# L3-switch CLI management manual

# The Directory

L3-switch CLI management manual ..... 1
The Directory ..... 1
Chapter 1 CLI Command-Line Introduction ..... 18
1.1 Access the CLI of the switch ..... 19
1.1.1 The user accesses The CLI through The Console port ..... 19
1.1.2 The USER accesses the CLI through TELNET ..... 20
1.2 Introduction to CLI patterns ..... 21
1.2.1 The role of the CLI pattern ..... 21
1.2.2 Identification of CLI patterns ..... 22
1.2.3 Classification of CLI patterns ..... 23
1.3 Command syntax Introduction ..... 1
1.3.1 commands ..... 1
1.3.2 The parameter types ..... 1
1.3.3 Command syntax rule ..... 1
1.3.4 Command abbreviations ..... 3
1.3.5 Grammar help ..... 3
1.3.6 Command line error message ..... 4
1.4 Command line shortcuts ..... 5
1.4.1 Line edit shortcut key ..... 5
1.4.2 Displays command shortcuts ..... 6
1.5 The history command ..... 6
Chapter 1 CLI Command-Line Introduction ..... 7
1.6 Access the CLI of the switch ..... 7
1.6.1 The user accesses The CLI through The Console port ..... 8

1.6.2 The USER accesses the CLI through TELNET ..... 9
1.7 Introduction to CLI patterns ..... 11
1.7.1 The role of the CLI pattern ..... 11
1.7.2 Identification of CLI patterns ..... 11
1.7.3 Classification of CLI patterns ..... 12
1.8 Command syntax Introduction ..... 15
1.8.1 commands ..... 15
1.8.2 The parameter types ..... 15
1.8.3 Command syntax rule ..... 16
1.8.4 Command abbreviations ..... 18
1.8.5 Grammar help ..... 18
1.8.6 Command line error message ..... 19
1.9 Command line shortcuts ..... 20
1.9.1 Line edit shortcut key ..... 20
1.9.2 Displays command shortcuts ..... 21
1.10 The history command ..... 22
Chapter 4 Configure port-based security ..... 23
1.11 Introduction to the ..... 23
1.12 MAC binding configuration ..... 24
1.13 MAC filter configuration ..... 26
1.14 Port learning limit configuration ..... 27
1.15 Secure port configuration ..... 28
1.15.1 Introduction to Protection port ..... 28
1.15.2 Secure port configuration ..... 29
Chapter 5 Configure port IP to bind to MAC ..... 31
1.16 Introduction to the ..... 32

1.17 IP and MAC binding configuration.....33
1.18 Configuration of the sample.....34
1.19 Configuration misarrangement.....37
Chapter 6 Port loop detection.....38
1.20 Introduction to the.....38
1.21 The agreement principle.....38
1.21.1 Testing process.....38
1.21.2 Recovery mode.....39
1.21.3 Security agreement.....39
1.22 Configuration is introduced.....40
1.22.1 Global configuration.....40
1.22.2 Interface configuration.....41
1.22.3 According to the configuration.....41
Chapter 7 Configuration VLAN.....42
1.23 VLAN is introduced.....43
1.23.1 The benefits of vlans.....43
1.23.2 VLAN ID.....45
1.23.3 VLAN port member types.....46
1.23.4 Default VLAN for ports.....46
1.23.5 VLAN mode for the port.....47
1.23.6 VLAN trunking.....47
1.23.7 The forwarding of a data stream within a VLAN.....48
1.24 VLAN configuration.....51
1.24.1 Create and delete vLAns.....51
1.24.2 Configure the VLAN mode for the port.....52
1.24.3 VLAN configuration in ACCESS mode.....54

1.24.4 VLAN configuration for TRUNK mode ..... 54
1.24.5 VLAN configuration for HYBRID mode ..... 56
1.24.6 View the VLAN information ..... 58
1.25 VLAN configuration example ..... 59
1.25.1 Port-based VLAN ..... 59
1.25.2 VLAN based on 802.1Q ..... 61
1.26 MAC, IP subnet, protocol VLAN ..... 65
1.26.1 MAC, IP subnet, protocol VLAN introduction ..... 65
1.26.2 MAC, IP subnet, protocol VLAN configuration ..... 65
1.27 Voice VLAN ..... 68
1.27.1 Voice VLAN is introduced ..... 68
1.27.2 Voice VLAN configuration ..... 69
1.27.3 Voice VLAN configuration example ..... 71
1.28 A VLAN map ..... 72
1.28.1 An introduction to VLAN mapping ..... 72
1.28.2 VLAN mapping configuration ..... 72
1.29 QinQ ..... 73
1.29.1 Qinq introduction ..... 73
1.29.2 Qinq configuration ..... 76
1.29.3 Qinq configuration example ..... 77
Chapter 8 To configure QoS ..... 80
1.30 QoS is introduced ..... 81
1.30.1 Cosine based QoS ..... 83
1.30.2 QoS based on DSCP ..... 84
1.30.3 QoS based on MAC ..... 84
1.30.4 Policy based QOS ..... 84

1.31 QoS configuration ..... 85
1.31.1 Default configuration for QoS ..... 85
1.31.2 Configuration scheduling mode ..... 87
1.31.3 Configuring queue weights ..... 87
1.31.4 Configure the mapping relationship between DSCP and QosProfile ..... 88
1.31.5 Configure ports based on DSCP QoS ..... 88
1.31.6 Configure port user priority (COS value) ..... 89
1.32 QoS configuration example ..... 89
1.33 Example of policy QoS configuration ..... 90
Chapter 9 Configuration of MSTP ..... 92
1.34 MSTP is introduced ..... 92
1.34.1 An overview of the ..... 92
1.34.2 Multiple spanning tree domain ..... 93
1.34.3 IST, CIST, and CST ..... 93
1.34.4 Field operations ..... 94
1.34.5 Inter-domain operation ..... 95
1.34.6 Hop count ..... 96
1.34.7 The border port ..... 97
1.34.8 Interoperability between MSTP and 802.1D STP ..... 97
1.34.9 Port role ..... 98
1.34.10 802.1d Spanning tree introduction ..... 101
1.35 MSTP configuration ..... 104
1.35.1 The default configuration ..... 104
1.35.2 General configuration ..... 105
1.35.3 Domain configuration ..... 109
1.35.4 The instance configuration ..... 110

1.35.5 Port configuration ..... 110
1.35.6 PORTFAST related configuration ..... 115
1.35.7 Root Guard related configuration ..... 118
1.36 MSTP configuration example ..... 119
Chapter 10 Configuration ERPS ..... 121
1.37 Summary of ERPS ..... 121
1.38 Introduction to ERPS technology ..... 121
1.38.1 ERPS ring ..... 121
1.38.2 ERPS node ..... 122
1.38.3 Links and Channels ..... 123
1.38.4 ERPS VLAN ..... 123
1.39 How ERPS works ..... 124
1.39.1 The normal state ..... 124
1.39.2 Link failures ..... 124
1.39.3 Link to restore ..... 125
1.40 ERPS technical features ..... 126
1.40.1 ERPS load balancing ..... 126
1.40.2 Good safety ..... 127
1.40.3 Support multi - ring intersection tangent ..... 128
1.41 ERPS protocol command ..... 128
1.42 Typical ERPS applications ..... 132
1.42.1 As single sample ..... 132
1.42.2 Polycyclic sample ..... 138
1.42.3 Multi-instance load balancing example ..... 147
Chapter 11 Configuration of AAA ..... 161
1.43 802.1 x introduces ..... 162

1.43.1 802.1X equipment composition ..... 163
1.43.2 Protocol Package Introduction ..... 164
1.43.3 Protocol flow interaction ..... 166
1.43.4 802.1X port status ..... 168
1.44 The RADIUS is introduced ..... 170
1.44.1 Protocol Package Introduction ..... 171
1.44.2 Protocol flow interaction ..... 172
1.44.3 User verification method ..... 174
1.45 The configuration of 802.1 x ..... 175
1.45.1 802.1x default configuration ..... 176
1.45.2 Start and close 802.1x ..... 177
1.45.3 Configure 802.1x port status ..... 177
1.45.4 Configure the recertification mechanism ..... 179
1.45.5 Configure the maximum number of port access hosts ..... 179
1.45.6 Configure interval times and number of retransmissions ..... 180
1.45.7 Configure ports as transport ports ..... 181
1.45.8 Configure the 802.1x client version number ..... 182
1.45.9 Whether the configuration checks the client version number ..... 182
1.45.10 Configuration authentication method ..... 183
1.45.11 Configure whether to check client timing packages ..... 183
1.45.12 Displays 802.1x information ..... 184
1.46 Configure the RADIUS ..... 184
1.46.1 RADIUS default configuration ..... 185
1.46.2 Configure the IP address of the authentication server ..... 185
1.46.3 Configure Shared keys ..... 186
1.46.4 Start and close billing ..... 186

1.46.5 Configure RADIUS port and property information ..... 187
1.46.6 Configure RADIUS roaming function ..... 188
1.46.7 Display RADIUS information ..... 188
1.47 Configuration of the sample ..... 189
Chapter 12 GMRP configuration ..... 190
1.48 GMRP introduction ..... 191
1.49 Configuration GMRP ..... 191
1.49.1 Turn on the GMRP Settings ..... 192
1.49.2 View the GMRP information ..... 192
1.50 Examples of typical GMRP configurations ..... 193
Chapter 13 IGMP SNOOPING configuration ..... 195
1.51 IGMP SNOOPING is introduced ..... 196
1.51.1 IGMP SNOOPING Process ..... 196
1.51.2 Layer 2 dynamic multicast ..... 198
1.51.3 Join a group ..... 198
1.51.4 Leave a group ..... 201
1.51.5 IGMP finder ..... 202
1.51.6 Igmp Snooping Group Playback filtering ..... 203
1.52 IGMP SNOOPING configuration ..... 203
1.52.1 IGMP SNOOPING Default configuration ..... 203
1.52.2 Open and close IGMP SNOOPING ..... 204
1.52.3 Configured survival time ..... 205
1.52.4 The configuration of fast - leave ..... 205
1.52.5 Configuration MROUTER ..... 206
1.52.6 Configure the IgMP Snooping Query port function ..... 207
1.52.7 Configure the IgMP Snooping Query function ..... 207

1.52.8 Configure igMP Snooping Group playback filtering ..... 207
1.52.9 According to the information ..... 208
1.53 Sample IGMP SNOOPING configuration ..... 209
1.53.1 configuration ..... 209
Chapter 14 MVR configuration ..... 211
1.54 Introduction of MVR ..... 212
1.55 Configure the MVR ..... 212
1.56 MVR configuration example ..... 214
Chapter 15 Configure the DHCP SNOOPING ..... 216
1.57 DHCP SNOOPING is introduced ..... 216
1.57.1 The DHCP SNOOPING process ..... 217
1.57.2 DHCP SNOOPING Binding Table ..... 218
1.57.3 DHCP SNOOPING specifies the physical port of the linked server ..... 219
1.58 DHCP SNOOPING configuration ..... 220
1.58.1 DHCP SNOOPING Default configuration ..... 220
1.58.2 Global open and close DHCP SNOOPING ..... 220
1.58.3 Interface open and close DHCP SNOOPING ..... 221
1.58.4 Interface open and close DHCP SNOOPING OPTION82 ..... 221
1.58.5 According to the information ..... 222
1.59 Example DHCP SNOOPING configuration ..... 223
1.59.1 configuration ..... 223
1.60 Configuration error for DHCP SNOOPING ..... 225
Chapter 16 The DHCP CLIENT configuration ..... 227
1.61 The DHCP CLIENT to introduce ..... 227
1.62 The DHCP CLIENT configuration ..... 227
Chapter 17 Configure the DHCP RELAY ..... 229

1.63 The DHCP RELAY is introduced.....230
1.64 The DHCP RELAY configuration.....231
1.64.1 Start the DHCP-Relay function of the interface.....232
1.64.2 According to the information .....232
1.65 DHCP RELAY configuration example .....232
Chapter 18 Configure the DHCP SERVER.....235
1.66 The DHCP SERVER is introduced .....236
1.67 The DHCP SERVER configuration.....237
1.67.1 Start the global DHCP Server function .....238
1.67.2 Start interface to receive DHCP Server message .....239
1.67.3 Configure address pool .....239
1.67.4 Configure the address pool scope .....240
1.67.5 Configure the address pool net mask .....240
1.67.6 Configure the address pool lease.....240
1.67.7 Configure the address pool default gateway .....241
1.67.8 Configure the address pool DNS server.....241
1.67.9 Configure the address pool to manually exclude addresses .....242
1.67.10 Configuration OPTION82.....243
1.67.11 Clears the assigned address table entry .....243
1.67.12 Clears the detected conflicting address table entries.....244
1.68 DHCP SERVER configuration example .....244
Chapter 19 Configure an ACL .....248
1.69 Introduction to ACL repository.....248
1.70 Introduction to ACL filtering .....251
1.71 ACL repository configuration .....253
1.72 Timetime-based ACLs.....258

1.73 ACL filtering configuration ..... 262
1.74 Example ACL configuration ..... 263
1.75 ACL configuration error ..... 264
Chapter 20 Basic TCP/IP configuration ..... 266
1.76 Configure the VLAN interface ..... 267
1.77 Configure the ARP ..... 270
1.77.1 Configure static ARP ..... 271
1.77.2 View ARP information ..... 272
1.78 Configure static routing ..... 273
1.79 TCP/IP Basic configuration example ..... 277
1.79.1 Three layer interface ..... 277
1.79.2 Static routing ..... 278
1.79.3 ARP ..... 279
Chapter 21 Configure SNMP ..... 280
1.80 SNMP introduce ..... 281
1.81 The SNMP configuration ..... 283
1.82 SNMP Configuration Example ..... 286
1.82.1 configuration ..... 286
Chapter 22 RMON configuration ..... 287
1.83 RMON introduction ..... 287
1.84 RMON configuration ..... 288
1.85 RMON configuration example ..... 292
Chapter 23 The cluster configuration ..... 294
1.86 Cluster Management Introduction ..... 295
1.86.1 The cluster definition ..... 295
1.86.2 The cluster character ..... 296

1.86.3 Introduction of NDP.....298
1.86.4 NTDP profile.....298
1.86.5 Cluster management and maintenance.....300
1.86.6 The management vlan.....304
1.87 Cluster configuration Introduction.....304
1.88 Configuration management equipment.....306
1.88.1 Enable NDP functionality for systems and ports.....306
1.88.2 Configure the NDP parameters.....307
1.88.3 Enable NTDP functionality for systems and interfaces.....308
1.88.4 Configure NTDP parameters.....309
1.88.5 Configure to collect NTDP information manually.....310
1.88.6 Enable clustering functionality.....310
1.88.7 Set up the cluster.....310
1.88.8 Configure cluster internal member interactions.....314
1.88.9 Configure cluster member management.....315
1.89 Configure member devices.....316
1.89.1 Enable NDP functionality for systems and ports.....316
1.89.2 Enable NTDP functionality for systems and ports.....316
1.89.3 Configure to collect NTDP information manually.....316
1.89.4 Enable clustering functionality.....316
1.90 Configure access to cluster members.....316
1.91 Cluster management display and maintenance.....317
1.92 Example of a typical cluster management configuration.....318
Chapter 24 SNTP configuration.....323
1.93 SNTP is introduced.....324
1.94 Configuration SNTP.....325

1.94.1 Default SNTP Settings ..... 325
1.94.2 Configure the SNTP Server address ..... 326
1.94.3 Configure the interval for the SNTP synchronization clock ..... 327
1.94.4 Configure the local time zone ..... 327
1.95 SNTP information display ..... 328
Chapter 25 Configure RIP ..... 329
1.96 RIP is introduced ..... 330
1.97 RIP configuration ..... 331
1.97.1 Start RIP and enter RIP configuration mode ..... 332
1.97.2 Enabled RIP interface ..... 333
1.97.3 Distribution list broadcast text transmission ..... 334
1.97.4 Configure the working state of the interface ..... 334
1.97.5 Configure the default routing weight ..... 335
1.97.6 Configuration management distance ..... 336
1.97.7 Configuration timer ..... 337
1.97.8 Configure version ..... 337
1.97.9 Introduce external routing ..... 338
1.97.10 Configure routing filtering ..... 339
1.97.11 Configure additional routing weights ..... 340
1.97.12 Configure the RIP version of the interface ..... 341
1.97.13 Configure the transceiver state of the interface ..... 342
1.97.14 Configure horizontal segmentation ..... 343
1.97.15 Message authentication ..... 344
1.97.16 Configure interface weights ..... 346
1.97.17 According to the information ..... 346
1.98 RIP configuration example ..... 347

Chapter 26 Configure OSPF ..... 350
1.99 OSPF is introduced ..... 351
1.100 OSPF configuration ..... 353
1.100.1 Start OSPF and enter OSPF mode ..... 355
1.100.2 Can make the interface ..... 356
1.100.3 Specify the host ..... 357
1.100.4 Configure router ID ..... 358
1.100.5 Configure the adjacency points ..... 359
1.100.6 Prohibit the interface from sending messages ..... 360
1.100.7 Configure SPF calculation time ..... 361
1.100.8 Configuration management distance ..... 362
1.100.9 Introduce external routing ..... 363
1.100.10 Configure the network type of the interface ..... 365
1.100.11 Configure the hello message dispatch time interval ..... 366
1.100.12 Configure the neighbor router outage time ..... 367
1.100.13 Configure the retransmission time ..... 368
1.100.14 Configure interface delay ..... 369
1.100.15 Configure the priority of the interface in the DR election ..... 370
1.100.16 The cost of sending a message on the configuration interface ..... 371
1.100.17 Configure whether the INTERFACE sends A DD message to fill an MTU field ..... 372
1.100.18 Configure interface message authentication ..... 372
1.100.19 Configure zone virtual links ..... 374
1.100.20 Configure zone routing aggregation ..... 376
1.100.21 Configure area message authentication ..... 377
1.100.22 Configuring stub areas ..... 378
1.100.23 Configure the NSSA region ..... 378

1.100.24 Configure external routing aggregation ..... 379

1.100.25 Configure default weights for external routes ..... 380

1.100.26 According to the information ..... 380

1.101 OSPF configuration example ..... 382

Chapter 27 Configuration VRRP ..... 385

1.101.1 VRRP terminology ..... 389

1.101.2 Election of virtual master routers ..... 397

1.101.3 Status of virtual routers ..... 399

1.101.4 VRRP Tracking ..... 402

1.102 VRRP Configuration ..... 404

1.102.1 Create and delete virtual routers ..... 404

1.102.2 Configure virtual IP addresses for virtual routers ..... 405

1.102.3 Configure parameters for virtual routers ..... 406

1.102.4 Configuration VRRP tracking ..... 408

1.102.5 Launch and close virtual routers ..... 410

1.102.6 View VRRP information ..... 411

1.103 VRRP Configuration examples ..... 411

Chapter 28 Configuration VLLP ..... 415

1.104 VLLP Introduction ..... 416

The ports involved in VLLP protocol message interaction need to be configured as VLLP ports within the vlan that started the VLLP protocol. VLLP ports can be valid tier 2 ports (including trunk groups), but members of the trunk are not allowed to be configured as VLLP ports. VLLP protocol messages are sent and received via VLLP ports. The VLLP ports and the VLLP ports configured within the vlan that initiate the VLLP protocol accordingly constitute a pair of mapping relationships, which are determined by sending a query message to receive a reply message or changing the message mapping relationship, and according to this mapping relationship and its own link state to calculate the possible existence of the loop in the network, according to the VLLP port state determination principle to maintain the STP state of the port, thus blocking the loop in the topology. ..... 422

Multiple VLLP ports can be started within the vlan where the VLLP protocol is started, which may or may not be physically linked to the peer switch. the same VLLP port also appears in multiple VLLP devices when the port belongs to multiple vlan. The VLLP council dynamically collects information VLLP port link state changes and STP state to the end VLLP port to calculate the loop in time and effectively prevent the network loop.....422

When there are multiple vlan, whose inner port configuration is completely consistent, but the VLLP protocol needs to be started on multiple vlan, each layer 2 port needs to send and receive multiple VLLP protocol messages running on different vlan, which causes the switch burden. that is, the port configuration is exactly the same vlan, running the VLLP protocol on only one vlan, i.e., the main vlan, while the rest is added on the instance of the main vlan as a subsidiary. Write the inner port state of the instance by the result of the loop calculated by VLLP protocol on the main vlan. Note that, when configuring the accessory vlan, ensure that the VLLP ports of the main vlan are within the accessory vlan and that all ports of the accessory vlan are within the primary. when the attached vlan, is configured to add a second layer port to the attached vlan, if the port is also in the main vlan, the port state is uniformly managed by the main vlan; if the port is not in the main vlan, the port state can not be managed, prompting alarm information.423

1.105 28.2 VLLP configuration .....423

1.105.1 Create vllp devices on the three-tier interface.....424

1.105.2 Enable vllp equipment.....424

1.105.3 Create vllp ports on tier 2 interfaces .....425

1.105.4 Configuration vllp Device Priority.....425

1.105.5 Configuration vllp Device Query Timer Interval .....426

1.105.6 Configuration vlan .....427

1.105.7 Configuration vllp Port Priority .....427

1.105.8 Display information .....428

1.106 VLLP Configuration examples .....429

Chapter 29 Configuration Policy Routing.....433

1.107 Introduction of Strategy Routing .....434

1.108 Policy Routing Configuration .....434

1.108.1 Create new policy routing .....434

1.108.2 Insert a policy route ..... 435

1.108.3 Delete a policy route ..... 436

1.108.4 Moving a Policy Route ..... 436

1.108.5 View Policy Routing Information ..... 437

1.109 Policy Routing Configuration Example ..... 437

Chapter 30 Configure the system log ..... 438

1.110 System Log Introduction ..... 439

1.110.1 The format of the log information ..... 439

1.110.2 Log storage ..... 442

1.110.3 Display of logs ..... 443

1.110.4 Debugging tool ..... 444

The debugging tool provides rich switches that enable administrators to track content of interest by controlling these switches.When abnormalities occur to the device or network, the administrator can turn on debugging switch related to the abnormality and find out the problem by tracking the execution process of the system and module. ..... 444

When this switch is turned on, the system generates logging information that is written to the corresponding log table.In general, the priority of logging produced by debugging is a anteage.When the terminal real-time display switch is on, the log information will be output to the terminal in real time.The system does not generate the associated logging information when the debugging switch is turned off. ..... 444

30.2 System log configuration ..... 444

1.110.5 Configure the terminal real-time display switch ..... 445

1.110.6 Set the log level ..... 446

1.110.7 View log information ..... 446

1.110.8 Configuring debugging switch ..... 447

1.110.9 To view the debugging information ..... 450

1.111 Configuration SYSLOG ..... 451

1.111.1 SYSLOG introduce ..... 451

1.111.2 SYSLOG configuration ..... 452

1.111.3 SYSLOG Configuration of the sample ..... 453

# Chapter 1 CLI Command-Line Introduction

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

- Access the CLI of the switch
- The Introduction to the CLI patterns
- The Command syntax;
- The Command line shortcuts
- The history command

## 1.1 Access the CLI of the switch

The CLI Command line interface of The switch provides The user-managed switch interface.Users can access The CLI Command line interface of The switch through The Console and Telnet Terminals,Which are brilliant below.

### 1.1.1 The user accesses The CLI through The Console port

The operation Steps are as follows:

Connect the serial port of PC to Console the switch by configuring cable.

Step 2:Start the terminal Emulator on PC (such as the Super terminal of Windows,(Configure the communication parameters of the terminal emulator.The communication parameters of the terminal are configured as follows:

Baud rate: 38400 or 115200

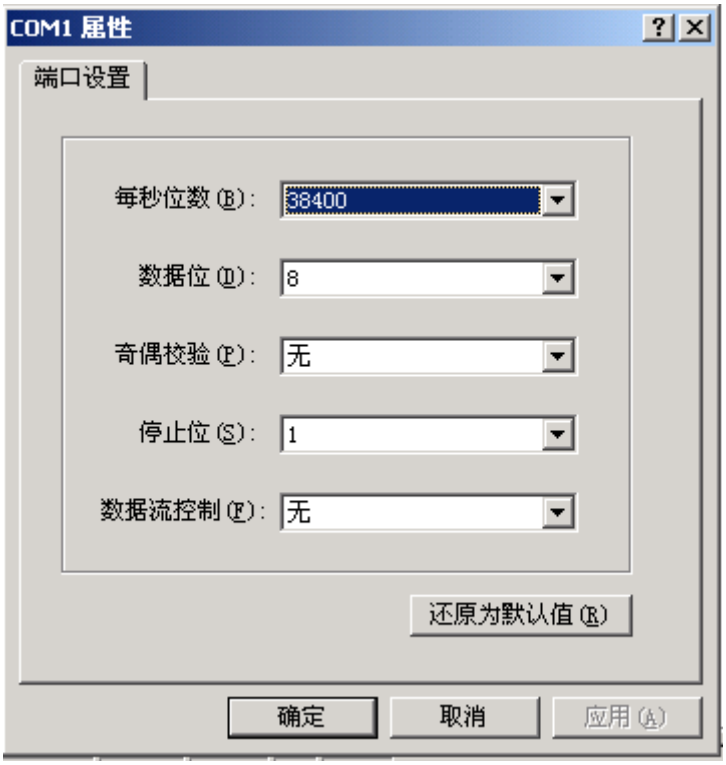
Data bits: 8

Parity: None

Stop bits: 1

The Data flow control: None

The Communication Parameter Configuration of The super terminal is as follows:




Step 3: start the Switch. After the Switch is started, the CLI prompt (default is Switch>) will be displayed on the terminal. The user can enter a command at this prompt, so that the user can access the CLI of the Switch.

### 1.1.2 The USER accesses the CLI through TELNET

Users can access the switch through its port.

The default IP address of the port of the switch is 192.168.0.1 (note: the actual product shall prevail). The operation steps of accessing the switch through the port are as follows:

Step 1: Connect the Ethernet port of the PC to the port of the switch over an Ethernet cable.

Step 2: Set the IP address of the PC's Ethernet port, which must be within 192.168.0.0/24 (e.g. 192.168.0.100). Ping 192.168.0.1 to determine the PC and switch connectivity.

Step 3: If the PC and the switch are connected, Telnet 192.168.0.1 enters the Telnet terminal interface. The diagram below:


Step 4: if the system does not set the password, the Telnet interface directly enters CLI, and the CLI prompt appears (default is Switch>); If the system has a password, you need to enter the password on the Telnet interface to enter the CLI.

There are two points to note in particular:

- The IP address of the switch port is built on the VLAN three-layer interface. Before accessing the switch, the IP address of a VLAN interface must be set. The default IP address of VLAN1 is 192.168.0.1 (note: it depends on the actual product), which can be used directly.The IP address of the VLAN interface can be configured through the Console port.
- The user accesses the switch via port, and can connect the PC and port directly via Ethernet cable, or through a network, as long as the PC and a VLAN of the switch can be intercommunicated.

## 1.2 Introduction to CLI patterns

### 1.2.1 The role of the CLI pattern

The role of CLI model is mainly as follows:

- Facilitate user classification and prevent unauthorized use of CLI.

Users can be divided into two levels, namely two categories: ordinary users and privileged users.

Ordinary users can only view some of the running state of the switch and can only use the display command.

In addition to being able to see the running state of the switch, privileged users can also maintain and configure the switch and change its behavior.

- Convenient for users to configure the switch

There are many configurations for switches, and it is very inconvenient for users to use them all in one mode. To this end, multiple patterns are established on CLI and similar commands are put into one pattern, which is easy for users to understand and use. For example, vLAn-related commands are placed in VLAN configuration mode and interface-related commands are placed in interface configuration mode.

### 1.2.2 Identification of CLI patterns

CLI prompt is the identity of CLI mode. When using CLI, users can know the CURRENT CLI mode by looking at the CLI prompt.

The CLI prompt consists of two parts, one that identifies the host and the other that identifies the schema.

The host part of the CLI prompt USES the system's host name, which is configurable and defaults to Switch, so the CLI prompt defaults to Switch, and the CLI descriptor mentioned later generally USES the default host name.

The pattern part of the CLI prompt is not configurable, and each pattern has its own corresponding pattern string, some of which are fixed and some of which are mutable. For example, the pattern string of VLAN configuration mode is fixed, while the pattern string of interface configuration mode is mutable.

Such as:

The CLI prompt Switch# identifies the privileged mode, Switch identifies the host, and

# identifies the mode.

The CLI prompt Switch(config-ge1/1)# identifies the interface configuration pattern and is configured with port GE1/1, Switch identifies the host, and (config-ge1/1)# identifies the pattern.

The CLI prompt Switch(config-vlan2)# identifies the interface configuration pattern, and the vLAN2 interface is configured, the Switch identifies the host, and (config-vlan2)# identifies the pattern.

## 1.2.3 Classification of CLI patterns

CLI patterns fall into four categories: general pattern, privileged pattern, global configuration pattern, and configuration subpattern, which consists of many CLI patterns.

Ordinary users can only access the ordinary mode, and privileged users can access all CLI modes.

The Console and Telnet terminals enter normal mode first, and enter privilege mode after entering enable command and successfully verifying password in normal mode. On the Telnet terminal, ordinary users can only stay in normal mode and cannot enter privileged mode. Enter Configure Terminal in privilege mode, and enter CLI mode into global configuration mode. Enter the relevant commands in global configuration mode to enter each configuration submode.

The following table lists the major CLI patterns for switches:

| model | describe | prompt | Enter mode commands | Exit mode command |
|---|---|---|---|---|
| Normal mode | Provides display command to view the status information of the switch. | The Switch > | The first mode that the terminal enters. | There is no exit mode command on the Console terminal, and exit or quit commands are used on the Telnet terminal to |

| | | | | |
|---|---|---|---|---|
| | | | | exit the Telnet terminal. |
| Privileged mode | n addition to providing display command to view the status information of the switch, it also provides commands such as debugging, version upgrading and configuration maintenance. | Switch# | Enter the enable command in normal mode. | Use the disable command to fall back into normal mode.<br>Use the exit or Quit command to exit normal mode on the Console terminal and exit or quit the Telnet terminal on the Telnet terminal. |
| Global configuration mode | Provides generic commands that cannot be implemented within a configuration subpattern, such as configuring static routing commands. | The Switch # (config) | Enter the configure Terminal command in privilege mode. | Exit to privileged mode using the exit, Quit, or end command. |
| Interface configuration mode | Commands to configure ports and VLAN interfaces are provided. | Port:<br>The Switch (config - ge1/1) #<br>VLAN interface:<br>The Switch (config - vlan1) # | Enter the interface <if-name> command in global configuration mode. | Exit to global configuration mode using the exit or Quit command and exit to privileged mode using the end command. |
| VLAN | The command to | The Switch | Enter the | Exit to global |

| | | | | |
|---|---|---|---|---|
| configuration mode | configure the VLAN is provided. For example, commands to create and delete a VLAN. | (config - vlan) # | VLAN Database command in global configuration mode. | configuration mode using the exit or Quit command and exit to privileged mode using the end command. |
| MSTP configuration mode | The command to configure MSTP is provided. For example, commands to create and delete MSTP instances. | The Switch (config - MST) # | Type the spanning-tree MST Configuration command in the global configuration mode. | Exit to global configuration mode using the exit or Quit command and exit to privileged mode using the end command. |
| Terminal configuration mode | Commands to configure the Console and Telnet terminals are provided, such as commands to configure the terminal timeout. | The Switch (# config - line) | Type the line vty command in global configuration mode. | Exit to global configuration mode using the exit or Quit command and exit to privileged mode using the end command. |

## 1.3 Command syntax Introduction

### 1.3.1 commands

The CLI command consists of two parts: keywords and parameters. The first word must be a keyword and the following word can be either a keyword or a parameter. Keywords and parameters can alternate. A command must have a keyword, but may have no arguments. For example, the command write has only one keyword and no arguments. The command Show Version has two keywords and no arguments; The command vlan <vlan-id> has a keyword and a parameter; The command instance <instance-id> vlan <vlan-id> has two keywords and two arguments and the keywords and arguments alternate.

### 1.3.2 The parameter types

CLI commands have two types of arguments: required and optional. Mandatory parameters must be entered when entering a command, while optional parameters may or may not be entered. For example, the parameter in the command vlan <vlan-id> is a required parameter, which must be entered when the command is entered. The arguments in the command Show Interface [iF-name] are optional and can be entered or not entered when the command is entered.

### 1.3.3 Command syntax rule

When describing commands in text, the following rules must be met:

1) Keywords are directly expressed as words.

The command show Version is shown.

2) parameters must be enclosed in < >.

Such as the command vlan <vlan-id>

3) If an optional parameter, the parameter must be enclosed in [].

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

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

Command Show VLAN [VLAN-ID]

The vLAN-ID parameter may or may not be entered.

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

4) if you must choose one of multiple keywords or parameters, enclose multiple keywords or parameters with {}, separate multiple keywords or parameters with |, and need a space before and after |.

If multiple keywords must be selected command:

So spanning tree MST link-type {point-to-point | Shared}

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

Mandatory commands with multiple parameters:

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

Keywords and parameters mixed with mandatory commands:

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

5) if one of multiple keywords or parameters is optional, enclose multiple keywords or parameters with [], and separate multiple keywords or parameters with |. A space is required before and after |.

The order is as follows:

Debug IP TCP [recv | send]

The keywords RECv and send may or may not be selected.

Show IP route [<ip-address> | <ip-prefix>]

Show interface [<if-name> | switchport]

6) If you have a keyword or parameter or a set of keywords or parameters, you can select the input repeatedly and add the symbol "*" after the keyword or parameter.

For example, the ping command:

Ping <ip-address> [-n <count b> >0-l <size> >1-r <count> >3-j <count> <ip-address>* >4-k <count> <ip-address>* >5-w <timeout>]*

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

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

The entire option can also be typed repeatedly.

6) Parameters are represented by descriptors of one or more words. If there are multiple words, separate each word with the symbol "-". Each word is lowercase.

Correct parameter representation: <vlan-id>, <if-name>, <router-id>, <count>, etc.

Incorrect parameter representation: <1-255>, < a.b.c.>, <WORD>, <IFNAME>, etc.

## 1.3.4 Command abbreviations

When the user enters a command on the CLI interface, the keywords of the command can be abbreviated. CLI supports the prefix matching function of commands, and the CLI resolves the input word into a matching keyword as long as it uniquely matches the keyword prefix. This makes it very convenient for users to use the CLI, where they can complete a command by typing very few characters, such as the Show Version command, where they can type only SH VER.

## 1.3.5 Grammar help

The CLI command line interface is set with syntax help to support the help functions of each level of commands and parameters, which are described as follows:

1) Direct input in a CLI mode? Key, the first keyword and description of all commands in this mode are listed on the terminal. For example, the Switch (config) #? .

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

3) Enter an incomplete keyword after direct input? Key, all keywords matching this input prefix and their descriptions are listed on the terminal. For example Switch# show ver? .

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

5) Enter the Tab key directly after an incomplete keyword. If only one keyword matches the input prefix, it will be completed directly. If more than one keyword matches the input prefix, all matching keywords will be listed on the terminal.

## 1.3.6 Command line error message

If a command entered by the user does not pass the syntax check, an error message is displayed on the terminal. The common error message is shown in the table below.

| The error message | The reason for the error |
|---|---|
| Invalid input or<br>Unrecognized command | No matching keyword was found.<br>Incorrect parameter input.<br>Too many keywords or arguments entered. |
| Incomplete command | Incomplete command input, and no keywords or parameters entered. |
| Ambiguous command | The keyword input is incomplete, with multiple keywords matching the input prefix. |

## 1.4 Command line shortcuts

### 1.4.1 Line edit shortcut key

The CLI command line interface supports the function of line editing shortcuts, which can facilitate the input and editing of CLI commands. The user can use the line edit shortcut to speed up command input when typing or editing a command. The following table lists all the row editing shortcuts and the functions implemented:

| shortcuts | function |
|---|---|
| Ctrl + p or write key | Previous command |
| Ctrl + n or left key | Next command |
| Ctrl + u | Delete the entire line |
| Ctrl + a | The cursor returns to the beginning of the line |
| Ctrl + f or - > key | Move the cursor one space to the right |
| Ctrl + b or please key | Move the cursor one space to the left |
| Ctrl + d | Deletes the character where the cursor is |
| Ctrl + h. | Delete the preceding character of the cursor |
| Ctrl + k. | Delete all characters at and after the cursor |
| Ctrl + w. | Delete all characters before the cursor |
| Ctrl + e | Move the cursor to the end of the line |
| Ctrl + c | Interrupt, do not execute command line. If the CLI is in global configuration mode or a configuration submode, the CLI reverts to privileged mode; If the CLI is in normal or privileged mode, the CLI mode stays the same, but the CLI starts a new row. |

| | |
|---|---|
| Ctrl + z | Same as Ctrl+ C. |
| The Tab | Use this key after inputting an incomplete keyword. If a keyword matches the input prefix, complete the keyword. If more than one keyword matches the input prefix, all the matching keywords are listed. If there is no keyword match, this key is invalid. |

**Note: Some Console terminals: ↑, ↓, → ← key is not available.**

## 1.4.2 Displays command shortcuts

For commands beginning with show keyword, they are all display commands. Some display commands cannot be displayed in one screen due to too much content displayed. The terminal provides the function of split screen display. After a screen is displayed, the terminal waits for user input to decide what to do next. The following table lists the display command shortcut keys and their functions.

| shortcuts | function |
|---|---|
| Blank Space | Show the next screen |
| Enter the Enter | Display the next line |
| Ctrl + c | Interrupt command execution, exit to CLI mode. |
| The other key | Same as Ctrl+ C. |

# 1.5 The history command

The CLI command-line interface supports a history of commands, remembers the last 20 historical commands the user has used, and saves the most recent commands the user has typed. You can use Show History to display the commands you have entered, or you can use Ctrl+ P,Ctrl+ N, ↑, ↓ to select the history command. The historical command function makes it easy for users to enter commands.

# Chapter 1 CLI Command-Line Introduction

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

- Access the CLI of the switch
- The Introduction to the CLI patterns
- The Command syntax;
- The Command line shortcuts
- The history command

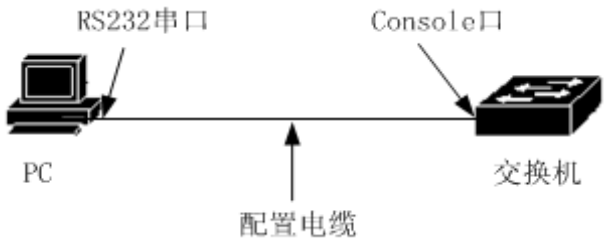
## 1.6 Access the CLI of the switch

The CLI Command line interface of The switch provides The user-managed switch interface.Users can access The CLI Command line interface of The switch through The Console and Telnet Terminals,Which are brilliant below.

### 1.6.1 The user accesses The CLI through The Console port

The operation Steps are as follows:

Connect the serial port of PC to Console the switch by configuring cable, as shown in the figure below:




Step 2:Start the terminal Emulator on PC (such as the Super terminal of Windows,(Configure the communication parameters of the terminal emulator.The communication parameters of the terminal are configured as follows:

Baud rate: 38400 (or 115200) (Note: The Actual Product shall prevail)

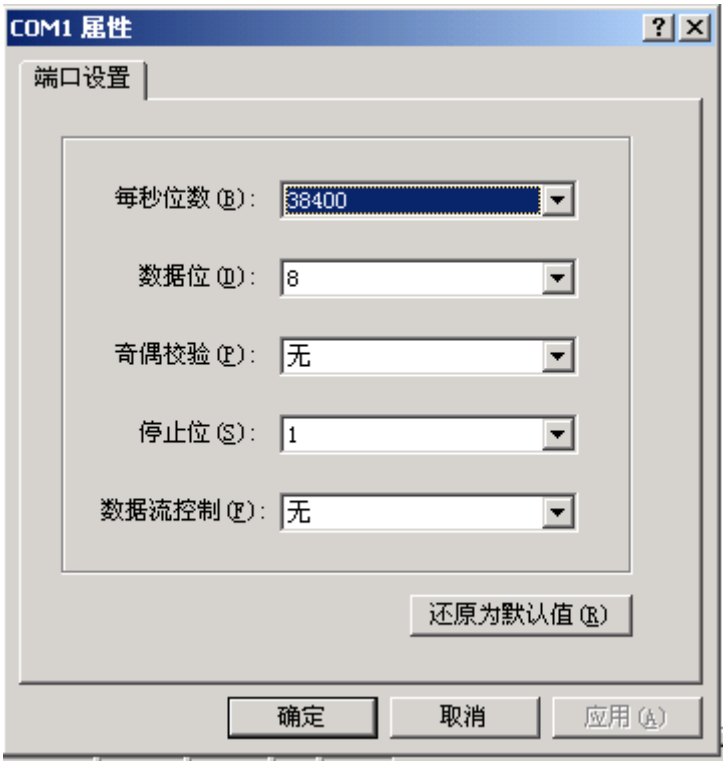
Data bits: 8

Parity: None

Stop bits: 1

The Data flow control: None

The Communication Parameter Configuration of The super terminal is as follows:



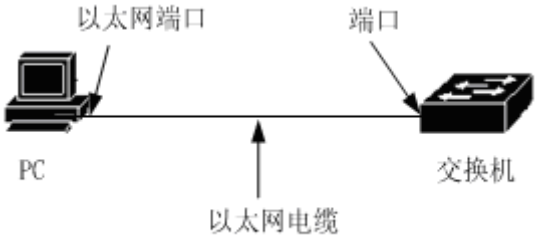

Step 3: start the Switch. After the Switch is started, the CLI prompt (default is Switch>) will be displayed on the terminal. The user can enter a command at this prompt, so that the user can access the CLI of the Switch.

## 1.6.2 The USER accesses the CLI through TELNET

Users can access the switch through its port.

The default IP address of the port of the switch is 192.168.0.1 (note: the actual product shall prevail). The operation steps of accessing the switch through the port are as follows:

Step 1: Connect the Ethernet port of the PC to the port of the switch over an Ethernet cable. The diagram below:




Step 2: Set the IP address of the PC's Ethernet port, which must be within 192.168.0.0/24 (e.g. 192.168.0.100). Ping 192.168.0.1 to determine the PC and switch connectivity.

Step 3: If the PC and the switch are connected, Telnet 192.168.0.1 enters the Telnet terminal interface. The diagram below:


Step 4: if the system does not set the password, the Telnet interface directly enters CLI, and the CLI prompt appears (default is Switch>); If the system has a password, you need to enter the password on the Telnet interface to enter the CLI.

There are two points to note in particular:

- The IP address of the switch port is built on the VLAN three-layer interface. Before accessing the switch, the IP address of a VLAN interface must be set. The default IP address of VLAN1 is 192.168.0.1 (note: it depends on the actual product), which can be used directly.The IP address of the VLAN interface can be configured through the Console port.
- The user accesses the switch via port, and can connect the PC and port directly via Ethernet cable, or through a network, as long as the PC and a VLAN of the

switch can be intercommunicated.

## 1.7 Introduction to CLI patterns

### 1.7.1 The role of the CLI pattern

The role of CLI model is mainly as follows:

- Facilitate user classification and prevent unauthorized use of CLI.

Users can be divided into two levels, namely two categories: ordinary users and privileged users.

Ordinary users can only view some of the running state of the switch and can only use the display command.

In addition to being able to see the running state of the switch, privileged users can also maintain and configure the switch and change its behavior.

- Convenient for users to configure the switch

There are many configurations for switches, and it is very inconvenient for users to use them all in one mode. To this end, multiple patterns are established on CLI and similar commands are put into one pattern, which is easy for users to understand and use. For example, vLAn-related commands are placed in VLAN configuration mode and interface-related commands are placed in interface configuration mode.

### 1.7.2 Identification of CLI patterns

CLI prompt is the identity of CLI mode. When using CLI, users can know the CURRENT CLI mode by looking at the CLI prompt.

The CLI prompt consists of two parts, one that identifies the host and the other that identifies the schema.

The host part of the CLI prompt USES the system's host name, which is configurable and defaults to Switch, so the CLI prompt defaults to Switch, and the CLI descriptor mentioned later generally USES the default host name.

The pattern part of the CLI prompt is not configurable, and each pattern has its own corresponding pattern string, some of which are fixed and some of which are mutable. For example, the pattern string of VLAN configuration mode is fixed, while the pattern string of interface configuration mode is mutable.

Such as:

The CLI prompt Switch# identifies the privileged mode, Switch identifies the host, and # identifies the mode.

The CLI prompt Switch(config-ge1/1)# identifies the interface configuration pattern and is configured with port GE1/1, Switch identifies the host, and (config-ge1/1)# identifies the pattern.

The CLI prompt Switch(config-vlan2)# identifies the interface configuration pattern, and the vLAN2 interface is configured, the Switch identifies the host, and (config-vlan2)# identifies the pattern.

### 1.7.3 Classification of CLI patterns

CLI patterns fall into four categories: general pattern, privileged pattern, global configuration pattern, and configuration subpattern, which consists of many CLI patterns.

Ordinary users can only access the ordinary mode, and privileged users can access all CLI modes.

The Console and Telnet terminals enter normal mode first, and enter privilege mode after entering enable command and successfully verifying password in normal mode. On the Telnet terminal, ordinary users can only stay in normal mode and cannot enter privileged mode. Enter Configure Terminal in privilege mode, and enter CLI mode into global configuration mode. Enter the relevant commands in global configuration mode to enter each configuration submode.

The following table lists the major CLI patterns for switches:

| model | describe | prompt | Enter mode commands | Exit mode command |
|---|---|---|---|---|
| Normal mode | Provides display command to view the status information of the switch. | The Switch > | The first mode that the terminal enters. | There is no exit mode command on the Console terminal, and exit or quit commands are used on the Telnet terminal to exit the Telnet terminal. |
| Privileged mode | In addition to providing display command to view the status information of the switch, it also provides commands such as debugging, version upgrading and configuration maintenance. | Switch# | Enter the enable command in normal mode. | Use the disable command to fall back into normal mode.<br>Use the exit or Quit command to exit normal mode on the Console terminal and exit or quit the Telnet terminal on the Telnet terminal. |
| Global configuration mode | Provides generic commands that cannot be implemented within a configuration subpattern, such as configuring static routing commands. | The Switch # (config) | Enter the configure Terminal command in privilege mode. | Exit to privileged mode using the exit, Quit, or end command. |
| Interface configuratio | Commands to configure ports and VLAN interfaces are provided. | Port:<br>The Switch (config - | Enter the interface <if-name> command | Exit to global configuration mode using the exit or Quit |

| | | | | |
|---|---|---|---|---|
| n mode | | ge1/1) #<br><br>VLAN interface:<br>The Switch (config - vlan1) # | in global configuration mode. | command and exit to privileged mode using the end command. |
| VLAN configuration mode | The command to configure the VLAN is provided. For example, commands to create and delete a VLAN. | The Switch (config - vlan) # | Enter the VLAN Database command in global configuration mode. | Exit to global configuration mode using the exit or Quit command and exit to privileged mode using the end command. |
| MSTP configuration mode | The command to configure MSTP is provided. For example, commands to create and delete MSTP instances. | The Switch (config - MST) # | Type the spanning-tree MST Configuration command in the global configuration mode. | Exit to global configuration mode using the exit or Quit command and exit to privileged mode using the end command. |
| Terminal configuration mode | Commands to configure the Console and Telnet terminals are provided, such as commands to configure the terminal timeout. | The Switch (# config - line) | Type the line vty command in global configuration mode. | Exit to global configuration mode using the exit or Quit command and exit to privileged mode using the end command. |

## 1.8 Command syntax Introduction

### 1.8.1 commands

The CLI command consists of two parts: keywords and parameters. The first word must be a keyword and the following word can be either a keyword or a parameter. Keywords and parameters can alternate. A command must have a keyword, but may have no arguments. For example, the command write has only one keyword and no arguments. The command Show Version has two keywords and no arguments; The command vlan <vlan-id> has a keyword and a parameter; The command instance <instance-id> vlan <vlan-id> has two keywords and two arguments and the keywords and arguments alternate.

### 1.8.2 The parameter types

CLI commands have two types of arguments: required and optional. Mandatory parameters must be entered when entering a command, while optional parameters may or may not be entered. For example, the parameter in the command vlan <vlan-id> is a required parameter, which must be entered when the command is entered. The arguments in the command Show Interface [iF-name] are optional and can be entered or not entered when the command is entered.

## 1.8.3 Command syntax rule

When describing commands in text, the following rules must be met:

1) Keywords are directly expressed as words.

The command show Version is shown.

2) parameters must be enclosed in < >.

Such as the command vlan <vlan-id>

3) If an optional parameter, the parameter must be enclosed in [].

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

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

Command Show VLAN [VLAN-ID]

The vLAN-ID parameter may or may not be entered.

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

4) if you must choose one of multiple keywords or parameters, enclose multiple keywords or parameters with {}, separate multiple keywords or parameters with |, and need a space before and after |.

If multiple keywords must be selected command:

So spanning tree MST link-type {point-to-point | Shared}

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

Mandatory commands with multiple parameters:

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

Keywords and parameters mixed with mandatory commands:

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

5) if one of multiple keywords or parameters is optional, enclose multiple keywords or parameters with [], and separate multiple keywords or parameters with |. A space is required before and after |.

The order is as follows:

Debug IP TCP [recv | send]

The keywords RECv and send may or may not be selected.

Show IP route [<ip-address> | <ip-prefix>]

Show interface [<if-name> | switchport]

6) If you have a keyword or parameter or a set of keywords or parameters, you can select the input repeatedly and add the symbol "*" after the keyword or parameter.

For example, the ping command:

Ping <ip-address> [-n <count b> >0-l <size> >1-r <count> >3-j <count> <ip-address>* >4-k <count> <ip-address>* >5-w <timeout>]*

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

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

The entire option can also be typed repeatedly.

6) Parameters are represented by descriptors of one or more words. If there are multiple words, separate each word with the symbol "-". Each word is lowercase.

Correct parameter representation: <vlan-id>, <if-name>, <router-id>, <count>, etc.

Incorrect parameter representation: <1-255>, < a.b.c.>, <WORD>, <IFNAME>, etc.

### 1.8.4 Command abbreviations

When the user enters a command on the CLI interface, the keywords of the command can be abbreviated. CLI supports the prefix matching function of commands, and the CLI resolves the input word into a matching keyword as long as it uniquely matches the keyword prefix. This makes it very convenient for users to use the CLI, where they can complete a command by typing very few characters, such as the Show Version command, where they can type only SH VER.

### 1.8.5 Grammar help

The CLI command line interface is set with syntax help to support the help functions of each level of commands and parameters, which are described as follows:

1) Direct input in a CLI mode? Key, the first keyword and description of all commands in this mode are listed on the terminal. For example, the Switch (config) #? .

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

3) Enter an incomplete keyword after direct input? Key, all keywords matching this input prefix and their descriptions are listed on the terminal. For example Switch# show ver? .

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

5) Enter the Tab key directly after an incomplete keyword. If only one keyword matches the input prefix, it will be completed directly. If more than one keyword matches the input prefix, all matching keywords will be listed on the terminal.

### 1.8.6 Command line error message

If a command entered by the user does not pass the syntax check, an error message is displayed on the terminal. The common error message is shown in the table below.

| The error message | The reason for the error |
|---|---|
| Invalid input or<br>Unrecognized command | No matching keyword was found.<br>Incorrect parameter input.<br>Too many keywords or arguments entered. |
| Incomplete command | Incomplete command input, and no keywords or parameters entered. |

| | |
|---|---|
| Ambiguous command | The keyword input is incomplete, with multiple keywords matching the input prefix. |

## 1.9 Command line shortcuts

### 1.9.1 Line edit shortcut key

The CLI command line interface supports the function of line editing shortcuts, which can facilitate the input and editing of CLI commands. The user can use the line edit shortcut to speed up command input when typing or editing a command. The following table lists all the row editing shortcuts and the functions implemented:

| shortcuts | function |
|---|---|
| Ctrl + p or write key | Previous command |
| Ctrl + n or left key | Next command |
| Ctrl + u | Delete the entire line |
| Ctrl + a | The cursor returns to the beginning of the line |
| Ctrl + f or - > key | Move the cursor one space to the right |
| Ctrl + b or please key | Move the cursor one space to the left |

| | |
|---|---|
| Ctrl + d | Deletes the character where the cursor is |
| Ctrl + h. | Delete the preceding character of the cursor |
| Ctrl + k. | Delete all characters at and after the cursor |
| Ctrl + w. | Delete all characters before the cursor |
| Ctrl + e | Move the cursor to the end of the line |
| Ctrl + c | Interrupt, do not execute command line. If the CLI is in global configuration mode or a configuration submode, the CLI reverts to privileged mode; If the CLI is in normal or privileged mode, the CLI mode stays the same, but the CLI starts a new row. |
| Ctrl + z | Same as Ctrl+ C. |
| The Tab | Use this key after inputting an incomplete keyword. If a keyword matches the input prefix, complete the keyword. If more than one keyword matches the input prefix, all the matching keywords are listed. If there is no keyword match, this key is invalid. |

**Note: Some Console terminals: ↑, ↓, → ← key is not available.**

## 1.9.2 Displays command shortcuts

For commands beginning with show keyword, they are all display commands. Some display commands cannot be displayed in one screen due to too much content displayed. The terminal provides the function of split screen display. After a screen is displayed, the terminal waits for user input to decide what to do next. The following table lists the display command shortcut keys and their functions.

| shortcuts | function |
| --- | --- |
| Blank Space | Show the next screen |
| Enter the Enter | Display the next line |
| Ctrl + c | Interrupt command execution, exit to CLI mode. |
| The other key | Same as Ctrl+ C. |

## 1.10 The history command

The CLI command-line interface supports a history of commands, remembers the last 20 historical commands the user has used, and saves the most recent commands the user has typed. You can use Show History to display the commands you have entered, or you can use Ctrl+ P,Ctrl+ N, ↑, ↓ to select the history command. The historical command function makes it easy for users to enter commands.

# Chapter 4 Configure port-based security

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

- Introduction to the
- MAC binding configuration
- MAC filter configuration
- Port learning limit configuration
- Secure port configuration

## 1.11 Introduction to the

Port-based MAC security can provide MAC binding, MAC filtering, port learning control and port protection to improve the security performance of switch layer 2 forwarding.

MAC binding allows you to bind a MAC to a port, restricting a given MAC address to access the network on a given port. The port also allows only those bound MAC addresses to access the network; Multiple MAC addresses can be bound to a single port. MAC bindings can be applied to a specified port at the same time as 802.1x. This feature is very useful for devices that do not have 802.1x or are not easy to use, such as printers, file servers, etc.

MAC filtering prevents certain MAC addresses from accessing the network, mainly to prevent illegal devices from accessing the network. When a MAC address is configured

for MAC filtering, the MAC address cannot access the network on any port of the switch, nor can it receive packets destined for those MAC addresses. As with MAC bindings, a port can be configured with multiple Mac-filtered MAC addresses simultaneously. In the application, if some virus software attacks the network with forged MAC addresses, the ACL can also be accessed through MAC filtering to control the attack of these forged packets.

Port learning control controls the number of MAC addresses a port can learn dynamically. If a port specifies the number of MAC addresses it can dynamically learn, when the number of MAC addresses learned on the port equals the number of port configurations, new MAC addresses will not be learned, and packets for these new MAC addresses will be discarded.

It should be noted that the MAC address referred to here is actually MAC+VID, which will not be described later in this chapter. In addition, MAC binding and 802.1x can be configured on the same port; MAC filtering and port learning restrictions can be configured on one port at the same time; MAC binding, 802.1x and MAC filtering, and port learning restrictions cannot be configured on the same port at the same time between the two groups.

## 1.12 MAC binding configuration

MAC binding configuration supports manual binding of MAC addresses and automatic binding of MAC addresses. Manually binding a MAC address means that the user enters the MAC address to bind to the port one by one through a command. Automatic binding of MAC addresses is to read out the existing entries of the port in the layer 2 hardware transfer publication and directly bind MAC addresses. The command to read the tier 2 hardware table is Show Bridge FDB.

Configuration commands

| The command | describe | CLI mode |
|---|---|---|
| Switchport-security | Manually bind a MAC | Interface |

| | | |
|---|---|---|
| mac-bind hhhh.hhhh.HHHH vlan <1-4094> qosprofile {qp0\|qp1\|qp2\|qp3\| qp4\|qp5\|qp6\|qp7} | address to an interface and configure the priority queue for that table entry. | configuration mode |
| Switchport-security mac-bind auto-conversion number <1-8191> qosprofile {qp0\|qp1\|qp2\|qp3\| qp4\|qp5\|qp6\|qp7} | Automatically converts a specified number of MAC addresses for an interface to the MAC binding configuration and configures the priority queue for that table entry. | Interface configuration mode |
| Switchport-security mac-bind auto-conversion vlan <1-4094> qosprofile {qp0\|qp1\|qp2\|qp3\| qp4\|qp5\|qp6\|qp7} | Automatically converts the MAC address of a specified VLAN for an interface to the MAC binding configuration and concodes the priority queue for that table entry. | Interface configuration mode |
| Show the port ws-security MAC - bind [IFNAME] | Displays the MAC binding configuration | Privileged mode |

Note:

Invalid or failed MAC address binding may occur for the following reasons:

The port is configured with 802.1x

The port is configured with MAC filters or port learning limits;

The MAC address is bound to another port, or MAC filtering is configured;

The L2 table of the switch is full.

## 1.13 MAC filter configuration

The MAC filter configuration supports manual and automatic binding of MAC addresses. Manually configuring MAC filtering means that the user enters the MAC that needs to be filtered to bind to the port one by one through a command. Automatic Configuration MAC filtering is a direct MAC filtering configuration by reading out the existing entries for the port in the layer 2 hardware transfer publication. The command to read the tier 2 hardware table is Show Bridge FDB.

Configuration commands

| The command | describe | CLI mode |
|---|---|---|
| Switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094> | Manually configure MAC filters for one interface | Interface configuration mode |
| Switch port-security mac-filter auto-conversion number <1-8191> | Automatically converts a specified number of MAC addresses of an interface to the MAC filtering configuration | Interface configuration mode |
| Switch port-security mac-filter HHHH.HHHH.HHHH vlan | Automatically converts the MAC address of a specified VLAN of an interface to the | Interface configuration mode |

| | | |
|---|---|---|
| <1-4094> | MAC filtering configuration | |
| Show the port ws-security MAC - filter [IFNAME] | Displays the MAC binding configuration | Privileged mode |

Note:

The MAC filter configuration is invalid or fails for the following reasons:

The port has MAC bindings configured or 802.1x protocol enabled;

The MAC address has been bound to another port, or a MAC binding has been configured.

The L2 table of the switch is full.

## 1.14 Port learning limit configuration

The switch can configure the maximum number of dynamic learning addresses per port. If a port is configured to dynamically learn the number of MAC addresses, then the port can only learn the corresponding number of MAC addresses, when the number of MAC addresses beyond this number, cannot be learned and forwarded on the port.

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

Configuration commands

| The command | describe | CLI mode |
|---|---|---|
| Switchport port ws-security learn - limit < 0-8191 > | Configure the number of MAC addresses an interface can learn. | Interface configuration mode |

| | | |
|---|---|---|
| No switchport port ws-security learn - limit | Delete the number of MAC addresses an interface can learn. | Interface configuration mode |
| Show the port ws-security learn - lmit [IFNAME] | Show port to learn configuration | Privileged mode |

Configuration of the sample

Configuring port Ge1/5 can only learn 7 MAC addresses

Switch# configure terminal

The Switch (config) interface ge1/5

The Switch (config - ge1/5) switchport port ws-security learn - limit 7

Note:

The reasons why the port learning setting is invalid or fails may be as follows:

The port is already configured with MAC bindings or 802.1x protocol functionality enabled.

## 1.15 Secure port configuration

### 1.15.1 Introduction to Protection port

To achieve a two-layer isolation between packets, ports can be divided into different VLANs, but vLAN resources can be wasted. Configure the port to protect the port, can

achieve the same VLAN port isolation, for users to provide a more secure, more flexible networking scheme.

Each port can be configured as a protected port. The protected ports cannot communicate with each other, but only with non-protected ports. There are two modes of application:

1. Only one port is not configured to protect the port, and all other ports are isolated;

2. Prevent some insecure ports from sniffing data on other ports (including the server) and set these ports to be protected.

## 1.15.2 Secure port configuration

Configure the port as a protected port. In config mode, enter the port configuration mode, such as Interface Ge1/1, and execute the following command:

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

Displays ports configured to protect ports

Switch# show port ws-security protect

Port the Port protected

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

Ge1/1 ON

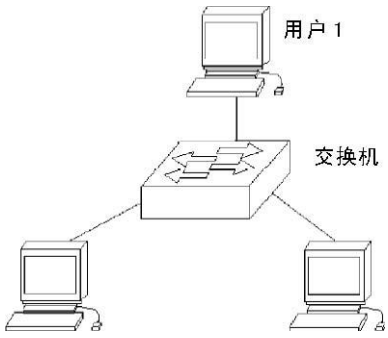
An example of a typical configuration of protected ports

Network requirements

User 1 User 2 servers are connected to switch port ge1/1 ge1/2 Ge1/3, respectively

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

Network diagram




The user 2 The server

The configuration steps

The Switch > enable

Switch# config terminal

The Switch (config) # interface ge1/1

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

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

The Switch (config - ge1/2) # switchport port ws-security protect

The Switch (config - ge1/2) # exit

The Switch (config) # exit

Switch# show port ws-security protect

Port the Port protected

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

Ge1/1 ON

Ge1/2 ON

# Chapter 5 Configure port IP to bind to MAC

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

- Introduction to the
- IP and MAC binding configuration
- Configuration of the sample

- Configuration misarrangement

,

## 1.16 Introduction to the

Configuring IP and MAC binding on switch ports at layer 2 is a static defense against ARP attacks. The ARP attacker attacks the user by sending ARP messages with false MAC addresses, which causes the user's local ARP cache table to be overwritten by the attacker's MAC address and causes the normal flow of data to the attacker. Static binding of user IP address and MAC address in switch port configuration command can effectively filter ARP attack message.

In addition to the function of preventing ARP spoofing, the IP MAC binding function can also guarantee the one-to-one mapping relationship between IP and MAC, that is, one IP can only correspond to one MAC, and one MAC can only correspond to one IP. If the access device changes this mapping relationship, it will not be able to communicate in

this network. 802.1X Anti-ARP spoofing and the DHCP SNOOPING protocol are dynamic implementations of this feature.

IP MAC binding, ACL, 802.1X anti-ARP spoofs, and DHCP SNOOPING all use the same system resource CFP. At design time, we made the compatibility relationship between them. The following table:

| | IP MAC binding | The ACL | 802.1 x | DHCP SNOOPING |
|---|---|---|---|---|
| IP MAC binding | Compatible with | Are not compatible | Compatible with | Compatible with |
| The ACL | Are not compatible | Compatible with | Are not compatible | Are not compatible |
| 802.1 x | Compatible with | Are not compatible | Compatible with | Are not compatible |
| DHCP SNOOPING | Compatible with | Are not compatible | Are not compatible | Compatible with |

CFP is a limited hardware resource and can only configure 16 IP MAC binding entries per port on average. Therefore, in a network with many access hosts, if only a few ports or a few IP and MAC addresses need to be controlled, the static IP MAC binding function can be adopted. Avoid data forwarding failure due to CFP function exhaustion.

Whether 802.1x or DHCP SNOOPING is performed depends on the current situation. If the network is configured using static IP address and accessed using 802.1x, 801.1x anti-ARP is required to be effective.

## 1.17 IP and MAC binding configuration

IP is bound to MAC in interface mode configuration

Configure port IP to bind to MAC

Switch# configure terminal

The Switch (config) # interface ge1/1

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

Remove port IP from MAC binding

Switch# configure terminal

The Switch (config) # interface ge1/1

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

According to the configuration

Displays binding table entries for all ports

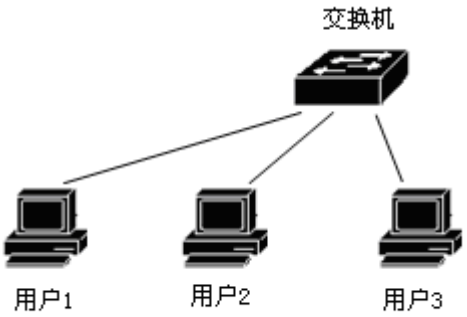
The show IP MAC - bind

Displays a binding table entry for an interface

The show IP MAC - bind IFNAME

## 1.18 Configuration of the sample

There are user 1, user 2 and user 3 in the network. Bind the user's IP and MAC on the port to defend against ARP attack.




Switch# configure terminal

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # IP MAC - bind 192.168.1.100 0011.5 b34.42 AD

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

The Switch (config - ge1/2) # IP MAC - bind 192.168.1.101 0011.6452.135 d

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

The Switch (config - ge1/3) # IP MAC - bind 192.168.1.102 da 246 0011.804

The Switch (config - ge1/3) # end

Switch# show IP MAC - bind

Ge1/1 sum: 1

MAC IP

0011.5 b34.42 AD 192.168.1.100

Ge1/2 sum: 1

MAC IP

0011.6452.135 d 192.168.1.101

Ge1/3 sum: 1

MAC IP

Da 246 0011.804 192.168.1.102

MAC - bind Switch# show IP ge1/1

Ge1/1 sum: 1

MAC IP

0011.5 b34.42 AD 192.168.1.100

Switch# show running - config

!

Spanning - tree the MST configuration

!

Interface vlan1

IP address 10.10.10.1/24

!

Interface ge1/1

IP MAC - bind 192.168.1.100 0011.5 b34.42 AD

!

Interface ge1/2

IP MAC - bind 192.168.1.101 0011.6452.135 d

!

Interface ge1/3

IP MAC - bind 192.168.1.102 da 246 0011.804

!

The line vty

!

The end

## 1.19 Configuration misarrangement

Failure to configure an IP MAC binding could be caused by:

1. System CFP resource is exhausted.

2. The current interface is configured with ACL filtering.

The configured interface is a three-tier interface or a TRUNK interface.

# Chapter 6 Port loop detection

This chapter mainly includes the following contents:

- introduce
- The agreement principle
- Configuration is introduced

## 1.20 Introduction to the

When there is a loop under a certain port of the switch, it will cause a broadcast storm under that port, and learn the MAC address of all broadcast packets to the port with a loop, which will cause device forwarding to fail to proceed normally.

## 1.21 The agreement principle

The Ethernet Loopback Detection protocol (ELD) detects loops through packet interactions and blocks the ports where the loops occur. The ELD protocol is a port-based protocol that can only detect loops that occur on that port.

### 1.21.1 Testing process

When a port is enabled when the ELD agreement, will be at this port to enable a timer,

regularly send loop testing kits when the timer expires, if in a timer cycle received his sending loop testing kits, argues that this port is the loop, will be executed on the port block loop operation, and empty this port FDB table.

If a port belongs to multiple VLANs, the port automatically sends loop detection packets to all VLANs. That is, the port automatically detects loops on all vLans to which it belongs.

## 1.21.2 Recovery mode

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

Automatic recovery is when a port is blocked on the loop, the ELD protocol enables a recovery timer. When the timer expires, an anti-blocking loop operation is performed and the loop detection timer is enabled again on the port.

Manual recovery means that after the port is blocked, the protocol no longer enables the timer to restore the port. Instead, the user enters a command to perform the anti-operation of the blocking loop.

## 1.21.3 Security agreement

The ELD protocol is vulnerable to attacks on the network, which means that users can send ELD packets to a port that has the ELD protocol enabled according to the format of the ELD packet, causing the port to be blocked without a possible loop, resulting in a bad decision.

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

Decision one: First, the ELD protocol is a non-interactive protocol, that is, it does not

depend on other devices, so the packet itself can be encrypted simply. What we're doing here is we're sending an ELD protocol package with a key that the user can't disguise without a key.

The second decision is mainly to prevent attackers from reflecting protocol packets by capturing packet attacks. The format of packets received by switches in a certain period can be configured to prevent attacks, which requires users to configure.

## 1.22 Configuration is introduced

The ELD protocol is port-based and does not have uniformly enabled commands.

### 1.22.1 Global configuration

Global configuration is a unified property of configuration protocols.

| The command | describe | model |
|---|---|---|
| Loop - detection detection - time > < 1-65535 | Configure the time for loop detection, which must be twice as long as the recovery time, with a default of 5 seconds. | Global configuration mode |
| Loop - detection resume - time > < 10-65535 | Configure the time for automatic recovery. The time for automatic recovery must be greater than 2 by loop check. This configuration will take effect if automatic recovery is enabled. The default recovery time is 600 seconds. | Global configuration mode |
| Loop - detection protocol - safety | Enables protocol security checking, which is turned off by default. | Global configuration mode |
| Loop - detection respond - packets | Configure the number of packets that must be received over a period | Global configuration |

| | | |
|---|---|---|
| | of time. This configuration takes effect if protocol security checks are enabled, with a default of 10 | mode |

## 1.22.2 Interface configuration

Interface configuration is the configuration for each port.

| The command | describe | model |
|---|---|---|
| Loop - detection enable | Enable the ELD protocol on a port. | Interface configuration mode |
| Loop - detection resume | Manually restore and restart loop check. | Interface configuration mode |
| Loop detection resumptive mode {automation \| manual} | Configure recovery mode and choose manual or automatic recovery. The default is automatic recovery. | Interface configuration mode |
| Loopback -detection shutdown-mode {no-shutdown \| shutdown} | The command conrates whether the port should shutdown when a loop occurs. | Interface configuration mode |

## 1.22.3 According to the configuration

Show loop - detection [ifname]

Displays all configuration of the protocol and the configuration of an interface.

# Chapter 7
# Configuration VLAN

VLAN is an important concept in switches, which is widely used in practical applications. It is the basis for internal division of multiple networks. A VLAN, short for virtual Local area network, is a network that logically organizes multiple devices together regardless of their physical location. Each VLAN is a logical network that has all the features and attributes of a traditional physical network. Each VLAN is a broadcast domain, broadcast packets can only be forwarded in a VLAN, not across the VLAN, the data communication between vLAns must be forwarded through three layers.

This chapter mainly includes the following contents:

- VLAN is introduced
- VLAN configuration
- VLAN configuration example

## 1.23 VLAN is introduced

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

- The benefits of vlans
- VLAN ID
- VLAN port member types
- Default VLAN for ports
- VLAN mode for the port
- VLAN trunking
- The forwarding of a data stream within a VLAN
- VLAN subnet

### 1.23.1 The benefits of vlans

Vlans greatly extend the size of physical networks. Traditional physical networks can only be small enough to hold thousands of devices at most, while vLAN-partitioned physical networks can hold tens or even hundreds of thousands of devices. A VLAN has the same functions and properties as a traditional physical network.

Using a VLAN has the following benefits:

- VLAN can effectively control the traffic in the network.

In a traditional network, all broadcast packets are sent to all devices, whether necessary

or not, increasing the load on the network and devices. And the VLAN can according to the need to organize the device in a logical network, a VLAN is a broadcast domain, broadcast packets only in the VLAN internal transmission, will not cross the VLAN. The traffic in the network can be controlled effectively by dividing the VLAN.

- Vlans can improve network security.

Devices in the VLAN can only communicate with the same VLAN device for two layers, if you want to communicate with another VLAN, must pass through three layers of forwarding, if you do not establish three layers of forwarding between VLAN, VLAN can not communicate at all, can play the role of isolation, to ensure the safety of data in each VLAN. For example, if the R&D department of a company does not want to share data with the Marketing Department, it can set up a VLAN for the R&D department and a VLAN for the Marketing Department. There is no three-layer communication channel between the two VLANs.

- A VLAN makes it easy to move devices.

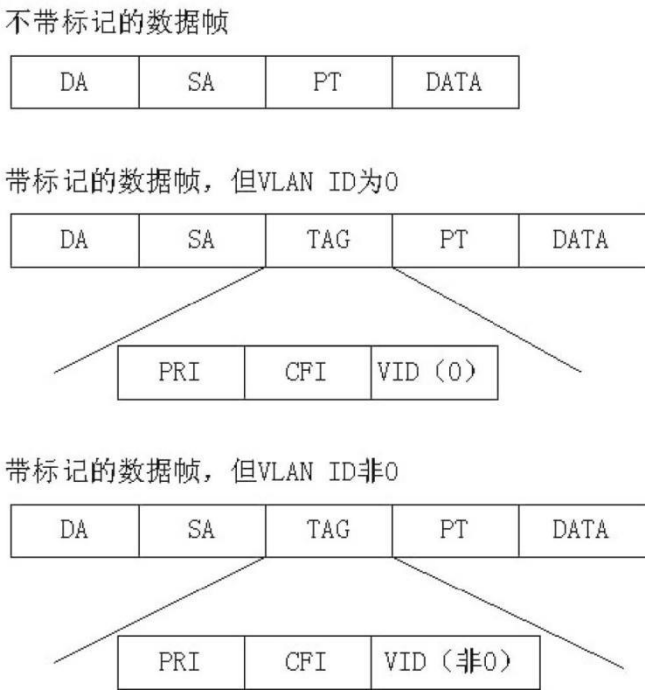
If the device in the traditional network is moved from one location to another and belongs to a different network, it needs to modify the network configuration of the mobile device, which is very inconvenient for users. The VLAN is a logical network, which can delimit devices not in the same physical location in the same network. When the device moves, the device can also belong to this VLAN, so that the mobile device does not need to modify any configuration.

## 1.23.2 VLAN ID

Each VLAN has an identification number, called a VLAN ID, and the VLAN ID ranges from 0 to 4095, where 0 and 4095 are not used, and only 1 to 4094 is actually valid. A VLAN ID uniquely identifies a VLAN.

The switch supports 4094 VLANs, and when creating a VLAN, select a VLAN ID ranging from 2 to 4094. The switch creates VLAN1 by default, and VLAN1 cannot be deleted.

There are three types of data frames that are transmitted within a VLAN in a network: unmarked data frames, marked with a VID of 0, and marked with a VID of non-0. Three different data frame formats are shown in the figure below.



All data frames inside the switch are tagged. If an untagged data frame is entered into the switch, the switch tags the data frame and selects a VLAN ID value to fill in the tagged VID. If a data frame is entered into the switch with a marked VID of 0, the switch selects a VLAN ID value to fill in the marked VID. If a data frame with a VID non-0 marker is entered into the switch, the frame does not change.

## 1.23.3 VLAN port member types

Switches support port-based VLANs and 802.1Q-based VLANs. A VLAN includes two port member types: untagged member and Tagged Member. A VLAN can include both untagged and tagged port members.

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

A port may belong to one or more TAGGED or untagged VLAN members. If a port belongs to two or more tagged VLAN members, this port is referred to as a VLAN relay port. A port may concurrently belong to one or more UNtagged VLAN members and to one or more tagged VLAN members.

## 1.23.4 Default VLAN for ports

The port has and only one default VLAN, which is used to determine the VLAN to which untagged or tagged packets with VID 0 are entered from the port. The default VLAN is also called port VID or PVID. By default, the default VLAN for the port is 1.

## 1.23.5 VLAN mode for the port

There are three VLAN modes for ports: ACCESS mode, TRUNK mode, and HYBRID mode. The user must first specify the VLAN mode of the port when configuring the port VLAN.

The port in ACCESS mode is an ACCESS port directly targeted at users, which can only belong to an UNtagged member of a VLAN. The default VLAN is a user-specified VLAN. When a port is an untagged member of a VLAN, the VLAN mode for that port can be specified as ACCESS mode.

The port in TRUNK mode is a relay port directly connected to the switch. This port may belong to one or more VLAN tagged members, but not to any VLAN untagged members. The default VLAN of this port is 1 and cannot be changed.

HYBRID mode's port is a relay port directly connected to a switch, which can belong to one or more TAGGED VLAN members and/or one or more tagged VLAN members. The default VLAN for this port can be changed.

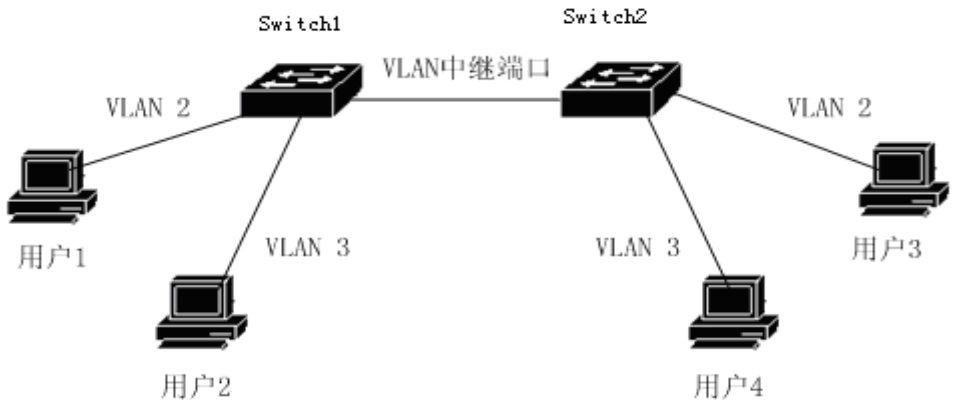
In practice, the user can choose the VLAN mode of the port according to the specific situation.

## 1.23.6 VLAN trunking

If a port belongs to two or more TAGGED members of a VLAN, it is also called a VLAN relay port. Two switches can be connected with VLAN relay ports, so that two or

more common VLANs can be divided between the two switches.

The following figure is an example of VLAN relay. Two switches are connected by VLAN relay port, which is the relay port of VLAN 2 and VLAN 3. Each switch is divided into two VLans, namely VLAN 2 and VLAN 3, and each VLAN contains a user. Thus, user 1 can communicate with user 3, user 2 can communicate with user 4, and user 1 and user 3 cannot communicate with user 2 and user 4.




## 1.23.7 The forwarding of a data stream within a VLAN

When the switch receives a packet from a port, it forwards it on the second level according to the following steps:

- Determines the VLAN to which the packet belongs.
- Determines whether the packet is a broadcast packet, multicast packet or unicast packet.
- Determine the output ports (which can be zero, one, or more) based on the

different packets, and discard the packets if there is no output port.

- Depending on the member type of the output port within the VLAN, the package being sent is marked or not.
- Send from the output port.

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

If the received packet is tagged and the VID field in the tag is not 0, the VLAN to which the packet belongs is the VID value in the tag.

The VLAN to which the packet belongs is the default VLAN for the port if it is received without a tag or if the tag has a VID value of 0.

2) How to determine the type of packet:

If the destination MAC address is FF:FF:FF:FF:FF:FF :FF:FF:FF:FF:FF:FF :FF:FF:FF:FF:FF:FF :FF:FF:FF:FF.

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

If it is neither a broadcast packet nor a multicast packet, the packet is unicast.

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

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

If the input packet is multicast data packets, first according to the purpose of multicast

MAC address and belonging to a VLAN find hardware multicast to turn on the second floor, multicast entries if a match is found, the multicast VLAN output port of entry and belong to members of the port to port (and action) is a packet of output port, if there is no common ports, the packet discard. If turn on the second floor hardware multicast published no match is found in the multicast entries, according to the second floor turn hardware multicast forwarding mode decision published output port, if is unregistered multicast forwarding mode, multicast packets as radio processing, all members belonging to a VLAN ports is the output of the packet, if it is registered forwarding mode, there is no output port, packet discard.

If the input packet is unicast, first of all, based on the destination MAC address and belonging to a VLAN for hardware to turn on the second floor, if a match is found in the entry, the output port of entry and belongs to a member of the VLAN port to port (and action) is a packet of output port, if there is no common ports, the packet discard. If no matching entry is found in the layer 2 hardware republish, the packet is treated as a broadcast packet and all member ports of the VLAN to which it belongs are the output ports of the packet.

4) Sending packet:

After determining the output port of the incoming packet, the packet should be sent out from all output ports.

If an output port is an untagged member of the VLAN to which the packet belongs, the packet is sent untagged from that output port.

Tagged if an output port is a TAGGED member of the VLAN to which the packet belongs, the packet is sent out with a tag. The VID value in the tag is the value of the VLAN to which the packet belongs.

## 1.24 VLAN configuration

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

- Create and delete vLAns
- Configure the VLAN mode for the port
- VLAN configuration in ACCESS mode
- VLAN configuration for TRUNK mode
- VLAN configuration for HYBRID mode
- VLAN subnet configuration
- View the VLAN information

### 1.24.1 Create and delete vLAns

Before creating and deleting a VLAN, the user needs to enter the VLAN configuration mode using the VLAN Database command in global configuration mode, where the VLAN is created and deleted.

VLAN 1 has been created by default and cannot be deleted by the user. The commands to create and delete a VLAN are shown in the following table:

| The command | describe | CLI mode |
| --- | --- | --- |
| Vlan < vlan - id > | Create a VLAN. If the VLAN already exists, no processing is done, otherwise the VLAN is created. The parameters range from 2 to 4094. | VLAN configuration mode |
| No vlan < vlan - id > | Deletes a VLAN. If the VLAN does not exist, do nothing or delete the VLAN. The parameters range from 2 to 4094. | VLAN configuration mode |

## 1.24.2 Configure the VLAN mode for the port

The VLAN mode of the port needs to be specified before configuring the VLAN of the port. By default, the VLAN mode of the port is ACCESS mode. The commands to specify the VLAN mode of the port are shown in the following table:

| The command | describe | CLI mode |
| --- | --- | --- |
| Switchport mode access | The VLAN mode for the specified port is ACCESS mode. After executing this command, the port is an | Interface configuration mode |

| | | |
|---|---|---|
| | untagged member of VLAN1, and the default VLAN is 1. | |
| Switchport mode trunk | The VLAN mode for the specified port is TRUNK mode. After executing this command, the port is a tagged member of VLAN1, and the default VLAN is 1. | Interface configuration mode |
| No switchport trunk | The VLAN mode of the port is no longer TRUNK mode, and it returns to the default, ACCESS mode. | Interface configuration mode |
| Switchport mode hybrid | The VLAN mode for the specified port is HYBRID mode. After executing this command, the port is an untagged member of VLAN1, and the default VLAN is 1. | Interface configuration mode |
| No switchport hybrid | The VLAN mode for the port is no longer HYBRID mode, but returns to the default, ACCESS mode. | Interface configuration mode |

## 1.24.3 VLAN configuration in ACCESS mode

Port VLAN configuration before you need to specify the port VLAN mode as ACCESS mode. The default port in this VLAN mode is an untagged member of VLAN1, and the default VLAN is 1. VLAN configuration commands in ACCESS mode are shown in the following table:

| The command | describe | CLI mode |
|---|---|---|
| Switchport access vlan < vlan - id > | The configured port is an untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. The parameters range from 2 to 4094. | Interface configuration mode |
| No switchport access vlan | The port VLAN configuration goes back to the default, that is, the port is an untagged member of VLAN1, and the default VLAN is 1. | Interface configuration mode |

## 1.24.4 VLAN configuration for TRUNK mode

The VLAN mode of the port needs to be specified as TRUNK mode before VLAN

configuration of the port can be done. Tagged member of VLAN1 is the default port in this VLAN mode and the default VLAN is 1. VLAN configuration commands for TRUNK mode are shown in the following table:

| The command | describe | CLI mode |
|---|---|---|
| The switchport trunk native vlan <vlan-id> | Configure the default VLAN for the port, also known as PVID.The parameters range from 2 to 4094. | Interface configuration mode |
| The Switchport trunk allows VLAN All | The configured ports are tagged members of all VLans, and will also be tagged members of all vLAns created in the future. | Interface configuration mode |
| Switchport trunk Allowed VLAN None | This port is no longer tagged on all other VLAN members except VLAN1. | Interface configuration mode |
| Switchport trunk vlan add <vlan-list> | Configure ports to be tagged members of one or more VLans as specified. The parameter <vlan-list> can be a vlan, a vlan range, or more vlans. For example, the parameters can be "1", "2-4", or "1,3,5". | Interface configuration mode |

| | | |
|---|---|---|
| Switchport trunk vlan remove <vlan-list> | Tagged members of one or more vLans that have ports removed from the specified VLAN. The parameter <vlan-list> can be a vlan, a vlan range, or more vlans. For example, the parameters can be "1", "2-4", or "1,3,5". | Interface configuration mode |

## 1.24.5 VLAN configuration for HYBRID mode

Before doing VLAN configuration for a port, you need to specify the VLAN mode for the port as HYBRID mode. The default port in this VLAN mode is an untagged member of VLAN1, and the default VLAN is 1. The VLAN configuration commands for HYBRID mode are shown in the following table:

| The command | describe | CLI mode |
|---|---|---|
| The switchport hybrid native vlan <vlan-id> | The configured port is an untagged member of the specified VLAN and the default VLAN of the port is the specified VLAN.The parameters range from 2 to | Interface configuration mode |

| | | |
|---|---|---|
| | 4094. | |
| No Switchport Hybrid Native VLAN | Clear port from default VLAN, no longer tagged or untagged member of the default VLAN, port default VLAN back to 1. | Interface configuration mode |
| Switchport hybrid allowed VLAN All | The configured ports are tagged members of all VLans (except VLAN1), and will also be tagged members of all vLANs that will be created in the future. | Interface configuration mode |
| Switchport hybrid allowed VLAN None | With the exception of VLAN1, this port is no longer tagged or untagged on all other VLANs, and the default VLAN port is back to 1. | Interface configuration mode |
| Switchport hybrid allowed vlan add <vlan-list> egres-tagged enable | Configure ports to be tagged members of one or more VLans as specified. The parameter <vlan-list> can be a vlan, a vlan range, or more vlans. For example, the parameters can be "1", | Interface configuration mode |

| | | |
|---|---|---|
| | "2-4", or "1,3,5". | |
| Switchport hybrid allowed vlan add <vlan-list> egres-tagged disable | Configure ports to be untagged members of one or more VLans as specified. The parameter <vlan-list> can be a vlan, a vlan range, or more vlans. For example, the parameters can be "1", "2-4", or "1,3,5". | Interface configuration mode |
| Switchport hybrid allowed vlan remove <vlan-list> | Ports are cleared from one or more vLans specified and are no longer tagged or untagged members of those VLANs. If the default VLAN for a port belongs to the specified VLAN, the default VLAN goes back to 1. | Interface configuration mode |

## 1.24.6 View the VLAN information

The commands to view VLAN information are shown in the following table:

| The command | describe | CLI mode |
|---|---|---|

| | | |
|---|---|---|
| Show vlan [vlan - id] | Displays all VLAN information if no parameters are entered, and a specified VLAN information if parameters are entered. The parameters range from 1 to 4094. | Normal mode, privileged mode |
| The show interface | Displays VLAN-related information for all ports of the system, such as VLAN mode, default VLAN, etc. | Normal mode, privileged mode |
| The show running - config | View the current configuration of the system. You can view the configuration of the VLAN. | Privileged mode |

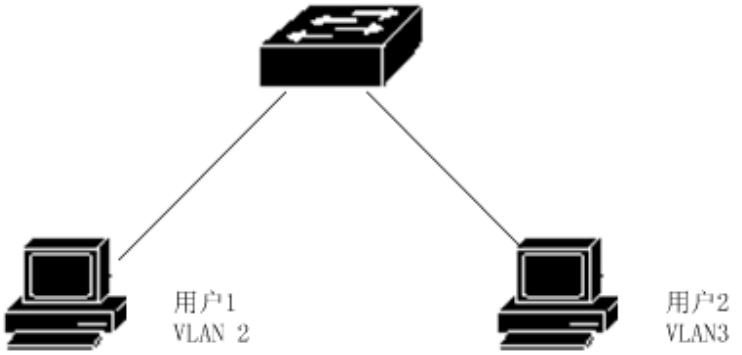
## 1.25 VLAN configuration example

### 1.25.1 Port-based VLAN

**1) configuration**

There are two users, user 1 and user 2, who need to be in different VLans due to

different network functions and environments. User 1 belongs to VLAN2, and the port ge1/1 connected to the switch and the port Ge1/2 connected to the switch belong to VLAN3.




The configuration of the switch is as follows:

Create a VLAN

Switch# config t

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # vlan 3

Assign the port to the VLAN

Switch# config t

The Switch (config) # interface ge1/1

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

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

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/2

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

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

**2) wrong**

If, after configuration, it is found that the PC between different VLANs cannot communicate, that is normal, because the communication between different VLans must go through three layers of routing and forwarding. If the PC in the same VLAN cannot communicate, the following verification shall be performed:

Show a vlan

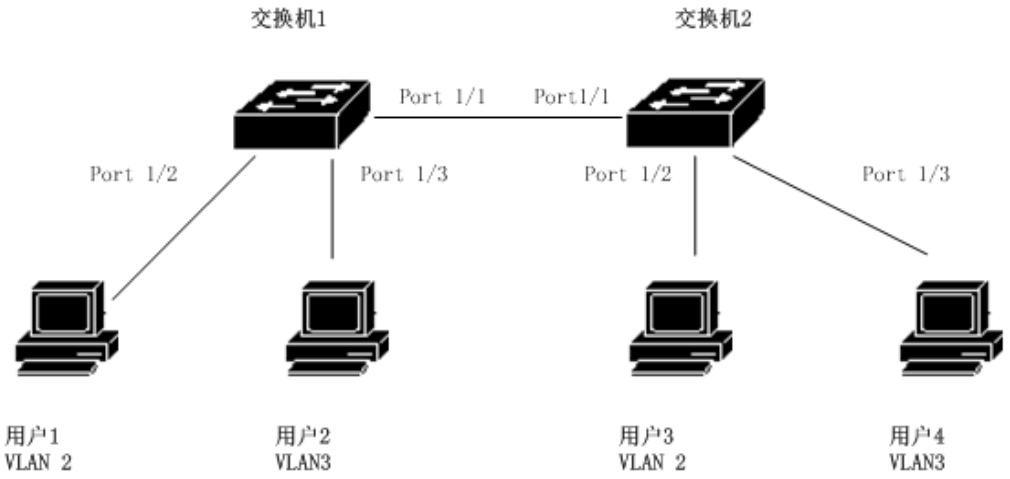
View all VLAN member ports

Show vlan < vlan - id >

Checks to see if the port to connect to a particular PC is within the specified VLAN

## 1.25.2 VLAN based on 802.1Q

**1) configuration**




There are two switches connecting two users respectively:

| The user | Belonging to a VLAN | End connections | Branch exchange | Cascade port |
|---|---|---|---|---|
| User 1 | 2 | 1/2 | Switch 1 | 1/1 |
| The user 2 | 3 | A third | Switch 1 | 1/1 |
| The user 3 | 2 | 1/2 | Switch 2 | 1/1 |
| User 4 | 3 | A third | Switch 2 | 1/1 |

You need to configure both switches.

Switch 1 configuration:

Switch# config t

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # vlan 3

Switch# config t

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

The Switch (config) # interface ge1/2

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

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

The Switch (config - ge1/2) # exit

The Switch (config) # interface ge1/3

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

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

Switch 2 configuration:

Switch# config t

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # vlan 3

Switch# config t

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

The Switch (config) # interface ge1/2

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

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

The Switch (config - ge1/2) # exit

The Switch (config) # interface ge1/3

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

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

**2) wrong**

Across the VLAN switch, in the same VLAN PC can communicate, if not. Check the following:

- Whether the port connected to the PC belongs to the corresponding VLAN, and the application of ACCESS mode to join this VLAN.
- Cascading port 1/1 is added to each VLAN, and port 1/1 is in TRUNK mode.

## 1.26 MAC, IP subnet, protocol VLAN

### 1.26.1 MAC, IP subnet, protocol VLAN introduction

A MAC - based VLAN is partitioned according to the MAC address of the source. After receiving untagged(or tag 0) messages from the port, the device will determine the VLAN to which the message belongs according to the MAC address of the source of the message, and then automatically divide the message into the designated VLAN for transmission.

An IP subnetwork-based VLAN is partitioned according to the IP address of the source and the subnet mask. After receiving an untagged message from a port, the device determines the VLAN to which the message belongs according to its source address, and then automatically divides the message into the designated VLAN for transmission. This feature is mainly used to send the message sent by the specified network segment or IP address in the specified VLAN.

A protocol-based VLAN assigns different VLAN ids to a packet based on the protocol type of the packet received by the port. The protocols used to partition the VLAN are IP, IPV6, IPX, and so on.

### 1.26.2 MAC, IP subnet, protocol VLAN configuration

Before configuring a MAC -, IP -, protocol - based VLAN, a corresponding VLAN must be created.

| The command | describe | CLI mode |
|---|---|---|
| MAC WORD vlan <1-4094> | Create a VLAN based on | VLAN |

| | | |
|---|---|---|
| | the source MAC address | configuration mode |
| No MAC MAC WORD - vlan | Deletes a VLAN based on the source MAC address | VLAN configuration mode |
| No MAC - vlan | Delete all VLANs based on the source MAC address | VLAN configuration mode |
| MAC - vlan enable | Start the MAC-VLAN function of the interface | Interface configuration mode |
| MAC - vlan disable | Turn off the MAC-VLAN function of the interface | Interface configuration mode |
| Show the MAC - vlan | Displays all VLANs based on the source MAC address | Privileged mode |
| IP -subnet-vlan IP A.B.C.D. vlan <1-4094> | Create a VLAN based on the source IP subnet | VLAN configuration mode |
| No IP-subnet-VLAN IP A.B.C.D. A.B.C.D | Deletes a VLAN based on the source IP subnet | VLAN configuration mode |
| No IP subnet configures - vlan | Remove all VLANs based on source IP subnets | VLAN configuration |

| | | |
|---|---|---|
| | | mode |
| IP subnet configures - vlan enable | Start the VLAN function of the interface based on the source IP subnet | Interface configuration mode |
| IP subnet configures - vlan disable | Turn off the VLAN function of the interface based on the source IP subnet | Interface configuration mode |
| The show IP subnet configures - vlan | Displays all vLAns based on source IP subnets | Privileged mode |
| IP protocol - vlan Mr -type (\| ipv6 the ipx \| \|...\| < > 0-65535) vlan < > 1-4094 | Create a protocol - based VLAN | Interface configuration mode |
| No protocol - vlan Mr -type (IP \| ipv6 the ipx \| \|... \| < > 0-65535) | Delete a protocol - based VLAN | Interface configuration mode |
| No protocol - a vlan | Delete all protocol-based VLans | Interface configuration mode |
| Show protocol - a vlan | Displays all protocol - based VLans | Privileged mode |
| Show vlan - partition interface IFNAME | Displays vLAns enabled on MAC, IP subnet interfaces | Privileged mode |

# 1.27 Voice VLAN

## 1.27.1 Voice VLAN is introduced

The Voice VLAN is a dedicated VLAN for the user's Voice data stream. By dividing Voice VLAN and adding the port connected to Voice devices into Voice VLAN, QoS parameters can be configured for Voice data to improve the priority of Voice data packets and ensure the Quality of calls.

The device can determine whether the data stream is a voice data stream based on the OUI field of the source MAC address in the data packet entering the port. Messages from a source MAC address that conforms to the OUI address of a Voice device set by the system are considered to be Voice data streams and are divided into Voice VLans for transmission.

The user can either pre-set the OUI address or use the default OUI address as a criterion, as follows

| The serial number | OUI address | Manufacturers, |
|---|---|---|
| 1 | 0001 - e300-0000 | Siemens phone |
| 2 | 0003-6 b00-0000 | Cisco phone |
| 3 | 0004-0 d00-0000 | How phone |
| 4 | 00 e00 d0-1-0000 | Pingtel phone |
| 5 | 0060 - b900-0000 | Philips/NEC phone |
| 6 | 00 e0-7500-0000 | Polycom phone |
| 7 | 00 e0 - bb00-0000 | 3 com phone |

Manually add IP phone access ports to the Voice VLAN. After identifying the source

MAC of the message, the OUI address is matched. After the match is successful, the system will issue ACL rules and configure the priority of the message.

## 1.27.2 Voice VLAN configuration

Before configuring the Voice VLAN, create the corresponding VLAN.

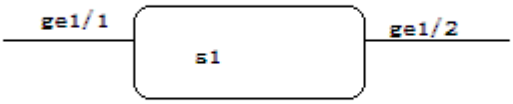
| The command | describe | CLI mode |
|---|---|---|
| Voice-vlan Oui WORD Mask WORD | Configure user OUI | Global configuration mode |
| Voice-vlan Oui WORD Mask WORD description WORD | Configure user OUI and name it | Global configuration mode |
| No Voice - Vlan Oui WORD Mask WORD | Remove the user OUI configuration through the OUI address and mask | Global configuration mode |
| No Voice - VLAN OUi Description WORD | Remove the user OUI configuration by name | Global configuration mode |
| No voice - vlan oui | Remove all user OUI configurations | Global configuration mode |
| No voice- VLAN Default-oui WORD Mask WORD | Remove the Defualt OUI configuration through the OUI address and mask | Global configuration mode |

| | | |
|---|---|---|
| No voice-vLAN Default-OUI Description WORD | Remove the Defualt OUI configuration by naming it | Global configuration mode |
| No voice - vlan default - oui | Remove all defualt OUI configurations | Global configuration mode |
| Voice - vlan default - oui resume | Restore all defualt OUI configurations | Global configuration mode |
| Show voice - vlan oui | Displays all defualt and user OUI configurations | Privileged mode |
| The voice vlan < > 1-4094 (enable \| disable) | Interface enables Voice VLAN | Interface configuration mode |
| Voice vlan qos remark cos <0-7> DSCP <0-63> | Interface configuration qos priority, cos value is 6, DSCP value is 46 | Interface configuration mode |
| No voice vlan qos | Restore the default configuration of interface qos priority | Interface configuration mode |
| No voice vlan | Remove interface to configure Voice VLAN | Interface configuration mode |
| Show voice - vlan | Shows all interfaces | Privileged mode |

| | | |
|---|---|---|
| | configured with the Voice VLAN | |

## 1.27.3 Voice VLAN configuration example

Configure voice data flow (0009.ca00.0000) to flow in and out of port Ge1/2 with TAG 2, as shown in the figure below




The configuration of switch S1 is as follows:

Switch# con t

The Switch # vlan da (config)

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # exit

The Switch (config) # int ge1/1

The Switch (config - ge1/1) # sw mod hy

Switch(Config-ge1/1)# SW hybrid Allowed VLAN Add 2 Egres-Tagged disable

The Switch (config - ge1/1) # 2 en voice vlan

The Switch (config - ge1/1) # 2 enable voice vlan

The Switch (config - ge1/1) # int ge1/2

The Switch (config - ge1/2) # sw mod tr

Switch(config-ge1/2)# SW trunk VLAN Add 2

The Switch (config - ge1/2) # exit

Switch(config)#voice-vlan Oui 0009.ca00.0000 Mask ffff.ff00.0000

The Switch # (config)

## 1.28 A VLAN map

### 1.28.1 An introduction to VLAN mapping

VLAN Mapping (VLAN Mapping) can modify the VLAN Tag carried by the message to provide the following Mapping relationship: 1:1 VLAN Mapping: change the VLAN ID in the VLAN Tag carried by the message to another VLAN ID.

Before configuring a VLAN map, you must first create the corresponding VLAN.

### 1.28.2 VLAN mapping configuration

| The command | describe | CLI mode |
|---|---|---|
| Vlan -mapping vlan <1-4094> map-vlan <1-4094> | A VLAN mapping relationship for configuring ports | Interface configuration mode |
| No vlan - mapping vlan < > | Deletes a VLAN mapping | Interface |

| | | |
|---|---|---|
| 1-4094 | relationship for the port | configuration mode |
| No vlan - mapping | Remove all VLAN mappings for ports | Interface configuration mode |
| Vlan - mapping the enable | VLAN mapping relationships for startup ports | Interface configuration mode |
| Vlan - mapping the disable | Close the VLAN mapping relationship for the port | Interface configuration mode |
| Show vlan - mapping | Displays VLAN mappings for all configurations | Privileged mode |

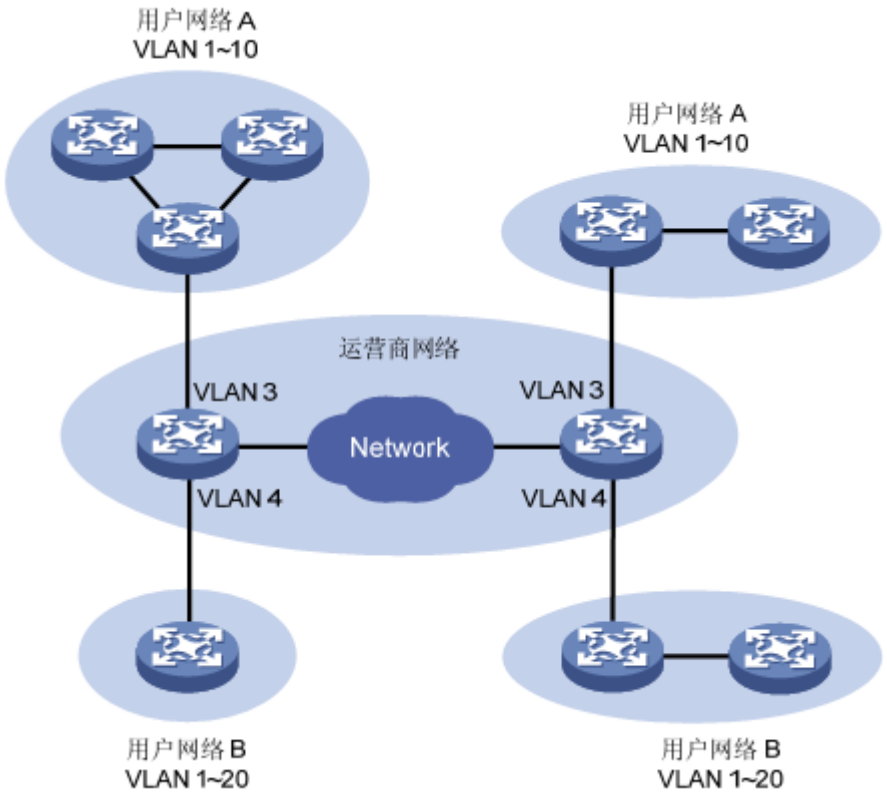
## 1.29 QinQ

### 1.29.1 Qinq introduction

The port QinQ provided by the device is a simple and flexible two-layer VPN technology, which encapsulates the outer VLAN Tag for the user's private network message on the operator's network edge device, so that the message carries two layers of VLAN Tag across the operator's backbone network (public network). In the public

network, the device only forwards the message according to the outer VLAN Tag, and learns the MAC address table item of the message source to the MAC address table of the VLAN where the outer Tag is located, while the VLAN Tag of the user in the private network will be transmitted as the data part of the message during transmission.

QinQ features enable operators to use one VLAN to serve user networks with multiple VLANs. As shown in the figure below, the VLAN of the private network of user Network A is VLAN 1 ~ 10, and that of user network B is VLAN 1 ~ 20. The VLAN assigned by the operator to user network A is VLAN 3, and the VLAN assigned to user network B is VLAN 4. When the message with VLAN Tag of user Network A enters the operator network, A LAYER of VLAN Tag with VLAN ID 3 will be wrapped outside the message. When the packet with VLAN Tag of user network B enters the operator network, a LAYER of VLAN Tag with VLAN ID 4 will be wrapped outside the packet. In this way, messages from different user networks are completely separated during public network transmission. Even if the VLAN range of two user networks overlaps, there will be no confusion during public network transmission.




QinQ features enable the network to provide a maximum of 4094X4094 VLans, to meet the number of VLAN requirements of man, it mainly solves the following problems:

(1) To alleviate the increasingly scarce public network VLAN ID resources.

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

(3) To provide a relatively simple two-layer VPN solution for small man or enterprise network.

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

(1) Basic QinQ: Basic QinQ is realized based on the port mode. After enabling basic QinQ function of the port, when a message is received on the port, the device will type the VLAN Tag of the default VLAN of the port for the message. If the message is received with a

VLAN Tag, the message becomes a double-tag message. If a message is received without a VLAN Tag, it becomes a message with the default VLAN Tag of the port.

QinQ is a more flexible realization of QinQ, which is based on the combination of ports and VLAN. In addition to realizing all basic functions of QinQ, messages received on the same port can also make different actions according to different VLans, adding different outer VLAN tags to messages with different inner VLAN ids.

## 1.29.2 Qinq configuration

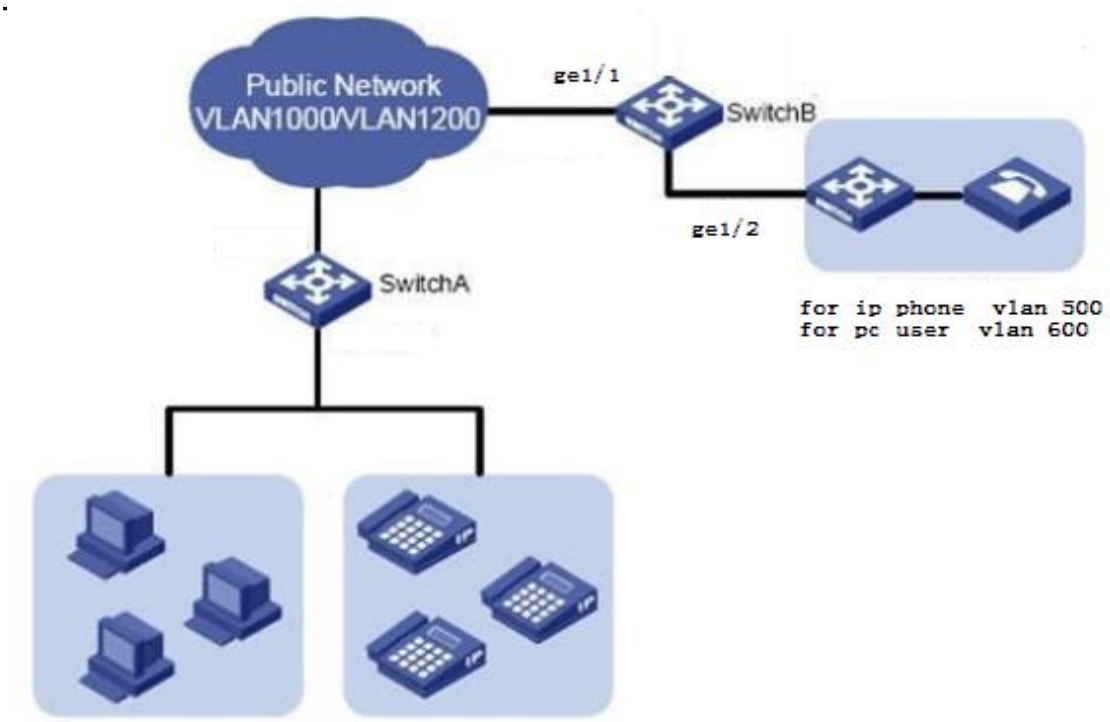
| The command | describe | CLI mode |
|---|---|---|
| Qinq tpid WORD | Configure the TPID value carried in the port VLAN Tag, which defaults to 0x8100 | Interface configuration mode |
| No qinq tpid | Restore port default TPID | Interface configuration mode |
| Qinq uplink | Configure port as Uplink port | Interface configuration mode |
| No qinq uplink | Unconfigure the uPLink port | Interface configuration |

| | | |
|---|---|---|
| | | mode |
| Qinq customer | Configure port as Customer port | Interface configuration mode |
| No qinq customer | Unconfigure the Customer port | Interface configuration mode |
| Qinq outer-vid <1-4094> inner-vid VLAN_ID | Configure a VLAN transformation for the interface | Interface configuration mode |
| Qinq outer-vid <1-4094> [inner-vid VLAN_ID] | Removes a VLAN transformation for the interface | Interface configuration mode |
| Show qinq | Qinq is displayed for all configuration | Privileged mode |

## 1.29.3 Qinq configuration example

The switch port Ge1/1 access to the public network, port GE1/2 access to PC and telephone server, the PC used by the VLAN is 600, IP phone used by the VLAN is 500, the public network allows vLAN100, VLAN200 message, in order to make the PC user data through VLAN200 in the public network transmission, IP phone data through VLAN100 in the public network transmission.

The networking diagram is shown below




The configuration of switch B is as follows:

Switch# con t

The Switch # vlan da (config)

The Switch (config - vlan) # vlan 100

The Switch (config - vlan) # vlan 200

The Switch (config - vlan) # exit

The Switch (config) # int ge1/1

The Switch (config - ge1/1) # sw mod tr

Switch(config-ge1/1)# Switchport trunk VLAN Add 100

Switch(config-ge1/1)# Switchport trunk VLAN Add 200

The Switch (config - ge1/1) # qinq uplink

The Switch (config - ge1/1) # int ge1/2

The Switch (config - ge1/2) # switchport mode hybrid

Tagged dis (Config-GE1/2)# Switchport hybrid Allowed VLAN Add 100 Egress-Tagged dis

Tagged dis (Config-GE1/2)# Switchport hybrid Allowed VLAN Add 200 Egress-Tagged dis

The Switch (config - ge1/2) # qinq customer

Qinq OUTER-vid 100 Nei-vid 500

Qinq OUTER-vid 200 Inner - VID 600

The Switch (# config - ge1/2)

```
Switch# show qinq
Ifname TPID DTAG-MODE OUTER-VID
Ge1/1 0x8100 Uplink --
Ge1/2 0x8100 Customer 100 500
Ge1/2 0x8100 Customer 200 600
Switch#
```

# Chapter 8 To configure QoS

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

- QoS is introduced
- QoS configuration
- QoS configuration example

## 1.30 QoS is introduced

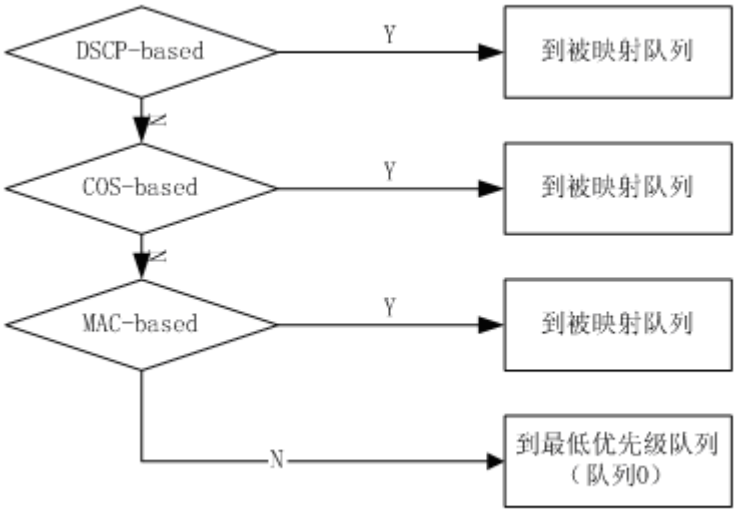
Using the switch's QoS capabilities, you can give priority to important data streams forwarded through the switch, make your network bandwidth utilization more reasonable, and make network performance predictable.

In a switch, a packet is queued at the output terminal based on its priority information at the input terminal.

The switch implements QoS based on COS(802.1p), QoS based on DSCP(DiffServ)

and QoS based on MAC.Dscp-based QoS can be configured on a physical port;Physical ports start cos-based QoS by default.Mac-based Qos functionality is configured in MAC binding functionality. Only one QoS function can be configured per physical port.

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




The switch supports eight priority queues from 0 to 7, with queue 7 having the highest priority and queue 0 having the lowest.Priority queues can be scheduled in four ways: SP, RR, WRR and WDRR.SP is strict priority scheduling, that is, it always forwards the packets of queue 7 first until the packets of queue 7 are forwarded, then the packets of queue 6 are forwarded until the packets of queue 6 are forwarded, then the packets of queue 5 are forwarded until the packets of queue 6 are forwarded, and finally the packets of queue 0 are forwarded. RR is the scheduling mode of polling. When the switch forwards packets, it polls the forwarding packets from the high-priority queue to the low-priority queue, and each queue forwards one packet.WRR is weighted priority polling, switches, when forwarding packets, according to the configuration of the right to priority queue to the low priority queue polling forwarding packets, start with high priority number of packets forwarding right, forward the second-highest number of right of priority packets, until the

lowest priority queue forwarding, and starting from the high-priority forwarding, to push the class.WDRR is a weighted default polling scheduling mode, that is, the weight of queue 3 is 4, so in one round, it can forward 5 packets, and in the next round, it only forwards 3 packets. This flexibility is more suitable for highly cohesive network environments.

To facilitate user configuration, we introduced the concept of QosProfile. QosProfile is a property configured with 802.1p and priority queues mapped, which cannot be configured by the user.Their mapping relationship is shown in the following table:

| QosProfile | 802.1 p (CoS) values | Priority queue |
|---|---|---|
| Qp0 | 0 | 0 |
| Qp1 | 1 | 1 |
| Qp2 | 2 | 2 |
| Qp3 | 3 | 3 |
| Qp4 | 4 | 4 |
| Qp5 | 5 | 5 |
| Qp6 | 6 | 6 |
| Qp7 | 7 | 7 |

## 1.30.1 Cosine based QoS

The port enables cos-based QoS by default.The switch gets the priority value of the VLAN TAG in the packet that enters the port, and determines the output queue of the

packet based on the mapping relationship between the user configuration COS value and the queue. If the packet does not have a VLAN TAG or the VLAN TAG's VID is 0, the exchange populates the packet based on the default VID of the user-configured port and the default priority of the port, and then determines the output queue of the packet based on the default priority.

## 1.30.2 QoS based on DSCP

If a port is enabled for DSCP-based QoS, the exchange takes the DSCP value in the IP packet that enters the port and determines the output queue of the packet based on the mapping relationship between the user's configured DSCP value and the queue.

## 1.30.3 QoS based on MAC

When a packet enters the switch, the switch will look for the switch's second layer transfer according to the destination MAC of the packet and the VID of the VLAN TAG of the packet. If a target table item is found, the output queue of the packet will be determined according to the queue mapping relationship configured by the target table item.

## 1.30.4 Policy based QOS

QoS policies include classes and policy actions.Class is used to identify the flow. Users can define a series of rules by command to classify packets. Policy actions are used to define QoS actions for packets that match rules.If a port is enabled policy-based QoS, exchange opportunities to enter the port of packet classification, to meet the requirements of the classification data packets, exchange opportunities according to the corresponding strategic action to deal with the port packets for did not meet the requirements of classification of packets are not for processing, then determine the data

packets output mapping relations according to the priority queue.

## 1.31 QoS configuration

### 1.31.1 Default configuration for QoS

| Configuration items | value | Configurable or not |
|---|---|---|
| The queue number | 8 | no |
| scheduling | WRR | is |
| Whether to enable SP scheduling | disable | is |
| Whether RR scheduling mode is enabled | disable | is |
| Whether WDRR scheduling mode is enabled | disable | is |
| The queue weight | QP1 QP0 [1], [2], QP2 [4], QP3 [8]<br>QP5 QP4 [16], [32], QP6 [64]<br>QP7 [127] | is |
| The mapping between COS and QOSprofile | COS0 ~ [qp0]<br>COS1 ~ [qp1] | no |

| | | |
|---|---|---|
| | COS2 ~ [qp2]<br>COS3 ~ [qp3]<br>COS4 ~ [qp4]<br>COS5 ~ [qp5]<br>COS6 ~ [qp6]<br>COS7 ~ [qp7] | |
| Mapping relationship between DSCP and QOSProfile | DSCP0 ~ DSCP7 [qp0]<br>DSCP8 ~ DSCP15 [qp1]<br>DSCP16 ~ DSCP23 [qp2]<br>DSCP24 ~ DSCP31 [qp3]<br>DSCP32 ~ DSCP39 [qp4]<br>DSCP40 ~ DSCP47 [qp5]<br>DSCP48 ~ DSCP55 [qp6]<br>DSCP56 ~ DSCP63 [qp7] | is |
| Whether the interface enables DSCP-based qos | disable | is |
| Whether the interface enables cosine-based qos | The enable | no |
| Interface user priority (COS value) | 0 | is |

## 1.31.2 Configuration scheduling mode

The default scheduling mode for switches is WRR.SP, RR, WDRR scheduling can be configured by command.

| The command | describe | CLI mode |
|---|---|---|
| Qos sched {rr \| sp \| WRR \| WDRR} | Configure QoS scheduling mode | Interface configuration mode |

## 1.31.3 Configuring queue weights

| The command | describe | CLI mode |
|---|---|---|
| Qosprofile {qp0\|qp1\|qp2\|qp3\| qp4\|qp5\|qp6\|qp7} weight<1-127> | Configure the weights for each priority queue | Interface configuration mode |
| No qos qosprofile {qp0\|qp1\|qp2\|qp3\| qp4\|qp5\|qp6\|qp7 | The weight of the recovery queue is configured as the default | Interface configuration mode |

Queue weight refers to the number of packets forwarded by the priority queue in a poll. Therefore, when configuring queue weight, it should be noted that the weight of the low-priority queue should not exceed that of the high-priority queue.

## 1.31.4 Configure the mapping relationship between DSCP and QosProfile

| The command | describe | CLI mode |
|---|---|---|
| Qosprofile {qp0 b\| qp1\|qp2\|qp3\| qp4\|qp5\|qp6\|qp7} | Configure the mapping relationship between DSCP and QOSProfile. | Interface configuration mode |
| No qos qosprofile {qp0\|qp1\|qp2\|qp3\| qp4\|qp5\|qp6\|qp7 | Restore the mapping relationship between DSCP and QOSProfile as the default configuration. | Interface configuration mode |

## 1.31.5 Configure ports based on DSCP QoS

Qos functionality can only be configured on physical ports, not in TRUNK or three-tier interfaces.

| The command | describe | CLI mode |
|---|---|---|
| Qos DSCP - -based | Enable port based Qos functionality of DSCP. | Interface configuration mode |
| No qos DSCP - -based | Turn off port based Qos feature of DSCP. | Interface configuration mode |

### 1.31.6 Configure port user priority (COS value)

| The command | describe | CLI mode |
|---|---|---|
| Qos user - priority < 7 > 0 - | User priority for configuring ports (COS value) | Interface configuration mode |
| No qos user - priority | The user priority (COS value) of the recovery port is the default configuration. | Interface configuration mode |

## 1.32 QoS configuration example

Configure ge1/3 user priority (COS value) to be 3. Cos-based QoS function starts by default:

Switch# configure terminal

Switch# (config) # interface ge1/3

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

Switch# (config - ge1/3) # end

Configuration interface GE1/3 starts QoS function based on DSCP. DSCP value 3 is mapped to priority queue 2:

Switch# configure terminal

Switch# (config) # interface ge1/3

Switch#(config-ge1/3)#qos DSCP-map-QP 3 QOSprofile QP2

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

Switch# (config - ge1/3) # end

## 1.33 Example of policy QoS configuration

Configure acLs to capture data streams from source MAC1, MAC2, and MAC3, respectively

(Acl rules can be modified according to requirements, here is a simple example)

Access-list 700 Permit Host 0000.0000.1111 vid Any IP Any Any

Access-list 701 permit host 0000.0000.2222 vid Any IP Any Any

Access-list 702 permit host 0000.0000.3333 vid Any IP Any any

Configure QOS classes to match the data streams of source MAC1, MAC2 and MAC3 respectively

(The matching rule cos or DSCP can be modified according to the requirements. Here is just a simple example.)

Qos class 10 match ACL 700

Qos Class 11 match ACL 701

Qos class 12 match ACL 702

Configure QOS policies to re-mark the 802.1P priority of data streams from MAC1, MAC2, and MAC3, respectively

(The strategy can be modified according to the requirements, here is a simple example)

Qos Policy 10 Class 10 Remark cos 7

Qos Policy 10 Class 11 Remark cos 5

Qos Policy 10 Class 12 Remark cos 3

Issue QOS policies to ports

Interface ge1/2

Qos apply the policy - 10

# Chapter 9
# Configuration of MSTP

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

- MSTP is introduced
- MSTP configuration
- MSTP configuration example

## 1.34 MSTP is introduced

Switch support IEEE 802.1D,IEEE 802.1W,IEEE 802.1S standard STP protocol.

### 1.34.1 An overview of the

MSTP USES RSTP for fast convergence to aggregate multiple VLANs into a spanning tree instance, each with a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forward paths for data flows, enables load balancing, and reduces the number of spanning tree instances required to support a large number of VLANs.

## 1.34.2 Multiple spanning tree domain

The same MST configuration information for switches must be configured consistently for instances that participate in multi-spanning tree (MST) calculations. A collection of connected switches with the same MST configuration constitutes an MST domain.

The MST configuration determines the domain to which each switch belongs. Configuration includes domain name, revision number, and MST instance and VLAN assignment mappings; This information generates a unique Digest in the MST configuration. The summaries in the same domain are, and must be, the same, and you can view this information through the show spanning tree MST config command.

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

## 1.34.3 IST, CIST, and CST

Internal spanning tree (IST), a spanning tree running within the MST domain.

In each MST domain, MSTP maintains multiple build instances. Instance 0 is a special instance of a domain, called IST. All other MST instances are Numbers 1 through 15.

This IST is simply a spanning tree instance of receiving and sending a BPDU; All other spanning tree instance information is compressed in MSTI BPDU. Because the MSTI

BPDU carries information for all instances, the number of BPDus that need to be processed by a switch that supports multiple spanning tree instances means simplification.

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

A common and internal spanning tree (CIST) is a collection of all IST's in each MST domain, and a common spanning tree that connects an MST domain to a single spanning tree.

A spanning tree calculated within a domain looks like a subtree of CST containing all switch domains. CIST is formed by running spanning tree calculations between switches that support the 802.1W and 802.1D protocols. The CIST in the MST domain is the same as the CST outside the domain.

Common spanning tree (CST), spanning tree running between MST domains.

## 1.34.4 Field operations

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

When an MSTP switch is initialized, it sends the BPDU and requires itself to be the CST root and IST master, and the path cost to the CST root and IST master is set to 0.

Switches also initialize all MST instances and ask to be their roots. If the switch receives MST root information that takes precedence over the information currently stored on the port (low bridge ID, low path cost, etc.), it waives its requirement to become IST Master.

In initialization, a domain may have many subdomains, each with its own IST master. When the switch receives a more priority IST message, it leaves its old subdomain and joins into a new subdomain that may contain a real IST master. So all the subdomains shrink, except the ones that contain the real IST master.

In order to operate correctly, all switches within the MST domain must recognize the same IST master. So, any two switches in the domain synchronize their port roles to an MST instance, only if they converge to a common IST master.

### 1.34.5 Inter-domain operation

If there are multiple domains or early 802.1D switches in the network, the MSTP establishes and maintains the CST, which includes all MST domains in the network and all early STP switches. The MST instance combines the IST of the domain boundary to become CST.

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

Only CST instances send and receive BPDU, and MST instances increase their spanning tree information to the BPDU interacting with neighbor switches and compute the final spanning tree topology. Because of this, spanning tree parameters that involve BPDU transfers (e.g., Hello Time, forward time, Max-age, and Max-Hops) are configured

only on CST instances without affecting all MST instances. Parameters that involve the spanning tree topology (e.g., Switch Priority, Port VLAN Cost, Port VLAN Priority) can be configured for both CST instances and MST instances.

MSTP switches use version 3 RSTP BPDU or 802.1d BPDU and 802.1d switch communication. MSTP switches communicate using MSTP BPDU and MSTP switches.

## 1.34.6 Hop count

Message-age and maximum-age information is not used by IST and MST instances in the BPDU configured to compute the spanning tree topology. Instead, use the path to the root and the hop-count mechanism equivalent to IP TTL.

You can configure the maximum number of hops for that domain and apply it to that domain IST and all MST instances. The hop count implementation is the same as the message-age result (determined after a reconfiguration is raised). The instance root switch always sends a BPDU (or-M-record) with cost of 0 and hop-count as the maximum. When a switch receives a BPDU, it subdivides the remaining hops by 1 and propagates the remaining hops within the BPDU it produces.When the count reaches 0, the switch discards the BPDU and age the port information.

In a domain, message-age and maximum-age information in the RSTP BPDU section are retained consistently, and the same value is propagated at the specified port in the boundary domain.

## 1.34.7 The border port

A boundary port is a spanning tree that connects the MST domain to a single running RSTP, or a single 801.1d spanning tree, or any other different configured MST domain. A boundary port is also connected to a LAN whose designated switch is either a separate spanning tree switch or a switch with a different MST domain configuration.

In the boundary ports, the MST port role is not significant, and their state is enforced to be the same as that of IST port (when IST port is forwarding, MST port at the boundary is forwarding). An IST port at the boundary can have any role other than the backup port.

On a Shared boundary connection, the MST port will wait forward-delay time at the blocking state before switching to the learning state. MST ports wait for another forward-delay time to expire before turning into Forwarding.

If the boundary port is a point-to-point connection and is an IST root port, the MST port switches to Forwarding state as soon as IST port switches to forwarding state.

If a boundary port transitions into forwarding state among instances, it is forwarding among all instances, and a topology change is triggered. If a boundary port with an IST root or specified port role receives a topology change notification, the MSTP switch triggers a topology change for IST instances and all MST instances on that active port.

## 1.34.8 Interoperability between MSTP and 802.1D STP

A switch running MSTP supports a built-in protocol migration mechanism that enables

it to coordinate with 802.1d. If the switch receives an 802.1D configured BPDU from a port, it sends 802.1d BPDU on that port. The MSTP switch can detect when a domain boundary port receives an 802.1D BPDU and an MSTP BPDU or RSTP BPDU for a different domain.

However, if the switch no longer receives 802.1d BPDU it will not automatically revert to MSTP mode because it cannot determine whether the other party's switch has been removed from the connection unless the other party's switch is the specified switch. Also, when a switch connected to the switch has joined the domain, the switch may continue to assign a boundary port role to a port. Restart the migration processing of the protocol (force negotiation with the neighbor switch).

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

### 1.34.9 Port role

MSTP adopts RSTP fast convergence algorithm. The following is a brief introduction to MSTP port roles and fast convergence combined with RSTP.

RSTP provides fast convergence for specifying port roles and determining active topologies. RSTP is based on IEEE802.1D STP and selects the high-priority switch as the root switch. When RSTP specifies a port role to a port:

Root port - Provides the optimal path cost when the switch forwards packets to the

Root switch.

Designated port - Connect to the Designated switch. The lowest path cost occurs when forwarding packets from LAN to root switch. The port through which the switch is connected to the LAN is called the specified port.

Alternate Port - Provides a Alternate path to the root switch for the current root port.

Backup port- ACTS as a Backup of the specified port to the path to the generated tree leaf. A Backup port exists only when two ports are connected together on a point-to-point loop or when a switch has two or more connections to a Shared LAN segment.

Disable port- There is no port role in the spanning tree operation.

Master port - Located at the domain root or shortest path to the total root, it is the port that connects the domain to the total root.

The root port or specified port role is contained in the active topology. The replacement port or backup port role is not included in the active topology.

In a network of stable topology and fixed port roles, RSTP ensures that every root port and specified port is immediately migrated into Forwarding state when all replacement ports and backup ports are always in Discarding state. Port state controls Forwarding and Learning processing.

Rapid convergence

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

Edge Ports - If you configure a port as an Edge port, Edge ports are immediately migrated to Forwarding state. You can open it for boundary ports only if the port is

connected to a separate terminal or if the device does not need to compute the spanning tree.

Root ports - If RSTP selects a new Root port. It blocks an old root port and immediately migrates the new root port to forwarding state.

Point-to-point links-If you connect one port to another by a point-to-point connection and the local port becomes a designated port, it and the other ports negotiate a quick migration via the proposal-Agreement handshake to determine a quick convergence loloop topology.

Topology changes

This section describes the difference between RSTP and 802.1d in handling the spanning tree topology change.

Unlike 802.1D, any migration between the blocking and forwarding states will cause topology change, only migration from the blocking to forwarding state will cause RSTP topology change (only topology change is considered to increase connectivity). State changes at an edge port do not cause topology changes. When an RSTP switch detects a topology change, it floods it learning information to all nonedge ports except the ports receiving TC information.

Notification - Unlike 802.1d, which USES TCN BPDU, RSTP does not use it. However, for interoperability with 802.1D, the RSTP switch processes and produces TCP BPDU.

Acknowledgement - When an RSTP switch receives a TCN message from an 802.1D switch on a specified port, it responds with an 802.1D BPDU and sets the TCA flag bit. However, if the TC-while timer(the same topology-change timer as 802.1d) is active, the TC-while timer resets when the root port connects to the 802.1d switch and receives a

configuration BPDU with TCA. This behavior is only required to support the 802.1d switch. RSTP BPDU never has the TCA flag bit.

Propagation - When an RSTP switch receives a TC message from another switch via a specified port or root port, it propagates to all non-edge ports, specifying ports and root ports (except the receive port). Switches all such ports start TC-While timer and flood the information they learn.

Protocol Migration - To backward-compatible 802.1d switches, RSTP selectively sends 802.1d BPDU and TCN BPDU based on each port.

When a migrate-delay timer is started (specifying the minimum duration for which RSTP BPDU is to be sent), RSTP BPDU is sent. When this timer is active, the switch handles all BPDU received from the port and ignores protocol types.

After the port migration-delay Timer has been aborted, if the switch receives an 802.1d BPDU, it assumes that it is connected to an 802.1d switch and starts using the 802.1d PROTOCOL BPDU. However, if the RSTP switch is using 802.1d BPDU on a port and receives an RSTP BPDU after the timer is aborted, that port restarts the timer and starts using RSTP BPDU.

## 1.34.10 802.1d Spanning tree introduction

Spanning tree protocol is based on the following points:

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

2) Each switch has a unique Brideg Identifier;

3) Each switch has a unique Port Identifier. Managing the configuration of the tree also requires: coordinating a relative priority for each switch; To assign a relative priority to each port of each switch; Cost of tuning a path per port.

The switch with the highest priority is called the root switch. Each switch port has a root path cost, which is the sum of the path costs of each network segment that the switch passes through. The port with the lowest value of root path cost in a switch is called the root port, and if multiple ports have the same root path cost, the port with the highest priority is the root port.

Within each LAN there is a switch called designated, which belongs to the switch with the least cost root path in the LAN. The port that connects the LAN to the designated switch is the DESIGNATED port of the LAN. If more than two ports in the specified switch are connected to the LAN, the port with the highest priority is selected as the specified port.

Elements that must be determined to form a spanning tree:

1) Determine the root switch

A. At the beginning, all switches consider themselves as root switches;

B. The switch sends configuration BPDU to the LAN broadcast connected to it with the same root_ID value as bridge_ID;

C. When the switch receives the configuration BPDU from another switch, if it finds that the value of root_ID field in the received configuration BPDU is greater than the value of root_ID parameter in the switch, the frame is discarded; otherwise, the switch will continue to broadcast the configuration BPDU with the new value after updating the parameters such as root_ID, root path cost, root_path_cost, etc.

2) Determine the root port

The port with the lowest root path cost value in a switch is called the root port.

If more than one port has the same lowest root path cost, the port with the highest priority is the root port. If two or more ports have the same lowest root path cost and highest priority, the port with the smallest port number is the default root port.

3) Identify the designated LAN switch

A. At the beginning, all switches consider themselves LAN specific switches.

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

C. If at some point the specified switch receives a configuration BPDU sent by another switch on the LAN in competition for a designated switch, the specified switch will send a response configuration BPDU to redetermine the specified switch.

4) Decide to specify ports

The port connected to the LAN on the specified switch of a LAN is the specified port. If the specified switch has two or more ports connected to the LAN, the port with the lowest identity is the specified port.

All ports will be blocked except the root port and the specified port. Thus, after determining the root switch, the root port of the switch, and the specified switch and port for each LAN, the topology of a spanning tree is determined.

## 1.35 MSTP configuration

### 1.35.1 The default configuration

| The command parameter | The default value |
|---|---|
| So "spanning tree MST enable" | Shut down |
| So Spanning tree MST priority | 32768 |
| So spanning-tree MST hellotime (switch cist hellotime) | 2 seconds, |
| So spanning-tree MST forward time. | 15 seconds |
| So let's spanning a tree MST max-age. | 20 seconds |
| So spanning tree MST max-hops(switch cist max-hops) | 20 seconds |
| Instance 1 Priority | 32768 |
| So spanning-tree MST instance 1 priority | 128 |
| So spanning-tree MST instance 1 path-cost(port instance path-cost) | 20000000 |
| So spanning tree MST priority | 128 |
| So spanning tree MST path-cost (port cist path-cost) | 20000000 |

## 1.35.2 General configuration

Start the MSTP

The default MSTP configuration is turned off at startup.

The configuration process to start the MSTP is:

Switch# configure terminal

The Switch (config) # spanning - tree MST enable

The command to turn off MSTP is:

Switch# configure terminal

The Switch # no spanning - tree MST (config)

Configuration of Max - age

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

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

Configuration process:

Switch# configure terminal

The Switch (config) # spanning - tree MST Max - age < seconds >

Configuration of Max - hops

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

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

Configuration process:

Switch# configure terminal

Switch (config) # spanning - tree MST Max - hops < hop count - >

Configure forward - time

Configuring forward-time is for all instances. Forward-time is the number of seconds that ports wait from Discarding to learning and from learning to Forwarding.

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

Configuration process:

Switch# configure terminal

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

Hello - time

Configuring Hellotime is a configuration for all instances. Hello-time is the interval between the root switch generating configuration information.

The default configuration time is 2 seconds and the configuration range is 1 to 10

seconds. According to the generation number protocol, hello-time must satisfy the following conditions: 2*(hello-time + 1) =< max-age.

Configuration process:

Switch# configure terminal

So let's spanning-tree MST hello-time <seconds>

Configure PRIORITY for the CIST Bridge

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

Configuration process:

Switch# configure terminal

The Switch (config) # spanning - tree MST priority < priority >

The configuration is CISCO compatible

The network switch USES the MSTP protocol based on 802.1s. The length of each MSTI message is 16 bytes. The BPDU of the CISCO switch is 26 bytes per MSTI message. To interoperate with CISCO switches, configure the network switch with a CISCO compatible switch on.

When starting a CSCO compatible configuration, it is considered the same domain as long as the domain name and revision number are the same when determining whether it is the same domain.

The default system does not enable this feature.

CISCO compatible:

Switch# configure terminal

The Switch (config) # spanning - tree MST cisco - interoperability enable

CISCO compatible with off:

Switch# configure terminal

The Switch (config) # spanning - tree MST cisco - interoperability disable

Reset the protocol check task

In order to be compatible with the 802.1D STP protocol, the system can automatically detect the operating protocol of the other system. The protocol to run on this port is determined by the protocol to run on the other side.

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

Reset the entire device for protocol reconnaissance missions:

Switch# clear spanning - tree detected separate protocols

Protocol reconnaissance mission to reset a port:

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

## 1.35.3 Domain configuration

Two or more devices in the same domain must have the same VLAN instance mapping, the same modified version number, and the same domain name.

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

For instance configuration, only domain name configuration and revision number configuration are described in 'Instance configuration'.

Configure domain name:

Switch# configure terminal

The Switch # spanning - tree MST configuration (config)

Switch (config - MST) # region < region - the name >

Configuration Revision number:

Switch# configure terminal

The Switch # spanning - tree MST configuration (config)

The Switch (config - MST) # revision revision - num >

## 1.35.4 The instance configuration

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

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

The process of configuring an instance:

Switch# configure terminal

The Switch # spanning - tree MST configuration (config)

The Switch (config - MST) # instance < instance id > - vlan < vlan id > -

Priority for configuring MSTI Bridge

Default configuration 32768, configuration range <0-61440>; MSTI priority values can only be multiples of 4096.

Configuration process:

Switch# configure terminal

The Switch # spanning - tree MST configuration (config)

The Switch (config - MST) # instance < instance id > - priority < priority >

## 1.35.5 Port configuration

The mSTP-related port configuration information is described below. This is a simple configuration section, with Port Fast and Root Guard covered separately.

The process of configuring a port to join an instance:

Switch# configure terminal

Switch (config) # interface < if - the name >

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

Configure PRIORITY for CIST ports

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

Configuration process:

Switch# configure terminal

Switch (config) # interface < if - the name >

The Switch (config) # spanning - tree MST priority < priority >

Priority for configuring MSTI ports

The default configuration is 128 with a range of <0-240> and MSTI port priority values that can only be multiples of 16.

Configuration process:

Switch# configure terminal

Switch (config) # interface < if - the name >

So let's spanning-tree MST instance <instance-id> priority <priority>

Configure path-cost of CIST port

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

| Bandwidth (BPS) | Path spending |
|---|---|
| 100000 (100 k) | 200000000 |
| 1000000 (1 m) | 20000000 |
| 10000000 (10 m) | 2000000 |
| 100000000 (100 m) | 200000 |
| 1000000000 (1 g) | 20000 |
| 10000000000 (10 g) | 2000 |
| 100000000000 (100 g) | 200 |
| 1000000000000 (1 t) | 20 |
| > 1000000000000 | 2 |

The configuration process

Switch# configure terminal

Switch (config) # interface < if - the name >

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

Path-cost to configure MSTI port

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

The configuration process

Switch# configure terminal

Switch (config) # interface < if - the name >

So let's spanning-tree MST instance <instance-id> path-cost <path-cost>

Configure the version number of the send protocol package

The default configuration sends the MSTP protocol package with a configuration range of 0-3 and a mapping relationship of 0-STP, 2-RSTP, and 3-MSTP.

Configuration process:

Switch# configure terminal

Switch (config) # interface < if - the name >

So let's let the Switch(config) tree MST force-version <version-id>

Configure the connection type

If a port is connected point-to-point to another port, and the local port is designated port,RSTP determines an acyclic topology by negotiating a fast migration of the port it is connected to through the proposal-Agreement process to become the root port.

The following is a brief introduction to the negotiation process of proposal-Agreement.

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

If all other ports are synchronized with superior root information received from the root port, then the switch is synchronized.

When RSTP forces it to synchronize new root information, if a specified port is in Forwarding state and is not configured as an edge port, it migrates to the blocking state. Typically, when RSTP forces a port to synchronize a new root message and the port does not satisfy the above criteria, the port state is set to blocking.

When ensuring that all ports are synchronized, the switch sends an agreement message to the corresponding specified port on the root port. When switches connect to a point-to-point connection in agreement to their port role, RSTP immediately migrates the port state as Forwarding.

In the case of a Shared connection, the state of the port is determined through the calculation of 802.1d.

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

The connection type for configuring ports is a point-to-point connection:

Switch# configure terminal

Switch (config) # interface < if - the name >

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

The connection type of the configured port is a Shared connection:

Switch# configure terminal

Switch (config) # interface < if - the name >

Switch (config - ge1/2) # spanning - tree MST link -type Shared

## 1.35.6 PORTFAST related configuration

**1) the Port Fast**

Port Fast immediately transfers an Access or trunk Port from blocking to forwarding, bypassing listening and learning. So you can connect a single workstation and server using Port Fast, so you can let these devices connect to the network immediately without waiting for the spanning tree to stop.

Configure a port as fast Port:

Switch# configure terminal

Switch (config) # interface < if - the name >

The Switch # spanning - tree MST portfast (config)

**2) bpdus Filtering**

BPDU Filtering can be turned on globally based switches or on a per-port basis, but they vary.

In the global layer, you can use the spanning tree MST portfast bpd-filter command to enable the BPDU filtering function on the portfast Bpd-Filter default state.

So at the port layer, you can let the bpdu filter open on any port by using spanning tree MST portfast bpd-filter enable.

This feature prevents the Port Fast port from receiving or sending the BPDU.

Configuration bpdus Filtering

In global configuration mode:

Switch# configure terminal

So let's let the Switch(config) tree MST portfast bpdu filter

In interface configuration mode:

Switch# configure terminal

Switch (config) # interface < if - the name >

So let's Switch(config)#spanning tree MST portfast bpdu-filter enable

**3) bpdus Guard**

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

At the global layer, you can open the BPDU guard function on the port in the portfast bdu-Gurad default state using spanning tree MST Portfast Bdu-Guard.

In the port layer, you can open BPDU Guard on any port.

So when the port configured with BPDU Gurad receives the BPDU, the spanning tree stops the port. In a valid configuration, the Port Fast-enabled Port does not receive BPDU. Receiving a BPDU on a Port fast-enabled Port indicates an invalid configuration, such as an unauthorized device connection, and the BPDU Guard enters an error-disabled state.

Error-disabled means that when the port starting BPDU Gurad receives BPDU, the error-disable timer will be started if the system is configured with the error-disable mechanism. Error-disable restarts the port after the system-configured timeout.

In global configuration mode:

Switch# configure terminal

So let's let the Switch(config) tree MST portfast bspanning -guard

In interface configuration mode:

Switch# configure terminal

Switch (config) # interface < if - the name >

So there's a Switch(config)#spanning tree MST portfast bpdu-guard enable

Error - disable configuration

Enable the error-disable mechanism

Switch# configure terminal

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

Configure the error-disable timeout period

Switch# configure terminal

So let's let the spanning tree MST errdisable-timeout interval <seconds>

## 1.35.7 Root Guard related configuration

A SP layer 2 network can contain many connections to switches that do not belong to it. In such a topology, the spanning tree can reconfigure itself and select a client switch as the root switch. You can avoid this by configuring root Guard on the SP switch's connection to the switch's port on the client network. If the port in the customer network is selected as root port due to spanning tree calculation, the root Guard conplans the port to be root-inconsistent(Blocked) state to prevent the customer switch from becoming a root switch or from an existing path to the root.

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

If the switch operates in MST mode, root Guard forces the port to be the specified port. If a port is blocked because root Guard is in the BLOCKED state on the IST instance, it is blocked on all MST instances. A boundary port is a port connected to a LAN, specifying either an 802.1D switch or a switch with a different MST domain configuration.

One port is opened by Root Guard and applied to all vLANs to which the port belongs. Vlans can be aggregated and mapped to an MST instance.

The configuration process

Switch# configure terminal

Switch (config) # interface < if - the name >

The Switch (config) # spanning - tree MST guard root

## 1.36 MSTP configuration example

**(1) configuration**

Three switches are connected into a ring, and the spanning tree protocol of each switch needs to be opened to avoid the occurrence of loops. Perform the configuration on each switch separately.

Configuration of Switch 1:

The Switch > en

Switch# configure terminal

The Switch (config) # spanning the MST enable

Configuration of Switch 2:

The Switch > en

Switch# configure terminal

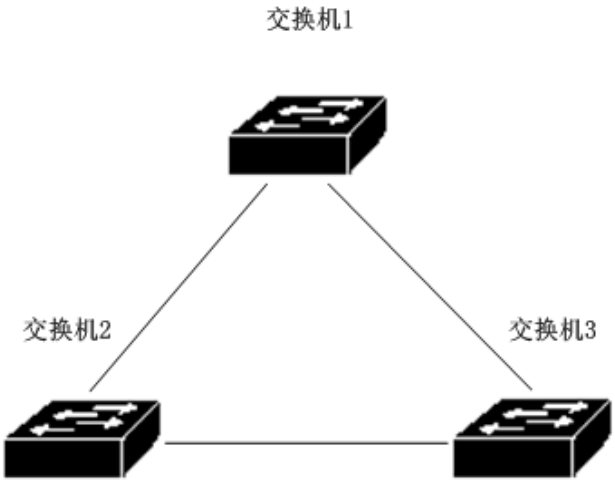
The Switch (config) # spanning the MST enable

Configuration of Switch 3:

The Switch > en

Switch# configure terminal

The Switch (config) # spanning the MST enable




**(2) the line fault:**

To see which switch is selected as the root bridge:

Perform show spanning tree MST and observe that the CISTRoot value is the smallest MAC address of the three exchanges, so that the root election result is correct.

Switch# show spanning - tree MST

View the port state of the switch in the spanning tree:

So let's execute the show spanning tree MST interface ge1/1 and look at the State value of PORT ge1/1 in instance 0

Switch#show spanning-tree MST interface ge1/1

# Chapter 10
# Configuration ERPS

## 1.37 Summary of ERPS

ERPS(Ethernet Ring Protection Switching Protocol) is a network Protection protocol (KNOWN as G.8032) developed by ITU. It is a link-layer protocol for Ethernet ring networks. It can prevent the broadcast storm caused by the data loop when the Ethernet ring network is complete, and can quickly restore the communication between the nodes of the Ethernet ring when a link is broken. ERPS protocol provides a fast Ethernet ring network protection mechanism, which can quickly restore network transmission in the case of ring network failure, thus ensuring high availability and high reliability of switches in the case of ring topology.

## 1.38 Introduction to ERPS technology

### 1.38.1 ERPS ring

The PRINCIPLE of ERPS rings is to minimize rings. Each ring must be the smallest ring. A ring that is not closed or closed; a subring. Both need to be configured by command.

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

## 1.38.2 ERPS node

The two-layer switching devices that join the ERPS ring are called nodes. No more than two ports per node can be added to the same ERPS ring, one RPL port and the other plain ring port.

Globally, the roles of nodes can be divided into the following two types: (1) Intersection nodes: In the intersecting ERPS ring, nodes belonging to multiple rings at the same time are called intersection nodes; (2) Non-intersecting nodes: In the intersecting ERPS ring, nodes that only belong to a certain ERPS ring are called non-intersecting nodes.

Node patterns stipulated in ERPS protocol mainly include THREE types: RPL owner node, RPL NEIGHBOUR node and common link point. A ERPS: (1) the RPL owner node only one ring RPL, owner node is determined by the user configuration, by blocking RPL port to prevent ERPS ring in the loop, when the RPL fault message owner node received ERPS ring other nodes or links that failure, will automatically open RPL port, the port to restore flow to send and receive, assure traffic not break; (2) RPL NEIGHBOUR node: the node directly connected with the RPL port of the RPL owner node. In normal circumstances, the RPL port of the RPL neighbour node and the RPL port of the RPL neighbour node are both blocked to prevent loop generation. When the ERPS ring fails, the RPL port of the RPL owner node and the RPL neighbour node are both released. (3)

common link point: in ERPS ring, in addition to the RPL owner node and RPL outside the neighbour node are ordinary link points, ordinary link point of RPL port and port is no different from ordinary ring, ordinary link point ring port is responsible for monitoring their direct agreement of link-state ERPS, and the change of link-state news timely notify the other nodes;

## 1.38.3 Links and Channels

(1)RPL (Ring Protection Link) : Each ERPS Ring has only one RPL, namely the Link where the RPL port of the RPL owner node is located. When the Ethernet ring is in Idle state, the RPL link is blocked and data packets are not forwarded to avoid loop formation.

(2) Sub-loop link: The link that belongs to and is controlled by a sub-loop in an intersection ring;

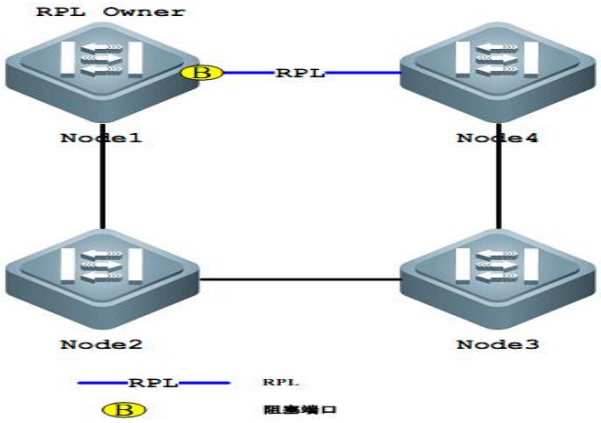
(3)RAPS (Ring Auto Protection Switch) Virtual Channel: In the intersecting Ring, the path not belonging to the sub-ring protocol is called RAPS virtual channel.

## 1.38.4 ERPS VLAN

There are two types of VLans in ERPS: (1)RAPS VLAN: RAPS VLAN is used to transmit ERPS protocol messages. Ports accessing ERPS ring belong to RAPS VLAN, and only ports accessing ERP ring can join this VLAN. The RAPS VLAN must be different for different rings. IP address configuration is not allowed on the interface of RAPS VLAN. (2) Data VLAN: As opposed to RAPS VLAN, data VLAN is used to transmit data messages. The data VLAN can contain both ERP ring ports and non-ERP ring ports.

## 1.39 How ERPS works

### 1.39.1 The normal state

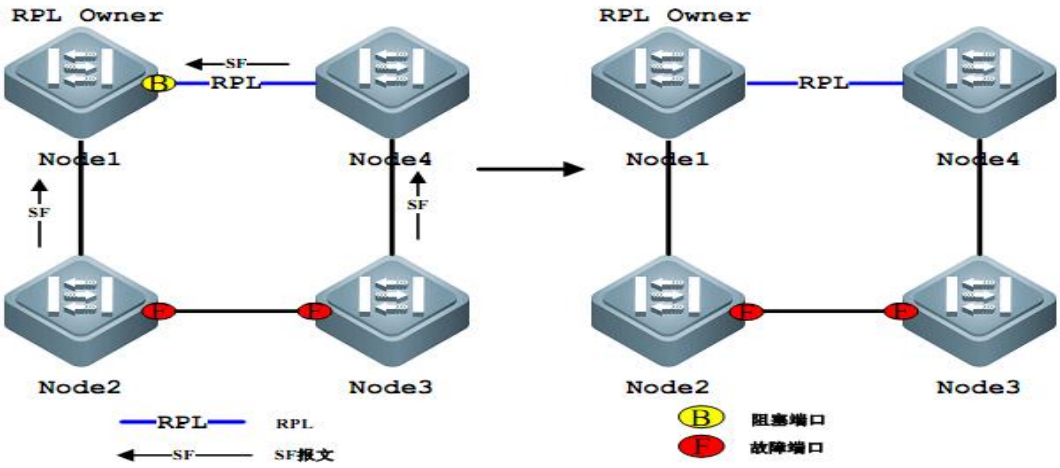



(1) All nodes are connected in the form of rings in the physical topology;

(2) Loop protection protocol ensures no loop formation by blocking RPL links. As shown in the figure above, the link between Node1 and Node4 is RPL link.

(3) Fault detection is carried out for each link between adjacent nodes.

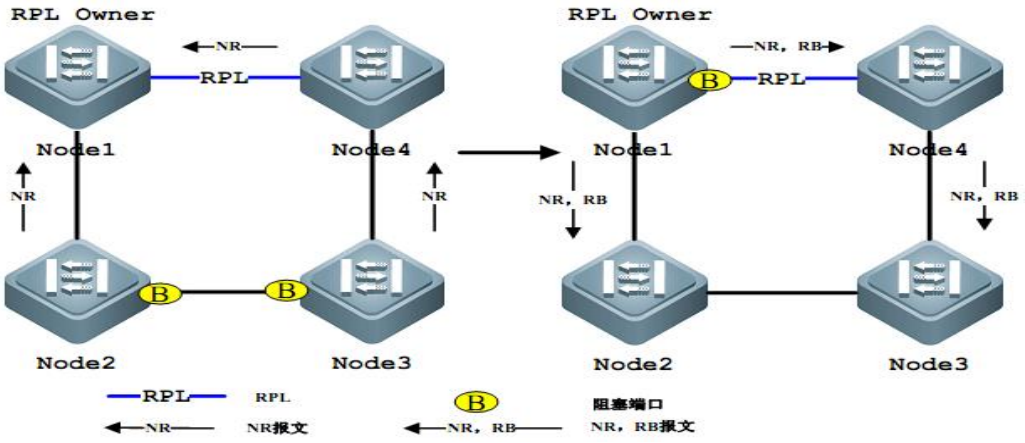
### 1.39.2 Link failures



(1) The nodes adjacent to the fault link block the fault link and use RAPS(SF) message to report the fault to other nodes on the ring, as shown in the figure above. Assuming that there is a link failure between Node2 and Node3, Node2 and Node3 will block the fault link after the holdoff timer times out, and send RAPS(SF) messages to each node on the ring network respectively;

(2) THE RAPS(SF) message triggers the RPL to have the node open the RPL port. The RAPS(SF) message also triggers all the nodes to update their MAC table entries, and then the nodes go into a protected state.

## 1.39.3 Link to restore




(1) When the fault recovers, the node adjacent to the fault continues to remain blocked and sends a RAPS(NR) message to indicate that there is no local fault;

(2) After the Guard timer runs out, the RPL Owner node starts the WTR timer after it receives the first RAPS(NR) message.

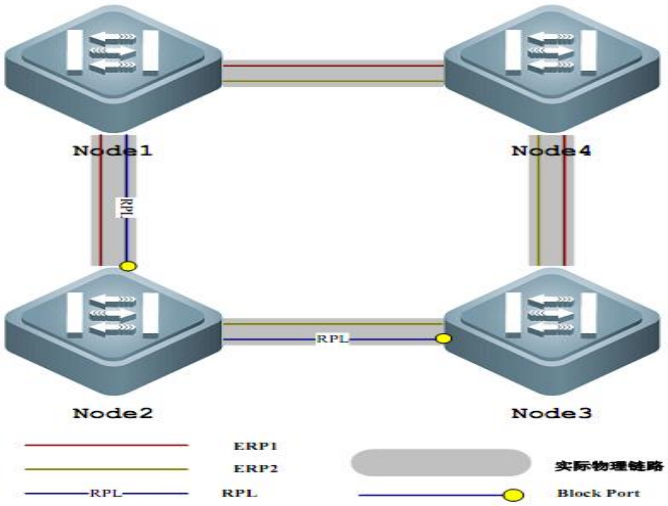
(3) When the WTR timer is exhausted, the RPL Owner node blocks the RPL and sends a RAPS(NR,RB) message;

(4) After receiving this message, other nodes update their MAC table entries, and the

node sending RAPS(NR) message stops sending messages periodically and opens the previously blocked port. The ring network returned to its original normal state.

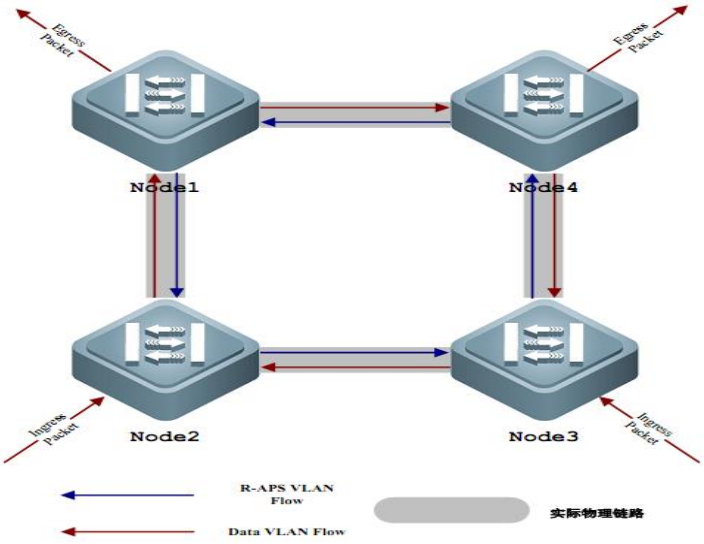
## 1.40 ERPS technical features

### 1.40.1 ERPS load balancing



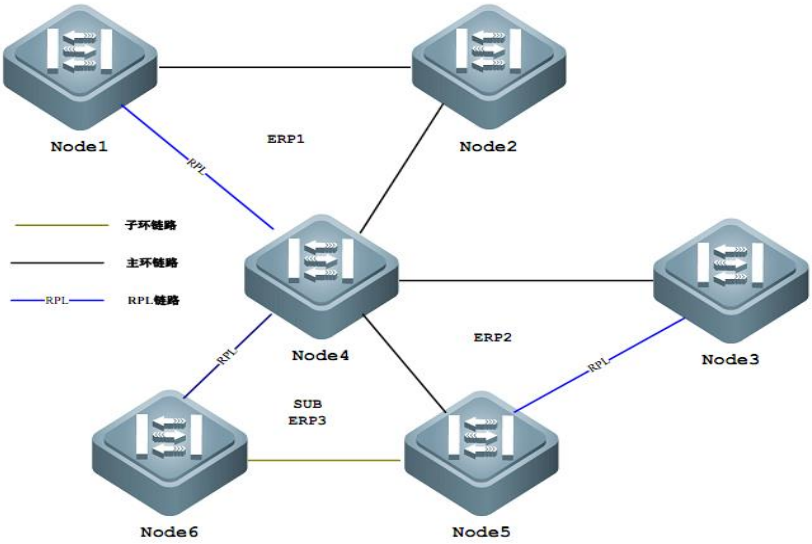

By configuring multiple instances and multiple ERPS rings in the same physical loop network, different ERPS loops transmit different VLAN (called protected VLAN) traffic, and different VLAN data traffic has different topology in the loop network, so as to achieve the purpose of load sharing. As shown in the figure above, a physical ring network corresponds to two instances of two ERPS rings. The vLans protected by the two ERPS rings are different. Node2 is the RPL owner node of ERP1 and Node3 is the RPL owner node of ERP2. Through configuration, different VLans can block different links, so as to realize the load sharing of a single ring.

## 1.40.2 Good safety




There are two types of VLANs in ERPS, RAPS vLANs and data VLANs. RAPS VLAN is only used to transmit ERPS protocol messages. However, ERPS only processes protocol packets from RAPS VLAN and will not process any protocol attack packets from data VLAN to improve the security of ERPS.

### 1.40.3 Support multi - ring intersection tangent




As shown in the figure above, ERPS supports the addition of multiple rings at the same node (Node4) in tangent or intersecting form, greatly increasing the flexibility of networking.

## 1.41 ERPS protocol command

| The command | describe | CLI mode |
|---|---|---|
| Erps predefine configuration (ring-node \| rpl-owner-node) | Enable ERPS predefined configuration | Global configuration mode |
| No erps predefine the configuration | Disable the ERPS predefined configuration | Global configuration mode |

| | | |
|---|---|---|
| Erps < 1-8 > | Create an instance of ERPS | Global configuration mode |
| No erps < 1-8 > | Delete an ERPS instance | Global configuration mode |
| Node - role (interconnection \| none - interconnection) | Configure the role of the node in the ERPS ring, connected or unconnected | ERPS mode |
| Ring < 1-32 > | Create an ERPS ring | ERPS mode |
| No ring < 1-32 > | Delete an ERPS ring | ERPS mode |
| Ring <1-32> ring-mode (major-ring \| sub-ring) | Configure ERPS ring mode, main ring or subring | ERPS mode |
| Ring <1-32> node-mode (rpl-owner-node \| rpl-neighbor-node \| ring-node) | Configure ERPS link point mode, RPL Owner node, RPL Neighbor node, or normal link point | ERPS mode |
| Ring < 1-32 > raps - vlan < > 2-4094 | Configure the ERPS ring protocol VLAN | ERPS mode |
| No ring < 1-32 > raps - vlan | Remove the ERPS ring protocol VLAN | ERPS mode |
| Ring < 1-32 > traffic - vlan < > 1-4094 | Configure the ERPS ring data VLAN | ERPS mode |

| | | |
|---|---|---|
| No ring <1-32> traffics-vlan <1-4094> | Delete the ERPS ring data VLAN | ERPS mode |
| Ring < 1-32 > (RPL - port \| rl - port) IFNAME | Configure ERPS ring ports, RPL ports, or plain ring ports | ERPS mode |
| No ring < 1-32 > (RPL - port \| rl - port) | Remove the ERPS ring port | ERPS mode |
| Ring < 1-32 > revertive - behaviour (revertive \| non - revertive) | Configure the ERPS ring recovery behavior, recoverable or unrecoverable | ERPS mode |
| Ring < 1-32 > hold - off - time > < 0-10000 | Configure the ERPS ring hold-off time | ERPS mode |
| No ring < 1-32 > hold - off - time | Restore the ERPS ring hold-off default time | ERPS mode |
| Ring < 1-32 > guard - time > < 10-2000 | Configure the ERPS ring Guard time | ERPS mode |
| No ring < 1-32 > guard - time | Restore ERPS ring Guard default time | ERPS mode |
| Ring < 1-32 > WTR - time > < 1-12 | Configure the ERPS ring WTR time | ERPS mode |
| No ring < 1-32 > WTR - time | Restore the default time of the ERPS ring WTR | ERPS mode |

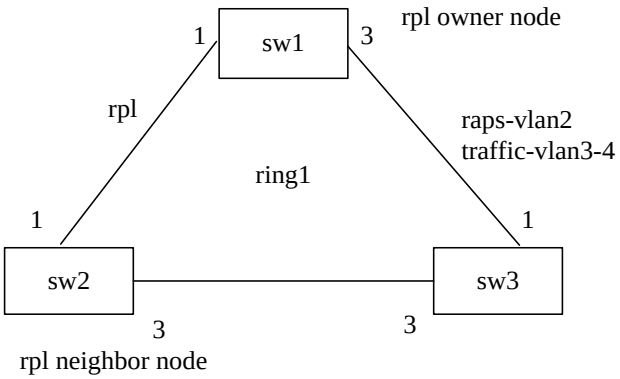
| | | |
|---|---|---|
| Ring < 1-32 > WTB - time allows 10 > < 1 - | Configure THE ERPS ring WTB time | ERPS mode |
| No ring < 1-32 > WTB - time allows | Restore the ERPS ring WTB default time | ERPS mode |
| Ring < 1-32 > raps - send - time 10 > < 1 - | Configure the ERPS ring protocol message sending time | ERPS mode |
| No ring < 1-32 > raps - send - time | Restore the default sending time of ERPS ring protocol message | ERPS mode |
| Ring < 1-32 > (enable \| disable) | Open or close the ERPS ring | ERPS mode |
| Ring < 1-32 > forced - switch IFNAME | Force a switch to the ERPS ring port | ERPS mode |
| Ring < 1-32 > clear forced - switch | Clear the forced switch of the ERPS ring | ERPS mode |
| Ring < 1-32 > manual - switch IFNAME | Manually switch the ERPS ring port | ERPS mode |
| Ring < 1-32 > clear manual - switch | Clear manual handoff of the ERPS ring | ERPS mode |
| Ring < 1-32 > clear recovery | Manual recovery when unrecoverable behavior of ERPS rings is removed or manual recovery before | ERPS mode |

| | | |
|---|---|---|
| | WTR/WTB expires | |
| Show erps | Displays a summary of all ERPS instances and rings of the device | Privileged mode |
| Show erps < 1-8 > | Displays the details of a single ERPS instance and ring for the device | Privileged mode |

## 1.42 Typical ERPS applications

### 1.42.1 As single sample

As shown in the figure below, sw1, SW2 and SW3 nodes constitute an ERPS single ring1. Ports 1 and 3 of each node are erPS ring ports. The protocol VLAN of the ring is 2, and the data VLAN is 3 and 4.



(1) Configure SW1:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-4

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS single ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode RPL-owner-node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

(2) the sw2 configuration:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-4

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS single ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode RPL-neighbor-Node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

(3) the configuration sw3:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-4

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS single ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode Ring-node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

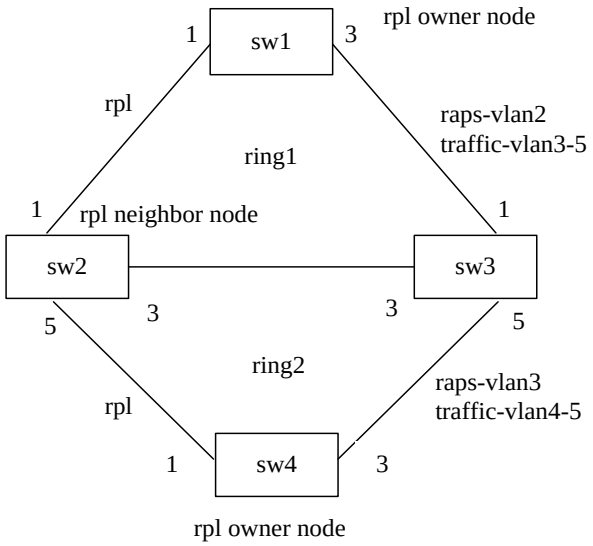
The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

## 1.42.2 Polycyclic sample

As shown in the figure below, sw1, SW2 and SW3 nodes form a ring1 ring of ERPS. Ports 1 and 3 of sw1, SW2 and SW3 nodes serve as the ring1 ring ports. The protocol VLAN of ring1 is 2, and the data VLAN is 3, 4 and 5.

Sw2, SW3 and SW4 nodes form a subring ring2 of ERPS. The 5 ports of sw2 and SW3 nodes and the 1 and 3 ports of SW4 nodes are the subring ring2 ring ports. The protocol VLAN of the subring ring2 is 3, and the data VLAN is 4 and 5.




(1) Configure SW1:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-5

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS main ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode RPL-owner-node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 Traffic_VLAN 5

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

(2) the sw2 configuration:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-5

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

The Switch (config - ge1/3) # exit

The Switch (config) # interface ge1/5

The Switch (config - ge1/5) # switchport mode trunk

Switch(config-ge1/5)# Switchport trunk VLAN Add 3

Switch(config-ge1/5)# Switchport trunk VLAN Add 4

Switch(config-ge1/5)# Switchport trunk VLAN Add 5

The Switch (config - ge1/5) # exit

Configure ERPS instance 1, ERPS main ring 1, and sub-ring 2

The Switch (config) erps # 1

The Switch (config - erps - 1) # node - role interconnection

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode RPL-neighbor-Node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 Traffic_VLAN 5

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # 2 ring

Switch(config-erps-1)# ring 2 Ring-mode sub-ring

Switch(config-erps-1)# ring 2 Node-mode Ring-node

Switch(config-erps-1)# ring 2 RAPs-VLAN 3

Switch(config-erps-1)# Ring 2 Traffics-VLAN 4

Switch(config-erps-1)# Ring 2 Traffics-VLAN 5

Switch(config-erps-1)# ring 2 RPL-port ge1/5

The Switch (config - erps - 1) # 2 enable ring

The Switch (config - erps - 1) # exit

(3) the configuration sw3:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-5

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

The Switch (config - ge1/3) # exit

The Switch (config) # interface ge1/5

The Switch (config - ge1/5) # switchport mode trunk

Switch(config-ge1/5)# Switchport trunk VLAN Add 3

Switch(config-ge1/5)# Switchport trunk VLAN Add 4

Switch(config-ge1/5)# Switchport trunk VLAN Add 5

The Switch (config - ge1/5) # exit

Configure ERPS instance 1, ERPS main ring 1, and sub-ring 2

The Switch (config) erps # 1

The Switch (config - erps - 1) # node - role interconnection

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode Ring-node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 Traffic_VLAN 5

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # 2 ring

Switch(config-erps-1)# ring 2 Ring-mode sub-ring

Switch(config-erps-1)# ring 2 Node-mode Ring-node

Switch(config-erps-1)# ring 2 RAPs-VLAN 3

Switch(config-erps-1)# Ring 2 Traffics-VLAN 4

Switch(config-erps-1)# Ring 2 Traffics-VLAN 5

Switch(config-erps-1)# ring 2 RPL-port ge1/5

The Switch (config - erps - 1) # 2 enable ring

The Switch (config - erps - 1) # exit

(4) Configure SW4:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 3-5

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS subring 2

The Switch (config) erps # 1

The Switch (config - erps - 1) # 2 ring

Switch(config-erps-1)# ring 2 Ring-mode sub-ring

Switch(config-erps-1)# ring 2 Node-mode RPL-owner-node

Switch(config-erps-1)# ring 2 RAPs-VLAN 3

Switch(config-erps-1)# Ring 2 Traffics-VLAN 1

Switch(config-erps-1)# Ring 2 Traffics-VLAN 4

Switch(config-erps-1)# Ring 2 Traffics-VLAN 5

Switch(config-erps-1)# ring 2 RPL-port ge1/1

Switch(config-erps-1)# ring 2 RL-port ge1/3

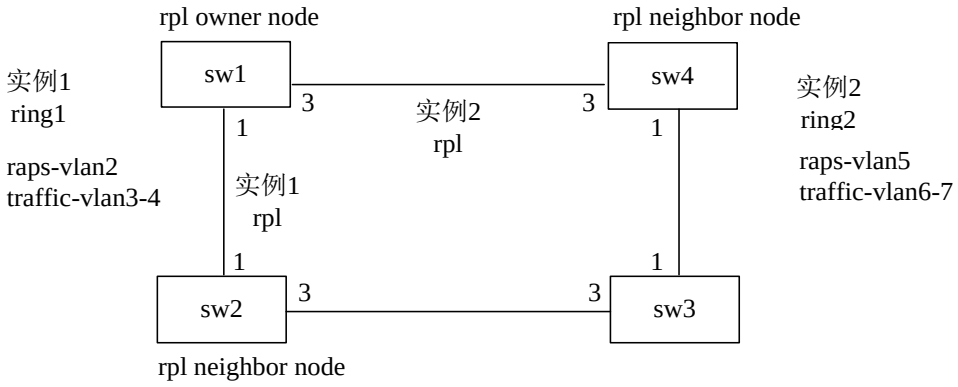
The Switch (config - erps - 1) # 2 enable ring

The Switch (config - erps - 1) # exit

## 1.42.3 Multi-instance load balancing example

As shown in the figure below, sw1, SW2, SW3 and SW4 nodes constitute a single ring1 of ERPS instance 1. Ports 1 and 3 of each node are erPS ring ports. The protocol VLAN of the ring is 2, and the data VLAN is 3 and 4.

Sw1, SW2, SW3 and SW4 nodes constitute a single ring2 of ERPS instance. Ports 1 and 3 of each node are erPS ring ports. The protocol VLAN of the ring is 5, and the data VLAN is 6 and 7.




(1) Configure Instance 1:

Configure sw1:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-4

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS single ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode RPL-owner-node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

Configure sw2:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-4

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS single ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode RPL-neighbor-Node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

Configuration sw3:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-4

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS single ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode Ring-node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

Sw4 configuration:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2-4

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 2

Switch(config-ge1/1)# Switchport trunk VLAN Add 3

Switch(config-ge1/1)# Switchport trunk VLAN Add 4

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 2

Switch(config-ge1/3)# Switchport trunk VLAN Add 3

Switch(config-ge1/3)# Switchport trunk VLAN Add 4

The Switch (config - ge1/3) # exit

Configure ERPS instance 1, ERPS single ring 1

The Switch (config) erps # 1

The Switch (config - erps - 1) ring # 1

Switch(config-erps-1)# ring 1 Ring-mode major-ring

Switch(config-erps-1)# ring 1 Node-mode Ring-node

Switch(config-erps-1)# ring 1 RAPs-VLAN 2

Switch(config-erps-1)# ring 1 Traffic_VLAN 1

Switch(config-erps-1)# ring 1 Traffic_VLAN 3

Switch(config-erps-1)# ring 1 Traffic_VLAN 4

Switch(config-erps-1)# ring 1 RPL-port ge1/1

Switch(config-erps-1)# ring 1 RL-port ge1/3

The Switch (config - erps - 1) # 1 enable ring

The Switch (config - erps - 1) # exit

(2) Configuration Instance 2:

Configure sw1:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 5-7

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

Switch(config-ge1/1)# Switchport trunk VLAN Add 6

Switch(config-ge1/1)# Switchport trunk VLAN Add 7

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

Switch(config-ge1/3)# Switchport trunk VLAN Add 6

Switch(config-ge1/3)# Switchport trunk VLAN Add 7

The Switch (config - ge1/3) # exit

Configure ERPS instance 2, ERPS single ring 2

The Switch # 2 erps (config)

The Switch (config - erps - 2) # 2 ring

Switch(config-erps-2)# ring 2 Ring-mode major-ring

Switch(config-erps-2)# ring 2 Node-mode RPL-owner-node

Switch(config-erps-2)# ring 2 RAPs-VLAN 5

Switch(config-erps-2)# ring 2 Traffics-VLAN 1

Switch(config-erps-2)# Ring 2 Traffics-VLAN 6

Switch(config-erps-2)# Ring 2 Traffics-VLAN 7

Switch(config-erps-2)# ring 2 RPL-port ge1/3

Switch(config-erps-2)# ring 2 RL-port ge1/1

The Switch (config - erps - 2) # 2 enable ring

The Switch (config - erps - 2) # exit

Configure sw2:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 5-7

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

Switch(config-ge1/1)# Switchport trunk VLAN Add 6

Switch(config-ge1/1)# Switchport trunk VLAN Add 7

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

Switch(config-ge1/3)# Switchport trunk VLAN Add 6

Switch(config-ge1/3)# Switchport trunk VLAN Add 7

The Switch (config - ge1/3) # exit

Configure ERPS instance 2, ERPS single ring 2

The Switch # 2 erps (config)

The Switch (config - erps - 2) # 2 ring

Switch(config-erps-2)# ring 2 Ring-mode major-ring

Switch(config-erps-2)# ring 2 Node-mode Ring-node

Switch(config-erps-2)# ring 2 RAPs-VLAN 5

Switch(config-erps-2)# ring 2 Traffics-VLAN 1

Switch(config-erps-2)# Ring 2 Traffics-VLAN 6

Switch(config-erps-2)# Ring 2 Traffics-VLAN 7

Switch(config-erps-2)# ring 2 RPL-port ge1/1

Switch(config-erps-2)# ring 2 RL-port ge1/3

The Switch (config - erps - 2) # 2 enable ring

The Switch (config - erps - 2) # exit

Configuration sw3:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 5-7

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

Switch(config-ge1/1)# Switchport trunk VLAN Add 6

Switch(config-ge1/1)# Switchport trunk VLAN Add 7

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

Switch(config-ge1/3)# Switchport trunk VLAN Add 6

Switch(config-ge1/3)# Switchport trunk VLAN Add 7

The Switch (config - ge1/3) # exit

Configure ERPS instance 2, ERPS single ring 2

The Switch # 2 erps (config)

The Switch (config - erps - 2) # 2 ring

Switch(config-erps-2)# ring 2 Ring-mode major-ring

Switch(config-erps-2)# ring 2 Node-mode Ring-node

Switch(config-erps-2)# ring 2 RAPs-VLAN 5

Switch(config-erps-2)# ring 2 Traffics-VLAN 1

Switch(config-erps-2)# Ring 2 Traffics-VLAN 6

Switch(config-erps-2)# Ring 2 Traffics-VLAN 7

Switch(config-erps-2)# ring 2 RPL-port ge1/1

Switch(config-erps-2)# ring 2 RL-port ge1/3

The Switch (config - erps - 2) # 2 enable ring

The Switch (config - erps - 2) # exit

Sw4 configuration:

The Switch > enable

Switch# configure terminal

Create ERPS protocol with data VLAN

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 5-7

The Switch (config - vlan) # exit

Configure ring port VLAN mode as trunk, add ERPS protocol and data VLAN

The Switch (config) # interface ge1/1

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

Switch(config-ge1/1)# Switchport trunk VLAN Add 5

Switch(config-ge1/1)# Switchport trunk VLAN Add 6

Switch(config-ge1/1)# Switchport trunk VLAN Add 7

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/3

The Switch (config - ge1/3) # switchport mode trunk

Switch(config-ge1/3)# Switchport trunk VLAN Add 5

Switch(config-ge1/3)# Switchport trunk VLAN Add 6

Switch(config-ge1/3)# Switchport trunk VLAN Add 7

The Switch (config - ge1/3) # exit

Configure ERPS instance 2, ERPS single ring 2

The Switch # 2 erps (config)

The Switch (config - erps - 2) # 2 ring

Switch(config-erps-2)# ring 2 Ring-mode major-ring

Switch(config-erps-2)# ring 2 Node-mode RPL-neighbor-Node

Switch(config-erps-2)# ring 2 RAPs-VLAN 5

Switch(config-erps-2)# ring 2 Traffics-VLAN 1

Switch(config-erps-2)# Ring 2 Traffics-VLAN 6

Switch(config-erps-2)# Ring 2 Traffics-VLAN 7

Switch(config-erps-2)# ring 2 RPL-port ge1/3

Switch(config-erps-2)# ring 2 RL-port ge1/1

The Switch (config - erps - 2) # 2 enable ring

The Switch (config - erps - 2) # exit

# Chapter 11
# Configuration of AAA

This chapter describes how to configure the 802.1x and RADIUS of the switch to prevent unauthorized access to the network. See the respective operating manuals for the 802.1X client and HyperBoss.This chapter mainly includes the following contents:

- 802.1 x introduces
- The RADIUS is introduced
- The configuration of 802.1 x
- Configure the RADIUS

AAA stands for Authentication, Authorization, and Accounting. It provides a consistent framework for configuring authentication, authorization, and billing for security functions. AAA configuration is actually a management of network security, which mainly refers to access control. Which users can access the network? What services are available to users with access rights? How do I account for users who are using network resources?

Authentication: Verifies that the user can gain access.

Authorization: which services can the authorized user use.

Accounting: To record the use of network resources by users.

The network companyLaunched a full suite of AAA solutions, products 802.1X client, a variety of supporting authentication switches and authentication billing system HyperBoss. 802.1X client is installed on the PC that the user accesses the Internet. When

the user needs to access the network, 802.1X client is required for authentication. Only authenticated users can use the network. It receives authentication requests from the client, sends username and password to the authentication billing system HyperBoss, and the switch itself does not do the actual authentication. HyperBoss receives the authentication request from the switch for actual authentication and charges the authenticated user.

The 802.1X protocol is used for communication between the 802.1X client and the switch, and the RADIUS protocol is used for communication between the switch and HyperBoss.

## 1.43 802.1 x introduces

The 802.1X protocol is a port-based access control and authentication protocol. Here, the port refers to the logical port, which can be physical port, MAC address or Vlan ID, etc. The network switch implements the 802.1X protocol based on MAC address.

802.1x is a two-layer protocol, the authenticated switch and the user's PC must be in the same subnet, and the protocol packet cannot span the network segment. 802.1X authentication is based on the client server model, where a server must authenticate all users. Before the user passes the authentication, only the authentication stream can pass through the port of the switch. After the authentication is successful, the data stream can only pass through the port of the switch, that is to say, the user can only access the network after the authentication has passed.

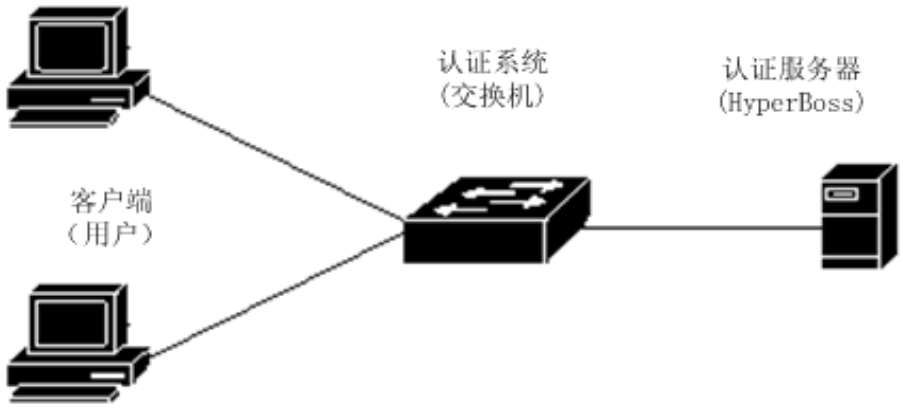
This section mainly includes the following contents:

- 802.1X equipment composition
- Protocol Package Introduction

- Protocol flow interaction
- 802.1X port status

## 1.43.1 802.1X equipment composition

An 802.1X device consists of three parts: Supplicant System, Authenticator System, and Authenticator SystemAuthentication Server System. As shown in the figure below.




802.1 x devices

The client refers to the device requesting access to the network, which is generally the user terminal system, such as the user's PC. An 802.1x client software must be installed on the user terminal system, which realizes the client part of the 802.1X protocol.The client initiates an 802.1X authentication request, which requests the authentication server to verify its user name and password. If the authentication is successful, the user can access the network.

An authentication system refers to an authenticated device, such as a switch. The authentication system controls whether the user can access the network through the state of the user's logical port (MAC address). If the user's logical port state is unauthorized, the

user cannot access the network. If the user's logical port state is authorized, the user can access the network.

The authentication system is a relay between the client and the authentication server. The authentication system requests the user's identity information, forwards the user's identity information to the authentication server, and forwards the authentication result sent by the authentication server to the client. Near the client authentication system in order to realize the service side part of 802.1 x agreement, near the authentication server to achieve the client part of the RADIUS protocol, the RADIUS protocol client authentication system sent 802.1 x client EAP information encapsulation were found in the RADIUS to the authentication server, and package from the authentication server RAIDUS agreement the decapsulation and EAP information through 802.1 x server part to 802.1 x clients.

The authentication server refers to the device that actually authenticates the user. The authentication server receives the user's identity information sent by the authentication system and authenticates. If the authentication is successful, the authentication server authorizes the authentication system and allows the user to access the network. If the authentication fails, the authentication server tells the authentication system that the user's authentication fails and the user cannot access the network. The authentication server and authentication system communicate via the EAP extended RADIUS protocol. The network provides an authentication billing system, HyperBoss, to authenticate and charge users.

## 1.43.2 Protocol Package Introduction

The authentication data stream transmitted Over the network by 802.1X protocol is in

EAPOL (EAP Over LAN) frame format, and all user identity information (including user name and password) is encapsulated in EAP (Extended Authentication Protocol), which is encapsulated in EAPOL frame. The user name exists in the EAP as clear text and the password as MD5 encryption.

The EAPOL frame format is shown below. PAE Ethernet Type is the Ethernet protocol Type number for EAPOL with a value of 0x888E. Protocol Version is the EAPOL Version number with a value of 1. Packet Type is the EAPOL frame Type. Packet Body Length is the Length of the EAPOL frames. Packet Body is the content of the EAPOL frames.

| | Octet Number |
|---|---|
| PAE Ethernet Type | 1-2 |
| Protocol Version | 3 |
| Packet Type | 4 |
| Packet Body Length | 5-6 |
| Packet Body | 7-N |

EAPOL frame format

The switch USES three EAPOL protocol frames, which are respectively:

The value of EAPol-Start: Packet Type is 1, and the frame is authenticated. When the user needs to authenticate, the frame is first launched and sent to the switch by the client.

Eapol-logoff: Packet Type is 2. Exit the request frame and send the frame notification switch when the user does not need to use the network.

Eap-packet: Packet Type is 0, authentication information frame, used to carry authentication information.

The EAP package format is shown below. Code refers to the type of EAP package,

including Request, Response, Success, and Failure. Identifier refers to an identifier that matches Response and Request. Length refers to the EAP packet Length, including the header. Data refers to EAP package Data.

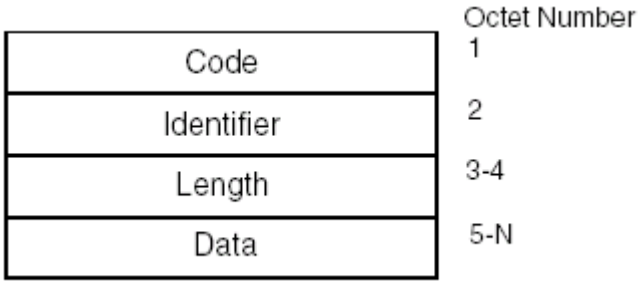
EAP packages include the following four types:

EAP-Request: Code value 1, EAP Request packet, from the switch to the client Request username and/or password.

Eap-response: Code value 2, EAP reply packet, sent from client to switch, sending username and/or password to switch.

Eap-success: Code value is 3. EAP Success packet is sent from the switch to the client to tell the client that the authentication is successful.

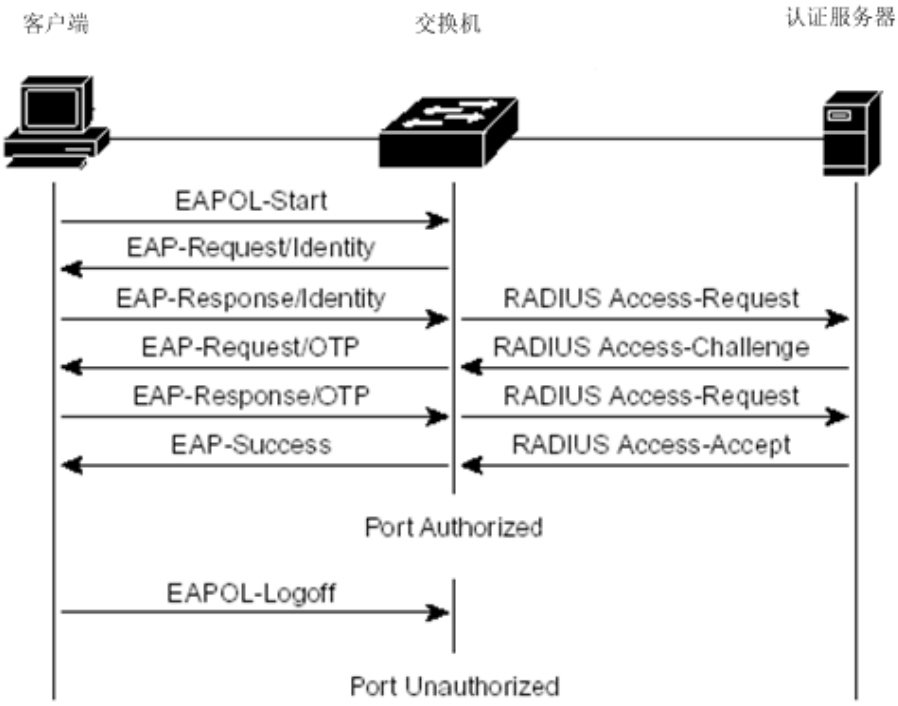
Eap-failure: Code value is 4. EAP Failure packet is sent from the switch to the client, telling the client user that authentication fails.




EAP package format

## 1.43.3 Protocol flow interaction

When the switch enables 802.1x and the state of the port is Auto, all access users under the port must be authenticated to access the network. The protocol interaction is shown below.

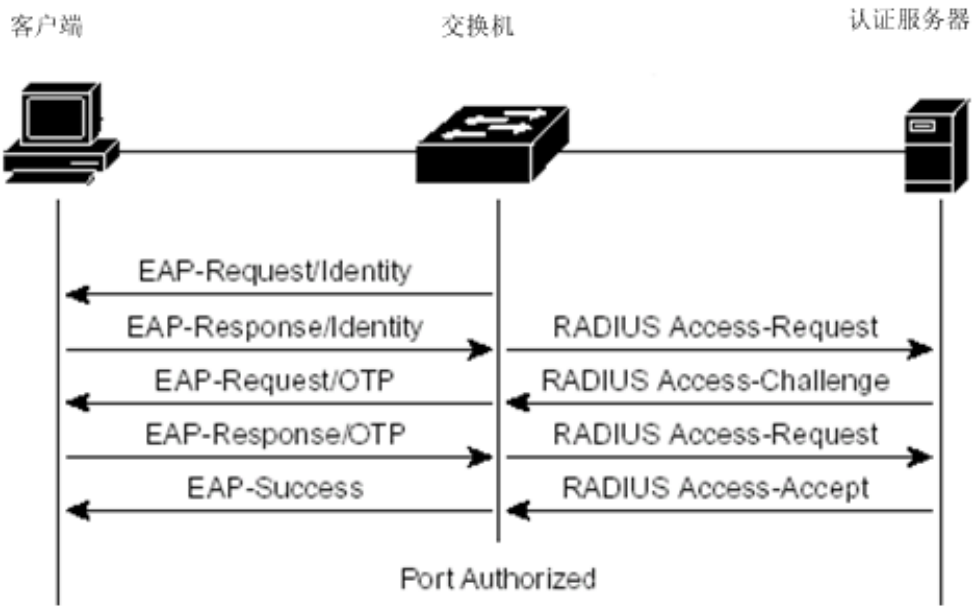



The client initiates the authenticated protocol interaction

When users need access to the network, the client Request certification first send EAPOL - Start to switch, switch sent after receipt of the authentication Request EAP - Request username of the user Request, the client send back EAP - Response, switches are extracted from the EAP information encapsulation in RADIUS packets sent to the authentication server, Request the user's password, the authentication server switches send EAP - the Request to the client Request the user's password, the client send back EAP - Response,The switch sends the EAP information encapsulated in a RADIUS packet to the authentication server, which authenticates the user based on the user name and password. If authentication is successful, the authentication server notifies the switch, which sends EAP-Success to the client and authorizes the user's logical port. When the client receives EAP-Success, the authentication is successful and the user can access the network.

When the user no longer needs to use the network, the client sends eapol-Logoff to the switch, which changes the logical port state of the user to the unauthorized state, at which time the user cannot access the network.

In order to prevent clients from abnormal offline, the switch provides a recertification mechanism. The interval of recertification can be set on the switch. When the recertification time arrives, the switch initiates recertification. The protocol interaction is shown below.




Recertification of protocol

## 1.43.4 802.1X port status

The port state referred to here is the physical port state of the switch. There are four states for the physical ports of the switch: N/A state, Auto state, Force-Authorized state,

and Force-UNAUTHORIZED state. When the switch is not on 802.1x, all ports are in N/A state. When the switch port is set to Auto status, Force-Authorized status, or force-UNAUTHORIZED status, the 802.1x of the switch must be enabled first.

When the port of the switch is in N/A state, all users under the port can access the network without authentication. When the switch receives 802.1X protocol packets from the port, the packets are discarded.

When the switch's port is in force-authorized status, all users under the port can access the network without authentication. When the switch receives an EAPol-Start packet from the port, the switch sends back an EAP-Success packet, and when the switch receives other 802.1x protocol packets from the port, these protocol packets are discarded.

When the switch's port is in a force-UNAUTHORIZED state, all users under the port will never have access to the network, and the authentication request will never pass. When the switch receives 802.1X protocol packets from the port, the packets are discarded.

When the switch's port is in Auto state, all users under the port must be authenticated to access the network. The 802.1X protocol interaction is shown in the figure. If the user needs to authenticate, the port is typically set to Auto.

When the switch port is set to Auto state, the anti-ARP spoofing function is enabled. The anti-ARP spoofing feature controls that only packets containing information provided by the client when both the source MAC and source IP of the IP packet are authenticated, and packets containing information provided by the client when both the SENDER IP of the ARP packet and the sender MAC are authenticated can be forwarded by this port, otherwise they will be discarded. To configure this function, the client must have a statically configured IP address. If the IP address is obtained dynamically through DHCP protocol, the DHCP SNOOPING protocol can be enabled to achieve this function. Refer to

the IP MAC binding configuration for more details.

## 1.44 The RADIUS is introduced

When a user authenticates, the switch and the authentication server interact using the RADIUS protocol that supports EAP extensions. RADIUS protocol adopts the client/server model, the switch needs to implement the RADIUS client, and the authentication server needs to implement the RADIUS server.

In order to ensure the security of the interaction between switch and authentication server and prevent the interaction between illegal switch or illegal authentication server, the switch and authentication server should authenticate each other. Switches and authentication server requires the same key, when the switch or authentication server send the RADIUS protocol packets, all protocols package according to the key USES HMAC algorithm to generate the message digest, when the RADIUS protocol packet switches and authentication server received, all of the agreements were tested, the news of the package in order to use the key if verification through, considered legitimate RADIUS protocol packets, otherwise it is illegal to RADIUS protocol packets, discarded.

This section mainly includes the following contents:

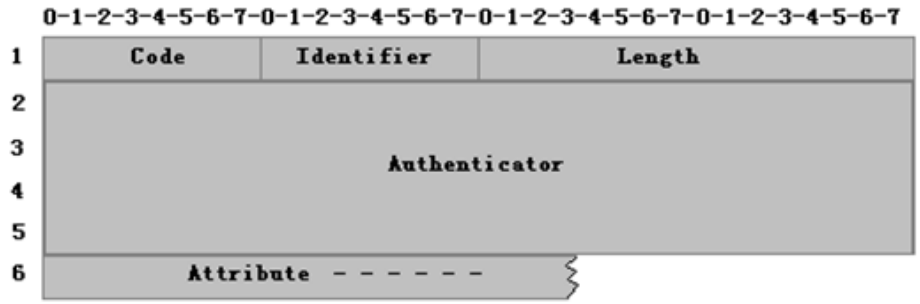
- Protocol Package Introduction
- Protocol flow interaction
- User verification method

## 1.44.1 Protocol Package Introduction

RADIUS is a protocol based on UDP. RADIUS can encapsulate authentication information and billing information. The early RADIUS authentication port was 1645, currently using port 1812, the early RADIUS charging port was 1646 and currently using port 1813.

Because RADIUS is hosted on UDP, there is a timeout replay mechanism for RADIUS. At the same time, in order to improve the reliability of the communication between the authentication system and the RADIUS server, two RADIUS server schemes are generally adopted, namely the standby server mechanism.

The FORMAT of RADIUS message is shown in the figure below. Code refers to the RADIUS protocol message type. The Identifier Identifier is used to match a request and a reply. Length refers to the Length of the entire message, including the header. The Authenticator is a 16-byte string, a random number for the request packet, and an MD5-generated message digest for the reply packet. Attribute refers to an Attribute in the RADIUS protocol package.




RADIUS message format

The network USES the following RADIUS protocol packages:

Access-request: Code value 1, authentication Request package from authentication system to authentication server, user name and password are enclosed in this package.

Access-accept: Code value is 2. The reply packet sent from the authentication server to the authentication system indicates that the user authentication is successful.

Access-reject: A Code value of 3 is sent to the authentication system from the authentication server as a reply packet indicating that the user has failed to authenticate.

Access-challenge: Code value 11, a response packet sent from the authentication server to the authentication system, indicating that the authentication server needs further information of the user, such as password, etc.

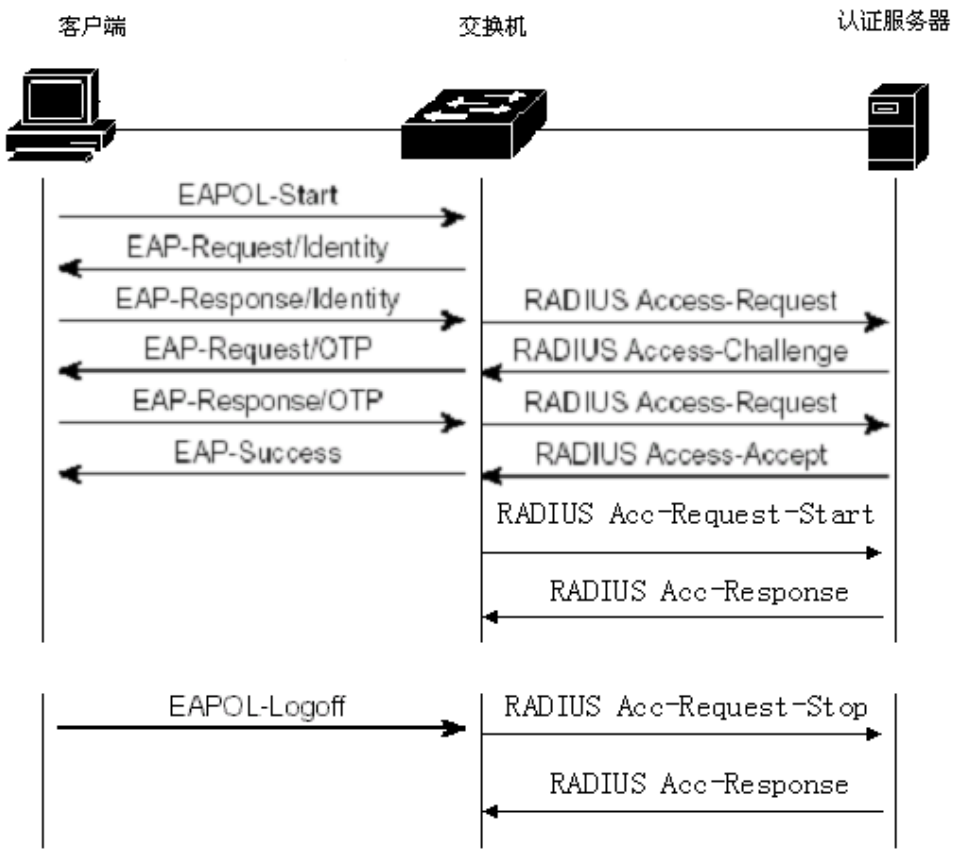
Accounting-request: Code value is 4. The billing Request package sent to the authentication server from the authentication system includes starting and ending billing packages, and the billing information is enclosed in this package.

Accounting-response: Code value is 5. The billing Response packet sent to the authentication system from the authentication server indicates that the billing information has been received.

## 1.44.2 Protocol flow interaction

When the user initiates authentication, the authentication system and the authentication server interact through the RADIUS protocol. The protocol flow interaction of the authentication system without RADIUS billing packet is shown below. In general, after the user authentication succeeds or when the user goes offline, the authentication system needs to send RADIUS billing package to the authentication server. The protocol

flow interaction is shown in the figure below.




User authentication, switches, encapsulate the user name in the Access - Request message sent to the authentication server, the server response Access - Challenge Request the user's password, switches, Request the client user's password, the client password encapsulated in EAP, switches, Access to the EAP after encapsulation in Access - the Request to the authentication server, authentication server for user authentication, if authentication is successful, the echo Access - Accept to switch, switch after receipt of this message to inform the client authentication is successful,At the same time, send Accounting-Request to notify the authentication server to start billing, and the authentication server sends Accounting-Response back.

When the user does not want to use the network, the switch will be notified to go offline, and the switch will send the Accountation-Request to the authentication server to

terminate the billing. The billing information will be encapsulated in this package, and the authentication server will send back the Accountation-Response.

### 1.44.3 User verification method

There are three methods of user authentication within RADIUS, as follows:

- Password Authentication Protocol. The user passes the username and password to the switch in clear text. The switch passes the username and password to the RADIUS server through the RADIUS protocol package, and the RADIUS server looks for the database. If the same username and password exist, the authentication passes; otherwise, the authentication fails.
- Authentication Protocol (CHAP). When a user requests an Internet connection, the switch generates a 16-byte random code to the user. The user generates a Response to random codes, passwords, and other domain encryption, and sends the user name and Response to the switch. The switch passes the username, Response, and the original 16-byte random code to the RADIUS server. RADIU looks up the database at the switch side according to the user name, gets the same password as that used by the client to encrypt, then encryfies according to the transmitted 16-byte random code, and compares its results with the transmitted response. If the same, the authentication passes; if not, the authentication fails.
- EAP (Extensible Authentication Protocol). With this method of authentication, the switch does not really participate in the authentication, only acting as a forward between the user and the RADIUS server. When a user request to get to the Internet, switches, request the user's user name, the RADIUS server and the

user name, the RADIUS server to produce a 16 bytes of random code to the user and store the random code, users of random code, password encryption and other various domain to generate a response, the user name and the response to the switch, switch is forwarded to the RADIUS server. RADIU looks up the database at the switch side according to the user name, gets the same password as that used by the client to encrypt, then encrypts according to the stored 16-byte random code, and compares its results with the transmitted response. If the same, the verification passes; if not, the verification fails.

The authentication billing solution of the network adopts the EAP user authentication method.

## 1.45 The configuration of 802.1 x

This section describes the configuration of 802.1x in detail, mainly including the following:

- 802.1x default configuration
- Start and close 802.1x
- Configure 802.1x port status
- Configure the recertification mechanism
- Configure the maximum number of port access hosts
- Configure interval times and number of retransmissions
- Configure ports as transport ports

- Configure the 802.1x client version number
- Whether the configuration checks the client version number
- Configuration authentication method
- Configure whether to check client timing packages
- Displays 802.1x information

## 1.45.1 802.1x default configuration

The default configuration of switch 802.1x is as follows:

- 802.1x is off.
- The state of all ports is N/A.
- The recertification mechanism is off and the recertification interval is 3600 seconds.
- The maximum number of access hosts for all ports is 100.
- The timeout interval for re-issuing an EAP-Request is 30 seconds.
- The number of times a timeout is repeated for an EAP-Request is 3.
- The wait time for user authentication failure is 60 seconds.
- The server timeout repeats at an interval of 10 seconds.

The switch provides a command in global CONFIG mode to return all configurations to their default state. The command is as follows:

The Switch (config) # dot1x default

## 1.45.2 Start and close 802.1x

The first step in configuring 802.1X is to start 802.1x. In global CONFIG mode, enter the following command to start 802.1x:

The Switch # dot1x (config)

When 802.1x is closed, all port states return to N/A. In global CONFIG mode, enter the following command to close 802.1x:

The Switch # no dot1x (config)

## 1.45.3 Configure 802.1x port status

Be sure to boot 802.1x before setting the 802.1X port state. If all users under the port must be authenticated to access the network, the port must be set to Auto.

The following command sets port Ge1/1 to Auto in interface configuration mode and enables anti-ARP spoofing:

The Switch (config - ge1/1) dot1x control auto

If the anti-ARP spoofing configuration fails, it can be caused by:

1. System CFP resource is exhausted.

2. The current interface is configured with ACL filtering.

3. The DHCP SNOOPING function is enabled in the current interface.

The configured interface is a three-tier interface or a trunk interface.

The following command sets the port ge1/1 to force-authorized status in interface configuration mode:

The Switch (config - ge1/1) dot1x control force - authorized

The following command sets the port Ge1/1 to force-UNAUTHORIZED status in interface configuration mode:

The Switch (config - ge1/1) dot1x control force - unauthorized

The following command sets port ge1/1 to N/A in interface configuration mode:

The Switch (config - ge1/1) no dot1x control

Note: If a port is already tied to a MAC address, the port can't be set to Auto, Force-Authorized, or Force-UNAUTHORIZED status.

## 1.45.4 Configure the recertification mechanism

In order to prevent the switch and the authentication server from being detected after the client goes offline abnormally, the switch provides a recertification mechanism, and every recertification interval the switch initiates an authentication.

The following command starts the recertification mechanism in global CONFIG mode:

The Switch (config) # dot1x reauthenticate

The following command turns off recertification in global CONFIG mode:

The Switch (config) # no dot1x reauthenticate

The following command sets the interval for recertification in global CONFIG mode:

The Switch (config) # dot1x timeout re - authperiod < interval >

Note: The interval of recertification time should not be set too short, otherwise the network bandwidth and THE CPU resource consumption of the switch will be too large.

## 1.45.5 Configure the maximum number of port access hosts

Each port of the switch can control the maximum number of hosts accessed, which can limit users to illegally access to the network using multiple hosts. The maximum number of port access hosts is 100 by default, and the maximum can be set to 100. If the maximum number of port access hosts is set to 0, the port denies access to any user.

The following command sets the maximum number of port ge1/1 access hosts in interface configuration mode:

The Switch (config - ge1/1) dot1x support - host < number >

## 1.45.6 Configure interval times and number of retransmissions

The 802.1x protocol standard specifies some interval times and retransmissions of protocol interaction and protocol state machines. The switch USES the standard interval times and retransmissions. It is recommended that users do not change these interval times and retransmissions when using the switch.

Tx-period refers to the time interval between the switch sending the EAP-Request protocol packet again. Max-req represents the number of times the switch resends EAP-Request; Quiet -period refers to the interval of waiting for recertification when user authentication fails. Server-timeout represents the interval between the switch sending RADIUS packets back to the authentication server. Supp-timeout represents the interval between the switch sending the EAP request packet back to the client.

The following command configures these interval times and retransmissions in global CONFIG mode:

The Switch (config) # dot1x timeout tx - period < interval >

The Switch (config) # dot1x Max - the req < number >

The Switch (config) # dot1x timeout quiet - period < interval >

The Switch (config) # dot1x timeout server - the timeout < interval >

The Switch (config) # dot1x timeout supp - timeout < interval >

## 1.45.7 Configure ports as transport ports

When the switch does not open 802.1X authentication, and other switches in the subnetwork open 802.1X authentication, the connection client of the switch and the port of the authentication switch can be configured as the transmission port, and the EAPOL authentication package can be forwarded between the client and the 802.1X authentication switch. Thus, other switches can realize 802.1X authentication for clients.

The following command sets port Ge1/1 as the transport port in interface configuration mode:

The Switch (config - ge1/1) dot1x transmit - port

The following command sets port Ge1/1 as a non-transport port in interface configuration mode:

The Switch (config - ge1/1) no dot1x transmit - port

## 1.45.8 Configure the 802.1x client version number

Configure the 802.1X client version number. Only clients whose version is not lower than the configured version number can be authenticated, otherwise the authentication fails. The default client version number of the switch is 2.0.

The following command configures the client version number in global CONFIG mode:

The Switch (config) # dot1x client - version < string >

## 1.45.9 Whether the configuration checks the client version number

Configure to check the 802.1x client version number. If configured to check, the switch first checks the client version number when doing authentication. The default is configured to check.

The following command is configured in global CONFIG mode to turn on checking for client version Numbers:

The Switch (config) # dot1x check - version open

## 1.45.10 Configuration authentication method

Configure the switch for 802.1X packet authentication. Client-initiated authentication can be divided into general authentication and extended authentication. The switch can be configured to first authenticate against which method. If the authentication method initiated by the client is inconsistent with the authentication method of the switch configuration, the client will convert to another authentication method to initiate authentication after a certain number of authentication failures.

In the global CONFIG mode, the following command can configure the authentication mode of the switch as extended authentication:

The Switch (config) # dot1x extended

## 1.45.11 Configure whether to check client timing packages

Configure whether the switch checks the client's timing packet. After the authentication is successful, the switch will require the client to send 802.1x packet regularly, but not all clients will send 802.1X packet regularly after the authentication is passed. In this way, configure whether the switch checks the client's timing packet by command.

The following command is configured in global CONFIG mode to check client timing

packages for switches:

The Switch (config) # dot1x check - the client

## 1.45.12 Displays 802.1x information

The following command displays 802.1x information in normal mode/privilege mode. When the command is show dot1x, it displays all 802.1X configuration information, including all port configuration information. When the command is Show dot1x Interface, the information of all access users under the port is displayed:

Switch# show dot1x

Switch# show dot1x interface

# 1.46 Configure the RADIUS

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

- RADIUS default configuration
- Configure the IP address of the authentication server
- Configure Shared keys
- Start and close billing
- Configure RADIUS port and property information

- Configure RADIUS roaming function
- Display RADIUS information

## 1.46.1 RADIUS default configuration

The default RADIUS configuration of the switch is as follows:

- The IP address of the primary and backup authentication servers is not configured, i.e., the IP address is 0.0.0.0.
- The Shared key is not configured, that is, the Shared key string is empty.
- Billing is enabled by default.
- RADIUS authenticates the UDP port as 1812 and billing UDP port as 1813.
- The value of the RADIUS attribute NASPort is 0xc353, the value of NASPortType is 0x0f, and the value of NASPortServer is 0x02.

## 1.46.2 Configure the IP address of the authentication server

To enable RADIUS communication between the switch and the authentication server, the IP address of the authentication server needs to be configured on the switch. In practical applications, you can use one or two authentication servers, one as the primary authentication server and one as the backup authentication server. If the switch is configured with the IP addresses of two authentication servers, it can switch to

communicating with the backup authentication server when the switch disconnects from the primary authentication server.

The following commands configure the IP address of the master authentication server in global CONFIG mode:

Switch (config) # radius server host < IP - address >

The following commands configure the IP address of the backup authentication server in global CONFIG mode:

Switch (config) # radius server option - host < IP - address >

## 1.46.3 Configure Shared keys

To authenticate each other, the switch and the authentication server both need to set up the same Shared key. Note that the Shared key on the switch must be the same as that of the authenticated server.

The following command configures the switch's Shared key in global CONFIG mode:

The Switch (config) # radius - server key < string >

## 1.46.4 Start and close billing

If the switch turns off billing, the switch will not send RADIUS billing packets to the authenticated server after successful authentication or when the user is offline. Usually in practice, billing is turned on.

The following command starts billing in global CONFIG mode:

The Switch (config) # radius - server accounting

The following command turns off billing in global CONFIG mode:

The Switch (config) # no radius - server accounting

## 1.46.5 Configure RADIUS port and property information

It is recommended that users do not modify RADIUS port and property information configurations.

The following command modifies the RADIUS authenticated UDP port in global CONFIG mode:

Switch (config) # radius server udp - port < port - number >

The following command modifies the RADIUS property information in global CONFIG mode:

The Switch (config) # radius server attribute nas - portnum < number >

The Switch (config) # radius server attribute nas - porttype < number >

The Switch (config) # radius - server attribute service -type < number >

## 1.46.6 Configure RADIUS roaming function

When a client is bound to a MAC, IP, or VLAN, the bound client cannot authenticate 802.1x because the MAC address, IP address, or VLAN is changed when the client is moved elsewhere.Turning on radius roaming will continue 802.1X authentication by ignoring the client's MAC, IP, or VLAN bindings.

The following commands configure RADIUS roaming in global CONFIG mode:

The Switch (config) # radius - server levenshtein distance

The following command turns off RADIUS roaming in global CONFIG mode:

The Switch (config) # no radius - server levenshtein distance

## 1.46.7 Display RADIUS information

The following command displays the RADIUS configuration information in normal/privileged mode:

Switch# show the radius server

## 1.47 Configuration of the sample

Open the 802.1X protocol, configure port Ge1/1 to Auto state, configure the master authentication server to 198.168.80.111, and configure the Shared key of the switch to ABCDEF.

Switch#

Switch# dot1x

Switch# config t

The Switch (config) # radius - server host 198.168.80.111

The Switch (config) # radius - server key abcdef

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # dot1x control auto

# Chapter 12 GMRP configuration

This chapter mainly includes the following contents:

- GMRP introduction
- Configuration GMRP
- Display GMRP

## 1.48 GMRP introduction

Currently, GMRP (GARP Multicast Registration Protocol) is a Multicast Registration Protocol based on GARP for maintaining Multicast Registration information in switches.All switches that support GMRP can receive multicast registration information from other switches, dynamically update local multicast registration information, and also propagate local multicast registration information to other switches.This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP supporting devices in the same switched network.

When a host wants to join a multicast group, it issues a GMRP join message.The switch adds the port receiving the GMRP message to the multicast group and broadcasts the GMRP message in the VLAN where the receiving port is located. The multicast source in the VLAN can know the existence of a multicast member.When a multicast source sends a multicast text to a multicast group, the switch only forwards the multicast text to the port that the multicast member is connected to, thus realizing the two-layer multicast in the VLAN.

## 1.49 Configuration GMRP

The main configuration of GMRP includes:

Open the GMRP

Check the GMRP

In the configuration task, the global GMRP must be turned on before port GMRP can be turned on.

## 1.49.1 Turn on the GMRP Settings

| The command | describe | Configuration mode |
|---|---|---|
| Set GMRP enable \| disable | Enable/enable all VLAN GMRP globally | Global configuration mode |
| Set GMRP enable vlan <vlan-id> | Enable global specific VLAN GMRP | Global configuration mode |
| Set GMRP registration{fixed \| forbidden \| normal} <if-name> | Configure the interface to register the multicast mode | Global configuration mode |
| Set GMRP timer {join \| leave \| nleaveall} <time-value> | Time to configure various timers | Global configuration mode |
| Set port GMRP enable <if-name> | Enable port GMRP functionality | Global configuration mode |
| Set port GMRP disable <if-name> | To enable port GMRP functionality | Global configuration mode |

## 1.49.2 View the GMRP information

After the above configuration, execute the show command in privileged mode to display the GMRP running after the configuration, and verify the configuration by viewing the display information.

| The command | describe | Configuration mode |
|---|---|---|
| Show GMRP configuration | View the GMRP configuration | Privileged mode |

| | | |
|---|---|---|
| | information | |
| Show GMRP machine | View the GMRP state machine information | Privileged mode |
| Show GMRP statistics vlanid | View the GMRP statistics for the specific VlanID | Privileged mode |
| Show GMRP timer < ifname > | View the timer information for the specific port | Privileged mode |

## 1.50 Examples of typical GMRP configurations

1. Network requirements

In order to realize dynamic registration and update of multicast information between switches, GMRP needs to be started on switches

2. Network diagram


GMRP sample networking diagram

3. The configuration steps

Configure SW1

Start the global GMRP

The Switch (config) # set GMRP enable

Start port GMRP on gigabit Ethernet port ge1/1

Switch(config)# set port GMRP enable ge1/1

The Switch # (config)

Configure SW2

Start the global GMRP

The Switch (config) # set GMRP enable

Start port GMRP on gigabit Ethernet port ge1/2

Switch(config)# set port GMRP enable ge1/2

The Switch # (config)

# Chapter 13 IGMP SNOOPING configuration

In metropolitan area network/Internet, using unicast way will be the same multiple, but not all the recipients of the packets sent to the network, because of the need to copy the grouping to each receiving endpoint, increase in the number of the receiver, number of packages need to send and linear will also increase, which makes the host, to exchange routing equipment and network bandwidth resources overall burden, efficiency greatly affected. With the increasing demand of multi-point video conferencing, video-on-demand and group communication applications, multicast has become a popular transmission method in multi-point communication to improve resource utilization.

The switch implements IGMP SNOOPING function as a multicast application service. IGMP SNOOPING is performed to monitor IGMP packets in the network to realize dynamic learning of IP multicast MAC addresses.

This chapter describes the concept and configuration of IGMP SNOOPING, including the following:

- IGMP SNOOPING is introduced
- IGMP SNOOPING configuration
- Sample IGMP SNOOPING configuration

## 1.51 IGMP SNOOPING is introduced

Traditional network in a subnet multicast packet as broadcast processing, which is easy to make the network traffic, causing network congestion. When IGMP SNOOPING is implemented on the switch, IGMP SNOOPING can be performed to dynamically learn IP multicast MAC address, maintain the list of IP multicast MAC address output ports, and make the multicast data stream only sent to the output port, so as to reduce the network traffic.

This section mainly includes the following contents:

- IGMP SNOOPING Process
- Layer 2 dynamic multicast
- Join a group
- Leave a group

### 1.51.1 IGMP SNOOPING Process

IGMP SNOOPING is a layer 2 network protocol that listens for IGMP packets passing through the switch, maintains a multicast group based on the receiving port, VLAN ID, and multicast address of the IGMP packets, and forwards the IGMP packets. Only ports with multicast group can receive multicast data stream. This reduces network traffic and saves network bandwidth.

Multicast group includes multicast group address, member port, VLAN ID, Age time.

The formation of an IGMP SNOOPING group is a learning process. When an IGMP REPORT package is received on a port of the switch, a new multicast group is generated for IGMP SNOOPING. The port receiving the IGMP REPORT package is added to the multicast group. When the switch receives an IGMP QUERY package, if the multicast group is already in the switch, the port that receives the IGMP QUERY is added to the multicast group; otherwise, the IGMP QUERY package is forwarded. IGMP SNOOPING also supports the Leave mechanism of IGMP V2; If IGMP SNOOPING is configured with fast-leave to ENABLE, the receiving port of IGMP V2 can leave the multicast group immediately upon receiving the IGMP V2 leave packet; If a fast-leave-timeout is configured, the multicast group will leave the multicast group after the expiration of the timeout.

There are two update mechanisms for IGMP SNOOPING. One is the leave mechanism introduced above. In most cases, IGMP SNOOPING is performed to remove an expired multicast group by age Time. When a multicast group joins IGMP SNOOPING, the time of joining is recorded. When the multicast group remains in the switch for longer than a configured Age time, the exchange removes the multicast group.

When a port receives the Leave protocol packet, it will immediately be deleted from the multicast group to which it belongs. This situation may affect the continuity of network data flow. This port may be connected to a HUB or network device that does not have an IGMP SNOOPING feature connected to a number of receiving multicast data streams. One device sending Leave may affect other devices also receiving multicast data streams. Fast-leave-timeout mechanism can prevent this from happening. Fast-leave-timeout is used to configure a time to leave the wait. After receiving the leave packet, the port waits for a long time of Fast-leave-timeout and then removes it from the multicast group to which it belongs.

## 1.51.2 Layer 2 dynamic multicast

The MAC address entries for multicast delivery can be dynamically learned by IGMP SNOOPING. The IP multicast MAC address is learned dynamically by IGMP SNOOPING.

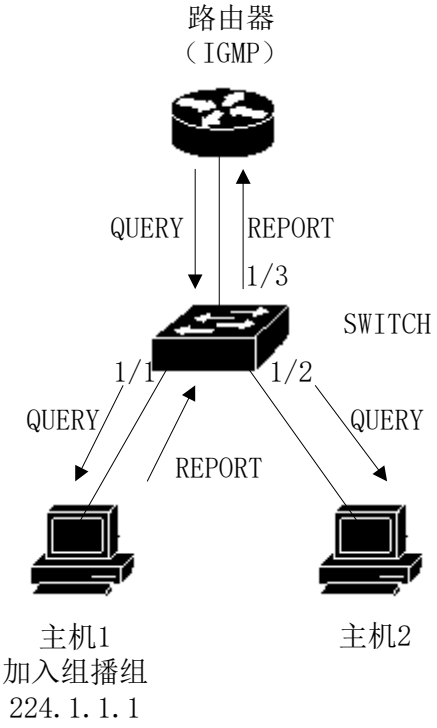
When the switch shuts down IGMP SNOOPING, the two-layer hardware multicast republication is in the unregistered forwarding mode, and the MAC address of the multicast cannot be dynamically learned. There is no entry in the two-layer hardware multicast republication, and all the two-layer multicast data streams are treated as broadcast.

When network with multicast environment, in order to effectively control the flow of multicast network, switch to open the IGMP SNOOPING, hardware multicast to turn on the second floor at this time, published in the register forwarding mode, switches can learn by listening to the IGMP protocol packets on the network to the multicast MAC address, and the second turn hardware multicast published the entry in the matching layer multicast stream to forward.

## 1.51.3 Join a group

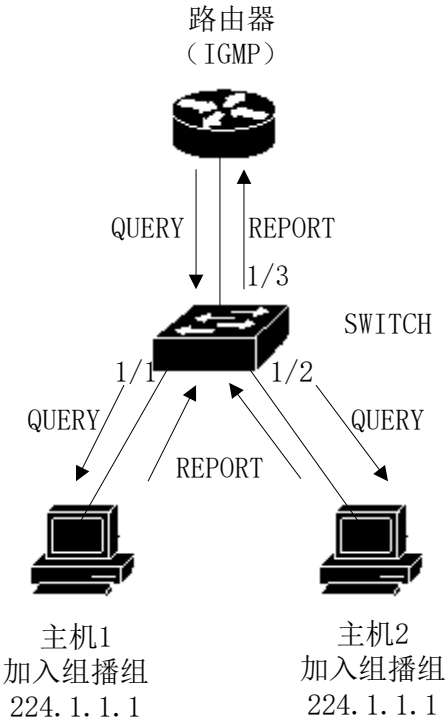
When a host wants to join a multicast group, the host sends an IGMP REPORT package that specifies the multicast group the host wants to join. When the switch receives an IGMP QUERY package, the switch forwards the package to all other ports in the same VLAN, and when the host under the port that wants to join the multicast group receives the IGMP QUERY package, an IGMP REPORT package is sent back. When the switch receives an IGMP REPORT package, a two-layer multicast entry is established.

The port receiving the IGMP QUERY package and the port receiving the IGMP REPORT package are added to the two-layer multicast entry and become its output port.




As shown above, all devices are in a subnet, assuming that the VLAN of the subnet is 2. The router runs the IGMPv2 protocol and sends the IGMP QUERY packet regularly. Host 1 wants to join multicast group 224.1.1.1. When the switch receives an IGMP QUERY packet from port 1/3, it logs the port and forwards the packet to ports 1/1 and 1/2. Host 1 sends back an IGMP REPORT package after receiving the IGMP QUERY package, while Host 2 does not send an IGMP REPORT package because it does not want to join the multicast group. When the switch receives the IGMP REPORT package from port 1/1, it forwards the package from query port 1/3 and creates a two-layer multicast entry (assuming it does not exist), which includes the following:

| Layer 2 multicast address | VLAN ID | List of output ports |
|---|---|---|
| 01:00:5 e: 01:01:01 | 2 | 1/1, 1/3 |




As shown in figure 1, host 1 has joined the multicast group 224.1.1.1, and now host 2 wants to join the multicast group 224.1.1.1. When host 2 receives the IGMP QUERY package, it sends back an IGMP REPORT package. After the switch receives the IGMP REPORT from port 1/2, it forwards the package from port 1/3 of the QUERY and adds it to the two-layer multicast entry by including port 1/2. The two-layer multicast entry becomes:

| Layer 2 multicast address | VLAN ID | List of output ports |
|---|---|---|

| | | |
|---|---|---|
| 01:00:5 e: 01:01:01 | 2 | 1/1, 1/2, 1/3 |

## 1.51.4 Leave a group

To form a stable multicast environment, devices running IGMP (such as routers) send an IGMP QUERY packet to all hosts at regular intervals. Hosts that have joined a multicast group or want to join a multicast group will send back an IGMP REPORT after receiving the IGMP QUERY.

If a host wants to leave a multicast group, it can do so in two ways: actively and passively. Active departure means that the host sends an IGMP LEAVE packet to the router, while passive departure means that the host does not send back the IGMP REPORT after receiving the IGMP QUERY sent by the router.

Corresponding to the way a host leaves a multicast group, there are also two ways to LEAVE a two-layer multicast entry on a switch port: timeout and IGMP LEAVE.

When the switch does not receive an IGMP REPORT package of a multicast group from a port over a certain period of time, the port is cleared from the corresponding two-level multicast entry. If the two-level multicast entry does not have a port, the two-level multicast entry is deleted.

When the switch's fast-leave is configured to ENABLE, if a port receives an IGMP Leave packet from a multicast group, the port is cleared from the corresponding two-layer multicast entry; if the two-layer multicast entry has no port, the two-layer multicast entry is deleted.

Fast-leave is generally used in a port connected to a host; If there are more than one host below a port, fast-leave-timeout wait time can be configured to ensure the continuity

and reliability of multicast streams in the network.

## 1.51.5 IGMP finder

In a network with three-tier multicast devices, the three-tier multicast device ACTS as an IGMP query.The two-layer multicast device only needs to listen IGMP message to establish and maintain the forwarding item and realize the two-layer multicast.In a network without a three-tier multicast device, the three-tier multicast device cannot act as an IGMP query.In order to enable the layer 2 multicast device to listen IGMP messages, the IGMP query function must be configured on the layer 2 device.The two-layer multicast device ACTS as an IGMP query and listens to IGMP messages in order to establish and maintain the forwarding item and realize the two-layer multicast.

The working principle of

IGMP query function: the two-layer device plays the role of IGMP routing query, regularly sends IGMP query message, listens and maintains the IGMP Report message replied by the user, and establishes the forwarding item of the two-layer multicast. The relevant parameters of the query message sent by IGMP query can be adjusted by the user through configuration.

Start the query

The user can be configured to enable the query functionality on the specified VLAN.

Specifies the IGMP version of the query to run

Specifies the version of IGMP used by the query message sent by the query-either

V1 or V2 or V3.

Configure the source IP of the query

Configure the source IP address carried by the query message sent by the query finder,

Configure the query interval for the query explorer

Configure the time interval between query messages sent by the global queriser

## 1.51.6 Igmp Snooping Group Playback filtering

The device running IGMP Snooping can control the range and load of the multicast services and effectively prevent illegal multicast streams.By configuring multicast filtering rules globally and applying rules on interfaces, you can allow or limit the addition of specific groups.

# 1.52 IGMP SNOOPING configuration

## 1.52.1 IGMP SNOOPING Default configuration

IGMP SNOOPING is closed by default, and layer 2 hardware multicast republication is in unregistered forward mode.

Fast-leave is turned off by default.

Fast-leave-timeout time is 300 seconds.

The age time of the multicast group REPORT port defaults to 400 seconds.

The age time of the multicast QUERY port defaults to 300 seconds.

## 1.52.2 Open and close IGMP SNOOPING

The IGMP SNOOPING protocol can be opened globally or separately. IGMP SNOOPING can only be opened or closed globally for a VLAN.

Open global IGMP SNOOPING

Switch# configure terminal

The Switch (config) # IP igmp snooping

Open a VLAN IGMP SNOOPING

Switch# configure terminal

Switch(config)# IP igmp snooping vlan <vlan-id>

Close global IGMP SNOOPING

Switch# configure terminal

The Switch (config) # no IP igmp snooping

Close IGMP SNOOPING for a VLAN

Switch# configure terminal

Switch(config)#no IP igmp snooping vlan <vlan-id>

## 1.52.3 Configured survival time

Configure the lifetime of a multicast group

Switch# configure terminal

Switch(config)# IP igmp snooping: group-membership timeout <interval> vlan <vlan-id>

The Interval is in milliseconds.

Configure the lifetime of the query group

Switch# configure terminal

Switch(config)# IP igmp snooping: query-membership timeout <interval> vlan <vlan-id>

The Interval is in milliseconds.

## 1.52.4 The configuration of fast - leave

Start a VLAN fast-leave

Switch# configure terminal

Switch(config)# IP igmp snooping: fast-leave vlan <vlan-id>

Closed fast - leave

Switch# configure terminal

Switch(config)#no IP igmp snooping: fast-leave vlan <vlan-id>

Configure the fast-leave wait time

Switch# configure terminal

Fast -leave-timeout <interval> vlan <vlan-id>

Restore the default fast-leave wait time

Switch# configure terminal

Switch(config)#no IP igmp snooping: fast-leave-timeout vlan <vlan-id>

## 1.52.5 Configuration MROUTER

Configure static query ports

Switch# configure terminal

Switch# interface ge1/6

Switch(Config-ge1/6)# IP IgMP Snooping MROUTER VLAN [VLAN-ID]

## 1.52.6 Configure the IgMP Snooping Query port function

Configure static query ports

Switch# configure terminal

The Switch (config) # interface ge1/6

Switch(Config-ge1/6)# IP IgMP Snooping MROUTER VLAN [VLAN-ID]

## 1.52.7 Configure the IgMP Snooping Query function

Start the IgMP Snooping query function for VLAN1

Switch# configure terminal

The Switch (config) # IP igmp sno

Switch(config)# IP IgMP Snooping Querier VLAN 1

## 1.52.8 Configure igMP Snooping Group playback filtering

Configure port ge1/1 to filter multicast at 235.0.0.1

Switch# configure terminal

Switch(config)# IP IgMP Snooping Filter - Rule 1 Deny 235.0.0.1

The Switch (config) # interface ge1/1

Switch(Config -ge1/1)# IP IgMP Snooping Filter - Group 1

## 1.52.9 According to the information

Displays IGMP SNOOPING configuration information

Switch# show IP igmp snooping

Displays configuration information for a VLAN

Switch#show IP igmp snooping vlan <vlan-id>

Displays aging information for the REPORT multicast group

Switch# Show IP IgMP Snooping Age - Table Group-membership

Displays the aging information for your QUERY

Switch# Show IP IgMP Snooping Require Age-Table query-membership

Displays the forwarding information of a multicast group

Switch#show IP igmp snooping forwarding-table

Display MROUTER information

Switch# Show IP IgMP Snooping MROuter

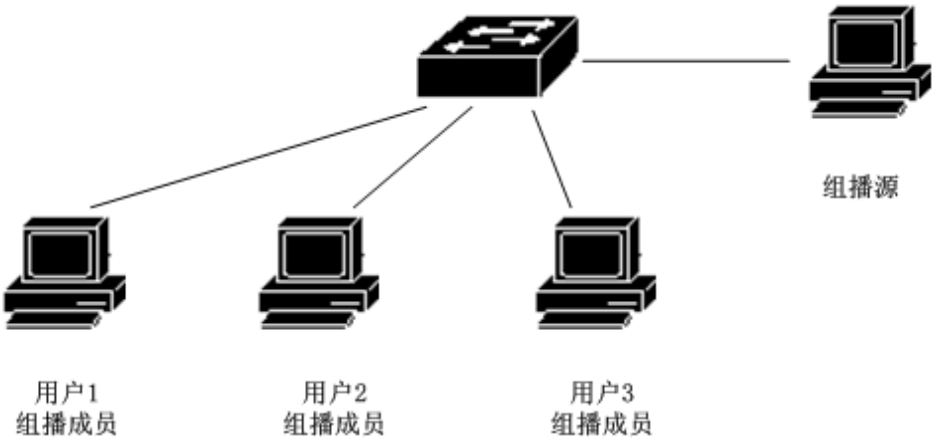
Displays the current configuration of the system, including the configuration of IGMP SNOOPING

Switch# show running - config

## 1.53 Sample IGMP SNOOPING configuration

### 1.53.1 configuration

Enable IGMP SNOOPING on the switch where user 1, user 2, and User 3 can join a specific multicast group.




Switch# config t

The Switch (config) # IP igmp snooping

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 200

The Switch (config - vlan) # exit

The Switch (config) # interface ge1/1

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

The Switch (config - ge1/1) # switchport access vlan 200

The Switch (config) # interface ge1/2

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

The Switch (config - ge1/2) # switchport access vlan 200

The Switch (config) # interface ge1/3

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

The Switch (config - ge1/3) # switchport access vlan 200

Switch(config)# IP IgMP Snooping VLAN 200

Switch(config)# IP IgMP Snooping Requires Group-members-Timeout 60000 VLAN 200

# Chapter 14 MVR configuration

This chapter mainly includes the following contents:

- Introduction of MVR
- Configure the MVR

## 1.54 Introduction of MVR

Multicast VLAN registration (MVR) for multicast streaming applications in service provider networks, such as TV on demand. MVR allows a subscriber on a port to subscribe to or cancel a multicast stream within a multicast VLAN, allowing data streams within one multicast VLAN to be Shared by other VLans. MVR has two purposes :(1) it can effectively and safely transmit multicast streams between vlans through simple configuration; (2) Support the dynamic joining and leaving of multicast groups;

MVR is similar to IGMP Snooping in that both functions can be started at the same time. The MVR only handles the joining and leaving of configured multicast groups, and the joining and leaving of other groups is managed by IGMP Snooping. The difference is that a multicast stream in IGMP Snooping may be forwarded only within one VLAN, whereas an MVR multicast stream may be forwarded within a different VLAN.

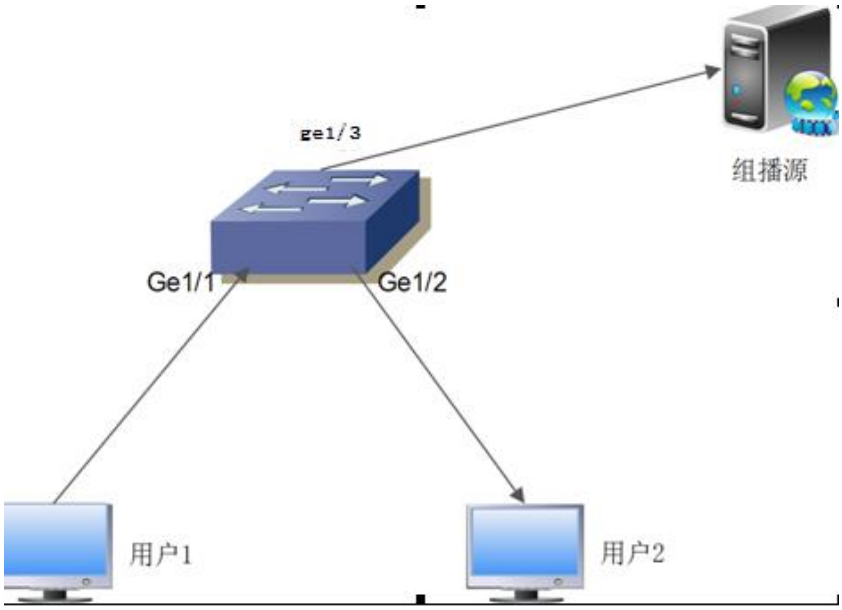
## 1.55 Configure the MVR

| The command | describe | CLI mode |
|---|---|---|
| MVR (enable \| disable) | Enable the global MVR | Global configuration mode |
| No MVR | Clear all MVR configurations | Global configuration |

| | | |
|---|---|---|
| | | mode |
| Nightly group A.B.C.D | Configure IP multicast addresses | Global configuration mode |
| No MVR group A.B.C.D | Delete the IP multicast address | Global configuration mode |
| Nightly group A.B.C.D < > 1-256 | Configure the IP multicast address to configure a contiguous MVR group address | Global configuration mode |
| MVR vlan < > 1-4094 | Specifies the VLAN to receive multicast data | Global configuration mode |
| No MVR vlan | Restore the default VLAN1 for receiving multicast data | Global configuration mode |
| MVR - interface (enable \| disable) | Boot interface MVR | Interface configuration mode |
| Show the MVR | Displays MVR configuration information | Privileged mode |

## 1.56 MVR configuration example

The network topology is shown in the figure below. User 1 and user 2 belong to VLAN10 and VLAN20 respectively. User 1 and user 2 watch the same program.




Configure the VLAN, start global IGMP Snooping, configure MVR VLAN, MVR program scope, global enabling MVR:

Switch# configure terminal

The Switch (config) # IP igmp snooping

The Switch (config) # MVR enable

The Switch (config) # MVR vlan 100

The Switch (config) # MVR group 225.1.1.1 64

Switch#

Configure switch user port Ge1/1 GE1/2 and uplink Ge1/3:

Switch# configure terminal

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # switchport mode hybrid

Switch(config-ge1/1)# Switchport Hybrid Native VLAN 10

Switch(config-ge1/1)# Switchport hybrid Allowed VLAN Add 100 Egres-Tagged disable

The Switch (config - ge1/1) # MVR enable

The Switch (config - ge1/1) #

Switch# configure terminal

The Switch (config) # interface ge1/2

The Switch (config - ge1/2) # switchport mode hybrid

Switch(config-ge1/2)# Switchport Hybrid Native VLAN 20

Switch(Config-GE1/2)# Switchport hybrid Allowed VLAN Add 100 Egres-Tagged disable

The Switch (config - ge1/2) # MVR enable

The Switch (# config - ge1/2)

Switch# configure terminal

The Switch (config) # interface ge1/3

Switch(Config-ge1/3)# Switchport Access VLAN 100

The Switch (config - ge1/3) #

# Chapter 15 Configure the DHCP SNOOPING

In dynamic access network environment, the host gets IP address and network parameters through DHCP server. DHCP SNOOPING is a listener protocol for ARP attacks. By listening to DHCP messages, the DHCP server dynamically binds the IP address of the client to the MAC address of the client, thus filtering ARP attack messages on the switch.

Switches support DHCP SNOOPING function to effectively defend against ARP attacks. DHCP SNOOPING listens for DHCP messages on the network, and binds port ARP information.

Four DHCP server physical ports can be configured to prevent unknown servers from interfering with the network to some extent.

This chapter describes the concept and configuration of DHCP SNOOPING, including the following:

- DHCP SNOOPING is introduced
- DHCP SNOOPING configuration
- Example DHCP SNOOPING configuration

## 1.57 DHCP SNOOPING is introduced

ARP protocol has caused vulnerabilities in network security due to its simple trust

mechanism. When an ARP attack packet with false MAC information arrives at the host, it will directly overwrite the local ARP cache table without restriction, causing normal data flow to the attacker. To this end, ARP information binding of ports is implemented on network layer 2 switches, which can effectively filter ARP attack packets and prevent them from reaching the attacked host. If an unanticipated DHCP server enters the network, IP address assignment will be chaotic. The DHCP SNOOPING Protocol provides the physical port that is bound to the linked server, and the non-specified physical port cannot forward the DHCP protocol packet sent by the DHCP server, thus reducing the chance of the unknown server entering the network.

This section mainly includes the following contents:

- The DHCP SNOOPING process
- DHCP SNOOPING Binding Table
- The physical port of the DHCP SNOOPING binding server

## 1.57.1 The DHCP SNOOPING process

DHCP SNOOPING Protocol only listens for DHCPrequest, DHCPack and DHCPrelease, does not receive other DHCP packets, and binds the MAPPING relationship between IP and MAC according to these packets.

The global DHCP SNOOPING switch is responsible for opening the switch to receive DHCP packets, i.e. IP packets with UDP ports of 67 and 68.

## 1.57.2 DHCP SNOOPING Binding Table

An DHCP SNOOPING Binding table entry is indexed by MAC address, containing the entry type, IP address, MAC address, interface information, delay timer, and lease timer. There are two types, REQ and ACK. An entry of REQ means that the DHCPrequest message has been received but the DHCPack message has not been received yet. At this time, the delay timer is started with a default interval of 10 seconds. An ACK type entry indicates that the DHCPack packet is received, and the IP address recorded is the IP address assigned by the server. At this time, the lease timer is started, and the time interval is the lease value provided by the DHCP server contained in the DHCPack packet. When the contract is renewed, the timer is restarted, and when the lease expires, the binding table entry is deleted. Interface information records the interface where the client is located, that is, the interface corresponding to the binding relationship between IP address and MAC address.

When DHCPrequest message is received, a binding table entry of type REQ is created, IP address, MAC address, interface information is recorded, and a 10-second delay timer is started.

When the DHCPrequest message is received, the bound table entry of type REQ already exists, then the entry is updated and the delay timer is restarted.

When the DHCPrequest message is received and the binding table entry of type ACK already exists, the interface information is recorded.

When the DHCPack packet is received, if there is a binding table entry of type REQ, the IP address assigned by the server in the DHCPack packet will be recorded, the delay timer will be turned off, and the lease timer will be started.

When a DHCPack packet is received and no REQ binding table entry is present, the

packet is discarded.

When the DHCPack packet is received, the binding table entry of type ACK already exists. If the interface has changed, the binding table entry of the original interface will be deleted and the entry will be updated.

If the interface does not change and the IP address assigned by the server changes, the binding table entry for the original interface is deleted and the entry is updated.

If the interface does not change and the IP address does not change, then it is a renewal process and just restart the lease timer.

The binding table entry of type REQ is deleted when the delay timer time out.

The binding table entry of type ACK is deleted when the lease timer timeouts.

### 1.57.3 DHCP SNOOPING specifies the physical port of the linked server

DHCP SNOOPING specifies the physical port of the linked server, and only DHCP messages may be received on the specified port. If there are multiple DHCP servers in the network, offers from servers not on the specified port will be filtered and the CLIENT cannot be assigned an IP address. The designated port is conducive to the uniform allocation of IP addresses in the network, avoiding that the address pool of unknown servers is not in the IP planning and some clients cannot connect to the network normally. To a certain extent, it reduces the probability of abnormal network communication caused by unauthorized access to the server.

# 1.58 DHCP SNOOPING configuration

## 1.58.1 DHCP SNOOPING Default configuration

DHCP SNOOPING is closed by default.

The default time interval for an entry delay timer of type REQ in the DHCP SNOOPING table is 10 seconds.

## 1.58.2 Global open and close DHCP SNOOPING

To open or close the DHCP SNOOPING of an interface, you must close all DHCP SNOOPING of all interfaces before closing the global DHCP SNOOPING.

Open global DHCP SNOOPING

Switch# configure terminal

The Switch (config) # IP DHCP snooping [IF_LIST]

Parameter is the physical port list of the DHCP server to be bound. A total of four ports can be specified. The port list is separated by '', '', such as :ge1/1, Ge1/4,ge1/5

Close global DHCP SNOOPING

Switch# configure terminal

The Switch (config) # no IP DHCP snooping

## 1.58.3 Interface open and close DHCP SNOOPING

Open DHCP SNOOPING for a port

Switch# configure terminal

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # DHCP snooping

Close DHCP SNOOPING for a port

Switch# configure terminal

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # no DHCP snooping

## 1.58.4 Interface open and close DHCP SNOOPING OPTION82

Open an interface for DHCP SNOOPING OPTION82

Switch# configure terminal

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # DHCP snooping option82

Close a port for DHCP SNOOPING OPTION82

Switch# configure terminal

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # no DHCP snooping option82

The circu-ID of DHCP SNOOPING OPTION82 is configured for a port

Switch# configure terminal

The Switch (config) # interface ge1/1

Switch(Config-ge1/1)# DHCP Snooping Option82 CircuitID Vlan111

Remove the circu-ID of DHCP SNOOPING OPTION82 for a port

Switch# configure terminal

The Switch (config) # interface ge1/1

Switch(Config-ge1/1)# No DHCP Snooping Option82 CircuitID

## 1.58.5 According to the information

Display the DHCP SNOOPING configuration information

Switch# show DHCP snooping

Displays the DHCP SNOOPING Binding table information

Switch# show DHCP snooping binding - table

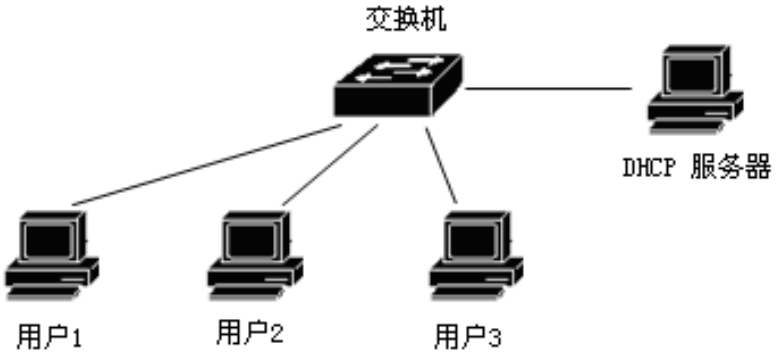
Displays the current configuration of the system, including the DHCP SNOOPING configuration.

Switch# show running - config

## 1.59 Example DHCP SNOOPING configuration

### 1.59.1 configuration

Enable DHCP SNOOPING function on the switch layer 2. User 1, user 2, and User 3 get the IP address and network parameters dynamically through the DHCP server. The interface of user 1, user 2 and user 3 starts DHCP SNOOPING OPTION82 function, with circuit- ID of AAA, and dynamically binds ARP information in the interface.




Switch# configure terminal

The Switch (config) # IP DHCP snooping ge1/5

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # DHCP snooping

The Switch (config - ge1/1) # DHCP snooping option82

Switch(Config-ge1/1)# DHCP Snooping Option82 CircuitID AAA

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

The Switch (config - ge1/2) # DHCP snooping

The Switch (config - ge1/2) # DHCP snooping option82

Switch(Config-ge1/2)# DHCP Snooping Option82 CircuitID AAA

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

The Switch (config - ge1/3) # DHCP snooping

The Switch (config - ge1/3) # DHCP snooping option82

Switch(Config-ge1/3)# DHCP Snooping Option82 CircuitID AAA

The Switch (config - ge1/3) # end

View DHCP Snooping Information

Switch# show DHCP snooping

DHCP Snooping is enabled fundamental

The DHCP Server interface: ge1/5

Enable interface: ge1/1, ge1/2, ge1/3

Option 82 Interface: GE1/1 (Circuit ID: AAA) GE1/2 (Circuit ID: AAA) GE1/3 (Circuit ID: aaa)

Switch#

Switch# show DHCP snooping binding - table

| IP | MAC | FLAG | The PORT | LEASE |
|---|---|---|---|---|
| 192.168.1.100 | 00:11:5 b: 34:42: AD | ACK | Ge1/1 | 23:59:58 |
| 192.168.1.101 | 00:11:6 4:52:13:5 d | ACK | Ge1/2, | 23:50:01 |
| 192.168.1.102 | 00:11:8 0-4 d: a2:46 | ACK | Ge1/3 | 20:34:45 |

## 1.60Configuration error for DHCP SNOOPING

If the DHCP Snooping configuration fails, it may be caused by:

1. System CFP resource is exhausted.

   If an interface is configured with ACL filtering, the global opening of DHCP SNOOPING fails

3. If an interface is configured with IP and MAC binding, the global opening of DHCP SNOOPING fails

4. The current interface is configured with ACL filtering.

5. The current interface enables 802.1x anti-ARP spoofing function.

The configured interface is a three-tier interface or a trunk interface.

# Chapter 16 The DHCP CLIENT configuration

## 1.61 The DHCP CLIENT to introduce

DHCP (Dynamic Host Configuration Protocol) is based on the working mode of Client/Server. The function of DHCP Client is to obtain the address and gateway of the three-tier interface address of the switch through DHCP Server.

This section mainly includes the following contents:

- Configuration of DHCP CLIENT

## 1.62 The DHCP CLIENT configuration

Open DHCP Client function of vlan1

The switch # (config)

The Switch (config) # interface vlan1

The Switch (config - vlan1) # DHCP client enable

The docking port vLAN1 retrieves the IP address

The switch # (config)

The Switch (config) # interface vlan1

The Switch (config - vlan1) # DHCP client to renew

Release the IP address of the interface VLAN1

The switch # (config)

The Switch (config) # interface vlan1

The Switch (config - vlan1) # DHCP client release

# Chapter 17
# Configure the DHCP RELAY

This chapter mainly includes the following contents:

- The DHCP RELAY is introduced
- The DHCP RELAY configuration
- DHCP RELAY configuration example

## 1.63 The DHCP RELAY is introduced

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP, which can dynamically configure the network environment for hosts on the network and is divided into server side and client side. The server manages IP network data centrally and processes client requests, dynamically configuring client TCP/IP environment. When DHCP is working, at least one server is on the network. It can listen for DHCP requests from hosts on the network and negotiate TCP/IP parameters. Its allocation has automatic and dynamic two kinds. Automatically, the client USES the IP address permanently once it has acquired it. In dynamic mode, the client gets an IP address with a lease and needs to release it once the lease expires. You can also renew your contract in advance, or rent another IP. Dynamic allocation can effectively solve the problem of IP deficiency.

Working process of DHCP:

If the client is logging into the network for the first time and does not have any IP data, it will broadcast a Discover message with the source address 0.0.0.0 and destination address 255.255.255.255. If the server does not respond, Discover requests are issued four times at regular intervals.

When the server receives Discover, it selects an idle IP to respond to the client Offer message.

If there are multiple servers on the network, the client will receive multiple Offer messages, generally select the Offer that arrives first, broadcast the Request message, and tell all servers which server has received the IP address.

If the client finds that the IP has been used through ARP, it will send Decline message to the server and reject the Offer. And restart the Discover process.

When the server receives the Request message, it will send an Ack message to the client to confirm the validity of the lease.

If the client has applied for DHCP lease, it is generally unnecessary to use Discover process. Request renewal is sent to the server using the IP already leased before the lease expires. The server will try its best to let the client use the original IP. If there is no problem, the server will reply Ack message for confirmation. If the IP is already used by another client, the server will reject the renewal request in response to the Nack packet.

The client can voluntarily rescind the lease using the Release message.

The workstation issues a Request when starting up; In the middle of the lease, the Request will be sent again. If there is no confirmation, the IP can still be used. A Request will be sent at 3/4 of the lease, and the IP will no longer be used if there is no confirmation.

Discover packets are broadcast and only within the same network segment. The router does not spread out the broadcast packets. When the server and client are not in the same network segment, the client has not obtained the IP environment setting and does not know the location of the router, then Discover message cannot reach the server. To solve this problem, the function of DHCP Relay can be used to ask routers to relay DHCP protocol messages, so that DHCP can operate across network segments.

## 1.64 The DHCP RELAY configuration

DHCP Relay function is mostly related to the interface. It realizes the protocol message forwarding of DHCP across the network segment and carries out relevant configuration in the interface mode.

The configuration of DHCP-Relay includes:

- Start the DHCP-Relay function of the interface

## 1.64.1 Start the DHCP-Relay function of the interface

Pattern: Interface configuration pattern

Command: DHCP Relay < 1 > IP address - [IP address - 2] Turn on the DHCP Relay protocol on the interface

Command: No DHCP Relay Close the DHCP Relay protocol on the interface

Default: The DHCP Relay protocol is not turned on.

## 1.64.2 According to the information

Display DHCP Relay configuration information

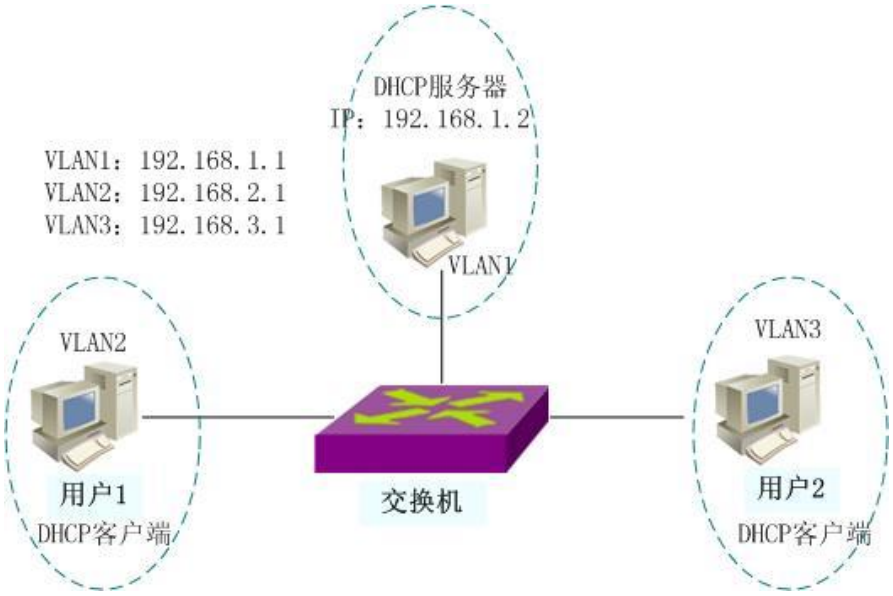
Switch# show the DHCP relay

# 1.65 DHCP RELAY configuration example

**(1) configuration**

The DHCP relay and forwarding configuration of the switch is required to enable the

switch to route and forward DHCP requests of user 1 and user 2 and DHCP reply confirmation information of the DHCP server. User 1 and User 2 can access the network by obtaining legitimate IP addresses through DHCP servers in different network segments.




The Switch > en

Switch# configure terminal

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # vlan 3

The Switch (config - vlan) # exit

The Switch IP interface vlan # 2 (config)

The Switch IP interface vlan # 3 (config)

The Switch (config) # int ge1/2

The Switch (config - ge1/2) # sw access vlan 2

The Switch (config - ge1/2) # int ge1/3

The Switch (config - ge1/3) # sw access vlan 3

The Switch (config - ge1/3) # interface vlan2

The Switch (config - vlan2) # IP address 192.168.2.1/24

The Switch (config - vlan2) # DHCP relay 192.168.1.2 instead

The Switch (config - vlan2) # interface vlan3

The Switch (config - vlan3) # IP address 192.168.3.1/24

The Switch (config - vlan3) # DHCP relay 192.168.1.2 instead

**(2) the validation**

The show running - config  Display configuration commands

Show DHCP Relay shows DHCP Relay configuration information

# Chapter 18
# Configure the DHCP SERVER

This chapter mainly includes the following contents:

- The DHCP SERVER is introduced
- The DHCP SERVER configuration
- DHCP SERVER configuration example

## 1.66 The DHCP SERVER is introduced

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP, which can dynamically configure the network environment for hosts on the network and is divided into server side and client side. The server manages IP network data centrally and processes client requests, dynamically configuring client TCP/IP environment. When DHCP is working, at least one server is on the network. It can listen for DHCP requests from hosts on the network and negotiate TCP/IP parameters. Its allocation has automatic and dynamic two kinds. Automatically, the client USES the IP address permanently once it has acquired it. In dynamic mode, the client gets an IP address with a lease and needs to release it once the lease expires. You can also renew your contract in advance, or rent another IP. Dynamic allocation can effectively solve the problem of IP deficiency.

Working process of DHCP:

If the client is logging into the network for the first time and does not have any IP data, it will broadcast a Discover message with the source address 0.0.0.0 and destination address 255.255.255.255. If the server does not respond, Discover requests are issued four times at regular intervals.

When the server receives Discover, it selects an idle IP to respond to the client Offer message.

If there are multiple servers on the network, the client will receive multiple Offer messages, generally select the Offer that arrives first, broadcast the Request message, and tell all servers which server has received the IP address.

If the client finds that the IP has been used through ARP, it will send Decline message to the server and reject the Offer. And restart the Discover process.

When the server receives the Request message, it will send an Ack message to the client to confirm the validity of the lease.

If the client has applied for DHCP lease, it is generally unnecessary to use Discover process. Request renewal is sent to the server using the IP already leased before the lease expires. The server will try its best to let the client use the original IP. If there is no problem, the server will reply Ack message for confirmation. If the IP is already used by another client, the server will reject the renewal request in response to the Nack packet.

The client can voluntarily rescind the lease using the Release message.

The workstation issues a Request when starting up; In the middle of the lease, the Request will be sent again. If there is no confirmation, the IP can still be used. A Request will be sent at 3/4 of the lease, and the IP will no longer be used if there is no confirmation.

DHCP Server protocol module receives Discover, Request, Decline and Release messages, which are used to dynamically assign IP addresses to clients in the network, and maintain their own address pool information and assigned client information.

## 1.67 The DHCP SERVER configuration

DHCP Server needs to be configured in global mode, interface mode and address pool mode, including startup command, address pool configuration, global setting, mode switch and other commands.

The configuration of DHCP Server includes:

- Start the global DHCP Server function
- Start interface to receive DHCP Server message
- Configure address pool
- Configure the address pool scope
- Configure the address pool net mask
- Configure the address pool lease
- Configure the address pool default gateway
- Configure the address pool DNS server
- Configure the address pool to manually exclude addresses

## 1.67.1 Start the global DHCP Server function

Pattern: Global configuration pattern

Command: IP DHCP Server Start the global DHCP Server protocol

Command: no IP DHCP Server Close the global DHCP Server protocol

Default: DO not open DHCP Server protocol; Use this command to start the DHCP Server protocol.

## 1.67.2 Start interface to receive DHCP Server message

Pattern: Interface configuration pattern

DHCP Server listen Interface starts to receive DHCP Server protocol message

Command: No DHCP Server listen interface closed do not receive DHCP Server protocol packets

Default: Interface does not start, cannot receive DHCP Server protocol message.

## 1.67.3 Configure address pool

Pattern: Global configuration pattern

Command: DHCP server pool <pool-name> Create an address pool and enter address pool mode

Command: no DHCP server pool <pool-name> Removes the specified address pool

Parameter: <pool-name> address pool name, used to distinguish different address pools. Maximum 16 characters.

Default: Address pool is not configured. Configure the address pool, only create the address pool name, enter the address pool configuration mode, not configure the actual address.

## 1.67.4 Configure the address pool scope

Mode: Address pool configuration mode

Command: range <low-address> <high-address> Configure the address pool scope

Command: no range Delete the address pool scope

Parameters: <low-address> address pool range starting address, dotted decimal format; <high-address> address pool range end address, dotted decimal format.

Default: Address pool scope is not configured. When a range is configured in the address pool, each dynamically allocable address entry in that range in the address pool is created.

## 1.67.5 Configure the address pool net mask

Mode: Address pool configuration mode

Command: subnet-mask <address> Configure the address pool net mask

Parameter: <address> mask address, dotted decimal format, for variable length mask.

Default: 255.255.255.0 defaults to a 24-bit mask.

## 1.67.6 Configure the address pool lease

Mode: Address pool configuration mode

Lease [<days> <hours> <minutes>|infinite] Configure the address pool lease

Parameter: <days> is the number of days and the range is 0-999; <hours> is the number of hours, ranging from 0 to 23; <minutes> is the number of minutes, and the range is 0-59; Are integers. Infinite is an Infinite lease.

Default: 8 days lease.

## 1.67.7 Configure the address pool default gateway

Mode: Address pool configuration mode

Default-router <ip-address> Configure the address pool default gateway

Command: No default-Router Remove the address pool default gateway

Parameter: <ip-address> default gateway IP address, dotted decimal format, should be in the same network segment as the address pool range.

Default: The default gateway is not configured.

## 1.67.8 Configure the address pool DNS server

Mode: Address pool configuration mode

DNS -server <ip-address1> [ip-address2] Configure the address pool DNS server

Command: No DNS - Server Delete the address pool DNS server

Parameters: <ip-address1> and <ip-address2> are DNS server IP addresses, dotted decimal format, two DNS servers can be configured at most, or one can be configured. If configuring two, type in one command instead of two. If entered twice, the DNS server IP address entered later overrides the DNS server address configured earlier, regardless of whether one or two were configured earlier.

Default: DNS server is not configured.

## 1.67.9 Configure the address pool to manually exclude addresses

Mode: Address pool configuration mode

Exclude-address <ip-address> Configure the address pool to manually exclude addresses

Exclude-address <low-address> <high-address> configure manually exclude address ranges

Command: no exclude-address <ip-address> Restore a manually excluded address

Exclude-address <low-address> <high-address> configure manually exclude address range recovery

Command: no exclude-Address all Restore all manually excluded addresses in the address pool

Parameter: <ip-address> manually excluded IP address, dotted decimal format, one command can exclude one available address in the address pool range at a

time.<low-address> and <high-address> are the starting and ending IP addresses that manually exclude the address range. In decimal format, one command can exclude multiple consecutive available addresses in the address pool range at a time. If the existing addresses in the range are manually excluded, it is only skipped without any prompt.Manual exclusion means that the address entry within the address pool scope will not be dynamically allocated.

Default: Manually excluding addresses is not configured.

## 1.67.10 Configuration OPTION82

Mode: Address pool configuration mode

Command: option82 circuit-id <circuit-id> Configure the circuit-ID for Option82

Parameters: < circuit-id > string, maximum length of 64.

## 1.67.11 Clears the assigned address table entry

Pattern: EXEC configuration pattern

Clear DHCP server address {[ip-address] | [all]}

Deletes an address or all address table entries that have been assigned.

### 1.67.12 Clears the detected conflicting address table entries

Pattern: EXEC configuration pattern

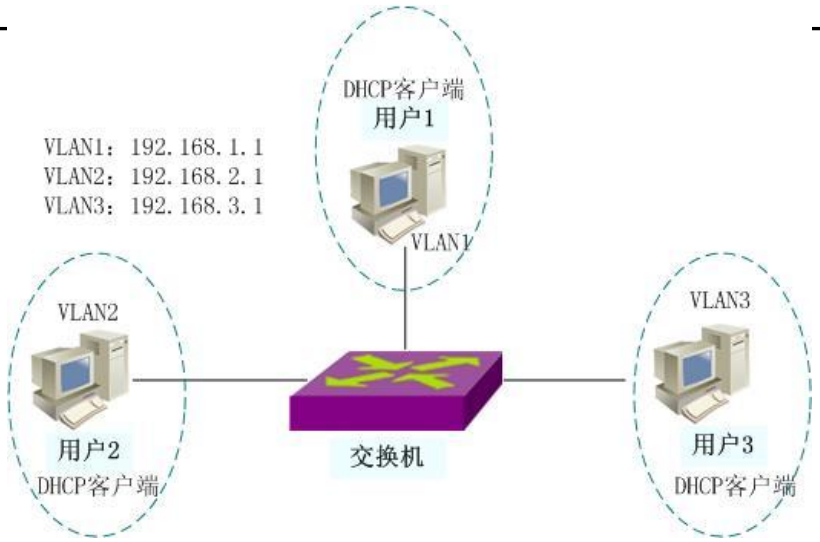
Command: clear DHCP server address conflict {[ip-address] | [all]}

Delete any address automatically excluded due to a conflict detected. Delete all conflicting addresses. Delete any single address automatically excluded due to a conflict.

## 1.68 DHCP SERVER configuration example

**(1) configuration**

For clients of three different subnets of VLAN1, VLAN2 and VLAN3, the corresponding address pool is configured, so that the switch as DHCP Server can allocate the IP address of corresponding network segment to clients in these three subnets.




The Switch > en

Switch# configure terminal

The Switch (config) # IP DHCP server

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # vlan 3

The Switch (config - vlan) # exit

The Switch IP interface vlan # 2 (config)

The Switch IP interface vlan # 3 (config)

The Switch (config) # int ge1/2

The Switch (config - ge1/2) # sw access vlan 2

The Switch (config - ge1/2) # int ge1/3

The Switch (config - ge1/3) # sw access vlan 3

The Switch (config - ge1/3) # interface vlan2

The Switch (config - vlan2) # IP address 192.168.2.1/24

The Switch (config - vlan2) # DHCP server listen

The Switch (config - vlan2) # interface vlan3

The Switch (config - vlan3) # IP address 192.168.3.1/24

The Switch (config - vlan3) # DHCP server listen

The Switch (config - vlan3) # interface vlan1

The Switch (config - vlan1) # DHCP server listen

The Switch (config) # DHCP server pool a

The Switch (config - DHCP) # range 192.168.2.1 192.168.2.20

The Switch (config - DHCP) # lease 2 0 0

The Switch (config - DHCP) # default - the router 192.168.2.1

The Switch (config - DHCP) # DNS server - 1.1.1.1 2.2.2.2

The Switch (config - DHCP) # exclude - address 192.168.2.10

The Switch (config - DHCP) # exit

Switch(config)# DHCP Server Pool B

The Switch (config - DHCP) # range 192.168.3.2 192.168.3.20

The Switch (config - DHCP) # default - the router 192.168.3.1

The Switch (config - DHCP) # exit

Switch(config)# DHCP Server Pool C

The Switch (config - DHCP) # range 192.168.1.2 instead 192.168.1.20

The Switch (config - DHCP) # default - the router 192.168.1.1

The Switch (config - DHCP) # exit

**(2) the validation**

The show running - config  Display configuration commands

Show the DHCP server  Displays global configuration information

Show DHCP Server Pool [Pool-Name] displays address pool configuration information, which can be used to display individual address pool information.

Show the DHCP server address  Displays the assigned address table entry information.

# Chapter 19
# Configure an ACL

In the actual network, the network access security is the administrator's concern. Switches support ACL filtering to provide network access security. By configuring ACL rules, switches secure access to the network by filtering incoming data streams based on these rules.

This chapter describes how to configure ACLs, mainly including the following:

- Introduction to ACL repository
- Introduction to ACL filtering
- ACL repository configuration
- ACL filtering configuration
- Example ACL configuration

## 1.69 Introduction to ACL repository

An Access List Control repository is a set of multiple Access rules. The ACL repository has no function to control the forwarding of data, but is only a set of rules with collation. After an ACL repository is referenced by an application, the application controls the forwarding of the data according to the rules provided by the ACL resource. Acls can

be applied to port access filtering, service access filtering, QoS, and so on.

ACL resource library has standard IP rule group (group no. 1-99, 1300-1999), extended IP rule group (group no. 100-199, 2000-2699), IP MAC group < group no. 700-799 >, ARP group (group no. 1100-1199); Each set of rules is automatically prioritized by conflicting rules. When a user concodes an ACL rule, the system inserts the rule into the appropriate place based on the collation rule.

In application, when a packet passes through a port, the switch compares the fields in each rule with all the corresponding fields in the packet; When more than one rule matches perfectly at the same time, the first rule that matches perfectly takes effect. This matching rule determines whether the packet is forwarded or discarded. A perfect match is when the value of the field in the rule is exactly the same as the value of the corresponding field in the packet. Only if a rule in the ACL is a perfect match will the rule perform a corresponding deny or permit operation.

In a switch, rules within the same set are automatically sorted. The automatic sorting of rules is relatively complex. In the sorting process, the rules with a large range are ranked in the back, while those with a small range are ranked in the front. The size of the scope is determined by the constraints of the rule; The fewer constraints a rule has, the larger the range of rule matches, and the more constraints a rule has, the smaller the range of rule matches. The constraints of the rule are mainly reflected in the address wildcard and the number of some non-address fields. A Wildcard is a bit string. The IP address is four bytes and the MAC address is six bytes. Bits' 1 'means no match is needed, bits' 0' means match is needed. Non-address fields are protocol types, IP protocol types, protocol ports, and these fields also hide a wildcard. Their length is the byte length of the corresponding field, so the same field length is uniform, just count the number of fields. The more bits a Wildcard has of '0', the more constraints there are.

The following is an example of port access filtering to illustrate the necessity of

rule-sorting and the advantages of automatic sorting. If the user needs to reject the address forwarding of the source address of 10.10.10.0/16 network segment and allow the address forwarding of the source address of 192.168.1.0/24 network segment, the following two rules can be configured:

Access-list 1 permit 192.168.1.0 0.0.0.255- Rule 1

Access-list 1 Deny 10.10.10.0 0.0.255.255 - Rule 2

This is abbreviated as Rule 1 and Rule 2.

These two rules are in conflict; Because the address of rule 1 is contained in the address of rule 2, and one is deny and the other is permit;Depending on the filtering principle of ACL, different orders have different results. To achieve this, the order of the two rules above must be: Rule 1 first, rule 2 second. The switch automatically implements the above sorting function, so that no matter in what order the user configures the above rules, the last order is rule 1 before rule 2. When a packet with the address of 192.168.1.1 is forwarded, the first rule is compared and then the second rule is compared. Both rules are matched, and the previous rule is effective (forwarding). If the source address is 10.10.10.1 and only the first match is made, it is discarded (not forwarded).

If no sort is performed, the user may configure rule 2 now and rule 1 later. Rule 1 is next and Rule 2 is first.

Access-list 1 Deny 10.10.10.0 0.0.255.255- Rule 2

Access-list 1 permit 192.168.1.0 0.0.0.255- Rule 1

Because the preceding rule 2 contains the following rule 1, it can result in a situation where packets that exactly match rule 1 also exactly match Rule 2, which takes effect each time; And can't meet the needs of the application.

In the switch, '0.0.255.255' is wildcard bits. '1' for bits means no match and '0' for bits

means match.It can be seen that wildcard bits of Rule 2 are '0.0.255.255', which need to match two bytes (16 bits).The wildcard bits in Rule 1 are '0 0.0.255', and three bytes (24 bits) need to be matched;So the rule 'range' of Rule 2 is larger, so it comes in second.In extended IP, sorting needs to consider more regular fields, such as IP protocol types, communication ports, and so on. The collation rules are the same, that is, the more restrictions the configuration has, the smaller the 'scope' of the rule will be, and vice versa. The ordering of rules is implemented in the background and user commands can only be displayed in the order in which the user is configured.

The filter fields supported by the ACL include source IP, destination IP, IP protocol type (e.g., TCP, UDP, OSPF), source port (e.g., 161), and destination port. Users can configure different rules for access control according to different needs.

In a switch, a set of rules can be applied by multiple applications. For example, a set of rules is referenced by both port access filtering and service access filtering or by both port access filtering.

## 1.70 Introduction to ACL filtering

ACL filtering is performed at the input port of the switch, and the data flow input to this port is matched by rules to achieve port filtering. ACL filtering is all processed by the line speed of the switch, which will not affect the forwarding efficiency of the data stream.

When a port on the switch is not configured with ACL filtering, all data flows entered through that port do not match rules and can be forwarded through that port. When an ACL filter is configured on a port of the switch, all input streams passing through the port perform a rule match. If the action of the matching rule is permit, the data flow allows

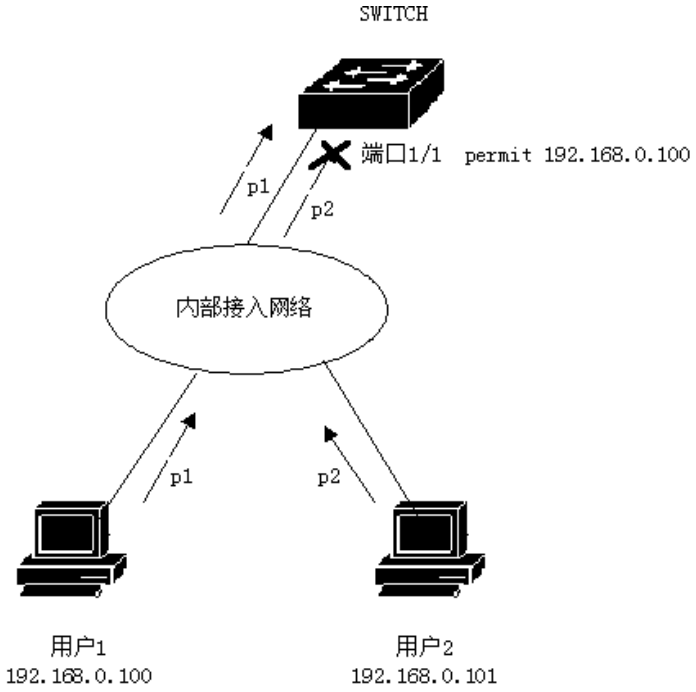
forwarding; if it is deny, the data flow does not allow forwarding and is discarded.

When configuring port ACL filtering, a port can select multiple ACL rule groups, which are then imported into the CFP of the port. If there are no rules in the group that reject or allow all IP protocol packets, then a rule that rejects all IP protocols is added to the CFP when written. When the rules in the ACL repository change, the rules in the CFP are automatically changed.

For example, there is only one rule in a set of rules: Access-List 1 permit 192.168.1.0 0.0.0.255, which hides a rule that rejects all IP protocol packages, and actually has two rules imported into the CFP of the port. In data stream filtering, only data streams from 192.168.1.0 to 192.168.1.255 of the source address can be forwarded through this port, and all other data streams are filtered out.

For example, there are two rules in a set of rules: Access-List 1 Deny 192.168.1.0 0.0.0.255 and Access-List 1 permit Any. There is a rule that allows all IP packets, there is no hidden rule, there are actually two rules imported into the CFP of the port. When filtering the data stream, only the data stream with the source address from 192.168.1.0 to 192.168.1.255 is filtered out, and all other data streams can be forwarded.

The following figure shows an example of ACL filtering. Port 1/1 of the switch selects an ACL rule group 1, which has only one rule, Access-List 1 permit 10.10.10.100. Under port 1/1 of the switch, two users want to access the network from that port. The IP address of User 1 is 10.10.10.100 and that of User 2 is 10.10.10.101. Only Subscriber 1 can access the network through port 1/1 of the switch, and subscriber 2 cannot access the network through port 1/1 of the switch. Data flow P1 from User 1 can be forwarded through port 1/1 of the switch, while data flow P2 from user 2 is discarded at port 1/1 of the switch.




Multiple ports can select the same ACL rule group and use the same filter rules.

Whether a set of rules or groups of rules are referenced by a port, they are automatically sorted, even if there is a crossover between the two sets of rules.

When a user references a set of rules, if the set of rules changes, the port referencing the set of rules will automatically respond to the user's configuration. There is no need to reconfigure the reference for this port.

## 1.71 ACL repository configuration

Switches have no rules by default.

The repository in the switch supports four types of ACL rules: standard IP rules, extended IP rules, IP MAC groups, and ARP groups. The following four types of rules

describe the configuration of acLs.

Standard IP rules: Standard IP rules control the forwarding of packets by the source IP address.

Access-list <groupId> {deny | permit} <source>

Parameter description:

GroupId: Access control list group number, standard IP ACL supports groups 1 through 99 or 1300 through 1999.

Deny /permit: If there is an exact match, the packet is rejected or allowed to be forwarded.

Source: Source IP has three input modes:

1)A.B.C.D wildcard can control the IP address from a network segment;

2) Any is equivalent to A.B.C.D. 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

Wildcard: Decide which bits need to match, '0' means match, '1' means no match.

Extended IP rules: Extended IP rules are extensions of standard IP rules that control packet forwarding through source IP, destination IP, IP protocol type, and service port.

Access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>

Parameter description:

GroupId: Access control list group number, extended IP ACL support from 100 to 199

or 2000 to 2699.

Deny /permit: If there is an exact match, the packet is rejected or allowed to be forwarded.

Protocol: The type of protocol above the IP layer, such as TCP, UDP, etc., can also be entered with the corresponding number 6(TCP). If you do not need to control these protocols, you can enter IP or 0.

Source: Source IP has three input modes:

1)A.B.C.D wildcard can control the IP address from a network segment;

2) Any is equivalent to A.B.C.D. 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

SrcPort: in the case where Protocol is TCP or UDP, the source port of the packet can be controlled. The input method can be some familiar port service names, such as WWW or a number, such as 80.

There are three ways to enter a destination IP:

1) A.B.C.D wildcard can control the IP address from a network segment;

2) Any is equivalent to A.B.C.D. 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

DestPort: In the case where Protocol is TCP or UDP, the destination port of the packet can be controlled, and the input mode is the same as srcPort.

TCP - Flag: For cases where Protocol is TCP. TCP field matching can be controlled for packets. Optional parameters include ACK, Fin, PSH, RST, SYN, urG.

IP MAC rules: THE IP MAC group controls both the source-destination MAC address and the source-destination IP address of the IP packet.

Access-list <groupid> {deny | permit} <src-mac> IP <src-ip> <dst-ip>

Parameter description:

GroupId: Access control list group number, extended IP ACL support from 700 to 799 groups.

Deny /permit: If there is an exact match, the packet is rejected or allowed to be forwarded.

Src-mac: Source MAC address.

MAC addresses can be entered in three ways:

1)HHHH.HHHH.HHHH wildcard can control MAC address from a segment;

2) Any is equivalent to hhhh.hhhh.HHHH.

3) Host A.B.C.D is equivalent to HHHh.HHHh.HHHH 0000.0000.0000

Src-ip: Source IP address.

DST - IP: Destination IP address.

There are three types of IP address input:

1) A.B.C.D wildcard can control the IP address from a network segment;

2) Any is equivalent to A.B.C.D. 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

ARP rules: ARP groups control the operation type of ARP packets, sender MAC, and sender IP.

Access-list <groupId> {deny | permit} arp {arp-type} <sender-mac> <sender- IP >

Parameter description:

GroupId: Access control list group number, extended IP ACL support from 1100 to 1199 groups.

Deny /permit: If there is an exact match, the packet is rejected or allowed to be forwarded.

Arp-type: any|reply|request. Any is the type that does not control the arp package. Reply is the response package that controls the arp package.

Sender-mac: The MAC address of the ARP packet sender.

MAC addresses can be entered in three ways:

1)HHHH.HHHH.HHHH wildcard can control MAC address from a segment;

2) Any is equivalent to hhhh.hhhh.HHHH

3) Host A.B.C.D is equivalent to HHHh.HHHh.HHHH 0000.0000.0000

Sender - IP: THE IP address of the sender of the ARP packet.

There are three types of IP address input:

1) A.B.C.D wildcard can control the IP address from a network segment;

2) Any is equivalent to A.B.C.D. 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

List of other commands:

Show the access - list (groupId)

Displays a list of rules configured in the current ACL. If groupId is entered, the list of rules for the current group; Otherwise all rule lists are displayed.

No access to a list < groupId >

Deletes the specified list of rules. GroupId group all rules.

## 1.72 Timetime-based ACLs

A time period is used to describe a particular time range. Users may have a need for some ACL rules to be in effect for a certain period of time, but not for other periods of time for message filtering, commonly known as time-by-time filtering. At this point, the user can configure one or more time periods and then refer to them by name under a rule that only takes effect for that specified time period, thus implementing ACL filtering based on the time period.

If the time period for a rule reference is not configured, the system prompts and allows such a rule to be created successfully, but the rule does not take effect immediately until the user has configured the time period for the reference and the SYSTEM time is within the specified time period range.

There are two configurations for the time period:

(1) Configure relative time period: adopt the form from a certain hour to a certain hour on a certain day;

(2) Allocation of absolute time period: adopt the form from a certain time of a certain month to a certain time of a certain day of a certain year.

Configure timetime-based ACLs:

| The command | describe | CLI mode |
| --- | --- | --- |
| Time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> | Configure a time period to include only a relative time period | Global configuration mode |
| Time-range WORD cycle-time days from <0-6> to <0-6> | Configure a time period to include only a relative time period of the week | Global configuration mode |
| The time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6> | Configure a time period to include a time period relative to the week | Global configuration mode |
| The time-range WORD utter-time from <2000-2100> <1-12 b> <1-31> <0-23> <0-59> to <2000-2100> <1-12> <1-31> <0-23> <0-59> | Assign a time period to such and such an absolute time period that includes the time of year, month and day | Global configuration mode |
| No time - range WORD cycle - time | Delete all relative time periods of such and such time periods | Global configuration mode |
| No time - range WORD utter - time | Delete all absolute time periods of a certain time period | Global configuration mode |
| No time - the range of | Delete x time period (including all relative and absolute time | Global configuration |

| | | |
|---|---|---|
| WORD | periods) | mode |
| No time - range | Delete all time periods | Global configuration mode |
| Show time - range WORD cycle - time | Displays all relative time periods for a certain time period | Privileged mode |
| Show time - range WORD utter - time | Displays all absolute time periods for a certain time period | Privileged mode |
| Show time - the range of WORD | Display such and such time periods (including all absolute and relative time periods) | Privileged mode |
| Show time - range | Show all time periods | Privileged mode |
| Time - the acl (< 1-99 > \| < > 100-199 \| < > 1300-1999 \| < > 2000-2699 \| < > 700-799 \| < > 1100-1199) time - the range of WORD | The so-and-so ACL rule applies the so-and-so period, when the ACL is applied to the interface | Global configuration mode |
| No time - acl (< 1-99 > \| < > 100-199 \| < > 1300-1999 \| < > 2000-2699 \| < > 700-799 \| < > 1100-1199) time - | Cancel the so-and-so ACL rule that applies a so-and-so period or all periods | Global configuration mode |

| | | |
|---|---|---|
| range (WORD \|) | | |
| Show time - acl (< 1-99 > \| < > 100-199 \| < > 1300-1999 \| < > 2000-2699 \| < > 700-799 \| < > 1100-1199) time - range | Displays all the time periods in which the so-and-so ACL rule was applied | Privileged mode |
| Show time - the acl all the time - range | Displays the period in which all ACL rules were applied | Privileged mode |

It should be noted that:

(1) Multiple relative time periods are configured for a certain time period, and the relation between relative time periods is or. In any relative time period, the system time is in active state.

(2) A certain time period is configured with multiple absolute time periods, and the relationship between absolute time periods is or. The system time is active in any absolute time period.

(3) If a certain time period is configured with both relative time period and absolute time period, relative time period and absolute time period are related to and, the time period will be activated only if the system time is both relative time period and absolute time period.

(4) A maximum of 256 time periods can be defined; A time period can be configured with a maximum of 256 relative and absolute time periods; An ACL rule can be applied for a maximum of 256 time periods; The time period comes into effect when the ACL rule associated with the time period is applied to the interface.

## 1.73 ACL filtering configuration

By default, all ports on the switch are not ACL filtered.

Command list:

Access - group < groupId >

Mode: Layer 2 interface configuration mode

Parameters:

GroupId: ACL group number that is bound to the port

Features: Configure ACL port filtering.

Note: If the above command configuration fails or is invalid, there may be the following reasons:

The rules in the ACL group are too many or the hardware resources are exhausted or occupied by other applications.

Displays the ACL port filter configuration

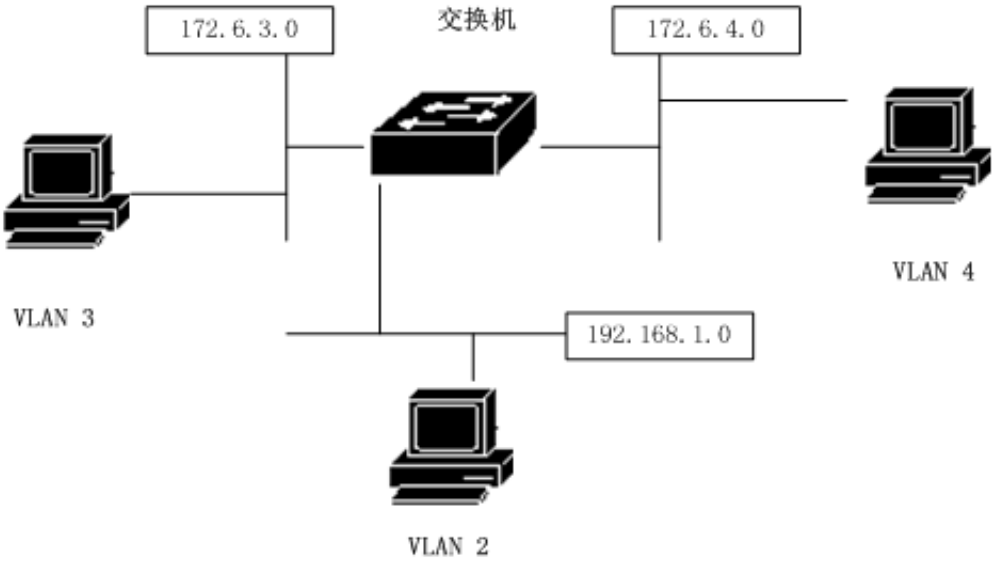
Show acccess - group

Remove the configuration associated with the current port and ACL port filtering

No acl - group < groupId >

## 1.74 Example ACL configuration

A switch is connected to three subnets, ACL is designed, blocking source address is 192.168.1.0 network address. Allowing traffic from other network addresses to pass through. 192.168.1.0 Network segment is connected to port 1/1 of the switch.




The configuration on the switch is as follows:

Switch# config t

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # vlan 3

The Switch (config) # interface ge1/1

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

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

The Switch (config) # interface vlan2

The Switch (config - vlan2) # IP add 192.168.1.1/24

The Switch (config) # interface ge1/2

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

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

The Switch (config) # interface vlan3

The Switch (config - vlan2) # IP add 172.16.3.1/24

Switch(config)# Access-List 10 deny 192.168.1.0 0.0.0.255

The Switch (config) # access - a list of 10 permit any)

The Switch (config) # interface ge1/1

The Switch (config - ge1/1) # access - group 10

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/2

The Switch (config - ge1/2) # access - group 10

## 1.75 ACL configuration error

If the ACL configuration fails, there may be the following reasons:

1. Make sure all IPs are common before configuring the Access control list, and then add the access control list.This access control list blocks IP data flowing through the switch at the source address of 192.168.1.0 segment. Pay attention to the subnet inverse code. Use the show Access-List command to list the

access control list and make sure that the source and destination addresses are not reversed. Then proceed to view the access Control list. Also, the default access control list always ends with an implicit deny any statement. If you want the rest to pass, you need to add a permit ANY statement, otherwise it will not pass.

2. The system is configured with static IP MAC binding.

3. The DHCP SNOOPING protocol is enabled for the current interface.

4. System CFP resource is exhausted.

# Chapter 20 Basic TCP/IP configuration

For a layer 2 switch with network management functions, the TCP/IP protocol needs to provide basic network configuration for communication with other devices.

This chapter mainly includes the following contents:

- Configure the VLAN interface
- Configure the ARP
- Configure static routing
- IP routing configuration example

## 1.76 Configure the VLAN interface

In a switch, each three-tier interface is attached to a VLAN, so the three-tier interface is also called a VLAN interface. The creation and deletion of VLAN interfaces is done manually, and a maximum of 4094 VLANs can be divided on the switch, but a maximum of 32 subnets can be established.Subnet interface can be created according to user requirements; The subnet interface can be removed by the user either manually or as the VLAN in which the subnet resides is deleted.

Each VLAN interface has a name, and the name of the VLAN interface is the string "VLAN" followed by the VLAN ID number. For example, the three-layer interface of VLAN 1 is named "vlan1", and the three-layer interface of VLAN 4094 is named "VLAN4094".

Like ports, VLAN interfaces have managed state and link state. Currently, switches do not provide configuration of the management state of VLAN interfaces, and the management state of VLAN interfaces is always UP as long as VLAN interfaces are created. The link state of the VLAN interface is related to the ports contained in the CORRESPONDING VLAN. As long as the link state of a port in the VLAN is RUNNING, the link state of the VLAN interface is RUNNING. If all ports in the VLAN are not RUNNING, the link state of the VLAN interface is also not RUNNING.

On a VLAN interface, you can configure IP addresses and specify the network prefix (which can be converted to a network mask) for the segment connected to the interface. Currently, switches only support configuring one IP address on one VLAN interface. The user needs to create a VLAN and add the associated port to the VLAN before configuring the IP address. By default, the switch has the VLAN1 interface, and the IP address is set on this interface 10.10.10.10.1/24. Users can also modify the IP address of the VLAN1 interface. IP addresses are not set by default for VLAN interfaces other than VLAN1.

The commands to configure the IP address of the VLAN interface are shown in the following table:

| The command | describe | CLI mode |
|---|---|---|
| The Ip interface vlan < 4094 > 2 - | Create a VLAN interface | Global configuration mode |
| No Ip interface vlan <2-4094> | Delete a VLAN interface | Global configuration mode |
| IP address < IP - prefix > | Set the IP address on the VLAN interface. Parameters include the IP address of the interface and the network prefix of the connected network segment. If the VLAN interface has an IP address, delete the original IP address before setting the specified IP address. The format of the parameters is A.B.C.D/M. | Interface configuration mode |
| No IP address [IP - prefix] | Delete the IP address of the VLAN interface. If a parameter is specified, it must be the same as the parameter given | Interface configuration mode |

| | | |
|---|---|---|
| | at the time of setting, otherwise this command is invalid. The format of the parameters is A.B.C.D/M. | |

The commands to view the VLAN interface are shown in the following table:

| The command | describe | CLI mode |
|---|---|---|
| The show interface [if - the name] | View VLAN interface information, including the INTERFACE's IP address, MAC address, management status, link status, etc. The parameter is the interface name of the VLAN interface. If no parameters are specified, view all ports and VLAN interface information. | Normal mode, privileged mode |
| The show running - config | To view the current configuration of the system, you can view the configuration of the VLAN interface. | Privileged mode |

Example:

Configure subnet 193.1.1.0 on VLAN3 interface with subnet prefix 24(i.e., mask 255.255.255.0), interface IP address 193.1.1.1, and view VLAN3 interface information. The order is as follows:

The switch (config) # interface vlan3

The switch (config - vlan3) # IP address 193.1.1.1/24

The switch (config - vlan3) # end

Switch# show interface vlan3

## 1.77 Configure the ARP

The ARP (Address Resolution Protocol) Protocol is a Protocol that maps IP addresses to corresponding MAC addresses. When the source sends Ethernet data frames to the destination in the same VLAN, the destination is determined based on the 48-bit Ethernet MAC address, and the destination determines whether the packet needs to be received or not based on the destination MAC address of the packet.

It is assumed that host A and B of two adjacent network segments communicate through the switch. Before sending data to host B, Host A first sends ARP request message to the interface of the switch directly connected to Host A, and sends packet to the interface after receiving ARP reply. After receiving this packet, the switch will first broadcast an ARP request packet to host B, and then send the packet to host B after receiving ARP response packet from Host B.

There is an ARP cache, called an ARP table, on the switch that holds a record of mapping IP addresses to MAC addresses in the directly connected network. Each item in

the ARP table has a lifetime, the default is 20 minutes. If the switch does not receive an ARP request or reply message for that IP address during the lifetime, the ARP table item corresponding to that IP address will be deleted.

This section includes the following:

- Configure static ARP
- Configure the ARP binding
- View ARP information

## 1.77.1 Configure static ARP

There are two different ARP items in ARP table, one is static ARP, the other is dynamic ARP. Static ARP is the ARP table item configured by the user through the command, the system will not automatically refresh and delete, need to be manually completed by the user. Dynamic ARP is the ARP automatically learned by the system according to the RECEIVED ARP request or reply packet. The system automatically creates and deletes, updates and maintains in real time, without user intervention, but users can manually delete dynamic ARP table entries.

The switch does not have static ARP table entries configured by default. It should be noted that when a VLAN interface is deleted or the IP of the interface subnetwork segment is changed, the static and dynamic ARP table items in the original subnetwork segment are deleted.

The commands to configure static ARP are shown in the following table:

| The command | describe | CLI mode |
| --- | --- | --- |
| Arp < IP - address > < MAC - address > | Configure static ARP table entries. The first parameter is the IP address, which must be in a subnetwork segment. The second parameter is MAC address, MAC address must be unicast MAC address, MAC address format is HHHH.HHHH.HHHH, such as 0010.5 CB1.7825. | Global configuration mode |
| No arp < IP - address > | Delete ARP table entries. Includes deleting an IP ARP table entry | Global configuration mode |

## 1.77.2 View ARP information

The commands to view ARP information are shown in the following table:

| The command | describe | CLI mode |
| --- | --- | --- |
| Show the arp | View ARP table item information in ARP table, including all ARP table | Normal mode, privileged mode |

| | | |
|---|---|---|
| | items, | |
| The show running - config | To view the current configuration of the system, you can view the configuration of ARP. | Privileged mode |

## 1.78 Configure static routing

Static routing is a user-defined route that takes packets from the source address to the destination address via a specified path. Packets that cannot be routed can be sent to the default gateway by configuring a static route as the default route.

Static routing is manually configured by the administrator. It is suitable for the network with simple network structure. The administrator only needs to configure the static route to make the switch work normally. Static routing does not consume valuable network bandwidth because there are no routing updates.

The default route is also a static route. Simply put, the default route is the one used when no matching route item is found. That is, the default route is used only if there are no suitable routes. In the routing table, the default route takes the form of a route to the network of 0.0.0.0/0 (with a mask of 0.0.0.0). If the destination of the message is not in the routing table and there is no route left in the routing table, an ICMP message will be returned to the source side indicating that the destination address or network is not reachable. Default routing is very useful in networks. In a typical network contains hundreds of switches, the dynamic routing protocol operation may take a large amount of bandwidth resources, using the default routing can be saves the time of occupied by

routing and packet forwarding occupied bandwidth resources, to some extent, so it can meet the needs of a large number of users at the same time to communicate.

Switches can configure multiple static routes to the same destination, but only one route is activated for actual data forwarding. The switch is not configured with static routing by default.

The commands to configure static routing are shown in the following table:

| The command | describe | CLI mode |
|---|---|---|
| IP route - < IP prefix > < nexthop - address > | Set up static routing. The first parameter specifies the segment IP and network prefix length, and the second parameter specifies the next-hop IP address. | Global configuration mode |
| IP route <ip-address> <mask-address> <nexthop-address> | It has the same function as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next-hop IP address. | Global configuration mode |

| | | |
|---|---|---|
| No IP route <ip-prefix> [nexthop-address] | Remove static routing. The first parameter specifies the segment IP and network prefix length, and the second parameter specifies the next-hop IP address. If there is no second argument, all routes matching the specified segment are deleted. If there is a second argument, the route that matches both the specified segment and the next hop is removed. | Global configuration mode |
| No IP route <ip-address> <mask-address> [nexthop-address] | It has the same function as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next-hop IP address. If there is no third parameter, all routes matching the specified segment are deleted. If there is a third parameter, the route that matches both the specified segment and the next hop is removed. | Global configuration mode |

See the following table for routing commands:

| The command | describe | CLI mode |
| --- | --- | --- |
| Show IP route [<ip-address> \| <ip-prefix> | View active route information, optionally view all routes, one route, one segment route, static route. | Normal mode, privileged mode |
| The show IP route database | View information for all routes (active and inactive), optionally viewing all routes. | Normal mode, privileged mode |
| The show running - config | View the current configuration of the system to see the configuration of the static route. | Privileged mode |

Example:

Set the destination network to 200.1.1.0, the subnet mask to 255.255.255.0, and the next hop to 10.1.1.2. The configuration command is:

Switch(config)# IP Route 200.1.1.0 255.255.255.0 10.1.1.2

or The Switch (config) # IP route 200.1.1.0/24 10.1.1.2

Delete the static route with destination IP address 200.1.1.0, subnet mask 255.255.255.0, and next hop 10.1.1.2. The configuration command is:

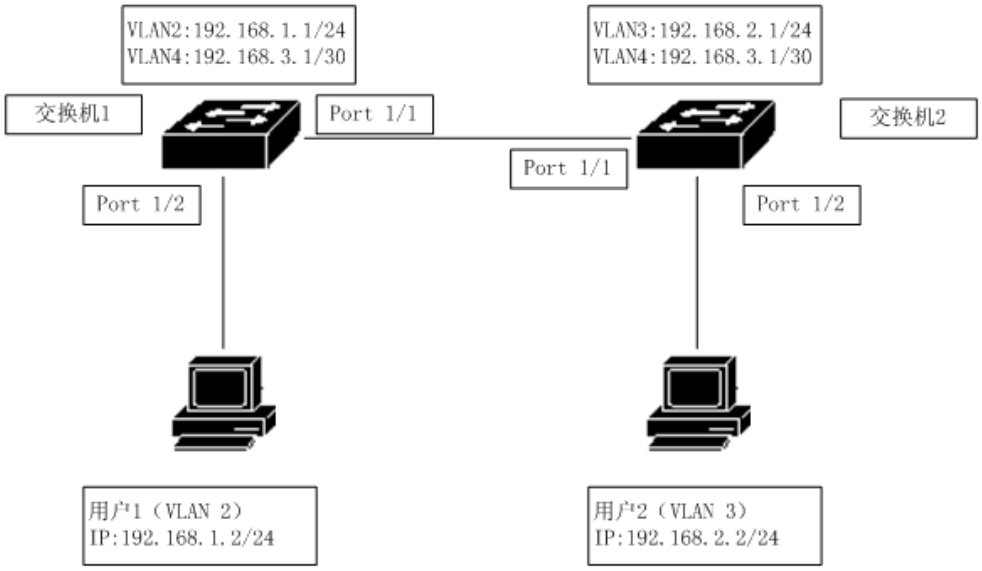
The Switch (config) # no IP route 200.1.1.0/24

Or Switch(config)#no IP Route 2001.1.0/24 10.1.1.2

or Switch(config)#no IP Route 200.1.1.0 255.255.255.0

or Switch(config)#no IP Route 200.1.1.0 255.255.255.0 10.1.1.2

## 1.79 TCP/IP Basic configuration example




In the figure, switch 1 is a two-layer switch and switch 2 is a three-layer switch.

### 1.79.1 Three layer interface

Configure the three-tier interface corresponding to VLAN2 on switch 1 and assign an IP address of 192.168.1.1/24 at the same time.

The configuration is as follows:

Switch# config t

The Switch (config) # vlan database

The Switch (config - vlan) # vlan 2

The Switch (config - vlan) # exit

The Switch (config) # interface ge1/2

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

The Switch IP interface vlan # 2 (config)

The Switch (config) # interface vlan2

The Switch (config - vlan2) # IP add 192.168.1.1/24

Verification: User 1 can ping the THREE-tier interface IP address corresponding to VLAN2 of switch 1.

## 1.79.2 Static routing

To access Switch 1, user 2 must access switch 1 through its routing function.

The configuration on switch 1 is as follows:

Switch# config t

192.168.2.0 255.255.255.0 192.168.3.2

The configuration on switch 2 is as follows:

Switch# config t

The Switch (config) # IP route 192.168.1.0/24 192.168.3.1

Verification: User 2 can ping general switch 1.

## 1.79.3 ARP

Configure user 1's static ARP to allow user 1 to access only from VLAN2. Assume that user 1's MAC address is 00:00:00:00:00:01.

Switch 1 configuration is as follows:

Switch# config t

The Switch (config) # arp 192.168.1.2 instead 0000.0000.0001

Verification: User 1 can ping the THREE-tier interface IP address corresponding to VLAN2 of switch 1.

# Chapter 21
# Configure SNMP

Switches provide SNMP for remote management of switches. This chapter describes

how to configure SNMP, mainly including the following contents:

This chapter mainly includes the following contents:

- SNMP introduce
- The SNMP configuration
- SNMP Configuration Example

## 1.80 SNMP introduce

SNMP is a simple network management protocol, is the most widely used network management protocol, it has five functions: fault management, billing management, configuration management, performance management, security management. It provides

information format for communication between network management application software and network management agent (Agent).

SNMP network management protocol has four elements: management workstation, management agent, management information base, network management protocol. On the switch, the management agent is the server that manages the workstation to access the switch. The information of the management workstation to access the network management agent is organized in the form of MIB to form the management information library.

SNMP has three major operations: GET operation, SET operation, TRAP operation. The GET operation enables the administrative workstation to GET the values of objects in the agent. The SET operation enables the administrative workstation to SET the values of objects in the agent. The TRAP operation enables the agent to notify the administrative workstation of events.

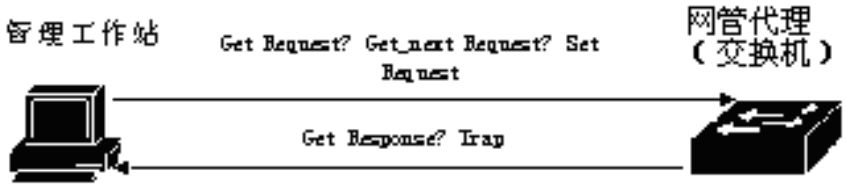
TRAP messages are actively sent to the management workstation when an event occurs in the switch. These messages include cold start, hot start, link up and Link down of the port, failure of common body name authentication, STP state switch, etc.

Currently, there are three versions of SNMP: SNMPV1, SNMPV2, and SNMPV3. The latter version is the upgraded version of the former, with enhanced functions and improved security. The switch supports all three versions of SNMP and can parse all three versions of SNMP protocol packages. When sending TRAP messages, you can use any of the versions of SNMPV1, SNMPV2, and SNMPV3.

Switches support RFC, BRIDGE, and private MIB objects and can be fully managed with SNMP. Some MIBs supported by switches are listed below: RFC 1213,RFC 1493,RFC 1724,RFC 1850,RFC 1907,RFC 2233,RFC 2571,RFC 2572,RFC 2573,RFC 2574,RFC 2575,

The MIB of RFC 2674.

The figure shows an example of SNMP protocol interaction between an administrative workstation and an administrative agent. The management workstation can access the switch management agent by sending SNMP messages of Get Request, GetNext Request, GetBulk Request and Set Request, Get or Set the MIB object value of the switch, and the switch management agent sends the SNMP message of Get Response back to the management workstation. When some events occur on the switch, the management agent of the switch actively sends SNMP TRAP messages to the management workstation.




Manage SNMP protocol interactions between the workstation and the administrative agent

## 1.81 The SNMP configuration

SNMP configuration includes community configuration of switches, TRAP workstation and CONFIGURATION of SNMP system information. By default, switches have a read-only shareware named PUBLIC. Switches can be configured with up to 8 shareware. The switch is not configured with TRAP workstations by default.

The commands of SNMP are shown in the following table:

| The command | describe | CLI mode |
| --- | --- | --- |
| SNMP community <community-name> {ro \| rw} | Configure the common name of the access network manager, which is an interactive command. At configuration time, the user is prompted for the name of the Shared body to be created and read/write permission. | Global configuration mode |
| No SNMP community < community - the name > | Deletes the specified SNMP common body name. | Global configuration mode |
| SNMP trap <notify-name> host <ipaddress> version {1 \| 2c \| 3} | Add or modify the sending target of SNMP trap. This is an interactive command.The notify Name is unique, and if you modify the existing name, you can modify the trap send target item.Host is the target address for sending trap;Version is sent as | Global configuration mode |

| | | |
|---|---|---|
| | snmpV1, snmpV2c or snmpV3.This command is configured to target port 162 by default. | |
| No SNMP trap < notify -name > | Deletes the specified SNMP trap. | Global configuration mode |
| SNMP system information <contact \| location \| name> <information-string> | Configure system information. Configurable system information includes contact, Location, and name. | Global configuration mode |
| No SNMP system information <contact \| location \| name > | Deletes a system configuration information. | Global configuration mode |
| Show the SNMP community | Displays all the current common body names and the corresponding read and write permission information. | Normal mode/privileged mode |
| Show the SNMP trap | Display all trap names and target IP addresses and version information sent by traps. | Normal mode/privileged mode |
| Show the SNMP system | Displays system information | Normal |

| | | |
|---|---|---|
| Information | for SNMP Settings. | mode/privileged mode |

## 1.82 SNMP Configuration Example

## 1.82.1 configuration

Configure a sharename operation called private to have read and write permissions.

Configure an SNMP trap named Test and send destination IP of 10.10.10.10; The SNMP version used is 1.

The specific content of contact of the configuration system is: E-mail:networks@acb.com.

The specific content of location of the configuration system is Shenzhen.

The specific content of configuration system name is: Switch.

The configuration of the switch is as follows:

Switch# config t

The Switch (config) # SNMP community private rw

Switch(config)# SNMP system information contact E-mail:networks@abc.com

Switch(config)# SNMP System Information Location Shenzhen

Switch(config)# SNMP System Information Name Switch

# Chapter 22 RMON configuration

This chapter mainly includes the following contents:

- RMON introduction
- RMON configuration
- RMON configuration example

## 1.83 RMON introduction

RMON (Remote Monitoring) is a standard Monitoring specification, which is mainly used to monitor the data traffic in a network segment or even the whole network. It is one of the widely used network management standards at present. The RMON specification is an extension of SNMP MIB, so it is also an MIB and the most important enhancement to the MIB II standard. RMON enables SNMP to monitor remote devices more effectively and proactively.

The RMON monitoring system has two parts: a detector (agent or monitor) and an administrative station. RMON agents store network information in RMON MIB that is directly embedded into network devices (such as routers, switches, and so on). The management station USES SNMP to obtain RMON data information.

The device supports the four most commonly used groups in RMON:

(1) Statistics group: Provides statistics for each interface, most of which are counters, and records the information collected by the monitor from the interface.

(2) History group: Saves the data sampled at a fixed time interval to the specified interface.

(3) Alarm group: Samples the specified data of all interfaces at a fixed time interval and compares it with the set threshold value, triggering the corresponding event when the conditions are met.

(4) Event group: Set the event, and log or Trap can be selected.

## 1.84 RMON configuration

The RMON command includes four configuration groups, view configuration and view data:

| The command | describe | CLI mode |
|---|---|---|
| Rmon statistics <1-100> (owner WORD\|) | Enables the statistics group configuration with specified ordinals for this port, which is an interactive command. Configuration is where the user is prompted to enter a sequence number and an owner, where the owner is optional (same below). The serial number is the number | Port configuration mode |

| | | |
|---|---|---|
| | of the statistical group configuration, with values ranging from 1 to 100. | |
| No rmon statistics < > 1-100 | Cancels the statistics group configuration that specifies an ordinal number. | Port configuration mode |
| Rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD\|) | This is an interactive command that specifies a history group parameter with an ordinal number for the port configuration. The configuration user can be prompted for a sequence number, number of buckets requested, time interval, and owner. The serial number is the number of the history group configuration, with values ranging from 1 to 100; The number of buckets is the maximum number of pieces of data that can be stored, with values ranging from 1 to 100; The sampling interval is measured in seconds and ranges from 1 to 3600. | Port configuration mode |
| No rmon history < > 1-100 | Cancels a history group configuration that specifies an | Port configuration |

| | | |
|---|---|---|
| | ordinal number. | mode |
| Rmon alarm <1-60> WORD <1-3600> (absolute\|delta) rise-threshold <1-2147483647> <1-60> fall-threshold <1-2147483647> <1-60> (owner WORD\|) | Configure an alarm group parameter with a specified ordinal number, which is an interactive command. The user can be prompted to enter the serial number, monitoring object, time interval, comparison mode, upper limit threshold, upper limit event number, lower limit threshold, lower limit part number and owner. The serial number is the number of the alarm group configuration, with values ranging from 1 to 60. The monitoring object is the OID of a MIB node. The sampling time interval is in seconds and the value range is 1 to 3600. The comparison method can be absolute or delta, respectively representing absolute value (the value of each sample) and relative value (the increment of each sample relative to the last sample). The upper and lower thresholds range from 1 to 2147483647;Events must be | Global configuration mode |

| | | |
|---|---|---|
| | configured ahead of time with Numbers ranging from 1 to 60. | |
| No rmon alarm < 1 > 60 - | Unconfigure an alarm group that specifies an ordinal number. | Global configuration mode |
| Rmon event <1-60> (log\|log-trap WORD\|none\|trap WORD) (description WORD\|) (owner WORD\|) | Configure event group parameters that specify an ordinal number, which is an interactive command. The configuration user can be prompted for a sequence number, event type, common body name, description, and owner. The serial number is the number of the event group configuration, with values ranging from 1 to 60; Event types can be log (logging), log-trap (logging and emitting TRAP), None (no action) and TRAP (emitting trap). When choosing log-trap or TRAP, the common body name must also be specified (common body name configuration in this device is ignored). | Global configuration mode |
| No rmon event < 1 > 60 - | Unconfigure an event group that specifies an ordinal number. | Global configuration |

| | | |
|---|---|---|
| | | mode |
| Show rmon (statistics \| history-control \| alarm \| event) config | View the RMON configuration information, which is an interactive command. Configure users to view objects when prompted for input. | Global configuration mode |
| Show rmon statistics-data interface IFNAME\| | To view the RMON statistics group data, the configuration user must enter the interface name. | Global configuration mode |
| Show rmon history-data interface IFNAME\| | To view the RMON history group data, the configuration user must enter the interface name. | Global configuration mode |

## 1.85 RMON configuration example

Enable the statistics group configuration for port Ge1/1, serial number 10, and owner Tereco.

Enable history group data collection on port Ge1/8, serial number 2, save up to 80 data, sample interval 1 minute, no owner.

Configure events with sequence number 1, log them, and have no owner.

Configure events with sequence number 3, send Trap, share body name public, no owner.

Enable alarm group with serial number 5, monitor the number of bytes received on each port, emit Trap alarm when the number of bytes per half minute is more than 1000,

and log when the number is less than 10. There is no owner.

Switch configuration is as follows:

Switch# configure terminal

The Switch (config) # interface ge1/1

Switch(config-ge1/1)# RMon Statistics 10 Owner Tereco

The Switch (config - ge1/1) # exit

The Switch (config) # interface ge1/8

Switch(config-ge1/8)#rmon History 2 BUCKETS 80 Interval 60

The Switch (config - ge1/8) # exit

1 the log Switch (config) # rmon event

Switch(config)#rmon Event 3 trap Public

Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3 falling threshold 10 1

# Chapter 23 The cluster configuration

Switches provide cluster management capabilities that enable a single device to manage a group of network devices.This chapter describes how to configure cluster management, including the following:

- Cluster Management Introduction
- Configuration management equipment
- Configure member devices
- Cluster management display and maintenance
- Example of a typical cluster management configuration

# 1.86 Cluster Management Introduction

## 1.86.1 The cluster definition

A cluster is a collection of network devices that can be managed as a single device.

Cluster management objective: To solve the problem of centralized management of a large number of scattered network equipment.

Advantages of clustering: saving public IP address; Simplify configuration management tasks. The network manager only needs to configure the public IP address on one switch in the cluster to realize the management and maintenance of other switches in the cluster.

The switches that configure public network IP addresses and perform management functions are command switches, while the others that are managed are member switches, which form a "cluster."

Clusters configure and manage switches within clusters through the following three protocols.

- NDP (Neighbor Discovery Protocol)
- NTDP (Neighbor Topology Discovery Protocol)
- Cluster Management Protocol

The working process of the cluster includes the topology collection and the establishment and maintenance of the cluster. The topology collection process and the cluster maintenance process are relatively independent. The topology collection process starts before the establishment of the cluster.

- All devices use the NDP to get information about their neighbors, including their

software version, host name, MAC address, and port name.

- Management devices use NTDP to collect device information in the user-specified hop range and connection information of each device, and identify cluster candidate devices from the collected topology information.

- The management device completes the operation of adding candidate devices into the cluster and leaving member devices from the cluster according to the information of candidate devices collected by NTDP.

The packets of the cluster are all two-layer Ethernet packets. For the specific format and interaction process, please refer to the national standard "YDT 1692-2007 Ethernet Switch Cluster Management Technical Requirements".

## 1.86.2 The cluster character

According to the different status and functions of each device in the cluster, different roles are formed. Users can specify roles through configuration. All roles are as follows:

1 ) Command switch:

In a cluster, the only switch that can configure and manage the entire cluster is also the only switch in the cluster that has a public network IP address.

- Command switches to create clusters;

- Command switches discover and identify candidate switches by collecting information about Neighbor Discovery Protocol (NDP) and NTDP (Neighbor Topology Discovery Protocol).

- Command switches to control the maintenance of the cluster. Candidate switches can be added to the cluster or member switches can be deleted from the cluster.

- After the cluster is established, the command switch provides the management channel for the cluster.

2 ) Member exchange

Switches managed in a cluster.

Member switches are candidate switches before joining the cluster.

No public IP is set in the member switch;

The management of the member switches is done through the command switch agent.

3 ) Candidate switch

Switches that have the ability to join clusters but have not yet joined any clusters.

Switches must be candidates before they can become member switches.

4 ) Independent switch

Switches that do not have clustering capabilities.

Roles can be changed according to certain rules:

- The user specifies the current candidate as the cluster management device while creating the cluster on the candidate device. Each cluster must specify one (and only one) management device. After the management device is designated, the management device discovers and identifies candidate devices by gathering relevant information. Users can configure to add candidate devices to the cluster.
- Candidates join the cluster and become member devices.
- Member devices in the cluster are restored as candidate devices when they are

deleted.

- Management devices can only be restored as candidate devices if the cluster is deleted.

## 1.86.3 Introduction of NDP

NDP is used to obtain the information of the neighboring devices directly connected, including the connection port, device name, software version and other information. The working principle is as follows:

- The device running the NDP periodically sends NDP messages to its neighbors, which contain NDP information (including the current device's device name, software version, connection port, etc.) and the age of THE NDP information on the receiving device. It also receives but does not forward NDP messages sent by neighboring devices.

- The device running the NDP stores and maintains the NDP neighbor information table, creating a table entry for each neighbor device in the NDP Neighbor Information table. If a new neighbor is discovered and the NDP message is received for the first time, a new entry will be added to the NDP neighbor information table. If the NDP information received from the neighbor device is different from the old information, the corresponding data items in the NDP table will be updated; if the same, only the aging time will be updated; if the NDP information sent by the neighbor has not been received after the aging time, the corresponding neighbor table items will be deleted automatically.

## 1.86.4 NTDP profile

NTDP is used to collect the information of each device and the connection information between devices within a certain network scope. NTDP provides clustering

device information for management devices and collects topology information for devices within a specified hop count.

NDP provides adjacency list information for NTDP. NTDP sends and forwards NTDP topology collection requests according to the adjacency information, and collects THE NDP information of each device within a certain network scope and its connection information with all its neighbors. After collecting this information, the management device or network manager can use this information as needed to complete the required functions. When the NDP on a member device finds a change in its neighbor, it notifies the management device of the change by shaking hands. The management device can start the NTDP for the collection of specified topology, so that the NTDP can reflect the change of network topology in a timely manner.

The management device can perform topology collections within the network on a regular basis, or the user can initiate a topology collection with a manual configuration command. The process of the management equipment to collect topology information is as follows:

- The management device periodically sends NTDP topology collection request packets from ports that enable NTDP functionality.

- The device that receives the request message immediately sends the topology response message to the management device, and copies the request message on the port that enables NTDP function and sends it to the adjacent device; The topology response message contains the basic information of the device and the NDP information of all adjacent devices.

- The adjacent device will perform the same operation after receiving the request message until the topology collection request message has diffused to all devices within the specified hop range.

When topology collection request packets are diffused within the network, a large number of network devices receive topology collection requests and send topology response packets at the same time. In order to avoid network congestion and busy task of management equipment, the following measures can be taken to control the diffusion speed of topology collection request packets:

- Instead of immediately forwarding the topology collection request message after receiving the topology collection request, the device waits a certain amount of time before starting forwarding the topology collection request message on the port enabling NTDP functionality.

- On the same device, except for the first port, each port that enables NTDP function will delay the forwarding of topology collection request message after sending topology collection request message from the previous port.

## 1.86.5 Cluster management and maintenance

1) Candidate devices join the cluster

Before setting up the cluster, users should first specify the management equipment. The management equipment finds and determines the candidate equipment through THE NDP and NTDP protocols and automatically joins the cluster, or manually configures the candidate equipment into the cluster.

After the candidate device joins the cluster successfully, it will get the cluster member serial number and cluster management assigned by the management device

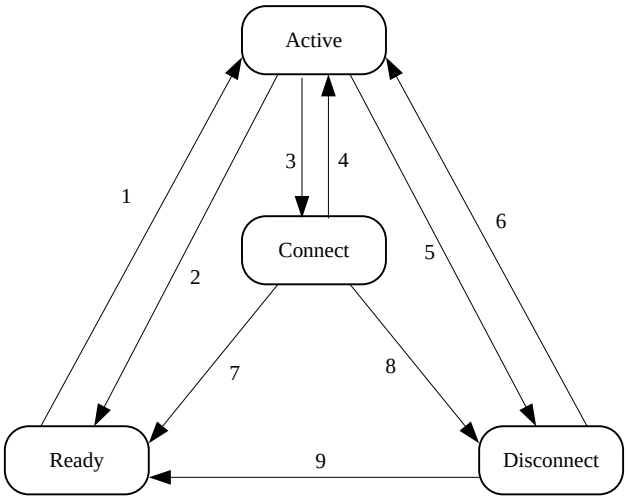
Private IP addresses used, etc.

2) Intra-cluster communication

Within the cluster, the management device and the member device communicate in

~~real time through the handshake message to maintain the communication between them~~

The connection status of the management device and the member device is shown in the figure below.




Member 1 joins member 6 to interrupt recovery and re-register through

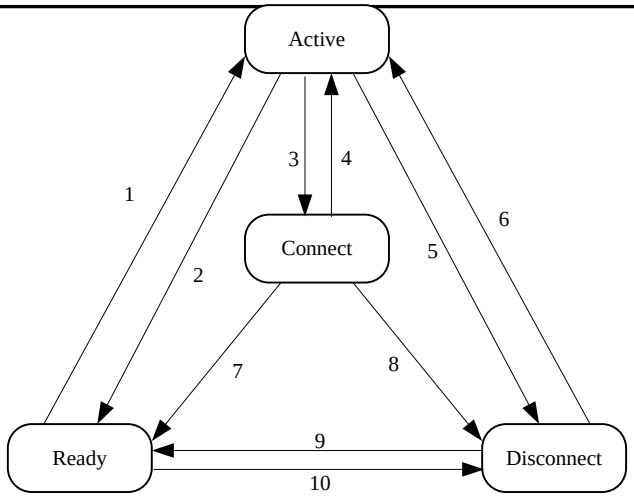
Member deletion 7 Member deletion

3. Three times in a row, no handshake signal is received

4 Received handshake signal 9 member removed

5 Recovery request received

Command switch status migration diagram




1 join cluster 6 interrupt recovery, re-register through

2 Exit cluster 7 Exit cluster

3. Failed to receive the handshake signal for three consecutive times. 8

4 Handshake signal received 9 exit cluster

5 Receive join request 10 configure restore

Member switch state migration diagram

The command switch collects basic information about the device, identifies a device as a candidate switch, and starts in the Ready state.

Deleting a member in any state migrates the state of the member switch back to the Ready state and identifies it as a candidate switch.

- The cluster is established successfully. After the candidate device joins the cluster and becomes a member device, the management device saves the state information of the member device locally and identifies the state of the member device as Active. The member device also saves its own state information locally and identifies its state as Active.

- Management devices and member devices regularly send handshake messages to each other. After receiving the handshake message from the member device, the management device does not make a reply and keeps the member device in the Active state. The member device also does not respond, leaving its state as Active.

- If the management device does not receive the handshake message sent by the member device within three times of the time interval after sending the handshake message to the member device, the state of the member device saved locally will be transferred from Active to Connect. Similarly, if a member device does not receive a handshake message from the management device within three times of sending the handshake message to the management device, its own state will also be migrated from Active to Connect.

- If the management device receives the handshake or management message sent by the member device in Connect within the valid retention time, the state of the member device will be migrated back to Active. Otherwise, it will be migrated to Disconnect, and the management device will consider the member disconnected. If a member device in Connect receives handshake or management packets from the management device within the valid retention time, it will migrate its state to Active, or it will migrate to Disconnect.

- When the disconnected communication between the management device and the member device resumes, the member device in Disconnect will rejoin the cluster, and after completion of the Disconnect, the member device's state in the management device as well as in the local area will revert to Active.

If a topology change is found, the member device also passes the change information to the management device through a handshake message.

### 1.86.6 The management vlan

The management VLAN limits the scope of cluster management. Through configuration management VLAN, the following functions can be achieved:

- Cluster management packets (including NDP, NTDP, and handshake packets) are restricted to the management VLAN, isolated from other packets, increasing security.

- Management devices and member devices communicate internally by managing the VLAN.

Cluster management requires management devices to be connected to member/candidate ports, including cascade ports (when candidate devices are connected to management devices through another candidate device, the ports between candidate devices are called cascade ports) to allow the management VLAN to pass, therefore:

- If the port does not allow the administrative VLAN to pass, then the device to which the port is connected cannot join the cluster, so before the cluster you should determine which ports the candidate device is connected to the administrative device, including cascading ports that allow the administrative VLAN to pass.

- Messages in a CONFIGURATION management VLAN are allowed to pass without a label only if the port to which the management device is connected to a member/candidate device and the default VLAN ID of the cascade port is a management VLAN. Otherwise, messages in the management VLAN must pass with a label.

For knowledge of VLANs, see "Configuring a VLAN."

## 1.87 Cluster configuration Introduction

Before users configure the cluster, the roles and functions of each device in the

cluster should be clearly defined. In addition, related functions should be configured to make communication planning with internal devices in the cluster.

| Configuration tasks | |
|---|---|
| Configuration management equipment | Enable NDP functionality for systems and ports |
| | Configure the NDP parameters |
| | Enable NTDP functionality for systems and ports |
| | Configure NTDP parameters |
| | Configure to collect NTDP information manually |
| | Enable clustering functionality |
| | Set up the cluster |
| | Configure cluster internal member interactions |
| | Configure cluster member management |
| Configure member | Enable NDP functionality for |

| | |
|---|---|
| devices | systems and ports |
| | Enable NTDP functionality for systems and ports |
| | Configure to collect NTDP information manually |
| | Enable clustering functionality |
| Configure cluster members to access each other | |
| | |
| | |

*Note:*

*When the NDP or NTDP function is turned off on the management device and member device after the cluster is established, the cluster will not be dissolved, but the normal operation of the established cluster will be affected.*

## 1.88 Configuration management equipment

### 1.88.1 Enable NDP functionality for systems and ports

| The command | describe | CLI mode |
|---|---|---|
| NDP global enable | Enable global NDP functionality.Global is closed by default. | Configuration mode |
| NDP enable | Enable port NDP functionality. NDP is closed by default for all ports | Interface configuration mode |

*Note:*

- *The NDP must have both global and port NDP capabilities enabled for the NDP to function properly.*
- *The NDP feature does not support aggregation ports.*
- *To avoid managing devices that collect topology information during topology collection and add it to the cluster, it is recommended that NDP functionality be turned off on ports connected to devices that do not need to join the cluster.*

## 1.88.2 Configure the NDP parameters

| The command | describe | CLI mode |
|---|---|---|
| NDP aging - timer < aging - time > | Configure the aging time of THE NDP message sent by the device on the receiving device. Default is 180 seconds. | Configuration mode |

| | | |
|---|---|---|
| NDP hello - timer < hello - time > | Configure the time interval for NDP message sending. The default is 60 seconds. | Configuration mode |

*Pay attention to*

*The aging time of NDP message on the receiving device generally cannot be less than the NDP sending time interval, otherwise it will cause the instability of NDP port neighbor information table.*

## 1.88.3 Enable NTDP functionality for systems and interfaces

| The command | describe | CLI mode |
|---|---|---|
| NTDP global enable | Enable global NTDP functionality.Global is closed by default. | Configuration mode |
| NTDP enable | Enable NTDP functionality for ports. NDP is closed by default for all ports | Interface configuration mode |

*Note:*

- *NTDP must have both global and port capabilities enabled in order for it to work properly.*
- *The NTDP feature does not support aggregation ports.*
- *To avoid management devices gathering topology information on devices that do not need to join the cluster during topology collection and adding it to the cluster, it is*

*recommended that NTDP functionality be turned off on ports connected to devices that do not need to join the cluster.*

## 1.88.4 Configure NTDP parameters

| The command | describe | CLI mode |
|---|---|---|
| NTDP hop < value > hop - | Configure the scope of the topology collection.By default, the farthest device in the collected topology has a maximum number of hops from the topology collection device of 3. | Configuration mode |
| NTDP timer < interval - time > | Configure the time interval for the timed topology collection. The default is 1 minute. | Configuration mode |
| NTDP timer hop - delay < time > | Configure the time the collected device waits before the first port forwarding topology collects the request message. Default is 200 milliseconds. | Configuration mode |
| NTDP timer port - delay < time > | Configure the port latency for the current device forwarding topology collection request. Default is 20 milliseconds. | Configuration mode |

## 1.88.5 Configure to collect NTDP information manually

After the cluster is established, the management device periodically collects topology information. In addition, users can initiate an NTDP information collection process by manually collecting NTDP information at any time through configuration (whether or not a cluster is established), thus enabling more effective real-time management and monitoring of devices.

| The command | describe | CLI mode |
|---|---|---|
| NTDP explore | Collect topology information manually once. | Normal mode, privileged mode |

## 1.88.6 Enable clustering functionality

| The command | describe | CLI mode |
|---|---|---|
| Cluster enable | Enable clustering functionality. The default cluster function is turned off. | Configuration mode |

## 1.88.7 Set up the cluster

The management VLAN limits the scope of cluster management. Through configuration management VLAN, the following functions can be achieved:

- Cluster management packets (including NDP, NTDP, and handshake packets) are restricted to the management VLAN, isolated from other packets, increasing security.

- Management devices and member devices communicate internally by managing the VLAN.

| The command | describe | CLI mode |
| --- | --- | --- |
| Cluster management - vlan < vlan - id > | Specify the administrative VLAN.The default administrative VLAN is VLAN1. | Configuration mode |

***Note:***

*If the current device is in the cluster, it is not allowed to modify the management VLAN.*

*Not in the cluster:*

*1 ) Check whether the VLAN exists, there is no direct failure, continue to the next step*

*2 ) Re-check all the interfaces. If the vLAN of the interface is not the same vLAN as the management VLAN, turn off the global switch of NDP and NTDP and do the corresponding operation of closing and clearing, then reopen.*

*3 ) Find the three-layer interface to configure THE VLAN. If it is not found, create a new three-layer interface corresponding to the VLAN. If the new interface fails, manage vLAN configuration successfully, NDP and NTDP can be used, but*

*cannot join the cluster.*

*4 ) Set the MAC of the current three-tier interface to dev_ID. If the VLAN setting is successful and the new three-tier interface fails, use the MAC of VLAN1 as dev_ID*

*If the management VLAN is configured, but the user directly deletes the VLAN in the VLAN Database, the management VLAN is automatically set to VLAN1, and the NDP, NTDP and cluster global switches are turned off and the corresponding shutdown and cleanup operation is made.*

In front of the building cluster, the user must first set up the cluster members in equipment use private IP address range, when the device candidates to join and management device dynamically allocated a can be used within a cluster of private IP addresses, and send to the candidate equipment, used for internal cluster communication, in order to realize the management of the members of the equipment maintenance and management.

| The command | describe | CLI mode |
|---|---|---|
| Cluster IP - pool < IP/MASK > | Configure the range of private IP addresses used by member devices in the cluster on the devices you want to set up as management devices. | Configuration mode |

***Note:***

- *The IP address and cluster address pool for the VLAN interface of the management*

*device and the member device cannot be configured in the same network segment, otherwise the cluster will not work properly.*

- *Only when the device is not in the cluster can it be configured.*
- *Use the management VLAN to find whether there is a corresponding three-layer port, if there is no three-layer port, directly return failure. If there is a three-tier interface, configure the base address of IP-Pool to the three-tier interface. If the configuration fails, the IP-Pool will also be configured to fail.*

By default, the devices are not management devices and the cluster is set up:

| The command | describe | CLI mode |
|---|---|---|
| Cluster build < name > | Manually set up the cluster, configure the current device as the management device, and assign a cluster name. | Configuration mode |
| Cluster auto - build < name > | Automatically set up the cluster.<br>The automatic clustering feature automatically adds any candidate devices found within the specified hop range to the created cluster. | Configuration mode |
| Cluster delete < name > | Remove the cluster. | Configuration mode |
| Cluster stop auto - add member | Automatically set up cluster configuration, stop automatically join the member switch. This operation can only stop | Configuration mode |

| | | |
|---|---|---|
| | adding new devices, and devices that are already in the cluster will remain in the cluster. | |

*Note:*

- *The user can only specify the management VLAN before setting up the cluster. After the device has joined the cluster, the user cannot modify the management VLAN.If you need to change the management VLAN after the cluster is established, you need to delete the cluster on the management device, reassign the management VLAN, and finally re-establish the cluster.*
- *For security reasons, it is recommended not to configure the administrative VLAN to be the default VLAN ID for managing the ports that the device connects to its member devices and for cascading ports.*
- *Only when all members of the management equipment and equipment connected to port and default VLAN ID is the management of the cascade port VLAN, can allow management VLAN message without a label, otherwise, you must configure management equipment, members connected port and allow all the cascade port management VLAN labeled by message, refer to the specific configuration VLAN.*
- *Configuration of the private IP address range for member devices in the cluster can only be done if the cluster has not yet been established, and only on management devices.If the cluster is already established, the IP address range is not allowed to be modified.*

## 1.88.8 Configure cluster internal member interactions

Within the cluster, the management device and the member device conduct real-time communication through handshake message to maintain the connection state between them. The time interval of handshake message sending and effective retention time of the

device can be configured on the management device. This configuration will take effect for all member devices within the cluster.

| The command | describe | CLI mode |
|---|---|---|
| Cluster timer < interval - time > | Configure the time interval for handshake packets to be sent.The default is 10 seconds. | Configuration mode |
| Cluster holdtime < hold - time > | Configure the effective retention time of the device. 60 seconds by default | Configuration mode |

## 1.88.9 Configure cluster member management

Users can manually specify candidates to join the cluster on the management device or manually delete the cluster

The specified member device. The join/delete of cluster members must be done on the management device or an error will be returned

False prompt message.

| The command | describe | CLI mode |
|---|---|---|
| Cluster add member mac-address <mac-address> | Add candidate devices to the cluster. | Configuration mode |
| Cluster delete member mac-address <mac-address> | Remove member devices from the cluster. | Configuration mode |

## 1.89 Configure member devices

### 1.89.1 Enable NDP functionality for systems and ports

See Enabling systems and ports for NDP functionality

### 1.89.2 Enable NTDP functionality for systems and ports

See Enabling systems and ports for NTDP functionality

### 1.89.3 Configure to collect NTDP information manually

See Configuring to collect NTDP information manually

### 1.89.4 Enable clustering functionality

See Enabling clustering capabilities

## 1.90 Configure access to cluster members

After the NDP, NTDP and cluster functions are properly configured, the member devices in the cluster can be configured, managed and monitored through the management devices. The member device can be configured on the management device by switching to the specified member device interface.

| The command | describe | CLI mode |
|---|---|---|

| | | |
|---|---|---|
| ~~Cluster switch - to member <~~ member - number > | ~~Switch from the~~ management device interface to the member device interface. | ~~Normal mode~~, privileged mode |

*Note:*

*Telnet connection is used to switch between cluster management devices and member devices, which requires notes*

*Meaning:*

- *执行切换前，对端设备需要执行"telnet server enable"命令使能telnet功能，否则将导致切换失败。*
- *从管理设备切换到成员设备，如果成员号n不存在，将显示出错信息*

*If the Telnet user on the requested device is full, the switch will fail.*

## 1.91 Cluster management display and maintenance

| The command | describe | CLI mode |
|---|---|---|
| Show NDP [interface < ifname >] | Displays NDP configuration information | Normal mode, privileged mode |
| Reset NDP statistics [interface <ifname>] | Clear NDP statistics | The configuration view |
| Show NTDP | Displays system NTDP information | Normal mode, privileged mode |
| Show NTDP device - the list | Displays device information collected by NTDP | Normal mode, privileged mode |
| Show NTDP single-device mac-address <mac-address> | Displays NTDP details for the specified device | Normal mode, privileged mode |

| | | |
|---|---|---|
| Show the cluster | Displays the status and statistics of the cluster to which the device belongs | Normal mode, privileged mode |
| Show cluster topology | Displays cluster topology information | Normal mode, privileged mode |
| Show cluster candidates [mac-address <mac-address>] | Displays candidate device information | Normal mode, privileged mode |
| Show cluster members [<member-number>] | Displays cluster member information. | Normal mode, privileged mode |

## 1.92 Example of a typical cluster management configuration

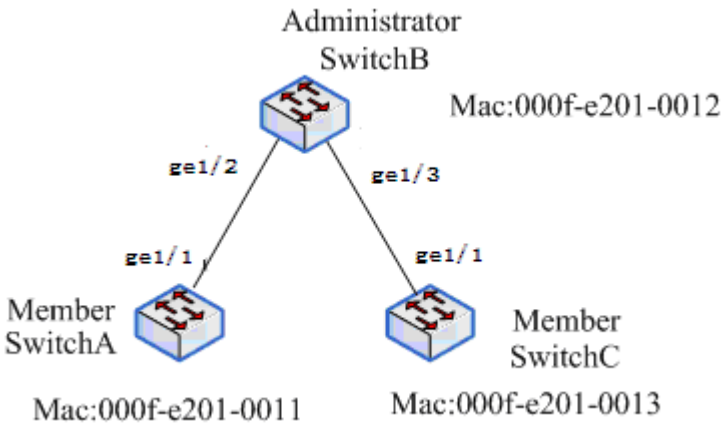
1. Networking requirements:

Cluster ABC consists of three switches and its management VLAN is VLAN 10. Where, Switch B is the management device

(Administrator); Switch A and Switch C are Member devices.

The base IP of the entire cluster address pool is 10.0.0.1, supporting 8 devices.

2. Networking diagram:



3. Configuration Steps:

Configure the member device SwitchA

Configuration management VLAN.

[SwitchA] cluster management - vlan 10

[SwitchA] interface ge1/1

Switch access VLAN 10

Enable global NDP functionality and NDP functionality on port Ge1/1.

[SwitchA] NDP global enable

[SwitchA] interface ge1/1

SwitchA - ge1/1 NDP enable

Enable global NTDP functionality and NTDP functionality on port Ge1/1.

[SwitchA] NTDP global enable

[SwitchA] interface ge1/1

SwitchA - ge1/1 NTDP enable

Enable clustering functionality.

[SwitchA] cluster enable

Configure the member device SwitchC

Since the configuration of the member devices is the same, the configuration on Switch C is similar to that of Switch A, with the configuration process omitted.

The configuration management device SwitchB

Configuration management VLAN.

[SwitchB] cluster management - vlan 10

[SwitchB] interface ge1/2

Switch b - GE1/2] Switch Access VLAN 10

[SwitchB] interface ge1/3

Switch b - GE1/3] Switch Access VLAN 10

Enable global NDP and NTDP functions and enable NDP and NTDP functions on ports GE1/2 and GE1/3, respectively.

[SwitchB] NDP global enable

[SwitchB] NTDP global enable

[SwitchB] interface ge1/1

[SwitchB ge1/2] NDP enable

[SwitchB ge1/2] NTDP enable

[SwitchB] interface ge1/3

[SwitchB ge1/3] NDP enable

[SwitchB ge1/3] NTDP enable

The aging time of THE NDP message sent by this device on the receiving device is 200 seconds.

[SwitchB] NDP Timer Aging 200

Configure NDP messages to be sent at an interval of 70 seconds.

NDP Timer Hello 70

The maximum number of hops collected by the configuration topology is 2 hops.

[SwitchB] NTDP hop 2

Configure the first port of the collected device to forward topology collection request message with a delay time of 150ms.

[SwitchB] NTDP Timer Hop-delay 150

The delay time for forwarding topology collection request packets to other ports of the collected device is 15ms.

[SwitchB] NTDP Timer port-delay 15

The time interval for the configuration topology collection is 3 minutes.

[SwitchB] NTDP timer 3

Enable clustering functionality.

[SwitchB] cluster enable

# Configure member devices with private IP addresses ranging from 10.0.0.1 to 10.0.0.9.

[SwitchB] Cluster IP-Pool 10.0.0.1 8

# Configure the current device as a management device and set up a cluster named ABC, with members automatically joining the cluster.

[SwitchB] cluster autobuild ABC

When you have added all the switches you want to add, you can turn off the automatic clustering feature

[SwitchB] cluster stop auto - add member

# Chapter 24 SNTP configuration

This chapter mainly includes the following contents:

- introduce
- Configuration SNTP
- According to SNTP

## 1.93 SNTP is introduced

At present, Network Time Protocol (NTP) is widely used to realize Network Time synchronization on the Internet. Another Protocol is a simplified version of NTP, namely Simple Network Time Protocol (SNTP).

NTP protocol can span a variety of platforms and operating systems, using very precise algorithms, so almost not affected by network delay and jitter, can provide 1-50ms accuracy.

SNTP(Simple Network Time Protocol) is a simplified version of NTP. In the

implementation, a simple algorithm is used to calculate the time and the performance is relatively high.

Since SNTP messages and NTP messages are completely consistent, the SNTP Client implemented by this switch is fully compatible with NTP Server

## 1.94 Configuration SNTP

### 1.94.1 Default SNTP Settings

| project | The default value |
|---|---|
| SNTP state | Disable disabling the SNTP service |
| The NTP Server | There is no |
| The interval of SNTP synchronization time | 1800 seconds |
| The local time zone | Plus eight, east Eight |

Turn SNTP on and off

The configuration is as follows:

Switch# configure terminal

Enter global configuration mode

The Switch (config) # SNTP enable

Open the SNTP

The Switch (config) # SNTP disable

Close the SNTP

## 1.94.2 Configure the SNTP Server address

Since SNTP message and NTP message are identical, SNTP Client is fully compatible with NTP Server. There are many NTP servers on the network, so you can choose one with less network delay as the NTP Server on the switch.

Specific the NTP server address can log on to http://www.time.edu.cn/ or http://www.ntp.org/.

Such as 192.43.244.18 (time. Nist. Gov)

The switch can be configured with a maximum of three Server addresses. The switch USES the first Server address to synchronize the time. If the synchronization fails, the switch USES the second Server address, and so on.

Add a Server address configuration as follows:

Switch# configure terminal

Enter global configuration mode

The Switch # SNTP server 210.72.145.44 (config)

Add SNTP Server IP. If the switch already has three Server addresses, it will fail to add, so it needs to delete the address before adding

The configuration for deleting the Server address is as follows:

The Switch (config) # no SNTP server

Delete all Server addresses

Switch(config)# no SNTP Server 210.72.145.44

Delete a Server address

## 1.94.3 Configure the interval for the SNTP synchronization clock

The SNTP Client needs a timed sync clock with the NTP Server so that the timing is more positive.

The configuration is as follows:

Switch# configure terminal

The Switch (config) # SNTP interval 60

Set the timing and synchronization clock interval in seconds, ranging from 60 seconds to 65535 seconds. The default is 1800 seconds, which is set to 60 seconds here

The Switch (config) # no SNTP interval

The interval of the timing sync clock is restored to the default of 1800 seconds

## 1.94.4 Configure the local time zone

The time acquired through SNTP protocol is Greenwich Mean Time (GMT). In order to prepare the local time, the local area needs to be set to adjust the standard time. The default setting of the switch is zone 8, which is also the time zone of China.

The configuration is as follows:

Switch# configure terminal

The Switch (config) # SNTP time zone - 8

Set the local time zone to W8

The Switch (config) # no SNTP time zone

The local time zone is restored to E8

## 1.95 SNTP information display

The configuration is as follows:

Switch# show SNTP

Switch# show running - config

# Chapter 25
# Configure RIP

This chapter mainly includes the following contents:

- RIP is introduced
- RIP configuration
- RIP configuration example

## 1.96 RIP is introduced

RIP (Routing Information Protocol) is a dynamic Routing Protocol developed earlier. It USES distance vector algorithm and is widely used in small networks. RIP packets are encapsulated in UDP packets, using UDP port 520. The main idea of RIP is to use hop to measure the distance to the host machine, and increase the number of hops per router by 1, so as to calculate the routing weight and select the route. The RIP convention has a maximum number of hops of 15, and the number of hops of 16 is marked as network unreachable. RIP USES broadcasting the entire routing table to network router in the synchronization of routing information, updated once every 30 seconds time message, if one of the routing entry in 180 seconds not received the update message from neighbors, it is marked as unreachable, if another 120 seconds effectively update has not yet received, will this by deleting.

RIP is easy to implement because of its simple idea, but also brings about the corresponding routing loop problem, in order to prevent the routing loop, RIP introduced a horizontal partition mechanism to avoid spoofing between routers. Horizontal segmentation means that routing updates are not published from the received interface. A horizontal partition with toxic inversion publishes routing updates from the received interface, but with weights marked as unreachable, allowing neighbor routers to quickly identify the loop without waiting for weights to increase to unreachable.

The routing entries in the routing table should contain the destination address (host or network) next-hop address, forwarding interface, routing weights, and a timer (the timer is reset when a routing update is received) routing markers.

When THE RIP is started, a full list request message is immediately sent in the form of broadcast (RIP-1) or multicast (RIP-2). When the neighboring router receives the

request message, it will send back its complete route list in response to the message. When the router receives the response message, it will process the route one by one and modify its routing table. When there is a new routing, a trigger update message will be generated immediately. After a series of updates, RIP convergence finally occurred, and each router in the network kept the latest and consistent routing information. After the network is stable, RIP still broadcasts the local routing table to the neighbors every 30 seconds, and each router maintains its routing information according to the received routing update message and makes the optimal route. RIP USES a timeout mechanism to handle unupdated routing entries to ensure that routing is correct in real time.

RIP is used in the campus network and simple structure of the more continuous regional network, complex large network RIP is not suitable.

## 1.97 RIP configuration

After starting the RIP protocol, the configuration of each function and attribute of RIP can be carried out. RIP configuration in the RIP configuration mode and interface configuration mode.

Configuration of RIP includes:

- Start RIP and enter RIP configuration mode
- Enabled RIP interface
- Distribution list broadcast text transmission
- Configure the working state of the interface
- Configure the default routing weight

- Configuration management distance
- Configuration timer
- Configure version
- Introduce external routing
- Configure routing filtering
- Configure additional routing weights
- Configure the RIP version of the interface
- Configure the transceiver state of the interface
- Configure horizontal segmentation
- Message authentication
- Configure interface weights

## 1.97.1 Start RIP and enter RIP configuration mode

Pattern: Global configuration pattern

Command: Router RIP

Start RIP and enter RIP configuration mode

Command: No Router RIP

Rip off

Default: RIP is not run

## 1.97.2 Enabled RIP interface

When RIP works, some interfaces can be specified, and the network where it is configured as RIP network, RIP protocol packets can be sent and received on it.

Mode: RIP configuration mode

Command: network <network-address>

Enabled RIP interface

Command: no network <network-address>

Close the RIP interface

Parameters: there are two forms: A.B.C.D/M and A.B.C.D. The former specifies the network IP and mask length, and the latter specifies the network IP and mask length.

Default: RIP is disabled on all interfaces after starting

After the RIP protocol is started, it must specify the network segment it works on. RIP can only run on the interface of the specified network segment. For those interfaces that are not in the specified network segment, RIP neither receives the sending route nor forwards the interface route. In the VIEW of RIP, interfaces that are not in the specified segment do not exist. The parameter net-address can be configured as the interface IP address for enabled or disabled network addresses. The network command enables the interface of a segment of the network at that address. For example, the IP address of an interface is 192.160.1.1, the command network 192.160.1.1/24 is used, and the command

Show run-config is used to see network 192.160.1.0/24.

## 1.97.3 Distribution list broadcast text transmission

Version 1 of THE RIP protocol USES broadcast switched messages and version 2 USES multicast (224.0.0.9) to exchange messages. When running RIP protocol on a link that does not support broadcast, a specific unicast address needs to be specified to exchange messages.

Mode: RIP configuration mode

The command: neighbor <ip-address>

Configure the opposite unicast IP address

The command: no neighbor <ip-address>

Unset the end unicast IP address

Parameter: IP-Address is the unicast IP address specified

Default: RIP does not send packets to any unicast address

## 1.97.4 Configure the working state of the interface

The RIP protocol, which runs on some networks, may only require RIP interface routing and do not want to broadcast RIP routing on that interface. The network command can be used to specify that RIP packets are sent and received on the interface and the route of the interface can be known. Using the passive-Interface command only knows the

interface route and blocks its broadcast.

Mode: RIP configuration mode

Command: passive-interface <if-name>

Configure the interface in a passive state

Command: no passive-interface <if-name>

Cancel the interface passive state

Parameter: IF-name is the agreed three layer interface name (for example: vlan1 vlan2...)

Default: Enabled RIP interfaces are not passive

## 1.97.5 Configure the default routing weight

When external routing is introduced, a routing weight needs to be specified. This default routing weight is used when its routing weight is not specified.

Mode: RIP configuration mode

Default-metric <metric>

Sets the default routing weight when external routing is introduced

No default-metric [metric]

The default routing weight is 1 when external routing is introduced

Parameter: Metric was between 1 and 16, greater than 1 and less than 16.

The default: metric value is 1, which is recovered using the no default-metric command.

## 1.97.6 Configuration management distance

Each protocol has a agreed priority, and distance management is the priority at which a route is selected when using a routing policy. When there are two identical routes to the same destination (from different routing protocols), the smaller the administrative distance, the preferred route is selected for that protocol.

Mode: RIP configuration mode

Command: distance <distance>

Sets the administrative distance value

No distance [distance]

The recovery management distance is the default

Parameter: Distance is between 1 and 255

Default: The value of distance is 120. Use the no Distance command to restore the default value.

## 1.97.7 Configuration timer

RIP protocol has three timers. One is that the complete routing table is broadcast to all RIP interfaces every 30 seconds. The other is that every route in the RIP routing table receives no update in 180 seconds and the metric is 16.

Mode: RIP configuration mode

Command: timbasic <update> <timeout> <garbage>

Set three timer values

Mandate: No Timbasic

The recovery timer is the default

Parameter: the first parameter update is the timing update timer of the entire RIP routing table, the second parameter TIMEOUT is the timer not updated for each routing timeout, and the third parameter Garbage is the timer deleted after each routing timeout marked as invalid. The value range of the three timers is 5~$(2)^{31}$1).

Default: Update is updated every 30 seconds; Timeout for 180 seconds is marked as invalid; Garbage is removed for 120 seconds.

## 1.97.8 Configure version

RIP currently has version 1 (RFC1058) and version 2 (RFC2453). The configured version value will be reflected in the version field of the protocol message.

Mode: RIP configuration mode

Command: version <version>

Set RIP to version 1 or version 2

No version [version]

Restore the RIP version as the default

Parameter: Version can take the value 1 or 2

Default: Version 2

## 1.97.9 Introduce external routing

RIP allows users to introduce routing information from other protocols into the ROUTING table of RIP. The types of routing protocols introduced by RIP include: Connected, static, OSPF, IS-IS, and BGP.

Mode: RIP configuration mode

Command: redistribute {kernel | static | ospf | ISIS | BGP} [metric <metric> | route-map <route-map-name>]

Introduce additional protocol routing

No redistribute {kernel | static | ospf | ISIS | BGP} [metric <metric> | route-map <route-map-name>] Cancel the incoming route

Parameters: The first parameter is the name of other protocols introduced, which can be directly connected, static, OSPF, IS-IS, BGP; The second parameter is the weight set at the time of introduction, which is between 1 and 16. The third parameter is the name of the referenced Route-map. Route-map is configured in global configuration mode, as shown in the command manual.

Default: RIP does not introduce any external protocols

## 1.97.10 Configure routing filtering

RIP provides routing filtering function, through the specified access control list and address prefix list, docking route received and published route, configuration policy rules for filtering.

Mode: RIP configuration mode

Distribute -list <acl-name> {in | out} [if-name]

Use access-List to filter the input and output of the interface

No cenot-list <acl-name> {in | out} [if-name]

Unfilter with Access-List

Parameter: ACL-name represents the name of the referenced Access-List; If-name represents the RIP interface applied to; In and out indicate the direction in which the route is received or published.

Command: placard-list prefix <pre-name> {in | out} [if-name]

Use the prefix- List filter

No place-list prefix <pre-name> {in | out} [if-name]

Unprefix - List filtering

Parameter: pre-name means the name of the referenced prefix-list; If-name represents the RIP interface applied to; In and out indicate the direction in which the route is received or published.

Default: RIP does not filter any receiving and sending routes

Access-list and Prefix - List are configured in global configuration mode and are available in the command manual.

## 1.97.11 Configure additional routing weights

The additional routing weight is an offset value added to the RIP protocol routing weight at the time of input and output. It does not directly change the routing weight in the routing table, but adds an offset value when the interface receives the sending route.

Mode: RIP configuration mode

Offset -list <acl-name> {in | out} <offset> [if-name]

Add an offset to the weight of the interface I/O route using the Access-List

Command: no offset-list <acl-name> {in | out} <offset> [if-name]

Cancel the offset of the weight of the input/output route

Parameter: ACL-name represents the name of the referenced Access-List; In and out mean apply in or out; Offset represents the value of offset, which is between 0 and 16.

If-name represents the RIP interface applied to.

Default: the additional weight of each route is 1 when the message is received and 0 when the message is sent.

## 1.97.12 Configure the RIP version of the interface

There are two versions of RIP, RIP-1 and RIP-2, which can specify the VERSION of RIP message processed by the enabled RIP protocol interface. The receiving direction can be distinguished as receiving riP-1 only or RIP-2 only, i.e., receiving both RIP-1 and RIP-2. In terms of sending direction, it can be divided into those sending RIP-1, those sending RIP-2 (in broadcast mode) and those sending RIP-2 (in multicast mode), which send both RIP-1 and RIP-2.Rip-2 has two ways of sending messages: broadcast and multicast. Using multicast can not only avoid the host running RIP in the same network not receiving the broadcast message of RIP, but also avoid the host running RIP-1 to deal with the ROUTE with subnet mask of RIP-2.

Pattern: Interface configuration pattern

IP rip receive version {1 | 2}

Set the interface to receive version 1 or version 2 messages only

Parameters: version 1 or version 2

IP rip receive version {1 2 | 2 1}

Set the interface to receive both Version 1 and version 2 messages

Parameter: can be written as 1, 2 or 2, 1

No IP rip receive version [1 | 2 | 1 2 | 2 1]

The recovery interface receives messages set to default

Default: version 2 multicast mode

IP rip send version {1 | 2 | 1-compatible}

Set the interface to send version 1 messages only or version 2 messages only

Parameters: version 1 or version 2; The 1-Compatible interface of Version 2 sends version 1-compatible messages, which are broadcast rather than multicast.

Command: IP rip send version {1 2 | 2 1}

Set the interface to send both Version 1 and version 2 messages

Parameter: can be written as 1, 2 or 2, 1

No IP rip send version [1 | 2 | 1-compatible | 1 2 | 2]

Restore interface send message set to default

Default: version 2 multicast mode

## 1.97.13 Configure the transceiver state of the interface

After using the network command to enable the RIP interface in THE RIP mode, it can also specify the state of its transceiver protocol message in the interface mode, whether to receive protocol message or whether to send protocol message.

Pattern: Interface configuration pattern

Command: IP RIP Receive -packet

Configure the interface to receive protocol messages

Command: No IP Rip Receive -packet

The configuration interface does not receive protocol messages

Command: IP RIP send-packet

Configure the interface to send protocol messages

Command: no IP RIP send-packet

The configuration interface does not send protocol packets

Default: enables receiving and sending protocol messages

Note the difference. The network command starts a network to run the RIP protocol, and the interface in the network to send and receive protocol message, the interface route is included in the routing table. The passive-interface command makes the interface not send or receive protocol packets after the network command takes effect, but the interface route is still included in the routing table. IP RIP Receive-packet and IP RIP Send-Packet also specify whether the interface receives or sends protocol packets after the network command takes effect.

## 1.97.14 Configure horizontal segmentation

Horizontal segmentation means that the route received from this interface is not

emitted from this interface. Horizontal segmentation with toxic inversion means that the route received from the interface is still emitted from the interface, but its metric value is marked as 16. Horizontal segmentation can avoid the generation of loop to a certain extent. The horizontal segmentation with toxicity reversal is more efficient than normal horizontal segmentation, and the direct labeling is unreachable. However, horizontal partitioning needs to be prohibited on THE NBMA network to obtain the correct routing.

Pattern: Interface configuration pattern

IP rip split-Horizon [poisoned]

Initiate interface horizontal segmentation function or with toxicity reversal

Command: No IP rip split-Horizon

Disable horizontal partitioning of interfaces

Parameters: Poisoned means normal level segmentation, poisoned means poisoned.

Default: Horizontal segmentation with toxicity reversal

## 1.97.15 Message authentication

Rip-1 does not support message authentication. Rip-2 supports message authentication. There are two authentication methods, plaintext authentication and MD5 authentication. The unencrypted authentication data in plaintext authentication is transmitted together with the message, which cannot provide security guarantee and cannot be applied to the network with higher security requirements. The setting of password can be divided into two types: common key and key chain. The common key

holds an independent string, and the key chain manages the key's ID, content, lifetime of receiving and lifetime of sending. See the command reference manual for key chain management.

Pattern: Interface configuration pattern

IP rip authentication mode {text | md5}

Set the authentication mode to plaintext or MD5

Command: no IP rip authentication mode [text | md5]

Cancel the certification

Parameters: Text for clear text authentication, MD5 authentication.

Default: No authentication

Command: IP rip authentication string <password>

Set the authenticated password string

Command: No IP RIP Authentication String [password]

A decertification password string

Parameter: 16-byte authentication password

Command: IP rip authentication key-chain <key-chain-name>

Set the authentication key-chain

Command: No IP rip authentication key-chain [key-chain-name] to de-authenticate the key-chain

Parameter: the name of the key-chain referenced; Key-chain is configured in global configuration mode, see the command manual.

## 1.97.16 Configure interface weights

Pattern: Interface configuration pattern

Command: IP rip metric <metric>

Configure interface weights

Command: no IP RIP metric

The restore interface weight is the default

Parameter: The metric value is between 1-16, which represents the weight to be added to the routing entry learned by the interface.

Default: 1

## 1.97.17 According to the information

Pattern: Normal or privileged pattern

Command: Show IP Protocols

Displays information about all running protocols

Command: Show IP Protocols RIP

Displays THE RIP protocol information

Command: Show IP RIP

Show RIP routing

Command: Show IP RIP Database

Display the RIP database

Command: Show IP RIP Database Count

Displays the number of RIP database entries

Command: Show IP RIP Interface [IF-name]

Displays the RIP interface information

Parameter: IF-name is the agreed three-tier interface name

Pattern: Privileged pattern

Command: Show running-config

Displays the current configuration of the switch, including RIP configuration.

Command: Show running-config rip

Displays the current configuration of RIP.

## 1.98 RIP configuration example

**(1) configuration**

The three switches are connected in pairs, with 6 network segments respectively. The RIP protocol is enabled in all of them, so that the three PCS can be interoperable in pairs.

On switch 1:

Switch# configure terminal

The Switch (config) # router rip

The Switch (config - rip) # network 192.168.1.0/24

The Switch (config - rip) # network 10.1.1.0/24

The Switch (config - rip) # network 10.1.2.0/24

On switch 2:

Switch# configure terminal

The Switch (config) # router rip

The Switch (config - rip) # network 192.168.2.0/24

The Switch (config - rip) # network 10.1.2.0/24

The Switch (config - rip) # network 10.1.3.0/24

On switch 3:

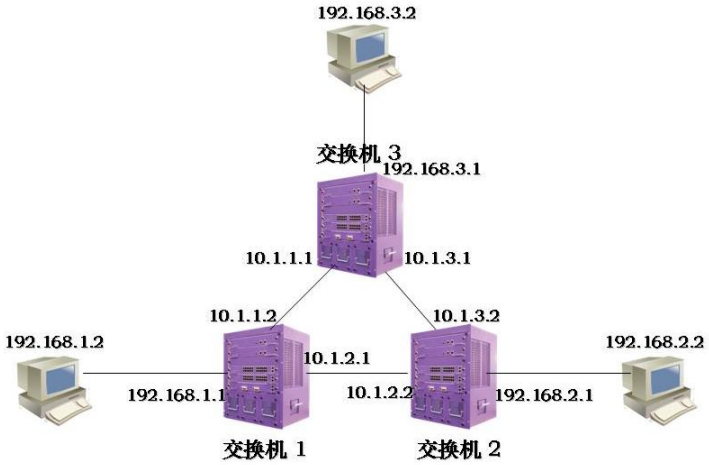
Switch# configure terminal

The Switch (config) # router rip

The Switch (config - rip) # network 192.168.3.0/24

The Switch (config - rip) # network 10.1.1.0/24

The Switch (config - rip) # network 10.1.3.0/24




**(2) the validation**

Use the following command to view the information of RIP:

The show IP separate protocols rip

The show IP rip the database

Rip the show IP interface

# Chapter 26
# Configure OSPF

This chapter mainly includes the following contents:

- OSPF is introduced
- OSPF configuration
- OSPF configuration example

## 1.99 OSPF is introduced

OSPF (Open Shortest Path First) is a link-state algorithm based protocol, which can support a relatively large scale network and achieve rapid convergence.

Routers running the OSPF protocol maintain their own link-state database (LSDB), which describes the topology of the entire autonomous system like a map. When the database of all routers is synchronized, each router calculates the shortest route to other destination nodes in the autonomous system from its own perspective and maintains it in its own routing table. When topology changes in the network, routers only need to package the changed link state in the Link State Update (LSU) message and broadcast it out. All routers will synchronize the local database again and recalculate the route. Each

router publishes the link state broadcast (LSA) it sees and gathers it together to form the topology description LSDB of the whole network, which is converted into a weighted directed graph, and then SPF algorithm can be used to calculate the outlet from the table.

In a broadcast network, each router needs to broadcast its own status information to other routers. Thus, multiple pairings will be established, which will lead to a large number of unnecessary message transmissions. For this purpose, OSPF specifies a designated router (DR) and a backup designated router (BDR). The router sends link information to DR, which is collected and then sent to all routers. The number of adjacency between routers on the broadcast network is effectively reduced.

OSPF supports five protocol messages:

HELLO message, periodically broadcast to neighbors, used to discover and maintain neighbors, DR election, contains some interface attribute values, some parameters in HELLO message must be consistent to establish neighbors.

DD packet (Database Description) USES DD packet to describe its OWN LSDB, including each LSA head. Through LSA head, one LSA can be uniquely identified, and the end-to-end router can determine whether it has this LSA or not. If not, request the full LSA.

LSR message (Link State Request) After two routers exchange DD message, they will know which LSA is missing locally on the opposite router, and then they need to send LSR message to Request the complete LSA. Only the LSA Head is required for the request.

LSU message (Link State Update) is a collection of multiple Lsas.

LSAck message (Link State Acknowledgement) is Acknowledgement of receipt of LSU message to ensure reliable transmission Link information. Use the LSA head for validation.

Router-id concept: Unique identification of a Router within an autonomous system.

Area: If OSPF is running in a larger network, LSDB will be very large due to the increase in the number of routers, and the synchronization time and computational routing time will increase, occupying a large amount of storage space and CPU resources. Moreover, the larger the network, the more frequent the topology changes, so that the network is always in flux. The router needs to spend a lot of time to transmit messages and calculate routes, which unnecessarily occupies the network bandwidth. Therefore, OSPF introduces the concept of region and divides routers into different regions. LSDB only synchronizes and computes routes within regions, and the route interaction between regions is completed by boundary router (ABR). In this way, the number of routers in the region will be limited, LSDB will be limited to a small capacity, the calculation time of routing will be greatly reduced, and the convergence will be fast when the topology changes. The concept of region effectively groups a large network and performs routing functions in a small range within each region. Routes between zones interact on backbone zones (zones with zone ID 0). Therefore, all non-backbone areas must be connected to the backbone area, that is, ABR has at least one interface to connect the backbone area. If in network planning, a non-backbone area cannot be connected with the backbone area, then virtual link must be configured to establish a logical path, that is, a certain ABR in the backbone area and a certain ABR in the non-backbone area establish a point-to-point link through a transmission area. Then the inter-domain routing information on the backbone region will also be released to the non-backbone region through the virtual link.

## 1.100 OSPF configuration

After OSPF protocol starts, enter OSPF configuration mode to set corresponding

properties and functions. OSPF configuration command in OSPF configuration mode and interface configuration mode.

OSPF configuration includes:

- Start OSPF and enter OSPF mode
- Can make the interface
- Specify the host
- Configure router ID
- Configure the adjacency points
- Prohibit the interface from sending messages
- Configure SPF timers
- Configuration management distance
- Introduce external routing
- Configure the network type of the interface
- Configure the hello message dispatch time interval
- Configure the neighbor router outage time
- Configure the retransmission interval
- Configure interface delay
- Configure the priority of the interface in the DR election
- The cost of sending a message on the configuration interface
- Configure whether the interface sends A DD message with an MTU value

- Configure interface message authentication
- Configure zone virtual links
- Configure zone routing aggregation
- Configure area message authentication
- Configuring stub areas
- Configure the NSSA region
- Configure external routing aggregation
- Configure default weights for external routes

## 1.100.1 Start OSPF and enter OSPF mode

OSPF protocol can run multiple copies, using process id to identify; When starting THE OSPF protocol, it is necessary to specify which process number is started. If there are no arguments, the process number is 0.

Pattern: Global configuration pattern

Router OSPF [Process-ID]

Start the OSPF process with process id and enter its mode

Command: No Router OSPF [Process-ID]

Close the OSPF process with process id

Parameter: Process-ID value 1~$(2)^{16}$-1), represents the OSPF process number started; Without the parameter process-ID, start OSPF with process number 0.

Default: The OSPF protocol is not run

## 1.100.2 Can make the interface

The value of OSPF protocol is that it introduces the idea of layering, dividing a complete autonomous system into different regions in order to build a conceptual hierarchical network model. A region is a logical grouping of routers in an autonomous system. When different interfaces of routers belong to different regions, that is, across regions, it is called border router ABR. For each network segment starting OSPF protocol, it can only belong to a specific region, that is, each interface running OSPF protocol on the router must belong to the specified region. Areas are identified by area number (AREa-ID), and areas with area number 0 are backbone areas. Routing information between different regions is passed through the border router. Unlike RIP, OSPF must be specified when running on an interface.

Pattern: OSPF configuration pattern

Command: network <network-address> area <area-id>

The specified region specifies the interface to run the OSPF protocol

Command: no network <network_address> area <area-id>

Close OSPF on a specific interface in a specific region

Parameters: Network-address has two forms, A.B.C.D/M and A.B.C.D. The former specifies the network IP and mask length, and the latter specifies the network IP and mask length. Area-id is also available in two forms, A.B.C.D and integer, the former using the dotted decimal format and the latter having values from 0 to (2)$^{32}$1).

Default: The OSPF protocol does not enable the interface after startup

## 1.100.3 Specify the host

Pattern: OSPF configuration pattern

Command: host <ip-address> area <area-id> [cost <cost>]

Configure host routing

Command: no host <ip-address> area <area-id> [cost <cost>] Cancel host routing

Parameter: IP-Address USES the A.B.C.D format to represent a specified host within an area, stub type on the router's link representation. The AREa-ID is shown in the network command. Cost represents the cost of specifying the link and is an optional parameter.

Default: Cost defaults to 0 if not configured

## 1.100.4 Configure router ID

The ID of the router is a 32-bit unsigned integer that is the unique identity of a router in the autonomous system. The router ID can be manually configured to ensure that any two routers in the autonomous system have different ids. If not configured, the router USES the IP address of the Loopback interface. If loopback has no IP, select the highest address from the IP address of the current interface as the ID. In order to ensure the stable operation of OSPF, the router ID should be partitioned and manually configured during network planning.

Pattern: OSPF configuration pattern

Command: ospf router-id <router-id>

Configure router ID

Command: No OSPF Router-ID

Cancel the router ID

Router-id <router-id>

The command: No Router-ID [Router-ID]

Parameter: Router-ID is in A.B.C.D format

Default: The ROUTER ID is automatically generated after the OSPF protocol is started according to the rules. The rules are as follows: First select the router-ID configured for the command; If not, select the LOOPback IP address. If none, select the highest IP address of the current interface; If none, 0.0.0.0.

Both sets of commands function the same.

## 1.100.5 Configure the adjacency points

OSPF protocol Interactive protocol message through multicast, using the multicast address 224.0.0.5 or 224.0.0.6. When the OSPF protocol runs on non-broadcast links, such as NBMA, it must be configured to use unicast interactive protocol messages. You can manually specify the IP address of the opposite side and the corresponding property value.

Pattern: OSPF configuration pattern

Neighbor <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>]

Specifies the end - to - end adjacency point and sets properties

Command: no neighbor <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>] cancel the opposite neighbor and properties Settings

Parameter: IP address opposite to IP address, in A.B.C.D format; Prio is the opposite priority, with values between 0 and 255. The value of deadtime is 1 to (2), which is considered to be down. If the timer terminates, no hello message is sent to the opposite end$^{16}$- 1); Cost is the cost of the link to the opposite end, and the value is 1~(2)$^{16}$1).

Default: Priority 1 (0 will not participate in DR election); Poll-interval is 120 seconds; Cost to 10.

## 1.100.6 Prohibit the interface from sending messages

In a simple network, the INTERFACE of THE OSPF protocol only represents a network segment between two devices for the purpose of transferring data. Then, the interface is set to passive and blocks the hello message from being broadcast on its link without affecting the route of the interface.

Pattern: OSPF configuration pattern

Command: passive-interface <if-name>

Configure the interface in a passive state

Command: no passive-interface <if-name>

Cancel the interface passive state

Parameter: IF-name is the three-tier interface name (for example: vlan1 vlan2...)

Default: The enabled interface is not passive after the OSPF protocol is started

If the interface running THE OSPF protocol is specified as passive, the direct route to the interface can still be published, but the OSPF packets on the interface will be blocked and the interface will not be able to establish neighborhood relationships. In some cases, network resources can be effectively saved.

## 1.100.7 Configure SPF calculation time

When the LINK state database LSDB of OSPF changes, the shortest path needs to be recalculated. If the shortest path is calculated immediately after each change, it will consume a lot of resources and affect the efficiency of the router. By configuring delay and hold to adjust the time interval of SPF calculation, excessively frequent SPF calculation caused by frequent changes in the network can be restrained, so as to avoid occupying a large amount of system resources within a single time and affecting the operation efficiency of the router.

SPF calculation has a timer, each time according to the stopping time to start the next calculation. When the timer terminates and SPF calculation needs to be started, recalculate the stopping time of the last SPF calculation to the current one. If the stopping time of the configured one has been exceeded, the configured delay time will be used to start the timer. If the configured inhibition time has not been exceeded, the delay time required is calculated using the configured inhibition time. If the delay time is less than the configured delay time, the configured delay time is used; otherwise, the calculated delay time is directly used to start the SPF calculation.

Pattern: OSPF configuration pattern

Command: elapsed SPF <delay> <hold>

Configure the delay and hold values for the calculated interval with SPF

Mandate: No Tick SPF

Revert to the default

Parameter: delay means the delay time needed to calculate SPF; Hold represents the amount of time between SPF calculations.

Default: delay is 5S; Hold for 10 seconds

## 1.100.8 Configuration management distance

Multiple routing protocols can run simultaneously on a router, and how to select among the routing information learned by multiple routing protocols requires the use of managed distance. When different protocols find the same route, the one with less management distance is preferred.

Pattern: OSPF configuration pattern

Command: distance <distance>

Configuration management distance

Command: no distance <distance>

The recovery management distance is the default

Distance ospf {intra-area <distance> | inter-area <distance> | external <distance>}

Configure different types of administrative distances

Command: No Distance OSPF

Restore the three types of administrative distance as the default

Parameters: Distance is between 1 and 255. Intra-area represents the managed distance of routing within the domain; Inter-area represents the management distance of inter-domain routing. External represents the administrative distance of an external route.

Default: OSPF protocol management distance is 110; The administrative distance for in-domain, interdomain, and external routes is 0.

## 1.100.9 Introduce external routing

Multiple dynamic routing protocols can run on the router, and routing information can be Shared between different routing protocols. OSPF treats the routing learned by other routing protocols as the routing outside the autonomous system, which is introduced by the autonomous system boundary router ASBR. The introduction of external routing can be assigned value, weight type and other attributes.

OSPF routing is divided into four types, one is intra-domain routing, the other is inter-domain routing, both of which are within the autonomous system; The third is the external route of Type-1, and the fourth is the external route of Type-2. These two types of routes describe the routes to destinations outside the autonomous system. Type-1 is a route from other IGPs, which OSPF believes has high reliability and is comparable to the routing weights in the autonomous system. Therefore, the cost of such external routes is the sum of the cost of the router itself to THE ASBR and the cost of the ASBR to the destination. Type-2 routing is a route from other EGPs, which OSPF considers not too

reliable, and its cost is much higher than that of the autonomous system, so it is not comparable. Therefore, the cost of such external routing only USES the cost of ASBR to the destination, while ignoring the cost of the router itself to ASBR.

Pattern: OSPF configuration pattern

Redistribute {kernel | static | rip | ISIS | BGP} [metric <metric> | metric <type >0 route-map <route-map-name> >1 tag <tag BBBGP]

No redistribute {kernel | connected | static | rip | ISIS | BGP} [metric <metric> | metric <type >0 route-map <route-map-name> >1 tag <tag BBBGP]

Parameters: The first required parameter IS the type of external routing that can be introduced, including direct connection, static, RIP, IS-IS, BGP; The second parameter is the weight set when external routing is introduced, with the value of 0~$(2)^{24}$- 1); The third parameter is the two types of external routes introduced, namely type-1 and Type-2. Type-1 is IGP route and Type-2 is EGP route. The third parameter is the name of the reference Route-map, which is configured in global configuration mode, as shown in the command manual; The fourth parameter is TAG, and its value is 0~$(2)^{32}$Is the external routing attribute.

Default: No external routing protocol is introduced

## 1.100.10 Configure the network type of the interface

OSPF protocol is the perspective of its own router, each router will describe its adjacent network topology, passed to other routers. OSPF divides the network types of interface links into four types according to the link-layer protocol types: one is broadcast type (link-layer protocol is Ethernet, FDDI etc); The other is NBMA non-broadcast multiplex access (link-layer protocols are FR, ATM, HDLC, X.25 etc.); The third is the point-to-multipoint type. No link layer agreement is considered to be a point-to-multipoint type by default. The point-to-multipoint type must be configured compulsively by another network type. The most common approach is to change the nonfully connected NBMA to a point-to-multipoint network. The fourth is the point-to-point type (link layer protocols are PPP, LAPB, POS).

On broadcast networks that do not have multipath access, interfaces can be configured to be of type NBMA. When not all routers in the NBMA network are directly reachable, interfaces can be configured as point-to-multipoint types.

The NBMA network agreed in OSPF protocol is fully connected, non - broadcast, multi - point accessible. A point-to-multipoint network is not necessarily fully connected. NBMA requires DR selection, and there is no DR in the point-to-multipoint network. The NBMA network USES a designated neighbor to broadcast content on a single, point-to-multipoint network.

Pattern: Interface configuration pattern

Command: IP ospf network <type>

Configure the network type of the interface link

Command: No IP OSPF Network

The network type for restoring interface links is the default

Parameter: type can be broadcast, non-broadcast, point-to-point, point-to-multipoint [non-broadcast]; The first is broadcast networks, the second is non-broadcast networks, known as NBMA, the third is point-to-point networks, and the fourth is point-to-multi-point networks. The point-to-multipoint network is divided into broadcast network and non-broadcast network. The non-broadcast neighbor cannot be found automatically and must be designated.

Default: broadcast network

## 1.100.11 Configure the hello message dispatch time interval

Hello messages are used to periodically send to a neighbor router, discover and maintain neighbor relationships, and elect DR and BDR. The interval of the Hello message can be configured manually, but care should be taken to keep the interval of the Hello timer consistent between neighbors in the network. The value of the Hello timer is inversely proportional to the convergence speed of the router and the network load.

Pattern: Interface configuration pattern

Command: IP ospf hello-interval <seconds>

Configure the interval for the Hello timer

Command: No IP OSPF Hello-interval

Restore the Hello timer interval to the default

Parameter: value of seconds: 1~$(2)^{16}$-1), represents the time interval between two hello messages.

Default: 10 seconds between Hello on broadcast network and point-to-point network; Hello is 30 seconds apart on the NBMA network and the point-to-multipoint network.

## 1.100.12 Configure the neighbor router outage time

Pattern: Interface configuration pattern

IP ospf dead-interval <seconds>

Configure neighbor invalidation time

Command: no IP OSPF dead-interval

The default value is to restore neighbor invalidation time

Parameter: value of seconds: 1~$(2)^{16}$Between -1), denotes that the hello message received by the neighbor after seconds is considered to be invalid; The neighbor's Dead

timer is updated every time a Hello message is received.

Default: Neighbors on broadcast network and point-to-point network expire in 40 seconds; Neighbor failure time is 120 seconds on NBMA network and point-to-multipoint network; When the network type is changed, the Hello and Dead intervals will use the default values.

## 1.100.13 Configure the retransmission time

OSPF is a reliable link-state protocol, which is manifested in the response lSU-ACK of the corresponding LSU message. When a confirmation message is received, the link state update is considered to be received. If no acknowledgement message is received within the retransmission interval, the LSA is retransmitted to the neighbor. The retransmission interval can be manually configured to be greater than the time it takes for a message to travel back and forth between two routers. Setting it too small can cause unnecessary retransmission.

Pattern: Interface configuration pattern

Command: IP ospf retransmit-interval <seconds>

Configure the retransmission interval for the interface

Command: No IP OSPF ReTransmit - Interval

The restore retransmission interval is the default

Parameter: value of seconds: 1~(2)$^{16}$Between -1), indicating the interval to be retransmitted when the LSA is not received by the opposite end.

Default: retransmission interval 5s

## 1.100.14 Configure interface delay

In LSU of link-state update message, each link-state broadcast LSA has age time domain, and the transmission delay of the transmission interface needs to be increased before transmission. This parameter mainly considers the time required by the interface to send messages, especially on the low-speed network, which needs to be configured.

Pattern: Interface configuration pattern

Command: IP ospf transmit-delay <seconds>

Set the transmission delay of the interface

Command: No IP OSPF Transmit -delay

The transmission delay of the recovery interface is the default

Parameter: value of seconds: 1~(2)$^{16}$Between -1), indicating that this delay value needs to be increased in the AGE field of the LSA sent from the interface.

Default: transmission delay of 1s for interface

## 1.100.15 Configure the priority of the interface in the DR election

In order to avoid repeated point-to-point transmission of link information in broadcast network, the designated router DR and BDR need to be selected to be responsible for the link information in the broadcast network segment. The priority of the interface indicates the qualification it has at the time of the DR election, and when the election conflicts, the priority of the high is considered first. If the priority is 0, it will not participate in the election. If the priority is greater than 0, it will be a candidate. Each router will include its own priority information and DR in its own Hello message, broadcast in the broadcast network, and finally select the one with high priority as DR. If the priority is equal, the router ID is greater than the router ID.

When DR fails, the router in the network needs to go through a process of re-electing DR, which takes a time, and during this time, it will cause routing calculation error. The idea of BDR is to smooth the transition to a new DR. BDR is a backup of DR, which is selected at the same time in the DR election. It also establishes adjacency relationship with other routers in the network, but the nodes of information collection and publication in the network are in DR instead of BDR. BDR only maintains adjacency synchronization. When a DR fails, the BDR becomes a DR immediately and is responsible for collecting information within the network segment. At this time, a new process elects the BDR, but the ELECTION of the BDR does not affect the calculation of the route.

Pattern: Interface configuration pattern

Command: IP ospf priority <prio>

Configure the priority of the interface in the DR election

Command: No IP OSPF Priority

The restore interface priority is the default

Parameter: PriO value is 0~255, indicating the priority in the DR selection, when 0, it means not participating in the election.

Default: priority 1

## 1.100.16 The cost of sending a message on the configuration interface

In a network, traffic is controlled by configuring different links at different costs. The cost of the interface represents the cost of sending messages from the interface. If not manually configured, OSPF will automatically calculate the interface cost based on the interface baud rate.

Pattern: Interface configuration pattern

Command: IP ospf cost <cost>

Command: No IP OSPF Cost

Parameter: Cos (T) is 1~$(2)^{16}$Represents the substitution value of the sent message on the interface.

Default: Interface costs 10

## 1.100.17 Configure whether the INTERFACE sends A DD message to fill an MTU field

Pattern: Interface configuration pattern

Command: IP OSPF mTU-ignore

Set not to check the MTU value in the DD message

Command: no IP OSPF mtu-ignore

Uncheck the MTU value in the DD message

Default: Check mTU value in DD message

## 1.100.18 Configure interface message authentication

OSPF supports plaintext and MD5 message authentication on the interface.

Pattern: Interface configuration pattern

Command: IP ospf authentication <mode>

Configure authentication mode

Command: No IP OSPF authentication

Cancel the certification

Parameter: No parameter means plaintext authentication; Message-digest means MD5 certification; Null means no authentication

Command: IP ospf authentication-key <password>

Configure plaintext authentication password string

Command: No IP OSPF authentication-Key

Cancel the plaintext authenticated password string

Parameter: password represents the plaintext authenticated password string

Command: IP ospf message-digest-key <key-id> md5 <password>

Configure the MD5 authentication password

Command: no IP ospf message-digest-key <key-id>

Cancel the MD5 authentication password

Parameter: Key-ID value between 1 and 255, used for sorting in the key chain; Password stands for password string.

Default: No authentication is configured

## 1.100.19 Configure zone virtual links

OSPF protocol adopts the idea of stratification to divide the routers in the autonomous system into different groups, which are called regions. All regions are not equal and parallel, but have hierarchical relationship. Among them, 0.0.0.0 region is the most special, which is the backbone region. Therefore, all non-backbone regions must be connected with backbone regions, that is, at least one interface on ABR is in region 0. If some regions cannot guarantee physical access to backbone regions due to network topology constraints, virtual links need to be configured to guarantee logical access. Both ends of the virtual link are ABR, passing through a non-backbone area in the middle, known as the transit area transit area. When configuring virtual links, the ID of the transmission area and the ID of the opposite side, ABR, must be configured on both sides of the ABR to take effect.

When the virtual link is activated after the routing of the transport area has been calculated, it is logically equivalent to forming a point-to-point connection between the two endpoints, so the interface parameters can be configured on its physical interface and authentication can be started.

A single broadcast message is transmitted between ABRs. The router forwarding the single broadcast message in the transmission area regards it as a common IP message for forwarding, so it can only be understood as providing a logical link in the transmission area. Protocol messages can be exchanged between two ABRs.

Pattern: OSPF configuration pattern

Command: area <area-id> virtual-link <router-id>

Configure the transfer area and the opposite ID of the virtual link

[authentication < mode > |

Configure the authentication mode for virtual links

Authentication - key < password > |

Configure the virtual link plaintext authentication password

Message-digest-key <key-id> md5 <password> |

Configure the virtual link MD5 authentication password

Hello - interval < seconds > |

Configure the Hello interval for virtual links

Dead - interval < seconds > |

Configure virtual link neighbor failure time

The retransmit interval - < seconds > |

Configure virtual link retransmission interval

The transmit - delay < seconds > |

Configure virtual link interface delays

Command: no area <area-id> virtual-link <router-id>

[authentication < mode > |

Authentication - key < password > |

Message-digest-key <key-id> md5 <password> |

Hello - interval < seconds > |

Dead - interval < seconds > |

The retransmit interval - < seconds > |

The transmit - delay < seconds >]

Cancel virtual link setup

Parameter: Area-ID represents the ID of the transfer area. It can be used in dotted decimal format A.B.C.D or integer format with values from 0 to $(2)^{32}1$). Router-id represents the ID of the virtual link-to-end router, using the A.B.C.D format. The authentication and sending interface properties are optional. Refer to the command description.

Default: Virtual links are not configured

## 1.100.20 Configure zone routing aggregation

Pattern: OSPF configuration pattern

Area <area-id> range <ip-prefix | [| not- renown]

Configure aggregation range

No area <area-id> range <ip-prefix | [| not- renown]

Cancel the aggregation

Parameter: Area-ID represents the region ID and specifies the route within the region to aggregate, either in decimal format A.B.C.D or integer format, with values from 0 to $(2)^{32}1$). Ip-prefix USES the prefix format A.B.C.D/M to indicate the scope of the aggregation. The optional parameters PI and NOT-PI prefix indicate whether or not to

broadcast the range of the aggregation, also known as IP-prefix. Existing network routes are broadcast.

## 1.100.21 Configure area message authentication

The authentication type of all routers in an area needs to be consistent. The authentication password string of all routers in a network segment should be consistent. Configure regional authentication only to enable authentication (plaintext or MD5), and the password USES the corresponding configuration value of the interface. Refer to the interface message authentication configuration.

Pattern: OSPF configuration pattern

Area <area-id> authentication [message-digest]

Configure the regional authentication mode

Command: no area <area-id> authentication

Deregistration of territory

Parameter: Area-ID represents the area ID and specifies the area to be authenticated; You can use the dotted decimal format A.B.C.D or the integer format, with values from 0 to $(2)^{32}1$). The optional parameter represents plaintext authentication without message-digest for MD5 authentication.

Default: Regional authentication is not enabled

## 1.100.22 Configuring stub areas

Pattern: OSPF configuration pattern

The command area <area-id> stub [no - the summary]

Configure the router in the stub area

No area <area-id> stub [no-summary]

Unproperties the router in the stub area

Area <area-id> default-cost <cost>

Configure the default cost of an ABR broadcast route connected in the stub area

Command: no area <area-id> default-cost

The default cost to restore is the default value

Parameter: Area-ID represents the area ID and indicates which area attribute is stub. You can use the dotted decimal format A.B.C.D or the integer format, with values from 0 to (2)$^{32}$1). No-summary indicates that inter-domain routing is not injected into a Stub area.

The first set of commands is to configure the router within the stub area, and the second set is to configure the ABR with an interface connected to the stub area.

Default: Stub areas are not configured

## 1.100.23 Configure the NSSA region

Pattern: OSPF configuration pattern

Command: area <area-id> nssa [options]

Configure THE NSSA properties

No area <area-id> nssa [options]

Cancel the NSSA region property

Parameter: Area-ID represents the area ID. See the command manual for options.

Default: NSSA zone is not configured

## 1.100.24 Configure external routing aggregation

Routes introduced from other protocols are broadcast one by one in type-5 Lsus.Aggregation commands are used to specify a prefix range in which routes covered are stopped and only the aggregated route is broadcast. When the number of external routes is large, LSDB size can be effectively reduced.

Pattern: OSPF configuration pattern

Summary -address <ip-prefix> [not- prefix>]

Configure the aggregation scope and properties

No summary-address <ip-prefix> [not- pickled | tag <tag>]

Cancel aggregation of external routes

Parameter: IP-prefix USES the address prefix format A.B.C.D/M to indicate the route range to be aggregated. Not-pigged means the route is not broadcast after aggregation; Tag is the set TAG value, which is 0~$(2)^{32}$-Between 1), the default is 0.

Default: Externally imported routes are not aggregated

## 1.100.25 Configure default weights for external routes

When an external route is introduced, a default weight is used if the redistribute command does not specify the metric value.

Pattern: OSPF configuration pattern

Default-metric <metric>

Configure the default weights when external routing is introduced

No default-metric [metric]

The default weight is the default value when restoring external routing

Parameter: 0~(2) for metric$^{24}$1)

Default: The default weight is 1

## 1.100.26 According to the information

Pattern: Normal or privileged pattern

Command: Show IP Protocols

Command: Show IP Protocols OSPF

Displays OSPF protocol information

Command: Show IP OSPF [Process-ID]

Displays OSPF process information

Parameter: Instance-ID for process number,

Accessor 0 - ($2^{16}$1).

Command: the show IP ospf border routers

Display ABR information

Command: show IP ospf database <type>

Displays LSDB information

Parameter: Type is each type of LSA and summary information, see the command manual for details.

Command: Show IP OSPF Interface [IF-name]

Displays OSPF interface information

Parameter: IF-name is the agreed three-tier interface name

Command: Show IP OSPF Route (count)

Displays the OSPF routing table

Parameter: Count represents the total number of entries in the display routing table

Command: Show IP OSPF Virtual-Links

Displays OSPF virtual connection information

Command: Show IP OSPF Neighbor [Options]

Displays OSPF neighbor information

Parameters: Options see the command manual

Pattern: Privileged pattern

Command: Show running-config

Displays current switch configuration, including OSPF configuration.

Command: Show Running-config OSPF

Displays the current configuration of the OSPF protocol.

## 1.101 OSPF configuration example

**(1) configuration**

The three switches are connected in pairs, with 6 network segments respectively. OSPF protocol is enabled to realize the interoperability between three PCS. The interface is required to be in the same area area 0.

On switch 1:

Switch# configure terminal

The Switch (config) # 100 router ospf

The Switch (config - ospf - 100) # network 10.1.1.0/24 area 0

The Switch (config - ospf - 100) # network 10.1.2.0/24 area 0

The Switch (config - ospf - 100) / 24 area 0 # network 192.168.1.0

On switch 2:

Switch# configure terminal

The Switch (config) # 100 router ospf

The Switch (config - ospf - 100) # network 10.1.2.0/24 area 0

The Switch (config - ospf - 100) # network 10.1.3.0/24 area 0

The Switch (config - ospf - 100) # network 192.168.2.0/24 area 0

On switch 3:

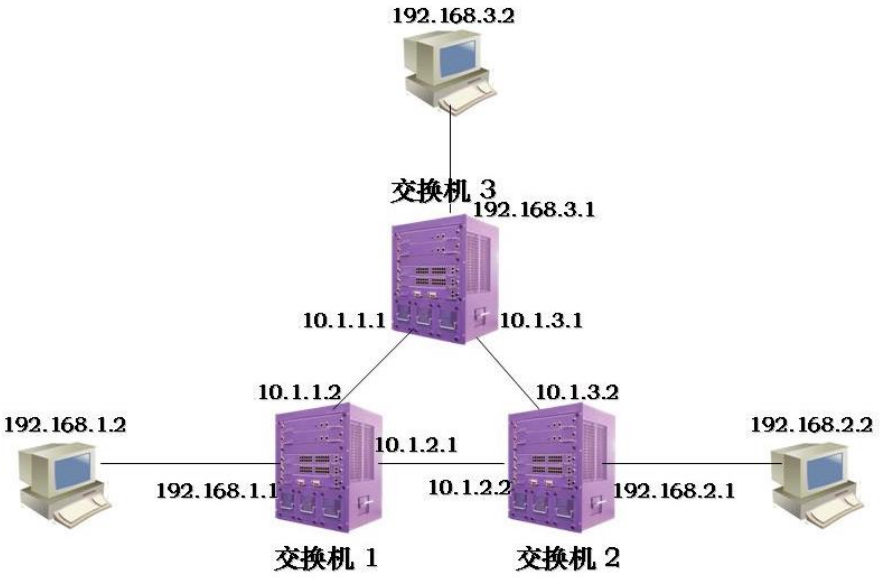
Switch# configure terminal

The Switch (config) # 100 router ospf

The Switch (config - ospf - 100) # network 10.1.1.0/24 area 0

The Switch (config - ospf - 100) # network 10.1.3.0/24 area 0

The Switch (config - ospf - 100) # network 192.168.3.0/24 area 0




**(2) the validation**

The show IP ospf database

Ospf show IP interface

The show IP ospf neighbor

The show IP route ospf

Ospf show IP route

# Chapter 27
# Configuration VRRP

This chapter mainly includes the following:

VRRP presentation

VRRP configuration

VRRP configuration examples

# VRRP presentation

VRRP is the abbreviation of virtual router redundancy protocol, which is an important three-layer reliability protocol for redundant backup of default gateway. A detailed description of the VRRP protocol is given in this section, which includes the following:

VRRP overview

VRRP terminology

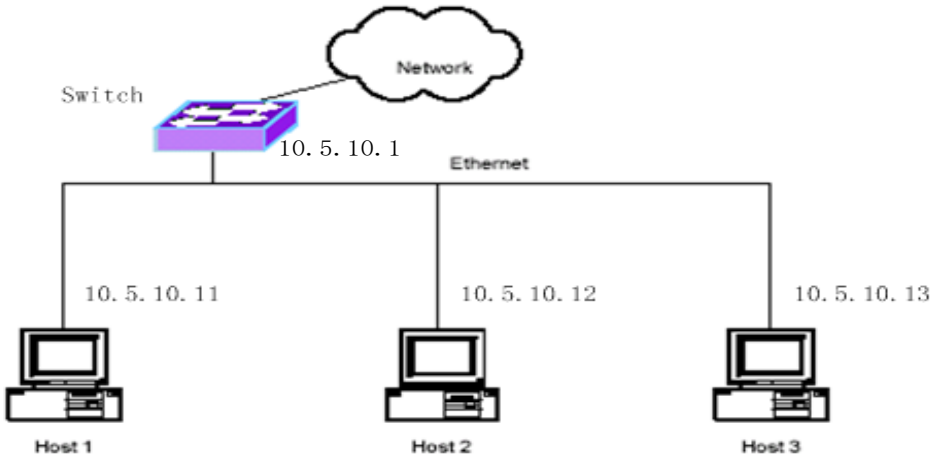
VRRP protocol interaction

Election of virtual master routers

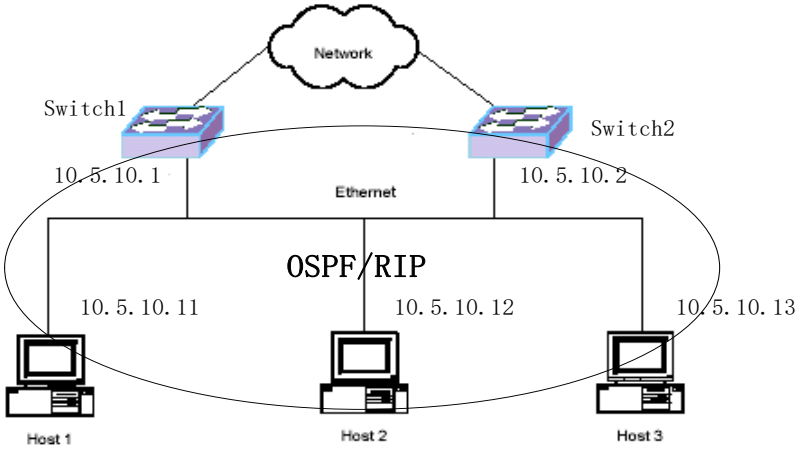
Status of virtual routers

VRRP tracking

The following figure is a typical intranet networking scheme. One interface of the switch is connected to the external network, one interface is connected to the internal network, the IP address of the interface connected to the internal network is 10.5.10.1, and the host 1,2,3 are all configured with IP addresses, all within the network segment 10.5.10.0/24. a default gateway is configured on host 1,2,3, with the next hop pointing to the switch and the IP address for the next hop being 10.5.10.1. As a result, the host sends a message whose destination IP address is not in the network segment that matches the default route to the switch, which forwards the message  The switch also forwards the message from the external network to the corresponding host, so that the host can communicate with the external network.



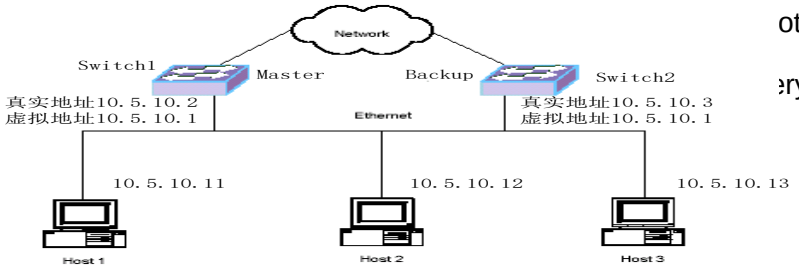

In the above networking scheme, the communication between the host and the external network can only pass through this unique switch, and when the switch fails, all the hosts are with the external interrupt. one solution to this problem is to extend a switch to two or more switches, running dynamic routing protocols between the host and the switch OSPF or RIP, as shown below.




When the host runs the dynamic routing protocol, the host can learn all the routing of the external network. When the host communicates with the external network, the next hop IP find the routing according to the destination and address of the message to decide whether the message is sent to the switch1 or switch2.. when one of the switches fails, the routing in the host can be re-learned in a very short time. the next hop of the routing will point to the router without failure, so that the communication between the host and the external network will not be interrupted.

However, it is not realistic to implement dynamic routing protocol on host. For the host, running dynamic routing protocol load is too large, for the network, running dynamic routing protocol on the host will cause too much unnecessary data traffic on the network, and some hosts do not support dynamic routing protocol at all.

VRRP protocol is the best option to fundamentally solve this single point of failure. VRRP agreement is specifically addressed to this issue. the Switch1 and Switch2 form a virtual router as shown in the following figure. the real IP address of the interface of the two switches is different, but there is a common virtual IP address 10.5.10.1, and the default gateway of the host is set to the virtual IP address 10.5.10.1. When the Switch1 is a virtual master switch, the communication between the host and the external network is forwarded by Switch1, but when Swit.  ch1 failure occurs, the Switch2 replacement Switch1 becomes a virtual master switch, and the communication between the host and the external network is forwarded through the Switch2. using the VRRP protocol, the host only ne otocols on the host. tl ery little VRRP protocc




## 1.101.1 VRRP terminology

The following are a few commonly used terms:

1)VRRP

Virtual Router Redundancy Protocol abbreviation, Virtual Router Redundancy Protocol, is a fault-tolerant protocol of default gateway, which can improve the reliability of network.

2)Virtual Router

Virtual Router, an abstract object, based on a subnet interface, includes a virtual router identifier (VRID) and a IP address, which is also called a virtual IP address, and the virtual IP address serves as the host's default gateway.

3)VRRP Router

VRRP router, the router that runs the VRRP protocol, a VRRP router can be added to a virtual router.

4)IP Address Owner

IP address owner, the virtual IP address of the virtual router is the same as the real IP address of the interface VRRP router.

5)Virtual Router Master

the virtual master router, which is responsible for forwarding three-tier packets through the virtual router, responds to the ARP request of the IP address of the virtual router. When a VRRP router is IP address owner, it is always virtual master router.

6)Virtual Router Backup

Virtual backup router, does not forward three layers of data packets, does not answer the ARP request of virtual IP address, when the virtual master router fails to replace the work of the virtual master router.

To better understand these terms, note the following:

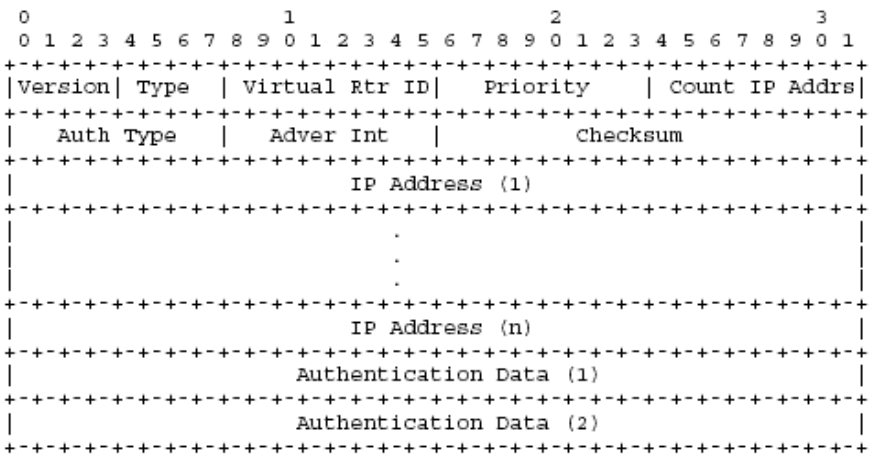
A switch may include multiple interfaces to initiate VRRP protocols on multiple interface subnets.

A virtual router can exist on an interface subnet.

A VRID identifies a virtual router.

VRRP protocol interaction

VRRP protocol package is enclosed in the IP package, VRRP the header is shown below:




1)VRRP package MAC frame header field

source MAC address: virtual MAC address of virtual router ,00-00-5 e-00-01-{VRID},VRID is virtual router identifier. The virtual MAC address is e-00-01-01.00-00-5 if the virtual router is 1

destination MAC address: VRRP multicast MAC address 01-00-5

2)VRRP package IP header field

Source IP address: the primary IP address of the interface that sends the VRRP package.

destination IP address: multicast IP address 224.0.0.18, can not do 3-layer forwarding.

TTL：255, to prevent remote VRRP packet attacks.

Protocol：112.

3)VRRP header field

Version：2.

Type : VRRP type of package, only one type is supported :1-ADVERTISEMENT,VRRP pass package.

VRID： identifies a virtual router.

Priority： the priority of the VRRP router sent for this virtual router.

Count IP Addrs： the number of virtual IP addresses, a virtual router can have multiple virtual IP addresses.

Auth Type： authentication method between VRRP routers in a virtual router.

Advertisement Interval： notice interval, default is 1 second.

Checksum： checksum from the Version of VRRP Baotou.

IP Address (es): one or more virtual IP addresses.

Authentication Data： certified data.

4)VRRP priority

each VRRP router in a virtual router needs to configure a priority priority. The range of priorities is from 0 to 255, where 0 and 255 have special uses, and the configurable priority range is from 1 to 254, with a default of 100. The higher the value of priority, the

higher the priority, the more likely it is to become a virtual master router.

When a VRRP router is the IP address owner in a virtual router, its priority is 255.

A VRRP with a priority of 0 is sent to other backup routers when the virtual master router needs to notify other backup routers that it is no longer the master, which can quickly trigger other backup routers to become virtual master routers.

5)VRRP certification

VRRP protocol provides three authentication methods, and different authentication methods can be selected according to the security requirements of the network in actual use.

0 --- No Authentication

No certification

1 --- Simple Text Password

Simple Password Authentication

2 --- IP Authentication Header

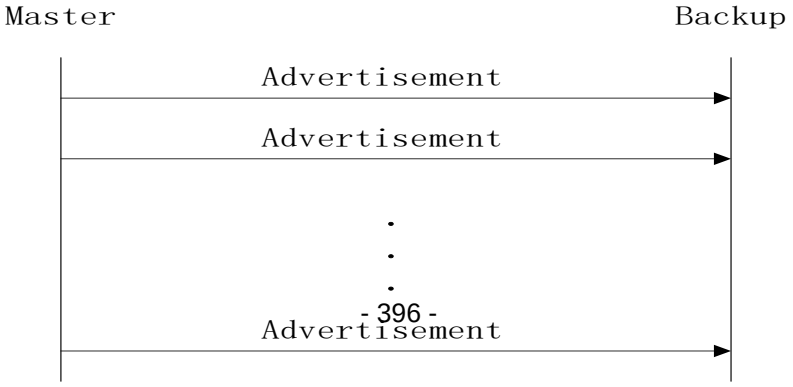
IP authentication header and calculate message summary by HMAC-MD5 method

A HMAC authentication method can be adopted in networks with low security without authentication or simple password authentication.

for 0 and 2 authentication methods, Authentication Data field fill 0, for 1 authentication method, Authentication Data field fill password. for the 2 authentication method, the message summary is filled in the IP Authentication Header field, that is, AH field is added at the IP head.

6)VRRP package interaction

VRRP protocol has only one type of package, ADVERTISEMENT notification package. in a virtual router, the virtual master router sends a notification packet every Advertisement Interval time (default is 1 second). a virtual backup router determines whether state migration is required based on the VRRP notification package received. The main and standby protocols interact as follows:



## 1.101.2 Election of virtual master routers

- The choice of virtual master router in a virtual router is determined by the following factors:

- IP Address Owner

- if a VRRP router is the IP address owner (its interface IP address is the same as the virtual IP address), if the router works properly, it is the virtual master router.

- VRRP priority

- A VRRP router with the highest priority working properly becomes a virtual master router. the priority range that can be matched is from 1 to 254, and the priority of the router IP the address owner is 255. when the virtual master router notifies the virtual backup router that it is no longer the master, priority 0 is given in the VRRP package.

- The actual IP address size of the interface, when the priority is the same, the actual IP address of the interface VRRP router becomes a virtual master router.

In virtual routers, master-standby switching occurs:

1) when a virtual master router fails, there are two more possibilities:

The backup router sends a VRRP packet with a priority of 0 if the virtual master router is still active and switches to the virtual master router after receiving the VRRP packet without receiving the virtual master router within Skew_Time time. In this case, the switching speed is relatively fast, and the switching can be achieved within 1 second. if the virtual master router can not be active, the virtual backup router will switch to the virtual master router after not receiving the VRRP package of the virtual master router in Master Down Interval time.

Master_Down_Interval = (3 * Advertisement_Interval) + Skew_Time

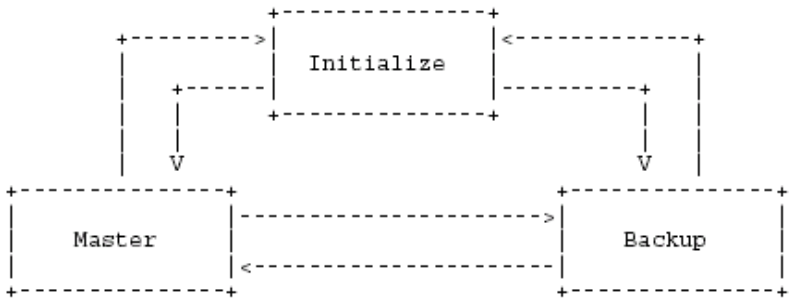
Skew_Time =(256- Priority)/256)

2) when the virtual master router is not the IP address owner, and now a router IP the address owner joins the network, the router becomes the virtual master router, and the master-standby switch appears.

3) when a VRRP router joins the network, if the priority of the router is higher than that of the virtual master router and is in preemption mode (the configuration variable is Preempt_Mode as TRUE), the router becomes the virtual master router and the main and standby switches appear.

## 1.101.3 Status of virtual routers

Each VRRP router in a virtual router performs a state machine. The state machine migrates as follows:




1 ) Initialize state

the Initialize state is the initial state of a virtual router in which Startup start events are awaited. If Startup event is received in this state, it is handled as follows:

this VRRP router becomes a virtual master router if its priority is 255(i.e. is 255(i.e., IP address owner).

otherwise, the router becomes a virtual backup router and migrates to the Backup state.

After the router migrates to the Master state, the actions are as follows:

send a VRRP notification package.

broadcast a ARP request containing the virtual IP address and the corresponding virtual MAC address.

Set Adver_Timer timer, timing interval is Advertisement_Interval..

- Set Master_Down_Timer timer, timing interval is Master_Down_Interval..

2 ) Backup state

- Backup status aims to monitor the availability and status of the virtual master router and replace the work of the virtual master router at any time.
-

- cancel the Master_Down_Timer timer and return to Initialize status if a Shutdown event is received.

- 

- When the Master_Down_Timer expires, become a virtual master router, migrate to the Master state.

- 

- If a VRRP notification package is received, the following situations exist:Set the Master_Down_Timer, time interval to Skew_Time. if the priority field in the VRRP package is 0

- Otherwise, if the preemption mode (Preempt_Mode) is the priority in the FALSE or VRRP package >=VRRP the priority of the router, reset the time interval to Master_Down_Interval..

- Otherwise, discard the VRRP package.

3 ) Master Status

VRRP routers in Master state are responsible for forwarding three layers of packets through virtual routers.

When Shutdown event is received, cancel the Adver_Timer timer, send a VRRP notification package with priority 0, and migrate to the Initialize state.

Send a VRRP notification package if the Adver_Timer timer expires reset the Adver_Timer timer.

If a VRRP notification package is received, the following situations exist:

Send a VRRP notification package if the priority in the package is 0, reset the Adver_Timer。

- Otherwise, if the priority in the package is greater than the same priority or priority of the VRRP router, but the IP address of sending the package is greater than the interface master IP address of the VRRP router, cancel the Adver_Timer timer and set the Master_Down_Timer, to migrate to the Backup state.

- Otherwise, discard the VRRP pass packet.

## 1.101.4 VRRP Tracking

VRRP protocol itself can only detect the internal faults of the virtual router, such as the interface LINK DOWN where the virtual router is located or the VRRP router is dead, and the failure outside the virtual router can not be detected. When there is a fault outside the virtual router, the virtual router can not select the virtual master router according to these faults, which will cause the interruption of network data. VRRP tracking can solve this problem, VRRP the router to track the specified external events, when there is an external fault VRRP the router changes its running priority, re-select the virtual main router, and ensure the number of networks No interruption.

The following figure, when the external interface Switch1 the virtual master router is LINK DOWN, if the VRRP tracking function is not enabled, Switch1 can not detect the other part of the fault, Swith1 continue to be the virtual master router, the host can not access the external network. When VRRP tracking is enabled, Switch1 can detect external failures and modify their own running priorities, re-select virtual master routers, Switch1 change to virtual backup routers, Switch2 to virtual master routers, so that the host can continue to access the external network collateral.

VRRP tracking includes three types: interface tracking, routing tracking and PING tracking. Interface tracking is VRRP router tracks the interface outside the virtual router, if a trace of an interface LINK DOWN, indicating an external fault. routing tracking is VRRP router tracks the routing in the routing table it has learned. if the routing does not exist or the routing exists but is not active, it indicates an external fault. PING tracking is a device VRRP the router has been PING to be tracked, indicating an external presence if the device does not PING a response within the specified time Failure. virtual routers can track interfaces, routes and PING at the same time. for each type of tracking, multiple

events can be tracked again. as long as one of the events being tracked fails, it indicates that the virtual router has an external fault. only if all the events being tracked are normal, does it indicate that the virtual router has no external fault.

## 1.102 VRRP Configuration

VRRP configuration includes the following:

- Create and delete virtual routers
- Configure virtual IP addresses for virtual routers
- Configure parameters for virtual routers
- Configuration VRRP tracking
- Launch and close virtual routers
- View VRRP information

## 1.102.1 Create and delete virtual routers

A virtual router is built on a subnet interface and needs to specify a VRID. virtual routers were not created by system default.

This virtual router can be deleted when a virtual router is no longer needed, and if the virtual router has been started, the virtual router will be closed first and then deleted. The commands to create and delete virtual routers are as follows:

| Command | Description | CLI Patterns |
| --- | --- | --- |
| router vrrp <vrid> | create a virtual router and go to VRRP configuration mode, if the virtual router already exists, go directly to VRRP configuration mode. parameter is VRID, range from 1 to 255. | Global Configuration Mode |
| no router vrrp [vrid] | Delete a virtual router, the parameter is VRID | Global Configuration Mode |

## 1.102.2 Configure virtual IP addresses for virtual routers

virtual IP addresses must be configured on virtual routers. in theory, one or more virtual IP addresses can exist in a virtual router, but a virtual router supports only one virtual IP address when the switch is implemented. By default, the switch is not configured with a virtual IP address.

Commands to configure the virtual IP address of the virtual router are as follows:

| Command | Description | CLI Patterns |
| --- | --- | --- |

| | | |
|---|---|---|
| virtual-ip <virtual-ip> <backup \| master> | Delete the virtual IP address of the virtual router. | VRRP Configuration mode |
| no virtual-ip | Delete the virtual IP address of the virtual router. | VRRP Configuration mode |

Note:

- configuring the virtual IP address of a virtual router must be successful if the virtual router has been turned off and can not be configured successfully when the virtual router is started.

- a set virtual IP address must be in the same network segment as the primary IP address of the interface, otherwise the configuration is not successful.

## 1.102.3 Configure parameters for virtual routers

The parameters of the virtual router include priority, preemption mode, announcement time interval, authentication method and authentication data, all of which have default values, as follows:

| parameter | Default value |
|---|---|
| priority | 100 |
| Preemption mode | TRUE |

| | |
|---|---|
| Notice interval | 1 second |
| Certification methodology | No certification |
| Certified data | None |

In configuration, for virtual routers, notification time intervals, authentication methods, and authentication data must be configured the same as priority and preemptive mode parameters.

for priority, it is divided into configuration priority and run priority. in most cases, run priority uses configuration priority, but when VRRP router is the IP address owner, run priority is 255, no configuration priority is used.

For authentication methods, switches only do not do authentication and simple password authentication two ways, but for IP authentication header mode has not been implemented.

The commands to configure the parameters of the virtual router are as follows:

| Command | Description | CLI Patterns |
|---|---|---|
| priority < priority-value > | Set the priority of a virtual router, ranging from 1 to 254. | VRRP Configuration mode |
| preempt-mode {false \| | Set the preemption mode of virtual router, TRUE means | VRRP Configuration |

| | | |
|---|---|---|
| true} | preemption, FALSE means no preemption. | mode |
| advertisement-interval <interval> | sets the announcement time interval for the virtual router, ranging from 1 to 255 in seconds. | VRRP Configuration mode |
| authentication none | Set the authentication method of virtual router to do not do authentication. | VRRP Configuration mode |
| authentication simple-password <key> | Set the authentication method of virtual router to simple password authentication, and to set authentication data, that is, password. | VRRP Configuration mode |

Note:

- The parameters to configure the virtual router must be successful when the virtual router has been turned off and can not be configured successfully when the virtual router is started.

## 1.102.4 Configuration VRRP tracking

At present, the switch only implements the VRRP interface tracking function. VRRP

the router can track a port, the interface can be a layer 2 interface or aggregation interface. the switch default does not configure the tracked interface.

VRRP the router is the IP address owner, the administrator can configure VRRP trace, but in fact the trace does not take effect, that is, the virtual master router will not be re-selected even if the virtual router has an external fault. To use VRRP tracking, do not configure virtual routers as IP address owners.

VRRP tracking takes effect when the administrator configures the VRRP trace, specifies one to trace and initiates a virtual router. when VRRP router finds an interface LINK DOWN being tracked, it is considered that there is an external fault. the running priority of the virtual router is set to source priority minus the value of the priority-value. by VRRP the interaction of the protocol package, the virtual master router can be re-selected. failure recovery when the tracked interfaces are all LINK UP, the running priority of the virtual router is reset to configuration priority.

Commands to configure VRRP trace are as follows:

| Command | Description | CLI Patterns |
|---|---|---|
| circuit-failover <if-name> <priority-value> | sets the interface the virtual router wants to track. | VRRP Configuration mode |
| no circuit-failover | clears the tracked interface of the virtual router. | VRRP Configuration mode |

Note:

Configuration VRRP tracking must be successful if the virtual router is turned off and can not be configured successfully when the virtual router is started。

## 1.102.5 Launch and close virtual routers

When the virtual router is created and the virtual IP address and parameters are set, the virtual router does not really run and is still in Initialize state. Starting a virtual router starts the protocol running, sends a Startup event to the protocol, and the state machine migrates to a Master or Backup state. Turning off the virtual router shuts down the protocol, sends a Shutdown event to the protocol, and the state moves back to the Initialize state.

A virtual IP address must be configured before starting a virtual router. If you need to modify the virtual IP address or parameters when the virtual router starts, you must close the virtual router and then configure it.

The commands to start and close the virtual router are as follows:

| Command | Description | CLI Patterns |
|---|---|---|
| enable | Launch virtual routers | VRRP Configuration mode |

| | | |
|---|---|---|
| disable | Turn off the virtual router. | VRRP Configuration mode |

## 1.102.6 View VRRP information

VRRP running status information and configuration information can be viewed through the command. The commands to view VRRP information are as follows:

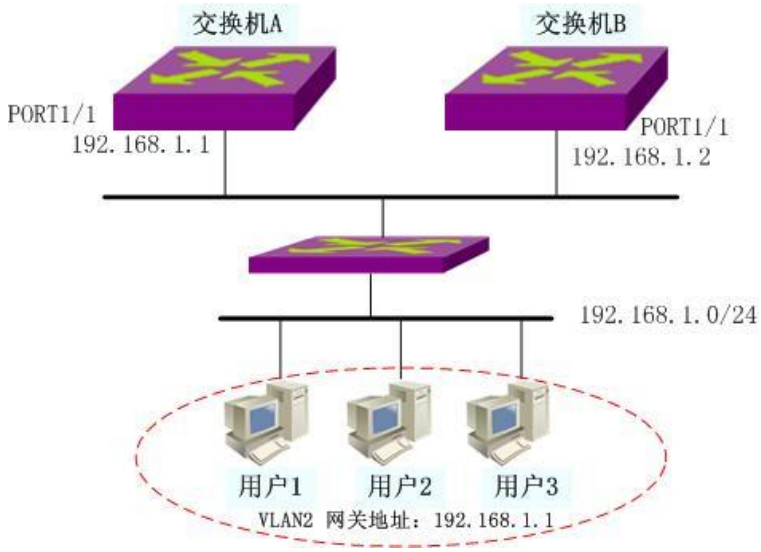
| Command | Description | CLI Patterns |
|---|---|---|
| show vrrp [vrid] | If you do not enter parameters, display information for all virtual routers. | Normal mode, privilege mode |
| show running-config | view the current configuration of the system, you can see the VRRP configuration. | Privilege mode |

# 1.103 VRRP Configuration examples

**(1 ) Configuration**

**Enable VRRP function on two switches, provide three layer routing**

**redundancy function for users in lan, eliminate routing fault in network, set switch 1 as main switch Master, switch 2 as backup switch Backup.。**




Configuration on switch A:

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/1

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

Switch(config-ge1/1)#exit

Switch(config)#ip interface vlan 2

Switch(config)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#exit

Switch(config)#router vrrp 1

Switch(config-vrrp)# virtual-interface vlan2

Switch(config-vrrp)# virtual-ip 192.168.1.1 master

Switch(config-vrrp)#enable

Configuration on switch B:

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/1

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

Switch(config-ge1/1)#exit

Switch(config)#ip interface vlan 2

Switch(config)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.2/24

Switch(config-vlan2)#exit

Switch(config)#router vrrp 1

Switch(config-vrrp)# virtual-interface vlan2

Switch(config-vrrp)# virtual-ip 192.168.1.1 backup

Switch(config-vrrp)#enable vrrp

**(2) 验证:**

通过以下命令查看VRRP的信息：

show running-config

show vrrp

show vrrp 1

# Chapter 28
# Configuration VLLP

This chapter mainly includes the following:

- VLLP presentation
- VLLP configuration
- VLLP configuration examples

## 1.104 VLLP Introduction

VLLP (VRRP layer 2 loop protection protocol VRRP Layer-2Loop Protect Protocol) is a private protocol proposed to solve the layer 2 loop problem in the application of VRRP protocol. When two layer 3 switches are used to realize redundant backup of virtual routing, the loop is formed between layer 3 switch and layer 2 switch. VLLP protocol notifies each other of the port state on their respective links through message interaction, and calculates that the loop sets the specific port state as block to cut off the loop. A port set to block state if the timer timed out and is reset to forward state. VLLP protocol monitors and maintains the loop state of the port by instantly notifying the port state change and timer timeout, and ensures that the loop is cut off in time. VLLP protocol uses query-response to collect port status information. when two layer 3 switches running the VLLP protocol are started, one is automatically elected in the sender state and the other in the receiver state. The sender is responsible for sending the query message periodically, and the receiver receives the query message and returns the reply message. When the receiver has a port state change, it needs to actively send a link state change message to notify the sender to do the phase Should change. VLLP protocol needs to work with VRRP protocol to start and maintain the relevant port status within the vlan on the vlan. VLLP protocol only needs to run on VRRP switch, and layer 2 switch does not need to run any loop protection protocol. Basic concepts of VLLP agreements:

VLLP device: a VLLP protocol entity running on a vlan is called a VLLP device.

VLLP port: a port that participates in VLLP protocol interaction within the corresponding vlan of the device.

VLLP device status: VLLP device has both sender and receiver states.

Sender: The VLLP device in the sender state actively and periodically sends VLLP query messages.

receiver: the VLLP device in the receiver state responds to the query message; when the link state changes, it actively sends VLLP link state change message.

VLLP port status: VLLP port has disable、block、forward three STP states.

main port: VLLP device is in the sender state to elect a VLLP port as the main port; one VLLP sender has only one main port. High-priority and mapped VLLP ports can be preempted as primary ports.

VLLP port mapping relationship: there are VLLP ports that interact with VLLP protocol packets on the opposite side switch.

Election principles for VLLP equipment recipients:

1. high priority to become a receiver;

2. the same priority, MAC large address become the receiver.

Main-port election principles:

1. port must be link up

2.VLLP port must have a mapping relationship

If the VLLP port does not satisfy the condition, the main port does not exist; If there are multiple VLLP ports that satisfy the criteria, select the one with high priority as the main port; if the priority is the same, select the first one to establish the mapping relationship as the main port.

VLLP Port Status Determination Principle:

VLLP the device is the sender, the state of the main port must be forward;.

VLLP device is the sender, the link state is link up and there is no mapping relationship VLLP the port state is forward.

VLLP device is the sender, the link state is link up and there is a mapping relationship VLLP the port state is block;.

VLLP device is receiver, link state is link up VLLP port state is forward;.

Link status is link down VLLP port status is disable..

<table>
<tr><td colspan="5">Destination MAC Address (6 bytes)</td></tr>
<tr><td colspan="5">Source MAC Address (6 bytes)</td></tr>
<tr><td colspan="2">0x8100</td><td>Prio</td><td>Vlan ID (12 bits)</td><td>Ethernet Type (2 bytes)</td></tr>
<tr><td>Version</td><td>Type</td><td colspan="3">Port1(2 bytes)</td></tr>
<tr><td>Priority</td><td>Query Inter</td><td colspan="3">Main port</td></tr>
<tr><td colspan="5">Reserved (4 bytes)</td></tr>
<tr><td colspan="2">Port2</td><td>Link state</td><td colspan="2">STP state</td></tr>
</table>

VLLP protocol packets have three types

LQ of Link Status Query Message

Link Status Response LA

LC of Message Change

Range of values for each domain in message format:

Des MAC： fixed at 00:09: ca：ff：ff：ff

MAC Src MAC： vlan sending protocol messages

Ethernet Type： fixed x268e 0

Version： currently 1

Type：LQ is 1; LA is 2; LC is 3;

The index value of the port Port1： the VLLP protocol message

Priority：VLLP device priority, value 1~255;

Query Interval：VLLP sender query timer interval, default 5 seconds;

Main port：VLLP sender main port index value, only in the LQ message; Reserved：retention domain zero

The index value of the port Port2：LC state change in the message is LQ consistent with the port2 and port1 in the LA message.

Link state：port2 link state, link up is 1, link down is 2;

The STP state of the STP state：port2 is 1 in disable ,2 in block and 3 in forward.

VLLP protocol principles:

the VLLP device is configured within a vlan and the VLLP protocol is started, and the VLLP device is also configured and started within the corresponding vlan of the opposite end switch. The VLLP protocol entity (VLLP device) running on the vlan then constitutes a pair of senders and receivers. When the protocol starts, both parties are senders and send LQ messages to each other. When the VLLP device receives the LQ message, it elects the receiver according to the priority carried in the message and the address to the end. The winning party becomes the receiver and no longer sends the LQ message but responds to the sender　Message. When the receiver has not received the LQ message, the receiver returns to the sender state and starts sending LQ message。

The ports involved in VLLP protocol message interaction need to be configured as VLLP ports within the vlan that started the VLLP protocol. VLLP ports can be valid tier 2 ports (including trunk groups), but members of the trunk are not allowed to be configured as VLLP ports. VLLP protocol messages are sent and received via VLLP ports. The VLLP ports and the VLLP ports configured within the vlan that initiate the VLLP protocol accordingly constitute a pair of mapping relationships, which are determined by sending a query message to receive a reply message or changing the message mapping relationship, and according to this mapping relationship and its own link state to calculate the possible existence of the loop in the network, according to the VLLP port state determination principle to maintain the STP state of the port, thus blocking the loop in the topology.

Multiple VLLP ports can be started within the vlan where the VLLP protocol is started, which may or may not be physically linked to the peer switch. the same VLLP port also appears in multiple VLLP devices when the port belongs to multiple vlan. The VLLP council dynamically collects information VLLP port link state changes and STP state to the end VLLP port to calculate the loop in time and effectively prevent the network loop.

When there are multiple vlan, whose inner port configuration is completely consistent, but the VLLP protocol needs to be started on multiple vlan, each layer 2 port needs to send and receive multiple VLLP protocol messages running on different vlan, which causes the switch burden. that is, the port configuration is exactly the same vlan, running the VLLP protocol on only one vlan, i.e., the main vlan, while the rest is added on the instance of the main vlan as a subsidiary. Write the inner port state of the instance by the result of the loop calculated by VLLP protocol on the main vlan. Note that, when configuring the accessory vlan, ensure that the VLLP ports of the main vlan are within the accessory vlan and that all ports of the accessory vlan are within the primary. when the attached vlan, is configured to add a second layer port to the attached vlan, if the port is also in the main vlan, the port state is uniformly managed by the main vlan; if the port is not in the main vlan, the port state can not be managed, prompting alarm information.

## 1.10528.2 VLLP configuration

After starting the VLLP protocol, the related property configuration and port creation can be carried out, and the related commands are in VLLP configuration mode.

VLLP configuration includes:

- Create vllp devices on the three-tier interface
- Enable vllp equipment
- Create vllp ports on tier 2 interfaces
- Configuration vllp Device Priority
- Configuration vllp Device Query Timer Interval

- Configuration vlan
- Configuration vllp Port Priority

## 1.105.1 Create vllp devices on the three-tier interface

Mode: Global Configuration Mode

Command: router vllp <if-name> create vllp device and enter VLLP configuration mode

Command: no router vllp <if-name> delete vllp device

Parameter: if-name is the agreed three-tier interface name (e.g. vlan1vlan2…)

Default: vllp protocol not started

## 1.105.2 Enable vllp equipment

Mode: VLLP Configuration Mode

Order: vllp enable enable vllp equipment

Order: vllp disable prohibit vllp equipment

Default: vllp device was not started after it was created

## 1.105.3 Create vllp ports on tier 2 interfaces

Mode: VLLP Configuration Mode

Command: vllp port <if-name> create vllp port

Command: no vllp port <if-name> delete vllp port

Parameter: if-name is the agreed two-tier interface name (e.g. ge1/1trunk1…)

Default: vllp protocol is not applied on tier 2 ports. vllp protocols can not be applied when a layer 2 interface is a trunk member.

## 1.105.4 Configuration vllp Device Priority

Mode: VLLP Configuration Mode

Command: vllp priority <priority> configuration vllp device priority

Command: no vllp priority [priority] recovery vllp device priority is default

parameter: the priority value is between 1~255. priority is used to select the receiver vllp the device.

Default :100

## 1.105.5 Configuration vllp Device Query Timer Interval

Mode: VLLP Configuration Mode

Command: vllp query-interval <interval> configure the local query timer interval

Command: no vllp query-interval [interval] restore query timer interval is default

Parameter: The interval value is between 1~255. Configuration values take effect when vllp device is a sender or when it migrates back to the sender.

Default :5 seconds

## 1.105.6 Configuration vlan

Mode: VLLP Configuration Mode

Command: vllp dependency <if-name> configuration vlan

Order: no vllp dependency <if-name> remove vlan appendages

Parameter: if-name is the agreed three-tier interface name (e.g. vlan1vlan2…)

Default: Dependent vlan not configured

## 1.105.7 Configuration vllp Port Priority

Mode: VLLP Configuration Mode

Command: vllp port <if-name>priority <priority> configuration vllp port priority

Command: no vllp port <if-name>priority [priority] recovery vllp port priority is default

parameter: if-name is the agreed two-tier interface name (e.g.: ge1/1trunk1…); the priority value is between 1~255. priority is used vllp the sender to elect the main port.

Default :100

## 1.105.8 Display information

Mode: Normal or privileged mode

Command: show vllp

List of vllp devices showing vllp protocols

Command: show vllp <if-name>

Display details of a vllp device

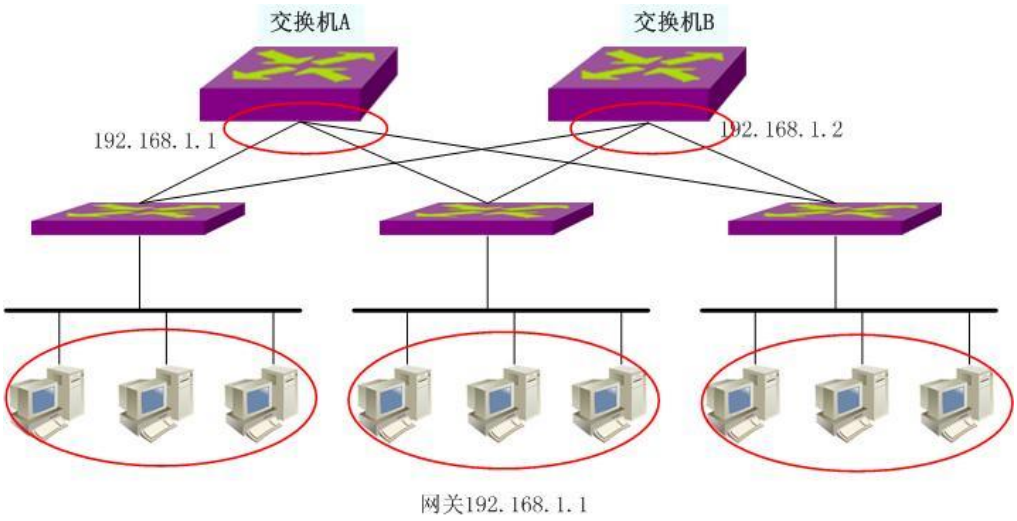
Parameter: if-name is the agreed three-tier interface name (e.g. vlan1vlan2…)

Command: show vllp map

Shows the mapping relationships of vlip ports in the vlip protocol

# 1.106 VLLP Configuration examples

**(1) Configuration**




Configuration on switch A:

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#ip interface vlan 2

Switch(config)#interface ge1/1

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

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

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

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

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

Switch(config-ge1/3)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#exit

Switch(config)#router vrrp 1

Switch(config-vrrp)# virtual-ip 192.168.1.1 master

Switch(config-vrrp)#enable

Switch(config-vrrp)#exit

Switch(config)#router vllp vlan2

Switch(config-vllp)#vlllp port ge1/1

Switch(config-vllp)#vllp port ge1/2

Switch(config-vllp)#vllp port ge1/3

Switch(config-vllp)#vllp enable

Configuration on switch B:

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config)#ip interface vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/1

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

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

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

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

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

Switch(config-ge1/3)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.2/24

Switch(config-vlan2)#exit

Switch(config)#router vrrp 1

Switch(config-vrrp)# virtual-ip 192.168.1.1 backup

Switch(config-vrrp)#virtual-interface vlan1

Switch(config-vrrp)#enable

Switch(config-vrrp)#exit

Switch(config)#router vllp vlan2

Switch(config-vllp)#vlllp port ge1/1

Switch(config-vllp)#vllp port ge1/2

Switch(config-vllp)#vllp port ge1/3

Switch(config-vllp)# enable

**(2) Verification**

View VLLP information using the following command:

show vllp

show vllp <if-name>

show vllp map

# Chapter 29 Configuration Policy Routing

This chapter mainly includes the following:

- Introduction of Strategy Routing
- Policy Routing Configuration
- Policy Routing Configuration Example

## 1.107 Introduction of Strategy Routing

Policy routing (policy-based-route) is a mechanism for routing selection based on the policies formulated by users. Different from the routing table based on the destination address of the IP message, the policy routing is based on some attributes of the message information, such as destination address, source address and so on. Rich knowledge of router routing.

## 1.108 Policy Routing Configuration

The configuration includes the following:

- Create new policy routing
- Insert a policy route
- Delete a policy route
- Moving a Policy Route
- View Policy Routing Information

### 1.108.1 Create new policy routing

The following command creates a new policy route in global configuration mode:

policy route <ID> <SIP> <DIP> <next-hop>

ID： represents the newly created policy routing rule ID, range 1-100.

SIP, DIP： Source IP has three types of input:

1)A.B.C.D wildcard Can control IP addresses from a segment；

2)any The equivalent of A.B.C.D 255.255.255.255

3)host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

wildcard：Decide which bits need to match ,'0' means need to match ,'1' means need not match.

next-hop：Represents the next hop host address in A.B.C format. D.

## 1.108.2 Insert a policy route

The following command inserts a new policy route in global configuration mode:

policy route insert <ID> <SIP> <DIP> <next-hop> before <EXIST_ID>

ID：denotes the policy rule ID, range 1-100 for the new insert.

SIP, DIP：A source IP has three types of input:

1)A.B.C.D wildcard Can control the IP address from a network segment;

2)any The equivalent of A.B.C.D 255.255.255.255

3)host A.B.C. D is equivalent to A.B.C.

wildcard： Decide which bits need to match ,'0' means need to match ,'1' means need

not match.

next-hop：Represents the next hop host address in A.B.C format. D.

EXIST_ID：indicates which rule to insert before, range 1-100.

## 1.108.3 Delete a policy route

The following command removes a policy route in global configuration mode:

no policy route <ID>

ID： Represents the range of policy rules to be deleted ID,1-100.

## 1.108.4 Moving a Policy Route

The following command moves the policy route to the destination in global configuration mode:

policy route move <ID> (before|after) <TO_ID>

ID：indicates the rules that need to move.

(before|after)： Represents before or after a moving target rule:

## 1.108.5 View Policy Routing Information

The following commands are executed in normal or privileged mode to view all policy routing information:

show policy route

# 1.109 Policy Routing Configuration Example

Configure the source IP address 192.168.3.100, go to the gateway 192.168.0.20.

Switch#configure terminal

Switch#(config)#policy route 1 host 192.168.3.100 any 192.168.0.20

Configure the destination IP address 192.168.10.100, go to the gateway 192.168.2.1.

Switch#configure terminal

Switch#(config)#policy route 2 any host 192.168.10.100 192.168.2.1

Configure source IP address 192.168.3.100, destination IP address 10.10.10.100, go to gateway 192.168.5.1.

Switch#configure terminal

Switch#(config)#policy route 3 host 192.168.3.100 host 10.10.10.100 192.168.5.1

# Chapter 30 Configure the system log

This chapter mainly includes the following:

- System Log Introduction
- System log configuration

## 1.110 System Log Introduction

The system log module is an important part of the switch, which is used to record the operation of the whole system, abnormal behavior and user's operation behavior, and help the administrator to understand and monitor the work of the system in time. The system log module manages all the log information of the system from the running modules, collecting, classifying, storing and displaying the log information.

Also an important debugging function in the logging system. system logs work with debugging to help administrators or other technicians monitor the operation of the network, debug and diagnose faults in the network. Administrators can easily select the content that needs debugging, by observing the log information output by the debugging, to locate and solve the fault of the device or network.

This section mainly includes the following:

- Format of log information
- Storage of logs
- Log display
- Debugging tools

### 1.110.1 The format of the log information

The format of the log information is as follows:

Timestamp Priority: Module name: log content

There is a space between the timestamp and the priority, a colon and a space between the priority and the module name, and a colon and a space between the module name and the log content.Examples of the format of the log information are as follows:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

In this log message, the timestamp is 2006/05/20 13:56:34;The priority is Warning;The module name is MSTP;The log content is Port up Notification Received for Port ge1/2.

1 ) The time stamp

Time stamp format: year/month/day hour: minutes: seconds.

The hours are 24 hours, from 0 to 23 hours.

The timestamp records the time when this log message was generated, using the system time of the switch.The system time has been set before the switch leaves factory, and the administrator can also modify it. The system time can still run after the device is disconnected.

2 ) Priority

According to the importance of the log information, the log information is classified into four levels. The order of priority from high to low is Critical, Warning, aantion and Debugging.The priority is described in the following table:

| Priority | Describe |
| --- | --- |

| | |
|---|---|
| Critical | Grave error |
| Warning | General errors, warnings, very important tips |
| Informational | Important tips, general tips, diagnostic information |
| Debugging | Debugging information |

3 ) Module name

The module name records the modules from which this log information is generated. The following table lists some of the main modules from which this log information is generated:

| Module name | Describe |
|---|---|
| CLI | Command line interface module |
| MSTP | Multi-instance spanning tree protocol module |
| VLAN | VLAN function module |
| ARP | ARP protocol module |
| IP | IP Protocol module |
| ICMP | ICMP protocol module |
| UDP | UDP protocol module |

| | |
|---|---|
| TCP | TCP protocol module |

4 ) Log contents

The log content is a phrase or sentence that represents the general idea of the log information. By reading the log content, the administrator can know what is happening in the system.

## 1.110.2 Log storage

- Logs are generally stored in three ways, namely:
- The logs are stored in memory.
- Logs are stored in the NVM.
- The logs are stored on the server

According to the priority of the log, there are four log tables in memory, and each table holds the log information of a priority. In other words, the logs are divided into four types according to the priority of the log, and each type of log is stored in a separate log table.Each log table has 1K entries, which can store 1K log information. When the log table is full, the log information that covers the longest time in the following logs.One problem with this storage is that when the system is rebooted, the log information is gone and the administrator cannot see the log information and locate the problem in the event of a system crash.

For important log information, such as those with a priority of Critical and Warning, this log information can be stored in the NVM of the system.This storage allows the log

information in the NVM to be retained after a system restart, allowing administrators to locate problems in the event of a system crash.One problem with this storage is that there are very few log entries stored in the NVM due to capacity constraints.

A better approach is to store the log information in the server, which can be implemented using the SYSLOG protocol. The log information can be sent to the server in real time. The server saves the log information and displays it in an interface.This storage mode is not only convenient for users to view log information, but also has a large capacity, which can store a large number of log information on the server.

Currently, the system only supports storing log information in memory, not in NVM or server.

### 1.110.3 Display of logs

Logs are displayed in two ways: manually and in real time.Manual display means that the user displays the log information by inputting commands, and real-time display means that when log information is generated, the log information is directly output to the terminal so that the user can see it in time.

For manual display, the user can view all the log information in the order that the last log information generated is displayed first, so that the user can see the latest running state of the switch first.

For real-time display, the user must turn on the terminal real-time display switch.If the switch is on, the resulting log information is not only written to the log table, but also output to the terminal. If the switch is off, the log information is not displayed in real time on the terminal.At present, the system can only output log information to the Console terminal in real time, but it does not support output log information to the Telnet terminal.

### 1.110.4 Debugging tool

Debugging is a diagnostic tool used for the equipment and network to track the packet transmission of the system and module, and the change of the state machine of the module, etc. It enables the administrator to understand and monitor the operation process of the system and module. If abnormal situation occurs with the network or the device, it can be traced with debugging.

The debugging tool provides rich switches that enable administrators to track content of interest by controlling these switches.When abnormalities occur to the device or network, the administrator can turn on debugging switch related to the abnormality and find out the problem by tracking the execution process of the system and module.

When this switch is turned on, the system generates logging information that is written to the corresponding log table.In general, the priority of logging produced by debugging is a anteage.When the terminal real-time display switch is on, the log information will be output to the terminal in real time.The system does not generate the associated logging information when the debugging switch is turned off.

## 30.2 System log configuration

- System log configuration includes the following:
- Configure terminal real - time display switch

- View log information
- Configuring debugging switch
- View debugging information

## 1.110.5 Configure the terminal real-time display switch

By default, the terminal real-time display switch is off, and the log information generated by the system is written to the log table, but not displayed on the terminal in real time.There are also some log messages in the system that are not restricted by this switch and will always be output to the Console terminal in real time.

Currently, the switch can only display real-time log information on the Console terminal, but cannot display real-time log information on the Telnet terminal.

When the user USES the write command to store the current configuration of the system in the configuration file, the configuration of the terminal real-time display switch will not be stored in the configuration file of the system. After the system restarts, these configurations will be lost and need to be reconfigured.

The commands to configure the terminal real-time display switch are shown in the following table:

| Command | Describe | CLIP mode |
|---|---|---|
| log stdout | Turn on the terminal real-time display switch. | Global configuration mode |
| no log stdout | Turn off terminal real - | Global |

| | | |
|---|---|---|
| | time display switch. | configuration mode |

## 1.110.6 Set the log level

The commands to set the log level are shown in the following table:

| Command | Describe | CLIP mode |
|---|---|---|
| log trap <[alerts \| critical \| debugging \| emergencies \| errors \| informational \| notifications \| warnings]> | Set the log level | Global configuration mode |

## 1.110.7 View log information

The commands to view log information are shown in the following table:

| Command | Describe | CLIP mode |
|---|---|---|
| show log | Displays all log | Global |

| | | |
|---|---|---|
| | information. | configuration mode |

## 1.110.8 Configuring debugging switch

The system is provided with rich debugging switch which is involved with multiple modules. Here only lists the schematic command of each module. For the complete format of the command, please refer to the command manual.

When the user stores the current configuration in the configuration file using the write command, the debugging switch configuration will not be stored in the configuration file. This configuration will be lost when the system reboots and needs to be reconfigured.

Configure the debugging switch with the following command:

| Command | Describe | CLIP mode |
|---|---|---|
| debug ip … | Turn on the relevant debugging switch for sending and receiving IP packets. | Privileged mode |
| no debug ip … | Turn off the relevant debugging switch for the system's TRANSCeiver IP packet. | Privileged mode |
| debug ip icmp … | Turn on the relevant | Privileged |

| | | |
|---|---|---|
| | debugging switch for the system's ICMP packet. | mode |
| no debug ip icmp … | Turn off the system transceiver by the related debugging switch of the ICMP packet. | Privileged mode |
| debug ip arp … | Turn on the system to transmit the ARP packet by the relevant debugging switch. | Privileged mode |
| no debug ip arp … | Turn off the system transceiver the ARP packet by the related debugging switch. | Privileged mode |
| debug ip udp … | Turn on the system to transmit the UDP packet with the relevant debugging switch. | Privileged mode |
| no debug ip udp … | Turn off the system's sending and receiving UDP packet by the related debugging switch. | Privileged mode |

| | | |
|---|---|---|
| debug ip tcp … | Turn on the debugging switch associated with sending and receiving TCP packets in the system. | Privileged mode |
| no debug ip tcp … | Turn off the relevant debugging switch for sending and receiving TCP packets in the system. | Privileged mode |
| debug mstp … | Turn on the RELATED debugging switch for MSTP protocol diagnosis. | Privileged mode |
| no debug mstp … | Turn off the MSTP protocol diagnostic associated with the debugging switch. | Privileged mode |
| debug igmp snooping … | Turn on the IGMP SNOOPING function to diagnose the associated debugging switch. | Privileged mode |
| no debug igmp snooping … | Turn off the IGMP SNOOPING function to | Privileged mode |

| | | |
|---|---|---|
| | diagnose the associated debugging switch. | |
| debug dhcp snooping … | Turn on the relevant debugging switch for DHCP SNOOPIN protocol diagnosis | Privileged mode |
| no debug dhcp snooping … | Turn off the DHCP SNOOPIN protocol diagnostic associated with the debugging switch | Privileged mode |
| no debug all | Turn off all the debugging switches in the system. | Privileged mode |

## 1.110.9 To view the debugging information

To view the debugging information, click here:

| Command | Describe | CLImode |
|---|---|---|
| show debugging [dhcp snooping \| erps \| igmp snooping \| ip \| mstp \| rip ] | View the debugging switch configuration.If there is no input parameter, view the debugging switch configuration for all the | Normal mode, privileged mode |

| | | |
|---|---|---|
| | modules; if only one of the parameters is entered, view only one module's debugging switch configuration.If the input parameter is IP, the debugging switch configuration for IP, ICMP, ARP, UDP, TCP module will be viewed. | |

# 1.111Configuration SYSLOG

SYSLOG Including the following:

- SYSLOG introduce
- SYSLOG configuration
- SYSLOG configuration of the sample

## 1.111.1 SYSLOG introduce

SYSLOG is a standard protocol for managing device log information, and it has gained great application due to its simplicity of design.In the SYSLOG system, there are three parts.One is to define each submodule to distinguish the log information

generated by different modules.Define different levels of log information to view the health of the device.The various log messages of the device are gathered according to this convention.The other is the configuration file, which defines how to deal with the collected log information. It can be saved locally, sent centrally to the designated server on the network, distributed to the designated logon user and so on. It is up to the configuration file to determine how to hold the log information generated by the device.Third, SYSLOG protocol messages are sent according to the message format defined by RFC.As you can see, in our switch system, the entire SYSLOG work convention is the system log module.The first part of SYSLOG protocol is completed by each functional submodule in the switch, sending each level of log information to the system log module.Maintains four levels of log tables in the system log module.The second part of SYSLOG protocol is distributed by the system log module. The first part is displayed on the serial port terminal in real time or manually through the terminal display switch.Two is to keep four levels of log table in memory;The third is to keep high-level log information on NVM to avoid losing important log records in case of power failure.Fourth, the logs are sent to the remote server to be saved, collected and sorted through SYSLOG message.The SYSLOG submodule in the system log module implements only the third part of the function to send the system log to the server.

## 1.111.2 SYSLOG configuration

The SYSLOG configuration command contains：

- Open the syslog server address
- Close the syslog server address
- Open the syslog protocol

| Command | Describe | CLI model |
| --- | --- | --- |
| syslog open <server-ip> | Open the syslog server address;The parameter server-IP is the server IP address | Global configuration mode |
| syslog close | Close the syslog server address | Global configuration mode |
| log syslog | Open the syslog protocol | Global configuration mode |

## 1.111.3 SYSLOG Configuration of the sample

Configure

Configure syslog server IP address to 192.168.0.201, and configure the switch as follows:

Switch#configure terminal

Switch(config)#syslog open 192.168.0.201

Switch(config)# log syslog

( 1 ) Verification

Switch#show syslog

Syslog is opened!

server ip address: 192.168.0.201

udp destination port: 514

severity level: debugging

local device name: switch