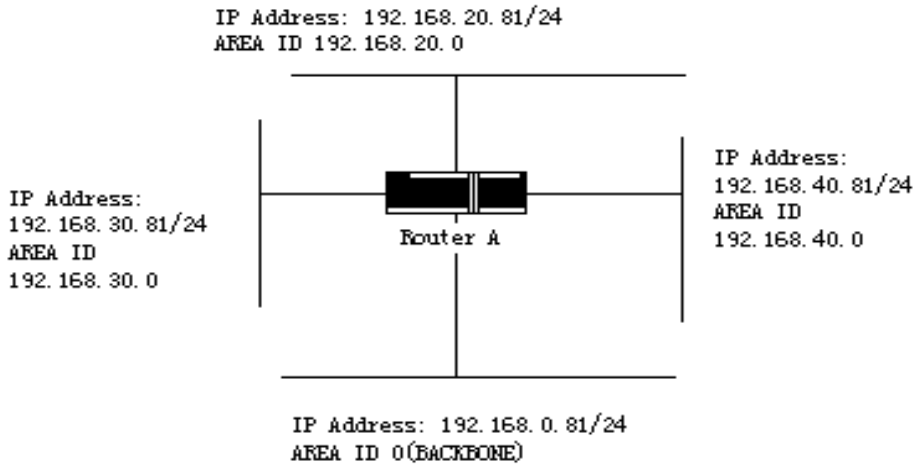


Figure 5-3 Range and allocation of network addresses

The basic configuration tasks for this example are as follows:

- Configure the address range for VLAN 1 to 4.
- Activate OSPF on each interface.
- Set the OSPF authentication password for each area and network.
- Set link state weights and other interface parameters.
- Create 36.0.0.0 in the Stub area. (Note: For the authentication and stub area parameter settings, use an area command respectively. You can also use one command to set these parameters.)
- Set the backbone area (Area 0).

The configuration tasks associated with the distribution are as follows:

- Distribute IGRP and RIP routes into OSPF parameter settings (including metric-type, metric, tag, and subnet).
- Distribute IGRP and OSPF routes into RIP.

Here is an example of OSPF configuration:

```
interface vlan 1
ip address 192.168.20.81 255.255.255.0
ip ospf password GHGHGHG
ip ospf cost 10
!
interface vlan 2
ip address 192.168.30.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf retransmit-interval 10
ip ospf transmit-delay 2
ip ospf priority 4
!
interface vlan 3
ip address 192.168.40.81 255.255.255.0
ip ospf password abcdefgh
ip ospf cost 10
!
interface vlan 4
ip address 192.168.0.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf dead-interval 80
!
router ospf 192
network 192.168.0.0 255.255.255.0 area 0
network 192.168.20.0 255.255.255.0 area 192.168.20.0
network 192.168.30.0 255.255.255.0 area 192.168.30.0
```

network 192.168.40.0 255.255.255.0 area 192.168.40.0

area 0 authentication simple

area 192.168.20.0 stub

area 192.168.20.0 authentication simple

area 192.168.20.0 default-cost 20

area 192.168.20.0 authentication simple

area 192.168.20.0 range 36.0.0.0 255.0.0.0

area 192.168.30.0 range 192.42.110.0 255.255.255.0

area 0 range 130.0.0.0 255.0.0.0

area 0 range 141.0.0.0 255.0.0.0

redistribute rip 1

RIP in network 192.168.30.0:

router rip 1

redistribute ospf 192

!

Chapter 71 Configure BGP

71.1 Overview

This chapter describes how to configure border gateway protocol (BGP). For complete description about BGP commands in this chapter, please refer to other sections related to "BGP command". BGP is an Exterior Gateway Protocol (EGP) defined in RFC1163, 1267 and 1771. It permits to establish a route selection mechanism among different autonomous systems, this mechanism can automatically guarantee the loop-free routing information exchange between the autonomous systems.

71.1.1 The BGP implementation of the router

In BGP, each route includes a network number, the autonomous system list this route has tranverse (called As-path) and other attribute lists. Our router software supports BGP v4 defined in RFC1771. The basic function of BGP is to exchange network reachability information with other BGP systems, including information about AS-path information. This information can be used to construct the AS connection graph which can eliminate route loop, and it can implement AS level routing policy with AS connection graph. BGP v4 supports classless inter-domain router (CIDR), CIDR can reduce the size of the routing table through creating summary routes and thus creates a super network. CIDR removes the concept of network level in BGP, and supports IP prefix broadcasting. CIDR route can be transferred through OSPF, Enhanced IGRP, ISIS-IP and RIP2.

An important difference between exterior gateway routing and interior gateway router is the former has better controllability. In order to control the route, the implementation of BGP provides several optional methods:

- In order to filter routes, it can be based on access-list based on neighbour, aspath-list, prefix-list and also use the access-list based on interface, prefix-list to filter routes or the Nexthop attribute of the routes.
- In order to change the attribute of the routes, you can use the route-map to mend the attributes of BGP routes including MED, Local preference, route value and etc.
- In order to interact with the interior gateway dynamic routing protocol (OSPF, RIP, etc.), you can redistribute route, so as to automatically generate BGP routing information. You can also generate BGP routes through manual configuration of network, aggregation. While generating BGP routes, you can use route-map to configure the attributes of the routes.
- In order to control the precedence of BGP routes in the system, you can use command "distance" to configure the management distance of BGP routes.

71.1.2 How does BGP select the path

The decision process of BGP is established on the basis of comparing route attribute value. When the same network has several routes, BGP selects the best route to the destination. The following process summarizes how BGP selects the best route:

- If it cannot arrive at the next hop, it will not be considered.
- If the path is internal and the synchronization is activated, and if the route is not in IGP, the route will not be considered.
- Select preferable path with the maximum precedence.
- If each route has the same value, preferably select the route with the maximum local precedence.
- If each route has the same local precedence, select preferably the route generated by local router. For example, route may be generated by local router through the using of command "network, aggregate" or by redistributing IGP route.

- If the local precedences are the same, or if there is no route generated by local router, then select preferably the route with the shortest AS path.
- If the AS path lengths are the same, then select preferably the route with the lowest attribute value of "origin" (IGP<EGP<IMCOMPLETE)
- If the attribute values of "Origin" are the same, then select preferable route with the lowest MED value. Unless "bgp always-compare-med" is activated, this comparable can only be carried out between the routes from the same neighbour AS.
- If each route has the same MED, select preferable external path (EBGP) rather than internal path (IBGP). All paths inside the autonomous system confederation are considered to be internal paths, but select preferably EBGP confederation not IBGP confederation.
- If each route has the same connection attribute, select preferable route with a smaller router-id.

71.2 BGP Configuration Task List

The configuration tasks of BGP can be divided into basic tasks and advanced tasks. The first two entries of basic tasks are necessary to configure BGP, other entries in basic tasks and all advanced tasks are optional.

71.2.1 Basic configuration task list of BGP

The basic configuration tasks of BGP include:

- Activate the route selection of BGP.
- Configure BGP neighbor.
- Configure BGP soft reconfiguration
- Reset BGP connection.
- Configure the synchronization between BGP and IGPs
- Configure BGP route value
- Configure BGP route filter based on the neighbour
- Configure BGP route filtration based on the interface
- Disable the nexthop treatment of BGP update

71.2.2 Advanced BGP configuration tasks list

Advanced, optional BGP configuration tasks are listed as the following:

- Use route-map to filter and modify route update
- Configure aggregate address
- Configure BGP community attribute
- Configure autonomous system confederation
- Configure route reflector
- Shut down peer entity
- Configure multihop external peer body
- Configure the management distance of BGP routes
- Adjust BGP timer.
- Compare MED of routes from different AS.
- Configure the MD5 authentication for BGP neighbor
- Configure BGP restart gracefully

- Configure output routing filtering (ORF)

For more related information about the configuration of the attributes of several IP route selection protocols, please refer to"The configuration of attributes of IP routing which are independent from the protocol".

71.3 BGP Configuration Task

71.3.1 Configuring Basic BGP Features

1. Activate the route selection of BGP

In order to activate BGP route selection, use the following commands under global configuration mode to activate BGP route selection:

Command	Purpose
router bgp autonomous-system	Under router configuration mode, activate BGP route selection process.
Network network-number/masklen [route-map route-map-name]	Tag the network as local autonomous system and add it to the BGP list.

NOTE: For exterior gateway routing protocol, the using of configuration command "network " to configure an IP network canand to only control which networks will be informed. This is opposite to interior gateway protocol (IGP), such as RIP, it is using command "network" to decide where to send the update.

Command "network" is used to import IGP routes to BGP routing table. Router resource, such as configured RAM, decides the upper limit of the usable command "network". As a choice, you can use command "redistribute" to achieve the same effect.

2. Configure BGP neighbour

To configure BGP neighbour is to establish the peer to exchange routing information. BGP neighbour ought to be configured in order to exchange routing information with the outer world.

BGP supports two kinds of neighbours: internal neighbour (IBGP) and external neighbour (EBGP). Internal neighbours are in the same AS; external neighbours are in different ASs. Normally, external neighbours are adjacent to each other and share the same sub-network. But internal neighbours can be at any place in the same AS.

Use configuration command "Neighbor" to configure BGP neighbour:

Command	Purpose
neighbor {ip-address | peer-group-name} **remote-as** number	Designate a BGP neighbour.

For example about the configuration of the BGP neighbor, please refer to the section in the bottom of this chapter "an example of the configuration of the BGP neighbor".

3. Configure BGP soft reconfiguration

Generally speaking, BGP neighbors only exchange all routes when the connections are established, after that, they only exchange update routes. So if the configured routing policy gently changes, in order to apply it on the received routes, it is necessary to clear BGP session. The clearing of BGP session will cause the invalidation of cache and will exert great

influence on the operation of the network. Soft reconfiguration function enables the configuration and activation of policy without clearing BGP session. So, we recommend you to use soft reconfiguration, currently, we enable the soft reconfiguration based on each neighbour. When the soft reconfiguration is used on the incoming update produced by the neighbor, it is called incoming soft reconfiguration; When the soft reconfiguration is used on the outcoming update to the neighbor, it is called outcoming soft reconfiguration. Applying incoming soft reconfiguration can make the new input policy effective, Applying outcoming soft reconfiguration makes new local output policy effective without the reset of BGP session.

In order to generate new incoming update without resetting of BGP session, local BGP speaker should save the received incoming update without any modification, regardless whether it would be accepted or denied under current incoming policy. This will be very memory consuming and should be avoided. On the other hand, outcoming reconfiguration does not have any extra memory consumption, so it is always effective. You can trigger outcoming soft reconfiguration on the other side of BGP session to make the new local incoming policy effective.

In order to permit incoming soft reconfiguration, you should configure the BGP to save all accepted routing update. Outcoming reconfiguration need not be pre-configured.

Use the following router configuration command to configure BGP soft reconfiguration:

Command	Purpose
Neighbor {*ip-address*| *peer-group-name*} soft-reconfiguration [inbound]	Configure BGP soft reconfiguration

If you use parameter **"peer-community-name"** to designate BGP peer community, all peer community members in it will inherit the feature of this command.

4. Reset BGP connection

Once two routers are defined as BGP neighbours, they create a BGP connection, and exchange routing information. If the BGP routing policy has been changed, or other configurations have been changed, then you should reset the BGP connection in order to make the change of configuration effective. Use one of the following two management mode commands to reset BGP connection:

Command	Purpose
clear ip bgp *	Recreate a special BGP connection.
clear ip bgp *address*	Reset all BGP connections.

5. Configure the synchronization between BGP and IGPs

If you permit another AS to transfer data to the third AS through your AS, then the synchronization between your AS internal routing state and the routing information it broadcasted to another ASs is very important. For example, if your BGP wants to broadcast routes before all routers in your AS get to know the routes through IGP, then your AS may receive some information that some routers cannot route. In order to prevent these situations, BGP should wait until all IGP routers inside AS get to know that routing information, this is the synchronization between BGP and IGP, and the synchronization is activated by default.

Under certain situations, it is not necessary to synchronize. If you do not permit other ASs to transfer data through your AS,

or if all routers in your AS will run BGP, your can cancel the Synchronization function. Cancelling that feature will enable you to put fewer routes in your IGP, and enable quicker convergence of BGP. Use the following router configuration command to cancel synchronization:

Command	Purpose
no synchronization	Cancel the synchronization between BGP and IGP.

While canceling synchronization, you should use command "clear ip bgp" to clear BGP dialogue.
For an example about BGP synchronization, please refer to the section in the bottom of this chapter "an example of BGP path filtration by the neighbors".
Normally, you do not expect to redistribute all routes to your IGP. A common design is to redistribute one or two routes, and make them the external routes in IGRP, or force the BGP session to generate an AS default route. When BGP redistribute routes to IGP, only the routes acquired through EBGP will be redistributed. Under most situations, you do not want to allocate your IGP to BGP, just use configuration command "network" to list the network in AS, then your network will be broadcasted. The networks listed in this form are called local network, and enables BGP to have attribute "Origin" of IGP. They must appear in the main IP routing table, and are effective; for example, they are direct-connected routes, static routes or routes known through IGP. BGP routing process periodically scans the main IP routing table to check the existence of a local network, and accordingly updates BGP routing table if you really want BGP to execute redistribution, you must be very careful, because these may be the routes in IGP that are injected by other routers through BGP, this may bring force a kind of situation that BGP potentially injects the information into IGP, and then send back the information to BGP. Vice versa.

6. Configure BGP route value
BGP route value is a number set to BGP route in order to control the route selection process, value is local for the router. The value ranges from 0 to 65535. BGP route generated locally has a default value of 32768, the route got from the neighbour values 0. The administrator can implement routing policy through the change of route value.
Use the following router configuration command to configure BGP route weight:

Command	Purpose
neighbor {ip-address | X:X::X:X } **weight** weight	Designate a value to each route from one neighbour.

Besides, you can change the route weight through route-map.

7. Configure BGP route filter based on the neighbour
There are 4 methods in BGP implementation of router software to filter BGP routes of the designated neighbours:
Use Aspath list filter together with global configuration command **"ip aspath-list"** and command "**neighbour filter-list**".

Command	Purpose
ip as-path access-list *aspaths-list-name* {**permit |**	Define an accessing list relative to BGP.

deny} *as-regular-expression*	
router bgp autonomous-system	Enter into router configuration mode.
neighbor {*ip-address* | *X:X::X:X*} **filter-list** *aspath-list-name* {**in | out**}	Establish a BGP filter.

Use access list together with global configuration command "ip access-list" and command "neighbour distribute-list".

Command	Purpose
ip access-list standard *access-list-name*	Define an access list.
router bgp autonomous-system	Enter into router configuration mode.
neighbor {*ip-address* | *X:X::X:X*} **distribute-list** *access-list-name* {**in | out**}	Establish a BGP filter.

Use prefix list together with global configuration command "ip prefix-list" and command "neighbour prefix-list".

Command	Purpose
ip prefix-list *prefixs-list-name* **{permit |deny}** A.B.C.D/n **ge** x **le** y	Define a prefix list.
router bgp autonomous-system	Enter into router configuration mode.
neighbor {*ip-address* | *X:X::X:X*} **prefix-list** *prefix-list-name* {**in | out**}	Establish a BGP filter.

Use route-map together with global configuration command "route-map" and command "neighbour route-map".
Using route-map cannot only filter routes, but also changes routes attribute, the usage will be described in the following chapters.
For example based on neighbour filter route, please refer to "example of BGP route filtration based on the neighbor".

8. Configure BGP route filtration based on the interface
Configuring BGP route filtration based on the interface can be achieved through using access list and prefix list. Network number and the gateway address of the routes can be filtered. It can designate "access-list" option to use access list for filtration of network number of the routes, designate "prefix-list" option to use prefix list for filtration of network number of the routes, designate "gateway" option to use access list for filtration of "nexthop" attribute of the routes. It can even filter the network number and "nexthop" attribute of routes at the same time, but "access-list" option cannot be used together with "prefix-list" option. Designate "*" can filter the routes on all interfaces.
To order to configure the filtration of BGP routes based on the interface, you should carry out the following configurations under BGP configuration mode:

Command	Purpose
filter interface {**in | out**} {**access-list** access-list-	Filter BGP routes based on the interface.

name) (**prefix-list** prefix-list-name) (**gateway** access-list-name)

For examples of route filtration based on the interface, please refer to "examples of BGP route filtration based on the interface".

9. Disable the nexthop treatment of BGP update

You can configure to disable the nexthop treatment of neighbour BGP update. This may be useful in non-broadcasting network (such as FR or X.25), in FR or X.25 network, BGP neighbour may not directly access all other neighbors in the same IP sub-network. There are two methods to cancel nexthop treatment:

1). Use the local IP address of this BGP connection to replace the nexthop address of the outcoming route;

2). Use route-map to designate the nexthop address of incoming or outcoming routes. (Please refer to other chapters)

Use the following router configuration command to disable nexthop treatment and use the local IP address of this BGP connection to replace the nexthop address of the outcoming routes.

Command	Purpose
neighbor {*ip-address* | *X:X::X:X*} **next-hop-self**	Disable the nexthop treatment while carrying out BGP neighbour update.

Using this command to configure will enable the current router to inform itself to be the nexthop of the route. So, other BGP neighbours will forward packets to this network to the current router. This is very useful in non-broadcasting network environment, because there exists a path from the current router to the designated neighbor. But it is not the case in broadcasting network environment, because this will induce unnecessary extra hops.

71.3.2 Configuring advanced BGP features

1. Use route-map to filter and modify route update

You can use route-map to filter route update and modify parameter attribute based on each neighbour. Route-map can be applied both on incoming update and outcoming update. Only the routes passing route-map can be processed while sending or accepting route update.

Route-map supports incoming and outcoming update to match with AS path, community and network number. AS matching demands the using of command "aspath-list"; the matching based on community demands the using of command "community-list", the matching based on the network demands the use of command "ip access-list".

Use the following BGP configuration command to configure route-map for filtration and modification of route update:

Command	Purpose
neighbor {*ip-address* | *X:X::X:X*} **route-map** *route-map-name* **{in | out}**	Apply route-map on incoming or outcoming routes.

For examples of using route-map to filter and modify the route update, please refer to "Examples of BGP route-map".

2. Configure aggregate address

Classless inter-domain routing can create aggregate routing (and super network) to minimize the routing table. You can

configure aggregate routing in BGP through redistributing aggregate routes to BGP or through using conditional aggregate attributes described in the following task list. If there is at least one more detailed record in BGP routing table, add the aggregate address to the BGP routing table.

Use one or more router configuration commands in the following to create an aggregate address in the routing table:

Command	Purpose
aggregate network/len	Create aggregate address in BGP routing table.
aggregate *network/len* summary-only	Broadcast summary address only.
aggregate *network/len* attribute-map *map-name*	Generate aggregate address according to conditions designated by route-map.

For examples regarding the using of BGP route aggregation, please refer to the section in the bottom of this chapter "examples of BGP route aggregation".

3. Configure BGP community attribute

The routing policy that BGP supports is mainly based on one of the 3 values in BGP routing information:

- Network number of routes:
- as path attribute value of routes:
- The "community" attribute value of routes

Dividing the routes into communities through "community" attribute, and applying the routing policy based on the community, thereby simplifies the configuration of control of routing information.

Community is a group of routes with the common attributes; each route may belong to several communities. AS administrators can define a certain route belongs to a certain community.

Community attribute is an optional and transferable global attribute ranging from 1 to 4,294,967,200. The famous communities pre-defined in the Internet communities include:

- **No-export**--- Do not advertise this route to EBGP peer (Including the EBGP peers inside the autonomous system confederation).
- **No-advertise**---Do not advertise this route to any peer .
- **local-as**---Do not advertise this route to the exterior of autonomous system (ca send this route to the other sub-AS peers in the autonomous system confederation.)

When generating, accepting or sending routes, BGP speakers can configure, add or modify the route community attribute. when aggregating routes, the generated aggregation includes the "community" attributes from complete communities of all original routes.

By default, "Community" attributes are not sent to the neighbor. Use the following BGP configuration command to designate sending "community" attribute to the neighbour:

Command	Purpose
neighbor {*ip-address*| *X:X::X:X*} **send-community**	Designate to send attribute "community" to the neighbor.

You need to do the following jobs to configure community attribute for the router:

Command	Purpose
route-map *map-name sequence-number* {**deny	permit**}	Configure route-map.
set community community-value	Configure rule of setting.
router bgp autonomous-system	Enter into router configuration mode.
neighbor{*ip-address*	*X:X::X:X*} **route-map** *access-list-name* {**in	out**}	Apply route-map.

To filter routing information based on community attributes, you need to do the following jobs:

Command	Purpose
ip community-list {expanded	standard } *community-list-name* {permit	deny} *communtiy-expression*	Define community list.
route-map *map-name sequence-number* {deny	permit}	Configure route-map.
match community community-list-name	Configure rules of matching.
router bgp autonomous-system	Enter into router configuration mode
neighbor {ip-address	peer-group-name} **route-map** route-map-name {**in	out**}	Apply route-map.

For examples of using community attributes, please refer to "Examples of route-map using BGP community attribute".

4. Configure autonomous system confederation

The way to reduce the number of IBGP connections is to divide an AS into several sub-AS, then form them into an autonomous system confederation. From the external perspective, the confederation looks like an AS. In the confederation, each sub-AS is full-mesh inside, and has connections with other sub-ASs in the same confederation. Even if there are EBGP sessions between peers of different sub-ASs, they may still exchange routing selection information like IBGP peers. Concretely speaking, it is saving the nexthop, MED and local precedence information.

To configure a BGP autonomous system confederation, you should designate the confederation identifier. The confederation identifier is an AS number, from an external perspective, the confederation is just like a single AS with AS number being the confederation identifier.

Use the following BGP configuration command to configure confederation identifier of the autonomous system:

Command	Purpose
bgp confederation identifier *autonomous-system*	Configure the confederation identifier of the autonomous system.

In order to designate the autonomous system number belonging to autonomous system confederation, use the following

BGP configuration command:

Command	Purpose
bgp confederation peers autonomous-system [autonomous-system ...]	Designate the AS belongs to the confederation of autonomous system.

For examples of autonomous system confederation, please refer to "examples of BGP autonomous system confederation".

5. Configure route reflector

Another method to reduce the number of IBGP connections instead of configuring autonomous system confederation is to configure route reflector.

The internal peers of the route reflector are divided into two groups: client peers and all other routers (non-client peers). The route reflector reflects the routes between the two groups; the route reflector and its client peers form a cluster. Non-client peers must be full-mesh connected, but client peers need not. The clients in the cluster do not communicate with IBGP speakers outside the cluster.

When route reflector receives routing information, it completes the following tasks:

- Broadcast the routes from external BGP speaker to all clents and non-client peers.
- Broadcast the routes from non-client to all clents.
- Broadcast the routes from the clients to all clients and non-client peers. So, the client peers need not be full-mesh-conneted.

Use the following router configuration command to configure the local router as the reflector and designate neighbors as the router reflector client:

Command	Purpose
Neighbor {*ip-address* | *X:X::X:X*} route-reflector-client	Configure the local router as route reflector and designate neighbors as the client.

An AS may have several route reflectors, the way route reflector to process other route reflectors is the same as the processing of IBGP speakers.Normally, a cluster of clients have only one route reflector, and then the cluster is identified by the route reflector 's router ID. In order to increase the redundancy and avoid the failure of single node, a cluster may have more than one route reflectors. In this case, all the route reflectors in the cluster should be configured with 4-bit cluster ID, so that the route reflector can identify the update information of the route reflector in the same cluster. All the route reflectors belonging to the same cluster should be full-mesh-connected, and they should have the same client and non-client peer set.

If there is more than one route reflector in the cluster, you can use the following BGP configuration command to configure cluster ID:

Command	Purpose
bgp cluster-id *cluster-id*	Configure cluster-ID.

For examples of the configuration of route reflector, please refer to "examples of the configuration of BGP route reflector".

6. Shut down peer entity

Use the following BGP configuration command to shut down BGP neighbour:

Command	Purpose
Neighbor {*ip-address* | *X:X::X:X*} **shutdown**	Shut down BGP neighbour.

Use the following BGP configuration command to activate the neighbour shut down previously:

Command	Purpose
no neighbor {*ip-address* | *X:X::X:X*} **shutdown**	Activate BGP neighbour.

7. Configure multihop external peer body

By default, external peers should be on a directly connected network, in order to configure multihop external peer, you need to carry out the following task:

Command	Purpose
neighbor {*ip-address* | *X:X::X:X*} **ebgp-multihop** ttl	Configure BGP neighbor as multihop external peer.

8. Configure the management distance of BGP routes

Management distance is a kind of measurement of the preference of different routing protocol. BGP uses 3 different management distances: external distance, internal distance and local distance. The routes obtained from external BGP will be assigned with the external distiance; the routes obtained from internal BGP will have a distance as internel distance, local routes will be given the local distance. Use the following BGP configuration command to configure BGP route management distance:

Command	Purpose
distance bgp {external-distance| internal-distance |local-distance}	Configure BGP route management distances.

The change of management distances of BGP route is dangerous, and normally it is not recommended. The external distance should be shorter than the distance of any other dynamic routing protocol and the internal distance should be longer than the distance of any other dynamic routing protocol.

9. Adjust BGP timer

Use the following BGP configuration command to adjust the BGP “keepalive” and “holdtime” timers of detailed neighbour:

Command	Purpose
neighbor {ip-address | X:X::X:X } **timers** keepalive holdtime	Set “keepalive” and “holdtime” timer interval (count with unit ‘second’) for designated peer or

peer community

Use command “no neighbour timers” to reset the timer interval of BGP neighbor or peer community to the default value.

10. Compare MED of routes from different AS

MED is a parameter to be considered when selecting the best route from several paths. The path with lower MED value will be preferably considered than the route with higher MED value.

Under default situation, during the process of selecting the best route, MED’s comparison only takes place in the routes from the same AS. You can permit the MEDs’ comparison to take place in routing selection, regardless of which AS the routes come from.

Use the following BGP configuration command to realize the above objective:

Command	Purpose
bgp always-compare-med	Permit to make MEDs comparison among routes from different AS.

11． Configure the MD5 authentication for BGP neighbor

To make sure of the secure routing information forwarding between ASs, perform the password authentication on the BGP connection through the MD5 option provided by TCP.

Run the following command to achieve the previous purpose:

Command	Purpose
neighbor *A.B.C.D* password *LINE*	Enables the MD5 authentication of the BGP neighbor and set the password.

You can run **no neighbor A.B.C.D password** to cancel the MD5 authentication for the BGP neighbor.

71.4 Monitoring and Maintaining BGP

The administrator can display or delete the 2BGP routing table or the content of other databases. Of course the detailed statistics information can also be displayed. The following are relative tasks:

- Deleting the BGP routing table and the database
- Displaying the routing table and the system statistics information
- Tracking the BGP information

71.4.1 Deleting the BGP Routing Table and the BGP Database.

The following table lists the tasks relative with high-speed cache deletion, table deletion or BGP database deletion. The commands listed in the following table are all run in EXEC mode.

Command	Purpose
clear ip bgp *	Resets all BGP connections.
clear ip bgp *as-number*	Resets the BGP connections of the designated autonomous system.
clear ip bgp *address*	Resets the BGP connections of the designated neighbor.
clear ip bgp *address* soft {in|out}	Deletes the incoming database or the outgoing database of the designated neighbor.
clear ip bgp *aggregates*	Deletes the routes generated in route aggregation.
clear ip bgp *networks*	Deletes the routes generated during forwarding process.
clear ip bgp redistribute	Deleting the routes generated by the **network** command.

71.4.2 Displaying the Routing Table and the System Statistics Information

The detailed statistics information about the BGP routing table or the database will be displayed. The provided information can decide resource utilization and help resolving network problems. The information about the node reachability can also be displayed.

You can run the following commands to display all kinds of routing statistics information:

Command	Purpose
show ip bgp	Displays the BGP routing table in the system.
show ip bgp prefix	Displays the routes which match the designated prefix list.
show ip bgp community	Displays the statistics information about the group attribute.
show ip bgp regexp *regular-expression*	Displays the routes which match the designated regular expression.
show ip bgp *network*	Displays the designated BGP route.
show ip bgp neighbors *address*	Displays the information about the TCP and the BGP connections of the designated neighbor.
show ip bgp neighbors *[address]* [received-routes | routes | advertised-routes]	Displays the routes learned from the special BGP neighbor.
show ip bgp paths	Displays the information about all BGP paths in the database.
show ip bgp summary	Displays the states of all BGP connections.

71.4.3 Tracking the BGP Information

You can observe BGP connection establishment and route transmission/reception by tracking the BGP information, which helps to locate the troubles and resolve the problems. The commands to track the BGP information are shown in the following table:

Command	Purpose
debug ip bgp	Tracks the general BGP information.
debug ip bgp all	Tracks all BGP information.
debug ip bgp fsm	Tracks the BGP state machine.
debug ip bgp keepalive	Tracks the KeepAlive packets of BGP.
debug ip bgp open	Tracks the OPEN packets of BGP.
debug ip bgp update	Tracks the UPDATE packets of BGP.

71.5 Examples of BGP configuration

The following sections provide the examples of BGP configuration:

71.5.1 Example of BGP route-map

The following example illustrates how to use route-map to change the incoming route attribute from the neighbor. Set the metric of all routes that come from neighbour 140.222.1.1 and meet the requirement of ASPATH accessing list “aaa” to 200, local precedence value to 250, and they are accepted, all other routes will be denied.

```
router bgp 100
 neighbor 140.222.1.1 route-map fix-weight in
 neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight 10 permit
 match as-path aaa
 set local-preference 250
 set weight 200
!
ip as-path access-list aaa permit ^690$
ip as-path access-list aaa permit ^1800
```

In the following example, the first entry of route-map “freddy” will set the MED attributes of all routes origining from autonomous system 690 to 127. The second entry allows the routes that don’t meet the above conditions to be transferred to neighbor 1.1.1.1.

```
router bgp 100
 neighbor 1.1.1.1 route-map freddy out
!
```

```
ip as-path access-list abc permit ^690_
ip as-path access-list xyz permit .*
!
route-map freddy 10 permit
 match as-path abc
 set metric 127
!
route-map freddy 20 permit
match as-path xyz
```

The following example illustrates how to use route-map to change the routes from route redistribution:

```
router bgp 100
 redistribute rip 1 route-map rip2bgp
!
route-map rip2bgp
 match ip address rip
 set local-preference 25
 set metric 127
 set weight 30000
 set ip next-hop 192.92.68.24
 set origin igp
!
ip access-list standard rip
 permit 131.108.0.0 255.255.0.0
 permit 160.89.0.0 255.255.0.0
 permit 198.112.0.0 255.255.128.0
```

71.5.2 Example of neighbour configuration

In the following example, BGP router belongs to AS109, and creates two networks. This router has 3 neighbors: the first neighbor is an external one (in different AS); the second is internal one (with the same AS number). The third is also an external one.

```
router bgp 109
 network 131.108.0.0
 network 192.31.7.0
 neighbor 131.108.200.1 remote-as 167
 neighbor 131.108.234.2 remote-as 109
 neighbor 150.136.64.19 remote-as 99
```

71.5.3 Example of BGP route filtration based on the neighbor

Here is an example of BGP path filtration based on the neighbor. The routes passing through as-path access list "test1" will receive a metric value as 100. Only routes passing through as-path access list "test2" will be sent to 193.1.12.10, similarly, only those routes passing access list "test3" will be accepted by 193.1.12.10:

router bgp 200

neighbor 193.1.12.10 remote-as 100

neighbor 193.1.12.10 filter-list test1 weight 100

neighbor 193.1.12.10 filter-list test2 out

neighbor 193.1.12.10 filter-list test3 in

!

ip as-path access-list test1 permit _109_

ip as-path access-list test2 permit _200$

ip as-path access-list test2 permit ^100$

ip as-path access-list test3 deny _690$

ip as-path access-list test3 permit .*

71.5.4 Examples of BGP route filtration based on the interface

The following is the example of the configuration of route filtration based on the interface. It filters the routes from interface vlan1 through access list "ac1":

router bgp 122

filter vlan1 in access-list acl

The following example uses access list "filter-network" to filter the network numbers of the routes, and meanwhile, uses access list "filter-gateway" to filter gateway address of the routes from interface vlan1.

router bgp 100

filter vlan1 in access-list filter-network gateway filter-gateway

The following example: uses prefix list "filter-prefix" to filter the network numbers of the routes, and meanwhile, use accessing list "filter-gateway" to filter gateway address of routes from all interfaces.

router bgp 100

filter * in prefix-list filter-prefix gateway filter-gateway

71.5.5 Examples of using prefix list to configure route filtration

In the following example default route 0.0.0.0/0 is denied.

ip prefix-list abc deny 0.0.0.0/0

The following example: permits routes matching prefix 35.0.0.0/8:

ip prefix-list abc permit 35.0.0.0/8

In the following example, BGP process only accepts prefix with length ranges from /8 to /24:

router bgp 1

```
 network 101.20.20.0
 filter * in prefix max24
!
 ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

In the following configuration, the router filters routes from all interfaces, it only accepts routes with prefix from 8 to 24:

```
router bgp 12
filter * in prefix-list max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

Here are some other examples of configuration of prefix lists

The following example: permits routes with prefix length no more than 24 in network 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

The following example: denies routes with prefix length of more than 25 in network 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

The following example: permits routes with prefix length of more than 8 yet less than 24 in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example: denies all routes with prefix length of more than 25 in all address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

This example: denies routes from network 10/8, because if the mask on class A network 10.0.0.0/8 is smaller or equal to 32 bit, all routes from that network will be denied:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

The following example: denies routes with mask length of more than 25 in network 204.70.1.24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

The following example: permits all routes:

```
ip prefix-list abc permit any
```

71.5.6 Example of BGP route aggregation

The following example illusrates how to create aggregation routes in BGP.It may be created by route redistribution or the

using of conditional route aggregation function.

In the following example, command "redistribute static" is used to redistribute aggregation route 193.*.*.*:

ip route 193.0.0.0 255.0.0.0 null 0

!

router bgp 100

redistribute static

When there is at least one route in the routing table within the designated range, the following configuration will create an aggregation route in BGP routing table. The aggregation route will be considered to be from your AS, and has the "atomic" attribution, to indicate the possibilities of the loss of information.

router bgp 100

aggregate 193.0.0.0/8

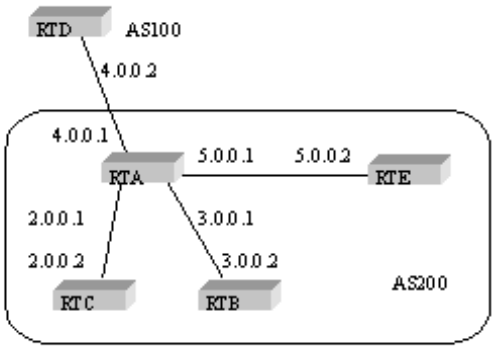
The following example not only creates an aggregation route 193.*.*.*, but also prohibit it to broadcast the more concrete routes to all the neighbours:

router bgp 100

aggregate 193.0.0.0/8 summary-only

71.5.7 Example of BGP route reflector

The following is an example of route reflector configuration. RTA, RTB, RTC, RTE all belong to the same autonomous system AS200, RTA serves as route reflector, RTB and RTC are route reflector clients, and RTE is normal IBGP neighbor. RTD belongs to AS100, and creates EBGP connection with RTA, the configuration is illustrated as the following:



- RTA configuration:

interface vlan2

ip address 2.0.0.1 255.0.0.0

!

interface vlan3

ip address 3.0.0.1 255.0.0.0

!

interface vlan4

ip address 4.0.0.1 255.0.0.0

!

```
interface vlan5
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200   /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200   /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200   /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100   /*RTD EBGP*/
network 11.0.0.0/8
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12
```

- RTB configuration:

```
interface vlan3
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
neighbor 3.0.0.1 remote-as 200   /*RTA IBGP*/
network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
```

- RTC configuration:

```
interface vlan2
ip address 2.0.0.2 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200   /*RTA IBGP*/
network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12
```

- RTD configuration:

```
interface vlan4
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
```

neighbor 4.0.0.1 remote-as 200 /*RTA EBGP*/

network 14.0.0.0/8

!

ip route 14.0.0.0 255.0.0.0 4.0.0.12

- RTE configuration:

interface vlan5

ip address 5.0.0.2 255.0.0.0

!

router bgp 200

neighbor 5.0.0.1 remote-as 200 /*RTA IBGP*/

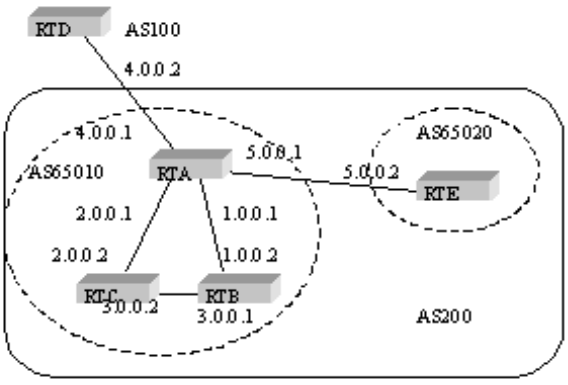
network 15.0.0.0/8

!

ip route 15.0.0.0 255.0.0.0 5.0.0.12

71.5.8 Example of BGP confederation

The following is the configuration of confederation. RTA, RTB, RTC create IBGP connections, and it belongs to a private autonomous system 65010; RTE belongs to another private autonomous system 65020; RTE and RTA establish internal EBGP connection of confederation; AS65010 AS65020 conprise the confederation, whose identifier is AS200; RTD belongs to autonomous system AS100, RTD establishes EBGP connection with autonomous system 200 through RTA.



- RTA configuration:

interface vlan1

ip address 1.0.0.1 255.0.0.0

!

interface vlan2

ip address 2.0.0.1 255.0.0.0

!

interface vlan4

```
ip address 4.0.0.1 255.0.0.0
!
interface vlan5
ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.2 remote-as 65010  /*RTB IBGP*/
neighbor 2.0.0.2 remote-as 65010  /*RTC IBGP*/
neighbor 5.0.0.2 remote-as 65020  /*RTE EBGP*/
neighbor 4.0.0.2 remote-as 100    /*RTD EBGP*/
```

- RTB configuration:

```
interface vlan1
ip address 1.0.0.2 255.0.0.0
!
interface vlan3
ip address 3.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.1 remote-as 65010  /*RTA IBGP*/
neighbor 3.0.0.2 remote-as 65010  /*RTC IBGP*/
```

- RTC configuration:

```
interface vlan2
ip address 2.0.0.2 255.0.0.0
!
interface vlan3
ip address 3.0.0.2 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 2.0.0.1 remote-as 65010  /*RTA IBGP*/
neighbor 3.0.0.1 remote-as 65010  /*RTB IBGP*/
```

- RTD configuration:

```
interface vlan4
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200  /*RTA EBGP*/
```

- RTE configuration:

```
interface vlan5
ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
bgp confederation identifier 200
bgp confederation peers 65010
neighbor 5.0.0.1 remote-as 65010  /*RTA EBGP*/
```

71.5.9 Example of route map with BGP group attribute

This section includes three examples of using route map with BGP community attribute.

In the first example, “route map set-community” is applied on the outcoming update of neighbor 171.69.232.50. Set the special community attribute with value “no-export” for the routes passing access list aaa, while other routes are broadcasted normally. This special community attribute will automatically prevent BGP speakers in AS200 from advertising the route outside of the autonomous system.

```
router bgp 100
 neighbor 171.69.232.50 remote-as 200
 neighbor 171.69.232.50 send-community
 neighbor 171.69.232.50 route-map set-community out
!
 route-map set-community 10 permit
 match ip address aaa
 set community no-export
!
 route-map set-community 20 permit
```

In the second example, “route map set-community” is used for the outcoming update of neighbour 171.69.232.90. All routes orgining from AS70 will insert value 200 into the community attribute 200, all other routes will just be advertised normally.

```
route-map bgp 200
 neighbor 171.69.232.90 remote-as 100
 neighbor 171.69.232.90 send-community
 neighbor 171.69.232.90 route-map set-community out
```

```
!
route-map set-community 10 permit
 match as-path test1
 set community-additive 200 200
!
route-map set-community 20 permit
 match as-path test2
!
ip as-path access-list test1 permit 70$
ip as-path access-list test2 permit .*
```

In the third example, selectively set the MED and local preference value of routes from neighbor 171.69.232.55 according to the commumity attribute value of the routes. All routers matching with community list com1will be set with MED as 8000, this may include routes with community value “100 200 300” or “900 901”. These routes may have other attribute values.

All routes transmitting community list com2 will be set with the local preference value as 500.

All other routes will be set with the local priority value as 50. So, all the rest of the routes of neighbor 171.69.232.55 have the preference of 50.

```
router bgp 200
neighbor 171.69.232.55 remote-as 100
neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
match community com1
set metric 8000
!
route-map filter-on-community 20 permit
match community com2
set local-preference 500
!
route-map filter-on-community 30 permit
set local-preference 50
!
ip community-list standard com1 permit 100 200 300
ip community-list standard com1 permit 900 901
!
ip community-list standard com2 permit 88
ip community-list standard com2 permit 90
!
```

Chapter 72 Congiuring PBR

72.1 Overview

This section descripe how to configure PBR. PBR is the abbrecation of Policy Based Routing. PBR make the user have the ability to route ip packet according some policy other than dynamic routing protocol. We currently support the following policy: based on the length of ip packet, source ip address. You can set gateway or outgoing interface for packets matching the policy. PBR can support load balance.

The rule for PBR selecting nexthop is following :

- If set ip next-hop is configured,and the gateway is reachble,the gateway will be used. If multiple gateway is configured, use the first reachable gateway, if load-balance key word is used, the load balance is used between these gateways.
- If set interface is configured, and the outgoing interface is routabale(interface protocol up, and ip address is confured), use the outgoing interface. If multiple outgoing interfaces are configured, first routable interface will be used. If load-balance key word is used, the load balance is used between these interface. If both set ip next-hop and set interface configured, , use set ip next-hop first.
- **set ip default next-hop** or **set default interface** won't be used untill routing lookup failed.

For the following packets, policy routing will not be applied:

- The destination address is a local packet.
- Multicast message.
- Local direct broadcast packet.

72.2 PBR Configuration Task List

If you want to use PBR, the following configuration is needed:

- Create standard access-list (optional)
- Creat route-map
- Apply route-map on interface

72.3 PBR Configuration Task

72.3.1 Create standard access-list

To create access-list, following the step bellow:

Command	Function
ip access-list standard net1	Enter access-list configurtion mode.

72.3.2 Create route-map

To create route-map, following the step bellow:

Command	Function
route-map pbr	Enter route-map configuration.

match ip address *access-list* **match length** min_length max_length	Configure matching policy.
set ip [default] next-hop *A.B.C.D* set [default] interface *interface_name*	Configure the next hop address or port of the IP packet.

72.3.3 Apply route-map on interface

To enable PBR on interface, following the step bellow:

Command	Function
interface interface_name	Enter interface configurtion mode.
ip policy route-map *route-map_name*	Apply PBR on interface.

72.3.4 Maintaining PBR

To maintain PBR, follow the steps below in the EXEC mode:

Command	Function
debug ip policy	View the results of applying policy routing.

72.4 PBR configution example

- Switch configuration:

```
!
interface Vlan1
ip address 10.1.1.3 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
!
interface Vlan2
ip address 13.1.1.3 255.255.255.0
no ip directed-broadcast
!
interface Vlan3
ip address 14.1.1.3 255.255.255.0
no ip directed-broadcast
!
ip access-list standard net1
permit 10.1.1.2 255.255.255.255
!
```

```
ip access-list standard net2
permit 10.1.1.4 255.255.255.255
!
ip access-list standard net3
permit 10.1.1.21 255.255.255.255
!
route-map pbr 10 permit
match ip address net1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address net2
set ip next-hop 14.1.1.99
!
route-map pbr 30 permit
match ip address net3
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
route-map pbr 40 permit
set ip default next-hop 13.1.1.99
```

- Configuration explanation

Policy routing is enabled on interface vlan1. For packets origined from 10.1.1.2, the next hop is 13.1.1.99 if 13.1.1.99 is reachable. If 13.1.1.99 isn't reachable, destination base routing is used. For packets from 10.1.1.21, route-map pbr 30 is used. Since load-balance key word is used, both 13.1.1.99 and 14.1.1.99 will be used as the next hop (assuming there are routes to 13.1.1.99 and 14.1.1.99 in the routing table).

Chapter 73 Switch Routing Protocol Highpriority Configuration

73.1 Overview

When testing routing protocols, the priority of routing protocol packets to the CPU can be improved through FP. This can ensure that the routing protocol packets can be received when the system receives overloaded background traffic (such as IP packets that need to be forwarded).

73.2 Configuration task list

To enable priority improving of the routing packets forwarding to CPU, following configuration task is necessary:

- Enable priority improving of the routing packets forwarding to CPU

73.3 Configuration task

73.3.1 Enable priority improving of the routing packets forwarding to CPU

In global configuration mode, configure as follows:

Command	Purpose
switch routing-protocol-highpriority	Enable priority improving of the routing packets forwarding to CPU.

Chapter 74 IP Hardware Subnet Routing Configuration

74.1 IP Hardware Subnet Configuration Task

74.1.1 Overview

IP hardware subnet routing is similar to IP fast exchange.

When the IP hardware subnet routing is not enabled, before forwarding message containing the IP address A at the next hop, the switch first checks whether the item of destination A exists in the IP cache of hardware. If the item exists, the message will be forwarded through hardware. If the item does not exist, the message is sent to CPU and then processed through software. IP hardware subnet routing items include the destination subnet, mask, IP address of the next hop, interface and so on. When the IP hardware subnet routing is enabled, after the IP cache fails to be matched, the system is to check the IP hardware subnet routing items. If the matched item is found, the message will be directly forwarded through the next-hop IP address and the interface designated in the matched item. If the IP hardware subnet routing item is not found, the message will be sent to CPU for processing.

74.1.2 Configuring IP Hardware Subnet Routing

Perform the following steps to configure the IP hardware subnet routing:

Step	Command	Description
1	[no] ip exf	Enable or disable the IP hardware subnet routing.
2	[no] ip exf down-up-threshold *rate*	Set the threshold (percentage) of the hardware subnet routing switch. Default: 90

74.2 Configuration Example

Pay attention to the following content when you configure the routing items:

- As to the direct-connecting routing, the next hop is CPU. If the next hop is a routing interface not an IP address, do as in the direct-connecting routing.
- The ARP of the next-hop IP address does not exist, the system will send an ARP request and temporarily designate the next-hop routing item as CPU. After the system receives the ARP response, the system then update the next hop to the user-designating address. If the VLAN interface where the next hop resides is found different from the configured interface during the ARP response, the next hop of the route is designated as CPU. Users then need to correct the configuration.
- If the next-hop interface or the interface protocol does not exist, the item will not be added to the hardware subnet routing table.

Suppose a switch is configured with the following commands:

ip exf down-up-threshold 80

The command indicates that when software routing entries exceed 80% of the upper limit of hardware subnet routing entries, the switch will automatically disable the hardware subnet routing function. When the software routing entries are reduced to less than 80% of the upper limit of hardware subnet routing entries, turn on the hardware subnet routing function again.

Chapter 75 IP-PBR Configuration

75.1 IP-PBR Configuration

IP-PBR realizes software PBR functions through the hardware of switch chip.

PBR stands for Policy Based Routing. PBR enables users to rely on a certain policy not on routing protocol for routing. Software based PBR supports multiple policies and rules and also load balance. You can designate the next hop's IP address or port for those packets that are in line with policy. PBR supports load balance and applies multiple next-hop IP addresses or ports on those policy-supported packets.

Only when the next-hop egress ARP designated by route map is already learned can IP-PBR regard that this egress is valid and then the corresponding rule is effective. When a packet satisfies IP-PBR policy, the hardware directly forwards this packet to the next-hop egress that the rule specifies. This process is finished by the hardware without the operation of CPU. The packets forwarded by IP-PBR have the highest priority and only those packets unmatched with IP-PBR rule are forwarded to CPU.

The current IP-PBR supports the IP ACL policy and the next-hop IP address policy. When multiple next hops are configured, the first effect next hop is chosen. IP-PBR also supports equivalent routing that is realized by the switch chip. Hardware equivalent routing needs no extra configuration.

IP-PBR supports the following policy routing commands:

route-map *WORD*

match ip address *WORD*

set ip next-hop *X.X.X.X* **[load-balance]**

ip policy route-map *WORD*

IP-PBR is a little different from router's policy routing. IP-PBR chooses an effective next hop as the egress and drops packets if no valid next hop available, while router's policy routing selects an effective next hop but packet loss happens if this next hop has not learned ARP. Once multiple sequences are set, one difference between IP-PBR and software policy routing must be noted. Software policy routing always chooses high-priority sequence routes no matter whether IP address matched by high-priority sequences overlaps with that matched by low-priority sequences and whether these routes are effective, while IP-PBR chooses low-priority sequence routes when high-priority sequence routes invalidate.

75.1.1 Enabling or Disabling IP-PBR Globally

Run the following commands in global configuration mode.

Command	Purpose
ip pbr	The IP-PBR function is disabled by default.
no ip pbr	Resumes the default settings.

IP-PBR is disabled by default.

75.1.2 ISIS Configuration Task List

To configure IP-PBR, do as follows:

Create ACL;

Create a route map;

Apply the route map on a port;

To create an ACL, run the following command globally:

Command	Remarks
ip access-list standard *net1*	Enters the ACL configuration mode and defines ACL.

To create a route map, run the following commands globally:

Command	Remarks
route-map *pbr*	Enters the route map configuration mode.
match ip address *access-list*	Configures the match-up policy.
set ip next-hop *A.B.C.D*	Configures the next-hop address of IP packet.

To apply policy routing on an IP-receiving port, run the following commands:

Command	Remarks
interface interface_name	Enters the interface configuration mode.
ip policy route-map *route-map_name*	Applies policy routing on the port.

75.1.3 Monitoring and Maintaining MVC

Run the following commands in EXEC mode:

Command	Operation
show ip pbr	It is used to display the information about RIP configuration.
show ip policy	Shows the port on which IP-PBR is applied.
show ip pbr policy	It is used to display the information about IP-PBR equivalent routing.
debug ip pbr	It is used to enable or disable the debugging switch of IP-PBR.

The information that IP-PBR is not running is shown:

```
switch#show ip pbr


IP policy based route state: disabled

No pbr apply item

No equiv exf apply item
```

All data related about IP-PBR running are shown below:

```
switch#show ip pbr
IP policy based route state: enabled

No equiv exf apply item

VLAN3 use route-map ddd, and has 1 entry active.
------------------
Entry sequence 10, permit
Match ip access-list:
ac1
Set Outgoing nexthop
90.0.0.3
```

The IP-PBR policy routing information is shown below:

```
switch#show ip pbr policy
IP policy based route state: enabled

VLAN3 use route-map ddd, and has 1 entry active.
------------------
Entry sequence 10, permit
Match ip access-list:
ac1
Set Outgoing nexthop
90.0.0.3
```

The equivalent routing information is shown below:

```
switch#show ip pbr exf
IP policy based route state: enabled

Equiv EXF has 1 entry active.
------------------
Entry sequence 1, handle c1f95b0
Dest ip: 1.1.0.0/16
90.0.0.3
192.168.213.161
```

75.1.4 IP-PBR Configuration Example

- Switch configuration:

!

ip pbr

```
!
interface vlan1
ip address 10.1.1.3 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
!
ip access-list standard ac1
permit 10.1.1.21 255.255.255.255
!
ip access-list standard ac2
permit 10.1.1.2 255.255.255.255
!
route-map pbr 10 permit
match ip address ac1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address ac2
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
```

- Configuration Description

The switch is to apply policy routing on the packets that are received from VLAN1. As to the packets whose source IPs are 10.1.1.21, their next hop is 13.1.1.99. As to the packets whose source IPs are 10.1.1.2, they are applied on **route-map pbr 20**; because **set ip next-hop** has the **load-balance** parameter, the switch chip will automatically choose 13.1.1.99 or 14.1.1.99 as the egress according to destination IP address.

Chapter 76 Multi-VRF CE Intro

76.1 Overview

The Virtual Private Network (VPN) provides a secure method for multiple client networks to share the ISP-supplied bandwidth. In general, one VPN comprises a team of client networks that share a public routing table on the ISP's routers. Each client network is connected to the interface of the network devices of ISP, while ISP's device will relate each interface to a VPN routing table. One VPN routing table is also called as a VRF (VPN Routing /Forwarding table).

VRF is usually deployed on a Provider Edge (PE) device, such as MPLS VRF VPN. A PE supports multiple VPNs, and each VPN has its independent IP address space among which IP addresses can be overlapped. The VPN of a different client connects a different interface of PE, while PE differentiates the to-be-checked routing tables according to the incoming port of the packet.

Multi-VRF CE is to remove the task of connecting multiple client networks from PE to CE, which only requires a physical link to connect CE and PE. In this way, the port resource of PE is saved. CE also maintains the VRF routing table for each VPN. The packets from the client network are first forwarded on CE and then transmitted to PE after the packets pass through the ISP network.

The switch which serves as MCE connects different client networks through different ports and then relates these ports to a VPN routing table. The switch only support VRF settings on the VLAN port.

The MCE function is usually deployed at the edge of the large-scale MPLS-VRF VPN network. The three functions, Multi-VRF CE, MPLS label switching and the function of MPLS control layer, are independent. Figure 1.1 shows an MPLS-VRF VPN network.

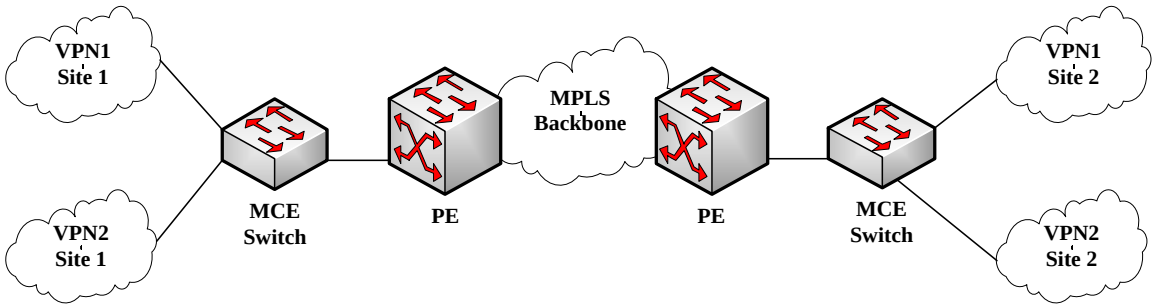


Figure 1.1 MCE in the MPLS-VRF VPN network

76.1.1 Establishing Routes with CE

The Multi-VRF CE switch can establish routes with CE through multiple dynamic routing protocols. CE can be routers or the Ethernet switches. The routing protocols which are supported include OSPF, RIP and BEIGRP. The MCE switch also supports static routing configuration.

The MCE switch generally needs different VLAN ports to connect CEs that belong to different VPNs. The VLAN ports that are used to connect the VPNs require to be related to a VRF. CE does not need to support VRF.

76.1.2 Establishing Routes with PE

The MCE switch (MCE) can connect one or multiple PEs, but both MCE and the connected PEs have to get VRF configured. MCE will provide PE the routes which MCE learns from CE and learns the routes of remote client networks from PE.

The VRF route can be established between MCE and PE through dynamic routing protocols such as BGP, OSPF, RIP and

BEIGRP. Of course, the VRF route can also be established statically.

In general, MCE and PE belong to different autonomous systems. Hence, the method to establish the VRF route between MCE and PE by using EBGP is the key point in this document.

Chapter 77 Multi-VRF CE Configuration

77.1 Default VRF Configuration

Function	Default Configuration
VRF	There is no configuration. All routes are added to the default routing table.
VPN expansibility of VRF	There is no Routing Distinguisher (RD). There is no input/output Routing Target (RT).
Maximum number of VRF routes	10240
VRF port	N/A. None of VLAN ports is related with VRF, and the routes of ports are added to the default routing table.
IP Express Forwarding	The hardware IP routing is not enabled.

77.2 MCE Configuration Tasks

- Configuring VRF
- Configuring a VPN Route
- Configuring BGP Route Between PE and CE
- Testifying the VRF Connectivity between PE and CE

77.3 MCE Configuration

77.3.1 Configuring VRF

Refer to the following steps to configure one or multiple VRFs.

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config# ip vrf *vrf-name*	Creates VRF and enters the VRF configuration mode. vrf-name: VRF name with up to 31 characters
Switch_config_vrf# rd *route-distinguisher*	Sets the route distinguisher of VRF. route-distinguisher: Stands for the distinguisher of the route. It consists of autonomous domain ID and random numbers, or IP and random numbers.
Switch_config_vrf# route-target { export | import | both } *route-target-extened-community*	Creates the expanded VPN attributes of input/output VRF objects. route-target-extended-community: It consists of autonomous domain ID and random numbers, or IP and

	random numbers.
Switch_config_vrf# **exit**	Exits from VRF configuration mode.
Switch_config# interface *intf-name*	Enters the interface configuration mode. intf-name: Stands for the name of an interface.
Switch_config_intf# ip vrf forwarding *vrf-name*	Relates the L3 interface with VRF. vfi-name: Means the name of VRF.
Switch_config_intf# exit	Exits from interface configuration mode.
Switch_config# **ip exf**	Enables ip hardware routing.
Switch_config# show ip vrf [brief | detail | interface] [*vrf-name*]	Browses the VRF information.
Switch_config#no ip vrf *vrf-name*	Deletes the configured VRF and the relation between VRF and the L3 interface. vfi-name: Means the name of VRF.
Switch_config_intf# no ip vrf forwarding [*vrf-name*]	Deletes the relation between the L3 interface and VRF.

77.3.2 Configuring VPN Route

The route can be established between MCE and customer device through the configuration of BGP, OSPF, RIP, BEIGRP or static route. The following takes OSPF configuration as an example, which is similar to other routes' configurations.

NOTE:

When a route is configured on MCE to connect the client network, the VRF attributes of the routing protocol need be specified. VRF need not be configured on the customer device.

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config# router ospf *process-id* **vrf** *vrf-name*	Starts the OSPF-VRF route and enters the configuration mode.
Switch_config_ospf# network *network-number* *network-mask* **area** *area-id*	Defines the OSPF network, mask and area ID.
Switch_config_ospf# **redistribute bgp** *ASN*	Forwards the designated BGP network to the OSPF network.
Switch_config_ospf# **exit**	Exits from the OSPF configuration mode.

Switch_config# **show ip ospf**	Browses the information about the OSPF protocol.
Switch_config# **no router ospf** *process-id*	Deletes the OSPF-VRF routing configuration.

77.3.3 Configuring the BGP Route between PE and CE

Refer to the following configuration commands:

Command	Purpose
Switch# **config**	Enters the switch configuration mode.
Switch_config# **router bgp** *autonomous-system-number*	Starts the BGP protocol by designating autonomous system number and enters the BGP configuration mode.
Switch_config_bgp# **bgp log-neighbor-changes**	Starts the record about BGP neighbor change.
Switch_config_bgp# **address-family ipv4 vrf** *vrf-name*	Enters the configuration mode of VRF address-family.
Switch_config_bgp_af# **redistribute ospf** *ospf-process-id*	Forwards the OSPF routing information to the BGP network.
Switch_config_bgp_af# **network** *network-number/prefix-length*	Configures the network number and the mask's length that are distributed by BGP.
Switch_config_bgp_af# **neighbor** *address* **remote-as** *ASN*	Configures the BGP neighbor and the autonomous system number of a neighbor.
Switch_config_bgp_af# **exit-address-family**	Exits from the configuration mode of address-family.
Switch_config_bgp# **exit**	Exits from the BGP configuration mode.
Switch_config# **show ip bgp vpnv4 [all | rd | vrf]**	Browses the BGP-VRF routing information.
Switch_config# **no router bgp** *ASN*	Deletes the BGP routing configuration.

77.3.4 Testifying the VRF Connectivity between PE and CE

Use the PING command with the VRF option to testify the VRF connectivity of PE and CE.

Command	Purpose
Switch# **ping –vrf** *vrf-name ip-address*	Conducts the PING operation to the addresses in VRF.

Chapter 78 MCE Configuration Example

Figure 77.1 shows a simple VRF network. Both S1 and S2 are the Multi-VRF CE switches. S11, S12 and S13 belong to VPN1, S21 and S22 belong to VPN2, and all of them are customer devices. The OSPF route should be configured between CE and customer device, while the BGP route is configured between CE and PE.

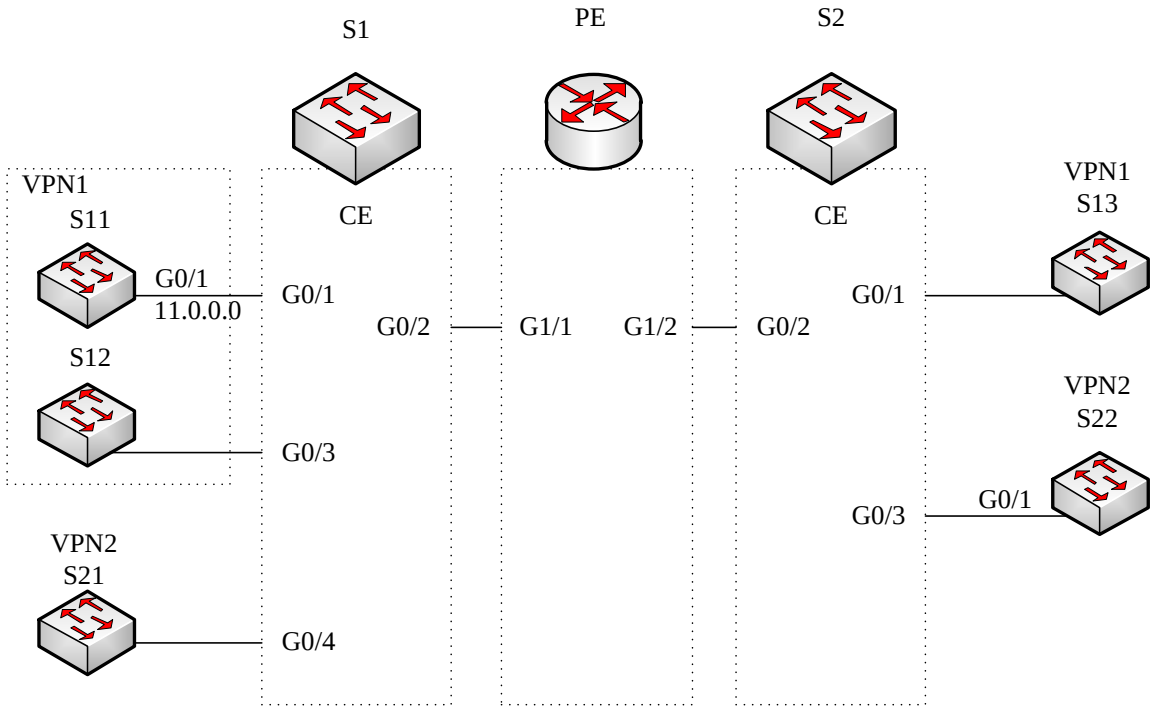


Figure 77.1 MCE configuration example

78.1 Configuring S11

Set the VLAN attributes of the physical interface that connects CE:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

Sets the IP address and the VLAN interface.

Switch_config# interface VLAN11

Switch_config_v11# ip address 11.0.0.2 255.0.0.0

Switch_config_v11# exit

Set the routing protocol between CE and customer's device:

Switch_config# router ospf 101

Switch_config_ospf_101# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_101# exit

78.2 Configuring MCE-S1

Configures VRF on the Multi-VRF CE device.

Switch#config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 100:1

Switch_config_vrf_vpn1# route-target export 100:1

Switch_config_vrf_vpn1# route-target import 100:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 100:2

Switch_config_vrf_vpn2# route-target export 100:2

Switch_config_vrf_vpn2# route-target import 100:2

Switch_config_vrf_vpn2# exit

Configure the loopback port and the physical port, and use the address of the loopback port as the router ID of the BGP protocol.

Switch_config# interface loopback 0

Switch_config_l0# ip address 101.0.0.1 255.255.255.255

Switch_config_l0# exit

S1 connects S11 through the F0/1 port, S21 through the G0/4 port and PE through the G0/2 port.

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/4

Switch_config_g0/4# switchport pvid 15

Switch_config_g0/4# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

Set the L3 VLAN port of a switch, bind the VRF to the VLAN port and set the IP address. S1 connects PE through two logical ports, VLAN21 and VLAN22. The two ports, VLAN11 and VLAN15, connect VPN1 and VPN2 respectively.

Switch_config# interface VLAN11

Switch_config_v11# ip vrf forwarding vpn1

Switch_config_v11# ip address 11.0.0.1 255.0.0.0

Switch_config_v11# exit

Switch_config# interface VLAN15

Switch_config_v15# ip vrf forwarding vpn2

Switch_config_v15# ip address 15.0.0.1 255.0.0.0

Switch_config_v15# exit

Switch_config# interface VLAN21

Switch_config_v21# ip vrf forwarding vpn1

Switch_config_v21# ip address 21.0.0.2 255.0.0.0

Switch_config_v21# exit

Switch_config# interface VLAN22

Switch_config_v22# ip vrf forwarding vpn2

Switch_config_v22# ip address 22.0.0.2 255.0.0.0

Switch_config_v22# exit

Configure the OSPF route between CE and customer device.

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 100

Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 15.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 100

Switch_config_ospf_2#exit

Configure the EBGP route between PE and CE.

Switch_config# router bgp 100

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 21.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 22.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Create VLAN.

Switch_config# vlan 1,11-12,21-22

Enables the forwarding of subnet route of the switch.

Switch_config# ip exf

78.3 Configuring PE

Set VRF on PE:

Switch#config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 200:1

Switch_config_vrf_vpn1# route-target export 200:1

Switch_config_vrf_vpn1# route-target import 200:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 200:2

Switch_config_vrf_vpn2# route-target export 200:2

Switch_config_vrf_vpn2# route-target import 200:2

Switch_config_vrf_vpn2# exit

Set the loopback interface as the router identifier:

Switch_config# interface loopback 0

Switch_config_l0# ip address 102.0.0.1 255.255.255.255

Switch_config_l0# exit

Set the physical interface which connects PE and CE: G1/1 and G1/2 connect S1 and S2 respectively:

Switch_config# interface gigaEthernet 1/1

Switch_config_g1/1# switchport mode trunk

Switch_config_g1/1# interface gigaEthernet 1/2

Switch_config_g1/2# switchport mode trunk

Switch_config_g1/2# exit

Set the L3 VLAN interface of PE, which connects S1:

Switch_config# interface VLAN21

Switch_config_v21# ip vrf forwarding vpn1

Switch_config_v21# ip address 21.0.0.1 255.0.0.0

Switch_config_v21# exit

Switch_config# interface VLAN22

Switch_config_v22# ip vrf forwarding vpn2

Switch_config_v22# ip address 22.0.0.1 255.0.0.0

Switch_config_v22# exit

Set the L3 VLAN interface of PE, which connects S2:

Switch_config# interface VLAN31

Switch_config_v31# ip vrf forwarding vpn1

Switch_config_v31# ip address 31.0.0.1 255.0.0.0

Switch_config_v31# exit

Switch_config# interface VLAN32

Switch_config_v32# ip vrf forwarding vpn2

Switch_config_v32# ip address 32.0.0.1 255.0.0.0

Switch_config_v32# exit

Set the EBGP of PE:

Switch_config# router bgp 200

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# neighbor 21.0.0.2 remote-as 100

Switch_config_bgp_vpn1# neighbor 31.0.0.2 remote-as 300

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# neighbor 22.0.0.2 remote-as 100

Switch_config_bgp_vpn2# neighbor 32.0.0.2 remote-as 300

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Set VLAN and enable the subnet routing forwarding.

Switch_config# vlan 1,21-22,31-32

Switch_config# ip exf

78.4 Configuring MCE-S2

Configures VRF:

Switch#config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 300:1

Switch_config_vrf_vpn1# route-target export 300:1

Switch_config_vrf_vpn1# route-target import 300:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 300:2

Switch_config_vrf_vpn2# route-target export 300:2

Switch_config_vrf_vpn2# route-target import 300:2

Switch_config_vrf_vpn2# exit

Configure the loopback port and the physical port, and use the address of the loopback port as the router ID of the BGP protocol.

Switch_config# interface loopback 0

Switch_config_l0# ip address 103.0.0.1 255.255.255.255

Switch_config_l0# exit

S2 connects S13 through the F0/1 port, S22 through the G0/3 port and PE through the G0/2 port.

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 41

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# switchport pvid 46

Switch_config_g0/3# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

Set the L3 VLAN port of a switch, bind the VRF to the VLAN port and set the IP address. S2 connects PE through two logical ports, VLAN31 and VLAN32. The two ports, VLAN41 and VLAN46, connect VPN1 and VPN2 respectively.

Switch_config# interface VLAN41

Switch_config_v41# ip vrf forwarding vpn1

Switch_config_v41# ip address 41.0.0.1 255.0.0.0

Switch_config_v41# exit

Switch_config# interface VLAN46

Switch_config_v46# ip vrf forwarding vpn2

Switch_config_v46# ip address 46.0.0.1 255.0.0.0

Switch_config_v46# exit

Switch_config# interface VLAN31

Switch_config_v31# ip vrf forwarding vpn1

Switch_config_v31# ip address 31.0.0.2 255.0.0.0

Switch_config_v31# exit

Switch_config# interface VLAN32

Switch_config_v32# ip vrf forwarding vpn2

Switch_config_v32# ip address 32.0.0.2 255.0.0.0

Switch_config_v32# exit

Configure the OSPF route between CE and customer device.

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 41.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 300

Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 46.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 300

Switch_config_ospf_2# exit

Configure the EBGP route between PE and CE.

Switch_config# router bgp 300

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 31.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 32.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Create VLAN.

Switch_config# vlan 1,31-32,41,46

Enables the forwarding of subnet route of the switch.

Switch_config# ip exf

78.5 Setting S22

Set the VLAN attributes of the physical interface of CE, and connect S22 and S2 through interface f0/1:

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 46

Switch_config_g0/1# exit

Sets the IP address and the VLAN interface.

Switch_config# interface VLAN46

Switch_config_v46# ip address 46.0.0.2 255.0.0.0

Switch_config_v46# exit

Set the routing protocol between CE and customer's device:

Switch_config# router ospf 103

Switch_config_ospf_103# network 46.0.0.0 255.0.0.0 area 0

Switch_config_ospf_103# exit

78.6 TestifyingVRF Connectivity

Run the PING command on S1 to testify the connectivity of VPN1 between S1 and S11:

Switch# ping -vrf vpn1 11.0.0.2

!!!!!

--- 11.0.0.2 ping statistics ---

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

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

Testify the connectivity between S1 and PE:

Switch# ping -vrf vpn1 21.0.0.1

!!!!!

--- 21.0.0.1 ping statistics ---

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

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

Chapter 79 VRRP Configuration

79.1 Overview

The Virtual Router Redundancy Protocol (VRRP) ensures the successful single-node service in the default static routing condition. VRRP avoids the defects of the statically designated gateway. A group of OLTs can work together as a virtual OLT through VRRP. The virtual OLT has a virtual IP address and a virtual MAC address for the outside. VRRP chooses one OLT from the OLT group as the master OLT, responsible for forwarding packet. When the master OLT has problems, the standby OLT will promptly take over the tasks of the master OLT without changing the default gateway address. The whole takeover process is transparent to the terminal system. This mechanism can provide fast and effective resolution when trouble occurs.

79.2 VRRP Configuration Task List

- Enabling/Disabling VRRP on the Interface
- Configuring VRRP authentication mode
- Configuring VRRP priority preemption
- Configuring VRRP priority
- Configuring VRRP clock value
- Monitoring and maintaining VRRP

79.3 VRRP Configuration Task

79.3.1 Configuring VRRP Virtual IP Address

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [vrid] **associate** virtual-address address-mask	Configures VRRP Virtual IP address on the interface
no vrrp [vrid] **associate** [virtual-address address-mask]	Deletes VRRP Virtual IP address on the interface

The virtual OLT is enabled after the virtual address of VRRP is configured. The virtual address and the primary IP address of the port must be in the same network segment. Otherwise, the virtual OLT remains in the Init state. When the virtual IP address and the IP address of the port are consistent, the system automatically promote the precedence of the routing OLT to 255.

79.3.2 Configuring VRRP Authentication Mode

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [*vrid*] authentication *WORD*	Configures VRRP authentication mode to

	simple-text.
no vrrp [*vrid*] authentication	Resumes the VRRP authentication mode to the default setting.

In simple-text authentication mode, the authentication character string is in the message as clear code and is forwarded out. The receiver checks the authentication character string in the message to see whether it matches the locally configured authentication character string. The authentication character string has eight characters at most.
By default, the authentication mode of VRRP is no-authen.

79.3.3 Configuring VRRP Description

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [*vrid*] description *WORD*	Configures VRRP description information
no vrrp [*vrid*] description	Deletes VRRP description information

VRRP description information, which is used for stating the usage of local VRRP.
By default, VRRP has no description information.

79.3.4 Configuring VRRP Priority Preemption

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [*vrid*] preempt [delay *second*]	Configures VRRP priority preemption
no vrrp [*vrid*] preempt [delay]	Resumes the default VRRP priority preemption mode.

The priority preemption is effective only to the backup OLT. After the backup OLT receives the announce message from the master OLT, it will examine the priority of the master OLT. If the priority level of the master OLT is lower than the locally configured priority level and the backup OLT is configured with priority preemption, the backup OLT will leap from the backup state to the master state and send the announce message to the outside. Otherwise, the backup OLT remains in the backup state.
In default state, the authentication mode of VRRP is no-authen.

79.3.5 Configuring VRRP Protocol Packet MAC Address

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [*vrid*] source-mac-use-system	Configures VRRP group to forward packets

	with system mac address
no vrrp [*vrid*] source-mac-use-system	Configures VRRP group to forward packets with protocol mac address

By default, VRRP protocol packet forward source address with protocol mac address; after the command is configured, VRRP protocol packet forwards the system mac address as the source address.

79.3.6 Configuring VRRP Priority

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [*vrid*] priority *value* (1~254)	Configures VRRP priority
no vrrp [*vrid*] priority	Resumes the default VRRP priority mode.

When the virtual address and the port address are same, VRRP will automatically increase its priority value to 255. After the virtual address or the port address changes, the priority value automatically resumes to the original value.
The default value is 100.

79.3.7 Configuring VRRP Clock Value

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [*vrid*] timer advertise { *value* | dsec *value* | csec *value*}	Configures VRRP clock value
no vrrp [*vrid*] timer advertise	Resumes the VRRP clock value to the default value.
no vrrp [*vrid*] timer learn	Configures VRRP clock as the learning mode

The clock value means the shortest time for the virtual routing OLT to recover from a trouble. When the master routing OLT is down, the backup routing OLT will serve as the master routing OLT after the 3*advertisement + skew_time interval. It is clear that the trouble cannot be removed immediately if the advertisement clock value is too big. Hence, the default value of the advertisement clock is recommended.
The default value is 1 second.

79.3.8 Configuring VRRP Monitoring Object

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp [*vrid*] track interface *intf-id value*	Configures VRRP monitoring local interface state
no vrrp [*vrid*] track interface *intf-id*	Resumes to the default setting
vrrp [vrid**] track ip** ip-address value	Configures VRRP monitoring to the static routing state to the designated address
no vrrp [*vrid*] track ip *ip-address*	Resumes to the default setting.

With the monitoring function, VRRP group can adjust the priority appropriately according to the change of the link state. It provides an opportunity of switching master line state to the backup line state. The change of the link state refers to whether the destination link bypass the VRRP routing OLT is reachable, rather than the VRRP OLT itself is reachable.
VRRP supports two monitoring objects: First, monitoring the interface status. When the monitored port link state is down, lower the priority of itself proactively. Second, monitoring the static route state of designated node. When the monitored route is unreachable, lower the priority of itself proactively. Monitoring the static route state of designated node needs to apply the function of BFD detecting static route.

79.3.9 Monitoring and Maintaining VRRP

Run the following commands in EXEC configuration mode.

Command	Purpose
show vrrp { brief | [interface *vlan_intf*] [detail]}	Displays the VRRP information.
debug vrrp [interface *intf-id vrid*] {errors | events | packets | all}	Enables the debugging on-off for VRRP packets and events.
no debug vrrp	Disables the debugging on-off for VRRP packets and events.

Displaying the VRRP information:

```
Switch_config#show vrrp interface vlan 1 detail
VLAN1 - Group 1
  VRRP State is Master
  Virtual IP address : 192.168.20.110/24
  Virtual Mac address : 0000.5e00.0101
  Current Priority : 100   (Config 100)
  VRRP timer : Advertise 1.0 s (default)   master_down 3.6 s
  VRRP current timer : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s
  Authentication string is not set
  Preempt is set  (delay : 0  s)
  Learn Advertise Interval is not set
```

Master Router IP : 192.168.20.118, priority : 100, advertisment : 1.0 s

79.3.10 VRRP Configuration Example

The network topology is shown in figure 1.

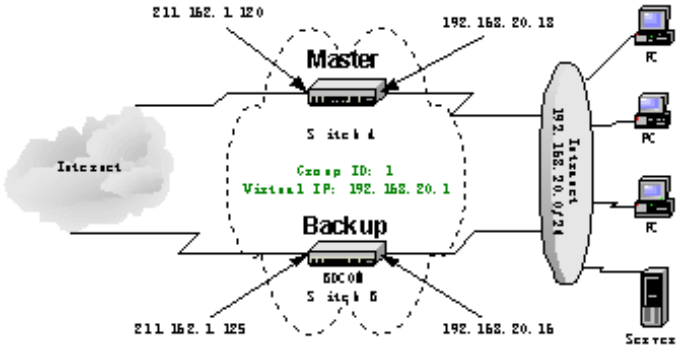


Figure1 Network topology

1. Configuring OLT Switch A

1). Fault 1: Configure the address for the interface of the private network.

Switch_config_v1# **ip address** *192.168.20.18 255.255.255.0*

2). Fault 2: Configure the address for the interface of the public network.

Switch_config_v2# **ip address** *211.162.1.120 255.255.255.0*

3). Fault 3: Configure virtual switch group 1 on the interface of the private network. The virtual address is 192.168.20.1. The priority value is 120.

Switch_config_v1# **vrrp** 1 **associate** *192.168.20.1 255.255.255.0*

Switch_config_v1# **vrrp** 1 **priority** *120*

4). Fault 4: Display information about the virtual OLT.

Switch_config#show vrrp detail

VLAN1 - Group 1

VRRP State is Master

Virtual IP address : 192.168.20.1/24

Virtual Mac address : 0000.5e00.0101

Current Priority : 120 (Config 120)

VRRP timer : Advertise 1.0 s (default) master_down 3.6 s

VRRP current timer : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s

Authentication string is not set

Preempt is set (delay : 0 s)

Learn Advertise Interval is not set

Master Router IP : 192.168.20.18, priority : 100, advertisment : 1.0 s

2. Configuring OLT Switch B

1) Configure the address for the interface of the private network.

Switch_config_v1# **ip address** *192.168.20.16 255.255.255.0*

2) Configure the address for the interface of the public network.

Switch_config_v2# **ip address** *211.162.1.125 255.255.255.0*

Configure virtual OLT group 1 on the interface of the private network. The virtual address is 192.168.20.1. The priority value is 120.

Switch_config_v1# **vrrp** 1 **associate** *192.168.20.1 255.255.255.0*

Display information about the virtual OLT.

Switch_config#show vrrp detail

Switch_config#show vrrp interface vlan *1* detail

VLAN1 - Group 1

VRRP State is Backup

Virtual IP address : 192.168.20.1/24

Virtual Mac address : 0000.5e00.0101

Current Priority : 100 (Config 100)

VRRP timer : Advertise 1.0 s (default) master_down 3.6 s

VRRP current timer : Advertise 0.0 s master_down 3.0 s preempt after 0.0 s

Authentication string is not set

Preempt is set (delay : 0 s)

Learn Advertise Interval is not set

Master Router IP : 192.168.20.18, priority : 120, advertisement : 1.0 s

3. Configuring PC and Server of the Private Network

Configure the default gateway for each PC and server in the private network to 192.168.20.1.

Chapter 80 Multicast Overview

The chapter describes how to cofigure the multicast routing protocol. For the details of the multicast routing commands, refer to the part "Multicast Routing Commands".

The traditional IP transmission allows only one host to communicate with a single host (unicast communication) or to communicate with all hosts (broadcast communication). The multicast technology allows one host to send message to some hosts. These hosts are called as group members.

The destination address of the message sent to the group member is a D-class address (224.0.0.0~239.255.255.255). The multicast message is transmitted like UDP. It does not provide reliable transmission and error control as TCP does.

The sender and the receiver make up of a multicast application. The sender can send the multicast message without joining in a group. However, the receiver has to join in a group before it receives the message from the group.

The relationship between group members is dynamic. The host can join in or leave a group at any time. There is no limitation to the location and number of the group member. If necessary, a host can be a member of multiple groups. Therefore, the state of the group and the number of group members varies with the time.

The router can maintain the routing table for forwarding multicast message by executing the multicast routing protocol such as PIM-DM and PIM-SM. The router learns the state of the group members in the directly-connected network segment through IGMP. The host can join in a designated IGMP group by sending the **IGMP Report** message.

The IP multicast technology is suitable for the one-to-multiple multimedia application.

Note:

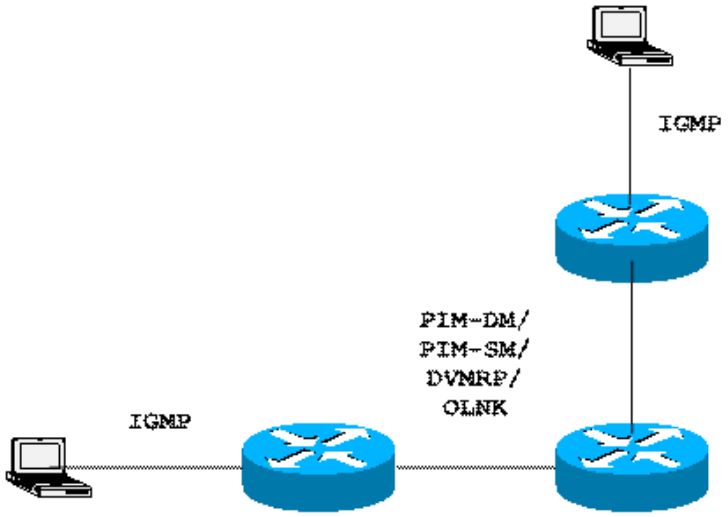
The "router" referred to in this chapter are Layer 3 switches running routing protocols, routers in the general network environment, and other devices running routing protocols.

80.1 Multicast Routing Realization

In the switch software, the multicast routing includes the following regulations:

- IGMP runs between the router and the host in the LAN, which is used to track the group member relationship.
- PIM-DM/PIM-SM is dynamic multicast routing protocols. They run between switches and realizes the multicast forwarding by creating the multicast routing table.

The following figure shows the multicast protocols used in the IP multicast applications:



80.2 Multicast Routing Configuration Task List

80.2.1 Basic Multicast Configuration Task List

- Starting up the multicast routing (mandatory)
- Configuring TTL threshold (optional)
- Canceling rapid multicast forwarding (optional)
- Configuring static multicast route (optional)
- Configuring multicast boundary (optional)
- Configuring multicast helper (optional)
- Configuring Stub multicast route (optional)
- Monitoring and maintaining multicast route (optional)

80.2.2 IGMP Configuration Task List

- Modifying the current version of IGMP
- Configuring the IGMP query interval
- Configuring IGMP Querier interval
- Configuring the maximum response time of IGMP
- Configuring the query interval of the last IGMP group member
- Static IGMP configuration
- Configuring the IGMP **Immediate-leave** list

80.2.3 PIM-DM Configuration Task List

- Regulating the timer
- Designate the PIM-DM version
- Configuring the state refreshment
- Configuring the filtration list
- Setting the DR priority
- Clearing (S,G) information

80.2.4 PIM-SM Configuration Task List

- Configuring static RP
- Configuring standby BSR
- Configuring standby RP
- Displaying PIM-SM multicast routing
- Clearing multicast routes learned by PIM-SM

Chapter 81 Basic Multicast Routing Configuration

NOTE:

The "router" referred to in this chapter are Layer 3 switches running routing protocols, routers in the general network environment, and other devices running routing protocols.

81.1 Starting up Multicast Routing

To allow the switch software to forward the multicast message, you must start up the multicast routing. Run the following command in global configuration mode to start up the multicast message forwarding:

Command	Purpose
ip multicast-routing	Starts up the multicast routing.

81.2 Starting up the Multicast Function on the Port

When the multicast routing protocol runs on a port, the IGMP is activated on the port. The multicast routing protocols include PIM-DM and PIM-SM. Only one multicast routing protocol is allowed to run on the same port. When the router connects multiple multicast domains, different multicast protocols can be run on different ports.

Although the switch software can function as the multicast boundary router (MBR). If possible, do not simultaneously run multiple multicast routing protocols on the same switch for some multicast routing protocols may be badly affected. For example, when PIM-DM (only supports (S, G) entries) and BIDIR PIM-SM (Only supports (*, G) entries) simultaneously run, confusion is to occur.

81.2.1 Starting up PIM-DM

Run the following command to run PIM-DM on a port and then activate the multicast dense mode function:

Command	Purpose
ip pim-dm	Enters the port where PIM-DM is running and then activates PIM-DM multicast routing process in port configuration mode.

81.2.2 Starting up PIM-SM

To run PIM-DM on a port and activate the PIM-DM multicast, perform the following operation:

Command	Purpose
ip pim-sm	Enters a port where PIM-SM needs to run and then activates the PIM-SM multicast routing process in port configuration mode.

81.3 Configuring TTL Threshold

Run the command **ip multicast ttl-threshold** to configure the TTL threshold of the multicast message that is allowed to

pass the port. Run the command **no ip multicast ttl-threshold** to use the default threshold value **1**.

Command	Purpose
ip multicast ttl-threshold *ttl-value*	Configures the TTL threshold on the port.

Example:

The following example shows how the administrator configures the TTL threshold on a port:

interface vlan1

ip multicast ttl-threshold 200

81.4 Configuring IP Multicast Boundary

Run the command **ip multicast boundary** to configure the multicast boundary for the port. Run the command **no ip multicast boundary** to cancel the configured boundary. The commands used in the second configuration will replace the commands used in the first configuration.

Command	Purpose
ip multicast boundary *access-list*	Configures the multicast boundary for the port.

Example:

The following example shows how to configure the management boundary for a port:

interface vlan1

ip multicast boundary acl

!

ip access-list standard acl

permit 192.168.20.97 255.255.255.0

81.5 Configuring IP Multicast Helper

Run the command **ip multicast helper-map** to use the multicast route to connect two broadcast networks in the multicast network. Run the command **no ip multicast helper-map** to cancel the command.

On the first hop router connected to the source broadcast network.

Command	Purpose
interface type number	Enters the interface configuration mode.
ip multicast helper-map broadcast *group-address access-list*	Configures the command ip multicast helper to convert the broadcast message to the multicast message.
ip directed-broadcast	Allows the directional broadcast.
ip forward-protocol [*port*]	Configures the port number allowing to forward the message.

On the last-hop router connecting the destination broadcast network, perform the following operations:

Command	Purpose
interface type number	Enters the interface configuration mode.
ip directed-broadcast	Allows the directional broadcast.
ip multicast helper-map group-address broadcast-address access-list	Configures the command **ip multicast helper** to convert the multicast message to the broadcast message.
ip forward-protocol [port]	Configures the port number allowing to forward the message.

Example:

The following example shows how to configure the command **ip multicast helper**.

The configuration of the switch is shown in the following figure. Configure the command **ip directed-broadcast** on the vlan1 port of the first-hop router to handle the directional message. Configure **ip multicast helper-map broadcast 230.0.0.1 testacl1**, allowing to convert the UDP broadcast message with port number 4000 that is sent from the source address 192.168.20.97/24 to the multicast message with the destination address 230.0.0.1.

Configure the command **ip directed-broadcast** on the vlan1 port of the last-hop router to handle the directional message. Configure **ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2**, allowing to convert the multicast message with port number 4000 and the destination address 230.0.0.1 that is sent from the source address 192.168.20.97/24 to the broadcast message with the destination address 172.10.255.255.

In the first-hop router connecting the source broadcast network, perform the following operations:

```
interface vlan1
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim-dm
!
ip access-list extended testacl
  permit udp 192.168.20.97 255.255.255.0 any
!
ip forward-protocol udp 4000
```

In the last-hop router connecting the destination broadcast network, perform the following operations:

```
interface vlan2
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim-dm
!
ip access-list extended testacl2
  permit udp 192.168.20.97 255.255.255.0 any
!
ip forward-protocol udp 4000
```

81.6 Configuring Stub Multicast Route

Run the commands **ip igmp helper-address** and **ip pim-dm neighbor-filter** to configure the Stub multicast route.

On the port where the stub router and the host are connected, perform the following operations:

Command	Purpose
interface type number	Enters the interface configuration mode.
ip igmp helper-address *destination-address*	Configures the command **ip igmp helper-address** to forward the multicast message to the central router.

On the port where the central router and the stub router are connected, perform the following operations:

Command	Purpose
interface type number	Enters the interface configuration mode.
ip pim-dm neighbor-filter *access-list*	Filters all **pim** messages on the stub router.

Example:

None

81.7 Monitoring and Maintaining Multicast Route

1. Clearing the multicast cache and the routing table

If special caches or the routing table is invalid, you need to clear its content. Run the following commands in management mode:

Command	Purpose
clear ip igmp group [type number] [group-address | <cr>]	Clears the items in the IGMP cache.
clear ip mroute [* | group-address | source-address]	Clears the items in the multicast routing table.

2. Displaying the multicast routing table and system statistics information

The detailed information about the IP multicast routing table, cache or database helps to judge how the resources are used and to resolve network problems.

Run the following commands in management mode to display the statistics information about the multicast route:

Command	Purpose
show ip igmp groups [*type number*| *group-address*] [**detail**]	Displays the information about the multicast group in the IGMP cache.

show ip igmp interface [*type number*]	Displays the IGMP configuration information on the interface.
show ip mroute mfc	Displays the multicast forwarding cache.
show ip rpf [pim-dm | pim-sm] *source-address*	Displays the RPF information.

Chapter 82 IGMP Configuration

82.1 Overview

1. IGMP

Internet Group Management Protocol (IGMP) is a protocol used to manage multicast group members. IGMP is an asymmetric protocol, containing the host side and the switch side. At the host side, the IGMP protocol regulates how the host, the multicast group member, reports the multicast group it belongs to and how the host responds to the query message from the switch. At the Router side, the IGMP protocol regulates how the IGMP-supported switch learns the multicast group member ID of the hosts in the local network and how to modify the stored multicast group member information according to the report message from the host.

Since our switches support the IGMP Router protocol, the multicast routing protocol can be provided with the information about the multicast group members in the current network and the switch decides whether to forward the multicast message. In a word, to enable the switch support the multicast process of the IP message, the switch need be configured to support the multicast routing protocol and the IGMP Router protocol. Currently, our switches support the IGMP Router protocol and version 3 IGMP, the latest version.

There is no independent startup commands for IGMP. The function of the IGMP-Router protocol is started up through the multicast routing protocol.

NOTE:

The "router" referred to in this chapter are Layer 3 switches running routing protocols, routers in the general network environment, and other devices running routing protocols.

82.2 IGMP Configuration

The commands to configure the attributes of the IGMP-Router mainly are the commands to adjust the IGMP parameters. The following is to describe these commands. For details about these commands, refer to explanation documents relative to the IGMP commands.

82.2.1 Changing Current IGMP Version

Up to now, the IGMP protocol has three formal versions. The corresponding RFCs are RFC1112, RFC2236 and RFC3376. IGMP V1 supports only the function to record the multicast group members. IGMP V2 can query the designated multicast group member, generates the leave message when an IGMP host leaves a multicast group, and shortens the change delay of the group member. IGMP V3 has additional functions to update and maintain the multicast group member IDs which correspond to the source host addresses. The IGMP Router protocol of IGMP V3 is fully compatible with the host side of IGMP V1 and IGMP V2. Our switch software supports the IGMP Router protocols of the three IGMP versions.

You can configure the IGMP-Router function at different interfaces (the multicast routing protocol configured on different interfaces can start up the IGMP-Router function) and different versions of IGMP can be run on different interfaces.

Note that a multicast switch can start up the IGMP-Router function on only one of the ports that connect the same network.

Run the following command in interface configuration mode to change the version of the IGMP-Router protocol on a port:

Command	Purpose
ip igmp version *version_number*	Changes the IGMP version running on the current port.

82.2.2 Configuring IGMP Query Interval

No matter what version number of the current IGMP-Router protocol is, the multicast switch can send the IGMP General Query message every a certain time on the port where the IGMP-Router function is started. The transmission address is 224.0.0.1. The purpose of the multicast switch is to get the report message from the IGMP host and therefore know which multicast group each IGMP host in the network belongs to. The interval to send the General Query message is called as IGMP Query Interval. If the parameter IGMP Query Interval is set to a big value, the switch cannot immediately receive the information about which multicast group the current IGMP host belongs to. If the parameter IGMP Query Interval is set to a small value, the flow of the IGMP message is to increase in the current network.

Run the following command in interface configuration mode to modify the IGMP query interval on a port:

Command	Purpose
ip igmp query-interval *time*	Modifies the IGMP query interval on the current interface (unit: second).

82.2.3 Configuring IGMP Querier Interval

As to version 2 and version 3 of the IGMP-Router protocol, if another switch that runs the IGMP-Router protocol exists in the same network, you need to choose a querier. Querier stands for a switch that can send the query message (In fact, it is a port of the switch where the IGMP-Router protocol is enabled). Normally, one network has only one querier, that is, only one switch sends the IGMP Query message. There is no querier choice for IGMP-Router V1 because the multicast routing protocol decides which switch to send the IGMP Query message in IGMP-Router V1.

IGMP-Router V2 and IGMP-Router V3 have the same querier choice mechanism, that is, the switch with the minimum IP address is the querier in the network. The switch that is not the querier needs to save a clock to record the existence of the querier. If the clock times out, the non-querier switch turns to be the querier until it receives the IGMP Query message from the switch with a smaller IP address.

For IGMP-Router V2, you can configure other querier intervals using the following command:

Command	Purpose
ip igmp querier-timeout *time*	Configures the interval for other queriers (unit: second).

For IGMP-Router V1, the interval of other queriers is useless. For IGMP-Router V3, the interval cannot be configured because it is decided by the protocol itself. Therefore, the above configuration commands are only valid for IGMP-Router V2.

82.2.4 Configuring Maximum IGMP Response Time

For IGMP-Router V2 and IGMP-Router V3, special data field in the transmitted IGMP General Query message regulates the maximum response time of the IGMP host. That is, the IGMP host has to send the response message before the regulated maximum response time expires, indicating that the General Query message is received. If the maximum response time is set to a big value, the change of multicast group members delays. If the maximum response time is set to a small value, the flow of the IGMP message will be increased in the current network.

NOTE: The maximum IGMP response time must be shorter than the IGMP query interval. If the value of the maximum

response time is bigger than the query interval, the system will automatically set the maximum response time to query-interval – 1.

For IGMP-Router V2 and IGMP-Router V3, run the following command in interface configuration mode to set the maximum IGMP response time:

Command	Purpose
ip igmp query-max-response-time *time*	Configures the maximum IGMP response time (unit: second).

For IGMP-Router V1, the maximum IGMP response time is decided by the protocol itself. Therefore, the previous command is useless to IGMP-Router V1.

82.2.5 Configuring IGMP Query Interval for the Last Group Member

For IGMP-Router V2 and IGMP-Router V3, When the Group Specific Query message for a specific multicast group is sent, the query interval of the last group member will be used as the maximum response time of the host. That is, the IGMP host has to send the response message before the maximum response time of the last group member expires, indicating that the Group Specific Query message is received. If the IGMP host finds that it need not respond to the query message, it will not respond to the message after the interval. In this case, the multicast switch is to update the saved multicast group member information. If the query interval of the last group member is set to a big value, the change of the multicast group member delays. If the query interval of the last group member is set to a small value, the flow of the IGMP message is to increase in the current network.

For IGMP-Router V2 and IGMP-Router V3, run the following command in interface configuration mode to configure the IGMP query interval of the last group member:

Command	Purpose
ip igmp last-member-query-interval *time*	Configures the IGMP query interval of the last group member (unit: ms).

The previous command is useless for IGMP-Router V1.

82.2.6 Static IGMP Configuration

Besides the functions regulated by the IGMP-Router protocol, BODCOM's switches support the static multicast group configuration on the port. For the IGMP host, its multicast group member relationship may vary. Suppose the IGMP host only belongs to the multicast group **group1**, it receives the multicast message from and sends the multicast message to the multicast group **group1**. After a period of time, it may belong to the multicast group **group2**, and receives the multicast message from and sends the multicast message to the multicast group **group2**. After another period of time, the IGMP host may not belong to any multicast group. Therefore, the multicast group assignment information varies.

Different the above "dynamic multicast group", if a port is configured to belong to a static multicast group, the multicast routing protocol then takes the port as one that always receives and sends the multicast message of the multicast group. To be better compatible with IGMP-Router V3, the static multicast group can be configured to receive the multicast message from the designated source address, that is, the source-filter function is added when the multicast message is received.

Run the following command in interface configuration mode to configure the static multicast group for a port:

Command	Purpose
ip igmp static-group { *| *group-address*} {**include** *source-address*| <*cr*>}	Configures the static multicast group attribute for a port.

82.2.7 Configuring the IGMP Immediate-leave List

If IGMP V2 is started up on a port of the switch and the network that the port connects has only one IGMP host, you can realize the Immediate Leave function of the IGMP host by configuring the **IGMP Immediate-leave** list. According to the regulations of IGMP V2, when a host leaves a specific multicast group, the host will send the Leave message to all multicast switches. After receiving the Leave message, the multicast switches send the Group Specific message to confirm whether any multicast message to be received from or sent to the multicast group by the host exists on the port. If the Immediate Leave function is configured, no message need be interacted between the IGMP host and the multicast switch, the change of the multicast group member IDs will not be delayed.

NOTE: The command can be configured both in global configuration mode and in interface configuration mode. The priority of the command configured in global configuration mode is higher than that configured in interface configuration mode. If the command is first configured in global configuration mode, the command configured in interface configuration mode will be omitted. If the command is first configured in interface configuration mode, the command configured in global configuration mode will delete the command configured in interface configuration mode.
For IGMP-Router V2, run the following command in interface configuration mode to configure the IGMP **Immediate-leave** list:

Command	Purpose
ip igmp immediate-leave group-list *list-name*	Configures the access list that realizes the function to immediately leave the multicast group for the IGMP host.
ip access-list standard *list-name*	Creates a standard IP access list named **list-name**.
permit source-address	Configures the IP address for the IGMP host that will realize the immediate-leave function in standard access-list configuration mode.

The previous command is invalid to IGMP-Router V1 and IGMP-Router V3.

82.3 IGMP Characteristic Configuration Example

82.3.1 Example for changing the IGMP version

The IGMP-Router protocol of latter version is compatible with the IGMP host of low version, but cannot be compatible with the IGMP-Router protocol of the earlier version. Therefore, if, there are switches running the IGMP-Router protocol of the earlier version in the current network, you need to change the IGMP-Router protocol of latter version to the IGMP-Router protocol of earliest version in the same network segment.
Suppose the administrator knows that switches running IGMP-Router V1 and IGMP-Router V2 exist in a network that the local switch connects, the administrator needs to change the version of the IGMP-Router protocol from version 2 to version 1 on a port of the switch that runs IGMP-Router V2.
interface vlan 1

ip igmp version 1

82.3.2 IGMP query interval configuration example

The following example shows how to modify the IGMP query interval to 50 seconds on the interface vlan 1:
interface vlan 1
ip igmp query-interval 50
Configure IGMP Querier interval
For IGMP-Router V2 and V3, if there are routers running the same IGMP-Router protocol in the same network, you need to select a querier. The querier refers to the router that can send query packets (actually a certain port with the IGMP-Router protocol enabled). Under normal operation, there is only one querier in the same network, that is, only one router is sending IGMP Query messages. For IGMP-Router protocol V1, there is no problem of querier selection, because the multicast routing protocol will specify the router to send IGMP Query packets.
The IGMP-Router V2 and V3 adopt the same querier selection mechanism in which the router with the smallest IP address is the querier. For non-queriers, a clock needs to be saved to record the existence time of the querie. When the clock times out, the non-querier becomes a querier and starts to send out IGMP Query packets. Until the router receives an IGMP Query packet from a smaller IP address, it becomes non-querier again.
For IGMP-Router protocol V2, the interval for other queriers can be configured with the following command:

Command	Purpose
ip igmp querier-timeout *time*	Configure the time interval for other queriers, in seconds.

For IGMP-Router protocol V1, the time interval value of other queriers is invlid. For IGMP-Router protocol V3, this time interval is specified by the protocol and cannot be configured. Therefore, the above command is only valid for IGMP-Router protocol V2.

82.3.3 IGMP Querier interval configuration example

The following example shows how to modify the IGMP Querier interval to 100 seconds on the interface vlan 1:
interface vlan 1
ip igmp querier-timeout 100

82.3.4 Maximum IGMP response time example

The following example shows how to modify the maximum IGMP response time to 15 seconds on the interface vlan 1:
interface vlan 1
ip igmp query-max-response-time 15

82.3.5 Example for configuring IGMP query interval for the last group member

The following example shows how to modify the IGMP query interval of the last group member to 2000 ms on the interface vlan 1:
interface vlan 1
ip igmp last-member-query-interval 2000

82.3.6 Static IGMP configuration example

The configuration command of the static multicast group can define different classes of static multicast groups by adopting different parameters. The following examples shows the results of running different command parameter.

interface vlan 1

ip igmp static-group *

The previous configuration command configures all static multicast groups on the interface vlan 1. The multicast routing protocol is to forward all IP multicast messages to the interface vlan 1.

interface vlan 1

ip igmp static-group 224.1.1.7 include 192.168.20.168

The previous configuration command configures the static multicast group 224.1.1.7 on the interface vlan 1, that is, the interface belongs to the multicast group 224.1.1.7. The multicast routing protocol is to forward all IP multicast messages that are finally sent to the multicast group 224.1.1.7 to the interface vlan 1.

interface vlan 1

ip igmp static-group 224.1.1.7 include 192.168.20.168

The previous command configures the static multicast group 224.1.1.7 on the interface vlan 1, and defines source-filter of the multicast group as 192.168.20.168. That is, the interface belongs to the multicast group 224.1.1.7, but it only receives the IP multicast messages from 192.168.20.168. The multicast routing protocol is to forward IP multicast messages that are received from 192.168.20.168 and finally sent to the multicast group 224.1.1.7 to the interface vlan 1.

Run the following command in interface configuration mode to receive the IP multicast message that is from 192.168.20.169 and finally sent to the multicast group 224.1.1.7:

ip igmp static-group 224.1.1.7 include 192.168.20.169

The previous command can be executed for many times to define different source addresses.

NOTE:

In a multicast group, the multicast group information cannot be simultaneously configured both for a specific source address and for all source addresses. The command used in the later configuration will be omitted. For example, If you run the command **ip igmp static-group 224.1.1.7** include 192.168.20.168 after the command **ip igmp static-group 224.1.1.7** is executed, the command **ip igmp static-group 224.1.1.7 include 192.168.20.168** will be omitted.

82.3.7 IGMP Immediate-leave list configuration example

The following example shows how to set the access list to **imme-leave** on the interface vlan 1 with the **immediate-leave** function and to add the IP address 192.168.20.168 of the IGMP host to the access list. The configuration ensures that the IGMP host with IP address 192.168.20.168 realizes the **immediate-leave** function.

interface vlan 1

ip igmp immediate-leave imme-leave

!

ip access-list standard imme-leave

permit 192.168.20.168

Chapter 83 PIM-DM Configuration

83.1 PIM-DM Introduction

Protocol Independent Multicast Dense Mode (PIM-DM) is a multicast routing protocol in dense mode. By default, when the multicast source starts to send the multicast data, all network nodes in the domain receive the data. Therefore, PIM-DM forwards the multicast packets in broadcast-pruning mode. When the multicast source starts to send data, the switches alongside forward the multicast packets to all PIM-activated interfaces except the RPF interface. In this way, all network nodes in the PIM-DM domain can receive these multicast packets. To finish the multicast forwarding, the switches alongside need create the corresponding multicast routing item (S,G) for group G and its source S. The routing item (S,G) includes the multicast source address, multicast group address, incoming interface, outgoing interface list, timer and logo.

If there is no multicast group member in a certain network segment, PIM-DM will send the pruning information, prune the forwarding interface connecting the network segment and then establish the pruning state. The pruning state corresponds to the timeout timer. When the timer times out, the pruning state turns to be the forwarding state again and the multicast data can be forwarded along these branches. Additionally, the pruning state contains information about the multicast source and the multicast group. When the multicast group member appears in the pruning area, PIM-DM actively sends the graft message to the upper field without waiting for the pruning state of the upper field to time out, turning the pruning state to the forwarding state.

As long as source S still sends information to group G, the first-hop switch will periodically send the refreshing information of the routing item (S,G) to the nether original broadcast tree to finish refreshing. The state refreshing mechanism of PIM-DM can refresh the state of the downstream, ensuring that the pruning of the broadcast tree does not time out.

In the multi-access network, besides the DR selection, PIM-DM also introduces the following mechanisms:

- Use the assertion mechanism to select the unique forwarder to prevent the multicast packet from being repeatedly forwarded.
- Use the add/prune restraint mechanism to reduce redundant add/prune information.
- Use the pruning deny mechanism to deny improper pruning actions.

In the PIM-DM domain, the routers that run PIM-DM periodically send the Hello information to achieve the following purposes:

- Discover neighboring PIM routers.
- Judge leaf networks and leaf routers.
- Select the designated router (DR) in the multi-access network.

To be compatible with IGMP v1, PIM-DM is in charge of the DR choice. When all PIM neighboring routers on the interface support DR Priority, the neighboring router with higher priority is selected as the DR. If the priority is the same, the neighboring router with the maximum interface IP value is selected as the DR. If the priority is not shown in the Hello message of multiple routers, the router whose interface has the biggest IP value is selected as the DR.

The PIM-DM v2 of DBCOM's switches supports the neighbor filtration list, CIDR, VLSM and IGMP v1-v3.

NOTE:

The "router" referred to in this chapter are Layer 3 switches running routing protocols, routers in the general network environment, and other devices running routing protocols.

83.2 Configuring PIM-DM

83.2.1 Modifying Timer

The routing protocol adopts several timers to judge the transmission frequency of Hello message and state-refresh control

message. The interval to transmit the Hello message affects whether the neighbor relationship can correctly created. Run the following commands in switch configuration mode to regulate the timer:

Command	Purpose
ip pim-dm hello-interval	Sets the interval (unit: second) to send the Hello message from the interface and the neighbor.
ip pim-dm state-refresh origination-interval	For the first-hop switch directly connecting the source, the interval to send the state-refresh message is only valid to the configurations at the upstream ports. For the following switches, the interval is the period to receive and handle the state-refresh message.

83.2.2 Designating the Version Number

PIM-DM of the router only supports PIM v2.
As PIM v1 is out of date, we supports PIM v2 by default. The command here only aims to be compatible with the former in style.

Command	Purpose
ip pim-dm version *version*	Configures PIM-DM version on the switch logical port.

83.2.3 Configuring State-Refresh

The state-refresh control information of the PIM-DM is forwarded in management mode by default. The configuration commands in interface configuration mode are effective only to the configurations at the upstream ports when the first-hop switch directly connecting the source sends the state-refresh message periodically. For the following switches, the interval is the period to receive and handle the state-refresh message.

Command	Purpose
no ip pim-dm state-refresh disable	Allows to send and receive the state-refresh message on the port.
ip pim-dm state-refresh origination-interval	Configures the interval to send and receive the state-refresh message on the port.

83.2.4 Configuring Filtration List

PIM-DM does not set the filtration list by default. The referred filtration list includes the neighbor filtration list and the multicast boundary filtration list. The filtration list requires to be configured in interface configuration mode.
To forbid a switch or switches at a network segment to join in the PIM-DM negotiation, the neighbor filtration list need be configured. To forbid or permit some groups to pass the local region, the multicast boundary filtration list need be configured.

Command	Purpose
ip pim-dm neighor-filter	Configures the neighbor filtration list.
ip multicast boundary	Configures the multicast boundary filtration list.

83.2.5 Setting DR Priority

To be compatible with IGMP v1, the DR choice is required. By default, the priority of the DR is set to **1**. When all PIM neighboring routers on the interface support DR Priority, the neighboring router with higher priority is selected as the DR. If the priority is the same, the neighboring router with the maximum interface IP value is selected as the DR. If the priority is not shown in the Hello message of multiple routers, the router whose interface has the biggest IP value is selected as the DR.

Run the following command in interface configuration mode:

Command	Purpose
ip pim-dm dr-priority	Configures the priority for the local DR on the designated port.

83.2.6 Clearing Item (S,G)

Normally, item (S,G) in the local MRT or the statistics value of the multicast message number forwarded through item (S,G) need be cleared. Run the following commands in management mode.

Command	Purpose
clear ip mroute pim-dm {* | *group* [*source*]}	Clears the item (S,G) in the local MRT. The operation is to delete all or part items of the local multicast routing table. Multicast message forwarding may be affected. The command is used to delete only the (S,G) items created by the PIM-DM multicast routing protocol on the upstream ports.
clear ip pim-dm interface	Resets the statistics value of multicast message forwarded by (S,G) on the PIM-DM port. The command is used to reset only the (S,G) items created by the PIM-DM multicast routing protocol on the upstream ports.

83.3 PIM-DM State-Refresh Configuration Example

Refer to section 82.2.3 “Configuring State-Refresh”.

Chapter 84 Configuring PIM-SM

84.1 PIM-SM Introduction

Protocol Independent Multicast Spare Mode (PIM-SM) means that the unicast routing table generated by any unicast routing protocol (such as RIP, OSPF, IS-IS, BGP, etc.) can be used to provide routes for IP multicast. Multicast routing has nothing to do with the unicast routing protocol used, as long as the corresponding multicast routing table entries can be generated. PIM uses the Reverse Path Forwarding (RPF) mechanism to forward multicast packets. When a multicast packet arrives at the device, the RPF check is first performed on it: if the RPF check passes, the corresponding multicast routing table entry is created to forward the multicast packet; if the RPF check fails, the packet is discarded. For a detailed introduction to RPF, please refer to Chapter 2 of this white paper.

According to different implementation mechanisms, PIM is divided into the following two modes:

Protocol Independent Multicast-Dense Mode (PIM-DM)

Protocol Independent Multicast-Sparse Mode (PIM-SM)

In addition, the Source-Specific Multicast (SSM) model is realized by using some technologies of PIM-SM.

The sparse mode is relative to the dense mode. The sparse mode is that the host must request to receive data, while the dense mode is that the host needs to receive data actively. The sparse mode is usually used in larger networks, while the dense mode is suitable for smaller networks with denser multicast members.

NOTE:

The "router" referred to in this chapter are Layer 3 switches running routing protocols, routers in the general network environment, and other devices running routing protocols.

84.2 PIM-SM Configuration List

- Enabling global multicast-routing
- Starting up pim-sm
- Configuring Neighbor Filter List
- DR Election
- Configuring Candidate RP
- Configuring Candidate BSR
- Configuring SPT-threshhold
- Configuring SSM
- Configuring Management Domain sz
- Configuring Source Address of Registered Packets
- Configuring anycast-rp
- Displaying PIM-SM Local Routing Entries
- Tracking pim-sm debugging information
- Clearing PIM-SM Routing Entries

84.2.1 Enabling Global Multicast

Command:

ip multicast-routing

no ip multicast-routing

If you want to use the protocol pim-sm, run the command in the configuration mode:

switch_config#ip multicast-routing

Show running as follows:

!

ip multicast-routing

!

If you don't want to use the protocol pim-sm, run the command in the configuration mode:

switch_config #no ip multicast-routing

84.2.2 Starting up PIM-SM

After enabling the multicast-routing function globally, you need to configure an interface supporting pim-sm to send and receive pim-sm protocol packets on the corresponding port. For each routing port, the multicast protocol is exclusive to the port. That is, if other multicast protocols are enabled on the port, pim-sm cannot be configured.

The preconditions for pim-sm to take effect on the port is:

1. The main ip address is configured on the port
2. Port protocol up
3. pim-sm is configured on the port

Configuration example:

switch_config#interface v8

switch_config_v8#ip address 172.17.21.173 255.255.255.0

switch_config_v8#ip pim-sm

After the configuration, use **show running** command to display the result:

!

interface VLAN8

ip address 172.17.21.173 255.255.255.0

no ip directed-broadcast

ip pim-sm

!

Use **show ip pim-sm interface** command to display the result:

switch#show ip pim-sm interface

Intf	Address	Ver/ Mode	Nbr Count	Hello Intvl	DR Prior	DR Addr
v8	172.17.21.173	V2/S	0	30	1	172.17.21.173

If you want to disable pim-sm on the port, use the no form of the command:

switch_config#interface v8

switch_config_v8#no ip pim-sm

You can also configure other pim-sm commands on the port, such as management domain boundary range, bsr boundary, DR priority, neighbor filtering list, hello interval, etc. Please refer to the "pim-sm command manual" for details.

84.2.3 Configuring Neighbor Filter List

Pim-sm needs to maintain neighbor relation in work. Pim-sm finishes negotiation of the detection and related parameters through Hello information. Pim-sm forwards pim-sm hello packet by multicast periodically to all pim routers (224.0.0.13)

and set up the neighbor relation by receiving hello information and agreed parameters. If one router receives Hello information before forwarding Hello information, the router will deem existence of the neighbor, otherwise, it will deem no existence of the neighbor.

Configure the neighbor filter list on the corresponding interface and check and filter the neighbor for the hello packet. If the neighbor filter list is deleted or the forbidden neighbor is relived just now, the neighbor information can only be acquired when the next hello period is appeared.

Steps for configuring neighbor access list:

1. Configure main ip address on the interface;
2. Port protocol up
3. Configure pim-sm on the interface;
4. Configure pim-sm standard access list on the interface and filter the neighbor.

Configuration instances:

```
switch_config#interface v9
switch_config_v9#ip address 172.20.21.172 255.255.255.0
switch_config_v9#ip pim-sm
switch_config_v9#ip pim-sm nbr-filter nbr_permit
switch_config_v9#exit
switch_config#ip access-list standard nbr_permit
switch_config_std_nacl#permit 172.20.21.174 255.255.255.0
```

Configuration result: enable hello packets from segment 172.20.21.0/24 and set up neighbor relation.

```
R172_config_std_nacl#show ip pim-s nei
PIM-SMv2 Neighbor Table
Neighbor        Interface          Uptime/Expires     DR
Address                                    Prior
172.20.21.173     v9          00:15:24/00:01:30   1(DR)
```

Change the configuration as follows and the interface v9 only enables hello packets from 172.20.21.174.

```
S172_config_std_nacl#permit 172.20.21.174 255.255.255.255
```

The debug information is as follows:

```
2004-1-1 00:16:26 PIM-SM: rcvd hello from 172.20.21.173, filter by acl
```

The former established neighbor will be aged gradually until timeout:

```
S172#show ip pim-s nei
PIM-SMv2 Neighbor Table
Neighbor        Interface          Uptime/Expires     DR
Address                                    Prior
172.20.21.173     v9          00:17:21/00:00:03   1(DR)
```

84.2.4 DR Election

DR election is to select DR for the router segment by comparing the priority and IP address in the Hello packets of each router.

The role of DR plays:

1. For response on the host IGMP(v1) information, if the host connects two or more PIM-SM routers directly by the Ethernet, only DR informs these information and forwards packets (*,g) join. If DR and assert winner on the receiver end confronts, the former prevails.

2. DR on the multicast source generates original registration packets and register to RP.

If a new neighbor is found, DR is responsible for forwarding the local memorized BSM packets.

If the locak tries to become DR, enhance the local DR priority and IP address value in condition of the same DR priority.

Steps for configuring DR priority:

1. Configures main ip address on the interface;
2. Port protocol up;
3. Configure pim-sm on the interface;
4. Configure ip pim-sm dr-pri ** on the interface;

84.2.5 Configuring Candidate RP

When you need to configure the switch as a candidate RP, use this command in the following four steps:

1. Configure an ip address for the routing port that needs to be a candidate rp.
2. Enable port pim-sm
3. Configure pim-sm in global configuration state: router pim-sm
4. Configure in pim-sm global configuration mode: c-rp ***

Configuration example:

switch_config#interface loopback1
switch_config_l1#ip addr 1.1.1.1 255.255.255.0
switch_config_l1#ip pim-sm
switch_config#router pim-sm
switch_config_ps#c-rp lo1 list rp-range
switch_config_ps#exit
switch_config#ip access-list stand rp-rang
switch_config_std_nacl#permit 225.1.1.0 255.255.255.0
switch_config_std_nacl#permit 226.1.1.0 255.255.255.0

The above configuration indicates that the candidate CRP address is 1.1.1.1, and the supported group ranges are 225.1.1.0/24 and 226.1.1.0/24.

Using the **show** command, you can see the local configuration of crp and the running state

switch_config#show ip pim-sm bsr
PIMv2 BSR information:
Candidate-RP: 1.1.1.1(Loopback1)
Interval of Advertisements: 60 seconds
Next Advertisement will be sent in 00:00:55
switch_config#

If you want to cancel the candidate RP function of the switch, you can configure in the pim-sm configuration mode. Use no

form of the command to clear the corresponding candidate RP configuration.

```
switch_config#router pim-sm
switch_config_ps#no c-rp loopback1
```

After clearing the corresponding configuration, display the current CRP status of the machine with the **show** command.

```
switch_config_ps#exit
switch_config#show ip pim-sm bsr
PIMv2 BSR information:
switch_config#
```

In addition, you can view the corresponding information in the pim-sm configuration state with **the show running-config** command. For specific usage, please refer to "pim-sm User Manual".

84.2.6 Configuring Candidate BSR

When you configure the switch as a candidate BSR, use this command in the following four steps:

1. Configure an ip address for the routing port that needs to be a candidate rp.
2. Enable port pim-sm
3. Configure pim-sm in global configuration state: router pim-sm
4. Configure in pim-sm global configuration mode: c-bsr ***

Configuration example:

```
switch_config#interface loopback1
switch_config_l1#ip addr 1.1.1.1 255.255.255.0
switch_config_l1#ip pim-sm
switch_config#router pim-sm
switch_config_ps#c-bsr loopback1 30 200
```

The above configuration indicates that after the candidate BSR is selected as the EBSR, the hash length is 30; the priority of this candidate BSR to participate in the election is 200.

Through the **show** command, you can display the local configuration of the candidate BSR and the running status

```
switch_config_ps#show ip pim-s bsr
PIMv2 BSR information:
I am a Candidate-BSR:Loopback1 in sz 224.0.0.0/4.
CBSR-STM state (0-c,1-p,2-e):1.
switch_config_ps#
```

Observe the state switching of CBSR, the following example shows that it has been elected as EBSR:

```
switch_config_ps#show ip pim-s bsr
PIMv2 BSR information:
I am BSR in sz 224.0.0.0/4
  CBSR-STM state (0-c,1-p,2-e):2.
  Address of BSR:      1.1.1.1
  BSR Priority:        200
```

Hash Mask Length: 30
Uptime: 02:54:12
BSR will expires in 00:00:51
switch_config_ps#

If you want to cancel the candidate BSR function, use no form of the command to clear the corresponding c-bsr configuration under the pim-sm configuration mode.

switch_config#router pim-sm
switch_config_ps#no c-bsr loopback1

After clearing the corresponding configuration, you can see the current candidate BSR status of the machine with the **show** command,

switch_config_ps#show ip pim-s bsr
PIMv2 BSR information:
I am NCBSR in sz 224.0.0.0/4
NCBSR-STM state(0-NI,1-AA,2-AP):1
switch_config_ps#

In addition, you can view the corresponding information in the pim-sm configuration state with the **show running-confiure** command. For specific usage, please refer to "pim-sm User Manual".

84.2.7 Configuring SPT-threshhold

When the data is forwarded on the switch, it needs to judge whether shift RPT to SPT. The evidence for this judge is spt-threshold. By default SPT switches if the receiver receives the first data packet. We can set the threshold of RPT switching to SPT; unit: KB/s. In general if RPT switches to SPT, there is no return.

switch_config#router pim-sm
switch_config_ps#spt-threshold 1000

84.2.8 Configuring SSM

SSM model needs support of IGMPv3 and enables IGMPv3 on the PIM-SM device of the receiver. SSM model can be realized by the subset function of pim-sm and the system enables functions of PIM-SM and SSM. When deploying pim-sm, it is recommend to enable pim-sm on all non-boundary interfaces.

During the process of transmitting the information of multicast source to the receiver, whether pim-ssm or pim-sm is determined by whether the multicast group of the receiver prescribed channel (S, G) exists within the multicast group of pim-ssm. Interfaces which enables pim-sm will deem the multicast group within the range adopting the model “pim-ssm”.

Before configuring the basic functions of pim-ssm, the unicast route needs to be configured first, which ensures the interaction of the inner network layer and available route.

Steps for configuring pim-ssm:

1. Enable pim-sm on the interface;
2. Enter pim-sm configuration mode and address range of SSM group address;
3. Configure other functions of pim-sm (optional).

Configuration instances:

switch_config#interface v8
switch_config_v8#ip addr 1.1.1.1 255.255.255.0

switch_config_v8#ip pim-sm
switch_config_v8#exit
switch_config#router pim-sm
switch_config_ps#ssm rang grp_range
switch_config_ps#exit
switch_config#ip access-list standard grp-range
switch_config_std_nacl#permit 233.1.0.0 255.255.0.0
switch_config_std_nacl#
The following configuration does not take the default 232.0.0.0/8 as the group range of SSM, but 233.1.0.0/8. If SSM is canceled, disable ssm related configuration with "no" in the configuration mode of pim-sm.

84.2.9 Configuring Management Domain sz

In the mechanism of non-management domain, one pim-sm domain only has an exclusive BSR. The whole network is controlled by the BSR. For better management, the whole pim-sm domain can be divided into many management domains: each management domain maintains one BSR respectively and serves the multicast group within a certain range; global domain also maintains one BSR, which serves all left multicast groups.
In the mechanism of management domain, the boundary of each management domain is consisted of ZBR and each management domain maintains one BSR, which serves the multicast group of a certain range. The packets (such as assert message and BSR BootStrap message) of multicast protocol belonging to this range cannot pass the boundary of the management domain.
In the network which applies the management domain mechanism, select BSR for different multicast groups from C-BSR. C-RP within the network only forward inform packets to the corresponding BSR and BSR summarizes these packets on RP-SET and inform all devices within the service management domain.
For a group, if you want to find its rp, find sz corresponding to this group based on the longest prefix and sub-mask prevails; and find the corresponding RP-SET in sz according to the prefix and sub-mask of the group, and then calculate rp.
Steps for configuring management domain:
1. On management boundary device ZBR, configuring the range of local management domain group.
2. In the management domain, enter the configuration of pim-sm:
   i. Configure the group range of standby BSR and keep consistent with the management domain boundary.
   ii. Configure standby BSR and designate standby BSR port.

Configuration instances:
1. Configure the management domain range on ZBR
Sa_config_v9#ip pim-sm admin-scope 225.1.1.0 255.255.255.0

2. Configure the group range and port of standby BSR on domain pim-sm device
Sb_config#interface loopback1
Sb_config_l1#ip addr 1.1.1.1 255.255.255.0
Sb_config_l1#ip pim-sm
Sb_config#router pim-sm
Sb_config_ps#c-bsr admin-scope 225.1.1.0 255.255.255.0 30 200
Sb_config_ps#c-bsr loopback1 32 250
30, 32 means the sub-mask length of hash, and 200, 250 means standby BSR priority. When there is inconsistency, the

designated value when configuring standby BSR is superior to that of configuring management domain.

84.2.10 Configuring Source Address of Registered Packets

By default, when DR on the data source forwarding register packets, the address with DR will be taken as the source address of the registered packets. We can designate any active pim-sm interface on the DR device as the source address of the registered packets.
Configuration instances:
Sb_config#interface loopback1
Sb_config_l1#ip addr 1.1.1.1 255.255.255.0
Sb_config_l1#ip pim-sm
Sb_config#router pim-sm
Sb_config_ps# reg-src loopback 1
Designate the main address of loopback1 as the source address of the registered packets.

84.2.11 Configuring anycast-rp

An individual RP has a great load in the domain of pim-sm. To lower such burden, we can designate many same rp. The multicast source and the receiver will forward registered packets and join requests based on the latest rp.
If there is no MSDP module introduced, the neighbor of anycast-rp must be clearly specified when configuring anycast-rp and the neighbor address and the port address acting as rp cannot be the same.
Refer to Pim-sm Command Manual for configuration instances.

84.2.12 Displaying pim-sm Local Routing Entries

If you want to display PIM-SM multicast routing information, you can use the **show ip mroute pim-sm** command.
show ip mroute pim-sm [*group-address*] [*source-address*]

Parameter

Parameter	Description
group-address	Group address
source-address:	Source address

Default

None

Command Mode

EXEC

Usage Guidelines

Use this command to display the multicast routing entries of the PIM-SM routing router.

Example

```
switch#show ip mroute pim-sm
IP PIM-SM Multicast Routing Table:
(source, group)  RP    Uptimer/Expires  Flags
(*, 225.1.1.10), 9.1.1.1, 00:15:14/00:02:37,JOIN|IGMP
Upstream interface: VLAN5, RPF nbr 192.168.100.143
Downstream interface list:
 VLAN2, 00:13:23/00:02:37
(192.166.1.253, 225.1.1.10), 00:15:14/00:02:46 JOIN|IGMP
Upstream interface: VLAN5, RPF nbr 192.168.100.143
Downstream interface list:
 VLAN2, 00:15:14/00:02:46
```

Related Command

None

84.2.13 Clearing pim-sm Routing Entries

If you want to clear the multicast routing information saved in the pim-sm multicast router, you can use the **clear ip mroute pim-sm** command.

clear ip mroute pim-sm [***** | *group-address*] [*source-address*]

Parameter

Parameter	Description
*	Delete all multicast routes created by PIM-SM.
group-address	Delete the multicast routing of the related group.
source-address	Delete the multicast route of the related source.

Default

None

Command Mode

EXEC

Usage Guidelines

Use this command to clear the multicast routing information saved in the router when errors occur.

Example

Example 1: The example shows how to clear all routes created by PIM-SM in the local MRT upstream port.

switch#clear ip mroute pim-sm *

Example 2: The example shows how to clear all routes created by PIM-SM in the local MRT upstream port and whose group address is 239.1.1.1.

switch#clear ip mroute pim-sm 239.1.1.1

Example 3: The example shows how to clear the local MRT upstream port created by PIM-SM (192.168.20.138, 239.1.1.1).

switch#clear ip mroute pim-sm 239.1.1.1 192.168.20.131

Related Command

None

84.2.14 Tracking pim-sm Debugging Information

If you want to track PIM-SM packets and state machine information, you can use the **debug ip pim-sm** command.

debug ip pim-sm [hello|jp|register|assert|bsr|timer] [packet]

Parameter

Parameter	Description
hello	Track the packet information sent and received by the hello module.
jp	Track Join/Prune packet information.
register	Track the register packet information.
assert	Track the register packet information.
bsr	Track BSR packet information.
time	Track timer information.
packet	Track state machine activity information.

Default

None

Command Mode

EXEC

Usage Guidelines

Use this command to track the status changes of the PIM-SM router and the sending and receiving of packets.

Example

Example 1 Trace hello packets interaction.

switch#debug ip pim-sm hello

2003-4-21 16:44:00 PIM-SM: VLAN5, Rcv Hello Msg, Source = 192.168.100.143, Destination = 224.0.0.13, len = 34

2003-4-21 16:44:07 PIM-SM: VLAN5, Send Hello Msg, Destination = 224.0.0.13, len = 34

2003-4-21 16:44:08 PIM-SM: VLAN2, Send Hello Msg, Destination = 224.0.0.13, len = 34

2003-4-21 16:44:10 PIM-SM: VLAN2, Rcv Hello Msg, Source = 192.168.21.144, Destination = 224.0.0.13, len = 34

Example 2 Tracking JP packets interaction and status changes.

switch#debug ip pim-sm jp

switch#PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 224.2.127.254

SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 224.2.127.254

SM state = PS_ST_JP_J, ev = PS_EV_JP_PRUNE.

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 239.255.255.250

SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 239.255.255.250

SM state = PS_ST_JP_J, ev = PS_EV_JP_PRUNE.

2003-4-21 16:48:52 PIM-SM: VLAN5, Rcv J/P Msg, Source = 192.168.100.143, Destination = 224.0.0.13, len = 42

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 225.1.1.10

SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.

Example 3 Tracking register packets interaction and status changes.

S142#debug ip pim-sm register

S142#2003-4-21 16:52:19 Line protocol on Interface VLAN5, changed state to up

2003-4-21 16:52:29 PIM-SM: VLAN5, Rcv Register Msg, Source = 192.168.100.143, Destination = 192.166.100.142, len = 57

2003-4-21 16:52:29 PIM-SM: VLAN5 Rcv Register Msg, Source = 192.168.100.143, Destination = 192.166.100.142, len = 57

Related Command

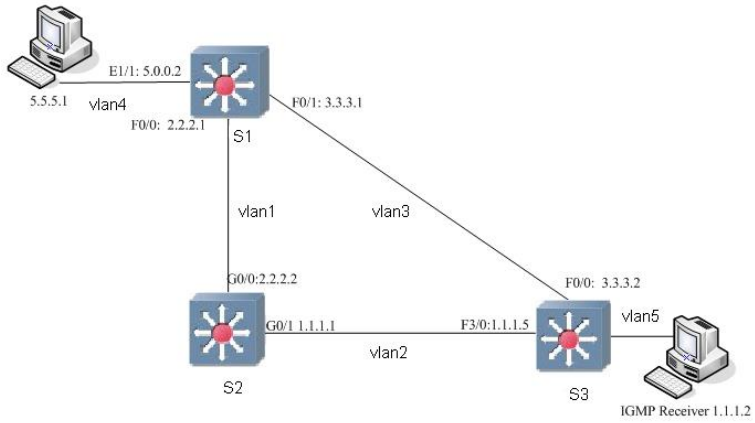
None

84.3 Configuration Example

NOTE:

The "router" referred to in this chapter are Layer 3 switches running routing protocols, routers in the general network environment, and other devices running routing protocols.

84.3.1 pim-sm Common Topology Configuration Examples



The topology shown in the figure above:

1. Enable the multicast forwarding function of all routers:

switch_config#ip multicast-routing

2. Configure the pim-sm protocol on all ports to be multicast forwarding:

Take S1 as an example:

S1_config_v4#ip pim-sm

S1_config_v3#ip pim-sm

S1_config_v1#ip pim-sm

3. Configure RP.

3.1 For dynamic rp, you only need to configure it on the route that is responsible for c-bsr and c-rp, c-bsr and c-rp do not need to be configured on the same machine

As shown in the figure: Choosing S2 to act as c-bsr and c-rp needs to be the routing port of candidate bsr or candidate rp, and the ip address needs to be configured first.

S2_config_l0#ip add 6.6.6.6 255.255.255.0

S2_config_l0# ip pim-s

S2_config#router pim-sm

S2_config_ps#c-bsr loopback0

S2_config_ps#c-rp loopback0

3.2 For static rp, you need to specify the reachable rp address on each pim router. The port as the rp address must be configured with pim-sm:

The configuration on S2 is as follows:

S2_config_l0#ip add 6.6.6.6 255.255.255.0

S2_config_l0# ip pim-s

S2_config_ps#static-rp 6.6.6.6

Only need to configure on S1 and S3:

S1_config_ps#static-rp 6.6.6.6

S3_config_ps#static-rp 6.6.6.6

4. To enable the ssm function, the entire pim domain must be consistent: (see 2.8)

The SSM model needs the support of IGMPv3, so ensure that the IGMPv3 function is enabled on the PIM-SM device

connected to the receiver. The SSM model is implemented through a subset of pim-sm functions. Therefore, the system has SSM capabilities while enabling the PIM-SM function. When deploying a pim-sm domain, it is recommended to enable pim-sm on all non-boundary interfaces.

In the process of delivering information from the multicast source to the receiver, whether the pim-ssm model or the pim-sm model is used depends on whether the multicast group in the receiver's subscribed channel (S, G) is within the range of the pim-ssm multicast group. All interfaces enabled with pim-sm will be considered that the multicast group within this range adopts the pim-ssm model.

Before configuring the basic functions of pim-ssm, you need to configure unicast routing to ensure that the network layer is interoperable and routes are reachable.

The following three steps to configure pim-ssm:

1. Enable pim-sm on the port.
2. Enter the pim-sm configuration state and configure the SSM group address range.
3. Configure other functions of pim-sm (optional).

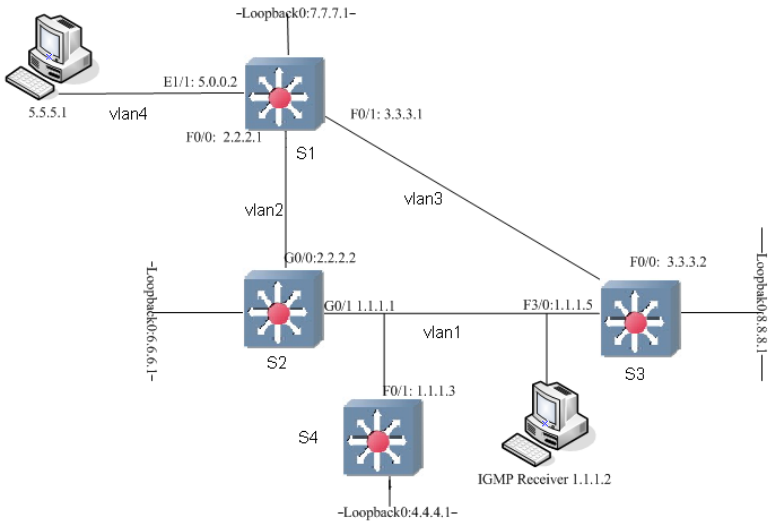
Configuration example:

```
switch_config#interface vlan8
switch_config_v8#ip addr 1.1.1.1 255.255.255.0
switch_config_v8#ip pim-sm
switch_config_v8#exit
switch_config#router pim-sm
switch_config_ps#ssm rang grp_range
switch_config_ps#exit
switch_config#ip access-list standard grp-range
switch_config_std_nacl#permit 233.1.0.0 255.255.0.0
switch_config_std_nacl#
```

The SSM group range of above configuration is not the default 232.0.0.0/8, but the configured 233.1.0.0/16. If you want to cancel the SSM, you can use no form of the command to cancel the ssm related configuratin.

Take the following topology as an example:

In the figure below, S2 is rp, and S3 is dr on the 1.1.1.0 network segment



To use the ssm function to forward multicast traffic in the range of 233.1.0.0/16, you must configure each route in the entire pimsm domain (in the topology in the above figure, that is, S1, S2, S3, and S4 need to be configured)

switch_config#router pim-sm

switch_config_ps#ssm rang grp_range

switch_config_ps#exit

switch_config#ip access-list standard grp-range

switch_config_std_nacl#permit 233.1.0.0 255.255.0.0

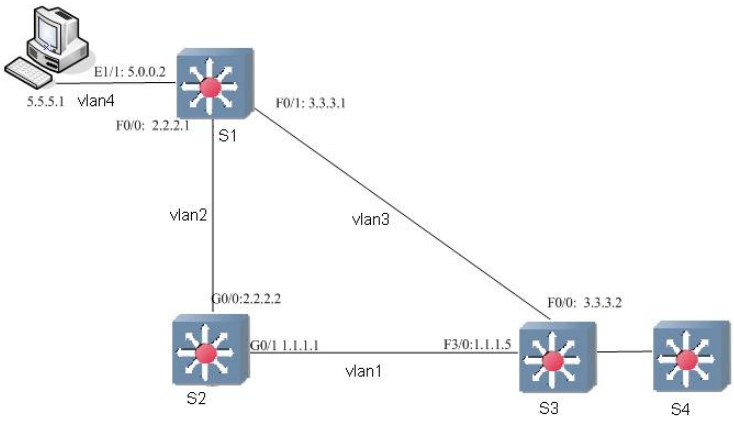
The igmp receiver 1.1.1.2 in the figure sends out the report of igmp v3. When including (5.5.5.1, 233.1.0.1), the dr (S3) of the lan will directly join the source (5.5.5.1) instead of joining rp.

If the direct-connected S1 router receives a packet (5.5.5.1, 233.1.0.1), it will directly forward the packet along the established spt tree without registering to rp.

In this way, the efficiency is improved because the overhead of register is saved and the spt tree is used for forwarding.

Note: If the report sent by igmp receiver 1.1.1.2 (*, 233.1.0.1), it will not be processed because this group address is covered by the ssm range. (For groups in the ssm range, only reports from the specified source are processed).

84.3.2 Mixing of Multi-Protocol Multicast



As shown in the above figure,

Configure ip pim-sm on vlan1 and vlan3 of S3.

Configure Ip pim-dm on Vlan4 of S1

S3 serves as the boundary between the pimsm domain and the pimdm domain, namely pmbr

At this time, S3 will generate an (**RP) entry for each rp. All traffic of groups using the rp address in the pimsm domain will flow along the (**RP) entry to S3, and forward to S4. Therefore, when using the mixed configuration function, you cannot mix the ssm function at the same time.

Chapter 85 IPv6 Protocol Configuration

85.1 IPv6 Protocol Configuration

The configuration of the IPv6 address of the router only takes effect on the VLAN interface, not on the physical interface. The IPv6 protocol is disabled in default state. If the IPv6 protocol need be used on a VLAN interface, this protocol should be first enabled in VLAN interface configuration mode. To enable the IPv6 protocol, users have to set the IPv6 address. If on a VLAN interface at least one IPv6 address is set, the VLAN interface can handle the IPv6 packets and communicates with other IPv6 devices.

To enable the IPv6 protocol, users should finish the following task:

- Setting at least one IPv6 address in VLAN interface configuration mode

85.2 Enabling IPv6

85.2.1 Setting the IPv6 Address

The IPv6 address is used to determine the destination address to which the IPv6 packets can be sent. There are three kinds of IPv6 addresses.

Kind	Referred Format	Remarks
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	**2001:0:0:0:0DB8:800:200C:417A** stands for a unicast address, while **64** stands for the length of the prefix of this address.
Multicast address	FF01:0:0:0:0:0:0:101	All multicast addresses begin with FF.
Any address	2002:0:0:0:0DB8:800:200C:417A/64	The format of this address is the same as that of the unicast address. Different VLAN interfaces can be set to have the same address, no matter it is a unicast/broadcast/multicast address.

For the further details of the IPv6 address, see RFC 4291.

In order to enable IPv6, users must set a unicast address in VLAN interface configuration mode. The set unicast address must be one or multiple addresses of the following type:

- IPv6 link-local address
- Global IPv6 address

To set an IPv6 link-local address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 enable	Sets a link-local address automatically.
ipv6 address fe80::x link-local	Sets a link-local address manually.

NOTE:

- The link-local address must begin with fe80. The default length of the prefix is 64 bit. At manual settings only the values at the last 64 bits can be designated.
- On a VLAN interface can only one link-local address be set.
- After IPv6 is enabled through the configuration of the link-local address, IPv6 only takes effect on the local link.

Chapter 86 Setting the IPv6 Services

86.1 Setting the IPv6 Services

After IPv6 is enabled, all services provided by IPv6 can be set. The configurable IPv6 service is shown below:

(1). Managing the IPv6 Link

86.1.1 Managing the IPv6 Link

IPv6 provides a series of services to control and manage the IPv6 link. This series of services includes:

(1). Setting the MTU of IPv6

(2). Setting the transmission frequency of the ICMPv6 packet

(3). Setting IPv6 destination unreachablity

(4). Setting IPv6 ACL

1. Setting the MTU of IPv6

All interfaces have a default IPv6 MTU. If the length of an IPv6 packet exceeds MTU, the router will fragment this IPv6 packet.

To set IPv6 MTU on a specific interface, run the following command in interface configuration mode:

Command	Purpose
ipv6 mtu bytes	Sets IPv6 MTU on an interface.

2. Setting IPv6 redirection

Sometimes, the route selected by the host is not the best one. In this case, when a switch receives a packet from this route, the switch will transmit, according to the routing table, the packet from the interface where the packet is received, and forward it to another router which belongs to the same network segment with the host. Under this condition, the switch will notify the source host of sending the packets with the same destination address to another router directly, not by way of the switch itself. The redirection packet demands the source host to replace the original route with the more direct route contained in the redirection packet. The operating system of many hosts will add a host route to the routing table. However, the switch more trusts the information getting from the routing protocol and so the host route will not be added according to this information.

IPv6 redirection is opened by default. However, if a hot standby router protocol is configured on an interface, IPv6 redirection is automatically closed. If the hot standby router protocol is canceled, this function will not automatically opened.

To open IPv6 redirection, run the following command:

Command	Purpose
ipv6 redirects	Allows IPv6 to transmit the redirection packets.

3. Setting IPv6 destination unreachablity

In many cases, the system will automatically transmit the destination-unreachable packets. Users can close this function. If this function is closed, the system will not transmit the ICMP unreachable packets.

To enable this function, run the following command:

Command	Purpose
ipv6 unreachables	Allows IPv6 to transmit the destination unreachable packets.

4. Setting IPv6 ACL

Users can use ACL to control the reception and transmission of packets on a VLAN interface. If you introduce ACL on a VLAN interface in global configuration mode and designate the filtration's direction, the IPv6 packets will be filtered on this VLAN interface.

To filter the IPv6 packets, run the following command in interface configuration mode.

Command	Purpose
ipv6 access-group *WORD*{ in | out }	Filters the IPv6 packets in the reception direction on a VLAN interface.

Chapter 87 ND Configuration

87.1 ND Overview

A node (host and router) uses ND (Neighbor Discovery protocol) to determine the link-layer addresses of the connected neighbors and to delete invalid cache rapidly. The host also uses the neighbor to discover the packet-forwarding neighboring routers. Additionally, the node uses the ND mechanism to positively trace which neighbors are reachable or unreachable and to test the changed link-layer address. When a router or the path to a router has trouble, the host positively looks for another working router or another path.

IPv6 ND corresponds to IPv4 ARP, ICMP router discovery and ICMP redirect. There is no corresponding neighbor unreachablity detection mechanism and protocol in IPv4.

ND supports the following link types: P2P, multicast, NBMA, shared media, changeable MTU and asymmetric reachability. The ND mechanism has the following functions:

(1) To discover routers: how the host to locate the routers on the connected links.

(2) To discover prefixes: how the host to find a group of address prefixes, defining which destinations are on-link on the connected links.

(3) To discover parameters: how the node to know the link-related or network-related parameters of the transmission interface.

(4) To automatically set addresses: how the node to set the address of an interface automatically.

(5) Address solution: When the IP of a destination is given, how a node determines the link-layer address of the on-link destination.

(6) To determine the next hop: it is an algorithm to map the IP address of a destination to the neighboring IP. The next hop can be a router or destination.

(7) To test unreachable neighbors: how a node to determine unreachable neighbors; if neighbor is a router, the default router can be used.

(8) To test repeated address: how a node to determine whether a to-be-used address is not used by another node.

(9) Redirect: how a router to notify the host of the best next hop.

87.1.1 Address Resolution

Address resolution is a procedure of resolving the link-layer address through node's IP. Packet exchange is realized through ND request and ND notification.

- Configuring a static ND cache

In most cases, dynamic address resolution is used and static ND cache configuration is not needed. If necessary, you can set static ND cache in global mode and the system will use it to translate IP into the link-layer address. The following table shows how to set a static-IP-to-link-layer-address mapping.

Run the following relative command in global mode:

Command	Purpose
ipv6 neighbor ipv6address **vlan** vlanid hardware-address	Sets a static ND cache and translates IPv6 address into a link-layer address.

Chapter 88 OSPFv3 Configuration

88.1 Overview

OSPFv3 is an IGP routing protocol developed by the OSPF working group of IETF for the IPv6 network. OSPFv3 supports the IPv6 subnet, the mark of the external routing information and the packet's authentication.

OSPFv3 and OSPFv2 have a lot in common:

- Both router ID and area ID are 32 bit.
- The following are the same type of packets: Hello packets, DD packets, LSR packets, LSU packets and LSAck packets.
- Having the same neighbor discovery mechanism and the same neighborhood generation mechanism
- Having the same LSA expansion mechanism and the same LSA aging mechanism

The main differences of both OSPFv3 and OSPFv2 are shown below:

- OSPFv3 is running on the basis of link, while OSPFv2 is running on the basis of network segment.
- OSPFv3can run multiple instances on the same link.
- OSPFv3 labels its neighbor through router ID, while OSPFv2 labels its neighbor through IP.
- OSPFv3 defines 7 classes of LSAs.

The following table shows some key functions in the realization of the OSPFv3 functions.

Key attributes	Description
Stub domain	Supports the stub domain.
Route forwarding	Means that routes that are learned or generated by any routing protocol can be forwarded to the domains of other routing protocols. In the autonomous domain, it means that OSPFv3 can input the RIPng learned routes. The routes learned by OSPFv3 can also be exported to RIPng. Between the autonomous domains, OSPFv3 can import the BGP-learned routes; OSPFv3 routes can also be exported to the BGPs.
Parameters of a routing interface	The following are configurable interface parameters: output cost, retransmission interval, interface's transmission delay, router's priority, interval for judging the shutdown of a router, hello interval, and authentication key.
Virtual link	Supports the virtual link.

88.2 OSPFv3 Configuration Task List

OSPFv3 demands the switchover of routing data between in-domain router, ABR and ASBR. In order to simplify the settings, you can make related configuration to enable them to work under the default parameters without any authentication; if you want to change some parameters, you must guarantee that the parameters on all routers are identical.

To set OSPFv3, you must perform the following tasks. Except that the task of activating OSPFv3 is mandatory, other settings are optional.

- Enabling OSPFv3
- Setting the parameters of the OSPFv3 interface

- Setting OSPFv3 on different physical networks
- Setting the parameters of the OSPFv3 domain
- Configuring the NSSA Domain of OSPFv3
- Setting the Route Summary in the OSPFv3 Domain
- Setting the Summary of the Forwarded Routes
- Generating a Default Route
- Choosing the route ID on the loopback interface
- Setting the management distance of OSPFv3
- Setting the Timer of Routing Algorithm
- Monitoring and Maintaining OSPFv3

88.3 OSPFv3 Configuration Tasks

88.3.1 Enabling OSPFv3

Before OSPFv3 is enabled, the function to forward the IPv6 packets must be enabled.

Enabling OSPFv3 requires creating an OSPFv3 routing process, specifying the router ID of the process, and enabling OSPFv3 on the interface. Run the following commands in global configuration mode:

Command	Purpose
router ospfv3 *process-id*	Activates OSPFv3 and enters the router configuration mode.
router-id *router-id*	Sets the router ID of a router on which OSPFv3 is running.

Run the following command in interface configuration mode:

Command	Purpose
ipv6 ospf *process-id* area *area-id* [instance *instance-id*]	Enables OSPFv3 on an interface.

NOTE: If the OSPFv3 process is still not created before OSPFv3 is enabled on an interface, the OSPFv3 process will be automatically created.

88.3.2 Setting the Parameters of the OSPFv3 Interface

During OSPFv3 realization, related OSPFv3 parameters on an interface are allowed to be modified according to actual requirements. Of cause you have no need to change every parameter, but you have to make sure that some parameters are consistent on all routers in the connected networks.

Run the following commands in interface configuration mode to do relevant configurations:

Command	Purpose
ipv6 ospf cost *cost*	Sets the cost of the packet that is transmitted from the

	OSPFv3 interface.
ipv6 ospf retransmit-interval *seconds*	Sets the LSA retransmission interval between neighbors.
ipv6 ospf transmit-delay *seconds*	Sets the delay time for transmitting LSA on an OSPFv3 interface.
ipv6 ospf priority *number*	Sets a router to be the priority of the OSPFv3 DR router.
ipv6 ospf hello-interval *seconds*	Sets the interval for the OSPFv3 interface to transmit the Hello packets.
ipv6 ospf dead-interval *seconds*	Means that in a regulated interval if the OSPFv3 packets are not received from a neighboring router, this neighboring router is viewed to be shut down.

88.3.3 Setting OSPFv3 on Different Physical Networks

OSPFv3 divides physical network media into the following three kinds:

- Broadcast networks (Ethernet, Token Ring, FDDI)
- Non-broadcast and multi-access networks (SMDS, Frame Relay, X.25)
- Point-to-point networks (HDLC, PPP)

The command can configure your network or broadcast network or non-broadcast, multi-access network.

X.25 and Frame Relay networks provide optional broadcast capabilities. OSPF can be configured to work on broadcast networks through the **map** command. For the **Map** command, please refer to the description of the x.25 and Frame Relay map commands in the WAN Command Reference.

88.3.4 Setting the OSPF Network Type

No matter what physical media type the network is, you can configure your network to be a broadcast network, a non-broadcast network or a multi-access network. So you can set your network flexibly and your network can be set to be a non-broadcast and multi-access one, or a broadcast network such as the X.25, Frame Relay or SMDS network. Also the neighbor's settings will be simplified.

To set an un-broadcast and multi-access network is to suppose that every two routers have a virtual link or suppose a full-mesh network. It is unrealistic due to unbearable cost. But you set this network to be a point-to-multipoint one. Between those routers which are not adjacent the routing information can be switched through the virtual link.

The OSPFv3 point-to-multipoint interface can be set to be multipoint-to-point interface, through which multiple routes of a host can be established. The OSPFv3 point-to-multipoint network, comparing with the non-broadcast and multi-access network or the point-to-point network, has the following advantages:

- The point-to-multipoint network is easy to be set without generating DR.
- This kind of network do not require the full-mesh topology, so the construction cost is relatively low.
- This kind of networks are more reliable. Even if its virtual link fails, the connection can be maintained.

The network type of the routers is the broadcast type.

88.3.5 Setting the Parameters of the OSPFv3 Domain

The configurable domain parameters include: authentication, designating a stub area and specifying a weight for a default summary route. Its authentication is based on password protection.

The stub area means that external routes cannot be distributed to this area. Instead, ABR generates a default external route that enters the stub area, enabling the stub area to communicate with external networks of an autonomous area. In order to make use of the attributes supported by the OSPF stub, the default route must be used in the stub area. To further reduce LSAs that are forwarded to the stub area, you can forbid the summary function on ABR.
Run the following command in router configuration mode to set the domain's parameters:

Command	Purpose
area *area-id* **stub** [no-summary]	Defines a stub area.
area *area-id* default-cost *cost*	Sets the weight of the default route of the stub area.

As to those areas that are not backbone areas and do not connect the backbone areas directly or as to those discontinuous areas, the OSPFv3 virtual link can be used to establish a logic connectivity. In order to create a virtual link, you have to perform configuration at the two terminals of the virtual link. If only one terminal is configured, the virtual link cannot work.
Run the following command in router configuration mode to set the domain's parameters:

Command	Purpose
area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*]	Establishes the virtual link.

88.3.6 Setting the Route Summary in the OSPFv3 Domain

With this function ABR can broadcast a summary route to other areas. In OSPFv3 ABR will broadcast each network to other areas. If network IDs are distributed to be continuous, you can set ABR to broadcast a summary route to other areas. The summary route can cover all networks in a certain range.
Run the following command in router configuration mode to set the address' range:

Command	Purpose
area area-id **range** ipv6-prefix /prefix-length	Sets the address' range of the summary route.

88.3.7 Setting the Summary of the Forwarded Routes

When routes are distributed from other routing areas to the OSPFv3 routing area, each route is singularly broadcasted as an external LSA. However, you can set a route on a router to make this route cover an address range. In this way, the size of the OSPFv3 link-state database can be reduced.
Run the following command in router configuration mode to set a summary route:

Command	Purpose
summary-prefix ipv6-prefix /prefix-length	Broadcasts only one summary route.

88.3.8 Generating a Default Route

ASBR should generate a default route to enter the OSPFv3 routing area. Whenever it is, you make configuration to enable a router to distribute a route to the OSPFv3 routing area and this route becomes ASBR automatically. However, ASBR does not generate a default route by default to enter the OSPFv3 routing area.

88.3.9 Choosing the Route ID on the Loopback Interface

OSPFv3 uses the maximum IPv4 address as its router ID. If the interface that connects the IPv4 address is down or the IPv4 address is deleted, the OSPF process will recalculate the ID of this new router and retransmit the routing information from all interfaces.

If an IPv4 address is configured on a loopback interface, the router will first use the IPv4 address of loopback as its ID. Because the loopback interface will never be down, the routing table is greatly stable.

The router can first select the loopback interface as its ID or select the maximum IPv4 address in all loopback interfaces as its ID. If there is no loopback interface, the IPv4 address of a router will be used as the router ID. You cannot specify OSPFv3 to use any specific interface.

Run the following commands in global configuration mode to set the IP loopback interface:

Command	Purpose
interface loopback *num*	Creates a loopback interface and enters the interface configuration mode.
ip address ip-address mask	Distributes an IPv4 address for an interface.

88.3.10 Setting the Management Distance of OSPFv3

The management distance means the trust level of the routing information source. Generally speaking, the management distance is an integer between 0 and 255. The bigger its value is, the lower the trust level is. If the management distance is 255, the routing information source will be distrusted and omitted.

OSPFv3 uses three different kinds of management distances: inter-domain, inner-domain and exterior. The routes in a domain are called inner-domain routes; the routes to other domains are called inter-domain routes; the routes transmitted from other routing protocols are called the exterior routes. The default value of each kind of routes is 110.

88.3.11 Setting the Timer of Routing Algorithm

You can set the delay between receiving the topology change information and calculating SPF. You can also set the interval between two continuous SFP algorithm. Run the following command in router configuration mode:

Command	Purpose
timers delay *delaytime*	Set a delay for routing algorithm in an area.
timers hold *holdtime*	Sets a minimum interval for routing algorithm in an area.

88.3.12 Monitoring and Maintaining OSPFv3

The network statistics information which can be displayed includes the content of the IP routing table, caching and database. This kind of information can help users to judge the usage of network resources and solve network problems.
You can run the following commands to display all kinds of routing statistics information:

Command	Purpose
show ipv6 ospf [*process-id*]	Displays the general information about the OSPFv3 routing process.
show ipv6 ospf [*process-id*] database show ipv6 ospf [*process-id*] database [router] [adv-router *router-id*] show ipv6 ospf [*process-id*] database [network] [adv-router *router-id*] show ipv6 ospf [*process-id*] database [inter-prefix] [adv-router *router-id*] show ipv6 ospf [*process-id*] database [inter-router] [adv-router *router-id*] show ipv6 ospf [*process-id*] database [external] [adv-router *router-id*] show ipv6 ospf [*process-id*] database [link] [adv-router *router-id*] show ipv6 ospf [*process-id*] database [intra-prefix] [adv-router *router-id*]	Displays the information about the OSPFv3 database.
show ipv6 ospf interface	Displays the information about the OSPFv3 interface.
show ipv6 ospf neighbor	Displays the information about OSPFv3 neighbors.
show ipv6 ospf route	Displays the routing information about OSPFv3.
show ipv6 ospf topology	Displays the OSPFv3 topology.
show ipv6 ospf virtual-links	Displays the virtual links of OSPFv3.
debug ipv6 ospf	Monitors all OSPFv3 behaviors.
debug ipv6 ospf events	Monitors the OSPFv3 events.
debug ipv6 ospf ifsm	Monitors the state machine of the OSPFv3 interface.
debug ipv6 ospf lsa	Monitors related behaviors about OSPFv3 LSA.
debug ipv6 ospf nfsm	Monitors the state machine of the OSPFv3 neighbors.

debug ipv6 ospf nsm	Monitors the information of which the management module notifies OSPFv3.
debug ipv6 ospf packet	Monitors the OSPFv3 packets.
debug ipv6 ospf route	Monitors the routing information about OSPFv3.

88.4 OSPFv3 Configuration Example

88.4.1 Example for OSPFv3 Route Learning Settings

OSPFv3 requires switching information among many internal routers, ABR and ASBR. In the minimum settings, the OSPFv3-based router works under the case that all its parameters take their default values and there is no authentication.

The following are three configuration examples:

The first example shows the commands for basic OSPFv3 settings.

The second example shows multiple OSPFv3 processes can be set on a router.

The third example shows how to use OSPFv3 to learn routes.

The fourth example shows how to set the OSPFv3 virtual link.

1. Basic OSPFv3 Configuration Example

The following example shows a simple OSPFv3 settings. In this example, you have to activate process 90, connect vlan 10 to area 0.0.0.0, and distribute OSPFv3 to RIPng.

```
ipv6 unicast-routing
!
interface vlan 10
ipv6 address 2001::1/64
ipv6 enable
ipv6 ospf 90 area 0
ipv6 ospf cost 1
!
router ospfv3 90
router-id 1.1.1.1
redistribute rip 1
!
router ripng 1
redistribute ospf 90
```

2. Configuring multiple OSPFv3 processes

The following example shows that two OSPFv3 processes are created.

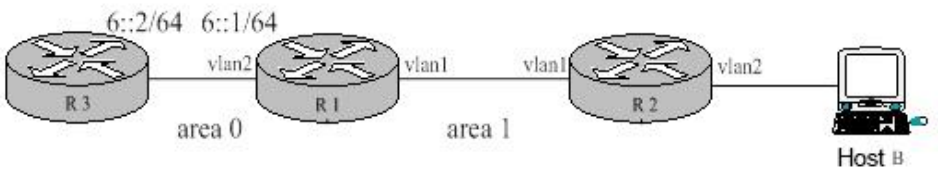
```
ipv6 unicast-routing
!
```

```
interface vlan 10
ipv6 address 2001::1/64
ipv6 enable
ipv6 ospf 109 area 0 instance 1
 ipv6 ospf 110 area 0 instance 2
!
!
interface vlan 11
ipv6 address 2002::1/64
 ipv6 enable
ipv6 ospf 109 area 1 instance 1
 ipv6 ospf 110 area 1 instance 2
!
!
router ospfv3 109
  router-id 1.1.1.1
  redistribute static
!
router ospfv3 110
  router-id 2.2.2.2
!
```

Each interface can belong to many OSPFv3 processes, but if an interface belongs to multiple OSPFv3 processes each OSPFv3 process must correspond to different instances.

3. Complicated configuration example

The following example shows how to configure multiple routers in a single OSPFv3 autonomous system. The following figure shows the network topology of the configuration example:



Configure the router according to the above-mentioned figure:

R1:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
```

```
interface vlan 2
  ipv6 enable
ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
 router-id 1.1.1.1
redistribute static
!
```

R2:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
!
router ospfv3 1
 router-id 2.2.2.2
!
```

Browsing the routing table of R2:

```
R2#show ipv6 route
O     6::/64[1]
      [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
O     2001::/64[1]  (Forwarding route )
      [110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
C     fe80::/10[1]
      is directly connected, L,Null0
C     fe80::/64[1]
      is directly connected, C, VLAN1
C     fe80::2e0:fff:fe26:a8/128[1]
      is directly connected, L, VLAN1
C     ff00::/8[1]
      is directly connected, L,Null0
```

From the command sentences above, we can see that R2 has learned route forwarding.

Setting area 1 to be the stub area:

R1:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
interface vlan 2
  ipv6 enable
ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
 router-id 1.1.1.1
 area 1 stub
redistribute static
!
```

R2:

```
interface vlan 1
  ipv6 enable
ipv6 ospf 1 area 1
!
!
router ospfv3 1
 router-id 2.2.2.2
 area 1 stub
!
```

Browsing the routing table of R2:

```
R2#show ipv6 route
O    ::/0[1]
     [110,11] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
O    6::/64[1]
     [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
C    fe80::/10[1]
     is directly connected, L,Null0
C    fe80::/64[1]
     is directly connected, C, VLAN1
```

C fe80::2e0:fff:fe26:a8/128[1]

is directly connected, L, VLAN1

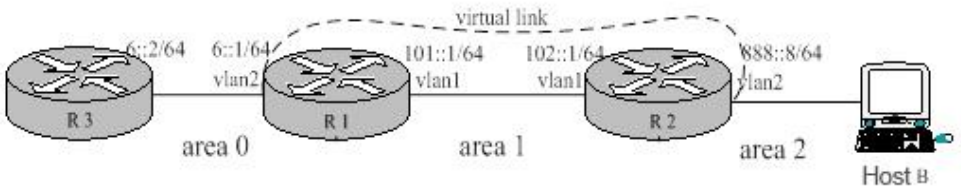
C ff00::/8[1]

is directly connected, L,Null0

It can be judged that ABR in the stub area can generate a default route normally and notify other routers in this area without importing ASE LSA into the stub area.

4. Configuring the virtual link

The following example shows how to configure a virtual link in a single autonomous OSPFv3 system. The following figure shows the network topology of the configuration example:



Configure the router according to the above-mentioned figure:

R1:

```
interface vlan 1
ipv6 address 101::1/64
  ipv6 enable
ipv6 ospf 1 area 1
!
interface vlan 2
ipv6 address 6::1/64
  ipv6 enable
ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
 router-id 200.200.200.1
 area 1 virtual-link 200.200.200.2
 redistribute static
!
```

R2:

```
interface vlan 1
```

```
ipv6 address 101::2/64
  ipv6 enable
ipv6 ospf 1 area 1
!
interface vlan 2
ipv6 address 888::8/64
  ipv6 enable
ipv6 ospf 1 area 2
!
!
router ospfv3 1
 router-id 200.200.200.2
 area 1 virtual-link 200.200.200.1
!
```

Browsing the state of the OSPFv3 neighbor:

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
200.200.200.2     1   Full/DR         00:00:35    VLAN1      0
200.200.200.2     1   Full/ -         00:00:36    VLINK1     0
```

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
200.200.200.1     1   Full/Backup     00:00:36    VLAN1      0
200.200.200.1     1   Full/ -         00:00:37    VLINK1     0
```

Browsing the information in the routing table:

```
R1#show ipv6 route
C     6::/64[1]
       is directly connected, C,VLAN2
C     6::1/128[1]
       is directly connected, L, VLAN2
C     101::/64[2]
       is directly connected, C, VLAN1
C     101::1/128[2]
```

is directly connected, L, VLAN1

O 101::2/128[2]

[110,10] via fe80:4::2e0:fff:fe26:a8(on VLAN1)

O 888::/64[2]

[110,20] via fe80:4::2e0:fff:fe26:a8(on VLAN1)

S 2001::/64[1]

[1,0] via 6::2(on VLAN2)

C fe80::/10[2]

is directly connected, L,Null0

C fe80::/64[2]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:2d98/128[2]

is directly connected, L, VLAN1

C fe80::/64[1]

is directly connected, C, VLAN2

C fe80::2e0:fff:fe26:2d99/128[1]

is directly connected, L, VLAN2

C ff00::/8[2]

is directly connected, L,Null0

R2#show ipv6 route

O 6::/64[1]

[110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C 101::/64[1]

is directly connected, C, VLAN1

O 101::1/128[1]

[110,10] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C 101::2/128[1]

is directly connected, L, VLAN1

C 888::/64[1]

is directly connected, C, VLAN2

C 888::8/128[1]

is directly connected, L, VLAN2

O 2001::/64[1]

[110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C fe80::/10[1]

is directly connected, L,Null0

C fe80::/64[1]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:a8/128[1]

is directly connected, L, VLAN1

C fe80::/64[1]

is directly connected, C, VLAN2

C fe80::2e0:fff:fe26:a9/128[1]

is directly connected, L, VLAN2

C ff00::/8[1]

is directly connected, L,Null0

Chapter 89 Overview of NTP Configuration

89.1 Stipulation

89.1.1 Format Stipulation in the Command Line

Syntax	Meaning
Bold	Stands for the keyword in the command line, which stays unchanged and must be entered without any modification. It is presented as a bold in the command line.
{italic}	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the brace.
<italic>	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the point bracket.
[ ]	Stands for the optional parameter, which is in the square bracket.
{ x | y | ... }	Means that you can choose one option from two or more options.
[x | y | ...]	Means that you can choose one option or none from two or more options.
{ x | y | ... } *	Means that you has to choose at least one option from two or more options, or even choose all options.
[x | y | ...] *	Means that you can choose multiple options or none from two or more options.
&<1-n>	Means that the parameter before the “&” symbol can be entered 1~n times.
#	Means that the line starting with the “#” symbol is an explanation line.

Chapter 90 NTP Configuration

90.1 Overview

Network Time Protocol (NTP) is a type of computer time synchronization protocol which can be used for time synchronization between distributed time servers and clients. It has highly accurate time correction function and can prevent malicious protocol attacks through encrypted authentication. Clients and servers communicate through the User Datagram Protocol (UDP), and the port number is 123.

90.2 NTP Configuration

90.2.1 Configuring the Equipment As an NTP Server

Configuration mode: Global

Command	Purpose
ntp master primary	In the event that the equipment does not have an upper-level NTP server, configure the equipment as the original NTP server (stratum = 1).
ntp master secondary	In the event that the equipment has an upper-level NTP server, configure the equipment as the secondary NTP server. (In other words, the equipment cannot provide time synchronization service for NTP clients unless the "ntp server" command is configured and time synchronization is achieved in designated servers.)

90.2.2 Configuring NTP Authentication Function

Configuration mode: Global

Command	Purpose
ntp authentication enable	Enable the authentication function (disabled by default).
ntp authentication key *keyid* md5 *password*	Configure NTP md5 authentication keyid and corresponding keys.
ntp authentication trusted-key *keyid*	Configure the keyid corresponding key as the trusted key.

90.2.3 Configuring NTP Association

Configuration mode: Global

Command	Purpose
ntp server *ip-address* [version *number*| key *keyid*]*	Configure the IP address of NTP server; the version number, key number.
ntp peer *ip-address* [version *number*| key *keyid*]*	Configure the IP address of equipment NTP peer; the version number, key number.

Usage Guidelines:

1. Equipment can provide time services for NTP clients provided that the equipment has achieved time synchronization; otherwise the client device that employs the equipment as its server cannot achieve time synchronization.
2. To conduct NTP authentication, both parties must open the NTP authentication function simultaneously, configure the same keyid and key, and designate the keyid as trusted; otherwise time synchronization would fail.

90.2.4 Configuring time zone

Configuration mode: Global

Command	Purpose
time-zone *name offset-hour* [*offset-minute*]	To configure the time zone, needs to manually add the offset time
no time-zone	Restore timezone to default: UTC

Usage Guidelines:

The time zone setting does not affect the clock synchronization of ntp, but only affects the display. The ntp synchronization time is calculated based on the UTC timestamp.

90.2.5 Configuring Summer Time

Configuration mode: Global

Command	Purpose
summer-time *name* absolute|periodical date|week start *start-time* end *end-time [offset]*	Configure and enable summer time
no summer-time	Disable summer time function

Usage Guidelines:

1. There are two types of types for summer time: absolute and periodic. absolute is to specify the specific year, month, day, and hour of summer time start and end. periodic is to specify the start and end time of summer time in the xth week of x month x, hh:mm time format, and repeat every year.

Chapter 91 IPv6 ACL Configuration

91.1 IPv6 ACL Configuration

91.1.1 Filtering IPv6 Packets

Filtering IPv6 packets helps the control packet run in the network. Such control can limit network transmission and network running by a certain user or device. For enabling or disabling packets from the cross designated port, we provide with ACL. You can use IPv6 ACL as follows:

- Limit of packet transmission on the port
- Limit of virtual terminal line access
- Limit of the route update

This chapter summarizes how to set up IPv6 ACL and how to apply them.

IPv6 ACL is a well-organized set which applies enable/disable of IPv6 address. ROS of the switch will test addresses in ACL accordingly. The first match determines whether the software accept or refuse the address. Because after the first match, the software will stop the match rule, the sequence of the condition is important. If there is no rule to match, the address will be refused.

Steps for using ACL:

(1) Set up ACL by designating ACL name and ACL conditions.

(2) Apply ACL to the port.

91.1.2 Setting up IPv6 ACL

Use a character string to set up IPv6 ACL.

NOTE:

The standard ACL and the expanded ACL cannot be the same.

In order to set up IPv6 ACL, run the following command in the global configuration mode.

Command	Purpose
IPv6 access-list *name*	Use the name to define an IPv6 ACL.
{**deny** | **permit**} protocol {source-ipv6-prefix/prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | **any** | **host** destination-ipv6-address} [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** value] [**time-range** name]	In the configuration mode of IPv6 ACL, designate one or multiple enable/disable conditions. This determines whether to pass the packet or not. (dscp is used for matching IPv6 grouping header Traffic Class domain, flow-label is used for matching Flow Label tag domain of IPv6 grouping header, fragments is used for matching fragment grouping when the grouping expansion header includes none-0 offset; log means whether to record log, routing is used for the source grouping of the route expansion header of IPv6 grouping header, time-range is used for limit the time range of ACL.)
Exit	Exit from the configuration mode of ACL.

After setting up ACL, any additional parts will be affiliated to the end of the ACL if no sequence is added to the rule deny or permit. In other words, add [**sequence** value] in the front or back of the rule deny/permit, you can add ACL commands in any position of the designated ACL.

Likewise, you can use "no permit" and "no deny" to delete an item in ACL or "no sequence" to delete the rule in a certain position directly.

NOTE:

When setting up ACL, please remember the end sentence of ACL by default covers the sentence of **deny ipv6 any any.**

The ACL must be applied to the line or port after being set up. Refer to the description of "Apply the ACL to the port".

91.1.3 Applying ACL to the Ports

ACL can be applied to one or multiple ports or the ingress.

Run this command in the configuration mode.

Command	Purpose
IPv6 access-group *name*	Apply ACL to the port.

For the standard ingress ACL, check the source address of the packet after receiving it. For the expanded ACL, the routing switch also checks the objective address. If the ACL enables the address, the software continues to handle the packet. If ACL does not allow the address, the software will drop the packet and returns one ICMP host unreachable packets.

If there is no designated ACL, all packets will be allowed to pass.

91.1.4 Examples of IPv6 ACL

In the following example, please first enable to connect with the individual destination host of the host A:B:C:D::E and disable the new TCP to connect with SMTP port whose host IPv6 source prefix 255:255:255::/48. The next rule sequence of the final ACL comes before the former rule.

```
Switch_config#ipv6 access-list  xxcom
Switch_config_ipv6acl#permit any host A:B:C:D::E sequence 20
Switch_config_ipv6acl#deny tcp any 255:255:255::/48 eq 25 sequence 10
Switch_config_ipv6acl#ex
Switch_config#show ipv6 access-lists xxcom
ipv6 access-list xxcom
  deny tcp any 255:255:255::/48 eq smtp sequence 10
  permit ipv6 any host A:B:C:D::E sequence 20
```

Chapter 92 IP-Attack Prevention Configuration

92.1 Overview

To ensure the reasonable use of network bandwidth, the company's switches provide the IP-Attack Prevention function to prevent malicious IP traffic from occupying the network bandwidth. For the common attacks at present, communication restrictions are imposed on hosts that send a large number of ICMP, IGMP or IP packets over a period of time, and no network services are provided to these hosts. This configuration can prevent the problem of network congestion caused by malicious packets occupying a large amount of network bandwidth.

92.2 IP-Attack Prevention Configuration Task List

When the number of IGMP, ICMP, or IP packets sent by a host within any specified time interval exceeds the threshold, we assume that an attack occurs on the network.

You can choose the anti-attack types (ICMP, IGMP or IP), the application ports and attack detection parameters. The configuration tasks inlclude:

- Configure IP-Attack Prevention type
- Configure IP attack detection parameters

92.3 IP-Attack Prevention Configuration

92.3.1 Configuring IP attack detection parameters

Command	Purpose
ip verify log-enable	Enable/disable attack detection system log
ip verify filter *time*	When the attack source is identified, stop service for them. The adjustment unit is seconds, the default time is 180 seconds

92.3.2 Configuring the IP attack detection type

Command	Purpose
ip verify icmp ping-flood *value*	Limit ping packet reception. **value** means the detection threshold.
ip verify icmp ping-sweep *time*	Limit ping scanning. **time** means detection period, unit is second.
ip verify tcp syn-flood *value*	Restrict tcp syn packet reception. **value** means the detection threshold.
ip verify tcp syn-sweep *time*	Limit tcp syn port scanning. **time** means detection period, unit is second.
ip verify tcp fin-scan *time*	Limit tcp stealth fin scanning. **time** means detection period, unit is second.

ip verify tcp rst-flood *value*	Limit tcp rst packet reception. **value** means the detection threshold.
ip verify udp udp-flood *value*	Limit udp packet reception. **value** means the detection threshold.
ip verify udp udp-sweep *time*	Limit udp scanning. **time** means detection period, unit is second.
ip verify attack Xmas-Tree *time*	Filter Xmas-Tree scanning attacks. **time** means detection period, unit is second.
ip verify attack Null-scan *time*	Filter Null scanning attacks. **time** means detection period, unit is second.
ip verify attack Land	Filter Land attacks.
ip verify attack Smurf	Filter Smurf attacks.
ip verify attack WinNuke	Filter WinNuke attacks.
ip verify attack TearDrop	Filter TearDrop attacks.
ip verify attack Fraggle	Filter Fraggle attacks.

92.3.3 Enabling IP-Attack Prevention function

When all the parameters for anti-attack are configured, the anti-attack function can be activated. It should be noted that the attack prevention function takes up a small amount of processor space.

Command	Purpose
ip verify enable	Enable/disable attack detection.

With no form of this command is used, the attack detection is disabled, and all blocked attack sources are unblocked.

92.4 Examples of IP-Attack Prevention Configuration

To enable the port scanning anti-attack, you can configure as follows. When any host scans the port more than one scanning unit in any 15 seconds, it is considered as an attack and block network service for 10 minutes.

ip verify icmp ping-sweep 15

ip verify tcp syn-sweep 15

ip verify udp udp-sweep 15

ip verify enable

ip verify log-enable

ip verify filter 600

Chapter 93 IP Attacks Prevention against Direct Network Segment Scanning

93.1 Overview

To prevent malicious attacks from sending a large number of scan packets to the directly connected route, the switch creates a software cache for unreachable addresses of the directly connected route to increase CPU utilization. The function of IP attacks prevention against direct network segment scanning can deal with attacks to reduce the CPU utilization.

93.2 Configuration task list of IP Attacks Prevention against Direct Network Segment Scanning

When the number of incomplete arps on a switch vlan exceeds a certain number, we think the switch has received an attack from direct network segment scanning.

When the number of unreachable IP packets within any specified time interval exceeds the threshold, we assume that an attack occurs, then record and print to prompt the user.

The user can select the function mode and attack detection parameters of the anti-direct network segment scanning attack. The configuration tasks include:

- Configure detection parameters of IP attacks prevention against direct network segment scanning
- Configure detection types of IP anti-direct network segment scanning detection types

NOTE:

The ip verify ip-sweep action rate-limit-attacker command will override the ip verify ip-sweep action rate-limit command, otherwise you need to configure no ip verify ip-sweep action rate-limit-attacker first to configure ip verify ip- sweep action rate-limit. Time and packet parameters are inherited when overwriting.

93.3 Configuring IP Attacks Prevention against Direct Network Segment Scanning

93.3.1 Configuring detection parameters of IP attacks prevention against direct network segment scanning

Command	Purpose
ip verify filter *time*	When the attack source is identified, stop service for the attack source. The adjustment unit is seconds, the default time is 180 seconds.

93.3.2 Configure detection types of IP anti-direct network segment scanning detection types

Command	Purpose
ip verify ip-sweep action rate-limit	Limit the number of IP packets
ip verify ip-sweep action rate-limit *time packets*	Limit the number of ip packets, configure the limited time period and the maximum number of ip packets allowed in this period.
ip verify ip-sweep action rate-limit-attacker	Only limit the number of packets defined as attacker's ip packets.
ip verify ip-sweep action rate-limit-attacker *time packets*	Limit the number of packets defined as attacker's ip packets. Configure the limited time period and the

	maximum number of ip packets allowed for the source address in the period.
ip verify ip-sweep action no-cache	Prohibit the creation of cache for unknown hosts directly connected to the network segment.

93.3.3 Enable IP Attacks Prevention against Direct Network Segment Scanning

When all the parameters are configured, you can enable the IP attacks prevention against direct network segment scanning. It should be noted that the attack prevention function takes up a small amount of processor space.

Command	Purpose
ip verify ip-sweep detect unknown-host	Enable/disable the anti-attack function for IP scanning of unknown hosts on the directly connected network.

With no form of this command is used, the attack detection is disabled, and all blocked attack sources are unblocked.

93.4 Examples of IP Attacks Prevention against Direct Network Segment Scanning

To enable the IP attacks prevention against direct network segment scanning, you can configure as follows. That is, the detected attacker is only allowed to forward 200 IP packets every two seconds and the cache of unknown direct network segment hosts is prevented. In addition, the entire test result is reset every 10 minutes,

ip verify filter 600

ip verify ip-sweep detect unknown-host

ip verify ip-sweep action no-cache

ip verify ip-sweep action rate-limit 2 200

93.5 Detection Results of IP Attacks Prevention against Direct Network Segment Scanning

Jan 1 00:07:14 Unknown-host (connected network sweep) attack detected

Jan 1 00:07:14 Action rate-limit-attacker is being used.

Jan 1 00:07:14 Action no-cache is being used.

Jan 1 00:07:14 Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

Jan 1 00:07:14 [SLOT 2]Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

When the anti-direct network segment scanning attack and rate-limit-attacker and action no-cache defense methods are enabled, an attacker's IP network segment scanning attack with port vlan 100, physical port g2/1, and IP address 100.1.1.2 is received, please deal with it as soon as possible.

Chapter 94 Configuring Time Range

94.1 Time Range Introduction

94.1.1 Overview

Time Range is a time module controlling the effective time and the failure time of a function (For instance, expansion IP access control list).

Time Range can play its role only when cooperating with other modules which support the Time Range function.

Time Range is consisted of separate time ranges. These time ranges have two kinds: one is absolute and the other is periodic. Of these, periodic is classified into two kinds further: isolate and from-to.

The whole system has many Time Ranges. Each Time Range is differentiated according to their names (case sensitive). Each Time Range has at most only one absolute time range but many periodic time ranges.

94.1.2 Absolute Time Range

Absolute Time Range is a time range starting and ending with concrete date and time (The Absolute Time Range without concrete starting date and time is taken as the current time; the absolute time range without concrete ending time is taken as effective forever.). For example, 08:08 8 8 2008 - 10:10 10 10 2010 is an absolute time range.

94.1.3 Periodic Time Range

Periodic Time Range is a back-and-forth time range. It has no concrete starting time and ending time, but it has concrete starting week and moment and ending date and moment. For example, a periodic time range starts from 20:00~21:00 on every Tuesday, Thursday and Sunday; or starts from 09:00 on every Tuesday to 18:00 on every Thursday. More examples such as 09:00~10:00 in every weekend; 23:00~07:00 everyday; and 09:00~18:00 on weekdays.

94.1.4 Isolating Time Range

Isolate Time Range is one type of Periodic Time Range. It is periodical. And its starting time and ending time will not span 24 hours. For example,19:00~19:30 on every Monday is an isolate time range; 20:00~21:00 on every Tuesday, Thursday and Sunday is an isolate time range; but time from 09:00 on Tuesday to 18:00 on every Thursday is not an isolate time range, but "from-to time range" described below.

94.1.5 From-to Time Range

From-to Time Range is also a type of Periodic Time Range. It is periodical. Moreover, its starting time and ending time must span at least 24 hours. For example, time from 09:00 on Tuesday to 18:00 on every Thursday is a from-to time range.

94.1.6 Activating Time Range

A Time Range can have the absolute time range and periodic time range simultaneously. The state of Time Range can be divided into 4 situations according to whether the absolute time range/periodic time range is configured.

Situation 1:

If a Time Range neither configure absolute time range nor periodic time range, it is called EMPTY. The Time Range does not exist activating time range.

Situation 2:

If a Time Range doesn't have the absolute time but has periodic time range, the activating time range of the Time Range is the total time ranges of the periodic time range.

Situation 3:

If a Time Range doesn't have the periodic time but has absolute time range, the activating time range of the Time Range is the total time ranges of the absolute time range.

Situation 4:

If a Time Range neither have the periodic time nor the absolute time range, the activating time range of the Time Range is set intersection of the set union of the absolute time range and all periodic time range.

The complementary set of the activating time range of a Time Range is considered as non-activating time range.

If the system time is in an activating time range of a Time Range, the Time Range is active; if a Time Range has the activating time range but the system time does not in the activating range, the time range is inactive; if a Time Range does not have the activating time range, the Time Range is empty.

When a Time Range changes among inactive, active and empty, the Time Range is changed. Otherwise, the Time Range is unchanged.

94.2 Time Range Configuration Task List

- Adding/Deleting Time Range
- Adding/Deleting Absolute Time Range
- Adding/Deleting Periodic Time Range
- Applying Time Range
- Monitoring the configuration and state of Time Range

94.3 Time Range Configuration Task

94.3.1 Adding/Deleting Time Range

The whole system has many Time Ranges. Each Time Range is differentiated according to their names (case sensitive).

Run the following commands to configure Time Range:

Command	Purpose
time-range *name*	Add a Time Range named name and enter the configuration mode of Time Range
exit	Exit the configuration mode of Time Range
no time-range *name*	Delete Time Range named name

NOTE: If the system has Time Range named name, *run command* time-range name to enter the **TimeRange** *configuration mode,* but not create the new TimeRange.

94.3.2 Adding/Deleting Absolute Time Range

Each TimeRange has only at most only one absolute time range. Absolute Time Range can have the starting time and the ending time simultaneously or it has the ending time but not the starting time, or it has the starting time but not the ending time. When the absolute time has no starting time, the current time is the starting time; when the absolute time

has no ending time, the absolute time is effective forever.

To configure the absolute time range, run the following command:

Command	Purpose
absolute {start hour:minute day month year **end** hour:minute day month year**| start** hour:minute day month year**| end** hour:minute day month year**}**	Adds an absolute time range
no absolute	Deletes the absolute time range

NOTE: If a Time Range has the absolute time range, the absolute command modifies the absolute time range.

94.3.3 Adding/Deleting Periodic Time Range

A Time Range can has many periodic time ranges. Each periodic time range is not all the same, but the time range can overlap.

To configure the periodic time, run the following command:

Command	Purpose
periodic {daily *hour:minute* to *hour:minute* | weekdays *hour:minute* to *hour:minute* | weekend *hour:minute* to *hour:minute* | {Friday | Monday | Saturday | Sunday | Thursday |Tuesday|Wednesday} *hour:minute* to *hour:minute* | {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday} *hour:minute* to {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday} *hour:minute* }	Adds a periodic time range
no periodic [daily *hour:minute* to *hour:minute* | weekdays *hour:minute* to *hour:minute* | weekend *hour:minute* to *hour:minute* | {Friday | Monday | Saturday | Sunday | Thursday |Tuesday|Wednesday} *hour:minute* to *hour:minute* | {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday} *hour:minute* to {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday} *hour:minute*]	Deletes a periodic time range

94.3.4 Applying Time Range

A created Time Range can be applied to one or more function modules. At present the Time Range can only be applied to IP ACL function module.

In order to apply Time Range to IP ACL, you must enter the name of Time Range to the end of the sub-command of time-range.

NOTE: Time Range can only be applied to extensible ACL, but not to the standard ACL.

94.3.5 Monitoring the configuration and state of Time Range

To monitor Time Range Configuration, run the following command:

Command	Purpose
show time-range	Shows the configuration of all Time Range in the system

show time-range *name*	Shows the configuration *of* Time Range named name.

Attach: The result analysis of the command

Take the result of the typical configuration as an example:

```
Switch_config#show time-range

Now: Date: 2008.3.4    Time: 13:16    Week: Tuesday

time-range entry: x (inactive)
absolute start 12:00 1 January 2000 end 13:00 2 January 2008
periodic weekdays  09:00 to 18:00
time-range entry: y (empty)
time-range entry: z (active)
periodic daily    12:00 to 13:00
periodic Monday    Thursday  Friday    08:00 to 09:00
periodic Saturday  15:00 to Sunday    20:00
periodic daily    09:00 to 18:00

Switch_config#
```

In the first line shows “Now: Date: 2016.3.4 Time: 13:16 Day: Tuesday”, which means the date is 4th March, 2016; the time is 13:16; the day is Tuesday.

Subsequently the screen shows the configuration and status of Time Ranges which named x, y and z respectively. Time Range x has two items: absolute time and period, and it is in the inactive state; Time Range y has no item and it is in the empty state; Time Range z has 4 periods and it is in active state.

94.4 Configuration Example

The following example shows how to apply a Time Range named sample to a rule of extensible IP ACL ex.

```
Switch_config#
Switch_config#time-range sample
Switch_config_time_range_sample#periodic monday 12:00 to 13:00
Switch_config_time_range_sample#exit
Switch_config#ip access-list extended ex
Switch_config_ext_nacl#
Switch_config_ext_nacl#permit ip 192.168.213.180 255.255.255.255 any time-range sample
Switch_config_ext_nacl#exit
Switch_config#
```

Chapter 95 uRPF Configuration

95.1 Overview of uRPF

95.1.1 uRPF (Unicast Reverse Path Forwarding)

uRPF (Unicast reverse path forwarding) is a mechanism for allowing devices to check if the source address is in the local routing table before forwarding it. This is useful to check for source address spoofing and protecting against DOS attacks. There are two modes of uRPF strict and loose mode. Strict mode checks that the source address has a routing table entry and that the egress interface for the route is the same as the interface the packet was received on. Loose mode only checks that a route is in the table before forwarding the packet.

95.2 uRPF Configuration

95.2.1 Enabling uRPF in the Global Configuration Mode

To use uRPF, enable uRPF in the global configuration mode:

Command	Purpose
[no] urpf check	Enable/disable uRPF check in the global configuration mode

95.2.2 Configuring uRPF Check Mode on the VLAN Interface

Configure uRPF check mode on the VLAN interface (strict mode or loose mode). In the strict mode, the source address of the packet will be used not only to check whether FIB table is reachable, but also to check whether the ingress port of the packet is consistent with the next hop interface. In the loose mode, the source address of the packet will only be used to check whether it is reachable in FIB table.

After configuring uRPF,the filter of the route is also supported. When the default route is configured and uRPF check the source address based on FIB table, all source addresses can find the matched item.By default, if the finding of uRPF check FIB is the default route, it will be taken as no entry found and the packets will be dropped.

NOTE: Enable urpf check in the global configuration mode and uRPF takes effect.

Configure uRPF mode in the VLAN interface and run the command in the interface configuration mode:

Command	Purpose
[no] urpf check strict/loose [uncheck-default-route]	Configure uRPF check mode in the VLAN interface. uncheck-default-route is disabled by default.

NOTE:

Enable **uncheck-default-route**. If the packet source address can check the matched item in the FIB table, the matched item whether it is the default route or not will be taken as pass and the packet will not be dropped. By default (uncheck-default-route is disabled), the packet source address finds the matched item in FIB table and if the matched item is taken as the default route, thus uRPF is failed and the packet will be dropped.

Chapter 96 Cable Diagnostic Configuration

96.1 Enable the Ethernet interface cable diagnostic

To enable cable diagnostic under interface mode, use the following command.

Command	Purpose
cable-diagnostic {**period** | <**cr**>} (TX port)	Set the period of the port cable check. If it is 0, it will be checked only once.
No cable-diagnostic	Restore the default setting without checking the port cable.

NOTE:

The diagnostic results cannot guarantee the accuracy of the cables produced by all manufacturers. The test results are for reference only.

This command may affect the normal use of the interface's services in a short time. After the execution, you can view the test result with the **show interface** command:

Examples are as follows:

show interface g0/4

.....

Cable Ok (4 pairs)

Pair A Ok, length < 1 metres

Pair B Ok, length < 1 metres

Pair C Ok, length < 1 metres

Pair D Ok, length < 1 metres

.....

Cable status:

l OK: indicates that the wire pair ends normally.

l Open: indicates that the wire pair is open.

l Short: indicates that the wire pair is short circuited.

l Crosstalk (crosstalk): indicates that there is crosstalk between the wire pairs (interference with each other).

l Unknown: Other causes of failure.

Chapter 97 Optical Port Additional Function Configuration

97.1 Enable Optical Port DDM Function

To enable ddm in the global configuration mode, use the following command.

Command	Purpose
ddm {enable}	Enable DDM check function for all optical ports.
No ddm	Disable DDM check function for all optical ports.

After the DDM check function is enabled, the DDM information of the optical module can be displayed through **show interface xxxx**. If the optical module is not inserted, the DDM information will not be displayed.

Note: After enabling, the CPU usage may increase slightly according to the hardware designs. The inspection information includes the specifications, wavelength, manufacturer information, serial number, production date, etc. If the optical module supports the **Digital diagnostic monitoring** function, the receiving optical power, voltage, bias current, temperature and related threshold information will also be displayed.

Examples are as follows:

Ddm enable

show int g0/25

.....

Transceiver Info:

SFP,LC,850nm,10000BASE-FX-SR,LOS:yes

MM 80M(50um OM2 fiber) 30M(62.5um OM1 fiber) 300M(50um OM3 fiber)

DDM:YES,Vend:FINISAR,PN:FTLX8571D3BCL-HW

SerialNum:AQN03Y5,Date:2018-04-04

DDM info:

TX power:-9.40 dBm, RX power:-36.99 dBm

SFP temperature:21.00 C,supply voltage :3.40V,Bias Current.:5.00mA

DDM Thresholds:	Low-Alarm	Low-Warning	High-Warning	High-Alarm
TX power(dBm):	-6.00	-5.00	0.50	1.50
RX power(dBm):	-13.00	-12.50	0.50	1.50
SFP temperature(C):	-10	0	75	85
Supply voltage(v):	3.00	3.10	3.50	3.60
Bias Current(mA):	1.00	1.00	100.00	110.00

97.2 Optical Port Single-fiber Transceiver Function

To enable optical port single-fiber transceiver function, use the following command:

Command	Purpose
single-fiber one-way {tx|rx}	Enable the port single-fiber (send or receive) function.
No single-fiber	Disable the port single-fiber transceiver function.

After this function is enabled, the port is in LINK UP state immediately. You can insert the optical fiber in the TX direction or RX direction of the optical module according to the configured function. Data will only flow in one direction.

97.3 Optical Port Adaptive Optical Module Function

Command	Purpose
fiber-auto-config {full}	Enable optical port adaptive optical module function configuration. With the parameter full, the device is switched to enforcement mode.
No fiber-auto-config	Disable the port single-fiber transceiver function.

After this function is enabled, the port will switch the working mode to match with the type of the inserted optical module. For example, the 10 Gigabit optical port inserted inserted with a Gigabit optical module will switch to the Gigabit optical mode, and the Gigabit optical port inserted with a 100M optical module will switch to the 100M optical mode.

Note:

10 Gigabit port has only one working mode and Gigabit port has two modes: auto-adaptive and enforcement. Therefore, the 10 Gigabit optical port inserted inserted with a Gigabit optical module will switch to the Gigabit adaptive mode by default. To switch to the Gigabit enforcement mode, you need to add the parameter **full** after this command. 100M port only has one working mode, so the Full parameter is no need. If the optical to electrical module is used, you must configure this **full** parameter to work properly.

Chapter 98 Power over Ethernet

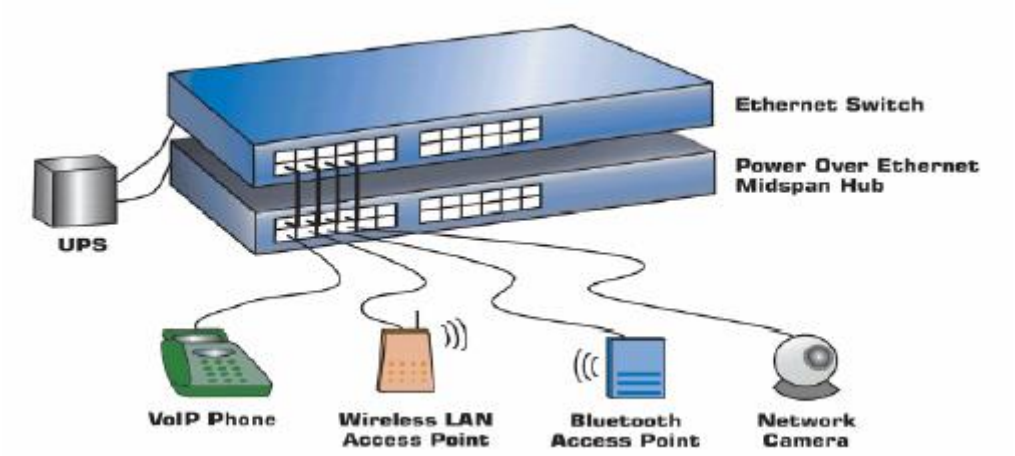
98.1 POE Overview

PoE, called Power over Ethernet, refers that power is supplied through the 10BASE-T, 100BASE-TX and 1000BASE-T Ethernet, and its reliable power supply reaches up to 100 meters at maximum. In this way, the centralized power supply problem of the IP phone, wireless AP, portable device charger, POS machine, camera and data collection and other terminals can be effectively solved. For these terminals, there is no need to consider the problem of indoor power system wiring; the device is supplied with power while access to the network. In terms of universality, the current PoE power supply has also a unified standard; as long as 802.3af Standard which has been released is followed, the problem of adaptability between the devices from different manufacturers can be solved.

98.1.1 Introduction to POE Power Supply

According to the definition of the 802.3af Standard, PoE power supply system involves two kinds of device: PSE and PD. PSE (power-sourcing equipment), is primarily used to supply power to other devices, which can be divided into two kinds: Midspan (PoE functions are out of the switch) and Endpoint (PoE functions are integrated into the switch).

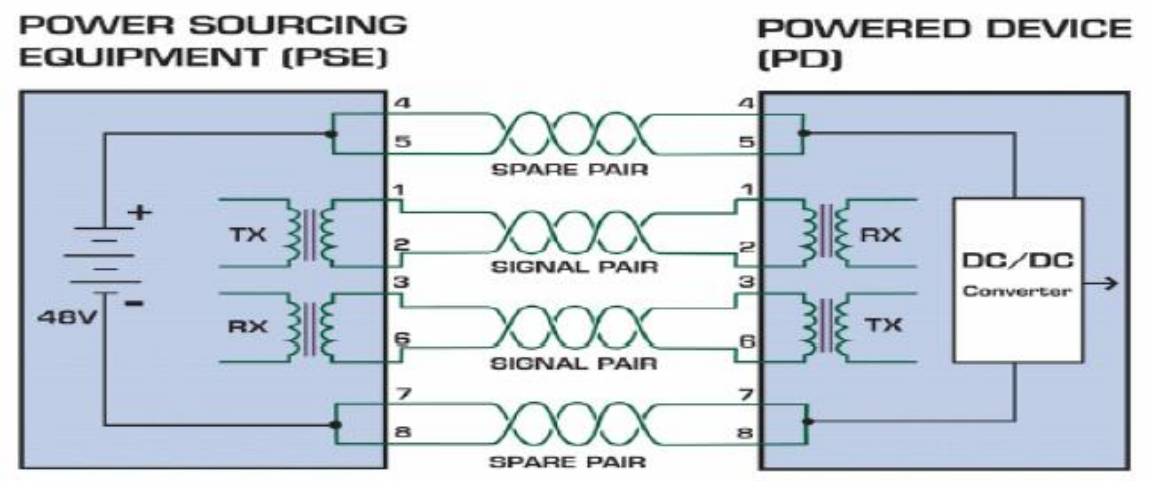
For the PoE-powered devices, their power supply systems are all integrated inside the device, which are the PSE device belonging to Endpoint. Meanwhile, the PD is defined as follows: PD (Powered Device) is the device which is used to receive power in the PoE power supply system, mainly referring to some wireless AP devices or some IP PHONE devices as well as some low power SOHO switches. Its typical networking diagram is as follows:



Meanwhile, 802.3af Standard also defines the PI (Power Interface: The interface between PSE/PD and network cable). At present, two power supply modes: Alternative A (Signal line No. 1, 2, 3, 6) and Alternative B (Free line 4, 5, 7, 8), have been defined, which are described as follows:

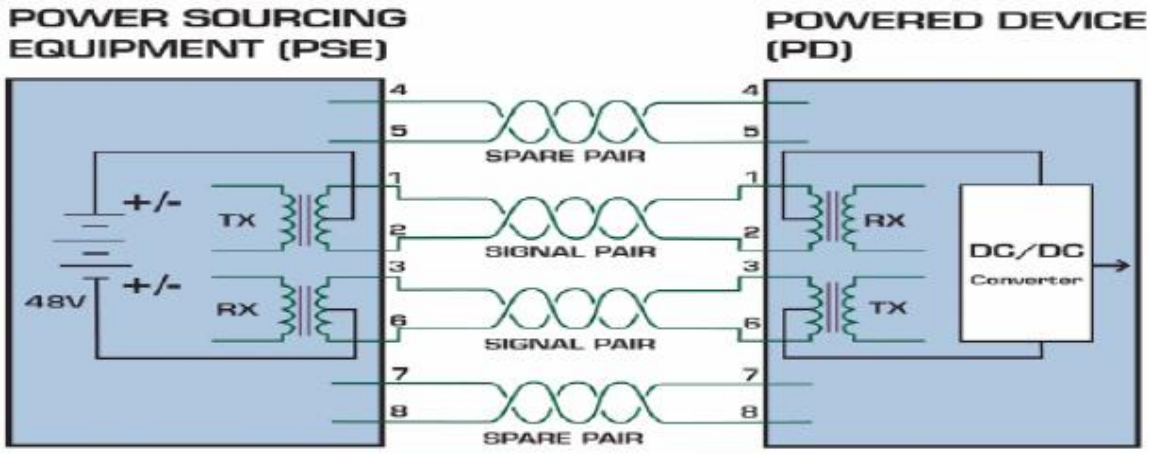
1) Supply the power through the idle pairs - Mode B (Alternative B)

As is shown below, Link 4 and Link 5 form a positive electrode; Link 7 and Link 8 form a negative electrode. PD is powered by PSE.



2) Supply the power through the data pair - Mode A (Alternative A)

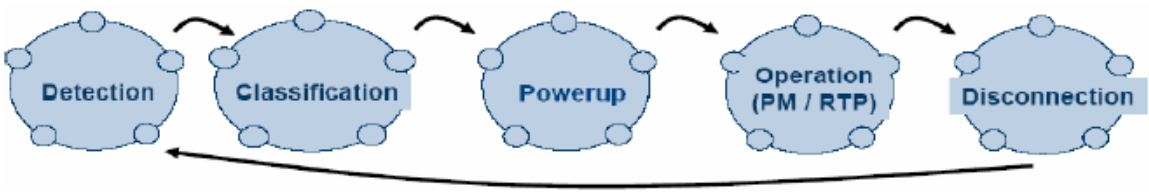
As is shown below, PSE can supply the power to the PD through the data pair. As the DC and the data frequency don't interfere with each other, both the current and data are transmitted through the same pair of lines at the same time. In fact, for the cable, it can be seen as a kind of "reuse". Link 1 and Link 2 can form a positive (or negative) electrode; Link 3 and Link 6 form a negative (or positive) electrode.



In general, the standard PD must support two kinds of ways of receiving power, but the PSE device only needs to support one of them; all products in our Company only support the power supply through the signal lines as PSE switch.

98.1.2 Power-Up Procedure of PoE

For PD, the flow of acquiring the power supply is as follows when accessing PSE system:



In the above process, the following steps are mainly described:

1) Detection: PSE detects whether the PD exists.

This step is mainly described as follows: PSE judges the existence of PD through detecting the RC value between the power

supply output wire pairs. In the detection phase, the output voltage is 2.8V~10V, and the voltage polarity is consistent with -48V output. Only when PD is detected, PSE will continue to do the next step.

Features of PD existence: a. The DC Resistance is between 19Kohm and 26.5Kohm; b. The capacitance does not exceed 150nF;

2) Classification (optional): PSE determine PD power consumption.

PSE determines the PD power level through detecting the power output current. In the classification phase, the port output voltage is between 15.5V and 20.5V. The voltage polarity is consistent with -48V output.

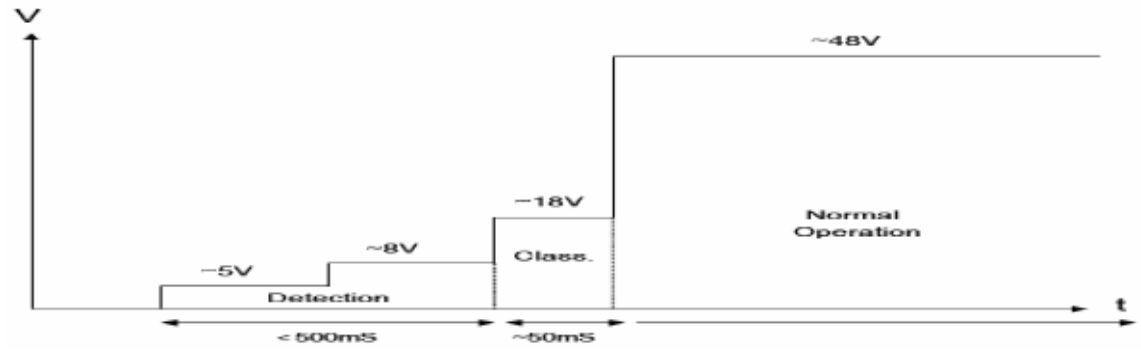
3) Powerup: PSE supplies the power to the PD.

When detecting that the device under the port is the legal PD device and PSE completes the classification of this PD (optional), PSE begins to supply power to this device, whose output voltage is -48V.

4) RTP & Power management: Real-time monitoring; power management.

5) Disconnection

PSE detects whether the PD disconnects — PSE uses a specific method to detect the disconnection of PD. If the PD is disconnected, PSE will close the port to output voltage. The port status returns to "Detection". For PSE power supply system, its ideal output waveform is shown in the figure below:



98.2 POE Configuration Task List

- Displaying the configuration
- Configuring port's power supply enabling
- Configuring the maximum power of the port
- Configuring the power supply priority
- Configuring the port description, usually describing the PD
- Configuring the forced power supply function of the port
- Configure high inrush of the port
- Configure the extra power of the device
- Configure the hot restart function
- Configuring the PSE detection method

98.3 POE Configuration Tasks

98.3.1 Displaying the information about POE-related systems.

The global and port information of the POE module can be observed through the display command.

Use the following display commands in the management mode:

Show poe system	Display the POE-related system information
Show poe all	Display POE port information description table
Show poe power	Display all the port power supply information
Show poe interface *type slot/port*	Display the detailed POE information of the specified port

98.3.2 Enabling the Power Supply of a Port

Provide two ways to control the port's power supply enabling: 1. directly enabling and disabling the port; 2. supplying power based on the time range.

Method 1:

By default, the port's power supply is enabled; in the port configuration mode, use the following commands to prohibit the port enabling:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**poe disable**	Prohibit the port's power supply enabling

Restore the default setting; enable the port's power supply enabling:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**no poe disable**	Enable the port's power supply

Method 2:

By default, there is no control over the port's power supply enabling based on time range; in the port configuration mode, use the following commands to configure the port's power supply enabling based on time range:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**poe disable time-range** *name*	Configure the control over the port's power supply enabling with the *name* "disable the port's power supply based on time range"

Restore the default setting; remove the control over the port's power supply enabling based on time range:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**no poe disable time-range**	Cancel the control over the port's power supply enabling based on time range"

98.3.3 Setting the Maximum Power of a Port

The default maximum power of a port is 30000mW and you can set the maximum power of this port by running this command in interface configuration mode:

Step	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	**poe max-power** *value*	Sets the maximum power of a port, whose unit is mW.

Resume the default settings by running the following commands:

Step	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	**no poe max-power**	The default maximum power of a port is 30000mW.

98.3.4 Setting the Power Supply Priority for a Port

The default power supply priority of a port is low and you can set the maximum power of this port by running this command in interface configuration mode:

Step	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	**poe priority** {critical | high | low }	Sets the power supply priority of a port to **critical**, **high** or **low**. Hardware support is required.

98.3.5 Configuring the Port Description (usually for PD)

By default, the port description is empty; in the port configuration mode, use the following commands to configure:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**poe PD-discription** *string*	Configure the port description

Restore the default setting:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**no poe PD-discription**	Remove the description string

98.3.6 Configuring the Forced Power Supply

By default, disable the force power supply; in the port configuration mode, use the following commands to configure:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**poe force-power**	Enable the port's force power supply. Hardware support is required.

Restore the default setting, and disable the port's force power supply:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**no poe force-power**	Disable the port's force power supply

98.3.7 Configuring port high inrush power-on function

By default, disable the high-current power-on; in the port configuration mode, use the following commands to configure:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode

Step3	**poe inrush high**	Enable port high-current power-on function. Hardware support is required.

Restore the default setting, and disable the high-current power-on:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**interface** intf-type intf-id	Enter the port configuration mode
Step3	**no poe inrush**	Disable the high-current power-on

98.3.8 Configuring the extra power of the device

By default, the extra power is 0. In the global configuration mode, use the following command to configure:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**poe extern-power 300**	The power of the device is increased by 300W, hardware support is required

Restore the default setting, and restore the original power:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**no poe extern-power**	Restore the original power

98.3.9 Configuring the hot restart function

By default, the hot restart is disabled. Use the following command in the global configuration mode to configure:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**poe perpetual**	Enable hot restart, hardware support is required

Restore the default settings and restore the original power function:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode

Step2	**no poe perpetual**	Disable the hot restart function

98.3.10 Configuring power supply detection mode

By default, resistance detection is enabled. Use the following command in the global configuration mode to configure:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**poe detection RES-CAP**	Set capacitance detection, hardware support is required

Restore default settings, resistance detection:

Step	Command	Purpose
Step1	**config**	Enter the global configuration mode
Step2	**poe detection RES**	Restore to resistance detection

Chapter 99 Configuring Virtualization

This chapter describes how to create and configure virtualization for your switch.

99.1 Overview

Virtualization is a technology for centralized management of the interface expansion. The user can enable virtualization of the switch and create a virtual device by connecting switches with the virtualized interfaces and connectors.

Virtualization has following advantages:

1. Virtualization can expand the interface density, because the interface number of the virtualized device equals the total interfaces of all member devices in the virtualization domain. That is, all member interfaces can be taken as one interface of the virtualized device.
2. This feature provides you with the tools to more closely and efficiently manage the system resources and users of the device. Virtualization enables the user to manage a group of switches as one logic object through one IP, which reduces the occupation of the IP address and is easy for management.
3. It expands uplink bandwidth.

Virtualization management is used for managing the configuration and operating state of the virtualization function. The user needs to enable the virtualization function. Restart the device after configuring virtualization and the virtualization function takes effect.

99.2 Virtualization Configuration Task List

- Configuring virtualized ports for interconnection
- Configuring Parameters of Virtualization
- Enabling Virtualization
- Save the configuration of virtualization and restart the device

99.3 Virtualization Configuration Task

99.3.1 Configuring virtualized ports for interconnection

Devices with different numbers in a virtual domain are connected to each other through virtualized ports. Each virtualized device must have at least one virtualized port.

To configure the virtualized ports, run the following command:

Command	Purpose
bvss interface *num* **slot** *slot* **port** *port* **group** *group*	Configures the slot/port as a virtualized port, its sequence number is num, and the port group number is group

99.3.2 Configuring parameters of virtualization

Virtualization uses the virtualization domain to manage the virtualized devices of one same group. Each member device in the virtualization domain has one ID. Every member device needs to configure its priority, so that it can be used in negotiating the master device. The device with the top priority will become the master device of the virtualization domain. Virtualization has two modes: the common mode and the enhanced mode. The common mode only supports virtualization of two devices and the enhanced mode supports virtualization of at most 4 devices. At present the system

supports virtualization of the common mode and enhanced mode.

MAC address of the virtualization system can be set in two ways: take MAC of the master device as the MAC of the virtualization system and take the reserved MAC as the MAC of the virtualization system.

To configure parameters of virtualization, run the following command:

Command	Purpose
bvss mode [normal | enhanced]	The command is used to configure the mode of virtualization
bvss domain-id *id*	The command is used to configure the domain of virtualization
bvss member-id *id*	The command is used to configure the member ID.
bvss priority *priority*	The command is used to configure the priority of the virtualized member device.
bvss mac-address mode [use-active-member | use-static-pool]	The command is used to configure the MAC address of the virtualization system.

99.3.3 Enabling Virtualization

The device runs in standalone mode by default, and the virtualization function is not enabled. After the virtualization-related parameters are configured, the virtualization function needs to be enabled.

To enable virtualization, run the following command:

Command	Purpose
bvss enable	The command is used to enable Virtualization.

99.3.4 Saving Virtualization Configuration

After finishing the parameter configuration, save the configuration and restart the device. Then the virtualization function takes effect.

To save virtualization, run the following command:

Command	Purpose
write bvss-config	The command is used to save virtualization configurations.

99.3.5 Showing virtualization configuration

On devices with virtualization enabled, you can use the following commands to display virtualization-related information.

To show the virtualization information, run the following command:

Command	Purpose
show bvss current-config	The command is used to show the current configuration of virtualization
show bvss running-config	The command is used to show the running configuration of virtualization
show bvss management	The command is used to show information of virtualization

show bvss statistics	The command is used to show statistics information of virtualization

The **current-config** of virtualization refers to the effect configuration on the device now; the running-config of virtualization refers to the configuration that may modify or add in running of the device. These configurations do not take effect only they are saved and the device is restarted.

Chapter 100 Introduction of Fast Ethernet Ring Network Protection

100.1 Overview

Fast Ethernet ring protection protocol is a special kind of link layer protocol, which is used to construct the ring Ethernet topology. The Ethernet protection protocol blocks a link in the case that the ring topology is complete, preventing the data loop against forming the broadcast storm. In case of link interruption, the protocol quickly enables the link to be restored to the status before link interruption so that the communication between the nodes of the loop can be restored.

Fast ring network protection protocol can ensure through controlling the aging of MAC address table for the switch that the data packets can be sent to the correct link when the topology takes change. Under normal circumstances, the aging time of the MAC address in the address table is 300 seconds. The ring network protection protocol can control the aging of the MAC address table for the switch in a very short period of time.

Ring network protection protocol and spanning tree protocol are both used for link layer topology control. The spanning tree protocol is suitable for all kinds of complex networks, which uses the hop-by-hop method to transmit the change in the network topology. The ring network protection protocol is dedicated to the ring topology, which uses the diffusion method to transmit the topological change. Therefore, in the ring network, the convergence performance of the ring protection protocol is better than that of the spanning tree protocol. In the case of good network condition, the ring network protection protocol can restore network communication within less than 50 ms.

NOTE:

Ring network protection protocol supports a switch configured as the node of multiple physical ring networks to form a tangent ring. It does not support the intersecting rings with public links.

100.2 ERPS-Related Concepts

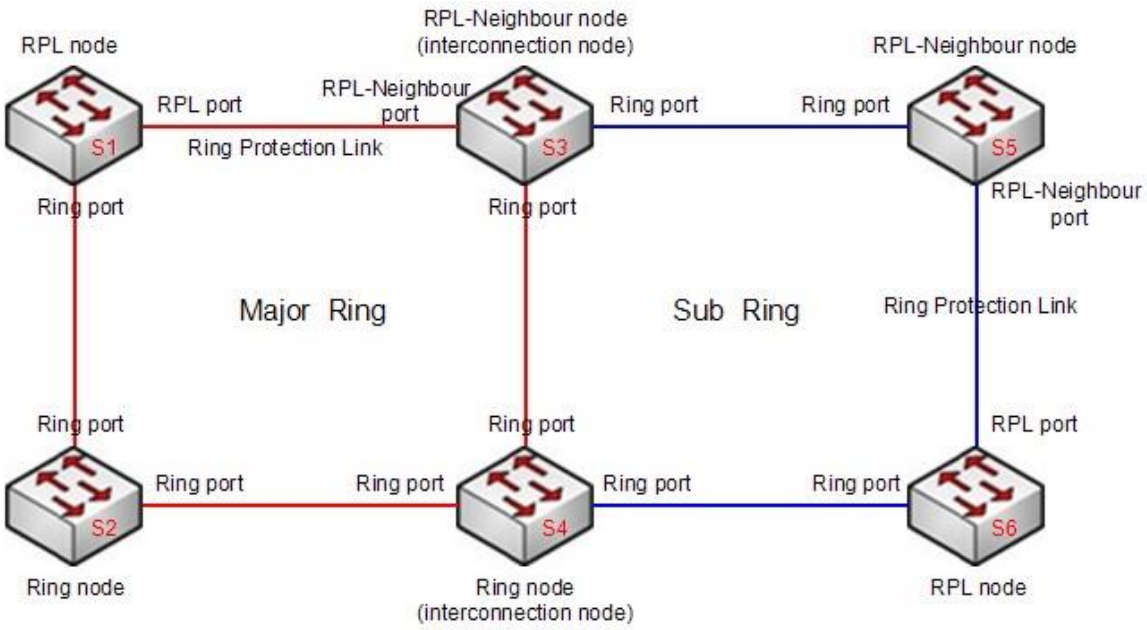


Figure 1 Diagram of ERPS Ethernet

100.2.1 Ring Network Level

ERPS supports multiple-ring or hierarchical transport network topology, as is shown in Figure 1. The major ring is a complete single ring; the sub-ring is connected to major ring (or sub-ring) through two interconnection-nodes. In Figure 1, red lines constitute a major ring, including Node S1, Link S1-S2, Node S2, Link S2-S4, Node S4, Link S4-S3, Node S3, Link S3-S1. Blue lines constitute a sub-ring, including Node S3, link, Link S3-S5, Node S5, Link S5-S6, Node S6, Link S6-S4, Node S4, but not including Link S4-S3.

100.2.2 Ring Network Node Role

Each switch constituting the ring network is a ring network node. The ring network node role falls into four kinds: RPL protection node, RPL neighbor node, interconnection node and ordinary node. A physical link is selected from each single ring as RPL protection link; one of two switches directly connected to this link is taken as RPL protection node and the other is taken as RPL neighbor node; and the remaining switches are used as ordinary nodes. The interconnection nodes are two intersecting nodes when the sub-ring is connected to major ring (or sub-ring).

As is shown in Figure 1, in the major ring, S1 is a RPL protection node; S3 is a RPL neighbor node, S4 and S2 are ordinary nodes; in the sub-ring, S6 is a RPL protection node, S5 is a RPL neighbor node, they are connected to the major ring through Interconnection Node: S4 and S3.

The node type of the ERPS protocol is determined by the port role, but the node type of the interconnection node needs to be determined in the configuration; by default, the node is not the interconnection-node.

For the ring network nodes, their functions are basically the same: detecting the status of local ring network port and sending a notification when the link fails. Differently, under normal circumstances, the RPL protection node and the RPL neighbor node block the RPL link, but the ordinary node does not block the RPL link. For the interconnection node, there is only one ring network port connected to the sub ring, and this node must also be a node in the other main ring (or sub ring).

100.2.3 Ring Network Port Role

The ERPS protocol requires that each node has two ports that are connected to the RING network. Each port is called “Ring Port”. In addition, in each single ring, there is also a ring network port as the ring network protection link (RPL). For the interconnection node, although only the ring port is connected to the sub-ring, there is also a virtual port to detect the connectivity between two interconnection nodes. This point will be discussed in the later part.

Under normal circumstances, all the ring network ports but the RPL link in the ring network are in the forwarding state. RPL ports of the RPL protection node and the RPL neighbor node are blocked to avoid the loop. In the case of the failure in the ring network link, the RPL protection node and RPL neighbor nodes don’t block the RPL port any more, restoring the network communication.

In one switch, each ring network node instance can only be configured with one RPL port.

NOTE:

ERPS protocol supports the configuration of the aggregated port as ring network port.

100.2.4 ERPS & CFM

In the ERPS port, MEP is configured to monitor the ring network link. The ring network port monitors the status of its ring network link through “Down MEP”; meanwhile, the ring network port where the interconnection node is connected to the sub-ring is configured with “Up MEP” to monitor the connectivity of the major ring, as is shown in Figure 2.

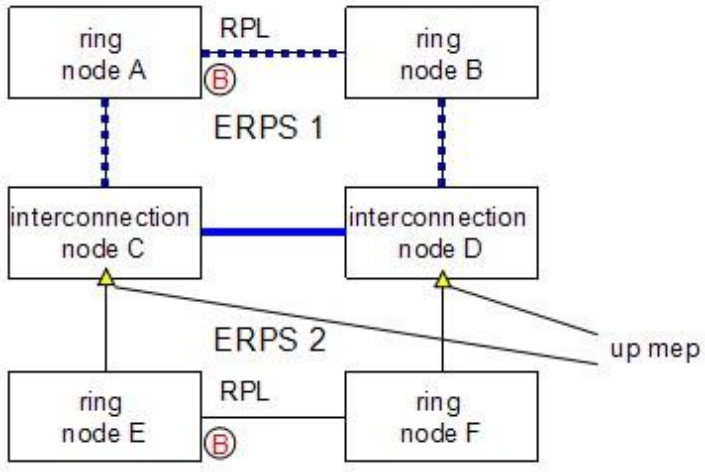


Figure 2 Virtual ports for interconnection nodes configured on the "Up MEP" port

In Figure 2, all the ERPS ring network ports are configured with "Down Mep" to monitor the ring network link through "Down MEP". For example, Ring Link A-C is later monitored as a ring network port of Node A and Node C is configured with "Down Mep"; when the link fails or restores from the failure, it will send the corresponding notice to ERPS control module; meanwhile, the "Down Mep" is responsible for receiving and sending R-APS messages. The "Up MEP" is only configured on the ring network port where the interconnection node is connected to the sub-ring to monitor the connectivity of major ring. When the major ring between the interconnection nodes is blocked or restored to smooth communication, it sends the corresponding notification to the ERPS control module. In addition, the ring network port where the interconnection node is connected to the sub-ring is not only configured with "Up MEP", but also "Down MEP".

NOTE:

The ring network port where the interconnection node is connected to the sub-ring is configured with "Up Mep" to monitor the connectivity of major ring; at this time, it means that the virtual port of major ring link is monitored.

100.2.5 Ring Network Interconnection Mode Using R-APS Virtual Channel

For the sub-rings, the interconnection node is a node that connects the sub rings and other networks. For example, in Figure 1, the major ring is connected. The "Up MEP" port of interconnection node monitors the connectivity of the major ring, which is called the R-APS virtual channel. Through the R-APS virtual channel, two interconnection nodes can conduct R-APS communication via other networks.

The sub-ring transmits R-APS information to the network (and receives R-APS message from the network) through the R-APS virtual channel; meanwhile, the R-APS information can be transmitted in the network as data stream. Of course, the R-APS information should be separated from the ordinary data stream; so for different ERPS ring networks, different "control VLANs" are used to carry the R-APS information.

Of course, when the interconnection node is connecting the sub-ring with other networks, the R-APS channel is not used, which is in the forwarding state.

100.2.6 R-APS Transmission VLAN

As R-APS packets are transmitted in the R-APS channel, a VLAN must be set up for R-APS channel. Different nodes have different VLANs, but for some node, other nodes' VLANs can be used as VLAN for ordinary data stream transmission.

When configuring R-APS's VLAN, if the VLAN has not been created, the ERPS system will automatically create the VLAN.
The state of the ERPS ring network port in the R-APS channel is consistent with that of ordinary data stream. But the sub-ring without using the R-APS virtual channel is an exception. The R-APS channel of interconnection node in this sub-ring is suspended, so the nodes on the sub-ring of the R-APS virtual channel are not used, and their R-APS channels are in the forwarding state.

NOTE:

The VLAN for the MEP port on the ERPS port is consistent with R-APS Transmission VLAN.

100.2.7 Revertive Mode

In some ring networks, under normal circumstances, the network resources of the link channel for data stream transmission would be better; but the channel of RPL is only used for backup; so the revertive mode is used in the switching clearance to return the data stream to the channel with better network resources. For some ring networks, as they don't have high requirements for network resources, they needn't immediately return to the original link channel after the switching is restored. So, the non-returning mode is adopted so that the times of returning to switching can be reduced.

In the operation of returning mode, when a switch is cleared, the data stream will return to the original channel, blocking RPL. In the case of fault clearance, the data stream returns under the premise of the timeout of the WTR timer, avoiding protection switching in the case of intermittent faults. In the case of clearing manual switching or forced switch commands, there is need to wait for the WTB timer. In the operation of non-revertive mode, when a switching is cleared, the data stream still remains in RPL channel as long as there is no fault in the RPL channel.

NOTE:

WTR timer and WTB timer are valid only in revertive mode.

100.3 Type of ERPS Packets

The type of packet used by the ERPS protocol is shown in table 2.1.

Type of packet	Description
Forced Switch (FS)	Ring network node (including RPL node) notifies other nodes after the forced switching command.
Signal Fail (SF)	Ring network node (including RPL node) notifies other nodes after finding the local link failure in the detection.
Manual Switch (MS)	Ring network node (including RPL node) notifies other nodes after manual switching commands.
No Request (NR)	Ring network node notifies other nodes after finding all the local ring network links are recovered in the detection.
No Request, RPL Blocked (NR-RB)	Ring network protection node notifies other nodes of the recovery of ring network protection switching.

Table 2.1 ERPS Ring Network Protection Protocol Packet Type

100.4 ERPS Ring Network Protection Mechanism

100.4.1 Stable State

In the stable state, the RPL port is blocked by the ring network protection node, which continuously sending the NR-RB protocol message with a configurable cycle.

For all the ordinary nodes that receive NR-RB packets, the local ring network port is set as the forwarding state. In the stable state, ordinary nodes do not send protocol packets.

The protection node is modified by configuring the command through the “send-time” node to send the cycle of the NR-RB packet.

100.4.2 Local Link Failure Processing

When a ring network node detects the local link failure, the blocking state of the enabled local port (including the RPL port or the ordinary ring port which has not yet entered the forwarding state) is immediately eliminated, and then the SF protocol message begins to be sent and the aging of local MAC address table begins.

For all other nodes receiving SF packets, the local packet sending first stops, and then the blocking state of the local enabled port is relieved and the address table aging starts.

The disabled node for the link continuously sends the SF packet taking the configured “send-time” as the cycle. In this process, if the port for another node recovers from the failure state, this node will restore the state of port as the forwarding state after receiving SF packets.

100.4.3 Local Link Recovery Processing

When the ring network node finds that the local ring network port recovers from the failure state in the detection, it will keep the port still in the blocking state and begins to continue to send NR packets.

In the process of sending NR packet, if the node receives the SF packet from other nodes, it indicates that there are other disabled links in the network; the local node stops sending the NR packet and sets the recovered port to be in the forwarding state.

If local node does not receive new SF packet, it will start switching recovery timer after the ring network protection node (RPL node) receives the NR packet; and after the timer timeout, RPL node blocks the RPL port once again and sends NR-RB packet and then starts the address table aging. The network communication recovers to the initial stable state.

100.4.4 Protection Switching - Link Recovery

When the ring network node finds that the local ring network port recovers from the failure state in the detection, it will keep the port still in the blocking state and begins to continue to send NR packets.

In the process of sending NR packet, if the node receives the SF packet from other nodes, it indicates that there are other disabled links in the network; the local node stops sending the NR packet and sets the recovered port to be in the forwarding state.

If local node does not receive new SF packet, it will recover the link after the ring network protection node (RPL node) receives the NR packet. But when the link is recovered, the revertive mode and non-revertive mode are not consistent in behavior and function.

1. Revertive mode

In revertive mode, the ring network link will be recovered. After RPL node receives the NR packet, it will start switching recovery timer; after the timer timeout, RPL node blocks the RPL port once again and sends the NR-RB packet; and then the

address table aging starts, the network communication is recovered to the initial stable state.

2. Non-revertive mode

In the non-revertive mode, the ring network link is not automatically recovered. After receiving the NR packet, the RPL node does not make any response; after other ring network nodes receive the NR packets, they don't do any action. Only when the RPL node receives the "Clear" command, the RPL node blocks the RPL link and continues to send RB NR packets to two ring network ports, and then execute Flush FDB. After the disabled node receives the RB NR packet, it relieves the blocking state of the port. After receiving the RB NR packet, the ring network node executes Flush FDB.

100.4.5 Protection Switching - Manual Switching

In the normal ring network state, after the ring network node receives a manual switching command, it blocks data stream channel and the R-APS channel (Blocking a data stream channel and R-APS channel port) and opens other ring network ports and continues to send MS packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the MS packet, they open RPL data stream channel and R-APS channel. After receiving the MS packet, the ring network node sending MS packet stops sending MS packet. After receiving the MS packet, the ring network nodes execute Flush FDB.

The above action completes an operation of manual switching; in order to keep switching operation normal, there are several points deserving our attention:

1). When a manual switching command has existed in the ring network, the later manual switching commands are invalid. The node receiving new switching command must refuse new switching command and give notice that the manual switching is rejected.

2). For the node which has generated manual switching command locally, if receiving MS packets of different node IDs, this node should remove the local manual switching command and send the NR packet. At the same time, the node continues to block the ring network port blocked by previous manual switching commands.

3). For the node which has generated manual switching command locally, if receiving higher priority of local request or packet, this node shall remove manual switching requests and execute the higher priority of requests.

For the node which generates manual switching command, after receiving the "Clear" command, it removes manual switch command. The node continues to block the ring network port blocked by previous manual switching commands and sends NR packets to two ring network ports. But when the link is recovered, the revertive mode and non-revertive mode are not consistent in behavior and function.

1. Revertive mode

In revertive mode, the ring network link will be recovered. After the RPL node receives the NR packet, it starts the WTB timer. After the timeout of the WTB timer, the RPL node will block the RPL link and send the RB NR packet, and then execute FDB Flush. After other ring network nodes receive the RB NR packet, they eliminate the blocking state of all non-RPL links, and then execute FDB Flush.

2. Non-revertive mode

In the non-revertive mode, the ring network link is not automatically recovered. After receiving the NR packet, the RPL node does not make any response; after other ring network nodes receive the NR packets, they don't do any action. Only when the RPL node receives the "Clear" command, the RPL node blocks the RPL link and continues to send NR RB packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the NR RB packet, they eliminate the blocking state of non-RPL link and execute Flush FDB.

100.4.6 Protection Switching - Forced Switching

In the normal ring network state, after the ring network node receives a forced switching command, it blocks data stream channel and the R-APS channel (Blocking a data stream channel and R-APS channel port) and opens other ring network ports and continues to send FS packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the FS packet, they open RPL data stream channel and R-APS channel. After receiving the FS packet, the ring network node sending FS packet stops sending FS packet. After receiving the FS packet, the ring network nodes execute Flush FDB.

The above action completes an operation of forced switching; in order to keep switching operation normal, there is one point deserving our attention:

When a forced switching command has existed in the ring network, the later forced switching commands are acceptable unless this node has accepted a forced switching request in advance. At the same time, the node receiving new switching command must execute forced switching once again, block the port and send FS packets. Of course, the repeated execution of forced switching command will segment the ring network, so it is appropriate to avoid such adverse situation.

For the node which generates forced switching command, after receiving the "Clear" command, it removes forced switching command. The node continues to block the ring network port blocked by previous forced switching commands and sends NR packets to two ring network ports. But when the link is recovered, the revertive mode and non-revertive mode are not consistent in behavior and function.

1. Revertive mode

In revertive mode, the ring network link will be recovered. After the RPL node receives the NR packet, it starts the WTB timer. After the timeout of the WTB timer, the RPL node will block the RPL link and send the RB NR packet, and then execute FDB Flush. After other ring network nodes receive the NR RB packet, they eliminate the blocking state of all non-RPL links, and then execute FDB Flush.

2. Non-revertive mode

In the non-revertive mode, the ring network link is not automatically recovered. After receiving the NR packet, the RPL node does not make any response; after other ring network nodes receive the NR packets, they don't do any action. Only when the RPL node receives the "Clear" command, the RPL node blocks the RPL link and continues to send NR RB packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the NR RB packet, they eliminate the blocking state of all non-RPL links and execute Flush FDB.

100.4.7 Switching Recovery Processing

The ring network protection node (RPL owner) realizes the ring network switching recovery through the WTR timer (Wait-to-Restore timer) and the WTB timer (Wait-to-Block timer). The WTR timer and WTB timer can be used to avoid frequent switching on the ring network.

The WTR timer is only valid in the revertive mode; in the non-revertive mode, after the fault recovery of the ring network from the protection state, the ring network doesn't recover, so there is no need to start the WTR timer. In the revertive mode, after the RPL node receives the NR message from other nodes, it starts the WTR timer; after the timeout of timer, the RPL node maintains the forwarding state of the RPL port, and it does not send the ring network recovery notification. If the RPL node receives the SF message, it indicates that the ring network has not been fully recovered; at this time, the node stop sthe WTR timer. After the timeout of WTR timer, the RPL node will re-block the RPL port.

The WTB timer is effective only in the revertive mode, which is used at the time of clearing the forced and manual switching command. When the forced switching command is cleared repeatedly, the WTB timer must ensure that a single forced switching command does not make RPL blocked repeatedly. When a manual switching command is cleared, the

WTB timer must prevent RPL node against causing a closed ring because of receiving an outdated remote MS request in the recovery process.

The WTB timer must ensure that there is sufficient time to receive the remote SF, FS and MS packets, so the time of defining the WTB timer is 5 seconds longer than that of defining the Guard timer. This period of time is enough for one ring network node sending the packet to send 2 R-APS packets and allow the entire ring network to confirm each situation.

Chapter 101 ERPS Configuration

101.1 ERPS Configuration Instructions

Please read the following instructions before configuring the ERPS ring network protection protocol:

- The ERPS port must be carried on the MEP port of the CFM; the MEP information must be configured to match with the MEP port for the ERPS port; after the configuration is successful, the ERPS port can be enabled normally.
- It must be configured that the default VLANs (or control VLANs) of all ring network ports are consistent, ensuring that the ERPS packet can be forwarded normally.
- In the case that the ERPS and EAPS protocols are used simultaneously, the default VLAN and control VLAN for ERPS ring network port cannot be the same as control VLAN for EAPS. The control VLAN for EAPS cannot forward the ERPS protocol packet.
- One port cannot be simultaneously used as the ring network port of ERPS and EAPS protocols.
- The ERPS protocol supports the configuration of physical port or aggregate port as the ring network port. However, the physical port that has been configured with the link aggregation, 802.1X authentication or port security cannot be configured as an ERPS ring network port.
- The nimble Mode is backward compatibility. It keeps the original configuration mode by default. Only after the device is configured with nimble mode, the nimble mod can take effect.

101.2 ERPS Configuration Tasks

- Configuring the nimble nodes
- Configuring the ring network nodes
- Configuring the ring network ports
- Checking ring network protection protocol status

101.2.1 Configuring the Ring Network Nodes

In the global configuration mode, the switch is configured as ERPS node according to the following steps.

Command	Purpose
Switch_config# **erps** *id*	Configure ERPS ring network node instance and enter the node configuration mode. id: Ring network instance number; Range 0-7.
Switch_config_ring# **control-vlan** *value*	Mandatory. Configure the control VLAN of the local node. No control VLAN: Delete the control VLAN of the local node. After the normal operation of the node, the change shall not be allowed. Value: Range: 1-4094. By default, no control-vlan.
Switch_config_ring# **interconnection-node**	Mandatory. Configure the local node as the interconnection node. No interconnection-node: Configure that the local node is not the interconnection node. After the normal operation of the node, the change shall not be allowed.

	By default, the local node is not the interconnection node.
Switch_config_ring# **raps-virtual-channel**	Mandatory. Configure that the local node uses the R-APS virtual channel. No Raps-virtual-channel: Configure that the local node doesn't use the R-APS virtual channel. After the normal operation of the node, the change shall not be allowed. By default, the local node uses the R-APS virtual channel.
Switch_config_ring# **revertive-mode**	Mandatory. Configure that the revertive mode of local node is the revertive mode. No revertive-mode: Configure that the revertive mode of local node is not the revertive mode. After the normal operation of the node, the change shall not be allowed. By default, the local node is the revertive mode.
Switch_config_ring# **version** *value*	Configure the local node's version. Value: By default, 1; range: 0-2.
Switch_config_ring# **wtr-time** *value*	Configure the timeout value of WTR timer. Value: Timeout value: by default, 20 seconds; range: 10-720 seconds.
Switch_config_ring# **guard-time** *value*	Configure the timeout value of Guard Timer. When a port is recovered from the failure state, the Guard timer is prohibited to handle the received protocol packets in a short period of time to avoid the wrong protocol action caused by receiving the outdated packet. Value: 10 ms as the unit; 50 as the default value; range of 10-2000;
Switch_config_ring# **send-time** *value*	Configure the protocol packet sending cycle. Value: Packet sending cycle: by default, 5 seconds; range: 1-10.
Switch_config_ring# **exit**	Exit from node configuration mode and enable the node.

NOTE:

Use the "**no erps** *id*" command to delete the ring network node configuration and node port configuration.

The "interconnection-node" "raps-virtual-channel" "revertive-mode" commands are mandatory, but they all have their default configuration, so when the local node is created, these commands can be omitted if the default values needn't be amended.

101.2.2 Configuring the Ring Network Ports

The switch port is configured as the ring network port according to the following steps.

Command	Purpose
Switch_config# **interface** *interface-type interface-number*	Enter the port configuration mode. intf-name: Port name.
Switch_config_intf# **erps** *id* **ring-port**	Configure the port as an ordinary ring network port for the specified node. Id: Ring network instance number.
Switch_config_intf# **erps** *id* **rpl**	Configure the port as a ring network protection link for the specified node. In the case of automatically discovering enabling, the function of this command is equivalent to the change of a priority value to 0. Id: Ring network instance number.
Switch_config_intf# **erps** *id* **neighbour**	Configure the port as a RPL neighbor port of the specified node; meanwhile, this port must be connected to the RPL port and must be configured as a RPL neighbor port. Id: Ring network instance number.
Switch_config_intf# **exit**	Exit from port configuration mode.

NOTE:

1. Configure the command through the "**no erps** *id* **rpl"** port, and change the RPL port into ordinary ring network port.
2. Configure the command through the "**no erps** *id* **ring-port(neighbor)"**port, delete the ordinary ring network port (RPL neighbor port) or RPL port configuration.
3. In the case that the ring network node is not configured globally, use the command "**erps id ring-port (neighbor)"** and **"rpl"** to simultaneously create the ring network nodes.
4. "up mep" is only configured in the interconnection-node, and the interconnection-node can only be configured with one ring network port.

101.2.3 Ring Network Control Commands

In the monitoring mode, use the following commands to control the ring network status.

Command	Purpose
erps *id* **ForcedSwitch interface** *interface-type interface-number*	For the node, execute the forced switching to the port "interface-type interface-number". Id: Ring network instance number.
erps *id* **ManualSwitch interface** *interface-type interface-number*	For the node, execute the manual switching to the port "interface-type interface-number". Id: Ring network instance number.

erps *id* **Clear**	Clear the switching command of the node. Id: Ring network instance number.

101.2.4 Checking Ring Network Protection Protocol Status

Use the following commands to check the ring network protection protocol status.

Command	Purpose
show erps *id*	Check the summary information of ring network protection protocol and ring network port. Id: Ring network instance number.
show erps *id* **detail**	Check the detailed information of ring network protection protocol and port.
show erps interface *interface-type interface-number*	Check the status information of ring network port.

101.3 ERPS Configuration Instance

101.3.1 Configuration example 1-ERPS single ring configuration

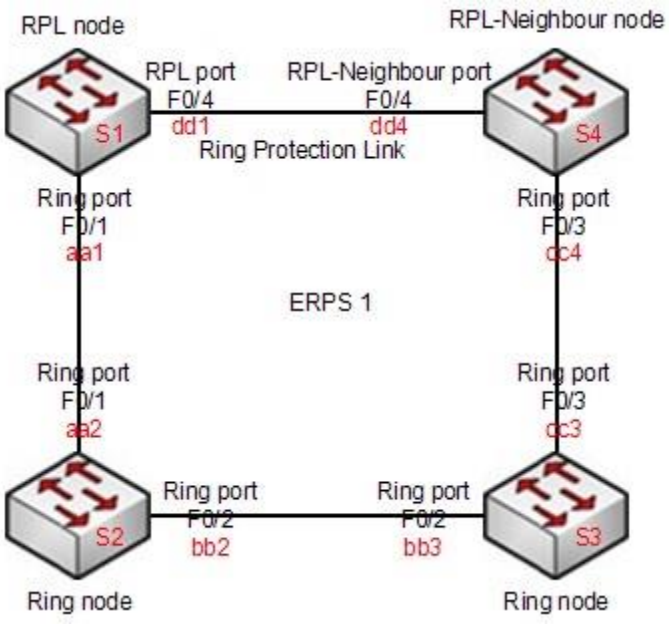


Figure 101. 1 ERPS Single Ring Configuration

As shown in Figure 101.1, S1, S2, S3, and S4 are configured as follows:

1. Configure switch S1:

Configure the CFM function:

Switch# config

Switch_config# ethernet cfm ENABLE

Switch_config# ethernet cfm md mdnf STRING mdn a level 4

Switch_config_cfm# ma manf STRING man a meps 1-2 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn d level 4

Switch_config_cfm# ma manf STRING man d meps 1,4 vlan 2

Switch_config_cfm#exit

Switch_config#interface f0/ 1

Switch_config_f0/1# ethernet cfm ENABLE

Switch_config_f0/1# ethernet cfm mep add mdnf STRING mdn a manf STRING man a mepid 1 rmepid 2

Switch_config_f0/1# ethernet cfm mep ENABLE mdnf STRING mdn a manf STRING man a mepid 1 rmepid 2

Switch_config_f0/1# ethernet cfm mep cci-ENABLE mdnf STRING mdn a manf STRING man a mepid 1 rmemid 2

Switch_config_f0/1# interface f0/4

Switch_config_f0/4# ethernet cfm ENABLE

Switch_config_f0/4# ethernet cfm mep add mdnf STRING mdn d manf STRING man d mepid 1 rmepid 4

Switch_config_f0/4# ethernet cfm mep ENABLE mdnf STRING mdn d manf STRING man d mepid 1 rmepid 4

Switch_config_f0/4# ethernet cfm mep cci-ENABLE mdnf STRING mdn d manf STRING man d mepid 1 rmepid 4

Configure ring network nodes:

Switch_config#erps 1

Switch_config_ring1#control-vlan 2

Switch_config_ring1#exit

Switch_config#

Configure the normal port:

Switch_config# interface f0/ 1

Switch_config_f0/1# erps 1 ring-port

Switch_config_f0/1# erps 1 mep down md a ma a level 4 local 1 remote 2

Configure the RPL port:

Switch_config# interface f0/4

Switch_config_f0/4# erps 1 rpl

Switch_config_f0/4# erps 1 mep down md d ma d level 4 local 1 remote 4

2. Configure switch S2:

Configure the CFM function:

Switch# config

Switch_config# ethernet cfm ENABLE

Switch_config# ethernet cfm md mdnf STRING mdn a level 4

Switch_config_cfm# ma manf STRING man a meps 1-2 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn b level 4

Switch_config_cfm# ma manf STRING man b meps 2-3 vlan 2

Switch_config_cfm#exit

Switch_config#interface f0/ 1

Switch_config_f0/1# ethernet cfm ENABLE

Switch_config_f0/1# ethernet cfm mep add mdnf STRING mdn a manf STRING man a mepid 2 rmepid 1

Switch_config_f0/1# ethernet cfm mep ENABLE mdnf STRING mdn a manf STRING man a mepid 2 rmepid 1

Switch_config_f0/1# ethernet cfm mep cci-ENABLE mdnf STRING mdn a manf STRING man a mepid 2 rmepid 1

Switch_config_f0/1# interface f0/2

Switch_config_f0/2# ethernet cfm ENABLE

Switch_config_f0/2# ethernet cfm mep add mdnf STRING mdn b manf STRING man b mepid 2 rmepid 3

Switch_config_f0/2# ethernet cfm mep ENABLE mdnf STRING mdn b manf STRING man b mepid 2 rmepid 3

Switch_config_f0/2# ethernet cfm mep cci-ENABLE mdnf STRING mdn b manf STRING man b mepid 2 rmepid 3

Configure ring network nodes:

Switch_config#erps 1

Switch_config_ring1#control-vlan 2

Switch_config_ring1#exit

Switch_config#

Configure the normal port:

Switch_config# interface f0/1

Switch_config_f0/1# erps 1 ring-port

Switch_config_f0/1# erps 1 mep down md a ma a level 4 local 2 remote 1

Switch_config_f0/1# interface f0/2

Switch_config_f0/2# erps 1 ring-port

Switch_config_f0/2# erps 1 mep down md b ma b level 4 local 2 remote 3

3. Configure switch S3:

Configure the CFM function:

Switch# config

Switch_config# ethernet cfm ENABLE

Switch_config# ethernet cfm md mdnf STRING mdn b level 4

Switch_config_cfm# ma manf STRING man b meps 2-3 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn c level 4

Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2

Switch_config_cfm#exit

Switch_config#interface f0/2

Switch_config_f0/2# ethernet cfm ENABLE

Switch_config_f0/2# ethernet cfm mep add mdnf STRING mdn b manf STRING man b mepid 3 rmepid 2

Switch_config_f0/2# ethernet cfm mep ENABLE mdnf STRING mdn b manf STRING man b mepid 3 rmepid 2

Switch_config_f0/2# ethernet cfm mep cci-ENABLE mdnf STRING mdn b manf STRING man b mepid 3 rmepid 2

Switch_config_f0/2# interface f0/3

Switch_config_f0/3# ethernet cfm ENABLE

Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 3 rmepid 4

Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c mepid 3 rmepid 4

Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c mepid 3 rmepid 4

Configure ring network nodes:

Switch_config#erps 1

Switch_config_ring1#control-vlan 2

Switch_config_ring1#exit

Switch_config#

Configure the normal port:

Switch_config# interface f0/2

Switch_config_f0/2# erps 1 ring-port

Switch_config_f0/2# erps 1 mep down md b ma b level 4 local 3 remote 2

Switch_config_f0/2# interface f0/3

Switch_config_f0/3# erps 1 ring-port

Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 3 remote 4

4. Configure switch S4:

To configure the CFM function:

Switch# config

Switch_config# ethernet cfm ENABLE

Switch_config# ethernet cfm md mdnf STRING mdn c level 4

Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn d level 4

Switch_config_cfm# ma manf STRING man d meps 1,4 vlan 2

Switch_config_cfm#exit

Switch_config#interface f0/3

Switch_config_f0/3# ethernet cfm ENABLE

Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 4 rmepid 3

Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c mepid 4 rmepid 3

Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c mepid 4 rmepid 3

Switch_config_f0/3#interface f0/4

Switch_config_f0/4# ethernet cfm ENABLE

Switch_config_f0/4# ethernet cfm mep add mdnf STRING mdn d manf STRING man d mepid 4 rmepid 1

Switch_config_f0/4# ethernet cfm mep ENABLE mdnf STRING mdn d manf STRING man d mepid 4 rmepid 1

Switch_config_f0/4# ethernet cfm mep cci-ENABLE mdnf STRING mdn d manf STRING man d mepid 4 rmepid 1

Configure ring network nodes:

Switch_config#erps 1

Switch_config_ring1#control-vlan 2

Switch_config_ring1#exit

Switch_config#

Configure the normal port:

Switch_config# interface f0/3

Switch_config_f0/3# erps 1 ring-port

Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 4 remote 3

Configure the RPL neighbor port:

Switch_config# interface f0/4

Switch_config_f0/4# erps 1 neighbour

Switch_config_f0/4# erps 1 mep down md d ma d level 4 local 4 remote 1

101.3.2 Configuration example 2-ERPS multi-ring configuration

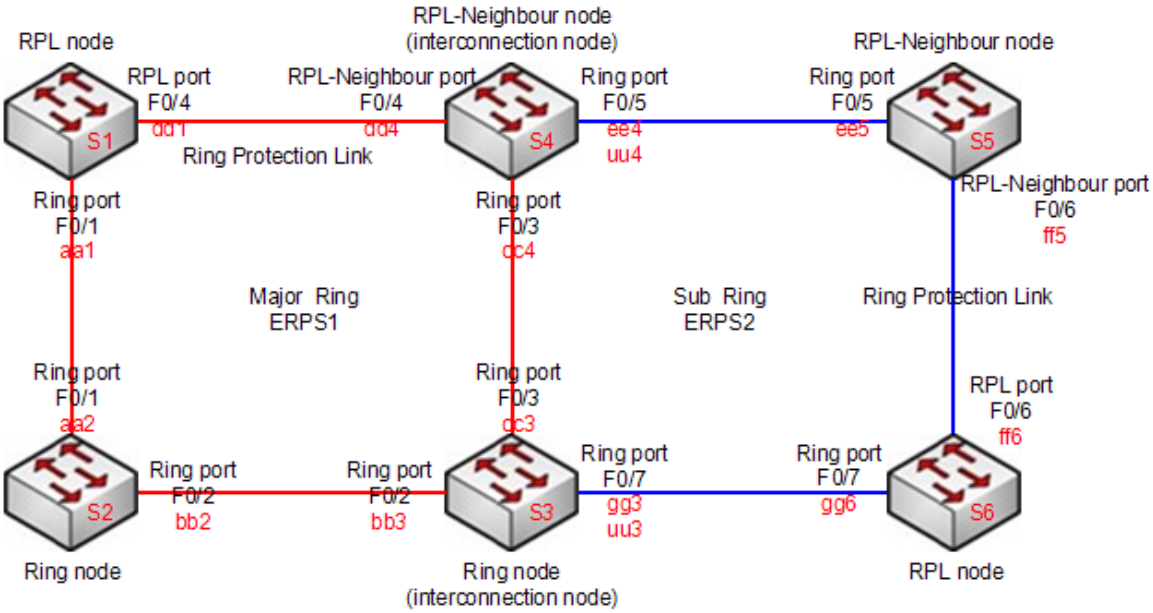


Figure 5.2 ERPS multi-ring configuration

As shown in Figure 5.2, the interconnection nodes S3 and S4 are configured as follows, and the configuration of other nodes is omitted.

1 Configure switch S3:

To configure the CFM function:

Switch# config

Switch_config# ethernet cfm ENABLE

Switch_config# ethernet cfm md mdnf STRING mdn b level 4

Switch_config_cfm# ma manf STRING man b meps 2-3 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn c level 4

Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn g level 4

Switch_config_cfm# ma manf STRING man g meps 3,6 vlan 3

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn u level 5

Switch_config_cfm# ma manf STRING man u meps 3-4 vlan 3

Switch_config_cfm#exit

Switch_config#interface f0/2

Switch_config_f0/2# ethernet cfm ENABLE

Switch_config_f0/2# ethernet cfm mep add mdnf STRING mdn b manf STRING man b mepid 3 rmepid 2

Switch_config_f0/2# ethernet cfm mep ENABLE mdnf STRING mdn b manf STRING man b mepid 3 rmepid 2

Switch_config_f0/2# ethernet cfm mep cci-ENABLE mdnf STRING mdn b manf STRING man b mepid 3 rmepid 2

Switch_config_f0/2# interface f0/3

Switch_config_f0/3# ethernet cfm ENABLE

Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 3 rmepid 4

Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c mepid 3 rmepid 4

Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c mepid 3 rmepid 4

Switch_config_f0/3# interface f0/7

Switch_config_f0/7# ethernet cfm ENABLE

Switch_config_f0/7# ethernet cfm mep add mdnf STRING mdn g manf STRING man g mepid 3 rmepid 6

Switch_config_f0/7# ethernet cfm mep ENABLE mdnf STRING mdn g manf STRING man g mepid 3 rmepid 6

Switch_config_f0/7# ethernet cfm mep cci-ENABLE mdnf STRING mdn g manf STRING man g mepid 3 rmepid 6

Switch_config_f0/7# ethernet cfm mep add mdnf STRING mdn u manf STRING man u mepid 3 rmepid 4 direction up

Switch_config_f0/7# ethernet cfm mep ENABLE mdnf STRING mdn u manf STRING man u mepid 3 rmepid 4

Switch_config_f0/7# ethernet cfm mep cci-ENABLE mdnf STRING mdn u manf STRING man u mepid 3 rmepid 4

Configure ring network nodes:

Switch_config#erps 1

Switch_config_ring1#control-vlan 2

Switch_config_ring1#exit

Switch_config#

Switch_config#erps 2

Switch_config_ring1#control-vlan 3

Switch_config_ring1#interconnection-node

Switch_config_ring1#exit

Switch_config#

Configure the normal port of ERPS1:

Switch_config# interface f0/2

Switch_config_f0/2# erps 1 ring-port

Switch_config_f0/2# erps 1 mep down md b ma b level 4 local 3 remote 2

Switch_config_f0/2# interface f0/3

Switch_config_f0/3# erps 1 ring-port

Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 3 remote 4

Configure the normal port of ERPS2:

Switch_config_f0/3# interface f0/7

Switch_config_f0/7# erps 2 ring-port

Switch_config_f0/7# erps 2 mep down md g ma g level 4 local 3 remote 6

Switch_config_f0/7# erps 2 mep down md u ma u level 5 local 3 remote 4

2. Configure switch S4:

Configure the CFM function:

Switch# config

Switch_config# ethernet cfm ENABLE

Switch_config# ethernet cfm md mdnf STRING mdn c level 4

Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn d level 4

Switch_config_cfm# ma manf STRING man d meps 1,4 vlan 2

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn e level 4

Switch_config_cfm# ma manf STRING man e meps 4-5 vlan 3

Switch_config_cfm#exit

Switch_config# ethernet cfm md mdnf STRING mdn u level 5

Switch_config_cfm# ma manf STRING man u meps 3-4 vlan 3

Switch_config_cfm#exit

Switch_config#interface f0/3

Switch_config_f0/3# ethernet cfm ENABLE

Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 4 rmepid 3

Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c mepid 4 rmepid 3

Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c mepid 4 rmepid 3

Switch_config_f0/3#interface f0/4

Switch_config_f0/4# ethernet cfm ENABLE

Switch_config_f0/4# ethernet cfm mep add mdnf STRING mdn d manf STRING man d mepid 4 rmepid 1

Switch_config_f0/4# ethernet cfm mep ENABLE mdnf STRING mdn d manf STRING man d mepid 4 rmepid 1

Switch_config_f0/4# ethernet cfm mep cci-ENABLE mdnf STRING mdn d manf STRING man d mepid 4 rmepid 1

Switch_config_f0/4# interface f0/5

Switch_config_f0/5# ethernet cfm ENABLE

Switch_config_f0/5# ethernet cfm mep add mdnf STRING mdn e manf STRING man e mepid 4 rmepid 5

Switch_config_f0/5# ethernet cfm mep ENABLE mdnf STRING mdn e manf STRING man e mepid 4 rmepid 5

Switch_config_f0/5# ethernet cfm mep cci-ENABLE mdnf STRING mdn e manf STRING man e mepid 4 rmepid 5

Switch_config_f0/5# ethernet cfm mep add mdnf STRING mdn u manf STRING man u mepid 4 rmepid 3 direction up

Switch_config_f0/5# ethernet cfm mep ENABLE mdnf STRING mdn u manf STRING man u mepid 4 rmepid 3

Switch_config_f0/5# ethernet cfm mep cci-ENABLE mdnf STRING mdn u manf STRING man u mepid 4 rmepid 3

Configure ring network nodes:

Switch_config#erps 1

Switch_config_ring1#control-vlan 2

Switch_config_ring1#exit

Switch_config#

Switch_config#erps 2

Switch_config_ring1#control-vlan 3

Switch_config_ring1#interconnection-node

Switch_config_ring1#exit

Switch_config#

Configure the normal port of ERPS1:

Switch_config# interface f0/3

Switch_config_f0/3# erps 1 ring-port

Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 4 remote 3

Configure the RPL neighbor port for ERPS1:

Switch_config# interface f0/4

Switch_config_f0/4# erps 1 neighbour

Switch_config_f0/4# erps 1 mep down md d ma d level 4 local 4 remote 1

Configure the normal port of ERPS2:

Switch_config# interface f0/5

Switch_config_f0/5# erps 2 ring-port

Switch_config_f0/5# erps 2 mep down md e ma e level 4 local 4 remote 5

Switch_config_f0/5# erps 2 mep down md u ma u level 5 local 4 remote 3

Display the erps of switch S3:

Switch_config# show erps

Ethernet Ring Protection Switching

Ring1

RPL Owner Priority Unknown

Address

This node is the RPL Owner

Node ID Priority 32770 (priority 32770 id 1)

Address 00E0.0F81. 111B

Control Vlan 2

Version 1

RAPS Virtual Channel: True

Revertive Mode: Revertive

State Pending WTR False

Signal Fail False Sending NR

WTR time 0/20 sec WTB time 0/6 sec

Guard time 0/500 ms Send time 1/5 sec

Interface	Role	State	Status	MEP Role
F0/2	Ring-Port	BLK	Link-down	DOWN-MEP
F0/3	Ring-Port	FWD	Link-down	DOWN-MEP

Ring2

RPL Owner Priority Unknown

Address

Node ID Priority 32770 (priority 32768 id 2)

Address 00E0.0F81. 111B

Control Vlan 3

Version 1

This node is the interconnection node

RAPS Virtual Channel: True

Revertive Mode: Revertive

State Protection

Signal Fail False Sending SF

WTR time 0/20 sec WTB time 0/6 sec

Guard time 0/500 ms Send time 1/5 sec

Interface	Role	State	Status	MEP Role

F0/7

F0/7

Ring-Port

(up) Ring-Port

FWD

BLK

Link-up

Link-down

DOWN-MEP

UP-MEP

Chapter 102 Loopback Detection Configuration

102.1 Introduction to Loopback Detection

Loopback in the network may cause the equipment repeatedly forward the broadcast, multicast and unknown unicast, resulting in the waste of network resources or the network breakdown. In order to timely inform the user the conditions of the network connection and configuration, a detection mechanism is necessary. So there is the Loopback Detection. It can detect if there is a loopback in the port of the equipment, i.e. forward packets from the port regularly and detect whether the packets are sent back from the forwarding port. If there is a loopback in the port, Loopback Detection will forward the warning information timely to the network management system. Thus, the equipment can avoid long-time off-line. Besides, the equipment supports three modes of port controls: block, no MAC learning, and shutdown (error-disable).

The BDCOM switch supports following characteristics:

- the loopback detection of the port;
- the destination MAC address of the loopback detection packet; the loopback detection packet forwarded by each port can be configured;
- the loopback detection for certain VLANs (at most 10) ;
- the loopback-detection hello-time and loopback-detection recovery-time;
- three modes of port controls: block, no MAC learning, and shutdown (error-disable);
- loopback detection existence configuration.

102.1.1 Format of Loopback Detection Packet

Field	Length/Byte	Value
DMAC	6	0x0180C2B0000A (Default, can be configured)
SMAC	6	MAC address of switch system
TPID	2	0x8100,VLAN tag type
TCI	2	The concrete value of VLAN tag, priority, VLAN ID
TYPE	2	Type: Protocol type, value 0x9001
CODE	2	The subtype of the protocol, represents loopback detection, value 0x0001
VERSION	2	0x0000, reserve at present
Length	2	0x0008, the length of the loopback detection packet head
RESERVE	2	Reserve the field
SYSMAC	6	MAC address of switch system
SEQUENCE	4	Serial number of the packet, it will be automatically generated before forwarding the packet
DiID	4	Port number, 85 Series is all global port numbers
End	2	0x0000 end mark

102.2 Loopback Detection Configuration Task List

- Configuring the global loopback detection
- Configuring the loopback detection of the port
- Configuring the loopback detection for certain VLANs
- Configuring the loopback-detection time

- Configuring the loopback-detection control
- Configuring Loopback Detection Destination MAC
- Configuring loopback detection existence
- Showing loopback detection global configuration information
- Showing loopback detection interface

102.3 Loopback Detection Configuration

102.3.1 Configuring the global loopback detection

Enable or disable the global loopback detection. The global commands are invalid for all physical ports. The loopback detection will take effect only when enabling the global loopback detection. The port configuration is invalid if the loopback detection disables.

Command	Purpose
[no] loopback-detection	Configuring the global loopback detection.

102.3.2 Configuring the loopback detection of the port

This command can be used to enable or disable loopback detection on a specified port. However, this settings takes effect only after loopback detection is enabled globally.

Command	Purpose
[no] loopback-detection enable	Configuring Port Loop Check

102.3.3 Configuring the loopback detection for certain VLANs

After loopback detection is configured on a specified VLAN, the port transmits multiple detection packets of specified VLAN tag regularly and the number of these detection packets transmitted by this port can be up to 10.
Note that: The port must be in the configured VLAN and the VLAN must be created, or the configuration is invalid. Specifically, if the port configures the loopback detection to the trunk mode in VLAN2-VLAN8 and trunk vlan-allowed is VLAN 5-8, packets with 2-4tag from switch cannot be forwarded through the port and the configuration is invalid. Meanwhile, configure trunk vlan-untagged to 2-8, so that the forwarded packets with vlan tag. The relevant VLAN must be created, or the tag with VLAN id will be invalid.

Command	Purpose
[no] loopback-detection vlan-control *vlanlist*	Configuring the loopback detection for certain VLANs

102.3.4 Configure Loopback Detection Time

Command	Purpose
[no] loopback-detection hello-time *time*	Configuring loopback-detection recovery-time

As the network is in change, the loopback detection is a lasting process. The port forwards loopback detection packets regularly. The time interval, i.e. loopback-detection hello-time is 3 seconds in default.

Command	Purpose
[no] loopback-detection recovery-time *time*	Configuring loopback-detection recovery-time

Configure the recovery time after the loopback is disappeared. The loopback is regarded to be disappeared if the port doesn't receive the forwarded loopback detection packet in 10s. It is recommended that the recovery time is at least 3 times of the packet forwarding time and the recovery time is more than 10s than the hello-time.

Command	Purpose
[no] loopback-detection delay-time *delay-time*	Configuring the time period for delaying the execution of controlled actions after a port detects a loop

Configure the delay time, that is, when a loop is detected, if a loop packet is still received after a delay of some seconds, the loop action will be performed, and the corresponding VLAN will be isolated. The smaller the delay time, the better. During the delay period, the loop packets will cause certain damage to the network. The default delay time is 0 second. The delay-time of the higher-level device must be more than the hello time interval of the lower-level device plus the delay-time time interval; the hello time interval of the higher-level device must be no less than the hello time interval of the lower-level device.

102.3.5 Configuring the loopback-detection control

Command	Purpose
[no] loopback-detection control {block|learning|shutdown|isolate-vlan}	Configure loopback detection control

If there is a loopback in the network, control the port by command [no] loopback-detection control. The port has three controlled modes: block, no MAC learning, shutdown (error-disable) and trap. The trap warning information will be forwarded no matter what control mode is configured. The trap configuration is by default.

After loopback detection is enabled globally, the port on which loopback detection is enabled transmits the loopback detection packets and receives the already transmitted loopback detection packets. Four control actions are conducted on the port:

Block: When detecting the loopback, the port will be isolated from other ports and the data forwarded into the port cannot be forwarded to other ports. When the port is in the state of protocol down, the MAC address table will age simultaneously.

Learning: Prohibit port MAC learning. When detecting the loopback, the port will have no MAC learning but the MAC address table ages.

Shutdown: Disable the port. When detecting the loopback, the port forwards trap warning information, ages the MAC address table and automatically disables the port (error-disable). Thus, the port cannot forward the packet until the error-disable-recover time.

Isolate-vlan: When multi-vlan loop detection is performed, if a vlan detects a loop, the vlan will be deleted from the vlan-allowed of the port, and the forwarding of data packets of this vlan is prohibited (the port needs to be configured in trunk

mode).

Trap: The port only report warning. When detect the loopback, the port only reports warning and ages MAC address. The default controlled configuration of the port is trap.

When the port is in block, the packet will not be forwarded into it and the port will continue forward the loopback detection packet. When the loopback disappears in detection, the port will automatically recover. By default, if the forwarded loopback detection packet is not received in 10s, the loopback will be regarded as disappeared.

In block, the port protocol is down; in shutdown, the port link is directly down.

102.3.6 Configuring the Upper Limit of Port Loop Detection Frames

Command	Purpose
[no] **loopback-detection frames-threshold** *frames-threshold*	Configuring the upper limit of the port loop detection frame.

When the control configuration of the port is block and the frame number detection function is enabled, if the received loop detection packet sent by the port is greater than the set frame number threshold, the port will be err-disable shutdown. The system default frame number threshold is 10.

102.3.7 Configuring the frame number detection function of the port

Run the following command to enable or disable frame detection on the specified port.

Command	Purpose
[no] loopback-detection frames-monitor	Configuring the Port Frame Number Detection Function

102.3.8 Configuring Loopback Detection Destination MAC

Command	Purpose
[no] loopback-detection dest-mac *Mac-address*	Configure the loopback detection dest-mac address

The default loopback detection destination mac is 01-80-C2-00-00-0a. If the user has configured, the MAC address configured by the user will be taken as the destination mac address.

102.3.9 Configuring loopback detection existence

Command	Purpose
[no] loopback-detection existence	Configuring loopback detection existence

This command is mainly used to solve the problem that loopback exists on a port or not when this port is up and its loopback detection function takes effect. When the controlled action of this port is set to shutdown, it is improper to regard that loopback exists on this port for a shutdown port has already not forwarded packets. There is no loopback by

default.

102.3.10 Configuring to prohibit forwarding of looped packets on port

Command	Purpose
[no] loopback-detection forbid-packet	Configuring whether to prohibit forwarding of all loopback-detect packets on this port

Configure to prohibit forwarding of all loopback-detect packets on this port, to prevent broadcast storms caused by looped packets.

102.3.11 Configuring Isolated VLAN Recovery on port

Command	Purpose
loopback-detection vlan-recovery	Configuring to recover the isolated vlan of a port in isolate-vlan mode.

In the isolate-vlan mode, run this command to release the VLAN that is isolated due to the detection of a loop.

102.3.12 Showing loopback detection global configuration information

Command	Purpose
show loopback-detection	Show global loopback detection configuration

It is mainly used for showing global loopback detection information, including global configuration, loopback existence and some configuration information.

102.3.13 Showing loopback detection interface

Command	Purpose
show loopback-detection interface *intf*	Show loopback detection interface

It is mainly used for showing loopback detection information, including the timer value and the packet information.

102.4 Configuration Example

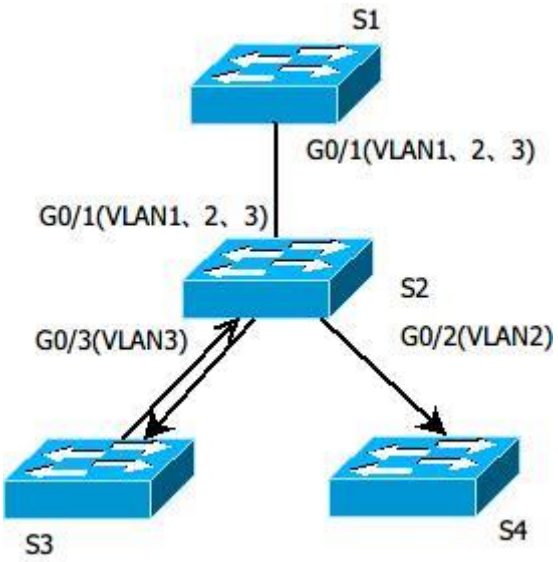


Figure 1.1 Loopback Detection Configurations

As shown in Figure 1.1, port switch S1 designates loopback detection of certain VLAN (1,2,3):

Switch S1:

Configure interface GigaEthernet0/1:

switchport trunk vlan-untagged 1-3

switchport mode trunk

loopback-detection enable

loopback-detection control block

loopback-detection vlan-control 1-5

Global Configuration:

loopback-detection

vlan 1-3

Switch S2:

Configure interface GigaEthernet0/1:

switchport mode trunk

Configure interface GigaEthernet0/2:

switchport mode trunk

Configure interface GigaEthernet0/3:

switchport mode trunk

Global Configuration:

vlan1-3

Switch S3:

Configure interface GigaEthernet0/1:

switchport pvid 3

If S3 has loopback and PVID of the port is 3, the packets will forward back to G0/1 of S1. S1 will block G0/1 if there is

loopback.

Chapter 103 MAD Configuration

103.1 MAD Overview

A virtualized link failure will cause a virtualized domain to split into two virtualized domains. The two virtualized domains have the same MAC address and IP address, which will cause address conflicts and network shocks. In order to improve the stability of the system, when the virtualized domain is split, a mechanism is needed to detect that two virtualized domains exist at the same time, and perform corresponding processing to minimize the impact on the business. MAD (Multi-Active Detection) is such a detection and processing mechanism.

After MAD detects that there are dual masters, it shuts down all common service ports in one of the virtualized domains.

103.2 MAD Configuration Task List

- LACP MAD Configuration

103.3 MAD Configuration Task

103.3.1 LACP MAD Configuration

LACP MAD needs to use an auxiliary device that supports Multi-Active Relay to aggregate with the active and standby devices in the virtualization domain.

Under the aggregation port on the virtualization device, use the following command to enable the LACP MAD function:

Command	Purpose
multi-active-detection	Enable LACP MAD detection function

Under the aggregation port on the auxiliary device, use the following command to enable the LACP Multi-Active Relay function:

Command	Purpose
multi-active-relay	Enable LACP Multi-Active Relay detection function

Chapter 104 RNP Configuration

104.1 RNP Overview

RNP (Role Negotiation Protocol) is mainly used for negotiating the role of each member device in the virtualization domain. The role of the device plays in the virtualization domain can be divided into three: global master device, global backup device and standby device.

104.2 RNP Configuration Task List

- Configuring the timeout of the RNP old master device
- Monitoring RNP State

104.3 RNP Configuration Tasks

104.3.1 Configuring the timeout of the RNP old master device

To configure the timeout period of the RNP old master device, run the following commands in virtualization configuration mode:

Command	Purpose
bvss rnp old-master-timeout *value*	Configures the timeout of the RNP old master device
no bvss rnp old-master-timeout	Restore the timeout of the RNP old master device to the default value (3 minutes)

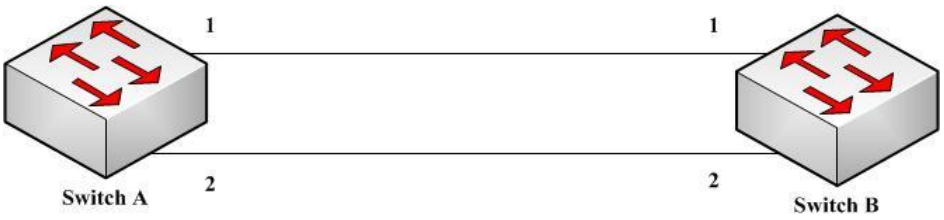
104.3.2 Monitoring RNP State

To monitor SNP configuration and SNP's state, run the following commands in EXEC mode:

Command	Purpose
show bvss rnp	The command is used to show RNP state information.

104.4 Configuration Example

As shown in the following figure, Switch A and Switch B constitute a virtualization domain. Ports G1/0/1 and G1/0/2 on Switch A are connected with G1/0/1 and G1/0/2 respectively on Switch B. Ports G1/0/1 and G1/0/2 on Switch A belong to the virtualization link group 1 and G1/0/1 and G1/0/2 on Switch B belong to the virtualization link group 2.



The settings are shown as follows:

1). Configuring the virtualization mode of Switch A

Switch_config_bvss# bvss mode normal

2). Configuring the virtualization domain of Switch A

Switch_config_bvss# bvss domain-id 1

3). Configuring the member ID of Switch A on the virtualization domain.

Switch_config_bvss# bvss member-id 1

4). Configuring the virtualization port on Switch A.

Switch_config_bvss# bvss interface 1 slot 0 port 1 group 1

Switch_config_bvss# bvss interface 2 slot 0 port 2 group 1

5). Configuring the virtualization mode of Switch B

Switch_config_bvss# bvss mode normal

6). Configuring the virtualization domain of Switch B

Switch_config_bvss# bvss domain-id 1

7). Configuring the member ID of Switch B on the virtualization domain.

Switch_config_bvss# bvss member-id 2

8). Configuring the virtualization port of Switch B.

Switch_config_bvss# bvss interface 1 slot 0 port 1 group 2

Switch_config_bvss# bvss interface 2 slot 0 port 2 group 2

Chapter 105 SGNP Configuration

105.1 SGNP Overview

SGNP (SL Group Negotiation Protocol) is mainly used for negotiating the member ports of the virtualization link group between two devices.

There are 2 virtual link groups: Group 1 and Group 2. The port can become a member port of the virtual link group only after configuring the corresponding virtual link group for the port.

Every virtualization device can connect to another one only through the virtualization link group. When two virtualization member devices are connected, the virtualization link groups which the virtualization link corresponds to cannot be the same.

105.2 SGNP Configuration Task List

- Configuring the timeout period of SGNP neighbors
- Monitoring SGNP configuration and status

105.3 SGNP Configuration Tasks

105.3.1 Configuring the timeout period of SGNP neighbors

To configure the timeout period of SGNP neighbors, run the following command in the virtualization configuration mode:

Command	Purpose
bvss sgnp neighbor-timeout *value*	Configures the timeout period for SGNP neighbors
no bvss sgnp neighbour-timeout	Restores SGNP neighbor timeout to default (3 seconds)

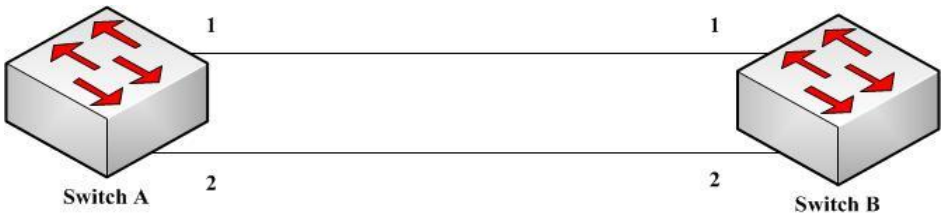
105.3.2 Monitoring SGNP configuration and status

For monitoring the configuration and status of SGNP, run the following command in the management mode:

Command	Purpose
show bvss sgnp	Show SGNP configuration and status information

105.4 Configuration Example

As shown in the following figure, Switch A and Switch B constitute a virtualization domain. Ports G1/0/1 and G1/0/2 on Switch A are connected with G1/0/1 and G1/0/2 respectively on Switch B. Ports G1/0/1 and G1/0/2 on Switch A belong to the virtualization link group 1 and G1/0/1 and G1/0/2 on Switch B belong to the virtualization link group 2.



The settings are shown as follows:

1). Configuring the virtualization mode of Switch A

Switch_config_bvss# bvss mode normal

2). Configuring the virtualization domain of Switch A

Switch_config_bvss# bvss domain-id 1

3). Configuring the member ID of Switch A on the virtualization domain.

Switch_config_bvss# bvss member-id 1

4). Configuring the virtualization port on Switch A.

Switch_config_bvss# bvss interface 1 slot 0 port 1 group 1

Switch_config_bvss# bvss interface 2 slot 0 port 2 group 1

5). Configuring the virtualization mode of Switch B

Switch_config_bvss# bvss mode normal

6). Configuring the virtualization domain of Switch B

Switch_config_bvss# bvss domain-id 1

7). Configuring the member ID of Switch B on the virtualization domain.

Switch_config_bvss# bvss member-id 2

8). Configuring the virtualization port on Switch B.

Switch_config_bvss# bvss interface 1 slot 0 port 1 group 2

Switch_config_bvss# bvss interface 2 slot 0 port 2 group 2