

---

# Table of Contents

|   |    |
|---|----|
| Table of Contents .....                               | 1  |
| Chapter1 Introduction to CLI command line.....        | 14 |
| 1.1 Accessing the Switch CLI .....                    | 15 |
| 1.1.1 Users access CLI through the console port ..... | 15 |
| 1.1.2 Users access CLI through TELNET.....            | 16 |
| 1.2 Introduction to CLI mode.....                     | 18 |
| 1.2.1 Function of CLI mode.....                       | 18 |
| 1.2.2 Identification of CLI model .....               | 18 |
| 1.2.3 Classification of CLI mode .....                | 19 |
| 1.3 Introduction to Command syntax .....              | 21 |
| 1.3.1 Command composition .....                       | 21 |
| 1.3.2 Parameter Type.....                             | 21 |
| 1.3.3 Command syntax rules.....                       | 21 |
| 1.3.4 Command abbreviations.....                      | 23 |
| 1.3.5 Grammar Help.....                               | 23 |
| 1.3.6 Command line error messages .....               | 24 |
| 1.4 Command line shortcuts .....                      | 24 |
| 1.4.1 Line edit shortcut .....                        | 24 |
| 1.4.2 Show command Shortcut .....                     | 25 |
| 1.5 Historical Command.....                           | 26 |
| Chapter2 System management configuration .....        | 26 |
| 2.1 System security configuration .....               | 27 |
| 2.1.1 Multi-user management control .....             | 27 |
| 2.1.2 Enable password control .....                   | 28 |
| 2.1.3 TELNET Service control .....                    | 29 |
| 2.1.4 SNMP Service control.....                       | 30 |
| 2.1.5 HTTP Service control.....                       | 31 |
| 2.2 System maintenance and commissioning.....         | 32 |
| 2.2.1 Configuring the system clock.....               | 32 |
| 2.2.2 Configure terminal timeout attributes .....     | 33 |
| 2.2.3 System reset .....                              | 33 |
| 2.2.4 View system information .....                   | 34 |
| 2.2.5 Network connectivity debugging.....             | 34 |
| 2.2.6 Traceroute debugging.....                       | 35 |

|  |    |
|--|----|
| 2.2.7 Telnet client .....                                      | 36 |
| 2.3 Configuration file management .....                        | 36 |
| 2.3.1 View configuration information .....                     | 37 |
| 2.3.2 Save configuration .....                                 | 37 |
| 2.3.3 Delete configuration file .....                          | 38 |
| 2.3.4 Configuration file download/upload .....                 | 38 |
| 2.4 Software version upgrade .....                             | 41 |
| 2.4.1 Command of software version upgrade .....                | 41 |
| 2.4.2 Software upgrade process .....                           | 42 |
| Chapter3 Port configuration.....                               | 45 |
| 3.1 Common port configuration .....                            | 46 |
| 3.1.1 Port opening and closing.....                            | 46 |
| 3.1.2 Port speed configuration .....                           | 46 |
| 3.1.3 Show port information .....                              | 47 |
| 3.2 MIRROR configuration.....                                  | 47 |
| 3.2.1 MIRROR monitor / monitored port configuration.....       | 47 |
| 3.2.2 Show MIRROR configuration .....                          | 48 |
| 3.3 STORM-CONTROL configuration.....                           | 49 |
| 3.3.1 Default configuration .....                              | 49 |
| 3.3.2 Broadcast suppression configuration .....                | 49 |
| 3.3.3 Multicast suppression configuration .....                | 50 |
| 3.3.4 DLF suppression configuration.....                       | 50 |
| 3.3.5 Suppression rate configuration.....                      | 50 |
| 3.3.6 Show STORM-CONTROL configuration .....                   | 51 |
| 3.4 STORM-CONSTRAIN configuration.....                         | 51 |
| 3.5 配置 FLOW-CONTROL.....                                       | 53 |
| 3.5.1 Default configuration .....                              | 54 |
| 3.5.2 Set port flow control .....                              | 54 |
| 3.5.3 Close port flow control.....                             | 54 |
| 3.5.4 Show flow control information .....                      | 54 |
| 3.6 Port bandwidth configuration .....                         | 55 |
| 3.6.1 Default configuration .....                              | 55 |
| 3.6.2 Configure port to send or receive bandwidth control..... | 55 |
| 3.6.3 Cancel port to send or receive bandwidth control.....    | 56 |
| 3.6.4 Show the bandwidth control of port configuration .....   | 56 |
| 3.7 TRUNK configuration.....                                   | 56 |
| 3.7.1 LACP protocol configuration.....                         | 57 |

|  |    |
|--|----|
| 3.7.2 TRUNK group configuration .....                    | 58 |
| 3.7.3 TRUNK member port configuration .....              | 59 |
| 3.7.4 TRUNK load balancing strategy configuration.....   | 60 |
| 3.7.5 Show TRUNK.....                                    | 60 |
| 3.8 Jumbo frames configuration .....                     | 60 |
| 3.8.1 Introduction to Jumbo Frames .....                 | 60 |
| 3.8.2 Jumbo Frame configuration .....                    | 61 |
| 3.9 Redundant ports configuration .....                  | 61 |
| 3.9.1 Redundant ports configuration.....                 | 61 |
| 3.9.2 Display of redundant ports .....                   | 63 |
| 3.10 DLDAP configuration.....                            | 63 |
| 3.11 LLDP configuration.....                             | 64 |
| 3.11.1 LLDP configuration .....                          | 64 |
| 3.11.2 LLDP display .....                                | 65 |
| Chapter4 Configure port-based MAC security .....         | 66 |
| 4.1 Introduction .....                                   | 67 |
| 4.2 MAC binding configuration .....                      | 67 |
| 4.3 MAC filtering configuration.....                     | 68 |
| 4.4 Port learning limit configuration .....              | 69 |
| 4.5 Port protection configuration.....                   | 70 |
| 4.5.1 Introduction to port protection configuration..... | 70 |
| 4.5.2 Port protection configuration .....                | 71 |
| Chapter5 Configure port IP and MAC binding .....         | 72 |
| 5.1 Introduction .....                                   | 73 |
| 5.2 IP / MAC binding configuration.....                  | 73 |
| 5.3 Configuration example .....                          | 74 |
| 5.4 Configuration Debug.....                             | 76 |
| Chapter6 Port loop detection .....                       | 76 |
| 6.1 Introduction .....                                   | 77 |
| 6.2 Protocol principle .....                             | 77 |
| 6.2.1 Testing process.....                               | 77 |
| 6.2.2 Recovery mode .....                                | 77 |
| 6.2.3 Protocol security .....                            | 77 |
| 6.3 Configuration Introduction.....                      | 78 |
| 6.3.1 Global configuration .....                         | 78 |
| 6.3.2 Interface configuration.....                       | 79 |
| 6.3.3 Show configuration.....                            | 79 |

|  |     |
|--|-----|
| Chapter7 VLAN configuration .....                        | 80  |
| 7.1 VLAN Introduction .....                              | 81  |
| 7.1.1 Benefits of VLAN .....                             | 81  |
| 7.1.2 VLAN ID .....                                      | 82  |
| 7.1.3 VLAN port member type .....                        | 83  |
| 7.1.4 The default VLAN of the port.....                  | 83  |
| 7.1.5 Port VLAN Mode.....                                | 83  |
| 7.1.6 VLAN Trunk .....                                   | 84  |
| 7.1.7 Data flow forwarding in VLAN.....                  | 85  |
| 7.2 VLAN configuration .....                             | 86  |
| 7.2.1 Creat and delete VLAN.....                         | 87  |
| 7.2.2 Port VLAN mode configuration.....                  | 87  |
| 7.2.3 VLAN configuration in ACCESS Mode.....             | 88  |
| 7.2.4 VLAN configuration in TRUNK mode.....              | 89  |
| 7.2.5 VLAN configuration in HYBRID mode.....             | 90  |
| 7.2.6 View VLAN information .....                        | 92  |
| 7.3 VLAN configuration example.....                      | 92  |
| 7.3.1 PORT based VLAN.....                               | 92  |
| 7.3.2 802.1Q based VLAN.....                             | 94  |
| 7.4 MAC, IP subnet, protocol VLAN.....                   | 96  |
| 7.4.1 Introduction to MAC、 IP subnet、 protocol VLAN..... | 96  |
| 7.4.2 MAC、 IP subnet、 protocol VLAN configuration .....  | 96  |
| 7.5 Voice VLAN.....                                      | 98  |
| 7.5.1 Voice VLAN introduction .....                      | 98  |
| 7.5.2 Voice VLAN configuration .....                     | 98  |
| 7.5.3 Voice VLAN configuration example.....              | 100 |
| 7.6 VLAN mapping.....                                    | 101 |
| 7.6.1 VLAN mapping introduction .....                    | 101 |
| 7.6.2 VLAN mapping configuration .....                   | 101 |
| 7.7 QinQ.....  | 102 |
| 7.7.1 Qinq introduction .....                            | 102 |
| 7.7.2 Qinq configuration .....                           | 104 |
| 7.7.3 Qinq configuration example.....                    | 105 |
| Chapter8 QoS configuration .....                         | 107 |
| 8.1 QoS introduction .....                               | 108 |
| 8.1.1 COS-based QoS .....                                | 109 |
| 8.1.2 DSCP-based QoS .....                               | 110 |

|  |     |
|--|-----|
| 8.1.3 MAC-based QoS .....  | 110 |
| 8.1.4 Policy-based QOS .....   | 110 |
| 8.2 QoS configuration .....  | 110 |
| 8.2.1 QoS default configuration .....                                      | 110 |
| 8.2.2 Configure scheduling .....   | 111 |
| 8.2.3 Configure queue weight .....   | 112 |
| 8.2.4 Configure the mapping relationship between DSCP and QoSProfile ..... | 112 |
| 8.2.5 Configure Port DSCP-based QoS .....                                  | 112 |
| 8.2.6 Configure port user priority (COS merit) .....                       | 113 |
| 8.3 QoS configuration example .....  | 113 |
| 8.4 Policy QoS configuration example .....                                 | 114 |
| Chapter9 MSTP configuration .....  | 115 |
| 9.1 MSTP introduction .....  | 115 |
| 9.1.1 Overview .....   | 115 |
| 9.1.2 Multiple spanning tree domain .....                                  | 115 |
| 9.1.3 IST, CIST and CST .....  | 116 |
| 9.1.4 Intra-domain operations .....  | 116 |
| 9.1.5 Interdomain operations .....   | 117 |
| 9.1.6 Hop count .....  | 118 |
| 9.1.7 Border port .....  | 118 |
| 9.1.8 Interoperability of MSTP and 802.1d STP .....                        | 119 |
| 9.1.9 Port role .....  | 119 |
| 9.1.10 Introduction to 802.1D Spanning tree .....                          | 121 |
| 9.2 MSTP configuration .....   | 123 |
| 9.2.1 Default configuration .....  | 123 |
| 9.2.2 General configuration .....  | 124 |
| 9.2.3 Domain configuration .....   | 126 |
| 9.2.4 Instance configuration .....   | 127 |
| 9.2.5 Port configuration .....   | 128 |
| 9.2.6 PORTFAST related configuration .....                                 | 130 |
| 9.2.7 Root Guard related configuration .....                               | 132 |
| 9.3 MSTP configuration example .....                                       | 133 |
| Chapter10 ERPS configuration .....   | 135 |
| 10.1 ERPS description .....  | 135 |
| 10.2 ERPS technology introduction .....                                    | 135 |
| 10.2.1 ERPS ring .....   | 135 |
| 10.2.2 ERPS node .....   | 136 |

|  |     |
|--|-----|
| 10.2.3 Links and channels.....                                       | 136 |
| 10.2.4 ERPS VLAN.....  | 137 |
| 10.3 ERPS working principle.....                                     | 137 |
| 10.3.1 normal status .....   | 137 |
| 10.3.2 Link failure .....  | 138 |
| 10.3.3 Link recovery .....   | 138 |
| 10.4 ERPS technical characteristics .....                            | 139 |
| 10.4.1 ERPS load balancing.....                                      | 139 |
| 10.4.2 Good security .....   | 140 |
| 10.4.3 Support multi-ring intersection and tangent.....              | 140 |
| 10.5 ERPS protocol commands.....                                     | 141 |
| 10.6 Typical application of ERPS .....                               | 143 |
| 10.6.1 Single ring example .....                                     | 143 |
| 10.6.2 Multi-ring example .....                                      | 146 |
| 10.6.3 Multi-instance load balancing example .....                   | 152 |
| Chapter11 AAA configuration.....                                     | 161 |
| 11.1 802.1x introduction.....  | 162 |
| 11.1.1 802.1x device composition.....                                | 162 |
| 11.1.2 Brief introduction of protocol package .....                  | 164 |
| 11.1.3 Protocol flow interaction.....                                | 165 |
| 11.1.4 802.1x port status .....                                      | 167 |
| 11.2 RADIUS introduction.....  | 168 |
| 11.2.1 Brief introduction of protocol package .....                  | 169 |
| 11.2.2 Protocol flow interaction.....                                | 170 |
| 11.2.3 User authentication method.....                               | 171 |
| 11.3 802.1x configuration.....                                       | 172 |
| 11.3.1 802.1x default configuration .....                            | 172 |
| 11.3.2 Start and shut down 802.1x .....                              | 173 |
| 11.3.3 Configure 802.1x port status .....                            | 173 |
| 11.3.4 Configure the re-authentication mechanism.....                | 174 |
| 11.3.5 Configure the maximum number of port access hosts .....       | 175 |
| 11.3.6 Configure interval time and retransmission times.....         | 176 |
| 11.3.7 Configure the port as a transmission port.....                | 176 |
| 11.3.8 Configure the 802.1x client version number .....              | 177 |
| 11.3.9 Configure whether to check the client version number.....     | 177 |
| 11.3.10 Configure authentication method.....                         | 177 |
| 11.3.11 Configure whether to check the client's timing package ..... | 178 |

|   |     |
|---|-----|
| 11.3.12 Display 802.1x information .....                          | 178 |
| 11.4 RADIUS configuration.....                                    | 179 |
| 11.4.1 RADIUS default configuration .....                         | 179 |
| 11.4.2 Configure the IP address of the authentication server..... | 179 |
| 11.4.3 Configure shared key .....                                 | 180 |
| 11.4.4 Turn billing on and off .....                              | 180 |
| 11.4.5 Configure RADIUS port and attribute information.....       | 181 |
| 11.4.6 Configure RADIUS roaming .....                             | 181 |
| 11.4.7 Display RADIUS information.....                            | 182 |
| 11.5 Configuration example .....                                  | 182 |
| Chapter12 GMRP configuration .....                                | 183 |
| 12.1 GMRP introduction .....                                      | 183 |
| 12.2 GMRP configuration .....                                     | 184 |
| 12.2.1 Open GMRP settings .....                                   | 184 |
| 12.2.2 View GMRP information .....                                | 184 |
| 12.3 GMRP typical configuration example.....                      | 185 |
| Chapter13 IGMP SNOOPING configuration .....                       | 186 |
| 13.1 IGMP SNOOPING introduction .....                             | 186 |
| 13.1.1 IGMP SNOOPING process .....                                | 187 |
| 13.1.2 Layer 2 dynamic multicast.....                             | 188 |
| 13.1.3 Join a group.....  | 188 |
| 13.1.4 Leave a group.....   | 190 |
| 13.1.5 IGMP Query.....  | 191 |
| 13.1.6 Igmp snooping multicast filtering .....                    | 192 |
| 13.2 IGMP SNOOPING configuration .....                            | 192 |
| 13.2.1 IGMP SNOOPING default configuration .....                  | 192 |
| 13.2.2 Enable and disable IGMP SNOOPING .....                     | 192 |
| 13.2.3 Configure time to live .....                               | 193 |
| 13.2.4 Fast-leave configuration.....                              | 193 |
| 13.2.5 MROUTER configuration .....                                | 194 |
| 13.2.6 配置 igmp snooping 查询端口功能..... 오류! 책갈피가 정의되어 있지 않습니다.        |     |
| 13.2.7 Configure igmp snooping query function .....               | 194 |
| 13.2.8 Configure igmp snooping multicast filtering .....          | 195 |
| 13.2.9 Display information .....                                  | 195 |
| 13.3 IGMP SNOOPING configuration example.....                     | 196 |
| 13.3.1 configuration.....   | 196 |
| Chapter14 MVR configuration .....                                 | 197 |

|   |     |
|---|-----|
| 14.1 MVR introduction .....   | 197 |
| 14.2 MVR configuration .....  | 198 |
| 14.3 MVR configuration example.....                                       | 198 |
| Chapter15 DHCP SNOOPING configuration.....                                | 200 |
| 15.1 DHCP SNOOPING introduction.....                                      | 201 |
| 15.1.1 DHCP SNOOPING process.....   | 201 |
| 15.1.2 DHCP SNOOPING binding table.....                                   | 202 |
| 15.1.3 DHCP SNOOPING specifies the physical port of the link server ..... | 203 |
| 15.2 DHCP SNOOPING configuration.....                                     | 203 |
| 15.2.1 DHCP SNOOPING default configuration .....                          | 203 |
| 15.2.2 Turning DHCP SNOOPING on and off globally.....                     | 203 |
| 15.2.3 Interface to turn DHCP SNOOPING on and off.....                    | 204 |
| 15.2.4 Interface opening and closing DHCP SNOOPING OPTION82 .....         | 204 |
| 15.2.5 Display information .....  | 205 |
| 15.3 DHCP SNOOPING configuration example .....                            | 205 |
| 15.3.1 configuration.....   | 205 |
| 15.4 DHCP SNOOPING configuration troubleshooting.....                     | 207 |
| Chapter16 DHCP CLIENT configuration.....                                  | 208 |
| 16.1 DHCP CLIENT introduction.....  | 208 |
| 16.2 DHCP CLIENT configuration.....                                       | 208 |
| Chapter17 DHCP RELAY configuration .....                                  | 209 |
| 17.1 DHCP RELAY introduction.....   | 210 |
| 17.2 DHCP RELAY configuration .....                                       | 211 |
| 17.2.1 Enable the DHCP-relay function of the interface .....              | 211 |
| 17.2.2 Display information .....  | 212 |
| 17.3 DHCP RELAY configuration example.....                                | 212 |
| Chapter18 DHCP SERVER configuration.....                                  | 214 |
| 18.1 DHCP SERVER introduction.....  | 215 |
| 18.2 DHCP SERVER configuration.....                                       | 216 |
| 18.2.1 Enable global DHCP server function.....                            | 216 |
| 18.2.2 Start interface to receive DHCP server message.....                | 217 |
| 18.2.3 Configure address pool .....                                       | 217 |
| 18.2.4 Configure address pool range .....                                 | 217 |
| 18.2.5 Configure the address pool subnet mask.....                        | 218 |
| 18.2.6 Configure address pool lease .....                                 | 218 |
| 18.2.7 Configure the default gateway of the address pool.....             | 219 |
| 18.2.8 Configure the address pool DNS server.....                         | 219 |
| 18.2.9 Configure to manually exclude addresses in the address pool.....   | 220 |

|           |  |     |
|-----------|--|-----|
| 18.2.10   | OPTION82 configuration .....                     | 220 |
| 18.2.11   | Clear the assigned address table entry .....     | 221 |
| 18.2.12   | Clear detected conflicting address entries ..... | 221 |
| 18.3      | DHCP SERVER configuration example .....          | 221 |
| Chapter19 | ACL configuration .....                          | 224 |
| 19.1      | Introduction to ACL Resource Library.....        | 224 |
| 19.2      | Introduction to ACL filtering .....              | 227 |
| 19.3      | ACL resource library configuration .....         | 228 |
| 19.4      | ACL based on time period.....                    | 232 |
| 19.5      | ACL filtering configuration.....                 | 235 |
| 19.6      | ACL configuration example.....                   | 235 |
| 19.7      | ACL configuration troubleshooting .....          | 237 |
| Chapter20 | TCP/IP basic configuration .....                 | 238 |
| 20.1      | Configure VLAN interface.....                    | 239 |
| 20.2      | ARP configuration.....                           | 241 |
| 20.2.1    | Configure static ARP .....                       | 242 |
| 20.2.2    | View ARP information.....                        | 243 |
| 20.3      | Configure static routing.....                    | 243 |
| 20.4      | TCP/IP Basic configuration example .....         | 247 |
| 20.4.1    | Layer 3 interface .....                          | 247 |
| 20.4.2    | Static routing.....                              | 248 |
| 20.4.3    | ARP.....   | 248 |
| Chapter21 | SNMP configuration .....                         | 249 |
| 21.1      | SNMP introduction.....                           | 250 |
| 21.2      | SNMP configuration.....                          | 251 |
| 21.3      | SNMP configuration example .....                 | 253 |
| 21.3.1    | configuration.....                               | 253 |
| Chapter22 | RMON configuration .....                         | 254 |
| 22.1      | RMON introduction .....                          | 254 |
| 22.2      | RMON configuration .....                         | 255 |
| 22.3      | RMON configuration example.....                  | 258 |
| Chapter23 | Cluster configuration.....                       | 259 |
| 23.1      | Introduction to cluster management.....          | 259 |
| 23.1.1    | Cluster definition .....                         | 259 |
| 23.1.2    | Cluster Role .....                               | 260 |
| 23.1.3    | NDP introduction .....                           | 262 |
| 23.1.4    | NTDP introduction.....                           | 262 |
| 23.1.5    | Cluster management and maintenance.....          | 263 |

|   |     |
|---|-----|
| 23.1.6 Management vlan.....                                       | 265 |
| 23.2 Introduction to cluster configuration.....                   | 266 |
| 23.3 Configuration management equipment .....                     | 267 |
| 23.3.1 Enable the NDP function of the system and port .....       | 267 |
| 23.3.2 Configure NDP parameters .....                             | 268 |
| 23.3.3 Enable the NTDP function of the system and interface ..... | 268 |
| 23.3.4 Configure NTDP parameters.....                             | 269 |
| 23.3.5 Configure to manually collect NTDP information.....        | 269 |
| 23.3.6 Enable the cluster function.....                           | 270 |
| 23.3.7 Establish a cluster .....                                  | 270 |
| 23.3.8 Configure member interaction within the cluster.....       | 273 |
| 23.3.9 Configure cluster member management .....                  | 273 |
| 23.4 Configure member devices.....                                | 273 |
| 23.4.1 Enable the NDP function of the system and port .....       | 273 |
| 23.4.2 Enabling the NTDP function of the system and port .....    | 274 |
| 23.4.3 Configure to manually collect NTDP information.....        | 274 |
| 23.4.4 Enable the cluster function.....                           | 274 |
| 23.5 Configuring access to cluster members.....                   | 274 |
| 23.6 Cluster management display and maintenance.....              | 275 |
| 23.7 Typical example of cluster management configuration.....     | 275 |
| Chapter24 SNTP configuration.....                                 | 279 |
| 24.1 SNTP introduction.....                                       | 280 |
| 24.2 SNTP configuration.....                                      | 280 |
| 24.2.1 Default SNTP settings.....                                 | 280 |
| 24.2.2 Configuring the SNTP Server Address .....                  | 281 |
| 24.2.3 Configure SNTP clock synchronization interval .....        | 281 |
| 24.2.4 Configure local time zone.....                             | 282 |
| 24.3 SNTP information display.....                                | 282 |
| Chapter25 RIP configuration .....                                 | 283 |
| 25.1 RIP introduction .....                                       | 283 |
| 25.2 RIP configuration .....                                      | 284 |
| 25.2.1 Start RIP and enter RIP configuration mode.....            | 285 |
| 25.2.2 Enable RIP interface .....                                 | 285 |
| 25.2.3 Configure unicast messaging .....                          | 286 |
| 25.2.4 Configure the working status of the interface.....         | 286 |
| 25.2.5 Configure the default routing metric.....                  | 287 |
| 25.2.6 Configure management distance.....                         | 287 |

|  |     |
|--|-----|
| 25.2.7 Configure Timer.....  | 288 |
| 25.2.8 Configuration version .....   | 289 |
| 25.2.9 Import external routes .....  | 289 |
| 25.2.10 Configure route filtering .....  | 290 |
| 25.2.11 Configure additional routing metric.....                                     | 290 |
| 25.2.12 Configure the RIP version of the interface .....                             | 291 |
| 25.2.13 Configure the transceiver status of the interface.....                       | 292 |
| 25.2.14 Configure split horizon .....  | 293 |
| 25.2.15 Message authentication.....  | 294 |
| 25.2.16 Configure interface metric .....   | 294 |
| 25.2.17 Display information .....  | 295 |
| 25.3 RIP configuration example.....  | 296 |
| Chapter26 OSPF configuration.....  | 298 |
| 26.1 OSPF introduction.....  | 299 |
| 26.2 OSPF configuration.....   | 300 |
| 26.2.1 Start OSPF and enter OSPF mode .....  | 301 |
| 26.2.2 Enable interface .....  | 302 |
| 26.2.3 Designated host.....  | 303 |
| 26.2.4 Configure router ID.....  | 303 |
| 26.2.5 Configure adjacency .....   | 304 |
| 26.2.6 Disable the interface from sending packets .....                              | 305 |
| 26.2.7 Configure SPF calculation time .....  | 305 |
| 26.2.8 Configure management distance.....  | 306 |
| 26.2.9 Import external routes .....  | 307 |
| 26.2.10 Configure the network type of the interface .....                            | 308 |
| 26.2.11 Configure the interval for sending hello packets .....                       | 309 |
| 26.2.12 Configure the neighbor router expiration time .....                          | 310 |
| 26.2.13 Configure retransmission time.....   | 310 |
| 26.2.14 Configure interface delay .....  | 311 |
| 26.2.15 Configure the priority of the interface in DR election.....                  | 312 |
| 26.2.16 Configure the cost of sending packets on the interface .....                 | 313 |
| 26.2.17 Configure whether the interface sends DD packets to fill the MTU field ..... | 313 |
| 26.2.18 Configure interface packet authentication .....                              | 313 |
| 26.2.19 Configure area virtual links .....   | 314 |
| 26.2.20 Configure regional route aggregation .....                                   | 316 |
| 26.2.21 Configure regional message authentication.....                               | 316 |
| 26.2.22 Configure stub area.....   | 317 |

|           |   |     |
|-----------|---|-----|
| 26.2.23   | Configuring the nssa area .....                             | 318 |
| 26.2.24   | Configure external route aggregation .....                  | 318 |
| 26.2.25   | Configuring the Default Weight of External Routes.....      | 318 |
| 26.2.26   | Display information .....                                   | 319 |
| 26.3      | OSPF configuration example .....                            | 320 |
| Chapter27 | VRRP configuration .....                                    | 322 |
| 27.1      | VRRP introduction .....                                     | 322 |
| 27.1.1    | VRRP Overview .....   | 323 |
| 27.1.2    | VRRP terminology.....                                       | 325 |
| 27.1.3    | VRRP protocol interaction.....                              | 326 |
| 27.1.4    | Election of Virtual Master Router .....                     | 329 |
| 27.1.5    | Status of Virtual Router.....                               | 330 |
| 27.1.4    | VRRP tracking .....   | 332 |
| 27.2      | VRRP configuration.....                                     | 333 |
| 27.2.1    | Create and delete virtual routers .....                     | 333 |
| 27.2.2    | Configure the virtual IP address of the virtual router..... | 334 |
| 27.2.3    | Configure the parameters of the virtual router.....         | 334 |
| 27.2.4    | Configure VRRP tracking.....                                | 336 |
| 27.2.5    | Start and shut down the virtual router.....                 | 337 |
| 27.2.6    | View VRRP information.....                                  | 337 |
| 27.3      | VRRP configuration example .....                            | 338 |
| Chapter28 | Configure VLLP.....   | 340 |
| 28.1      | VLLP introduction .....                                     | 341 |
| 28.2      | VLLP configuration .....                                    | 344 |
| 28.2.1    | Create a vllp device on the layer 3 interface .....         | 345 |
| 28.2.2    | Enable vllp device.....                                     | 345 |
| 28.2.3    | Create a vllp port on the Layer 2 interface.....            | 345 |
| 28.2.4    | Configuring VLLP Device Priority.....                       | 345 |
| 28.2.5    | Configure the VLLP device query timer interval.....         | 346 |
| 28.2.6    | Configure affiliate VLAN .....                              | 346 |
| 28.2.7    | Configure vllp port priority.....                           | 346 |
| 28.2.8    | Display information .....                                   | 346 |
| 28.3      | VLLP configuration example .....                            | 347 |
| Chapter29 | Configure policy routing .....                              | 350 |
| 29.1      | Introduction to policy routing .....                        | 351 |
| 29.2      | Policy routing configuration.....                           | 351 |
| 29.2.1    | Create a new policy route .....                             | 351 |
| 29.2.2    | Insert a policy route .....                                 | 352 |

---

|   |     |
|---|-----|
| 29.2.3 Delete a policy route .....                      | 352 |
| 29.2.4 Move a policy route .....                        | 352 |
| 29.2.5 View policy routing information.....             | 353 |
| 29.3 Policy routing configuration example .....         | 353 |
| Chapter30 Configure System Log .....                    | 354 |
| 30.1 Introduction to System Log.....                    | 354 |
| 30.1.1 Log information format.....                      | 354 |
| 30.1.2 Storage of logs .....                            | 356 |
| 30.1.3 Log display .....                                | 357 |
| 30.1.4 debugging tool .....                             | 357 |
| 30.2 System log configuration .....                     | 358 |
| 30.2.1 Configure terminal real-time display switch..... | 358 |
| 30.2.2 Set log level .....                              | 359 |
| 30.2.3 View log information .....                       | 359 |
| 30.2.4 Configure debugging switch .....                 | 359 |
| 30.2.5 View debugging information .....                 | 361 |
| 30.3 SYSLOG configuration.....                          | 362 |
| 30.3.1 SYSLOG introduction .....                        | 362 |
| 30.3.2 SYSLOG configuration .....                       | 363 |
| 30.3.3 SYSLOG configuration example.....                | 364 |

---

# Chapter1 Introduction to CLI command line

---

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

- Accessing the Switch CLI
- Introduction to CLI mode
- Introduction to the command syntax
- Command line shortcuts
- History command

---

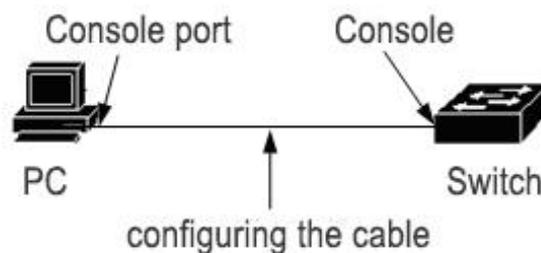
## 1.1 Accessing the Switch CLI

The CLI command line interface of the switch provides an interface for users to manage the switch. Users can access the CLI command line interface of the switch through two terminals, Console port and Telnet.

### 1.1.1 Users access CLI through the console port

The operation steps are as follows:

Step 1: Connect the serial port of the PC to the console port of the switch through the configuration cable, as shown below:



Step 2: Start the terminal emulation program on the PC (such as the Windows Hyper Terminal, etc.) and configure the communication parameters of the terminal emulation program. The communication parameter configuration of the terminal is as follows:

Baud rate: 38400 (or 115200) (Note: the actual product shall prevail)

Data bits: 8

Parity: None

Stop bit: 1

Data flow control: none

The communication parameter configuration of the hyper terminal is as follows:



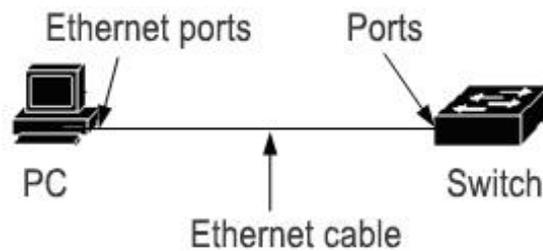
Step 3: Start the switch, the switch will show CLI prompt (default is Switch>) on the terminal after the switch is started, the user can enter the command at this prompt, so that the user can access the switch's CLI.

## 1.1.2 Users access CLI through TELNET

Users can access the switch through the port of the switch.

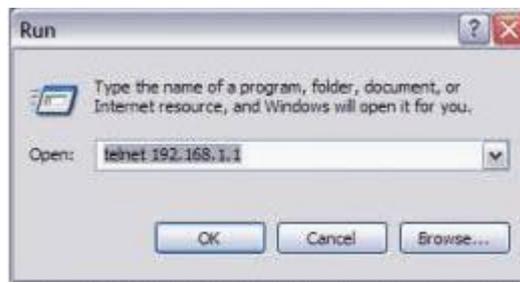
The IP address of the port of the switch defaults to 192.168.0.1 (Remarks: The actual product shall prevail). The steps to access the switch through the port are as follows:

Step 1: Connect the Ethernet port of the PC machine and the port of the switch through the Ethernet cable. As shown below :



Step 2: Set the IP address of the Ethernet port of the PC. The IP address must be in the 192.168.0.0/24 segment (such as the IP address 192.168.0.100). Determine the connectivity between the PC and the switch by ping 192.168.0.1.

Step 3: If the PC is connected to the switch, Telnet 192.168.0.1 enters the Telnet terminal interface. As shown below:



Step 4: If the system does not set the password, Telnet interface directly into the CLI, appears CLI prompt (default is Switch>); if the system set the password, you need to enter the password on the Telnet interface, so that can enter the CLI.

There are two points to pay special attention to:

- the IP address of the switch port is based on the VLAN layer 3 interface. the IP address of a VLAN interface must be set before accessing the switch. the default IP address of the VLAN1 is 192.168.0.1(Remarks: The actual product shall prevail), which can be used directly. The IP address of the VLAN interface can be configured through the Console port.
- The user accesses the switch through the port, can connect the PC and port directly through the Ethernet cable and connect through a network, just need the PC to be able to interworking with a certain VLAN of the switch.

o

---

## 1.2 Introduction to CLI mode

### 1.2.1 Function of CLI mode

CLI model has two main functions: :

- Facilitate grading of users and prevent unauthorized users from using CLI illegally.

Users can be divided into two categories: ordinary and privileged.

Ordinary users can only view some of the running state of the switch and can only use show commands.

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

- Convenient for users to configure the switch

The switch has a lot of configuration, and if you put all the configuration in one mode, the user is very inconvenient to use. For this reason, establish multiple patterns on the CLI, put similar commands in one mode, easy for users to understand and use. For example, put VLAN related commands in VLAN configuration mode, and interface related commands in interface configuration mode.

### 1.2.2 Identification of CLI model

CLI prompt is the identity of the CLI mode, and the user knows the CLI mode by looking at the CLI prompt.

CLI prompt consists of two parts, one identifying the host and the other identifying the pattern.

CLI host part in the prompt uses the host name of the system, the host name of the system is configurable and the default is Switch, so the CLI prompt default begins with the Switch, and the following mentioned CLI descriptor generally uses the default host name.

CLI the pattern part in the prompt is not configurable, each pattern has its own corresponding pattern string, some pattern strings are fixed and some pattern strings are variable. If the mode string of the VLAN configuration mode is fixed, the mode string of the interface configuration mode is variable.

For example:

CLI prompt Switch# identify privileged mode, Switch identify host, and # identify mode.

CLI prompt Switch (config-ge1/1)# identifies the interface configuration mode, and is

configured with ge1/1 ports, Switch identifies the host, while (config-ge1/1)# identifies the mode.

CLI prompt Switch (config-vlan2)# identifies the interface configuration mode and configures the vlan2 interface, Switch identifies the host, while (config-vlan2)# identifies the mode.

o

### 1.2.3 Classification of CLI mode

CLI mode is divided into four categories: Normal mode, privilege mode, global configuration mode and configuration sub-mode. Configuration sub-mode consists of many CLI modes.

Common users can only access normal mode, privileged users can access all CLI modes.

Console and Telnet terminals first enter normal mode, enter enable command in normal mode and enter privilege mode after successfully verifying password. At Telnet terminals, ordinary users can only stay in normal mode and can not enter privileged mode. enter configure terminal, CLI mode into global configuration mode in privileged mode. Input related commands in global configuration mode can enter each configuration sub-mode.

A table below lists the main CLI modes of the switch:

| Mode           | Description   | Prompt  | Command to enter mode               | Command to exit mode   |
|----------------|---|---------|-------------------------------------|--|
| Normal mode    | The show command is provided to view the status information of the switch.                    | Switch> | The mode the terminal first enters. | There is no exit mode command on the Console terminal, use exit or quit command on the Telnet terminal to exit the terminal. |
| Privilege mode | In addition to providing show commands to view the status information of the switch, commands | Switch# | Enter the enable command in normal  | Use the disable command to return to normal mode. Use the exit or quit   |

|                              |   |  |   |  |
|------------------------------|---|--|---|--|
|                              | such as debugging, version upgrading and configuration maintenance are also provided.   |  | mode.   | command on the Console terminal to retreat to normal mode and exit the Telnet terminal using the exit or quit command on the Telnet terminal.. |
| Global configuration mode    | Provides generic commands that can not be implemented within the configuration sub-mode, such as configuration static routing commands. | Switch(config)#  | Enter configure terminal command in privileged mode.                            | Exit to privileged mode using exit,quit or end commands.   |
| Interface configuration mode | Provide commands to configure ports and VLAN interfaces.  | Port:<br>Switch(config-ge1/1)#<br>VLAN interface:<br>Switch(config-vlan1)# | Enter the interface <if-name> command in global configuration mode.             | Exit to global configuration mode using exit or quit commands, exit to privileged mode using end commands.                                     |
| VLAN Configuration Mode      | Provide configure VLAN commands. For example, create and delete VLAN commands.  | Switch(config-vlan)#   | Enter the vlan database command in global configuration mode.                   | Exit to global configuration mode using exit or quit commands, exit to privileged mode using end commands.                                     |
| MSTP Configuration Mode      | Provide configure MSTP commands. For example, create and delete commands for MSTP instances.  | Switch(config-mst)#  | Enter the spanning-tree mst configuration command in global configuration mode. | Exit to global configuration mode using exit or quit commands, exit to privileged mode using end commands.                                     |

|                             |   |                      |  |  |
|-----------------------------|---|----------------------|--|--|
| Terminal Configuration Mode | Provide command to configure the Console and Telnet terminal, such as the command to configure the timeout of the terminal. | Switch(config-line)# | Enter the line vty command in global configuration mode. | Exit to global configuration mode using exit or quit commands, exit to privileged mode using end commands. |
|-----------------------------|---|----------------------|--|--|

## 1.3 Introduction to Command syntax

### 1.3.1 Command composition

CLI command consists of two parts: keyword and parameter, the first word must be keyword, the following word can be keyword or parameter, keyword and parameter can appear alternately. A command must have keywords, but it can be without parameters. The command write, for example, has only one keyword without arguments; the command show version has two keywords without arguments; the command vlan <vlan-id> has one keyword and one argument; the command instance <instance-id> vlan <vlan-id> have two keywords and two parameters and the keywords and parameters appear alternately.

### 1.3.2 Parameter Type

CLI commands have two parameters: required and optional. The selected parameters must be entered when entering a command, and the optional parameters can or can not be entered. The parameter in the command vlan <vlan-id> must be entered when the command is entered; the parameter in the command show interface [if-name] is optional and can or may not be entered when the command is entered.

### 1.3.3 Command syntax rules

The following rules must be met when describing commands in text :

1 ) Key words are expressed directly in words.

For example, command show version.

2 ) Parameters must be enclosed in <>.

For example, command vlan <vlan-id>

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

For example, command show vlan [<vlan-id>]

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

command show vlan [vlan-id]

A parameter vlan-id can or can not be entered.

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

4 ) If you have to select 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 |.

Such as multiple keywords required command :

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

One must be chosen between point-to-point and shared.

Multiple Parameter Required Commands :

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

Keyword and parameter hybrid required command :

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 [], separate multiple keywords or parameters with |, and require a space before and after |.

The command as follows :

debug ip tcp [recv | send]

Keyword recv and send can choose one or not.

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

show interface [<if-name> | switchport]

6 ) If there is a keyword or parameter or a set of keywords or parameters that can be

repeatedly selected input, add the symbol "\*" after this (group) keyword or parameter.

For example ping command :

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

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

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

The entire option can be repeated.

6 ) Parameters are represented by a descriptor of one or more words, and if it is multiple words, separate each word with the symbol "-", each word being lowercase.

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

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

### 1.3.4 Command abbreviations

The user enters a command on the CLI interface, the keyword of the command can be abbreviated. CLI support the prefix matching function of the command, as long as the input word and keyword prefix unique match, CLI will parse the input word into the matching keyword. This makes it easy for users to use CLI. Users can complete a command by typing very few characters, for example show version commands can type only sh ver.

### 1.3.5 Grammar Help

CLI the command-line interface with syntax help, support each level of command and parameter help function described below :

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

2 ) Enter the front part of a command, then enter the space before entering? Key, all keywords or parameters at the next level and their description are listed on the terminal. For example Switch#show ?.

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

4 )Enter the front part of a command, then enter the space, then enter the Tab key, on the terminal will list all the keywords of the next level, the next level if is not listed if it is a parameter.

5 ) Enter an incomplete keyword and enter the Tab key directly. If only one keyword matches this input prefix, fill it directly. If more than one keyword matches this input prefix, list all matching keywords on the terminal.

### 1.3.6 Command line error messages

If the command entered by the user does not pass the syntax check, the error message will be showed on the terminal. The common error message is as follows.

| Error information                        | Error reason   |
|--|--|
| Invalid input or<br>Unrecognized command | No matching keywords found.<br>Parameter input is incorrect.<br>Too many keywords or parameters entered. |
| Incomplete command                       | Command input is incomplete and keywords or parameters are not entered.                                  |
| Ambiguous command                        | The keyword input is incomplete and multiple keywords match the input prefix.                            |

## 1.4 Command line shortcuts

### 1.4.1 Line edit shortcut

CLI command line interface supports line editing shortcut key function, line editing shortcut key can facilitate CLI command input and editing. When you enter or edit a command, you can use the line edit shortcut to speed up the command's input. The following table lists all the line-editing shortcuts and functions implemented:

| Shortcuts        | Function   |
|------------------|------------|
| Ctrl+p or ↑ keys | Last order |

|                  |   |
|------------------|---|
| Ctrl+n or ↓ keys | Next order  |
| Ctrl+u           | Delete entire line  |
| Ctrl+a           | cursor back to the line   |
| Ctrl+f or →keys  | Move the cursor to the right  |
| Ctrl+b or ←keys  | Move the cursor to the left   |
| Ctrl+d           | Delete the character where the cursor is located  |
| Ctrl+h           | Delete the first 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 cursor to end of line  |
| Ctrl+c           | Interrupt, do not execute command line. CLI fall back to privileged mode if CLI are in global configuration mode or configuration sub-mode; if CLI are in normal or privileged mode, the CLI mode remains the same but CLI a new line.              |
| Ctrl+z           | same as Ctrl c function.  |
| Tab              | Use this key after entering an incomplete keyword, if one keyword matches the entered prefix, fill this keyword; if more than one keyword matches the entered prefix, all matching keywords are listed; if no keyword matches, this key is invalid. |

**Note: Some Console terminal ↑,↓,→, and ← keys are not available.**

## 1.4.2 Show command Shortcut

For commands that start with show keywords are show commands, some show commands can not be showed in one screen because of the show content, the terminal provides the function of split screen show. After the show screen, the terminal waits for user input to determine the subsequent processing. The following table lists the show command shortcuts and their functions.

| Shortcuts  | Function                                       |
|------------|--|
| Space      | show next screen                               |
| Enter      | Show the next line                             |
| Ctrl+c     | Interrupt command execution, exit to CLI mode. |
| Other keys | Same as Ctrl c function.                       |

---

## 1.5 Historical Command

CLI command-line interface supports the command history function, can remember the user's recent use of 20 history commands, the user recently typed commands saved. You can use show history to show commands that have been entered, and you can also use Ctrl+ p, Ctrl+n or ↑, ↓ keys to select historical commands. The history command feature facilitates user input commands.

# Chapter2 System management configuration

---

Before learning the relevant function configuration of the switch, users need to master some basic configuration of the system management and maintenance of the switch. This chapter describes the basic configuration of these system management and maintenance, mainly including the following content:

- System security configuration
- System maintenance and commissioning
- System monitoring
- Profile Management

- 
- Software version upgrade

## 2.1 System security configuration

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

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

### 2.1.1 Multi-user management control

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

Multi-user management divides user rights into two levels: ordinary users and privileged users. Common users can only stay in the normal mode of CLI command line interface, can only use the show command, query the information of the switch. Privileged users can access all modes CLI the command line interface, use all the commands provided by the CLI, can query the information of the switch, and can maintain and manage the switch.

The multi-user management function is only applied to the Telnet terminal and does not control the Console terminal. There is no need to verify the user name and password when using the Console terminal to access the switch CLI. the user can access the switch directly, and the user name and password need to be verified when accessing the switch through the Telnet terminal, and the CLI can be accessed only after the user name and

password are verified and passed.

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

Multi-user management related commands are listed below:

| Command  | description  | CLI mode                  |
|--|--|---------------------------|
| username <user-name><br>password <key> {normal  <br>privilege} | Add a user and modify the password and permissions of that user if the specified user already exists. The first parameter is the user name, the second parameter is the password, the optional represents the permission, the normal represents the ordinary user, privilege represents the privileged user. | Global Configuration Mode |
| no username [user-name]  | Delete a user with the specified username.   | Global Configuration Mode |
| show running-config  | view the current configuration of the system, you can view the multi-user managed configuration.   | Privilege mode            |

## 2.1.2 Enable password control

Enable password is used to control the switch from normal mode to privileged mode. before enable password verification, the user can only view the information of the switch, and after enable password verification, it is possible for the user to configure and maintain the switch.

enable password is not attached to the user, any user login to the Console terminal

or Telnet terminal, if you want to enter privileged mode must verify the enable password, if the verification is not successful, can only stay in normal mode.

Enter the enable command in normal mode, the terminal will prompt the user to enter the password, at this time the user can enter the enable password, if the password verification is successful, the terminal enters the privileged mode, otherwise, stay in the ordinary mode, for the ordinary user, no matter whether the password verification is successful or not, can not enter the privileged mode.

enable password is empty by default, in this case the terminal does not prompt to enter the password directly into privileged mode after entering enable command in normal mode.

enable password related commands are listed below:

| Command               | Description   | CLI mode                  |
|-----------------------|---|---------------------------|
| enable password <key> | Sets the enable password for the system.  | Global Configuration Mode |
| no enable password    | Clear the enable password of the system, enable password is empty.  | Global Configuration Mode |
| show running-config   | Check the current configuration of the system to see enable password configuration.   | Privilege mode            |
| enable                | Interactive command, verify the enable password of the system, after the verification is successful, the terminal enters privileged mode. | Normal mode               |

Note: For system security, administrators need to set the system enable password.

### 2.1.3 TELNET Service control

In some cases, the administrator does not need to manage the switch remotely, just need to manage the switch locally through the Console terminal. at this time, in order to improve the security of the system and prevent illegal users from landing Telnet terminal remotely, the administrator can close the Telnet service. Telnet service is open by default.

Telnet Service Control commands are listed below:

| Command   | Description  | CLI mode                  |
|---|--|---------------------------|
| security-manage telnet enable   | Open Telnet service.   | Global Configuration Mode |
| security-manage telnet disable  | Close Telnet service.  | Global Configuration Mode |
| security-manage telnet number <1-100>   | Number parameters range from 1 to 100 and default is 5.  | Global Configuration Mode |
| security-manage telnet access-group <1-99><br>(Remarks: Subject to actual products) | Specifies a ACL group, opens the source IP address control.<br>If the specified ACL group does not exist or is not a standard group, no need to control the source IP address. | Global Configuration Mode |
| no security-manage telnet access-group  | Close source IP address control.   | Global Configuration Mode |
| show security-manage  | Can view the configuration of the service control.   | Privilege mode            |

## 2.1.4 SNMP Service control

SNMP service controls can turn on/off SNMP services, and control the IP address of access switches through ACL.

SNMP Service Control commands are listed below:

| command                     | Description         | CLI mode                  |
|-----------------------------|---------------------|---------------------------|
| security-manage snmp enable | Open SNMP services. | Global Configuration Mode |
| security-manage snmp        | Close SNMP service. | Global                    |

|   |  |                           |
|---|--|---------------------------|
| disable   |  | Configuration Mode        |
| Security-manage snmp access-group <1-99><br>(Remarks: Subject to actual products) | Specifies a ACL group, opens the source IP address control.<br>If the specified ACL group does not exist or is not a standard group, no need to control the source IP address. | Global Configuration Mode |
| no security-manage snmp access-group  | Close source IP address control.   | Global Configuration Mode |
| show security-manage  | Can view the configuration of the service control.   | Privilege mode            |

## 2.1.5 HTTP Service control

HTTP service controls can turn on/off HTTP services, and control the IP address of access switches through ACL.

HTTP Service Control commands are listed below:

| Command   | Description  | CLI mode                  |
|---|--|---------------------------|
| security-manage http enable   | Open HTTP service.   | Global Configuration Mode |
| security-manage http disable  | Close HTTP service.  | Global Configuration Mode |
| security-manage http access-group <1-99><br>(Remarks: Subject to actual products) | Specifies a ACL group, opens the source IP address control.<br>If the specified ACL group does not exist or is not a standard group, no need to control the source IP address. | Global Configuration Mode |
| no security-manage http access-group  | Close source IP address control.   | Global Configuration      |

|                      |  | Mode           |
|----------------------|--|----------------|
| show security-manage | Can view the configuration of the service control. | Privilege mode |

## 2.2 System maintenance and commissioning

Basic system maintenance and debugging functions include the following :

- Configure the system clock
- Configure terminal timeout attributes
- System reset
- View system information
- Network connectivity debugging
- Traceroute debugging

### 2.2.1 Configuring the system clock

The switch provides the function of real-time clock. You can set the current clock and view the current clock through Command. The system clock is internally powered to ensure the continuous operation of the real-time clock when the system is powered off. There is no need to reset the clock after the system starts.

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

The related commands of the system clock are as follows:

| Command   | Description   | CLI mode        |
|---|---|-----------------|
| set date-time <year><br><month> <day> <hour><br><minute> <second> | Set the current clock of the system, you need to enter the year, month, day, hour, minute, and second parameters. | Privileged mode |

|                |  |                                  |
|----------------|--|----------------------------------|
| show date-time | shows the current clock of the system. | Normal mode ,<br>Privileged mode |
|----------------|--|----------------------------------|

## 2.2.2 Configure terminal timeout attributes

For the security of the terminal, when there is no key input on the terminal, the terminal will perform the exit process after a certain period of time. The console terminal and the Telnet terminal have different exit processes. For the Console terminal, when the terminal times out, the CLI mode returns Normal mode, for Telnet terminals, when the terminal times out, the Telnet connection is interrupted and the Telnet terminal exits.

The terminal timeout time defaults to 10 minutes, and users can also set the terminal to never time out..

The related commands for terminal timeout are as follows:

| Command                             | Description   | CLI mode                    |
|-------------------------------------|---|-----------------------------|
| exec-timeout <minutes><br>[seconds] | Set the terminal timeout time, if the parameters are 0, it means that the terminal will never time out. | Terminal configuration mode |
| no exec-timeout                     | Set the terminal timeout time back to the default, which is 10 minutes.                                 | Terminal configuration mode |
| show running-config                 | View the current configuration of the system, you can view the terminal timeout configuration.          | Privileged mode             |

## 2.2.3 System reset

The system provides a reset method :

- Reset switches

The related commands for system reset are as follows:

| Command | Description     | CLI mode        |
|---------|-----------------|-----------------|
| reset   | Reset switches. | Privileged mode |

## 2.2.4 View system information

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

| Command                      | Description   | CLI mode                         |
|------------------------------|---|----------------------------------|
| show version                 | show the system version number and the time to execute the file compilation and connection.                       | Normal mode ,<br>Privileged mode |
| show snmp system information | Displays basic information about the system, including how long it has been running since the system was started. | Normal mode ,<br>Privileged mode |
| show history                 | shows the list of recently entered Commands on the CLI Command line.  | Normal mode ,<br>Privileged mode |

## 2.2.5 Network connectivity debugging

In order to debug the connectivity between the switch and another device in the network, you need to implement ping command on the switch and ping the IP address of the other side on the switch. If the switch receives a ping response from the other side, it means that both ends are connected, otherwise it indicates that the two terminals cannot communicate.

The switch not only implements ping command, but also supports many options on

ping command. Users can use these options for more precise and complex debugging.

The ping command is as follows:

| Command  | Description   | CLI mode        |
|--|---|-----------------|
| ping <ip-address> [-n <count>   -l <size>   -w <timeout>]* | You can use it without any options or one or more options. If you don't have any options, it is the simplest ping command. When executing, you can type Ctrl + c to interrupt the execution of the Command. | Privileged mode |

## 2.2.6 Traceroute debugging

In order to debug the intermediate devices that the switch and another device in the network pass through during communication, you need to implement trace-route command on the switch. When using trace-route command on the switch, specify the IP address of the other party. All the paths in the middle are showed.

The switch not only implements trace-route command, but also supports many options on trace-route command. Users can use these options for more precise and complex debugging.

The trace-route command is as follows:

| Command   | Description   | CLI mode        |
|---|---|-----------------|
| trace-route <ip-address> [-h <maximum-hops>   -j <count> <ip-address>*   -w <timeout>]* | You can use it without any options or one or more options. If you don't have any options, it is the simplest trace-route command. Command can be executed by typing Ctrl + c to interrupt the execution of the Command. | Privileged mode |

---

## 2.2.7 Telnet client

The switch provides the Telnet client function, and users can remotely access other devices through the Telnet client.

| Command             | Description   | CLI mode        |
|---------------------|---|-----------------|
| telnet <ip-address> | The parameter is the IP address of the target device. | Privileged mode |

## 2.3 Configuration file management

The configuration is divided into two types: the current configuration and the initial configuration. The current configuration refers to the configuration when the system is running, which is stored in the system's memory, and the initial configuration is the configuration used when the system is started, and is stored in the system FLASH, which is the configuration file. When the user executes the relevant Command, the current configuration of the system is modified. Only after the Save Command is executed, the current configuration is written to the initial configuration for the next startup of the system. When the system starts, the user does not make any configuration. In the case of, the current configuration information of the system is the same as the initial configuration information.

The current configuration and the initial configuration use the same format, both are Command line text format, very intuitive and easy for users to read. The configuration file format has the following characteristics :

- The configuration file is a text file.
- Commands are saved.
- Only save the non-default configuration, do not save the default configuration.
- Commands are organized according to CLI mode. Commands in the same CLI

mode are organized together to form a segment, which is separated by "!". For

Commands in Global configuration mode, Commands with the same function or similar functions are organized into a paragraph, separated by "!".

- For the Command in the configuration sub-mode, there is a space before the Command, and for the Command in the Global configuration mode, there is no need for a space before the Command.

- End the configuration with "end".

---

Configuration file management mainly includes the following :

- View configuration information
- Save configuration
- Delete configuration file
- configuration file download/upload

### 2.3.1 View configuration information

View configuration information includes viewing the current configuration and initial configuration of the system. The initial configuration is actually the configuration file in FLASH. When there is no configuration file in FLASH, the default configuration is used when the system is started. During initial configuration, the system will prompt that the configuration file does not exist..

The command of view configuration information is as follows:

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

### 2.3.2 Save configuration

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

The command of save configuration is as follows:

| Command | Description                 | CLI mode        |
|---------|-----------------------------|-----------------|
| write   | Save current configuration. | Privileged mode |

---

Note: The user needs to use this Command Save configuration after configuring the switch, otherwise the configuration will be lost after the system restarts.

### 2.3.3 Delete configuration file

When the user wants the initial configuration of the system to return to the default configuration, you can delete the configuration file. Delete configuration file has no effect on the current configuration, if you want the current configuration of the system to return to the default configuration, you need to restart the switch. Be careful when you file, otherwise the configuration will be lost.

The Command of Delete configuration file is as follows:

| Command               | Description                           | CLI mode        |
|-----------------------|---------------------------------------|-----------------|
| delete startup-config | Delete the system configuration file. | Privileged mode |

### 2.3.4 Configuration file download/upload

For the security of the configuration file, users can use the command to upload the configuration file to the PC for backup. When the system configuration is abnormally lost or modified and you want to return to the original configuration, you can download the original configuration file from the PC to the switch. Downloading the configuration file has no effect on the current configuration of the system. The configuration must take effect after restarting the switch and also can upload and download configuration files through WEB. For specific operations, please refer to the WEB operation manual. Download on The Command of the configuration file download/upload is as follows:

| Command                                      | Description   | CLI mode        |
|--|---|-----------------|
| upload configure<br><ip-address> <file-name> | Upload the configuration file to the PC, the first parameter is the IP address of the PC, the second parameter is the file name of the configuration file | Privileged mode |

|  |   |                 |
|--|---|-----------------|
|  | stored on the PC.   |                 |
| download configure<br><ip-address> <file-name> | Download the configuration file to the PC, the first parameter is the IP address of the PC, and the second parameter is the file name of the configuration file stored on the PC. | Privileged mode |

Configuration file download/upload uses the TFTP protocol, runs the TFTP client software on the switch, and runs the TFTP server software on the PC. The steps for download on configuration file are as follows :

Step 1 : build a network environment.

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

Step 3: Save configuration on the switch.

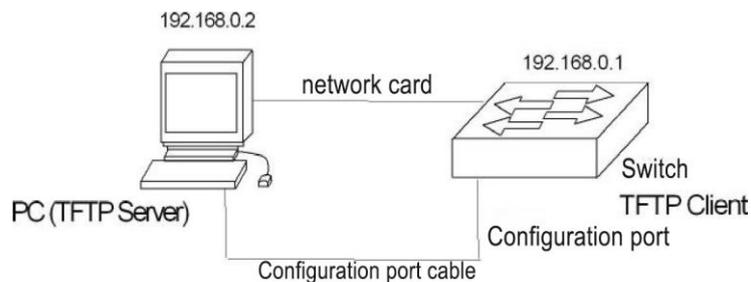
Step 4: Execute the configuration file upload command on the switch to back up the configuration file to the PC..

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

Step 6: Restarted the switches for the configuration to take effect.

Example: A switch that has been configured with VLANs and interface addresses requires download/upload on configuration file operation.

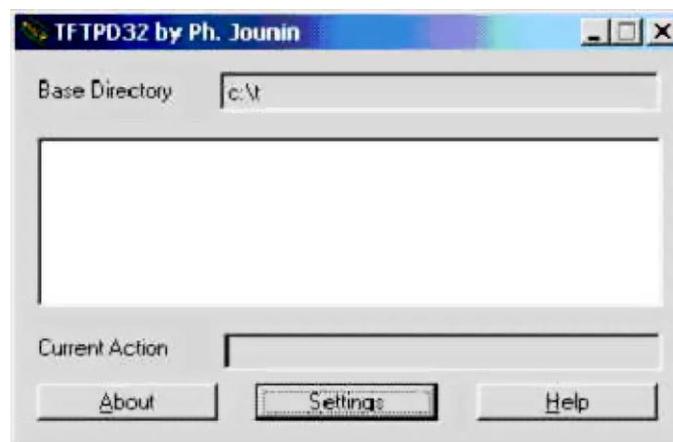
Step 1 : build a network environment.



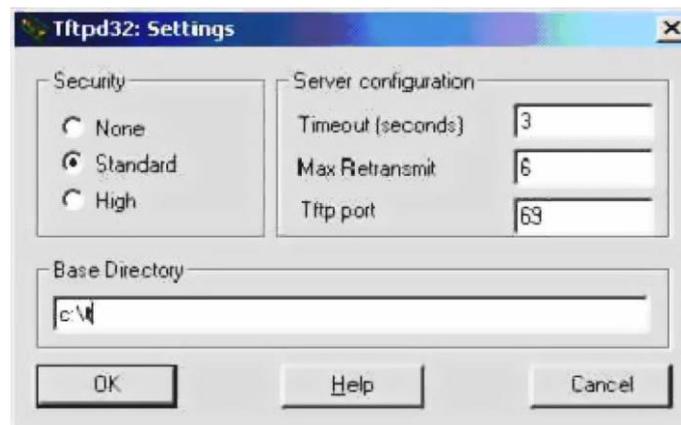
Connect the configuration port of the switch to a configuration terminal via a cable, and connect it to a PC via a network cable. Install the TFTP server on the PC and configure the IP address of the Ethernet port of the PC. Here, the IP address of the PC is assumed to be 192.168.0.2. Then, configure the IP address of the switch. Here, the IP address of the switch is assumed to be 192.168.0.1 to ensure the connectivity between the PC and the switch.

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

Run TFTP Server, the window interface is as follows:



Then, set the directory of the backup configuration file. The specific operation is to click the [Settings] button to set the interface, as shown below:



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

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

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

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

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

## 2.4 Software version upgrade

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

### 2.4.1 Command of software version upgrade

To upgrade the image file of the switch in Global configuration mode, the command is as follows:

```
download switch <ip-address> <file-name>
```

<ip-address> is the IP address of the PC running the TFTP server, and <file-name> is the name of the image file saved on the TFTP server.

To upgrade the kernel file of the switch in the global configuration mode, the command is as follows:

```
download kernel <ip-address> <file-name>
```

<ip-address> is the IP address of the PC running the TFTP server, and <file-name> is the name of the kernel file saved on the TFTP server.

To upgrade the patch file of the switch in the global configuration mode, the command is as follows:

```
download patch <ip-address> <file-name>
```

<ip-address> is the IP address of the PC running the TFTP server, and <file-name> is the name of the patch file saved on the TFTP server.

To upgrade the uboot file of the switch in the global configuration mode, the command is as follows:

download uboot <ip-address> <file-name>

<ip-address> is the IP address of the PC running the TFTP server, and <file-name> is the name of the uboot file saved on the TFTP server.

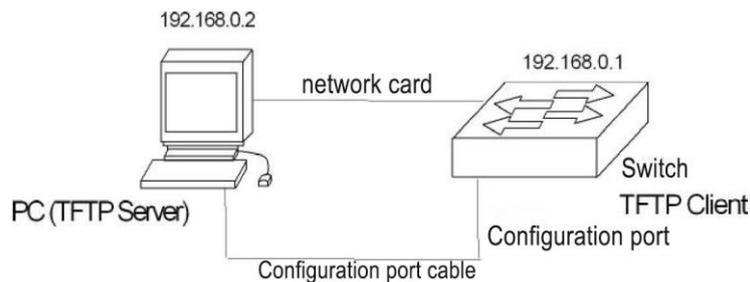
The power cannot be cut off during the upgrade process, otherwise the image file of the switch may be damaged and the switch will not start. After completed, restart the switch to run the newly downloaded image file program. The entire upgrade process takes a few minutes, please wait patiently .

Software version upgrade can also be achieved through WEB, specific operations can refer to WEB operation manual.

## 2.4.2 Software upgrade process

The steps to upgrade the image file are as follows :

Step 1: build an upgrade environment. As shown in the figure below.

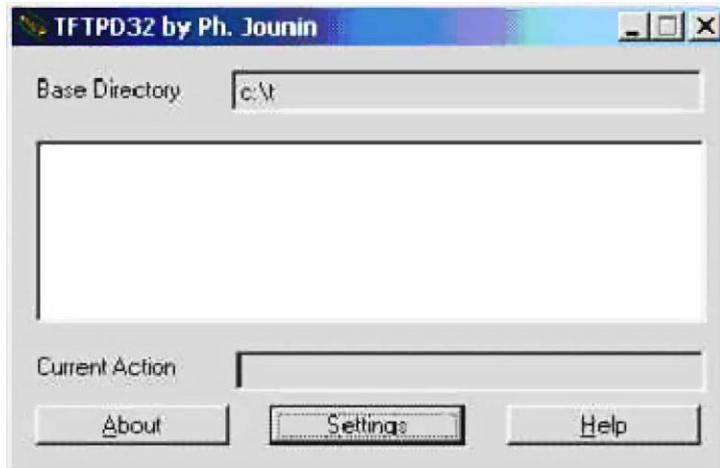


The construction process is as follows :

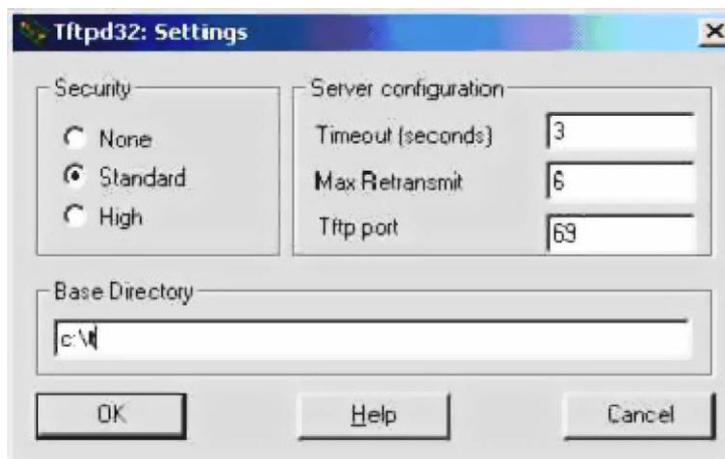
- Connect the console port of the switch to a configuration terminal (PC) through a cable.
- Install TFTP Server on the PC.
- Copy the new image file to a certain path of the PC, here assume the path is c: \ t ;
- Configure the IP address of the Ethernet port of the PC. It is assumed that the IP address of the PC is 192.168.0.2 .
- Configure the IP address of the switch, here it is assumed that the IP address of the switch is 192.168.0.1.

Step 2: Run TFTP Server and configure TFTP server.

First: Run TFTP Server. The TFTP32 window interface is as follows:



Then: Set the TFTP Server file directory. After starting the TFTP Server, reset the TFTP Server file directory, copy the image file to be loaded into this directory. The specific operation is to click the [Settings] button, the TFTP32 setting interface appears, as follows Figure:



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

Step 3: Upgrade files.

First: Connect the port of the switch to the PC running the TFTP Server program via an Ethernet cable. Use ping Command to check whether the host is connected to the switch..

Then: Enter Command at the Super terminal Switch # prompt:

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

|

---

to finish.

Software is updating. Please wait and don't power down!

.....

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

After the file transfer is completed, the system will prompt you whether you need to restart the switch; under normal circumstances, we recommend that you select 'Y' to restart the switch, because the system upgrade can only take effect after restart; if your configuration file is not saved, you can select 'N ', Do not restart first; restart the switch after completing other operations such as saving.

Switch#

**Note : The switch cannot be powered off during the upgrade process.**

Step4 : Reset switches.

Switch# reset

---

## Chapter3 Port configuration

---

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

- Common port configuration
- Configure MIRROR
- Configure STORM-CONTROL
- Configure FLOW-CONTROL
- Configure port bandwidth
- Configure TRUNK

---

## 3.1 Common port configuration

The administrator configures the port of the switch to control the users connected under the port. If the user under the port is not allowed to access the network, the administrator can close the port. This section introduces Common port configuration, mainly including: :

- Port opening and closing
- Port speed configuration
- Show port information

### 3.1.1 Port opening and closing

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

The following command opens the management status of the port in interface configuration mode:

```
no shutdown
```

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

```
Switch(config-ge1/1)#no shutdown
```

The following command closes the management status of the port in interface configuration mode:

```
Shutdown
```

For example, close the management status of port ge1/1 :

```
Switch(config-ge1/1)#shutdown
```

### 3.1.2 Port speed configuration

The default rate configuration of all ports is adaptive (autonegotiate).

The following Command Configure port rate in interface configuration mode:

```
speed {autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 }
```

```
autonegotiate---autonegotiate
```

|

---

full-1000-----full duplex gigabit  
full-100-----full-duplex 100M  
full-10 -----full-duplex 10M  
half-100-----half duplex 100M  
half-10-----half duplex 10M

For example, the rate of port 1/1 is configured as full duplex 100M:

```
Switch(config-ge1/1)# speed full-100
```

### 3.1.3 Show port information

The following Command shows the information of one or more ports in Normal mode or Privileged mode:

```
show interface [if-name]
```

For example, show the information of port ge1/1:

```
Switch# show interface ge1/1
```

For example, show the information of all ports:

```
Switch# show interface
```

## 3.2 MIRROR configuration

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

- Configure MIRROR monitor port and monitored port
- Show MIRROR configuration

### 3.2.1 MIRROR monitor / monitored port configuration

When the administrator configures the monitor port, you need to enter this interface configuration mode to set the monitored port. For example, to set the port ge1 / 1 to listen to the port ge1 / 2, you need to enter the port ge1 / 1 and type Command :

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

At this time, port ge1 / 1 is set as the monitor port, and ge1 / 2 is set as the monitored port.

The command to set the monitored port is as follows :

```
Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}
```

At this time, port ge1 / 1 is set as the monitor port, and <if-name> is set as the monitored port, and the following {both | receive | transmit} indicates the direction of monitoring: receive means monitoring the received packets; transmit means monitoring the sent packets. both means listen to all packets sent and received. For example :

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

Show to set port ge1 / 1 to listen to the data packets sent and received by port ge1 / 2.

If set multiple monitored ports, Need to execute Command multiple times.

The administrator can cancel the monitored port in the interface configuration mode, the command is as follows :

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

At this time, <if-name> is the port that is no longer being monitored. For example :

```
Switch(config-ge1/1)# no mirror interface ge1/2
```

Show that the port ge1 / 1 is no longer monitor to the data packets of port ge1 / 2.

When all monitored ports are canceled, the monitor ports will also be cleared.

### 3.2.2 Show MIRROR configuration

The administrator can view the MIRROR configuration that has been set by using the following Command in Normal mode or Privileged mode:

```
Switch# show mirror
```

Pay attention to the following points :

- 
- A port cannot be set as a monitor port and a monitored port at the same time.
  - There can only be one monitor port, but there can be multiple monitor ports.

### **3.3 STORM-CONTROL configuration**

In real life, a NIC card sends out high-rate unicast, multicast, and broadcast packets, which can cause the network to malfunction. In this case, the suppression function on the switch is particularly important, it can prevent data packets from flooding the network caused network congestion. All ports of the switch support the suppression of broadcast packets, multicast packets and DLF packets:

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

- Default configuration
- Broadcast suppression configuration
- Multicast suppression configuration
- DLF suppression configuration
- Show STORM-CONTROL configuration

#### **3.3.1 Default configuration**

The switch supports setting broadcast, multicast, and dlf switches for each port. The three settings use different rate limits. Broadcast packet suppression on the default port is turned on, and the suppression rate is 64K. The purpose is to prevent the network from forming a broadcast storm. DLF packets and multicast packets are not suppressed by default.

#### **3.3.2 Broadcast suppression configuration**

The following command configures broadcast suppression for this port in interface configuration mode:

```
storm-control broadcast
```

|

---

The following command cancels the configuration of broadcast suppression for this port in interface configuration mode:

```
no storm-control broadcast
```

### **3.3.3 Multicast suppression configuration**

The following command configures multicast suppression for this port in interface configuration mode:

```
storm-control multicast
```

The following command cancels the configuration of multicast suppression for this port in interface configuration mode:

```
no storm-control multicast
```

### **3.3.4 DLF suppression configuration**

The following command configures DLF suppression for this port in interface configuration mode:

```
storm-control dlf
```

The following Command cancels the configuration of DLF suppression for this port in interface configuration mode:

```
no storm-control dlf
```

### **3.3.5 Suppression rate configuration**

The following command configures the suppression rate of this port in interface configuration mode:

```
storm-control ratelimit <1-1024000>
```

---

### 3.3.6 Show STORM-CONTROL configuration

The following Command Shows the STORM-CONTROL configuration in Normal mode or Privileged mode:

```
show storm-control
```

### 3.4 STORM-CONSTRAIN configuration

The port flow threshold control function is used to control the packet storm on Ethernet. A port enabled with this function will periodically detect the unicast packet traffic, multicast packet traffic and broadcast packet traffic arriving at the port. If the traffic of a certain type of packet exceeds the preset upper threshold, the user can configure it to decide whether to block the port or close the port, and whether to log the log information.

When the traffic of a certain type of packet exceeds the preset upper threshold of that type of packet, the system provides two processing methods:

(1) Block mode: If the traffic of a certain type of packet on the port is greater than the upper threshold, the port will suspend forwarding the packet, the port is blocked, but the port still counts the traffic of this type of packet. When the traffic of this type of packet is less than the preset lower threshold, the port will resume the forwarding of the packet.

(2) Shutdown mode: If the traffic of certain types of packets on the port is greater than the upper threshold, the port will be shut down and the system will stop forwarding all packets. You can restore the port status by executing the no shutdown command, or by canceling the port traffic threshold configuration.

Note: For certain types of packet traffic, you can use this function or the storm suppression function of the Ethernet port to suppress, but these two functions cannot be configured at the same time, otherwise the suppression effect is uncertain. For example, you cannot configure the unicast packet traffic threshold control function and unicast storm suppression function of the port at the same time.

The CLI configuration commands are as follows:

| command  | description   | CLI mode                           |
|--|---|------------------------------------|
| storm-constrain<br>(broadcast multicast unicast)<br>min-rate <1-1488100> max-rate<br><1-1488100> | Storm control of<br>broadcast, multicast or<br>unknown unicast packets<br>under the interface | Interface<br>configuration<br>mode |

|   |   |                                 |
|---|---|---------------------------------|
| no storm-constrain<br>(broadcast multicast unicast all) | Cancel storm control  | Interface<br>configuration mode |
| storm-constrain action<br>(block shutdown)              | Configure the action of<br>storm control. By default, no<br>storm control is performed<br>on packets                      | Interface<br>configuration mode |
| no storm-constrain action                               | Cancel the configured<br>storm control action   | Interface<br>configuration mode |
| storm-constrain enable (trap)                           | Switch on logging when<br>storm control is turned on  | Interface<br>configuration mode |
| no storm-constrain enable (log)                         | Switch off logging when<br>storm control is turned off  | Interface<br>configuration mode |
| storm-constrain interval <6-180>                        | Configure the storm<br>control detection interval. By<br>default, the storm control<br>detection interval is 5<br>seconds | Interface<br>configuration mode |
| no storm-constrain interval                             | Restore the storm<br>control detection interval to<br>the default value   | Interface<br>configuration mode |
| no storm-constrain                                      | Remove the storm<br>control function of the<br>interface  | Interface<br>configuration mode |
| show storm-constrain                                    | View storm control<br>information for all interfaces  | Privileged<br>mode              |
| show storm-constrain interface<br>IFNAME                | View storm control<br>information on the interface  | Privileged<br>mode              |

Configuration instructions:

(1)View the storm control information description table of the interface

| project   | description  |
|-----------|--|
| interface | Interface name   |
| type      | Message type(1)broadcast-Broadcast<br>message;(2)multicast-Multicast message;(3)unicast-Unicast<br>message |
| rate      | min-Low threshold;max-High threshold   |

|                  |   |
|------------------|---|
| action           | Storm control actions,include(1)block-Blocking message;(2)shutdown-Close the interface  |
| punish-status    | Packet status of the current interface,including(1)block-When the rate is greater than max-rate and the storm control action is blocked, the status is blocked; (2)Normal-Forward normally;(3)shutdown-When the rate is greater than max-rate and the storm control action is to shut down the interface, the status is shut down |
| log              | Log switch status , on/off  |
| interval         | Storm control detection time interval, the unit is second, the default value is 5 seconds   |
| last-punish-time | Last time to implement storm control penalties  |

(2)By executing the storm- constrain action command to configure storm control actions and the storm- constrain command to configure storm control high and low thresholds, you can control storm packets to prevent flooding. During the storm control detection interval, when the average rate of receiving broadcast, multicast, or unicast packets on an interface is greater than the specified high threshold, Storm Control will block the interface or shut down the interface according to the configured action. When the storm control action is a blocking packet, if the traffic is below the minimum threshold, the interface returns to the normal forwarding state; when the storm control action is to shut down the interface, the interface cannot be automatically restored, you need to manually execute the no shutdown command to restore, you can cancel by Port storm control shutdown action configuration to restore.

(3The port traffic exceeds the upper threshold or falls back from the upper limit to the lower threshold and outputs log/trap information.

### 3.5 FLOW-CONTROL configuration

FLOW-CONTROL (flow control) is used to prevent data loss in the case of port blockage. In half-duplex mode, flow control is implemented by Backpressure technology, which makes the information source reduce the transmission rate. In full-duplex mode, the

|

---

flow control follows the IEEE802.3x standard, and the blocked port sends a "Pause" packet to the information source to suspend its transmission.

This section provides a detailed description of the configuration of FLOW-CONTROL, mainly including the following :

- Default configuration
- Set port flow control
- Close port flow control
- show flow control information

### **3.5.1 Default configuration**

The switches supports setting flow control for sending and receiving for each port. The default port haven't the function to open the flow control.

### **3.5.2 Set port flow control**

The following command configures port flow control to open in interface configuration mode:

```
flowcontrol
```

### **3.5.3 Close port flow control**

The following Command in the interface configuration mode close the port to send and receive side flow control:

```
no flowcontrol
```

### **3.5.4 Show flow control information**

The following Command in Normal mode or Privileged mode will show the flow control information of all the port:

```
show flowcontrol
```

The following Command in Normal mode or Privileged mode will show the flow control information of a certain port:

|

---

show flowcontrol interface <if-name>

Among them, <if-name> is the name of the port to query flow control information.

## 3.6 Port bandwidth configuration

Port bandwidth control is used to control the rate of port sending and receiving.

This section provides a detailed description of the port bandwidth configuration, mainly including the following: :

- Default configuration
- Configure port to send or receive bandwidth control
- Cancel port to send or receive bandwidth control
- Show the bandwidth control of port configuration

### 3.6.1 Default configuration

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

### 3.6.2 Configure port to send or receive bandwidth control

The following Command sets the port to send or receive bandwidth control in interface configuration mode:

```
portrate {egress | ingress} <rate>
```

egress means to control the bandwidth of the sent packet.

ingress means to control the bandwidth of the received data packets.

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

---

### 3.6.3 Cancel port to send or receive bandwidth control

The following Command cancels the bandwidth control of the port in the interface configuration mode :

```
no portrate {egress | ingress}
```

egress means to cancel the bandwidth control of sending packets.

ingress means to cancel the bandwidth control of received packets.

### 3.6.4 Show the bandwidth control of port configuration

The following Command can check the bandwidth control of port configuration in Normal mode or Privileged mode:

```
show portrate interface <if-name>
```

Among them, <if-name> is the name of the port to query bandwidth control information.

## 3.7 TRUNK configuration

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

All ports in the TRUNK group must be configured for the same speed and in full-duplex mode. The switch can support up to 32 groups of TRUNK, each group of TRUNK members can be up to 8. Please note that each port can only belong to a trunk group.

The LACP protocol is a protocol based on the IEEE802.3ad standard. The LACP protocol exchanges information with the peer through LACPDU (Link Aggregation Control Protocol Data Unit).

The LACP protocol is enabled on the interface in the aggregation group. The interface will notify the peer of its system LACP protocol priority, system MAC, port LACP protocol priority, port number, and operation key by sending LACPDUs. After receiving the LACPDU, the peer compares the information in it with the information received by other interfaces to select the interface that can be in the Selected state, so that both parties can agree on the interface in the Selected state

The operation key is a configuration combination that is automatically generated according to certain configurations of member ports during link aggregation, including port rate, duplex mode, up/down status, allowed VLANs on the port, and default VLAN ID of the port, The link type of the port (ie Trunk, Hybrid, Access type), etc. In the aggregation group, the member ports in the Selected state have the same operation key.

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

- LACP protocol configuration
- TRUNK group configuration
- TRUNK member port configuration
- TRUNK load balancing strategy configuration
- Show TRUNK

### 3.7.1 LACP protocol configuration

| command                           | description   | CLI mode                  |
|-----------------------------------|---|---------------------------|
| lacp system-priority <1-65535>    | Set the priority of lacp system                                       | Global configuration mode |
| no lacp system-priority           | Restore the default value of system priority 32768                    | Global configuration mode |
| lacp max-active-link-number <1-8> | Set the upper limit of LACP active aggregation port                   | Global configuration mode |
| no lacp max-active-link-number    | Restore the default upper limit of the LACP active aggregation port 8 | Global configuration mode |
| lacp port-priority <1-65535>      | Set the priority of lacp port   | Interface                 |

|                           |  |                              |
|---------------------------|--|------------------------------|
|                           |  | configuration mode           |
| no lacp port-priority     | Restore the default port priority 32768          | Interface configuration mode |
| lacp timeout (short long) | Set lacp port timeout, default long timeout      | Interface configuration mode |
| show lacp summary         | Show a simple situation of all lacp aggregation  | Privileged mode              |
| show lacp detail          | Show all lacp aggregation                        | Privileged mode              |
| show lacp <1-8>           | Display the details of the lacp aggregation port | Privileged mode              |
| show lacp port IFNAME     | Display the details of the lacp port             | Privileged mode              |
| show lacp system-id       | Display the status of lacp system                | Privileged mode              |
| show lacp counter <1-8>   | Display statistics of lacp aggregation port      | Privileged mode              |
| show lacp counter         | Display statistics of all lacp aggregation ports | Privileged mode              |
| clear lacp <1-8> counters | Clear the statistics of lacp aggregation port    | Privileged mode              |
| clear lacp counters       | Clear statistics of all lacp aggregation ports   | Privileged mode              |

### 3.7.2 TRUNK group configuration

The following Command creates a TRUNK group in Global configuration mode:

```
trunk <trunk-id>
```

Create a TRUNK group, the value range of <trunk-id> is 1-32, which means the ID of the TRUNK group to be created. Up to 8 groups of TRUNK can be configured; after the creation is successful, the interface name of the TRUNK group is trunk + id, such

as, the interface name of the TRUNK group with the group ID number 1 is trunk1. You can use the "interface trunk + id" Command in the configuration mode to enter the interface configuration mode, and then operate the trunk group. For example, use Command interface trunk1 to enter the trunk mode of trunk 1 and configure trunk 1.

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

```
trunk <1-32> dynamic
```

The following Command deletes a trunk group in Global configuration mode:

```
no trunk <trunk-id>
```

Ensure that the TRUNK group has no member ports when deleting the TRUNK group.

### 3.7.3 TRUNK member port configuration

The following Command adds a member port of the trunk group in the interface configuration mode:

```
trunk interface IFNAME (passive|)
```

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

The following Command deletes all member ports of the trunk group in interface configuration mode:

```
no trunk interface
```

The following Command deletes the specified trunk group member port in the interface configuration mode:

```
no trunk interface <if-name>
```

Can use this command multiple times to delete multiple member ports of the trunk group.

---

## 3.7.4 TRUNK load balancing strategy configuration

The following Command sets the load balancing strategy of TRUNK in the interface configuration mode:

```
trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip}
dst-mac-----Balanced strategy based on destination MAC
dst-ip-----Balanced strategy based on destination IP
src-dst-mac---Balanced strategy based on source MAC and destination MAC
src-dst-ip----Balanced strategy based on source IP and destination IP
src-mac-----Balanced strategy based on source MAC
src-ip-----Balanced strategy based on source IP
```

The following Command sets the default TRUNK load balancing strategy in interface configuration mode:

```
no trunk load-balance
```

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

## 3.7.5 Show TRUNK

The following Command checks all TRUNK group configurations in Normal mode or Privileged mode:

```
show trunk
```

The following Command checks the configuration of the specified trunk group in Normal mode or Privileged mode:

```
show trunk <trunk-id>
```

Among them,<trunk-id> is the ID number of the TRUNK group to be queried.

## 3.8 Jumbo frames configuration

### 3.8.1 Introduction to Jumbo Frames

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

---

## 3.8.2 Jumbo Frame configuration

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

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

Show the Jumbo frame length supported by port

```
Switch#show jumbo frame ge1/1
```

| Port  | Jumbo frame(bytes) |
|-------|--------------------|
| ge1/1 | 2000               |

## 3.9 Redundant ports configuration

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

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

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

- Redundant ports configuration
- Display of redundant ports

### 3.9.1 Redundant ports configuration

The switch can be configured with 8 groups of redundant ports, and a group of redundant ports can only be configured with 2 ports; one port can only be configured into one redundant port group.

A redundant port group can be configured with a primary-port and secondary-port.

When the configuration enables redundant port groups:

- 1、 When the two ports are in the LINK UP state at the same time, the primary-port is set to the Active state, and the secondary-port is set to the Disable state;
- 2、 If only one port is in the LINK UP state, the current LINK UP port is set to the Active state, and the other port is in the Disable state;
- 3、 Otherwise, both ports are in Disable state.

If a LINK DOWN event occurs on a port in the Active state, another port will be tried to be placed in the Active state.

Another configuration parameter is the force-switch, which is when the secondary-port is Active and the primary-port is in the Disable state. If a LINK UP event occurs in the primary-port at this time, it is decided whether to switch to the primary-port again. Active, secondary-port is Disabled. If force-switch is configured as enable, the switch is forced, otherwise the port status of the original redundant port group will be retained.

| command  | description  | CLI mode                        |
|--|--|---------------------------------|
| redundant-port <1-8><br>primary-port IFNAME<br>secondary-port IFNAME<br>[force-switch] | Configure a set of redundant ports,<br><1-8> is the group number<br>primary-port IFNAME is the name of<br>the primary port interface,<br>secondary-port IFNAME is the name<br>of the secondary port interface,<br>force-switch is whether enables the<br>force switch. | Global<br>configuration<br>mode |
| redundant-port <1-8><br>force-switch   | Switch of Enable the forced switch of<br>the redundant port  | Global<br>configuration<br>mode |
| no redundant-port <1-8>  | Delete redundant port group  | Global<br>configuration<br>mode |
| no redundant-port <1-8><br>force-switch  | Switch of turn off the forced switch of<br>the redundant port  | Global<br>configuration<br>mode |

---

## 3.9.2 Display of redundant ports

Commands to display redundant ports

| command             | description  | CLI mode        |
|---------------------|--|-----------------|
| show redundant-port | Display the configuration of all redundant port groups in the system | Privileged mode |

## 3.10 DLDP configuration

DLDP (device link detection protocol): is a Layer 2 protocol used to monitor the physical configuration of Ethernet links connected by optical fibers or twisted pairs. When a unidirectional link occurs (only one direction can be transmitted) For example, if I can send the data to you, you can also receive it, but when you send me the data that I cannot receive), DLDP can detect this situation, close the corresponding interface and send a warning message. Unidirectional links may cause many problems, especially spanning tree, which may cause loopback. Note: DLDP needs to be supported by devices at both ends of the link to function properly..

DLDP supports two working modes; normal mode (default) and aggressive mode.

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

Aggressive mode: In this mode, DLDP can detect unidirectional links. And it will try to rebuild the link and send a DLDP message for 8 seconds continuously. If there is no DLDP echo response, the port will be placed in errdisable state.

| command                  | description                  | CLI mode                  |
|--------------------------|------------------------------|---------------------------|
| dldp enable              | Enable DLDP globally         | Global configuration mode |
| dldp message time <time> | DLDP packet sending interval | Global configuration mode |
| dldp port                | Port enable DLDP             | Interface                 |

|                    |  |                              |
|--------------------|--|------------------------------|
|                    |  | configuration mode           |
| dldp aggressive    | Enable port aggressive mode, default normal mode | Interface configuration mode |
| show dldp <ifname> | View port DLDP information                       | Privileged mode              |

## 3.11 LLDP configuration

At present, there are more and more types of network devices and their respective configurations are intricate. In order to enable devices of different manufacturers to discover and interact with their systems and configuration information on the network, a standard information exchange platform is required.

LLDP (Link Layer Discovery Protocol) was created in this context, it provides a standard link layer discovery method, you can the main capabilities of the local device, management address, device identification , Interface identification and other information are organized into different TLV (Type/Length/Value), and encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit) and released to direct After receiving this information, the neighbor saves it in the form of a standard MIB (Management Information Base) for the network management system to query and judge the communication status of the link. .

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

- LLDP configuration
- LLDP display

### 3.11.1 LLDP configuration

There are 4 working modes of LLDP port:

TxRx : Both send and receive LLDP messages.

Tx : Only send and do not receive LLDP packets.

Rx : Only receive and do not send LLDP packets.

Disable : Neither send nor receive LLDP messages.

When the LLDP working mode of the port changes, the port will initialize the protocol state machine. In order to avoid frequent changes of the port working mode and cause the port to continuously perform the initialization operation, the port initialization delay time can be configured. When the port working mode changes, the initialization operation is delayed for a period of time before the initialization operation is performed.

| command  | description   | CLI mode                     |
|--|---|------------------------------|
| lldp global enable   | LLDP global enable command.                                 | Global configuration mode    |
| lldp hold-multiplier <num>   | Lldp TTL multiple   | Global configuration mode    |
| lldp timer<br>[<reinit-delay><time>][<tx-delay><time>][<tx-interval ><time>] | Configure various LLDP timers                               | Global configuration mode    |
| lldp enable  | Enable interface LLDP                                       | Interface configuration mode |
| lldp admin-status{ disable rx tx rxtx}                                       | Configure the working mode of the LLDP port.                | Interface configuration mode |
| lldp check-change-interval <time>  | Configure the interval for refreshing interface information | Interface configuration mode |
| lldp management-address <A.B.C.D>  | Configure the interface LLDP management address             | Interface configuration mode |
| lldp tlv-enable{ dot1-tlv dot3-tlv med-tlv }                                 | Configure interface LLDP extended capability set switch     | Interface configuration mode |

### 3.11.2 LLDP display

LLDP commands

| command | description | CLI mode |
|---------|-------------|----------|
|---------|-------------|----------|

---

|   |  |                 |
|---|--|-----------------|
| show lldp configuration [ifname]        | Display lldp configuration information | Privileged mode |
| show lldp local-information [ifname]    | Show lldp local information            | Privileged mode |
| show lldp neighbor-information [ifname] | Display lldp neighbor information      | Privileged mode |
| show lldp statistics [ifname]           | Display lldp packet statistics         | Privileged mode |
| show lldp status [ifname]               | Display lldp status information        | Privileged mode |

## Chapter4 **Configure** **port-based MAC security**

---

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

- Introduction
- MAC binding configuration

- 
- MAC filtering configuration
  - Port learning limit configuration
  - Port protection configuration

## 4.1 Introduction

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

MAC binding can bind MAC and port together, restricting a specified MAC address to access the network only on a specified port; at the same time, this port can only allow these bound MAC addresses to access the network; a port can be simultaneously Bind multiple MAC addresses. MAC binding can be applied to a designated port at the same time as 802.1x. This function is very useful for some devices that do not have 802.1x functions or devices that are inconvenient to use 802.1x, such as printers and file servers.

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

Port learning control can control the number of MAC addresses that a port can learn dynamically. If a port specifies that it can dynamically learn the number of MAC addresses, when the number of MAC addresses learned by this port is equal to the number configured for this port, it will no longer learn new MAC addresses. For these new MAC addresses The packet will be dropped.

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

## 4.2 MAC binding configuration

MAC binding configuration supports manual binding of MAC addresses and automatic binding of MAC addresses. Manually binding the MAC address is that the user enters the MAC address one by one through the command to bind to the port. The automatic MAC address binding is to read the existing entry of the port in the layer 2 hardware forwarding table and directly perform MAC address binding. The command to read the second layer hardware table is Show bridge fdb.

#### Configuration command

| command  | description   | CLI mode                           |
|--|---|------------------------------------|
| switchport-security mac-bind<br>HHHH.HHHH.HHHH vlan<br><1-4094> qosprofile<br>{qp0 qp1 qp2 qp3 <br>qp4 qp5 qp6 qp7}    | Manually bind a MAC<br>address to an interface and<br>configure the priority queue<br>of the entry.   | Interface<br>configuration<br>mode |
| switchport-security mac-bind<br>auto-conversion number<br><1-8191> qosprofile<br>{qp0 qp1 qp2 qp3 <br>qp4 qp5 qp6 qp7} | Automatically convert the<br>specified number of MAC<br>addresses of an interface<br>into MAC binding<br>configuration and configure<br>the priority queue of the<br>entry. | Interface<br>configuration<br>mode |
| switchport-security mac-bind<br>auto-conversion vlan<br><1-4094> qosprofile<br>{qp0 qp1 qp2 qp3 <br>qp4 qp5 qp6 qp7}   | Automatically convert the<br>MAC address of a specified<br>VLAN of an interface into<br>MAC binding configuration,<br>and configure the priority<br>queue of the entry.     | Interface<br>configuration<br>mode |
| show port-security mac-bind<br>[IFNAME]  | Show MAC binding<br>configuration   | Privileged<br>mode                 |

Note :

The reasons for invalid or failed MAC address binding may be as follows :

The port has been configured with 802.1x ;

The port has been configured with MAC filtering or port learning restrictions ;

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

The switch's L2 table is full.

### 4.3 MAC filtering configuration

MAC filtering configuration supports manual binding of MAC addresses and automatic binding of MAC addresses. Manually binding of MAC address is that users can

input the MAC to be filtered one by one through Command to bind to the port. automatic binding of MAC addresses is to read the existing entries of the port in the layer 2 hardware forwarding table and directly perform MAC filtering configuration. The command to read the second-level hardware table is Show bridge fdb.

Configuration command

| command   | description   | CLI mode                     |
|---|---|------------------------------|
| switch port-security<br>mac-filter<br>HHHH.HHHH.HHHH vlan<br><1-4094> | Manually configure MAC filtering for an interface   | Interface configuration mode |
| switch port-security mac-filter auto-conversion<br>number <1-8191>    | Automatically convert the specified number of MAC addresses of an interface into MAC filtering configuration. | Interface configuration mode |
| switch port-security mac-filter<br>HHHH.HHHH.HHHH vlan<br><1-4094>    | Automatically convert the MAC address of a specified VLAN of an interface into MAC filtering configuration.   | Interface configuration mode |
| show port-security mac-filter<br>[IFNAME]                             | Show MAC binding configuration  | Privileged mode              |

Note :

The reasons for MAC filtering configuration being invalid or failing may be as follows :

The port has been configured with MAC binding or enabled 802.1x protocol function ;

The MAC address has been bound to another port, or MAC binding is configured ;

The switch's L2 table is full.

## 4.4 Port learning limit configuration

The switch can configure the maximum number of dynamic learning addresses for each 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 MAC address exceeds this number, it cannot learn and forward on this port.

If no learning limit is configured, a port can learn up to 8191 MAC addresses.

#### Configuration commands

| command  | description  | CLI mode                           |
|--|--|------------------------------------|
| switchport port-security<br>learn-limit <0-8191> | Configure the number of<br>MAC addresses that an<br>interface can learn. | Interface<br>configuration<br>mode |
| no switchport port-security<br>learn-limit       | Delete the number of MAC<br>addresses that an interface<br>can learn.    | Interface<br>configuration<br>mode |
| show port-security learn-limit<br>[IFNAME]       | Display port learning<br>configuration                                   | Privileged<br>mode                 |

#### Configuration example

Configure port ge1/5 to learn only 7 MAC addresses.

```
Switch#configure terminal
```

```
Switch(config)interface ge1/5
```

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

#### Note:

The reasons for invalid or failed port learning may be as follows:

The port has been configured with MAC binding or enabled 802.1x protocol function.

## 4.5 Port protection configuration

### 4.5.1 Introduction to port protection configuration

In order to achieve Layer 2 isolation between data packets, ports can be divided into different VLANs, but VLAN resources will be wasted. Configuring the port as a protection port can achieve the isolation of ports in the same VLAN, providing users with a safer and more flexible networking solution.

Each port can be configured as a protected port. The protected ports cannot communicate with each other and can only communicate with unprotected ports.

There are two application modes:

1. Only one port is not configured as a protection port, all other ports are isolated;
2. To prevent some unsafe ports from sniffing data from other ports (even servers), set these ports as protection ports.

---

## 4.5.2 Port protection configuration

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

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

Display ports configured as protection ports

```
Switch#show port-security protect
```

```
Port    Port protected
```

```
-----
```

```
ge1/1   ON
```

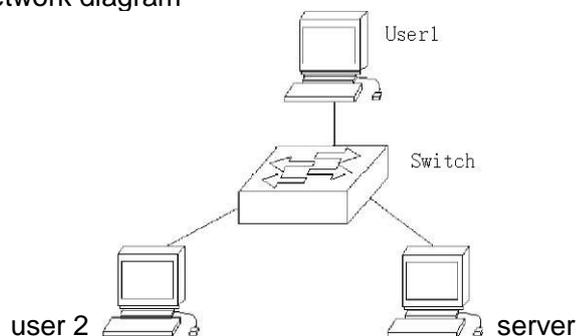
Typical examples of protection ports configuration

Networking requirements

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

User 1 and user 2 servers belong to the same vlan. It is required that user 1 and user 2 cannot communicate with each other, but can communicate with the server.

Network diagram



Configuration steps

```
Switch>enable
```

```
Switch#config terminal
```

```
Switch(config)#interface ge1/1
```

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

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

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

```
Switch(config-ge1/2)#exit
```

```
Switch(config)#exit
```

```
Switch#show port-security protect
```

|

---

| Port  | Port protected |
|-------|----------------|
| ----- | -----          |
| ge1/1 | ON             |
| ge1/2 | ON             |

## Chapter5 **Configure port IP and MAC binding**

---

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

- Introduction
- IP and MAC binding configuration
- Configuration example
- Configuration troubleshooting

,

---

## 5.1 ,Introduction

Configuring IP and MAC binding on the Layer 2 switch port is a static defense measure against ARP attacks. The ARP attacker attacks the user by sending an ARP message carrying a fake MAC address, causing the user's local ARP cache table to be overwritten by the attacker's MAC address, and normal data flow to the attacker. Configuring static binding of the user's IP address and MAC address on the switch port can effectively filter ARP attack packets.

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

IP MAC binding, ACL, 802.1x anti-ARP spoofing and DHCP SNOOPING all use the same system resource CFP. When configuring, pay attention to whether the resources of CFP are exhausted. During design, we formulate the compatibility relationship between them. The following table:

|                | IP MAC Binding | ACL            | 802.1x         | DHCP SNOOPING  |
|----------------|----------------|----------------|----------------|----------------|
| IP MAC binding | compatible     | Not compatible | compatible     | compatible     |
| ACL            | Not compatible | compatible     | Not compatible | Not compatible |
| 802.1x         | compatible     | Not compatible | compatible     | Not compatible |
| DHCP SNOOPING  | compatible     | Not compatible | Not compatible | compatible     |

CFP is a limited hardware resource. On average, only 16 IP MAC binding entries can be configured per port. Therefore, in a network with many access hosts, if only a few ports or a few IP and MAC addresses need to be controlled, you can use the static IP MAC binding function to avoid CFP function exhaustion and lead to data forwarding failure.

In addition, as for whether to use 802.1x or DHCP SNOOPING protocol, it depends on the current situation. If you use a static IP address configuration and use 802.1x protocol to access the network, you must use 801.1x anti-ARP spoofing to be effective. Situation, you need to use DHCP SNOOPING protocol.

## 5.2 IP / MAC binding configuration

IP and MAC binding configured in interface mode

Configure port IP and MAC binding

Switch#configure terminal

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

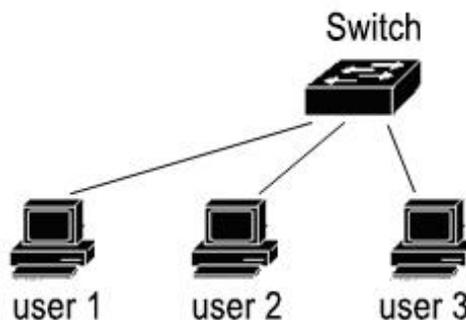
Delete port IP and MAC binding  
Switch#configure terminal  
Switch(config)#interface ge1/1  
Switch(config-ge1/1)#no ip mac-bind A.B.C.D MAC

Show configuration  
Show binding entries for all ports  
show ip mac-bind

Show binding entries for an interface  
show ip mac-bind IFNAME

## 5.3 Configuration example

There are user 1, user 2, and user 3 in the network, and the user's IP and MAC are bound to the port to prevent ARP attacks.



```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip mac-bind 192.168.1.100 0011.5b34.42ad
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#ip mac-bind 192.168.1.101 0011.6452.135d
```

```
|  


---

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

---

## 5.4 Configuration Debug

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

- 1、 The system CFP resources are exhausted.
- 2、 The current interface is configured with ACL filtering.
- 3、 The configured interface is a Layer 3 interface or a trunk interface.

## Chapter6 Port loop detection

---

This chapter mainly including the following :

- Introduction
- Protocol principle
- Configuration introduction

---

## 6.1 Introduction

When a loop occurs on a port of the switch, it will cause a broadcast storm on this port, and learn the source MAC addresses of all broadcast packets to this looped port, which will cause the device to fail to forward normally.

## 6.2 Protocol principle

The Ethernet Loopback Detection (ELD) protocol can detect loops through the interaction of data packets and block the ports where loops occur. The ELD protocol is a protocol based on port calculation, and can only detect the loop that occurs on this port.

### 6.2.1 Testing process

When the ELD protocol is enabled on a port, a timer will be enabled on this port periodically. When the timer expires, a loop detection packet will be sent. If a loop detection packet sent by itself is received within a timer period, then If there is a loop on this port, it will perform the operation of blocking the loop on this port and clear the FDB table of this port.

If a port belongs to a port member of multiple VLANs, then this port will automatically send loop detection packets to all VLANs. In other words, this port will automatically detect whether there is a loop in all VLANs to which it belongs.

### 6.2.2 Recovery mode

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

Automatic recovery is that when a port is blocked by a loop, the ELD protocol enables a recovery timer. After the timer expires, it will perform a reverse operation to block the loop and enable the loop detection timer again at this port.

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

### 6.2.3 Protocol security

The ELD protocol is vulnerable to attacks in the network, which means that users can send ELD protocol packets to a port enabled with the ELD protocol according to the packet format of the ELD protocol, resulting in the port being blocked and causing errors

in the absence of loops.

The ELD protocol uses two strategies to prevent similar attacks and reduce errors to a minimum.

Decision one, first of all, the ELD protocol is a non-interactive protocol, which means that it does not depend on other devices, then the data packet itself can be simply encrypted. Our operation here is to send an ELD protocol packet carrying a key, and the user cannot disguise this protocol packet without the key.

Decision two, mainly to prevent attackers from reflecting protocol packets through packet capture attacks, you can configure the format of the data packets received by the switch within a certain period to prevent attacks, this requires the user to configure.

## 6.3 Configuration Introduction

The ELD protocol is implemented based on the port, and there is no unified enable command.

### 6.3.1 Global configuration

Global configuration is the uniform property of the configuration protocol.

| command                                 | description   | mode                      |
|---|---|---------------------------|
| loop-detection detection-time <1-65535> | Configure the time period for loop detection. The double time must be less than the recovery time period. The default value is 5 seconds.   | Global configuration mode |
| loop-detection resume-time <10-65535>   | Configure the automatic recovery time period. The automatic recovery time must be greater than 2 times of the loop check time. If automatic recovery is enabled, this configuration will take effect. The default recovery time is 600 seconds. | Global configuration mode |
| loop-detection protocol-safety          | Enable protocol security check, which is off by default.  | Global configuration mode |
| loop-detection respond-packets          | Configure the number of packets that must be received within a certain period of time. If the protocol security check is enabled, this configuration will take effect. The default value is 10  | Global configuration mode |

---

## 6.3.2 Interface configuration

Interface configuration is the configuration of each port.

| command   | description   | mode                         |
|---|---|------------------------------|
| Loop-detection enable                                     | Enable ELD protocol on a port   | Interface configuration mode |
| Loop-detection resume                                     | Manually recover and restart the loop check.  | Interface configuration mode |
| loop-detection resume-mode {automation   manual}          | Configure the recovery mode, select manual recovery or automatic recovery, the default is automatic recovery. | Interface configuration mode |
| loopback-detection shutdown-mode {no-shutdown   shutdown} | Command to configure whether the port shuts down when a loop occurs.  | Interface configuration mode |

## 6.3.3 Show configuration

Show loop-detection [ifname]

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

---

## Chapter7 VLAN configuration

---

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

This chapter mainly includes the following :

- VLAN Introduction
- VLAN Configuration
- VLAN Configuration example

---

## 7.1 VLAN Introduction

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

- Benefits of VLAN
- VLAN ID
- VLAN port member type
- The default VLAN of the port
- Port VLAN mode
- VLAN trunking
- Data flow forwarding in VLAN
- VLAN subnet

### 7.1.1 Benefits of VLAN

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

Using VLAN has the following benefits :

- VLAN can effectively control the traffic in the network.

In a traditional network, regardless of whether it is necessary, all broadcast packets are transmitted to all devices, which increases the load on the network and devices.

But the VLAN can organize the devices in a logical network as needed. A VLAN is a broadcast domain. Broadcast packets are only transmitted inside the VLAN and do not cross the VLAN. By dividing the VLAN, you can effectively control the traffic in the network.

- VLAN can improve the security of the network.

The devices in a VLAN can only communicate with devices in the same VLAN at Layer 2. If you want to communicate with another VLAN, you must use Layer 3 forwarding. If you do not establish Layer 3 forwarding between VLANs, it can not communicate. The role of isolation ensures data security in each VLAN. For example, a company's R & D department does not want to share data with the marketing department. You can establish

a VLAN in the R & D department, establish a VLAN in the marketing department, and do not establish a Layer 3 communication channel between the two VLANs. .

- VLAN makes the movement of the device convenient.

If a device moves from one location to another and belongs to a different network in traditional network, you need to modify the network configuration of the mobile device, which is very inconvenient for users.

VLAN is a logical network, you can put Devices that are not in the same physical location are placed on the same network. When the device moves, the device can also belong to this VLAN, so that the moving device does not need to modify any configuration.

## 7.1.2 VLAN ID

Each VLAN has an identification number, called VLAN ID. The range of VLAN ID is from 0 to 4095, where 0 and 4095 are not used, and the actual effective is only 1 to 4094. The VLAN ID uniquely identifies a VLAN.

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

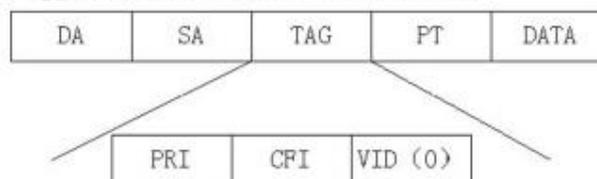
There are three types of data frames transmitted in a VLAN in the network: untagged data frames, tagged data frames with VID 0, and tagged data frames with VID non-zero.

The following figure shows three different data frame formats.

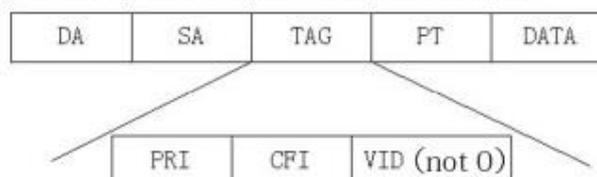
Unmarked data frame



Tagged data frame, but VLAN ID is 0



Tagged data frame, but VLAN ID is not 0



---

All data frames inside the switch are marked.

If a untagged data frames is entered into the switch, the switch will add a tag to the data frame and select a VLAN ID value to fill in the tagged VID.

If a tagged data frames with VID 0 enters the switch, the switch selects a VLAN ID value to fill in the tagged VID.

If a tagged data frames with VID non-zero is entered into the switch, the frame will not change.

- 

### **7.1.3 VLAN port member type**

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

A port can belong to tagged or untagged members of one or more VLANs. If a port belongs to tagged members of two or more VLANs, this port is also called VLAN trunking port.. A port can belong to untagged members of one or more VLANs and tagged members of one or more VLANs.

### **7.1.4 The default VLAN of the port**

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

### **7.1.5 Port VLAN Mode**

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

port's VLAN.

The port in ACCESS mode is an access port that directly faces the user. The port can only belong to an untagged member of a VLAN. The default VLAN is the VLAN specified by the user. When the port belongs to an untagged member of only one VLAN, you can specify the Port VLAN mode is ACCESS mode.

The port in TRUNK mode is a trunk port that is directly connected to the switch. The port can belong to one or more VLAN tagged members, but cannot belong to any VLAN untagged members. The default VLAN of the port is 1, and it cannot be changed.

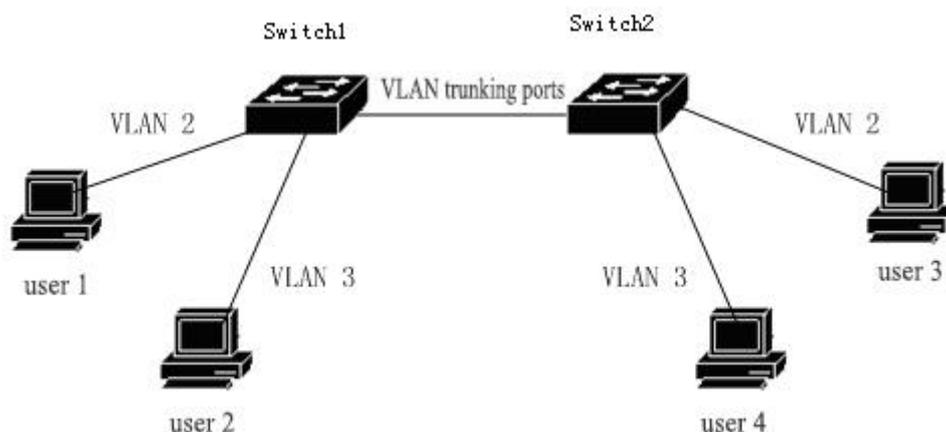
The port in HYBRID mode is a trunk port that is directly connected to the switch. The port can belong to one or more VLAN tagged members and / or one or more VLAN untagged members. The default VLAN of the port can be changed.

In practical applications, users can choose Port VLAN mode according to the specific situation.

## 7.1.6 VLAN Trunk

If a port belongs to tagged members of two or more VLANs, then this port is also called VLAN trunking port. Two switches can be connected by VLAN trunking ports, so that two or more common VLANs can be divided between the two switches.

The following figure is an example of VLAN trunking. The two switches are connected by VLAN trunking ports, which are the trunk ports of VLAN 2 and VLAN 3. Each switch is divided into two VLANs, namely VLAN 2 and VLAN 3, and there is one user in each VLAN. user1 can communicate with user 3, user 2 can communicate with user 4, user 1 and user 3 cannot communicate with user 2 and user 4.



---

## 7.1.7 Data flow forwarding in VLAN

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

- Determine the VLAN to which the packet belongs .
- Determine whether the packet is a broadcast packet, a multicast packet or a unicast packet.
  - Determine the output port according to different data packets (can be zero, one or more output ports), if there is no output port, discard the data packet.
  - Determine whether the outgoing packet is tagged according to the member type of the output port in the VLAN
    - Sent 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.

If the received packet is not tagged or tagged but the VID value in the tag is 0, the VLAN to which the packet belongs is the default VLAN of the port.

2) How to determine the type of packet :

If the destination MAC address of the received packet is FF: FF: FF: FF: FF: FF, then the packet is a broadcast packet.

If the received packet is not a broadcast packet and the 40th bit of its destination MAC address is 1, the packet is a multicast packet.

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

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

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

If the input packet is a multicast packet, first look up the Layer 2 hardware multicast forwarding table based on the destination multicast MAC address and the VLAN to which it belongs. If a matching multicast entry is found, the common port (AND operation) in the

---

output port in the multicast entry and the member port in the VLAN belongs to the output port of the packet. If there is no common port, the packet is discarded. If no matching multicast entry is found in the Layer 2 hardware multicast forwarding table, the output port is determined according to the forwarding mode of the Layer 2 hardware multicast forwarding table. If it is in the unregistered multicast forwarding mode, multicast packets are treated as broadcasts, and all member ports of the VLAN to which they belong are the output ports of the packets. If it is in register forwarding mode, there is no output port and the packet is dropped.

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

#### 4) Send data packets :

After determining the output port of the input data packet, the data 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 out of the output port without a tag.

If an output port is a tagged member of the VLAN to which the packet belongs, the packet is tagged when it is sent from the output port, and the VID value in the tag is the value of the VLAN to which the packet belongs.

## 7.2 VLAN configuration

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

- Create and delete VLAN
- VLAN mode of the Configure port
- VLAN configuration in ACCESS mode
- VLAN configuration in TRUNK mode
- VLAN configuration in HYBRID mode

- VLAN subnet configuration
- View VLAN information

## 7.2.1 Create and delete VLAN

Before creating and deleting VLANs, users need to use the `vlan database` command in the global configuration mode to enter the VLAN configuration mode, and create and delete VLANs in this mode..

The system has created VLAN 1 by default, and VLAN 1 cannot be deleted by users. The commands for creating and deleting VLANs are as follows:

| command                              | description   | CLI mode                |
|--------------------------------------|---|-------------------------|
| <code>vlan &lt;vlan-id&gt;</code>    | 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 |
| <code>no vlan &lt;vlan-id&gt;</code> | Delete a VLAN, if the VLAN does not exist, it will not be processed, otherwise delete the VLAN. The parameters range from 2 to 4094.  | VLAN configuration mode |

## 7.2.2 Port VLAN mode configuration

Before configuring a port's VLAN, you need to specify the port's VLAN mode. By default, the port's VLAN mode is ACCESS. The commands for specifying the VLAN mode of the port are as follows:

| command                             | description   | CLI mode                     |
|-------------------------------------|---|------------------------------|
| <code>switchport mode access</code> | The VLAN mode of the designated port is ACCESS mode. After this command is executed, the port is an untagged member of VLAN | Interface configuration mode |

|                        |   |                              |
|------------------------|---|------------------------------|
|                        | 1, and the default VLAN of the port is 1.   |                              |
| switchport mode trunk  | The VLAN mode of the designated port is TRUNK mode. After this command is executed, the port is a tagged member of VLAN 1, and the default VLAN of the port is 1.     | Interface configuration mode |
| no switchport trunk    | The VLAN mode of the port is no longer the TRUNK mode, and returns to the default situation, namely the ACCESS mode.  | Interface configuration mode |
| switchport mode hybrid | The VLAN mode of the designated port is HYBRID mode. After this command is executed, the port is an untagged member of VLAN 1, and the default VLAN of the port is 1. | Interface configuration mode |
| no switchport hybrid   | The VLAN mode of the port is no longer HYBRID mode, and returns to the default situation, namely ACCESS mode.   | Interface configuration mode |

### 7.2.3 VLAN configuration in ACCESS Mode

Before configuring the port for VLAN, you need to specify the VLAN mode of the port as ACCESS mode. In this VLAN mode, the port is the untagged member of VLAN 1 by default, and the default VLAN of the port is 1. The VLAN configuration commands in ACCESS mode are as follows: :

| command                | description              | CLI mode  |
|------------------------|--------------------------|-----------|
| switchport access vlan | Configure the port as an | Interface |

|                           |  |                              |
|---------------------------|--|------------------------------|
| <vlan-id>                 | untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. The parameters range from 2 to 4094.                  | configuration mode           |
| no switchport access vlan | The VLAN configuration of the port returns to the default, that is, the port is an untagged member of VLAN 1, and the default VLAN of the port is 1. | Interface configuration mode |

## 7.2.4 VLAN configuration in TRUNK mode

Before configuring the port for VLAN, you need to specify the VLAN mode of the port as TRUNK mode. In this VLAN mode, the port is the tagged member of VLAN 1 by default, and the default VLAN of the port is 1. The VLAN configuration commands in TRUNK mode are as follows:

| Command                                   | Description   | CLI mode                     |
|---|---|------------------------------|
| switchport trunk native vlan<br><vlan-id> | Configure the default VLAN of the port, which is pvid. The parameters range from 2 to 4094.                                       | Interface configuration mode |
| switchport trunk allowed<br>vlan all      | The configuration port is a tagged member of all VLANs. For newly created VLANs, the port is also a tagged member of these VLANs. | Interface configuration mode |
| switchport trunk allowed<br>vlan none     | Except for VLAN1, this port is no longer a tagged member of all other VLANs.  | Interface configuration mode |
| switchport trunk allowed                  | Configure the port to   | Interface                    |

|   |  |                              |
|---|--|------------------------------|
| vlan add <vlan-list>                                | become a tagged member of one or more VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".  | configuration mode           |
| switchport trunk allowed<br>vlan remove <vlan-list> | Remove the port from the specified VLAN or VLANs and no longer be a tagged member of these VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5". | Interface configuration mode |

## 7.2.5 VLAN configuration in HYBRID mode

Before configuring the port for VLAN, you need to specify the VLAN mode of the port as HYBRID mode. In this VLAN mode, the port is the untagged member of VLAN 1 by default, and the default VLAN of the port is 1. The VLAN configuration commands in HYBRID mode are as follows:

| Command                                    | Description   | CLI mode                     |
|--|---|------------------------------|
| switchport hybrid native vlan<br><vlan-id> | Configure the port as an untagged member of the specified VLAN and the default VLAN of the port as the specified VLAN. The parameters range from 2 to 4094. | Interface configuration mode |
| no switchport hybrid native<br>vlan        | Remove the port from the default VLAN and no longer   | Interface configuration      |

|  |  |                                    |
|--|--|------------------------------------|
|  | be a tagged or untagged member of the default VLAN. The default VLAN of the port returns to 1.   | mode                               |
| switchport hybrid allowed<br>vlan all                                      | The configuration port is a tagged member of all VLANs (except VLAN 1). For newly created VLANs, the port is also a tagged member of these VLANs.  | Interface<br>configuration<br>mode |
| switchport hybrid allowed<br>vlan none                                     | Except for VLAN1, the port is no longer a tagged or untagged member of all other VLANs, and the default VLAN of the port returns to 1.   | Interface<br>configuration<br>mode |
| switchport hybrid allowed<br>vlan add <vlan-list><br>egress-tagged enable  | Configure the port to become a tagged member of one or more VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".              | Interface<br>configuration<br>mode |
| switchport hybrid allowed<br>vlan add <vlan-list><br>egress-tagged disable | Configure the port to become an untagged member of the specified VLAN or VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5". | Interface<br>configuration<br>mode |
| switchport hybrid allowed<br>vlan remove <vlan-list>                       | Remove the port from the specified VLAN or VLANs and no longer be a tagged   | Interface<br>configuration<br>mode |

|  |   |  |
|--|---|--|
|  | or untagged member of these VLANs If the default VLAN of the port belongs to the specified VLAN, the default VLAN returns to 1. |  |
|--|---|--|

## 7.2.6 View VLAN information

The commands for viewing VLAN information are as follows:

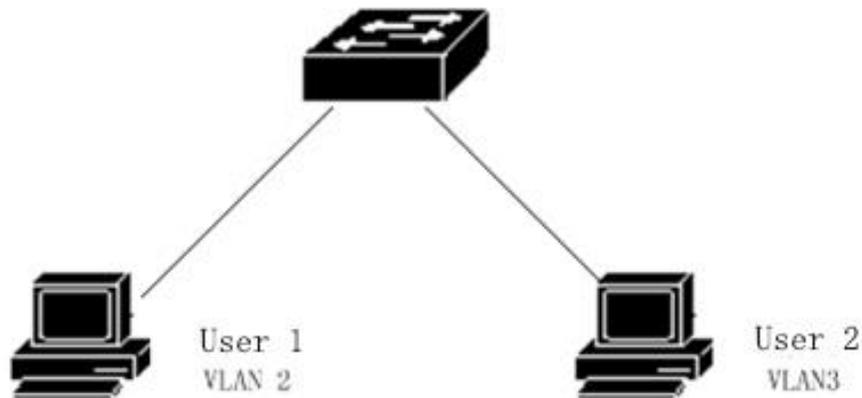
| Command             | Description  | CLI mode                         |
|---------------------|--|----------------------------------|
| show vlan [vlan-id] | If no parameters are entered, all VLAN information is displayed, and if parameters are entered, the information of a specified VLAN is displayed. The parameters range from 1 to 4094. | Normal mode ,<br>Privileged mode |
| show interface      | Display the VLAN related information of all ports of the system, such as VLAN mode, default VLAN, etc.   | Normal mode ,<br>Privileged mode |
| show running-config | View the current configuration of the system, you can view the VLAN configuration.   | Privileged mode                  |

## 7.3 VLAN configuration example

### 7.3.1 PORT based VLAN

#### 1) configuration

There are two users, user 1 and user 2. The two users need to be in different VLANs due to different network functions and environments. User 1 belongs to VLAN 2 and is connected to port ge1 / 1 of the switch. User 2 belongs to VLAN 3 and connects to port ge1 / 2 of the switch.



The configuration of the switch is as follows:

Crear VLAN

```
Switch#config t
```

```
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2
```

```
Switch(config-vlan)#vlan 3
```

Assign ports to VLAN

```
Switch#config t
```

```
Switch(config)#interface ge1/1
```

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

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

```
Switch(config-ge1/1)#exit
```

```
Switch(config)#interface ge1/2
```

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

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

## 2) Debug

After configuration, it is a normal phenomenon that PCs in different VLANs cannot communicate, because communication must go through Layer 3 routing and forwarding between different VLANs. If PCs in the same VLAN cannot communicate, you must Do the following verification:

show vlan

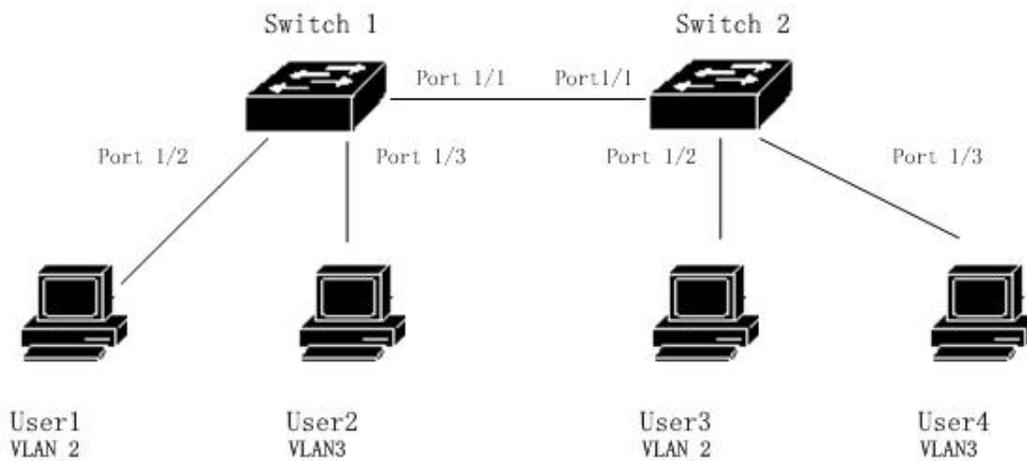
View the status of all VLAN member ports

show vlan <vlan-id>

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

## 7.3.2 802.1Q based VLAN

### 1) Configuration



There are two switches to connect two users:

| Users | VLAN | Connection port | switch  | Cascade port |
|-------|------|-----------------|---------|--------------|
| User1 | 2    | 1/2             | Switch1 | 1/1          |
| User2 | 3    | 1/3             | Switch1 | 1/1          |
| User3 | 2    | 1/2             | Switch2 | 1/1          |
| User4 | 3    | 1/3             | Switch2 | 1/1          |

Need to configure on two switches.

Switch 1 configuration:

```
Switch#config t
```

```
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2
```

```
Switch(config-vlan)#vlan 3
```

|

---

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

Switch 2 configuration:

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

## 2) Debug

Cross-switch vlan, PCs in the same vlan can communicate. If not, please check the following :

- Whether the port connected to the PC belongs to the corresponding VLAN, and apply the ACCESS mode to join this vlan.

- Cascade port 1/1 is added to each vlan, and port 1/1 is in trunk mode.

## 7.4 MAC, IP subnet, protocol VLAN

### 7.4.1 Introduction to MAC, IP subnet, protocol VLAN

MAC-based VLANs are divided according to the source MAC address of the message. After receiving the untagged (or tag is 0) packet from the port, the device determines the VLAN to which the packet belongs according to the source MAC address of the packet, and then automatically divides the packet into the designated VLAN for transmission;

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

Protocol-based VLANs assign different VLAN IDs to packets based on the protocol type to which the packets received by the port belong. The protocols that can be used to divide VLANs are IP, IPV6, IPX, etc.

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

Before configuring a VLAN based on MAC, IP subnet, or protocol, you must first create the corresponding VLAN.

| command                            | description                                   | CLI mode                |
|------------------------------------|---|-------------------------|
| mac-vlan mac WORD vlan<br><1-4094> | Create a VLAN based on the source MAC address | VLAN configuration mode |
| no mac-vlan mac WORD               | Delete a VLAN based on source MAC address     | VLAN configuration mode |

|  |  |                              |
|--|--|------------------------------|
| no mac-vlan  | Delete all VLANs based on source MAC address                             | VLAN configuration mode      |
| mac-vlan enable  | Enable the MAC-VLAN function of the interface                            | Interface configuration mode |
| mac-vlan disable   | Disable the MAC-VLAN function of the interface                           | Interface configuration mode |
| show mac-vlan  | Display all VLANs based on source MAC address                            | Privileged mode              |
| ip-subnet-vlan ip A.B.C.D A.B.C.D vlan <1-4094>                    | Create a VLAN based on the source IP subnet                              | VLAN configuration mode      |
| no ip-subnet-vlan ip A.B.C.D A.B.C.D                               | Delete a VLAN based on the source IP subnet                              | VLAN configuration mode      |
| no ip-subnet-vlan  | Delete all VLANs based on the source IP subnet                           | VLAN configuration mode      |
| ip-subnet-vlan enable  | Enable the VLAN function of the interface based on the source IP subnet  | Interface configuration mode |
| ip-subnet-vlan disable   | Disable the VLAN function of the interface based on the source IP subnet | Interface configuration mode |
| show ip-subnet-vlan  | Display all VLANs based on source IP subnet                              | Privileged mode              |
| protocol-vlan ether-type (ip ipv6 ipx ... <0-65535>) vlan <1-4094> | Create a protocol-based VLAN   | Interface configuration mode |
| no protocol-vlan ether-type (ip ipv6 ipx ... <0-65535>)            | Delete a protocol-based VLAN   | Interface configuration mode |
| no protocol-vlan   | Delete all protocol-based VLANs  | Interface configuration mode |
| show protocol-vlan   | Show all protocol-based VLANs  | C                            |
| show vlan-partition interface                                      | Display the status of MAC  | Privileged mode              |

|        |   |  |
|--------|---|--|
| IFNAME | and IP subnet-based VLAN enabled on the interface |  |
|--------|---|--|

## 7.5 Voice VLAN

### 7.5.1 Voice VLAN introduction

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

The device can determine whether the data stream is a voice data stream according to the source MAC address OUI field in the data packet entering the port. Packets whose source MAC address matches the OUI address of the voice device set by the system are considered to be voice data streams and are divided into Voice VLANs for transmission.

The user can set the OUI address in advance, or use the default OUI address as the judgment criterion, as follows:

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

Add the IP phone access port to the Voice VLAN manually. Then, by identifying the source MAC of the message and matching the OUI address, after the match is successful, the system will issue ACL rules and configure the priority of the message.

### 7.5.2 Voice VLAN configuration

Before configuring Voice VLAN, you must first create the corresponding VLAN.

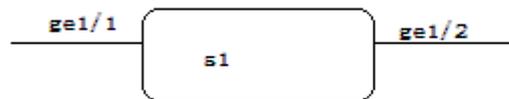
| command                          | description        | CLI mode                |
|----------------------------------|--------------------|-------------------------|
| voice-vlan oui WORD mask<br>WORD | Configure user OUI | Global<br>configuration |

|   |  |                                 |
|---|--|---------------------------------|
|   |  | mode                            |
| voice-vlan oui WORD mask<br>WORD description WORD | Configure user OUI and<br>name   | Global<br>configuration<br>mode |
| no voice-vlan oui WORD<br>mask WORD               | Delete user OUI<br>configuration by OUI<br>address and mask                  | Global<br>configuration<br>mode |
| no voice-vlan oui description<br>WORD             | Delete user OUI<br>configuration by naming                                   | Global<br>configuration<br>mode |
| no voice-vlan oui                                 | Delete all user OUI<br>configuration   | Global<br>configuration<br>mode |
| no voice-vlan default-oui<br>WORD mask WORD       | Delete default OUI<br>configuration by OUI<br>address and mask               | Global<br>configuration<br>mode |
| no voice-vlan default-oui<br>description WORD     | Delete default OUI<br>configuration by naming                                | Global<br>configuration<br>mode |
| no voice-vlan default-oui                         | Delete all default OUI<br>configuration                                      | Global<br>configuration<br>mode |
| voice-vlan default-oui<br>resume                  | Restore all default OUI<br>configuration                                     | Global<br>configuration<br>mode |
| show voice-vlan oui                               | Display all default and user<br>OUI configuration                            | Privileged mode                 |
| voice vlan <1-4094><br>(enable disable)           | Voice VLAN enabled on the<br>interface                                       | Interface<br>configuration mode |
| voice vlan qos remark cos<br><0-7> dscp <0-63>    | Interface configuration qos<br>priority, cos value is 6, dscp<br>value is 46 | Interface<br>configuration mode |
| no voice vlan qos                                 | Restore the default<br>configuration of interface<br>qos priority            | Interface<br>configuration mode |
| no voice vlan                                     | Delete interface   | Interface                       |

|                 |   |                    |
|-----------------|---|--------------------|
|                 | configuration Voice VLAN                                  | configuration mode |
| show voice-vlan | Display the configuration of Voice VLAN on all interfaces | Privileged mode    |

### 7.5.3 Voice VLAN configuration example

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



The configuration of switch S1 is as follows:

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

---

## 7.6 VLAN mapping

### 7.6.1 VLAN mapping introduction

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

Before configuring VLAN mapping, you must first create the corresponding VLAN.

### 7.6.2 VLAN mapping configuration

| command  | description  | CLI mode                     |
|--|--|------------------------------|
| vlan-mapping vlan<br><1-4094> map-vlan<br><1-4094> | Configure a VLAN mapping relationship for the port | Interface configuration mode |
| no vlan-mapping vlan<br><1-4094>                   | Delete a VLAN mapping relationship of the port     | Interface configuration mode |
| no vlan-mapping                                    | Delete all VLAN mappings of the port               | Interface configuration mode |
| vlan-mapping enable                                | VLAN mapping of the start port                     | Interface configuration mode |
| vlan-mapping disable                               | Close the port's VLAN mapping                      | Interface configuration mode |
| show vlan-mapping                                  | Display all configured VLAN mappings               | Privileged mode              |

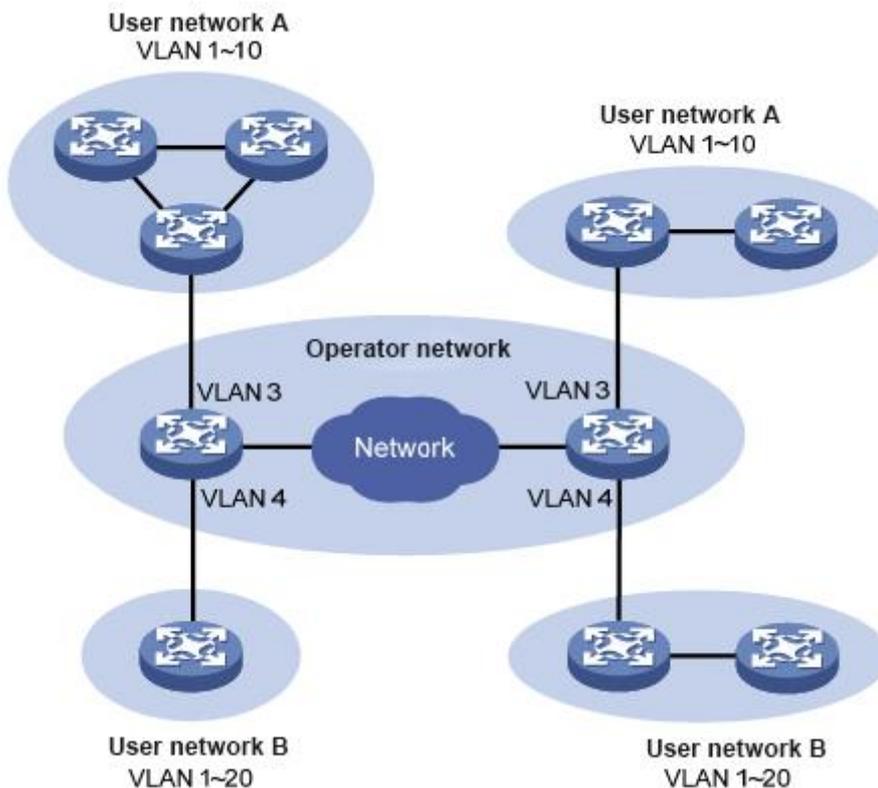
---

## 7.7 QinQ

### 7.7.1 QinQ introduction

The port QinQ feature provided by the device is a simple and flexible Layer 2 VPN technology. It encapsulates the outer VLAN Tag for the user's private network packet on the edge device of the operator's network, so that the packet carries two Layer VLAN Tag through the operation Backbone's backbone network (public network). In the public network, the device only forwards the packet according to the outer VLAN tag, and learns the source MAC address entry of the packet into the MAC address table of the VLAN where the outer tag is located, while the user's private network VLAN tag is transmitting. In the process, it will be transmitted as the data part of the message.

The QinQ feature allows operators to use one VLAN to serve user networks with multiple VLANs. As shown in the following figure, the private network VLAN of user network A is VLAN 1 to 10, and the private network VLAN of user network B is VLAN 1 to 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 packets with VLAN Tag of user network A enter the operator's network, the packets will be encapsulated with a layer of VLAN Tag with VLAN ID 3; when packets with VLAN Tag of user network B enter the operator's network, The packet will be encapsulated with a layer of VLAN tag with VLAN ID 4. In this way, the packets of different user networks are completely separated when they are transmitted on the public network. Even if the VLAN ranges of the two user networks overlap, they will not be confused when they are transmitted on the public network.



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

- (1) Alleviate the shortage of public network VLAN ID resources.
- (2) Users can plan their own private network VLAN ID without conflicting with public network VLAN ID.
- (3) Provide a relatively simple Layer 2 VPN solution for small metropolitan area networks or enterprise networks.

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

- (1) Basic QinQ: Basic QinQ is implemented based on the port method. After the basic QinQ function of the port is enabled, when the port receives a packet, the device will tag the packet with the VLAN tag of the default VLAN of the port. If a packet with a VLAN tag is received, the packet becomes a double-tag packet; if a packet without a VLAN tag is received, the packet becomes a default VLAN tag with a port 'S message.
- (2) Flexible QinQ: Flexible QinQ is a more flexible implementation of QinQ, which is based on the combination of ports and VLANs. In addition to implementing all basic QinQ functions, you can also perform different actions for packets received on the same port according to different VLANs, adding different outer VLAN tags to packets with different inner VLAN IDs.

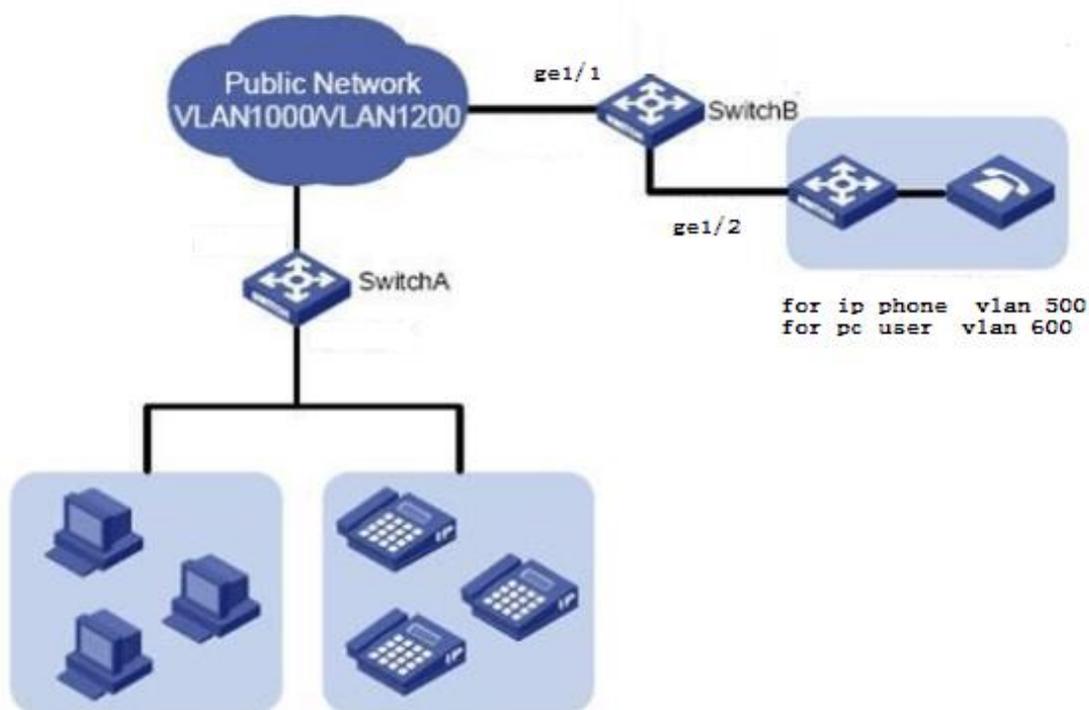
## 7.7.2 Qinq configuration

| command   | description   | CLI mode                     |
|---|---|------------------------------|
| qinq tpid WORD                                    | Configure the tpid value carried in the VLAN tag of the port, the default is 0x8100 | Interface configuration mode |
| no qinq tpid                                      | Restore port default tpid   | Interface configuration mode |
| qinq uplink                                       | Configure the port as an uplink port  | Interface configuration mode |
| no qinq uplink                                    | Cancel the uplink configuration of the port   | Interface configuration mode |
| qinq customer                                     | Configure the port as a customer port   | Interface configuration mode |
| no qinq customer                                  | Cancel the customer configuration of the port                                       | Interface configuration mode |
| qinq outer-vid <1-4094><br>inner-vid VLAN_ID      | Configure a VLAN translation for the interface                                      | Interface configuration mode |
| no qinq outer-vid <1-4094><br>[inner-vid VLAN_ID] | Delete a VLAN translation of the interface  | Interface configuration mode |
| show qinq   | Display all configured qinq conditions  | Privileged mode              |

## 7.7.3 QinQ configuration example

SwitchB's port ge1/1 is connected to the public network, and port ge1/2 is connected to the PC and the phone server. Among them, the vlan used by the PC is 600, the vlan used by the ip phone is 500, and vlan100 and vlan200 packets are allowed to pass through the public network. , In order to transmit PC user data on the public network through vlan200, ip phone data is transmitted on the public network through vlan100.

The network diagram is as follows:



The configuration of switch B is as follows :

```
Switch#con t
Switch(config)#vlan da
Switch(config-vlan)#vlan 100
Switch(config-vlan)#vlan 200
Switch(config-vlan)#exit
Switch(config)#int ge1/1
Switch(config-ge1/1)#sw mod tr
Switch(config-ge1/1)#switchport trunk allowed vlan add 100
Switch(config-ge1/1)#switchport trunk allowed vlan add 200
```

|

---

```
Switch(config-ge1/1)#qinq uplink
Switch(config-ge1/1)#int ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged dis
Switch(config-ge1/2)#switchport hybrid allowed vlan add 200 egress-tagged dis
Switch(config-ge1/2)#qinq customer
Switch(config-ge1/2)#qinq outer-vid 100 inner-vid 500
Switch(config-ge1/2)#qinq outer-vid 200 inner-vid 600
Switch(config-ge1/2)#
```

|

---

Switch#show qinq

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

Switch#

## Chapter8 QoS configuration

---

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

- QoS introduction
- QoS configuration
- QoS Configuration example

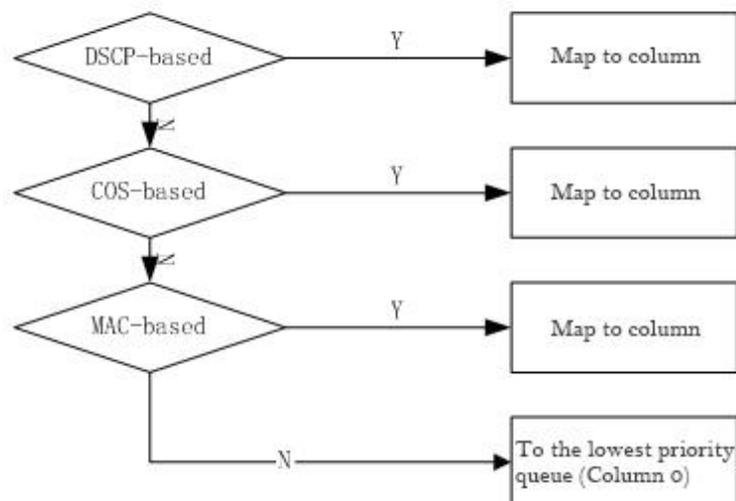
## 8.1 QoS introduction

Using the switch's QoS feature, you can prioritize important data streams forwarded through the switch, making your network's bandwidth utilization more reasonable and network performance predictable.

In the switch, the queue of the packet at the output is determined at the input according to the priority information of the packet.

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; COS-based QoS is enabled by default on physical ports. The MAC-based QoS function is configured in the MAC binding function. Only one QoS function can be configured for each physical port.

The following figure is the QoS-enabled packet forwarding process :



The switch supports eight priority queues from 0 to 7, with queue 7 having the highest priority and queue 0 having the lowest priority. There are four scheduling methods for priority queues: SP, RR, WRR, and WDRR. SP is a strict priority scheduling, that is, the packets of queue 7 are always forwarded first, and the packets of queue 6 are not forwarded until the packets of queue 7 are forwarded, and the packets of queue 5 are not forwarded until the packets of queue 6 are forwarded. , And finally forward the packets of queue 0. RR is a polling scheduling method. When forwarding data packets, the switch

polls and forwards the data packets in turn from the high-priority queue to the low-priority queue, and each queue forwards one data packet. WRR refers to weighted priority polling.

When forwarding data packets, the switch polls and forwards the data packets from the high priority queue to the low priority queue according to the configuration of the weight, and then forwards the right number of data packets from the high priority. When forwarding the next highest priority weight packet, until the lowest priority queue is forwarded, it will be forwarded from the high priority, and so on. WDRR is a weighted delinquent polling scheduling method, that is, the weight of queue 3 is 4, then in a certain round, it can forward 5 packets, while in the next round, it only has the quota of forwarding 3 packets. This flexible adaptability is more suitable for highly aggregated network environment.

In order to facilitate user configuration, we introduced the concept of QosProfile. QosProfile is an attribute configured with the mapping relationship between 802.1p and priority queue. This attribute cannot be configured by the user. Their mapping relationship is as follows:

| QosProfile | 802.1p(CoS) merit | 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              |

### 8.1.1 COS-based QoS

The port has COS-based QoS enabled by default. The switch will obtain the priority value of the VLAN TAG in the data packet entering the port, and determine the output queue of the data packet according to the user-configured COS value and the mapping relationship of the queue. If the data packet does not have VLAN TAG or the VID of VLAN TAG is 0, the switch will fill the data packet according to the default VID of the port configured by the user and the default priority of the port, and then determine the data packet according to the default priority Output queue.

---

## 8.1.2 DSCP-based QoS

If DSCP-based QoS is enabled for a port, the switch will obtain the DSCP value of the IP packet entering the port, and determine the output queue of the packet according to the mapping relationship between the user-configured DSCP value and the queue.

## 8.1.3 MAC-based QoS

When a packet enters the switch, the switch searches the switch's Layer 2 forwarding table based on the packet's destination MAC and the packet's VLAN TAG VID. If a target entry is found, then the queue mapping is configured according to the target entry Relationship to determine the output queue of the packet.

## 8.1.4 Policy-based QoS

QoS policy includes class and policy actions. Classes are used to identify flows, and users can define a series of rules through commands to classify packets; Policy actions are used to define the QoS actions performed by packets matching the rules. If policy-based QoS is enabled for a port, the switch will classify the packets entering the port. For the packets that meet the classification requirements, the switch will process the packets of the port according to the corresponding policy actions. For those that do not meet the classification requirements The data packet is not processed, and then the output queue of the data packet is determined according to the priority mapping relationship.

## 8.2 QoS configuration

### 8.2.1 QoS default configuration

| Configuration item              | merit   | Is it configurable |
|---------------------------------|---------|--------------------|
| Queue number                    | 8       | no                 |
| Scheduling method               | WRR     | yes                |
| Whether to enable SP scheduling | disable | yes                |
| Whether to enable RR            | disable | yes                |

|  |   |     |
|--|---|-----|
| scheduling   |   |     |
| Whether to enable WDRR scheduling mode               | disable   | yes |
| Queue weight   | QP0[1],QP1[2],QP2[4],QP3[8]<br>QP4[16],QP5[32],QP6[64]<br>QP7[127]  | yes |
| The mapping relationship between COS and qosprofile  | COS0~ [qp0]<br>COS1~ [qp1]<br>COS2~ [qp2]<br>COS3~ [qp3]<br>COS4~ [qp4]<br>COS5~ [qp5]<br>COS6~ [qp6]<br>COS7~ [qp7]  | no  |
| The 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] | no  |
| Whether the interface enables qos based on DSCP      | disable   | yes |
| Whether the interface enables COS-based qos          | enable  | no  |
| Interface user priority (COS value)                  | 0   | yes |

## 8.2.2 Configure scheduling

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

| command                          | description              | CLI mode                |
|----------------------------------|--------------------------|-------------------------|
| qos sched {rr   sp   wrr   wdrr} | Configure QoS scheduling | Interface configuration |

|  |  |      |
|--|--|------|
|  |  | mode |
|--|--|------|

### 8.2.3 Configure queue weight

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

Queue weight refers to the number of packets forwarded by the priority queue in one poll forwarding, so pay attention to when configuring queue weight: the weight of the low priority queue should not exceed the weight of the high priority queue.

### 8.2.4 Configure the mapping relationship between DSCP and QosProfile

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

### 8.2.5 Configure Port DSCP-based QoS

The Qos function can only be configured on the physical port, not on the trunk or Layer 3 interface.

| command | description | CLI mode |
|---------|-------------|----------|
|---------|-------------|----------|

|                   |   |                              |
|-------------------|---|------------------------------|
| qos dscp-based    | Enable the Qos function of the port based on DSCP.  | Interface configuration mode |
| no qos dscp-based | Disable the Qos function of the port based on DSCP. | Interface configuration mode |

## 8.2.6 Configure port user priority (COS merit)

| command                 | description   | CLI mode                     |
|-------------------------|---|------------------------------|
| qos user-priority <0-7> | Configure the user priority of the port (COS value)                                 | Interface configuration mode |
| no qos user-priority    | The user priority (COS value) of the restoration port is the default configuration. | Interface configuration mode |

## 8.3 QoS configuration example

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

```
Switch#configure terminal
Switch#(config)#interface ge1/3
Switch#(config-ge1/3)#qos user-priority 3
Switch#(config-ge1/3)#end
```

Configure interface ge1/3 to enable DSCP-based QoS function, 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
```

---

## 8.4 Policy QoS configuration example

Configure ACL to capture the data flow of source MAC1, MAC2, MAC3 respectively  
( The acl rules can be modified as needed, here are just a simple example )

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

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

( You can modify the matching rules cos or dscp according to your needs, here are just simple examples )

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

Configure the QOS policy to re-mark the 802.1p priority of the data flows with the source MAC1, MAC2, and MAC3 respectively

( The strategy can be modified according to demand, here is just 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
```

Deliver QOS policy to the port

```
interface ge1/2
qos apply-policy 10
```

---

## Chapter9 MSTP configuration

---

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

- MSTP introduction
- MSTP configuration
- MSTP configuration example

### 9.1 MSTP introduction

The switch supports IEEE802.1d, IEEE802.1w, IEEE802.1s standard STP protocol.

#### 9.1.1 Overview

MSTP uses RSTP to quickly converge and aggregate multiple VLANs into a spanning tree instance. Each instance has a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data streams, can load balance, and reduces spanning tree instances that are required to support a large number of VLANs.

#### 9.1.2 Multiple spanning tree domain

For instances involved in multiple spanning tree (MST) calculations, the switch must be configured with the same MST configuration information. A set of connected switches with the same MST configuration constitute an MST region.

MST configuration determines the domain to which each switch belongs. Configuration includes domain name, revision number, and MST instance and VLAN assignment mapping ; This information will generate a unique digest in the MST configuration. The digests in the same domain are the same, and they must be the same. You can view these information with the show spanning-tree mst config command.

---

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

### **9.1.3 IST, CIST and CST**

Internal spanning tree (IST), a spanning tree running in the MST region.

In each MST region, MSTP maintains multiple generation instances. Instance 0 is a special instance of a domain, called IST. All other MST instances are numbers 1 to 15.

This IST is just an example of a spanning tree that receives and sends BPDUs ; All other spanning tree instance information is compressed in MSTI BPDU. Because MSTI BPDUs carry information for all instances, the number of BPDUs that need to be processed by a switch that supports multiple spanning tree instances means simplifying.

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 consumption, etc. By default, all VLANs are assigned to IST.

A common and internal spanning tree (CIST) is a collection of all ISTs in each MST region, and a common spanning tree (connecting the MST region to a single spanning tree).

The spanning tree calculated in one domain looks like a subtree containing the CST of all switch domains. CIST is formed by the result of spanning tree calculation between switches supporting 802.1W and 802.1D. The CIST in the MST domain is the same as the CST outside the domain.

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

### **9.1.4 Intra-domain operations**

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

---

When an MSTP switch is initialized, it sends BPDUs requesting it to act as the CST root and IST master, and the path cost to the CST root and IST master is set to 0. The switch also initializes all MST instances and requires to be their root. If the MST root information received by the switch has priority over the information stored on the current port (low bridge ID, low path spend, etc.), it abandons its requirement to become an IST master.

During initialization, a domain may have many subdomains, each with its own IST master. When the switch receives a higher priority IST message, it leaves its old subdomain and joins the new subdomain that may contain the real IST master. Therefore, all subdomains shrink, except those containing real IST masters.

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

## **9.1.5 Interdomain operations**

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

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

It's just that the CST instance sends and receives BPDUs, and the MST instance adds their spanning tree information to the BPDU to affect neighbor switches and calculate the final spanning tree topology. Because of this, the spanning tree parameters involved in BPDU transmission (such as hello time, forward time, max-age, and max-hops) are configured only in the CST instance but do not affect all MST instances. Parameters related to spanning tree topology (for example: switch priority, port VLAN cost, port VLAN priority) can be configured in the CST instance and MST instance.

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

---

## 9.1.6 Hop count

IST and MST instances do not use message-age and maximum-age information in BPDUs configured with spanning tree topology calculation. Instead, use the path cost to the root and a hop-count mechanism equivalent to IP TTL.

You can configure the maximum hop count for that domain and apply it to that domain IST and all MST instances. The hop count calculation is the same as the message-age result (decided after initiating a reconfiguration). The instance root switch always sends a BPDU (or-M-record) with a cost of 0 and a hop-count of the maximum value. When a switch receives a BPDU, it decrements the remaining hops by 1 and propagates the remaining hops in the BPDUs it generates. When the count reaches 0, the switch discards the BPDU and ages the port information.

In a domain, the Message-age and maximum-age information in the RSTP BPDU part remains the same, and the same value is propagated on the designated port of the boundary domain.

## 9.1.7 Border port

A boundary port (boundary) is a spanning tree domain that connects the MST region to a single RSTP running, or a separate spanning tree domain of 801.1D, or other MST regions with different configurations. A border port is also connected to a LAN. The designated switch for this LAN is either a separate spanning tree switch or a switch with different MST region configurations.

At the border port, the role of the MST port is not important, and their status is forced to be the same as the IST port status (when the IST port is forwarding, the MST port at the border is forwarding). An IST port at the border can have any role except the backup port.

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

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

If a boundary port transitions to the forwarding state in an instance, it is forwarding in all instances, and a topology change is triggered. If a border port with IST root or specified port role receives a topology change notification, the IST instance and all MST instances

on the active port of the MSTP switch trigger a topology change.

## 9.1.8 Interoperability of MSTP and 802.1d STP

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

However, if the switch no longer receives 802.1D BPDUs, it will not automatically return to MSTP mode because it cannot determine whether the other party's switch has been deleted from the connection unless the other party's switch is the designated switch. Similarly, when the switch connected to this switch has joined the domain, the switch may continue to assign a boundary port role to a port. Restart the protocol migration process (force to negotiate with neighbor switch).

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

## 9.1.9 Port role

MSTP uses RSTP fast convergence algorithm. The following briefly introduces the role of MSTP ports and fast convergence in conjunction with RSTP.

RSTP provides fast convergence of designated port roles and determining active topology. RSTP is based on IEEE802.1D STP and selects a high priority switch as the root switch. When RSTP assigns a port role to a port :

Root port-Provides optimal path consumption when the switch forwards packets to the root switch.

Designated port - Connect to the designated switch. When forwarding packets from the LAN to the root switch, the lowest path cost is generated. The port through which

|

---

the designated switch connects to the LAN is called the designated port.

Alternate port - Provide an alternative path from the current root port to the root switch.

Backup port - Act as a backup of the path from the designated port to the leaves of the spanning tree. A Backup port exists only when two ports are connected together in a point-to-point loop or when a switch has two or more connected to a shared LAN segment.

Disable port - No port role in spanning tree operation.

Master port - Located on the domain root or the shortest path to the root, it is the port connecting the domain to the root.

The root port or designated port role is included in the active topology. The role of replacement port or backup port is not included in the active topology.

In a network with a stable topology and a fixed port role, RSTP ensures that each root port and designated port immediately transition to the forwarding state when all replacement ports and backup ports are always in the discarding state. Port state control forwarding and learning processing.

Fast convergence

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

Edge ports - If you configure a port as an edge port, the edge port immediately transitions to the forwarding state. You can open it as a boundary port only when this port is connected to a separate terminal or to determine the device that does not need to calculate the spanning tree.

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

Point-to-point links - If you connect a port to other ports through a point-to-point connection and the local port becomes a designated port, it negotiates a fast transition with other ports through a proposal-agreement handshake to determine a fast-convergence loop-free topology.

Topology change

This section describes the difference between RSTP and 802.1D in handling

spanning-tree topology changes.

**Detection** - Unlike 802.1D, any transition between the blocking and forwarding states will cause a topology change, only the transition from blocking to the forwarding state will cause a RSTP topology change (only the topology change is considered to increase connectivity). A state change on an edge port (edge port) will not cause a topology change. When a RSTP switch detects a topology change, it floods it learns information to all nonedge ports (nonedge ports) except for the ports that receive TC information.

**Notification** - Unlike 802.1D, use TCN BPDU, RSTP does not use it. However, for interoperability with 802.1D, the RSTP switch processes and generates TCP BPDUs.

**Acknowledgement** - When an RSTP switch receives a TCN message from an 802.1D switch on a designated port, it responds with an 802.1D BPDU and sets the TCA flag. However, if the TC-while timer (same as the topology-change timer of 802.1D) is active, connect to the 802.1D switch at the root port and receive a configuration BPDU with TCA, the TC-while timer resets (reset). This behavior is only required to support 802.1D switches. RSTP BPDU never has TCA flag.

**Propagation** - When an RSTP switch receives a TC message from another switch through a designated port or root port, it propagates to all non-edge ports, designated ports and root ports (except the receiving port). All such ports of the switch start the TC-while timer and flood the information they learned.

**Protocol migration** - For backward compatibility with 802.1D switches, RSTP selectively sends 802.1D configuration BPDUs and TCN BPDUs based on each port.

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

After the port's migration-delay timer has been suspended, 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 BPDUs on a port and receives a RSTP BPDU after the timer is suspended, it restarts the timer on that port and starts using RSTP BPDUs.

## **9.1.10 Introduction to 802.1D Spanning tree**

The spanning tree protocol is based on the following :

|

---

1 ) There is a unique group address (01-80-C2-00-00-00) to identify all the switches on a specific LAN. This group address can be recognized by all switches;

2 ) Each switch has a unique identification ( Bridge Identifier ) ;

3 ) Each switch port has a unique port identifier ( Port Identifier). Management of spanning tree configuration is also required : Set a relative priority for each switch ; Adjust a relative priority for each port of each switch ; One path cost for each port.

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

There is a switch in each LAN called a designated switch, which belongs to the switch with the least root path cost in the LAN. The port connecting the LAN to the designated switch is the designated port of the LAN. If more than two ports in the designated switch are connected to this LAN, the port with the highest priority is selected as the designated port.

The elements necessary to form a spanning tree :

1 ) determine root switch

a、 At first, all the switches considered themselves as root switches ;

b、 The switch sends a configuration BPDU to the connected LAN broadcast, and its root\_id and bridge\_id have the same value;

c、 When the switch receives the configuration BPDU from another switch, if the value of the root\_id field in the received configuration BPDU is greater than the value of the root\_id parameter in the switch, the frame is discarded, otherwise the root\_id and root path cost of the switch are updated root\_path\_cost and other parameters, the switch will continue to broadcast configuration BPDUs with new values.

2 ) Determine root port

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

If there are multiple ports with 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 ) Authorized LAN designated switch

a. At the beginning, all the switches considered themselves as the designated switches of the LAN.

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

c. If the designated switch receives a configuration BPDU from another switch on the LAN due to competition for the designated switch at a certain time, the designated switch will send a response configuration BPDU to re-determine the designated switch.

### 4 ) Determine designated port

The port connected to the LAN in the designated switch of the LAN is the designated port. If the designated switch has two or more ports connected to the LAN, the port with the lowest identification is the designated port.

Except for the root port and designated ports, all other ports will be placed in the blocked state. In this way, after determining the root switch, the root port of the switch, and the designated switch and designated port of each LAN, the topology of a spanning tree is also determined.

## 9.2 MSTP configuration

### 9.2.1 Default configuration

| Command parameter  | Default merit |
|--|---------------|
| spanning-tree mst enable(enable mstp)                    | disable       |
| Spanning-tree mst priority(switch cist priority)         | 32768         |
| spanning-tree mst hello-time( switch cist hello-time)    | 2seconds      |
| spanning-tree mst forward-time(switch cist forward-time) | 15seconds     |

|   |           |
|---|-----------|
| spanning-tree mst max-age(switch cist max-age)                  | 20seconds |
| spanning-tree mst max-hops(switch cist max-hops)                | 20seconds |
| instance 1 priority (instance priority)                         | 32768     |
| spanning-tree mst instance 1 priority([port instance priority)  | 128       |
| spanning-tree mst instance 1 path-cost(port instance path-cost) | 20000000  |
| spanning-tree mst priority ( port cist priority )               | 128       |
| spanning-tree mst path-cost ( port cist path-cost )             | 20000000  |

## 9.2.2 General configuration

Enable MSTP

MSTP is turned off by default when the system is started..

The configuration process to start MSTP is:

Switch#configure terminal

Switch(config)#spanning-tree mst enable

关闭MSTP的命令是：

Switch#configure terminal

Switch(config)#no spanning-tree mst

Configure max-age

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

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

Configuration process:

Switch#configure terminal

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

Configure max-hops

max-hops is the number of hops specified in a field 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

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

The default configuration is 15 seconds, and the configuration range is 4 to 30 seconds. According to the generated number protocol, the forward-time must meet the following conditions :  $2 * (\text{forward-time} - 1) \geq \text{max-age}$ .

Configuration process :

Switch#configure terminal

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

Configure hello-time

Configuring hello-time is the configuration for all instances. The hello-time is the interval at which the root switch generates configuration information.

The default configuration time is 2 seconds, and the configuration range is 1 to 10 seconds. According to the generated number protocol hello-time must meet the following conditions :  $2 * (\text{hello-time} + 1) \leq \text{max-age}$ .

Configuration process :

Switch#configure terminal

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

Configure the priority of the CIST bridge ( priority )

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

Configuration process :

Switch#configure terminal

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

Configuration compatible with CISCO

The network switch adopts the MSTP protocol based on 802.1s, and the length of each MSTI message is 16 bytes ; The length of each MSTI message of the BPDU of the

CISCO switch is 26 bytes. In order to interoperate with CISCO switches, switches that are compatible with CISCO must be activated when configuring switches for the network.

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

The default system does not enable this function.

Enable compatible with CISCO :

```
Switch#configure terminal
```

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

Disable compatible with CISCO :

```
Switch#configure terminal
```

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

Reset protocol check task

In order to be compatible with the 802.1D STP protocol, the system can automatically detect the protocol that the opposing system is running. Determine the protocol that this port runs according to the protocol that the other party runs.

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

Reset the reconnaissance mission of the entire device :

```
Switch#clear spanning-tree detected protocols
```

Reset the protocol reconnaissance task of a port :

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

### 9.2.3 Domain configuration

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

A domain has one or more members with the same MST configuration, and each

member can handle RSTP BPDUS capability. There is no limit to the number of members in a network, but each domain can support up to 16 instances.

The configuration of the instance is described in 'Instance Configuration'. Here only the domain name configuration and revision number configuration are introduced.

Configure Domain :

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#region <region-name>
```

Configure revision number :

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# revision <revision-num>
```

## 9.2.4 Instance configuration

The system supports 16 instances, and the range of instance ID numbers is 0-15. Only one spanning tree instance can be assigned to a VLAN at a time.

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

The process of configuring an instance :

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance <instance-id> vlan <vlan-id>
```

Configure MSTI bridge priority ( priority )

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

Configuration process :

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance <instance-id> priority <priority>
```

---

## 9.2.5 Port configuration

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

The process of configuring a port to join an instance :

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id>
```

Configure the priority of the CIST port ( priority )

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

Configuration process :

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst priority <priority>
```

Configure MSTI port priority ( priority )

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

Configuration process :

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id> priority <priority>
```

Configure path cost elimination for CIST ports ( path-cost )

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

| bandwidth(bps) | Path cost |
|----------------|-----------|
|----------------|-----------|

|                       |           |
|-----------------------|-----------|
| 100,000(100K)         | 200000000 |
| 1,000,000(1M)         | 20000000  |
| 10,000,000(10M)       | 2000000   |
| 100,000,000(100M)     | 200000    |
| 1,000,000,000(1G)     | 20000     |
| 10,000,000,000(10G)   | 2000      |
| 100,000,000,000(100G) | 200       |
| 1,000,000,000,000(1T) | 20        |
| >1000000000000        | 2         |

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

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

Configure path consumption for MSTI ports ( path-cost )

Default configuration 20000000 , configuration range 1-200000000. The bandwidth and path consumption are the same as the table above.

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

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

Configure the version number of the sent protocol packet

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

Configuration process :

Switch#configure terminal

Switch(config)#interface <if-name>

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

Configure connection type

If a port is connected to other ports in a point-to-point manner, and the local port becomes a designated port, RSTP negotiates a rapid transition through the proposal-agreement process to connect it to become the root port To determine an acyclic

topology.

The following briefly introduces the proposal-agreement negotiation process.

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, the switch is synchronized.

When RSTP forces it to synchronize new root information, if a designated port is in forwarding state and is not configured as an edge port, it transitions to the blocking state.

Normally, when RSTP forces a port to synchronize new root messages and the port cannot meet the above conditions, the port status is set to blocking.

When ensuring that all ports are synchronized, the switch sends an agreement message to the designated port corresponding to the root port.

When the switch connects to a point-to-point connection in agreement on their port role, RSTP immediately migrates the port state to forwarding.

If it is a shared connection, it is necessary to go through the calculation process of 802.1D to determine the status of the port.

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

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

```
Switch#configure terminal
```

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

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

The connection type of the configuration port is shared connection :

```
Switch#configure terminal
```

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

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

## 9.2.6 PORTFAST related configuration

### 1) Port Fast

Port Fast immediately transfers an access or trunk port from the blocking state to the forwarding state, bypassing the listening and learning states.

You can use Port Fast to connect a single workstation and server, allowing these devices to connect to the network immediately without waiting for the spanning tree to

converge.

Configure a port as fast port :

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast

## 2) BPDU Filtering

BPDU filtering can be opened globally based on the switch or based on each port, but their characteristics are different.

At the global level, you can use the spanning-tree mst portfast bpdu-filter command to enable the BPDU filtering function of the port in the portfast bpdu-filter default state.

At the port layer, you can use spanning-tree mst portfast bpdu-filter enable to enable BPDU filter on any port.

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

Configure BPDU Filtering

In global configuration mode :

Switch#configure terminal

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

In interface configuration mode :

Switch#configure terminal

Switch(config)#interface <if-name>

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

## 3) BPDU Guard

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

At the global level, you can use spanning-tree mst portfast bpdu-guard to enable the BPDU guard function for ports in the portfast bpdu-guard default state.

At the port layer, you can enable BPDU guard on any port.

When a port configured with BPDU guard receives a BPDU, the spanning tree will shut down this port.

In a valid configuration, Port Fast-enabled ports do not receive BPDUs. A BPDU received 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 is when the port that starts the BPDU guard receives the BPDU, if the system configures the error-disable mechanism, it will start the error-disable timer. error-disable will restart this port after the system configured timeout.

In global configuration mode :

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

In interface configuration mode :

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast bpdu-guard enable
```

error-disable configuration

Start the error-disable mechanism

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

Configure error-disable timeout

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

## 9.2.7 Root Guard related configuration

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

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

If the switch is operating in MST mode, the root guard forces the port to become the designated port. If a border port is blocked in the IST instance because of root guard, this

port is blocked in all MST instances. A border port is a port connected to a LAN, and the designated switch is either an 802.1D switch or a switch configured in a different MST region.

When a port is opened, the root guard is applied to all VLANs to which the port belongs. VLANs can be aggregated and mapped to an MST instance.

Configuration process

```
Switch#configure terminal
```

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

```
Switch(config)#spanning-tree mst guard root
```

## 9.3 MSTP configuration example

### (1) configuration

The three switches are connected in a ring. You need to open the spanning tree protocol of each switch to avoid loops. Perform configuration on each switch separately.

Switch 1 configuration :

```
Switch>en
```

```
Switch#configure terminal
```

```
Switch(config)#spanning mst enable
```

Switch 2 configuration :

```
Switch>en
```

```
Switch#configure terminal
```

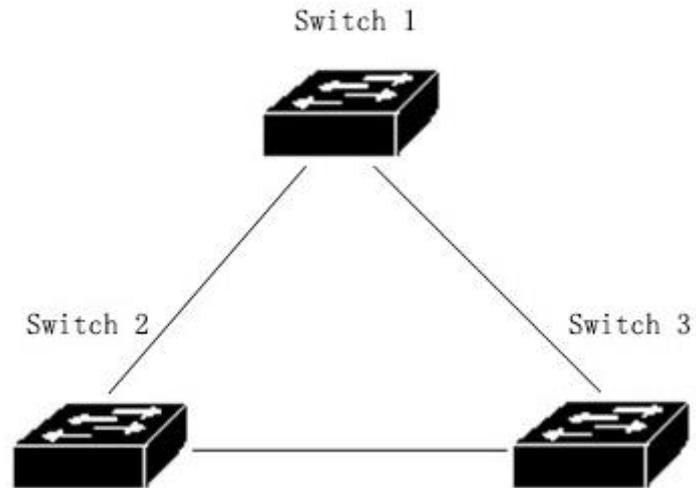
```
Switch(config)#spanning mst enable
```

Switch 3 configuration :

```
Switch>en
```

```
Switch#configure terminal
```

```
Switch(config)#spanning mst enable
```



**(2)Debug :**

See which switch is selected as the root bridge :

Run `show spanning-tree mst` and observe that the value of CISTRoot is the one with the smallest MAC address among the three switches, that is, the root election result is correct.

`Switch#show spanning-tree mst`

View the port status of switches in the spanning tree :

Execute the `show spanning-tree mst interface ge1/1` command and observe the State value of PORT `ge1/1` in instance 0

`Switch#show spanning-tree mst interface ge1/1`

---

# Chapter10 ERPS configuration

---

## 10.1 ERPS description

ERPS (Ethernet Ring Protection Switching) is a ring network protection protocol developed by ITU, also known as G.8032. It is a link layer protocol specifically applied to the Ethernet ring network. 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 various nodes on the ring network when a link on the Ethernet ring network is disconnected. The ERPS protocol provides a fast Ethernet ring network protection mechanism, which can quickly restore network transmission in the event of a ring network failure, thereby ensuring high availability and high reliability of the switch in the case of ring network topology.

## 10.2 ERPS technology introduction

### 10.2.1 ERPS ring

The ERPS ring is based on the principle of minimizing the ring. Each ring must be the smallest ring, which is divided into a main ring and a sub-ring: the main ring is a closed ring; the sub-ring is a non-closed ring or a closed ring; both need to be configured by commands.

Each ERPS ring (whether it is a main ring or a sub-ring) has five states: (1) Idle state: when each physical link of the ring network is connected; (2) Protection state: a certain one in the ring network Or the state when multiple physical links are disconnected; (3) Manual switch state: manually change the state of the ring; (4) Forced switch state: forcefully change the state of the ring; (5) Pending state: pending intermediate state.

---

## 10.2.2 ERPS node

The layer 2 switching equipment that joins the ERPS ring is called a node. Each node cannot add more than two ports to the same ERPS ring. One port is an RPL port, and the other port is an ordinary ring port.

For the overall situation, the role of nodes is divided into the following two types: (1) Intersecting nodes: in intersecting ERPS rings, nodes that belong to multiple rings at the same time are called intersecting nodes; (2) Non-intersecting nodes: in intersecting ERPS rings, nodes that only belong to a certain ERPS ring are called non-intersecting nodes.

The node modes specified in the ERPS protocol mainly include three types: RPL owner node, RPL neighbour node and ordinary ring node. (1) RPL owner node: There is only one RPL owner node in an ERPS ring, which is determined by user configuration. Blocking the RPL port prevents loops in the ERPS ring. When the RPL owner node receives a fault message, it learns about other nodes on the ERPS ring. Or, when the link fails, the RPL port will be automatically opened. This port resumes the reception and transmission of traffic to ensure that the traffic will not be interrupted; (2) RPL neighbour node: a node directly connected to the RPL port of the RPL owner node. Normally, the RPL port of the RPL owner node and the RPL port of the RPL neighbour node are blocked to prevent loops. When the ERPS ring fails, both the RPL port of the RPL owner node and the RPL port of the RPL neighbour node will be released; (3) Normal ring node: In the ERPS ring, all nodes except the RPL owner node and the RPL neighbour node are ordinary ring nodes. The RPL port of the ordinary ring node is no different from the ordinary ring port. The ring port of the ordinary ring node is responsible for monitoring the link status of its directly connected ERPS protocol, and notifying other nodes of the link status changes in a timely manner ;

## 10.2.3 Links and channels

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

(2) Sub-ring link: Among intersecting rings, a link belonging to the sub-ring and controlled by the sub-ring ;

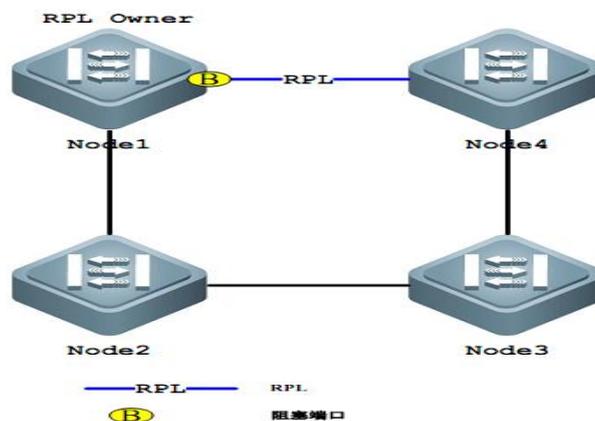
(3)RAPS ( Ring Auto Protection Switch ) virtual channel : In the intersecting ring, the inter-nodes are used to transmit sub-ring protocol packets, but the path that does not belong to the sub-ring is called the sub-ring's RAPS virtual channel.

## 10.2.4 ERPS VLAN

There are two types of VLANs in ERPS: (1) RAPS VLAN: used to transmit ERPS protocol packets. The ports on the device that access the ERPS ring belong to the RAPS VLAN, and only the ports that access the ERP ring can join this VLAN. The RAPS VLAN of different rings must be different. It is not allowed to configure an IP address on the interface of the RAPS VLAN; (2) Data VLAN: Compared with the RAPS VLAN, the data VLAN is used to transmit data packets. The data VLAN can contain both ERP ring ports and non-ERP ring ports.

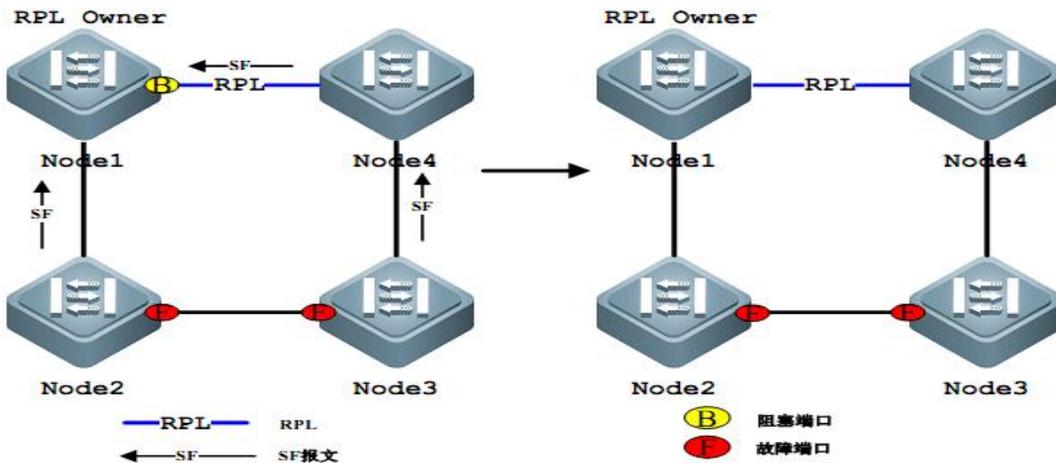
## 10.3 ERPS working principle

### 10.3.1 normal status



- (1)All nodes are connected in a ring on the physical topology ;
- (2)The loop protection protocol ensures that no loops are formed by blocking RPL links. As shown in the figure above, the link between Node1 and Node4 is an RPL link ;
- (3)Perform fault detection on each link between adjacent nodes。

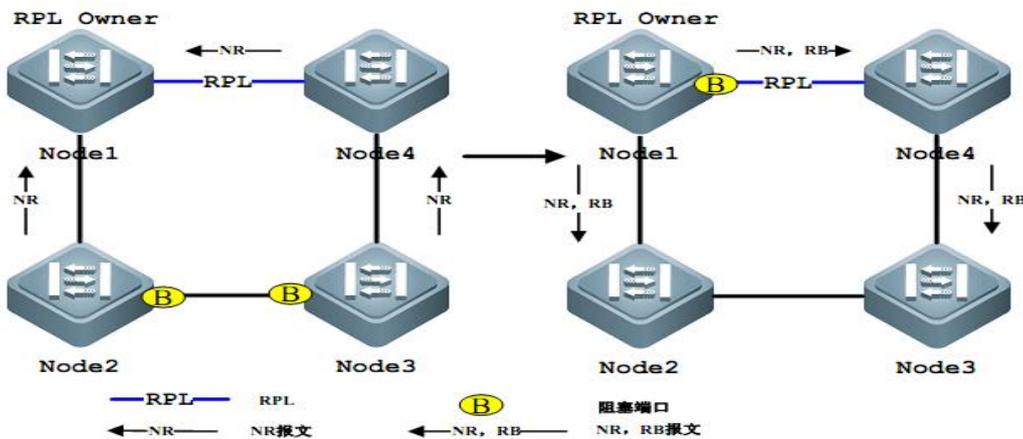
### 10.3.2 Link failure



(1)The node adjacent to the failed link blocks the failed link and uses RAPS (SF) messages to report the failure to other nodes on the ring. As shown in the figure above, assuming that the link between Node2 and Node3 fails, Node2 and After Node3 waits for the holdoff timer to expire, it will block the faulty link and send RAPS (SF) messages to each node on the ring network.

(2)The RAPS (SF) message triggers the RPL owner node to open the RPL port. The RAPS (SF) message also triggers all nodes to update their MAC entries, and then the node enters the protected state。

### 10.3.3 Link recovery



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

(2)After the guard timer expires, the RPL Owner node starts the WTR timer after

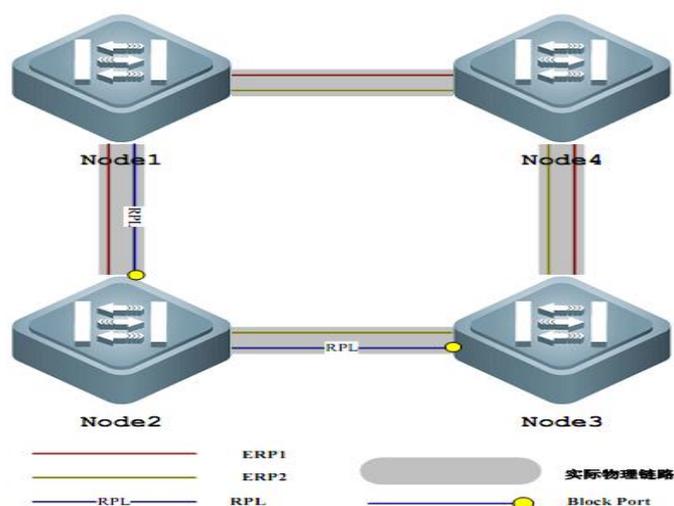
receiving the first RAPS (NR) message ;

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

(4)After receiving this message, the other nodes update their MAC entries, the node that sent the RAPS (NR) message stops periodically sending the message, and opens the originally blocked port. The ring network has returned to its original normal state.

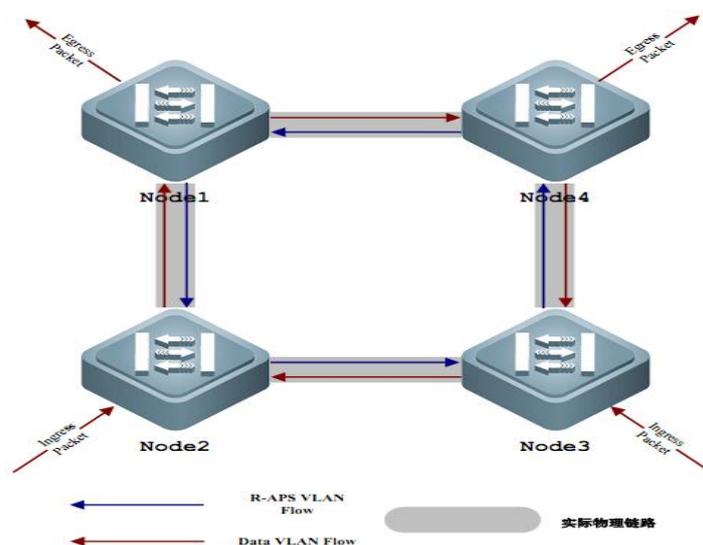
## 10.4 ERPS technical characteristics

### 10.4.1 ERPS load balancing



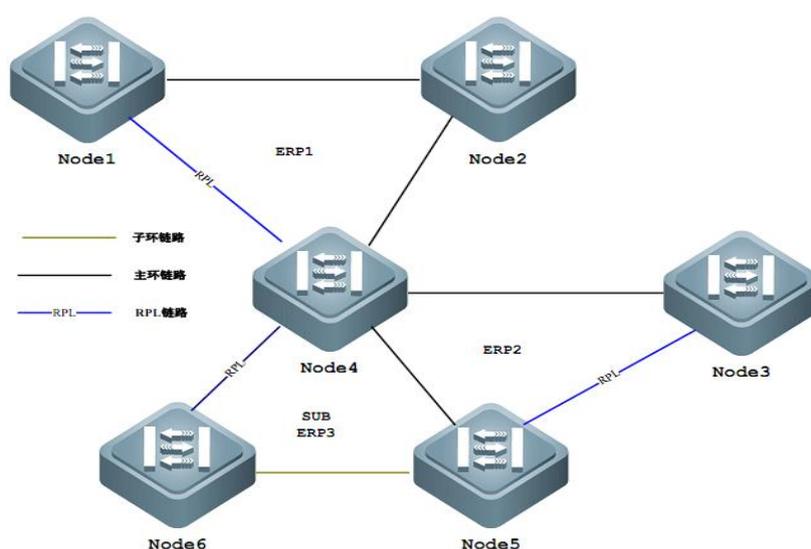
By configuring multiple instances and multiple ERPS rings on the same physical ring network, different ERPS rings send traffic in different VLANs (called protection VLANs) to achieve different topology of data traffic in different VLANs in the ring network, thereby achieving load sharing the goal of. As shown in the figure above, a physical ring network corresponds to two instances and two ERPS rings. The two ERPS rings protect different VLANs. Node2 is the RPL owner node of ERP1, and Node3 is the RPL owner node of ERP2. Through configuration, different VLANs can be used to block different links, thereby achieving load sharing for a single ring.

## 10.4.2 Good security



There are two types of VLANs in ERPS, one is RAPS VLAN and the other is data VLAN. RAPS VLAN is only used to transmit ERPS protocol messages; ERPS only processes protocol messages from RAPS VLAN, and does not process any protocol attack messages from data VLAN, improving the security of ERPS.

## 10.4.3 Support multi-ring intersection and tangent



As shown in the figure above, ERPS supports adding multiple rings in the same node (Node4) in the form of tangent or intersection, which greatly increases the flexibility of networking.

## 10.5 ERPS protocol commands

| command   | description  | CLI mode                  |
|---|--|---------------------------|
| erps predefine configuration<br>(ring-node   rpl-owner-node)              | Enable ERPS predefined configuration   | Global configuration mode |
| no erps predefine configuration   | Disable ERPS predefined configuration  | Global configuration mode |
| erps <1-8>  | Create an ERPS instance  | Global configuration mode |
| no erps <1-8>   | Delete an ERPS instance  | Global configuration mode |
| node-role (interconnection   none-interconnection)                        | Configure the role of nodes in the ERPS ring, interconnected nodes or non-interconnected nodes | 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<br>(major-ring   sub-ring)                          | Configure ERPS ring mode, major ring or sub-ring   | ERPS mode                 |
| ring <1-32> node-mode<br>(rpl-owner-node   rpl-neighbor-node   ring-node) | Configure ERPS ring node mode, RPL owner node, RPL neighbor node or ordinary ring node         | ERPS mode                 |
| ring <1-32> raps-vlan<br><2-4094>   | Configure ERPS ring protocol VLAN  | ERPS mode                 |
| no ring <1-32> raps-vlan  | Delete ERPS ring protocol VLAN   | ERPS mode                 |
| ring <1-32> traffic-vlan<br><1-4094>                                      | Configure ERPS ring data VLAN  | ERPS mode                 |
| no ring <1-32> traffic-vlan<br><1-4094>                                   | Delete the ERPS ring data VLAN   | ERPS mode                 |
| ring <1-32> (rpl-port rl-port)  | Configure ERPS ring port,  | ERPS mode                 |

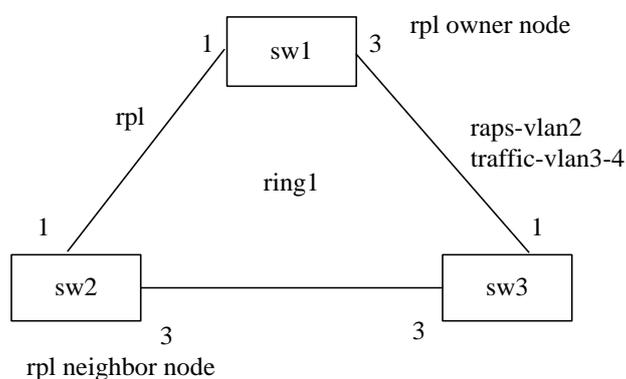
|   |   |           |
|---|---|-----------|
| IFNAME  | RPL port or ordinary ring port  |           |
| no ring <1-32> (rpl-port rl-port)                               | Delete ERPS ring port   | ERPS mode |
| ring <1-32><br>revertive-behaviour<br>(revertive non-revertive) | Configure ERPS ring recovery behavior, recoverable or non-recoverable | ERPS mode |
| ring <1-32> hold-off-time<br><0-10000>                          | Configure ERPS ring hold-off time                                     | ERPS mode |
| no ring <1-32> hold-off-time                                    | Restore ERPS ring hold-off default time                               | ERPS mode |
| ring <1-32> guard-time<br><10-2000>                             | Configure 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 ERPS ring wtr time  | ERPS mode |
| no ring <1-32> wtr-time   | Restore ERPS ring wtr default time                                    | ERPS mode |
| ring <1-32> wtb-time <1-10>                                     | Configure ERPS ring wtb time  | ERPS mode |
| no ring <1-32> wtb-time   | Restore the default time of ERPS ring wtb                             | ERPS mode |
| ring <1-32> raps-send-time<br><1-10>                            | Configure the ERPS ring protocol packet sending time                  | ERPS mode |
| no ring <1-32> raps-send-time                                   | Restore the default sending time of ERPS ring protocol packets        | ERPS mode |
| ring <1-32> (enable disable)                                    | Open or close ERPS ring   | ERPS mode |
| ring <1-32> forced-switch<br>IFNAME                             | Forcibly switch ERPS ring ports                                       | ERPS mode |
| ring <1-32> clear<br>forced-switch                              | Clear forced switching of ERPS ring                                   | ERPS mode |
| ring <1-32> manual-switch<br>IFNAME                             | Manually switch ERPS ring ports                                       | ERPS mode |

|                                 |  |                 |
|---------------------------------|--|-----------------|
| ring <1-32> clear manual-switch | Clear manual switching of ERPS ring  | ERPS mode       |
| ring <1-32> clear recovery      | Manual recovery when clearing unrecoverable behavior of ERPS ring or manual recovery before WTR/WTB expiration | ERPS mode       |
| show erps                       | Display a brief overview of all ERPS instances and rings of the device   | Privileged mode |
| show erps <1-8>                 | Display the details of a single ERPS instance and ring of the device   | Privileged mode |

## 10.6 Typical application of ERPS

### 10.6.1 Single ring example

As shown in the figure below, the sw1, sw2 and sw3 nodes form an erps single ring ring1. The 1, 3 ports of each node are used as erps ring ports. The protocol vlan of the ring is 2, the data vlan is 3, 4, the sw1 node is the rpl owner node, sw2 The node is an rpl neighbor node, and the link between sw1 and sw2 is an rpl link.



(1)configure sw1 :

Switch>enable

---

```
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure erps instance 1, erps single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(2)configure sw2:

```
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure erps instance 1, erps single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-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
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(3)configure sw3:

```
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Configure the ring port vlan mode to trunk, add erps protocol and data vlan

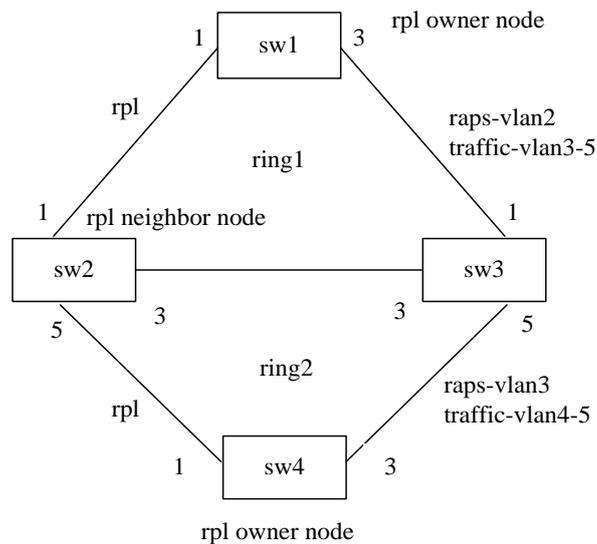
```
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure erps instance 1, erps single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

## 10.6.2 Multi-ring example

As shown in the following figure, the sw1, sw2, and sw3 nodes form an erps main ring ring1, and the ports 1 and 3 of the sw1, sw2, and sw3 nodes are used as the main ring ring1 ring port, the protocol vlan of the main ring ring1 is 2, and the data vlan is 3, 4, 5. The sw1 node is the primary ring1 rpl owner node, the sw2 node is the primary ring1 rpl neighbor node, and the link between sw1 and sw2 is the primary ring ring1 rpl link.

The sw2, sw3, and sw4 nodes form an erps sub-ring ring2. The 5 ports of the sw2

and sw3 nodes and the 1 and 3 ports of the sw4 node serve as the sub-ring ring2 ring ports. The protocol vlan of the sub-ring ring2 is 3, and the data vlan is 4, 5. , Sw4 node is the subring ring2 rpl owner node, the link between sw2 and sw4 is the subring ring2 rpl link.



(1)configure sw1 :

Switch>enable

Switch#configure terminal

Create erps protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-5

Switch(config-vlan)#exit

Configure the ring port vlan mode to trunk, add erps protocol and data vlan

Switch(config)# interface ge1/1

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

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

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

Switch(config-ge1/1)# switchport trunk allowed vlan add 4

Switch(config-ge1/1)# switchport trunk allowed vlan add 5

Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3

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

Switch(config-ge1/3)# switchport trunk allowed vlan add 2

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

```
|  


---

  
Switch(config-ge1/3)# switchport trunk allowed vlan add 4  
Switch(config-ge1/3)# switchport trunk allowed vlan add 5  
Switch(config-ge1/3)#exit  
Configure erps instance 1, erps main ring 1  
Switch(config)#erps 1  
Switch(config-erps-1)#ring 1  
Switch(config-erps-1)# ring 1 ring-mode major-ring  
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node  
Switch(config-erps-1)# ring 1 raps-vlan 2  
Switch(config-erps-1)# ring 1 traffic-vlan 1  
Switch(config-erps-1)# ring 1 traffic-vlan 3  
Switch(config-erps-1)# ring 1 traffic-vlan 4  
Switch(config-erps-1)# ring 1 traffic-vlan 5  
Switch(config-erps-1)# ring 1 rpl-port ge1/1  
Switch(config-erps-1)# ring 1 rl-port ge1/3  
Switch(config-erps-1)# ring 1 enable  
Switch(config-erps-1)#exit
```

(2)configure sw2:

```
Switch>enable  
Switch#configure terminal  
Create erps protocol and data VLAN  
Switch(config)#vlan database  
Switch(config-vlan)#vlan 2-5  
Switch(config-vlan)#exit  
Configure the ring port vlan mode to trunk, add erps protocol and data vlan  
Switch(config)# interface ge1/1  
Switch(config-ge1/1)# switchport mode trunk  
Switch(config-ge1/1)# switchport trunk allowed vlan add 2  
Switch(config-ge1/1)# switchport trunk allowed vlan add 3  
Switch(config-ge1/1)# switchport trunk allowed vlan add 4  
Switch(config-ge1/1)# switchport trunk allowed vlan add 5  
Switch(config-ge1/1)#exit  
Switch(config)# interface ge1/3  
Switch(config-ge1/3)# switchport mode trunk  
Switch(config-ge1/3)# switchport trunk allowed vlan add 2  
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
```

```
|  


---

  
Switch(config-ge1/3)# switchport trunk allowed vlan add 4  
Switch(config-ge1/3)# switchport trunk allowed vlan add 5  
Switch(config-ge1/3)#exit  
Switch(config)# interface ge1/5  
Switch(config-ge1/5)# switchport mode trunk  
Switch(config-ge1/5)# switchport trunk allowed vlan add 3  
Switch(config-ge1/5)# switchport trunk allowed vlan add 4  
Switch(config-ge1/5)# switchport trunk allowed vlan add 5  
Switch(config-ge1/5)#exit  
Configure erps instance 1, erps main ring 1, subring 2  
Switch(config)#erps 1  
Switch(config-erps-1)# node-role interconnection  
Switch(config-erps-1)#ring 1  
Switch(config-erps-1)# ring 1 ring-mode major-ring  
Switch(config-erps-1)# ring 1 node-mode rpl-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  
Switch(config-erps-1)# ring 1 enable  
Switch(config-erps-1)#ring 2  
Switch(config-erps-1)# ring 2 ring-mode sub-ring  
Switch(config-erps-1)# ring 2 node-mode ring-node  
Switch(config-erps-1)# ring 2 raps-vlan 3  
Switch(config-erps-1)# ring 2 traffic-vlan 4  
Switch(config-erps-1)# ring 2 traffic-vlan 5  
Switch(config-erps-1)# ring 2 rpl-port ge1/5  
Switch(config-erps-1)# ring 2 enable  
Switch(config-erps-1)#exit
```

(3)configure sw3:

```
Switch>enable
```

```
Switch#configure terminal
```

```
Create erps protocol and data VLAN
```

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit
Switch(config)# interface ge1/5
Switch(config-ge1/5)# switchport mode trunk
Switch(config-ge1/5)# switchport trunk allowed vlan add 3
Switch(config-ge1/5)# switchport trunk allowed vlan add 4
Switch(config-ge1/5)# switchport trunk allowed vlan add 5
Switch(config-ge1/5)#exit
Configure erps instance 1, erps main ring 1, subring 2
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
```

|

---

```
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

(4)configure sw4 :

```
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 3-5
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit
Configure erps instance 1, erps subring 2
Switch(config)#erps 1
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode rpl-owner-node
```

```

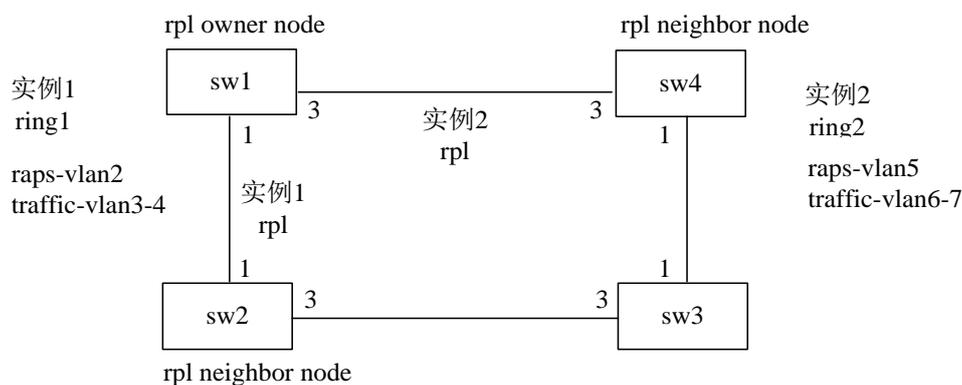
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 1
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/1
Switch(config-erps-1)# ring 2 rl-port ge1/3
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

```

### 10.6.3 Multi-instance load balancing example

As shown in the following figure, the sw1, sw2, sw3, and sw4 nodes form an erps instance 1 single ring ring1, the ports 1 and 3 of each node are used as erps ring ports, the protocol vlan of the ring is 2, the data vlan is 3, 4, and the sw1 node is rpl owner node, sw2 node is rpl neighbor node, the link between sw1 and sw2 is rpl link.

The sw1, sw2, sw3, and sw4 nodes form an erps instance 2 single-ring ring2, and the ports 1 and 3 of each node are erps ring ports. The protocol vlan of the ring is 5, the data vlan is 6, 7, and the sw1 node is the rpl owner node. The sw4 node is an rpl neighbor node, and the link between sw1 and sw4 is an rpl link.



(1Configuration example1 :

Configure sw1 :

```
Switch>enable
```

```
Switch#configure terminal
```

```
Create erps protocol and data VLAN
```

```
Switch(config)#vlan database
```

---

```
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure erps instance 1, erps single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
Configure sw2:
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
```

```
|  


---

  
Switch(config-ge1/1)# switchport mode trunk  
Switch(config-ge1/1)# switchport trunk allowed vlan add 2  
Switch(config-ge1/1)# switchport trunk allowed vlan add 3  
Switch(config-ge1/1)# switchport trunk allowed vlan add 4  
Switch(config-ge1/1)#exit  
Switch(config)# interface ge1/3  
Switch(config-ge1/3)# switchport mode trunk  
Switch(config-ge1/3)# switchport trunk allowed vlan add 2  
Switch(config-ge1/3)# switchport trunk allowed vlan add 3  
Switch(config-ge1/3)# switchport trunk allowed vlan add 4  
Switch(config-ge1/3)#exit  
Configure erps instance 1, erps single ring 1  
Switch(config)#erps 1  
Switch(config-erps-1)#ring 1  
Switch(config-erps-1)# ring 1 ring-mode major-ring  
Switch(config-erps-1)# ring 1 node-mode rpl-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  
Switch(config-erps-1)# ring 1 enable  
Switch(config-erps-1)#exit  
Configure sw3:  
Switch>enable  
Switch#configure terminal  
Create erps protocol and data VLAN  
Switch(config)#vlan database  
Switch(config-vlan)#vlan 2-4  
Switch(config-vlan)#exit  
Configure the ring port vlan mode to trunk, add erps protocol and data vlan  
Switch(config)# interface ge1/1  
Switch(config-ge1/1)# switchport mode trunk  
Switch(config-ge1/1)# switchport trunk allowed vlan add 2  
Switch(config-ge1/1)# switchport trunk allowed vlan add 3  
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
```

```
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure erps instance 1, erps single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
Configure sw4:
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
```

|

---

```
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure erps instance 1, erps single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(2)Configuration example 2 :

Configure sw1 :

```
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
```

---

```
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure erps instance 2, erps single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-owner-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/3
Switch(config-erps-2)# ring 2 rl-port ge1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
Configure sw2:
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure erps instance 2, erps single ring 2
Switch(config)#erps 2
```

```
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/1
Switch(config-erps-2)# ring 2 rl-port ge1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
Configure sw3:
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure erps instance 2, erps single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
```

```
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/1
Switch(config-erps-2)# ring 2 rl-port ge1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
Configure sw4:
Switch>enable
Switch#configure terminal
Create erps protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the ring port vlan mode to trunk, add erps protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure erps instance 2, erps single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-neighbor-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/3
```

|

---

```
Switch(config-erps-2)# ring 2 rl-port ge1/1
```

```
Switch(config-erps-2)# ring 2 enable
```

```
Switch(config-erps-2)#exit
```

---

## Chapter11 AAA configuration

---

This chapter describes how to configure 802.1x and RADIUS of the switch to prevent illegal users from accessing the network. For the use of the 802.1x client and HyperBoss, please refer to the respective operation manuals. This chapter mainly includes the following :

- 802.1x introduction
- RADIUS introduction
- 802.1x configuration
- RADIUS configuration

AAA is short for Authentication, Authorization, and Accounting. It provides a consistent framework for configuring the three security functions of authentication, authorization, and accounting. The configuration of AAA is actually a management of network security. Network security here mainly refers to access control. Including who can access the network? What services can users with access rights get? How to account for users who are using network resources?

Authentication (Authentication): verify whether the user can get access.

Authorization (Authorization): Authorized users can use which services.

Accounting (Accounting): record the user's use of network resources.

---

The network company has launched a complete set of AAA solutions, with products including 802.1x clients, various switches that support authentication, and HyperBoss, an authentication and accounting system. The 802.1x client is installed on the PC where users access the Internet. When users need to access the network, they need to use the 802.1x client for authentication. Only users who pass the authentication can use the network. It receives the client's authentication request, and transmits the user name and password to the authentication and accounting system HyperBoss. The switch itself does not perform the actual authentication work. HyperBoss receives the authentication request sent by the switch to perform the actual authentication, and performs accounting processing for the users who have successfully authenticated.

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.

## **11.1 802.1x introduction**

The 802.1x protocol is a port-based access control and authentication protocol. The port here refers to a logical port, which can be a physical port, MAC address, or VLAN ID. The switches of the network implement the 802.1x protocol based on the MAC address.

802.1x is a Layer 2 protocol. The authenticated switch and the user's PC must be on the same subnet, and protocol packets cannot cross network segments. 802.1x authentication uses a client server model, and there must be a server to authenticate all users. Before the user passes the authentication, only the authentication flow can pass through the port of the switch. After the authentication is successful, the data flow can pass through the port of the switch, that is, the user must access the network after passing the authentication.

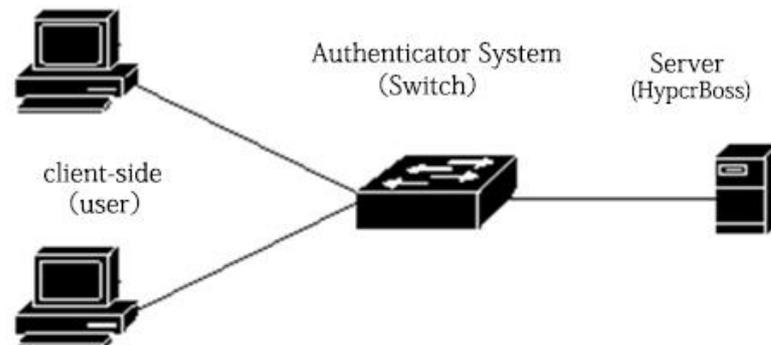
This section mainly includes the following :

- 802.1x device composition
- Introduction to protocol package
- Protocol flow interaction
- 802.1x port status

### **11.1.1 802.1x device composition**

An 802.1x device is composed of three parts: a client (Supplicant System), an

authentication system (Authenticator System), and an authentication server (Authentication Server System). As shown below:



802.1x device

The client refers to a device requesting access to the network, which is generally a user terminal system, such as a user's PC. An 802.1x client software must be installed on the user terminal system, which implements the client part of the 802.1x protocol. The client initiates an 802.1x authentication request and 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 (referred to as the 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, Then 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, and forwards the user's identity information to the authentication server, and forwards the authentication result from the authentication server to the client. The authentication system needs to implement the server part of the 802.1x protocol near the user side, and the client part of the RADIUS protocol near the authentication server side. The RADIUS protocol client of the authentication system encapsulates the 802.1x client with EAP information in RADIUS Send to the authentication server, and decapsulate the EAP information from the RAIDUS protocol packet sent from the authentication server and transmit it to the 802.1x client through the 802.1x server part.

An authentication server refers to a device that actually authenticates users. The authentication server receives the identity information of the user from the authentication system and verifies it. If the authentication succeeds, the authentication server authorizes

the authentication system to allow the user to access the network. If the authentication fails, the authentication server tells the authentication system that the user failed authentication and the user cannot access the network . The authentication server and the authentication system communicate through the RADIUS protocol extended by EAP. The network provides an authentication and charging system HyperBoss to authenticate and charge users.

## 11.1.2 Brief introduction of protocol package

The authentication data stream transmitted by the 802.1x protocol on the network is in EAPOL (EAP Over LAN) frame format. All user identity information (including user name and password) is encapsulated in EAP (Extended Authentication Protocol), and EAP is encapsulated in EAPOL frame. The user name exists in EAP in plain text, and the password exists in EAP in MD5 encrypted form.

The format of the EAPOL frame is shown below. PAE Ethernet Type is EAPOL's Ethernet protocol type number, with a value of 0x888E. Protocol Version is the EAPOL version number, with a value of 1. Packet Type refers to the EAPOL frame type. Packet Body Length is the length of the EAPOL frame content. Packet Body refers to the content of the EAPOL frame.

|                    | 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 :

**EAPOL-Start:** The value of Packet Type is 1, an authentication initiation frame. When the user needs to authenticate, this frame is first initiated and sent by the client to the switch.

**EAPOL-Logoff:** The value of Packet Type is 2, exit the request frame, and send this frame to notify the switch when the user does not need to use the network.

**EAP-Packet :** Packet Type value is 0, authentication information frame, used to carry

authentication information.

The EAP packet format is shown below. Code refers to the types of EAP packets, including Request, Response, Success, and Failure. Identifier refers to the identifier used to match Response and Request. Length refers to the length of the EAP packet, including the packet header. Data refers to EAP packet data.

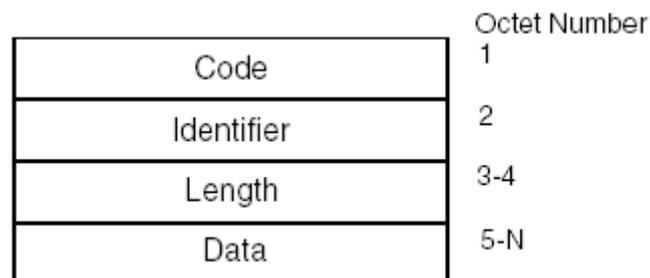
EAP package includes the following four types :

EAP-Request : Code value is 1, the EAP request packet is sent from the switch to the client to request the user name and/or password.

EAP-Response : Code value is 2, EAP response packets are sent from the client to the switch, and the user name and/or password are sent to the switch.

EAP-Success : The Code value is 3, and the EAP success packet is sent from the switch to the client to tell the client that the user authentication is successful.

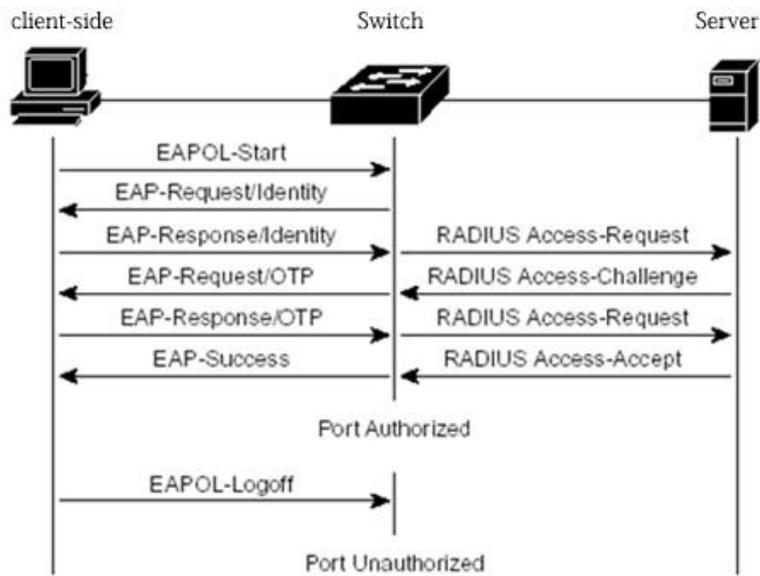
EAP-Failure : The Code value is 4, and the EAP failure packet is sent from the switch to the client to tell the client that the user authentication failed.



EAP packet format

### 11.1.3 Protocol flow interaction

When 802.1x is enabled on the switch and the port status is Auto, all access users under this port must pass authentication before they can access the network. The protocol interaction is as follows.

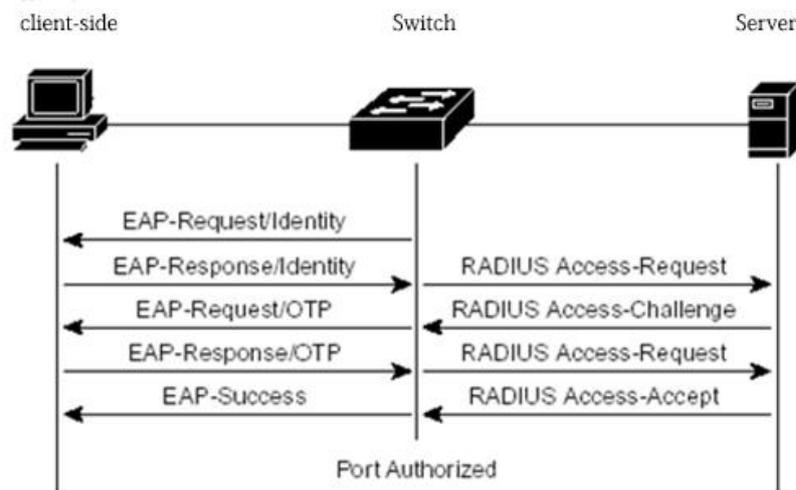


Client initiates authentication protocol interaction

When the user needs to access the network, the client first sends EAPOL-Start to the switch to request authentication. After the switch receives the authentication request, it sends an EAP-Request to request the user's username. The client sends back EAP-Response. The switch extracts the EAP information and encapsulates it in the RADIUS packet is sent to the authentication server. The authentication server requests the user's password. The switch sends an EAP-Request to the client to request the user's password. The client sends back EAP-Response. The switch encapsulates the EAP information in the RADIUS packet and sends it to the authentication server. The server authenticates the user based on the user name and password. If the authentication is successful, the authentication server notifies the switch, and the switch sends EAP-Success to the client and puts the user's logical port in the authorized state. When the client receives the 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, and the switch changes the user's logical port status to the unauthorized state, at which time the user cannot access the network.

In order to prevent the client from going offline abnormally, the switch provides a re-authentication mechanism. You can set the re-authentication interval on the switch. When the authentication time arrives, the switch initiates re-authentication. If the authentication is successful, the user can continue to use the network. Failure, users will not be able to use the network. The protocol interaction is shown below.



Re-authentication protocol interaction

### 11.1.4 802.1x port status

The port status here refers to the physical port status of the switch. There are four states of the physical port of the switch: N/A state, Auto state, Force-authorized state and Force-unauthorized state. When the switch does not open 802.1x, all ports are in N/A state. When the switch port is set to the Auto state, Force-authorized state, or Force-unauthorized state, you must first enable 802.1x on the switch.

When the port of the switch is in the N/A state, all users under the port can access the network without authentication. When the switch receives 802.1x protocol packets from this port, it discards these protocol packets.

When the port of the switch is in Force-authorized state, all users under the port can access the network without authentication. When the switch receives the EAPOL-Start packet from the port, the switch returns an EAP-Success packet. When the switch receives other 802.1x protocol packets from the port, it discards these protocol packets.

When the port of the switch is in Force-unauthorized state, all users under the port cannot always access the network, and the authentication request will never pass. When the switch receives 802.1x protocol packets from this port, it discards these protocol packets.

When the port of the switch is in the Auto state, all users under the port must pass

|

---

authentication before they can access the network. The 802.1x protocol interaction is shown in the figure. If the user needs to do authentication, the port should generally be set to the Auto state.

When the switch port is set to the Auto state, the anti-ARP spoofing function is enabled at the same time; the anti-ARP spoofing function can control only the data packets of the source MAC and source IP of the IP packet that meet the information provided by the client during authentication and the sender IP of the ARP packet. Data packets that match the sender's MAC and the information provided by the client during authentication can be forwarded by this port, otherwise they will be discarded. To configure this function, the client must be a statically configured IP address. If the IP address is obtained dynamically through the DHCP protocol, the DHCP SNOOPING protocol can be enabled to achieve this function; if you need a more detailed introduction, please refer to the IP MAC binding configuration.

## 11.2 RADIUS introduction

When the user performs authentication, the RADIUS protocol that supports EAP extension is used for interaction between the switch and the authentication server. The RADIUS protocol uses a client/server model. The switch needs to implement a RADIUS client, and the authentication server needs to implement a RADIUS server.

In order to ensure the security of the interaction between the switch and the authentication server and prevent the interaction between the illegal switch or the illegal authentication server, the switch and the authentication server must authenticate each other. The switch and the authentication server need the same key. When the switch or the authentication server sends a RADIUS protocol packet, all protocol packets use the HMAC algorithm to generate a message digest based on the key. When the switch and the authentication server receive the RADIUS protocol packet, all The message digest of the protocol package must be verified with a key. If the verification is passed, it is considered to be a legitimate RADIUS protocol package, otherwise it is an illegal RADIUS protocol package and discarded.

This section mainly includes the following :

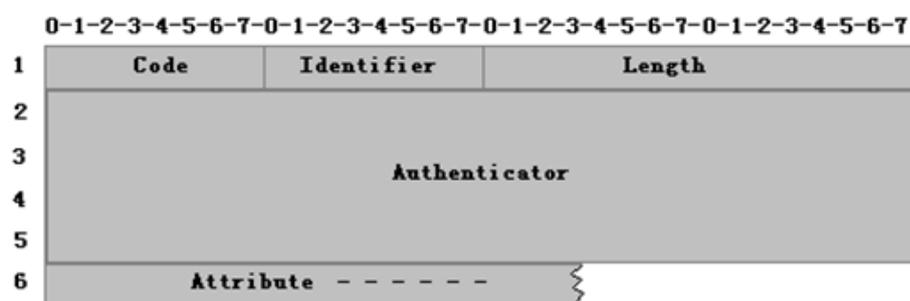
- Introduction to protocol package
- Protocol flow interaction
- User authentication method

## 11.2.1 Brief introduction of protocol package

RADIUS is a protocol built on UDP. RADIUS can encapsulate authentication information and accounting information. The early RADIUS authentication port is 1645, currently using port 1812, the early RADIUS accounting port is 1646, and currently using port 1813.

Because RADIUS is carried on UDP, RADIUS must have a timeout retransmission mechanism. At the same time, in order to improve the reliability of the communication between the authentication system and the RADIUS server, two RADIUS server schemes are generally adopted, that is, a backup server mechanism.

The format of the RADIUS message is shown below. Code refers to the RADIUS protocol packet type. Identifier refers to an identifier used to match requests and responses. Length refers to the length of the entire message (including the message header). Authenticator is a 16-byte string, a random number for the request packet, and a message digest generated by MD5 for the response packet. Attribute refers to the attribute in the RADIUS protocol package.



RADIUS packet format

The network uses the following RADIUS protocol packages :

**Access-Request:** Code value is 1, an authentication request packet sent from the authentication system to the authentication server, and the user name and password are encapsulated in this packet.

**Access-Accept:** Code value is 2, a response packet sent from the authentication server to the authentication system, indicating that the user authentication is successful.

**Access-Reject:** Code value is 3, a response packet sent from the authentication server to the authentication system, indicating user authentication failure.

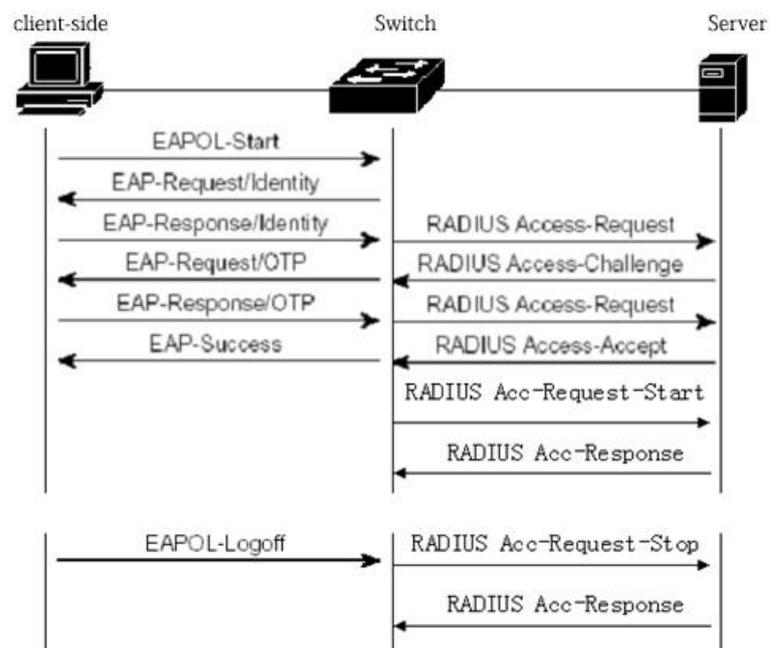
Access-Challenge: Code value 11, a response packet sent from the authentication server to the authentication system, indicating that the authentication server needs further information of the user, such as password.

Accounting-Request: Code value is 4, the accounting request packet sent from the authentication system to the authentication server, including the start accounting and end accounting packets, and the accounting information is encapsulated in this packet.

Accounting-Response: Code value is 5, a charging response packet sent from the authentication server to the authentication system, indicating that accounting information has been received.

## 11.2.2 Protocol flow interaction

When the user initiates authentication, the authentication system and the authentication server interact through the RADIUS protocol. The following figure shows the protocol flow interaction of the authentication system without sending RADIUS accounting packets. In general, after a successful user authentication or when a user goes offline, the authentication system needs to send a RADIUS accounting packet to the authentication server. The protocol flow interaction is shown in the following figure.



When the user performs authentication, the switch encapsulates the user name in an Access-Request message and sends it to the authentication server. The server responds

---

to the Access-Challenge request for the user's password. The switch requests the client user's password. The client encapsulates the password in the EAP. The switch After obtaining this EAP, it is encapsulated in Access-Request and sent to the authentication server. The authentication server authenticates the user. If the authentication is successful, it returns Access-Accept to the switch. After receiving this message, the switch notifies the client that the authentication is successful and sends Accounting-Request informs the authentication server to start charging, and the authentication server sends back Accounting-Response.

When the user does not want to use the network, notify the switch user to go offline, the switch sends Accounting-Request to notify the authentication server to end the accounting, the accounting information is encapsulated in this package, and the authentication server sends back Accounting-Response.

### 11.2.3 User authentication method

RADIUS has three user authentication methods, as follows :

- PAP (Password Authentication Protocol). The user passes the user name and his password to the switch in clear text. The switch passes the user name and password to the RADIUS server through the RADIUS protocol package. The RADIUS server looks up the database. If the same user name and password exist, the authentication is passed, otherwise the authentication is not passed.
- CHAP (Challenge Handshake Authentication Protocol). When a user requests Internet access, the switch generates a 16-byte random code to the user. The user encrypts the random code, password and other domains to generate a response, and transmits the user name and response to the switch. The switch transmits the user name, response and the original 16-byte random code to the RADIUS server. RADIUS looks up the database on the exchange side according to the user name, obtains the same password used for encryption at the user side, and then encrypts it according to the 16-byte random code transmitted, and compares the result with the transmitted response. If the same indicates Verification passed, if not the same, verification failed.

EAP (Extensible Authentication Protocol). With this authentication method, the switch does not really participate in the authentication, but only serves as a forwarding function

---

between the user and the RADIUS server. When a user requests Internet access, the switch requests the user's user name and forwards the user name to the RADIUS server. The RADIUS server generates a 16-byte random code for the user and stores the random code. The user pairs the random code, password, and other fields. Encryption generates a response, passes the user name and response to the switch, and the switch forwards it to the RADIUS server. RADIUS searches the database on the switch side according to the user name, obtains the same password used for encryption at the user side, and then encrypts according to the stored 16-byte random code, and compares the result with the response received. If the same indicates verification Passed, if not the same, it means that the verification failed.

The authentication and charging solution of the network uses the EAP user authentication method.

## **11.3 802.1x configuration**

This section describes the configuration of 802.1x in detail, mainly including the following content :

- 802.1x default configuration
- Start and shut down 802.1x
- Configure 802.1x port status
- Configure re-authentication mechanism
- Configure the maximum number of port access hosts
- Configure interval time and retransmission times
- Configure the port as a transmission port
- Configure the 802.1x client version number
- Configure whether to check the client version number
- Configure authentication method
- Configure whether to check the client's timing package
- Display 802.1x information

### **11.3.1 802.1x default configuration**

|

---

The default configuration of the switch 802.1x is as follows :

- 802.1x is off.
- The status of all ports is N/A.
- The re-authentication mechanism is closed, and the re-authentication interval is 3600 seconds.
- The maximum number of access hosts on all ports is 100.
- The timeout interval for resending EAP-Request is 30 seconds.
- The number of times to retransmit EAP-Request is 3.
- The waiting time for user authentication failure is 60 seconds.
- The timeout interval of the server overtime retransmission is 10 seconds.

The switch provides a command in the global CONFIG mode to return all configurations to the default state. The command is as follows :

```
Switch(config)#dot1x default
```

### **11.3.2 Start and shut down 802.1x**

The first step in configuring 802.1x is to start 802.1x. Enter the following command in global CONFIG mode to start 802.1x :

```
Switch(config)#dot1x
```

When 802.1x is turned off, all ports return to N/A state. Enter the following command in global CONFIG mode to close 802.1x :

```
Switch(config)#no dot1x
```

### **11.3.3 Configure 802.1x port status**

Before setting the 802.1x port status, be sure to enable 802.1x. If all users under the

|

---

port must pass authentication to access the network, the port must be set to the Auto state.

The following command sets the port ge1/1 to Auto state in the interface configuration mode and enables the anti-ARP spoofing function :

```
Switch(config-ge1/1)dot1x control auto
```

If the anti-ARP spoofing configuration fails, it may be caused by the following reasons :

- 1、 System CFP resources are exhausted。
- 2、 The current interface is configured with ACL filtering。
- 3、 DHCP SNOOPING is enabled on the current interface。
  
- 4、 The configured interface is a Layer 3 interface or trunk interface。

The following command sets the port ge1/1 to Force-authorized state in interface configuration mode :

```
Switch(config-ge1/1)dot1x control force-authorized
```

The following command sets port ge1/1 to Force-unauthorized state in interface configuration mode :

```
Switch(config-ge1/1)dot1x control force-unauthorized
```

The following command sets port ge1/1 to N/A state in interface configuration mode :

```
Switch(config-ge1/1)no dot1x control
```

Note: If a port has been bound to a MAC address, then this port cannot be set to Auto, Force-authorized or Force-unauthorized state.

### **11.3.4 Configure the re-authentication mechanism**

To prevent the switch and authentication server from being noticed after the client

|

---

goes offline abnormally, the switch provides a re-authentication mechanism. The switch initiates authentication every re-authentication interval.

The following command starts the re-authentication mechanism in global CONFIG mode :

```
Switch(config)#dot1x reauthenticate
```

The following command turns off the re-authentication mechanism in global CONFIG mode :

```
Switch(config)#no dot1x reauthenticate
```

The following command sets the re-authentication interval in global CONFIG mode :

```
Switch(config)#dot1x timeout re-authperiod <interval>
```

Note: Do not set the re-authentication interval too short, otherwise the network bandwidth and the CPU resource consumption of the switch will be too high.

## **11.3.5 Configure the maximum number of port access hosts**

Each port of the switch can control the maximum number of hosts that can be accessed. This function can restrict users from using multiple hosts to illegally access the network. The maximum number of port access hosts is 100 by default, and the maximum number can be set to 100. If the maximum number of access hosts on the port is set to 0, then the port denies any user access.

The following command sets the maximum number of ports ge1/1 connected to the host in interface configuration mode :

```
Switch(config-ge1/1)dot1x support-host <number>
```

---

## 11.3.6 Configure interval time and retransmission times

The 802.1x protocol standard specifies some intervals and retransmission times of the protocol interaction and protocol state machine. The switch uses standard intervals and retransmission times. It is recommended that users do not change these interval times and retransmission times when using them.

tx-period indicates the interval between the switch retransmitting EAP-Request protocol packets; max-req indicates the number of times the switch retransmits EAP-Request; quiet-period indicates the interval between waiting for re-authentication when user authentication fails; server-timeout indicates Interval time for the switch to resend the RADIUS packet to the authentication server; supp-timeout indicates the time interval for the switch to resend the eap request packet to the client.

The following command configures these intervals and retransmission times in global CONFIG mode :

```
Switch(config)#dot1x timeout tx-period <interval>
Switch(config)#dot1x max-req <number>
Switch(config)#dot1x timeout quiet-period <interval>
Switch(config)#dot1x timeout server-timeout <interval>
Switch(config)#dot1x timeout supp-timeout <interval>
```

## 11.3.7 Configure the port as a transmission port

When the switch does not open 802.1x authentication, and other switches in the subnet have 802.1x authentication turned on, you can configure the switch to connect the client and the port of the certified switch as a transmission port, and forward eapol between the client and the 802.1x certified switch Certification package. In order to achieve the 802.1x authentication of the client by other switches.

The following command sets port ge1/1 as a transmission port in interface configuration mode :

```
Switch(config-ge1/1)#dot1x transmit-port
```

|

---

The following command sets port ge1/1 as a non-transport port in interface configuration mode :

```
Switch(config-ge1/1)no dot1x transmit-port
```

### **11.3.8 Configure the 802.1x client version number**

Configure the version number of the 802.1x client. 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 :

```
Switch(config)# dot1x client-version <string>
```

### **11.3.9 Configure whether to check the client version number**

Configure whether to check the version number of the 802.1x client. If it is configured to check, the switch must first check the client version number when doing authentication. The default is configured to check.

The following command configures to open the client version number check in global CONFIG mode :

```
Switch(config)# dot1x check-version open
```

### **11.3.10 Configure authentication method**

Configure the switch's authentication method for 802.1x packets. The authentication method initiated by the client is divided into general authentication and extended authentication. The switch can be configured to authenticate first. If the authentication

method initiated by the client is inconsistent with the authentication method configured on the switch, the client will switch to another authentication method to initiate authentication after a certain number of authentication failures.

The following command configures the authentication mode of the switch to the extended authentication mode in the global CONFIG mode :

```
Switch(config)# dot1x extended
```

### **11.3.11 Configure whether to check the client's timing package**

Configure whether the switch checks the client's timed packets. After the authentication is successful, the switch will require the client to send 802.1x packets regularly, but not all clients will send 802.1x packets regularly after passing the authentication.

In this way, configure whether the switch checks the client's timing packets through commands.

The following command is configured for the switch to check the client's timing packets in global CONFIG mode :

```
Switch(config)# dot1x check-client
```

### **11.3.12 Display 802.1x information**

The following command displays 802.1x information in normal mode/privileged mode. When the command is show dot1x, it displays all 802.1x configuration information, including configuration information of all ports; when the command is show dot1x interface, it displays the information under the port Information of all access users :

```
Switch#show dot1x
```

```
Switch#show dot1x interface
```

---

## 11.4 RADIUS configuration

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

- Default configuration of RADIUS
- Configure the IP address of the authentication server
- Configure shared key
- Starting and closing billing
- Configure RADIUS port and attribute information
- Configure RADIUS roaming function
- Display RADIUS information

### 11.4.1 RADIUS default configuration

The default configuration of the switch RADIUS is as follows :

- The IP addresses of the primary authentication server and the backup authentication server are not configured, that is, the IP address is 0.0.0.0.
- No shared key is configured, that is, the shared key string is empty.
- Billing is enabled by default.
- RADIUS authentication UDP port is 1812, accounting UDP port is 1813.
- The RADIUS attribute NASPort value is 0xc353, NASPortType value is 0x0f, NASPortServer value is 0x02.

### 11.4.2 Configure the IP address of the authentication server

To enable RADIUS communication between the switch and the authentication server, you need to configure the IP address of the authentication server on the switch. In practical applications, one authentication server or two authentication servers can be used, one as the main authentication server and one as the backup authentication server. If the

|

---

switch is configured with the IP addresses of two authentication servers, when the switch interrupts communication with the main authentication server, it can switch to communicating with the backup authentication server.

The following command configures the IP address of the primary authentication server in global CONFIG mode :

```
Switch(config)#radius-server host <ip-address>
```

The following command configures the IP address of the backup authentication server in global CONFIG mode :

```
Switch(config)#radius-server option-host <ip-address>
```

### 11.4.3 Configure shared key

The switch and the authentication server must authenticate each other. Both the switch and the authentication server need to be set with the same shared key. Note that the shared key on the switch must be the same as the authentication server.

The following command configures the shared key of the switch in global CONFIG mode :

```
Switch(config)#radius-server key <string>
```

### 11.4.4 Turn billing on and off

If accounting is disabled on the switch, the switch will not send RADIUS accounting packets to the authentication server after the authentication is successful or the user goes offline. Generally, in practical applications, billing is turned on.

The following command starts charging in global CONFIG mode :

```
Switch(config)#radius-server accounting
```

The following command turns off accounting in global CONFIG mode :

|

---

Switch(config)#no radius-server accounting

## 11.4.5 Configure RADIUS port and attribute information

It is recommended that users do not modify the RADIUS port and attribute information configuration.

The following command modifies the RADIUS authentication UDP port in global CONFIG mode :

```
Switch(config)#radius-server udp-port <port-number>
```

The following command modifies RADIUS attribute information in global CONFIG mode :

```
Switch(config)#radius-server attribute nas-portnum <number>
```

```
Switch(config)#radius-server attribute nas-porttype <number>
```

```
Switch(config)#radius-server attribute service-type <number>
```

## 11.4.6 Configure RADIUS roaming

When MAC, IP, or VLAN binding is performed on the client, and when the client is moved to another location, the bound client cannot perform 802.1x authentication because the MAC address, IP address, or VLAN of the client changes. Turn on radius roaming function, will ignore the client's MAC, IP or VLAN binding, thus continue to achieve 802.1x authentication.

The following command configures the RADIUS roaming function in the global CONFIG mode :

```
Switch(config)#radius-server roam
```

The following command disables RADIUS roaming function in global CONFIG mode :

|

---

```
Switch(config)#no radius-server roam
```

## 11.4.7 Display RADIUS information

The following command displays RADIUS configuration information in normal mode/privileged mode :

```
Switch#show radius-server
```

## 11.5 Configuration example

Open the 802.1x protocol, configure port ge1/1 as Auto, configure the main authentication server as 198.168.80.111, and configure the shared key of the switch as abcdef.

```
Switch#  
Switch# dot1x  
Switch#config t  
Switch(config)#radius-server host 198.168.80.111  
Switch(config)#radius-server key abcdef  
Switch(config)# interface ge1/1  
Switch(config-ge1/1)# dot1x control auto
```

---

# Chapter12 **GMRP**

## **configuration**

---

This chapter mainly includes the following :

- GMRP introduction
- GMRP configuration
- Displaying GMRP

### **12.1 GMRP introduction**

At present, GMRP (GARP Multicast Registration Protocol, GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP, used to maintain multicast registration information in the switch. All switches that support GMRP can receive multicast registration information from other switches, and dynamically update local multicast registration information, and can also propagate local multicast registration information to other switches. This information exchange mechanism ensures the consistency of the multicast information maintained by all GMRP-enabled devices in the same switching network.

When a host wants to join a multicast group, it will send a GMRP join message. The

switch joins the port that receives the GMRP join message to the multicast group, and broadcasts the GMRP join message in the VLAN where the receiving port is located, so that the multicast source in the VLAN can know the existence of the multicast member. When a multicast source sends a multicast message to a multicast group, the switch only forwards the multicast message to the port connected to the member of the multicast group, thereby implementing Layer 2 multicast in the VLAN.

## 12.2 GMRP configuration

GMRP main configuration includes:

Enable GMRP

View GMRP

In the configuration task, global GMRP must be enabled before port GMRP can be enabled.

### 12.2.1 Open GMRP settings

| command  | description                                     | Configuration mode        |
|--|---|---------------------------|
| set gmrp enable   disable                                    | Enable/disable all global vlan gmrp             | 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 interface registration multicast mode | Global configuration mode |
| set gmrp timer {join   leave   nleaveall} <time-value>       | Configure the time of various timers            | Global configuration mode |
| set port gmrp enable <if-name>                               | Enable port GMRP function                       | Global configuration mode |
| set port gmrp disable <if-name>                              | Disable the port GMRP function                  | Global configuration mode |

### 12.2.2 View GMRP information

After completing the above configuration, execute the show command in privileged mode to display the running status of GMRP after configuration, and verify the effect of the configuration by viewing the displayed information.

| command                 | description                         | Configuration mode |
|-------------------------|-------------------------------------|--------------------|
| show gmrp configuration | View GMRP configuration information | Privileged mode    |
| show gmrp machine       | View GMRP state machine             | Privileged mode    |

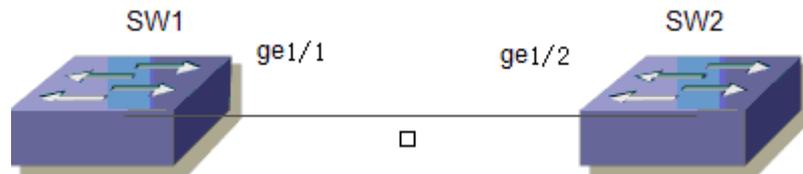
|                             | information                               |                 |
|-----------------------------|---|-----------------|
| show gmrp statistics vlanid | View specific vlanid's gmrp statistics    | Privileged mode |
| show gmrp timer <ifname>    | View timer information for specific ports | Privileged mode |

## 12.3 GMRP typical configuration example

### 1. Network requirements

In order to achieve dynamic registration and update of multicast information between switches, GMRP needs to be started on the switch.

### 2. Network diagram



GMRP example network diagram

### 3. Configuration steps

Configure SW1

Start global GMRP

```
Switch(config)# set gmrp enable
```

Start port GMRP on the Gigabit Ethernet port ge1/1

```
Switch(config)# set port gmrp enable ge1/1
```

```
Switch(config)#
```

Configure SW2

Start global GMRP

```
Switch(config)# set gmrp enable
```

Start port GMRP on Gigabit Ethernet port ge1/2

```
Switch(config)# set port gmrp enable ge1/2
```

```
Switch(config)#
```

---

# Chapter13 IGMP SNOOPING configuration

---

In the metropolitan area network/Internet, when the same data packet is sent to multiple but not all receivers in the network by unicast, since the packet needs to be copied to each receiving endpoint, as the number of receivers increases, the need The number of packets sent will also increase linearly, which makes the overall burden on the host, switching routing equipment and network bandwidth resources increase, and the efficiency is greatly affected.

With the increasing demand for multi-point video conferencing, video-on-demand, and group communication applications, in order to improve resource utilization, the multicast method has increasingly become a commonly used transmission method in multi-point communication.

The switch implements the IGMP SNOOPING function and serves multicast applications. IGMP SNOOPING monitors IGMP packets on the network to achieve dynamic learning of IP multicast MAC addresses.

This chapter describes the concept and configuration of IGMP SNOOPING, including the following contents :

- IGMP SNOOPING introduction
- IGMP SNOOPING configuration
- IGMP SNOOPING configuration example

## 13.1 IGMP SNOOPING introduction

In a traditional network, multicast data packets are treated as broadcasts in a subnet, which easily causes large network traffic and causes network congestion. When IGMP SNOOPING is implemented on the switch, IGMP SNOOPING can dynamically learn the IP multicast MAC address and maintain the output port list of the IP multicast MAC address, so that the multicast data stream is only sent to the output port, which can reduce network traffic.

---

This section mainly includes the following :

- IGMP SNOOPING process
- Layer 2 dynamic multicast
- Join a group
- Leave a group

### **13.1.1 IGMP SNOOPING process**

IGMP SNOOPING is a Layer 2 network protocol that listens for IGMP protocol packets passing through the switch, maintains a multicast group based on the receiving ports, VLAN IDs, and multicast addresses of these IGMP protocol packets, and then forwards these IGMP protocol packets. Only ports that have joined the multicast group can receive multicast data streams; this reduces network traffic and saves network bandwidth.

Multicast group includes multicast group address, member port, VLAN ID, Age time.

The formation of IGMP SNOOPING multicast group is a learning process. When a port of the switch receives an IGMP REPORT packet, IGMP SNOOPING generates a new multicast group, and the port that receives the IGMP REPORT packet is added to the multicast group. When the switch receives an IGMP QUERY packet, if the multicast group already exists in the switch, the port that received the IGMP QUERY also joins the multicast group, otherwise it simply forwards the IGMP QUERY packet. IGMP SNOOPING also supports IGMP V2's Leave mechanism; if IGMP SNOOPING is configured with fast-leave as ENABLE, the receiving port can immediately leave the multicast group when receiving the IGMP V2 leave packet; if fast-leave leave wait time is configured ( fast-leave-timeout), then the multicast group waits for this time to expire before leaving the multicast group.

IGMP SNOOPING has two update mechanisms. One is the leave mechanism introduced above. In most cases, IGMP SNOOPING deletes expired multicast groups by age time. When a multicast group joins IGMP SNOOPING, the time of joining is recorded. When the multicast group stays in the switch for more than a configured age time, the switch deletes the multicast group.

When a port receives the Leave protocol packet, the port will be immediately deleted from the multicast group to which it belongs. This situation may affect the continuity of the network data flow; because the port may be connected to a HUB or no IGMP SNOOPING

---

A functional network device, a lot of devices for receiving multicast data streams are connected to this device. If a device sends a Leave, other devices may not receive the multicast data stream. The fast-leave-timeout mechanism can prevent this from happening. Configure a time to leave and wait through Fast-leave-timeout. After receiving a leave packet from the port, the port waits for Fast-leave-timeout for a long time before retrieving from the multicast group to which it belongs Delete in the middle, may guarantee the continuity of the network multicast stream.

### **13.1.2 Layer 2 dynamic multicast**

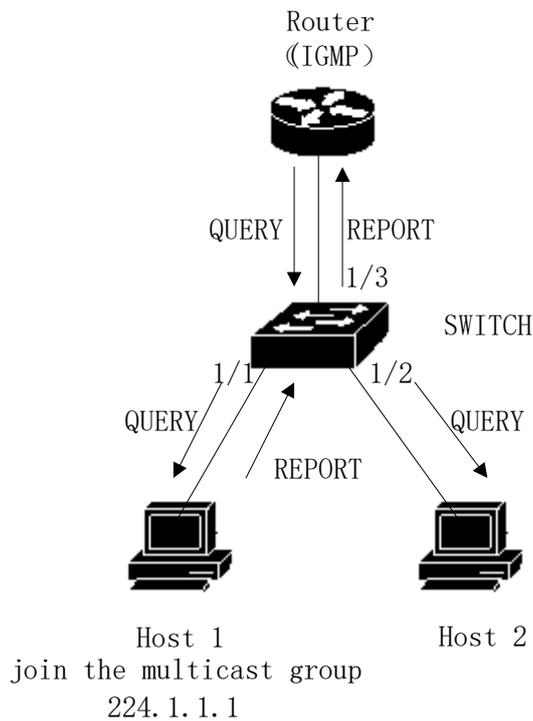
The multicast MAC address entries in the Layer 2 hardware multicast forwarding table can be dynamically learned through IGMP SNOOPING. What I learned dynamically through IGMP SNOOPING is the IP multicast MAC address.

When the switch turns off IGMP SNOOPING, the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode, the multicast MAC address cannot be learned dynamically, there is no entry in the Layer 2 hardware multicast forwarding table, and all Layer 2 multicast data streams are treated as Broadcast processing.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can turn on IGMP SNOOPING. At this time, the Layer 2 hardware multicast forwarding table is in the registered forwarding mode, and the switch can learn the group by listening to the IGMP protocol packets on the network. Only the MAC address can be forwarded if the layer 2 multicast stream matches the entry in the layer 2 hardware multicast forwarding table.

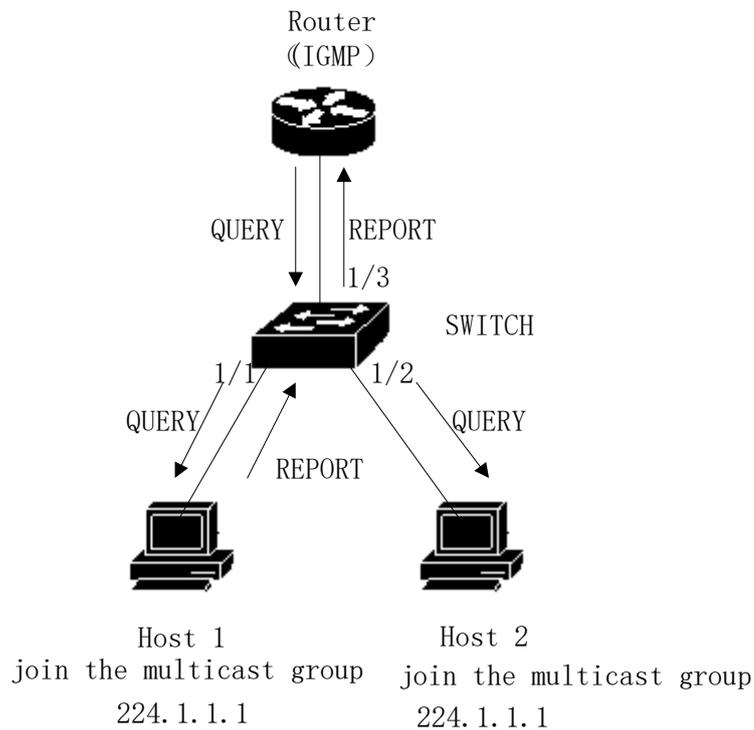
### **13.1.3 Join a group**

When a host wants to join a multicast group, the host sends an IGMP REPORT packet, which specifies the multicast group the host wants to join. When the switch receives an IGMP QUERY packet, the switch will forward the packet to all other ports in the same VLAN. When the host under the port who wants to join the multicast group receives the IGMP QUERY packet, it will return an IGMP REPORT packet. When the switch receives an IGMP REPORT packet, it will create a Layer 2 multicast entry. The port that receives the IGMP QUERY packet and the port of the IGMP REPORT packet will be added to the Layer 2 multicast entry and become its output port..



As shown above, all the devices are in a subnet, assuming that the VLAN of this subnet is 2. The router runs the IGMPv2 protocol and regularly sends IGMP QUERY packets. Host 1 wants to join the multicast group 224.1.1.1. After receiving the IGMP QUERY packet from port 1/3, the switch records this port and forwards the packet to ports 1/1 and 1/2. Host 1 sends back an IGMP REPORT packet after receiving the IGMP QUERY packet. Host 2 does not send the IGMP REPORT packet because it does not want to join the multicast group. After receiving the IGMP REPORT packet from port 1/1, the switch forwards the packet from query port 1/3 and creates a Layer 2 multicast entry (assuming that the entry does not exist). The Layer 2 multicast entry includes the following items :

| Layer 2 multicast address | VLAN ID | Output port list |
|---------------------------|---------|------------------|
| 01:00:5e:01:01:01         | 2       | 1/1 , 1/3        |



As shown in the above picture, the conditions are the same as 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 an IGMP QUERY packet and sends back an IGMP REPORT packet, the switch forwards the packet from query port 1/3 after receiving the IGMP REPORT from port 1/2 and adds the packet port 1/2 to the Layer 2 group. In the broadcast entry, the layer 2 multicast entry becomes :

| Layer 2 multicast address | VLAN ID | Output port list |
|---------------------------|---------|------------------|
| 01:00:5e:01:01:01         | 2       | 1/1 , 1/2 , 1/3  |

### 13.1.4 Leave a group

In order to form a stable multicast environment, devices running IGMP (such as routers) will send an IGMP QUERY packet to all hosts at regular intervals. The host that has joined the multicast group or wants to join the multicast group will send back an IGMP

---

REPORT after receiving the IGMP QUERY.

If the host wants to leave a multicast group, there are two ways: active leave and passive leave. Active leaving means that the host sends an IGMP LEAVE packet to the router. Passive leaving means that the host does not send back IGMP REPORT after receiving the IGMP QUERY from the router.

Corresponding to the way the host leaves the multicast group, there are also two ways to leave the layer 2 multicast entry on the switch: leave overtime and leave after receiving the IGMP LEAVE packet.

When the switch does not receive an IGMP REPORT packet of a multicast group from a port for more than a certain time, the port should be cleared from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, delete the two Layer multicast entry.

When the switch's fast-leave is configured as ENABLE, if a port receives an IGMP LEAVE packet from a multicast group, the port is cleared from the corresponding layer 2 multicast entry, and if the layer 2 multicast entry has no port , Then delete the Layer 2 multicast entry.

Fast-leave is generally used when a host is connected to a port; if there is more than one host under a port, fast-leave-timeout latency can be configured to ensure the continuity and reliability of the multicast stream in the network.

### **13.1.5 IGMP Query**

In a network with Layer 3 multicast devices, Layer 3 multicast devices act as IGMP queriers. Layer 2 multicast devices only need to listen to IGMP messages to establish and maintain forwarding entries to achieve Layer 2 multicast. In a network without Layer 3 multicast devices, Layer 3 multicast devices cannot act as IGMP queriers. To enable the Layer 2 multicast device to listen to IGMP messages, the IGMP querier function must be configured on the Layer 2 device. The Layer 2 multicast device must act as an IGMP querier and listen to IGMP messages before it can establish and maintain forwarding entries and implement Layer 2 multicast.

working principle

In the IGMP querier function, the Layer 2 device plays the role of IGMP routing query, periodically sends IGMP query messages, listens and maintains the IGMP Report messages answered by users, and establishes a Layer 2 multicast forwarding entry. The relevant parameters of the query message sent by IGMP query can be adjusted by the user through configuration.

---

### Start querier

The user can configure to enable the querier function on the specified VLAN.

Specify the IGMP version that the querier is running

Specify the IGMP version used by the query message sent by the querier, which can be configured as v1, v2, or v3.

Configure the source IP of the querier

Configure the source IP address carried in the query message sent by the querier,

Configure the query interval of the querier

Configure the interval of query messages sent by the global querier.

## 13.1.6 Icmp snooping multicast filtering

Devices running IGMP Snooping can control the scope and load of multicast services, and can effectively prevent illegal multicast streams. By configuring multicast filtering rules globally and applying rules on interfaces, you can allow or restrict the joining of specific groups.

## 13.2 IGMP SNOOPING configuration

### 13.2.1 IGMP SNOOPING default configuration

IGMP SNOOPING is off by default, and the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode.

Fast-leave is off by default.

Fast-leave-timeout time is 300 seconds.

The age of the multicast group REPORT port defaults to 400 seconds.

The age of the multicast group QUERY port defaults to 300 seconds.

### 13.2.2 Enable and disable IGMP SNOOPING

Open IGMP SNOOPING protocol can be opened globally or part of the VLAN can be opened separately; Only if IGMP SNOOPING is enabled globally can IGMP SNOOPING

|

---

for a VLAN be turned on or off.

Turn on global IGMP SNOOPING

Switch#configure terminal

Switch(config)#ip igmp snooping

Turn on IGMP SNOOPING for a VLAN

Switch#configure terminal

Switch(config)#ip igmp snooping vlan <vlan-id>

Turn off global IGMP SNOOPING

Switch#configure terminal

Switch(config)#no ip igmp snooping

Disable IGMP SNOOPING for a VLAN

Switch#configure terminal

Switch(config)#no ip igmp snooping vlan <vlan-id>

### 13.2.3 Configure time to live

Configure the time to live for multicast groups

Switch#configure terminal

Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan  
<vlan-id>

The unit of Interval is milliseconds.

Configure the time to live for a query group

Switch#configure terminal

Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan  
<vlan-id>

The unit of Interval is milliseconds.

### 13.2.4 Fast-leave configuration

Enable a VLAN fast-leave

Switch#configure terminal  
Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Disable fast-leave  
Switch#configure terminal  
Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

Configure fast-leave wait time  
Switch#configure terminal  
Switch(config)# ip igmp snooping 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>

### **13.2.5 MROUTER configuration**

Configure a static query port  
Switch#configure terminal  
Switch#interface ge1/6  
Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

### **13.2.6 Configure igmp snooping port query function**

Configure a static query port  
Switch#configure terminal  
Switch(config)#interface ge1/6  
Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

### **13.2.7 Configure igmp snooping query function**

Enable the igmp snooping query function of vlan1  
Switch#configure terminal

Switch(config)#ip igmp sno  
Switch(config)#ip igmp snooping querier vlan 1

## 13.2.8 Configure igmp snooping multicast filtering

Configure port ge1/1 to filter the multicast address to 235.0.0.1  
Switch#configure terminal  
Switch(config)#ip igmp snooping filter-rule 1 deny 235.0.0.1  
Switch(config)#interface ge1/1  
Switch(config-ge1/1)#ip igmp snooping filter-group 1

## 13.2.9 Display information

Display IGMP SNOOPING configuration information  
Switch#show ip igmp snooping

Display configuration information of a VLAN  
Switch#show ip igmp snooping vlan <vlan-id>

Display REPORT multicast group aging information  
Switch#show ip igmp snooping age-table group-membership

Display QUERY's aging information  
Switch#show ip igmp snooping age-table query-membership

Display the forwarding information of the multicast group  
Switch#show ip igmp snooping forwarding-table

Display MROUTER information  
Switch#show ip igmp snooping mrouter

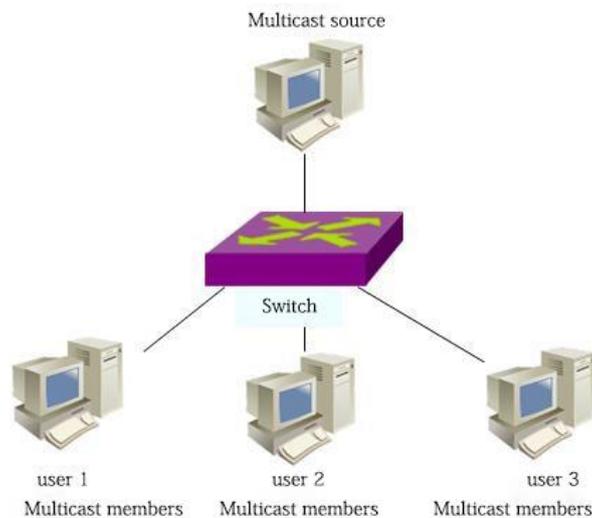
Display the current configuration of the system, including the configuration of IGMP SNOOPING  
Switch#show running-config

---

## 13.3 IGMP SNOOPING configuration example

### 13.3.1 configuration

Enable IGMP SNOOPING on the switch, user 1, user 2, and user 3 can join a specific multicast group.



```
Switch#config t
Switch(config)#ip igmp snooping
Switch(config)#vlan database
Switch(config-vlan)#vlan 200
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 200
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ip igmp snooping vlan 200
Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200
```

---

# Chapter14 MVR configuration

---

This chapter mainly includes the following :

- MVR introduction
- MVR configuration

## 14.1 MVR introduction

Multicast VLAN registration (MVR) is used for multicast streaming applications in service provider networks, such as TV on demand. MVR allows subscribers on a port to subscribe to or cancel multicast streams in a multicast VLAN, and allows data streams in a multicast VLAN to be shared by other VLANs. MVR has two purposes: (1) through simple configuration, it can effectively and safely transfer multicast streams between VLANs; (2) support dynamic joining and leaving of multicast groups ;

The operation mode of MVR is similar to IGMP snooping. The two functions can be started at the same time. MVR only handles the joining and leaving of the configured multicast group. The joining and leaving of other groups are managed by IGMP snooping. The difference between the two is that multicast streams in IGMP snooping can only be forwarded in one VLAN, while MVR multicast streams can be forwarded in different

---

VLANs.

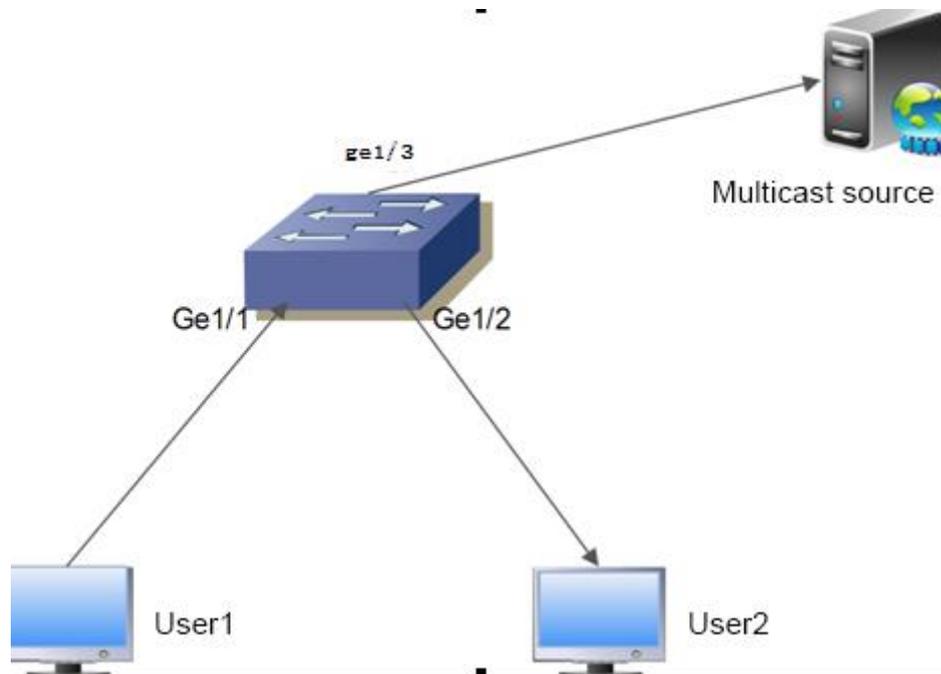
## 14.2 MVR configuration

| command                        | description  | CLI mode                     |
|--------------------------------|--|------------------------------|
| mvr (enable disable)           | Start global MVR   | Global configuration mode    |
| no mvr                         | Clear all MVR configuration  | Global configuration mode    |
| mvr group A.B.C.D              | Configure IP Multicast Address                                       | Global configuration mode    |
| no mvr group A.B.C.D           | Delete IP Multicast Address  | Global configuration mode    |
| mvr group A.B.C.D <1-256>      | Configure an IP multicast address and a continuous MVR group address | Global configuration mode    |
| mvr vlan <1-4094>              | Specify 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) | Enable interface MVR   | Interface configuration mode |
| show mvr                       | Display MVR configuration information                                | Privileged mode              |

## 14.3 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. The program range is 225.1.1.1~225.1.1.64, and mvr vlan is 100. :



Configure vlan, enable global IGMP snooping, configure mvr vlan, mvr program group range, globally enable mvr :

```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)# mvr enable
Switch(config)#mvr vlan 100
Switch(config)#mvr group 225.1.1.1 64
Switch#
```

Configure switch user ports ge1/1 ge1/2 and upstream port ge1/3:

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)# switchport hybrid native vlan 10
Switch(config-ge1/1)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/1)#mvr enable
Switch(config-ge1/1)#
```

```
Switch#configure terminal
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)# switchport hybrid native vlan 20
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/2)#mvr enable
Switch(config-ge1/2)#
```

```
Switch#configure terminal
```

|

---

```
Switch(config)#interface ge1/3
Switch(config-ge1/3)# switchport access vlan 100
Switch(config-ge1/3)#
```

## Chapter15 DHCP SNOOPING configuration

---

In a dynamically connected network environment, the host obtains the IP address and network parameters through the DHCP server. DHCP SNOOPING is a listening protocol proposed for ARP attacks. By listening to DHCP packets, the IP address and client MAC address assigned by the DHCP server to the client are dynamically bound to filter ARP attack packets on the switch.

The switch supports DHCP SNOOPING function, which can effectively prevent ARP attacks. DHCP SNOOPING listens for DHCP messages on the network and binds port ARP information.

Four physical ports of the DHCP server can be configured to prevent unknown servers from interfering with the network to a certain extent.

This chapter describes the concept and configuration of DHCP SNOOPING, mainly

---

including the following content :

- DHCP SNOOPING introduction
- DHCP SNOOPING configuration
- DHCP SNOOPING configuration example

## 15.1 DHCP SNOOPING introduction

The ARP protocol has created a loophole in network security due to a simple trust mechanism. When an ARP attack packet carrying false MAC information reaches the host, it will directly cover the local ARP cache table without restriction, resulting in normal data flow to the attacker. To this end, the port's ARP information binding is implemented on the network layer 2 switch, which can effectively filter ARP attack packets, so that the attack packets cannot reach the attacked host. If an unpredictable DHCP server enters the network, the IP address allocation will be confused. The DHCP SNOOPING protocol provides a physical port for binding the link server. Unspecified physical ports cannot forward DHCP protocol packets sent by the DHCP server, which can reduce this unknown. The opportunity for the server to enter the network.

This section mainly includes the following :

- DHCP SNOOPING process
- DHCP SNOOPING binding table
- DHCP SNOOPING is bound to the physical port of the server

### 15.1.1 DHCP SNOOPING process

The DHCP SNOOPING protocol only listens to DHCPrequest, DHCPack, and DHCPrelease messages, does not receive other types of DHCP messages, and binds the mapping relationship between IP and MAC according to these messages.

The global DHCP SNOOPING switch is responsible for turning on the switch to receive DHCP messages, that is, IP messages with UDP ports 67 and 68.

---

## 15.1.2 DHCP SNOOPING binding table

The DHCP SNOOPING binding table entry is indexed by the MAC address and contains the entry type, IP address, MAC address, interface information, delay timer, and lease timer. There are two types of REQ and ACK. The REQ type entry indicates that a DHCPrequest message has been received and a DHCPack message has not been received. At this time, a delay timer is started. The default interval is 10 seconds. If the DHCPack message is not received in 10 seconds Text, the binding table entry of the REQ type is deleted; The ACK type entry indicates that a DHCPack message is received. The recorded IP address is the IP address assigned by the server. At this time, the lease timer is started. The time interval is the lease value provided by the DHCP server included in the DHCPack message. The server is restarted, and when the lease expires, the binding table entry is deleted. The interface information records the interface where the client is located, that is, the interface corresponding to the binding relationship between the IP address and the MAC address.

When a DHCPrequest message is received, a binding table entry is created, the entry type is REQ, the IP address, MAC address, interface information is recorded, and a 10-second delay timer is started.

When a DHCPrequest message is received, there is already a REQ type binding table entry, the entry is updated, and the delay timer is restarted.

When a DHCPrequest message is received and an ACK type binding table entry already exists, the interface information is recorded.

When a DHCPack message is received, if there is a REQ type binding table entry, the IP address assigned by the server in the DHCPack message is recorded, the delay timer is turned off, and the lease timer is started.

When a DHCPack message is received, there is no REQ type binding table entry, the message is discarded.

When a DHCPack message is received, a binding table entry of the ACK type already exists. If the interface has changed, the binding table entry of the original interface is deleted and the entry is updated.

If the interface has not changed and the IP address assigned by the server has changed, delete the binding table entry of the original interface and update the entry.

If the interface has not changed and the IP address has not changed, it indicates that it is a renewal process, and the lease timer can be restarted.

When the delay timer expires, the REQ type binding table entry is deleted.

When the lease timer expires, the ACK type binding table entry is deleted.

---

### **15.1.3 DHCP SNOOPING specifies the physical port of the link server**

DHCP SNOOPING specifies the physical port of the link server, and DHCP messages can only be received on the specified port. If there are multiple DHCP servers in the network, the OFFER provided by the server from a non-specified port will be filtered, and the client cannot be assigned an IP address. The designated port is conducive to the unified allocation of IP addresses in the network, to avoid 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, the probability of abnormal network communication caused by private access to the server is reduced.

## **15.2 DHCP SNOOPING configuration**

### **15.2.1 DHCP SNOOPING default configuration**

DHCP SNOOPING is off by default.

The default timer interval of the REQ entry in the DHCP SNOOPING binding table is 10 seconds.

### **15.2.2 Turning DHCP SNOOPING on and off globally**

The DHCP SNOOPING of an interface can be turned on or off only after the DHCP SNOOPING is turned on globally. The DHCP SNOOPING of all interfaces must be turned off before the global DHCP SNOOPING can be turned off.

Turn on global DHCP SNOOPING

Switch#configure terminal

Switch(config)#ip dhcp snooping [IF\_LIST]

The parameter is the physical port list of the linked DHCP server to be bound. A total of four can be specified. The port list is separated by "," signs, such as: ge1/1,ge1/4,ge1/5

Turn off global DHCP SNOOPING

Switch#configure terminal  
Switch(config)#no ip dhcp snooping

### 15.2.3 Interface to turn DHCP SNOOPING on and off

Open a port of DHCP SNOOPING  
Switch#configure terminal  
Switch(config)#interface ge1/1  
Switch(config-ge1/1)#dhcp snooping

Turn off DHCP SNOOPING for a port  
Switch#configure terminal  
Switch(config)#interface ge1/1  
Switch(config-ge1/1)#no dhcp snooping

### 15.2.4 Interface opening and closing DHCP SNOOPING OPTION82

Open an interface for DHCP SNOOPING OPTION82  
Switch#configure terminal  
Switch(config)#interface ge1/1  
Switch(config-ge1/1)#dhcp snooping **option82**

Disable DHCP SNOOPING OPTION82 of a port  
Switch#configure terminal  
Switch(config)#interface ge1/1  
Switch(config-ge1/1)#no dhcp snooping **option82**

Configure the circuit-id of the DHCP SNOOPING OPTION82 of a port  
Switch#configure terminal  
Switch(config)#interface ge1/1  
Switch(config-ge1/1)# dhcp snooping option82 circuit-id vlan111

Delete the circuit-id of DHCP SNOOPING OPTION82 of a port  
Switch#configure terminal

|

---

```
Switch(config)#interface ge1/1
Switch(config-ge1/1)# no dhcp snooping option82 circuit-id
```

## 15.2.5 Display information

Display DHCP SNOOPING configuration information  
Switch#show dhcp snooping

Display DHCP SNOOPING binding table information  
Switch#show dhcp snooping binding-table

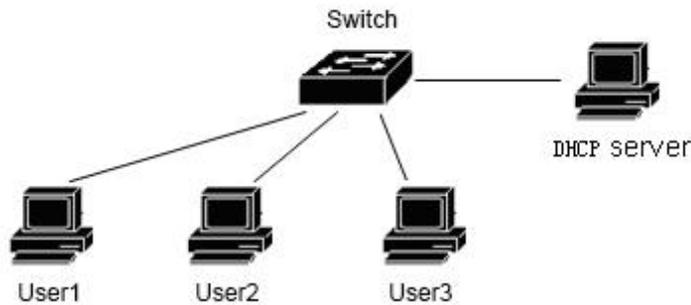
Display the current configuration of the system, including DHCP SNOOPING configuration.

```
Switch#show running-config
```

## 15.3 DHCP SNOOPING configuration example

### 15.3.1 configuration

Enable the DHCP SNOOPING function on the Layer 2 switch. User 1, User 2, and User 3 dynamically obtain IP addresses and network parameters through the DHCP server. The interface where user 1, user 2, and user 3 are enabled starts the DHCP SNOOPING OPTION82 function, the circuit-id is aaa, and the ARP information is dynamically bound to the interface.



```

Switch#configure terminal
Switch(config)#ip dhcp snooping ge1/5
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#dhcp snooping option82
Switch(config-ge1/1)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#dhcp snooping
Switch(config-ge1/2)#dhcp snooping option82
Switch(config-ge1/2)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#dhcp snooping
Switch(config-ge1/3)#dhcp snooping option82
Switch(config-ge1/3)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/3)#end
View dhcp snooping information
Switch#show dhcp snooping
DHCP Snooping is enabled globally
DHCP Server interface: ge1/5
Enable interface: ge1/1 ge1/2 ge1/3
Option 82 interface: ge1/1(Circuit ID: aaa) ge1/2(Circuit ID: aaa) ge1/3(Circuit

```

ID: aaa)

```

Switch#
Switch#show dhcp snooping binding-table

```

| IP | MAC | FLAG | PORT | LEASE |
|----|-----|------|------|-------|
|----|-----|------|------|-------|

|

---

|               |                   |     |       |          |
|---------------|-------------------|-----|-------|----------|
| 192.168.1.100 | 00:11:5b:34:42:ad | ACK | ge1/1 | 23:59:58 |
| 192.168.1.101 | 00:11:64:52:13:5d | ACK | ge1/2 | 23:50:01 |
| 192.168.1.102 | 00:11:80:4d:a2:46 | ACK | ge1/3 | 20:34:45 |

## 15.4DHCP SNOOPING configuration troubleshooting

If DHCP snooping configuration fails, it may be caused by the following reasons :

- 1、 System CFP resources are exhausted。
- 2、 If an interface is configured with ACL filtering function, DHCP SNOOPING fails to be enabled globally
- 3、 DHCP SNOOPING fails globally if an interface is configured with IP and MAC binding
- 4、 The current interface is configured with ACL filtering。
- 5、 The current interface is enabled with 802.1x anti-ARP spoofing。
- 6、 The configured interface is a Layer 3 interface or trunk interface。

---

# Chapter16 DHCP CLIENT configuration

---

## 16.1 DHCP CLIENT introduction

DHCP (Dynamic Host Configuration Protocol), based on the Client/Server working mode, the DHCP CLIENT function is that the switch's three-layer interface address can obtain the address and gateway through the DHCP server.

This section mainly includes the following :

- DHCP CLIENT configuration

## 16.2 DHCP CLIENT configuration

Enable the dhcp client function of interface vlan1

```
switch(config)#
```

```
Switch(config)#interface vlan1
```

```
Switch(config-vlan1)#dhcp client enable
```

Reacquire an IP address for interface vlan1

```
switch(config)#
```

```
Switch(config)#interface vlan1
```

```
Switch(config-vlan1)#dhcp client renew
```

Release the IP address of interface vlan1

```
switch(config)#
```

```
Switch(config)#interface vlan1
```

```
Switch(config-vlan1)#dhcp client release
```

---

## Chapter17 **DHCP RELAY** **configuration**

---

This chapter mainly includes the following :

- DHCP RELAY introduction
- DHCP RELAY configuration
- DHCP RELAY configuration example

---

## 17.1 DHCP RELAY introduction

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP. It dynamically configures the network environment for hosts on the network and is divided into server and client. The server side centrally manages IP network data and processes client requests, and dynamically configures the client's TCP/IP environment. When DHCP works, at least one server is on the network. It can listen to DHCP requests from hosts on the network and negotiate TCP/IP parameters. There are two ways of allocation: automatic and dynamic. Automatic mode, once the client obtains the IP address, it will be used permanently. Dynamic way, the IP address obtained by the client has a lease, and the IP needs to be released once the lease expires ; You can also renew the contract in advance, or rent another IP. Dynamic allocation can effectively solve the problem of insufficient actual IP.

The working process of DHCP :

If the client logs into the network for the first time, it does not have any IP information, and it will broadcast a Discover message with the source address 0.0.0.0 and the destination address 255.255.255.255. If the server does not respond, it will issue a Discover request four times at a certain interval.

After receiving the Discover, the server 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, the Offer that arrives first is selected and a Request message is broadcast to tell all servers that it has received the IP address provided by which server.

If the client finds that the IP has been used through ARP, it sends a Decline message to the server, rejects the Offer, and restarts the Discover process.

After receiving the Request message, the server sends an Ack message to the client to confirm that the lease takes effect.

If the client has already applied for a DHCP lease, it is generally unnecessary to use the Discover process. Before the lease expires, use the leased IP to send a request to the

server to renew the contract. The server will try to let the client use the original IP. If there is no problem, the server responds with an Ack message to confirm. If the IP is already used by other clients, the server responds to the Nack message and rejects the renewal request.

The client can use the Release message to actively cancel the lease.

The workstation issues a Request when it is turned on ; Request will be sent again when the lease is halfway, and the IP can still be used without confirmation ; Requests will also be sent when the lease is 3/4. If there is no confirmation at this time, the IP will no longer be available.

Discover messages are published by broadcast, and can only be in the same network segment, and routers will not spread broadcast messages. When the server and the client are not on the same network segment, the client has not yet obtained the IP environment settings and does not know the location of the router, then the Discover message cannot reach the server. To solve this problem, the DHCP relay function can be used to allow the router to relay DHCP protocol packets so that DHCP can operate across network segments.

## 17.2 DHCP RELAY configuration

The DHCP relay function is mostly related to the interface, and it realizes the forwarding of DHCP protocol packets across network segments, and the related configuration is performed in the interface mode.

DHCP-relay configuration includes :

Enable the DHCP-relay function of the interface

### 17.2.1 Enable the DHCP-relay function of the interface

mode : Interface configuration mode

command : dhcp relay <ip-address-1> [ip-address-2]

Open the dhcp relay protocol on the interface

command : no dhcp relay

Close the dhcp relay protocol on the interface

Default: do not open dhcp relay protocol.

## 17.2.2 Display information

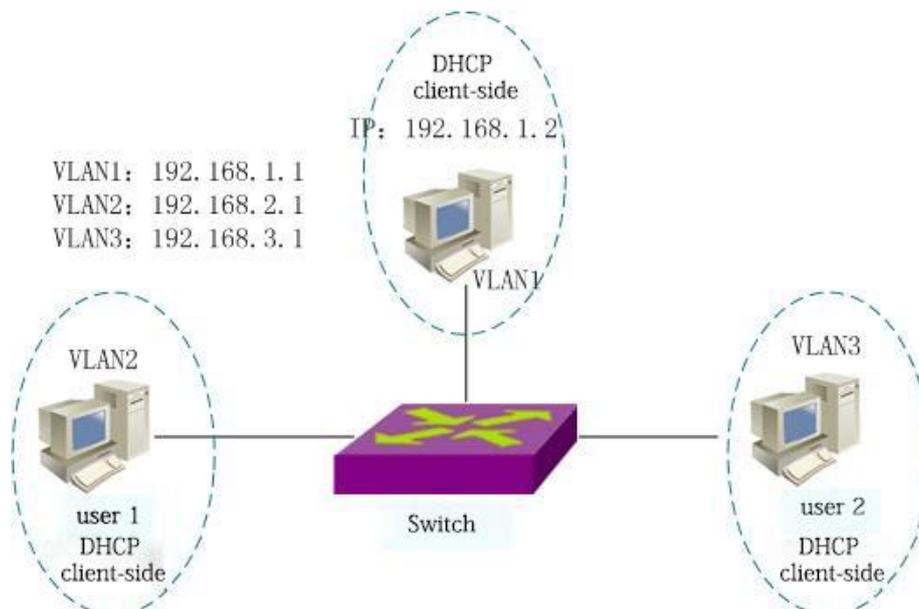
Display DHCP relay configuration information

```
Switch#show dhcp relay
```

## 17.3 DHCP RELAY configuration example

### (1) configuration

The switch needs to be configured for DHCP relay forwarding, so that the switch can route and forward the DHCP requests of user 1 and user 2 and the DHCP server's DHCP reply confirmation information. Allows user 1 and user 2 to obtain legal IP addresses through DHCP servers on different network segments to access the network.



```
Switch>en
```

```
Switch# configure terminal
```

```
Switch(config)# vlan database
```

```
Switch(config-vlan)#vlan 2
```

```
Switch(config-vlan)#vlan 3
```

```
Switch(config-vlan)#exit
```

|

---

```
Switch(config)#ip interface vlan 2
Switch(config)#ip interface vlan 3
Switch(config)#int ge1/2
Switch(config-ge1/2)#sw access vlan 2
Switch(config-ge1/2)#int ge1/3
Switch(config-ge1/3)#sw access vlan 3
Switch(config-ge1/3)# interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#dhcp relay 192.168.1.2
Switch(config-vlan2)#interface vlan3
Switch(config-vlan3)#ip address 192.168.3.1/24
Switch(config-vlan3)#dhcp relay 192.168.1.2
```

## **(2) verification**

```
show running-config      Display configuration commands
show dhcp relay          Display dhcp relay configuration information
```

---

## Chapter18 **DHCP SERVER** **configuration**

---

This chapter mainly includes the following :

- DHCP SERVER introduction
- DHCP SERVER configuration
- DHCP SERVER configuration example

---

## 18.1 DHCP SERVER introduction

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP. It dynamically configures the network environment for hosts on the network and is divided into server and client. The server side centrally manages IP network data and processes client requests, and dynamically configures the client's TCP/IP environment. When DHCP works, at least one server is on the network. It can listen to DHCP requests from hosts on the network and negotiate TCP/IP parameters. There are two ways of allocation: automatic and dynamic. Automatic way , Once the client obtains the IP address, the address is used permanently. Dynamic way , The IP address obtained by the client has a lease, and the IP needs to be released once the lease expires ; You can also renew the contract in advance, or rent another IP. Dynamic allocation can effectively solve the problem of insufficient actual IP.

The working process of DHCP :

If the client logs into the network for the first time, it does not have any IP information, and it will broadcast a Discover message with the source address 0.0.0.0 and the destination address 255.255.255.255. If the server does not respond, it will issue a Discover request four times at a certain interval.

After receiving the Discover, the server 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, the Offer that arrives first is selected and a Request message is broadcast to tell all servers that it has received the IP address provided by which server.

If the client finds that the IP has been used through ARP, it sends a Decline message to the server, rejects the Offer, and restarts the Discover process.

After receiving the Request message, the server sends an Ack message to the client to confirm that the lease takes effect.

If the client has already applied for a DHCP lease, it is generally unnecessary to use the Discover process.

Before the lease expires, use the leased IP to send a request to the server to renew the contract. The server will try to let the client use the original IP. If there is no problem,

|

---

the server responds with an Ack message to confirm. If the IP is already used by other clients, the server responds to the Nack message and rejects the renewal request.

The client can use the Release message to actively cancel the lease.

The workstation issues a Request when it is turned on; Request will be sent again at half of the lease, and the IP can still be used without confirmation; Requests will also be sent when the lease is 3/4. If there is no confirmation at this time, the IP will no longer be available.

The DHCP server protocol module receives Discover, Request, Decline, and Release messages, and is used to dynamically assign IP addresses to clients in the network, and maintain its own address pool information and assigned client information.

## 18.2 DHCP SERVER configuration

The DHCP server function needs to be configured in global mode, interface mode, and address pool mode, including commands such as startup commands, address pool configuration, global settings, and adjustable switches.

The configuration of the DHCP server includes :

- Start global DHCP server function
- Start interface to receive DHCP server message
- Configure address pool
- Configure address pool range
- Configure the address pool subnet mask
- Configure address pool lease
- Configure the default gateway of the address pool
- Configure address pool DNS server
- Manually exclude addresses in the address pool

### 18.2.1 Enable global DHCP server function

mode : Global configuration mode

command : ip dhcp server

enable global dhcp server protocol

command : no ip dhcp server

Disable global dhcp server protocol

default : Do not open the dhcp server protocol; use this command to start the dhcp server protocol.

## 18.2.2 Start interface to receive DHCP server message

mode : interface configuration mode

command : dhcp server listen

Interface starts to receive dhcp server protocol packets

command : no dhcp server listen

The interface shuts down and does not receive dhcp server protocol packets

default :The interface does not start and cannot receive dhcp server protocol packets.

## 18.2.3 Configure address pool

mode : global configuration mode

command : dhcp server pool <pool-name>

Create an address pool and enter address pool mode

command : no dhcp server pool <pool-name>

Delete the specified address pool

parameter : <pool-name>Address pool name , used to distinguish between different address pools.Up to 16 characters.

default : No address pool is configured.To configure an address pool, only create the address pool name, enter the address pool configuration mode, and do not configure the actual address.

## 18.2.4 Configure address pool range

mode : Address pool configuration mode

|

---

command : range <low-address> <high-address>

Configure address pool range

command : no range

Delete address pool range

parameter : <low-address>starting address of the address pool range, in dotted decimal format ;<high-address>End address of the address pool range , in dotted decimal format.

default : Do not configure the address pool range. When a range is configured in the address pool, each dynamically assignable address entry in the range in the address pool is created.

## 18.2.5 Configure the address pool subnet mask

mode : Address pool configuration mode

command : subnet-mask <address>

Configure the address pool subnet mask

parameter : <address> the mask address, in dotted decimal format, is a variable-length mask.。

default : 255.255.255.0The default is a 24-bit mask.

## 18.2.6 Configure address pool lease

mode : Address pool configuration mode

command : lease [<days> <hours> <minutes>|infinite]

Configure address pool lease

parameter : <days> is the number of days ,the range is 0-999 ;<hours> is the number of hours, the range is 0-23 ;<minutes> is the number of minutes ,the range is 0-59 ;all are integer numbers. Infinite is an unlimited lease.

default : lease is about 8 days.

---

## 18.2.7 Configure the default gateway of the address pool

mode : Address pool configuration mode

command : default-router <ip-address>

Configure the default gateway of the address pool

command : no default-router

Delete the default gateway of the address pool

parameter : <ip-address> the default gateway IP address, in dotted decimal format, should be on the same network segment as the address pool.

default : No default gateway is configured.

## 18.2.8 Configure the address pool DNS server

mode : Address pool configuration mode

command : dns-server <ip-address1> [ip-address2]

Configure the address pool DNS server

command : no dns-server

Delete the address pool DNS server

parameter :<ip-address1> and <ip-address2> are DNS server IP addresses, in dotted decimal format, up to two DNS servers can be configured, or one. If two units are configured, they should be entered in one command, instead of entering them in two. If entered twice, the DNS server IP address entered later overrides the previously configured DNS server address, regardless of whether one or two were previously configured.

Default: No DNS server is configured.

---

## 18.2.9 Configure to manually exclude addresses in the address pool

mode : Address pool configuration mode

command : exclude-address <ip-address>

Configure to manually exclude addresses in the address pool

command : exclude-address <low-address> <high-address>

Configure manual exclusion of address ranges

command : no exclude-address <ip-address>

Restore a manually excluded address

command : exclude-address <low-address> <high-address>

Configure manual exclusion of 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. <low-address> and <high-address> are the starting and ending IP addresses of the address range manually, in dotted decimal format, one command can exclude multiple consecutive available addresses in the address pool range, if there are already addresses in the range are manually exclude, just skip without any prompt. Manual exclusion is also possible. The address entry in the address pool range cannot be dynamically allocated.

Default: Manually exclude addresses is not configured.

## 18.2.10 OPTION82 configuration

mode : address pool configuration mode

command : option82 circuit-id <circuit-id>           Configure option82 circuit-id

parameter : < circuit-id > string, the maximum length is 64.

---

## 18.2.11 Clear the assigned address table entry

mode : EXEC configuration mode

command : clear dhcp server address {[ip-address] | [all]}

Delete an assigned address or all address entries.

## 18.2.12 Clear detected conflicting address entries

mode : EXEC configuration mode

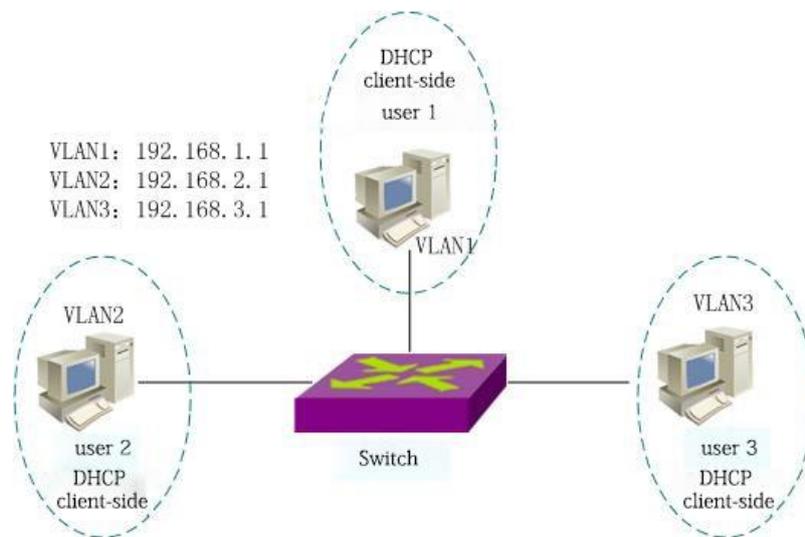
command : clear dhcp server address conflict {[ip-address] | [all]}

Delete addresses that are automatically excluded when a conflict is detected. You can delete all conflicting addresses. You can delete a single address that is automatically excluded due to a conflict.

## 18.3 DHCP SERVER configuration example

### (1) configuration

Configure corresponding address pools for clients in three different subnets of vlan1, vlan2, and vlan3, so that the switch acting as a DHCP server can allocate IP addresses of corresponding network segments to clients in these three subnets.



```

Switch>en
Switch# configure terminal
Switch(config)#ip dhcp server
Switch(config)# vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#exit
Switch(config)#ip interface vlan 2
Switch(config)#ip interface vlan 3
Switch(config)#int ge1/2
Switch(config-ge1/2)#sw access vlan 2
Switch(config-ge1/2)#int ge1/3
Switch(config-ge1/3)#sw access vlan 3
Switch(config-ge1/3)#interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#dhcp server listen
Switch(config-vlan2)#interface vlan3
Switch(config-vlan3)#ip address 192.168.3.1/24
Switch(config-vlan3)#dhcp server listen
Switch(config-vlan3)#interface vlan1
Switch(config-vlan1)#dhcp server listen
Switch(config)#dhcp server pool a
Switch(config-dhcp)#range 192.168.2.1 192.168.2.20
Switch(config-dhcp)#lease 2 0 0
Switch(config-dhcp)#default-router 192.168.2.1

```

|

---

```
Switch(config-dhcp)#dns-server 1.1.1.1 2.2.2.2
Switch(config-dhcp)#exclude-address 192.168.2.10
Switch(config-dhcp)#exit
Switch(config)# dhcp server pool b
Switch(config-dhcp)#range 192.168.3.2 192.168.3.20
Switch(config-dhcp)#default-router 192.168.3.1
Switch(config-dhcp)#exit
Switch(config)# dhcp server pool c
Switch(config-dhcp)#range 192.168.1.2 192.168.1.20
Switch(config-dhcp)#default-router 192.168.1.1
Switch(config-dhcp)#exit
```

## **(2) verification**

```
show running-config      show configuration command
show dhcp server         Display global configuration information
show dhcp server pool [pool-name] Display address pool configuration information ,
Can display a single address pool information.
show dhcp server address  Display the information of allocated address entries.
```

---

# Chapter19 ACL configuration

---

In an actual network, network access security is an issue that administrators are very concerned about. The switch supports ACL filtering to provide network access security. By configuring ACL rules, the switch filters incoming data streams according to these rules to achieve network access security.

This chapter describes how to configure ACL, mainly including the following :

- Introduction of ACL resource library
- Introduction to ACL filtering
- ACL resource library configuration
- ACL filtering configuration
- ACL configuration example

## 19.1 Introduction to ACL Resource Library

The ACL (Access list control) resource library is a collection of multiple sets of access rules. The ACL resource library does not have the function of controlling data forwarding, but is a set of rules with conflicting ordering. After the ACL resource library is referenced by applications, these applications control the forwarding of data according to the rules provided by the ACL resources. ACL can be applied to port access filtering, service access filtering and QoS, etc.

ACL resource library has standard IP rule group ( group numbers 1 ~ 99 , 1300 ~ 1999 ) , Extended IP Rule Group ( group numbers 100 ~ 199 , 2000 ~ 2699 ) , IP MAC group<group numbers 700~799> , ARP group (group numbers 1100~1199) ; Priority order of conflict rules is automatically sorted within each group of rules. When the user configures an ACL rule, the system will insert this rule to the corresponding position according to the sorting 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 multiple rules match at the

|

---

same time, the first rule that matches exactly takes effect ; This matching rule determines whether the packet is forwarded or dropped. The so-called perfect match is that the value of the field in the rule is exactly equal to the value of the corresponding field in the packet. Only if it matches a certain rule of ACL exactly, this rule will make corresponding deny or permit operation.

In the switch, the rules in the same group are automatically ordered. The automatic sorting of rules is relatively complicated. In the sorting process, the rules with a large range are ranked at the back, and the rules with a small range are ranked at the front. The size of the range is determined by the constraints of the rule ; The fewer the constraints of the rule, the larger the range of the rule matching, and the more the constraints of the rule, the smaller the range of the rule matching. The constraints of the rule are mainly reflected in the wildcard of the address and the number of non-address fields. Wildcard is a bit string. IP address is four bytes, MAC address is six bytes. "1" bits means no match , bits" 0' means match. The non-address field refers to the protocol type, IP protocol type, and protocol port. These fields also hide a wildcard. Their length is the byte length of the corresponding field, so the length of the same field is uniform, only need to count the number of fields. The more wildcard bits are "0", the more constraints.

The following uses port access filtering as an example to illustrate the necessity of rule ordering and the advantages of automatic ordering. If the user needs to reject the address forwarding with the source address 10.10.10.0/16 network segment and allow the address forwarding with the source address 192.168.1.0/24 network segment, you can configure the following two rules :

```
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
```

Hereinafter referred to as Rule 1 and Rule 2.

These two rules are in conflict; because the address of rule 1 is included in the address of rule 2, and one is deny and the other is permit ; According to the filtering principle of ACL, different orders have different results. If you want to achieve the above

requirements, the order of the above two rules must be : Rule 1 comes first, Rule 2 comes first. The switch automatically implements the above sorting function. No matter what order the user configures the above rules, the last order is rule 1 in front of rule 2. When a packet with a source address of 192.168.1.1 is forwarded, the first rule is compared first, and then the second rule is compared. Both rules match and the previous one takes effect (forwarding) ; If the source address is 10.10.10.1, only the first match, then discarded (not forwarded).

If there is no sorting, the user may now configure rule 2 first, then configure rule 1 ;

Rule 1 comes first, Rule 2 comes 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 previous rule 2 contains the following rule 1, the situation that may result is : Packets that match rule 1 exactly also match rule 2, rule 2 will take effect every time ; But can not meet the needs of the application.

In a switch, '0.0.255.255' is wildcard bits, bits '1' means no match is needed, and bits '0' means match. It can be seen from this that the wildcard bits of rule 2 are '0.0.255.255', which needs to match two bytes (16 bits) ; The wildcard bits in Rule 1 are '0 0.0.255' , Need to match three bytes (24 bits) ; So the rule 2's scope is bigger, so it's behind. In extended IP, sorting needs to consider more rule fields, such as IP protocol type, communication port, etc. Their ordering rules are the same, that is, the more the configuration limit, the smaller the "range" of the rule, and conversely, the larger the "range". The ordering of rules is implemented in the background, and user commands can only be displayed in the order of user configuration.

The filtering fields supported by ACL include source IP , destination IP , IP protocol type (like :TCP ,UDP ,OSPF) ,source port( like 161 ) ,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 ; like : A set of rules is referenced by port access filtering and service access filtering at the same time or by port access filtering of two ports at the same time.

---

## 19.2 Introduction to ACL filtering

ACL filtering is performed on the input port of the switch, and the data flow input to this port is matched by rules to realize port filtering. ACL filtering is processed by the line speed of the switch, and will not affect the forwarding efficiency of the data flow.

When a port of the switch is not configured with ACL filtering, all data flows input through this port will not be matched by rules, and can be forwarded through this port. When ACL filtering is configured on a port of the switch, all input data flows passing through the port will be matched by rules. If the action of the matched rule is permit, the data flow is allowed to be forwarded. If it is deny, the data stream is not allowed to be forwarded and discarded.

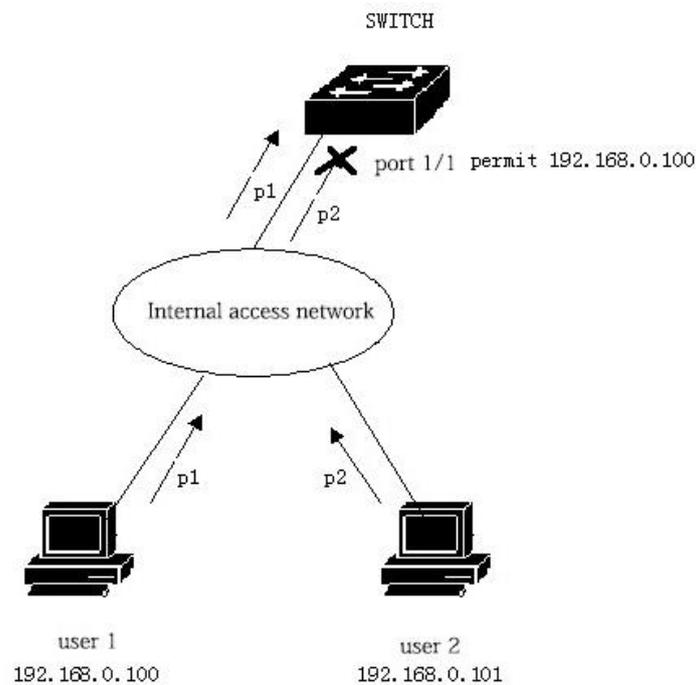
When configuring ACL filtering for a port, multiple ACL rule groups can be selected for a port. After the selection, the rules of the group are imported into the CFP of the port. If there are no rules that reject or allow all IP protocol packets in the group rules, the CFP is written. Will add a rule that rejects all IP protocols. When the rules of the ACL resource library change, the rules written in the CFP will also change automatically.

For example, there is only one rule in a set of rules : `access-list 1 permit 192.168.1.0 0.0.0.255` , By default, a rule that rejects all IP protocol packets will be hidden , There will actually be two rules imported into the port's CFP. During data flow filtering, only data flows with source addresses from 192.168.1.0 to 192.168.1.255 can be forwarded through this port, and all other data flows 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`. At this time, there is a rule that allows all IP protocol packets. At this time, there are no hidden rules. In fact, there will be two rules imported into the CFP of the port. During data flow filtering, only data flows with source addresses from 192.168.1.0 to 192.168.1.255 are filtered out, and all other data flows can be forwarded.

The following figure is an example of ACL filtering. The port 1/1 of the switch selects an ACL rule group 1. There is only one rule in this group of rules `access-list 1 permit 10.10.10.100`. Under port 1/1 of the switch, there are two users who want to access the network from this port. The IP address of user 1 is 10.10.10.100, and the IP address of user 2 is 10.10.10.101. Only user 1 can access the network through port 1/1 of the switch, and user 2 cannot access the network through port 1/1 of the switch. The data stream p1

from user 1 can be forwarded through the port 1/1 of the switch, while the data stream p2 from user 2 is discarded at port 1/1 of the switch.



When performing ACL filtering on multiple ports, you can select the same ACL rule group and use the same filtering rule.

Regardless of whether a set of rules or multiple sets of rules are referenced by a port, they will be sorted automatically, even if the sorting between the two sets of rules overlaps.

After a user references a set of rules, if the set of rules changes, the port that references the set of rules will automatically respond to the user's configuration; there is no need to reconfigure the port reference.

### 19.3 ACL resource library configuration

The switch has no rules by default.

The resource library in the switch supports four types of ACL rules : Standard IP rules ,Extended IP rules ,IP MAC group ,ARP group. The following are four types of rules to introduce ACL configuration.

|

---

Standard IP rules : Standard IP rules control the forwarding of data packets by source IP address.

Command form : `access-list <groupId> {deny | permit} <source>`

Parameter Description :

`groupId` : Access control list group number, standard IP ACL support from 1 to 99 groups or 1300 to 1999.

`deny/permit` : If there is an exact match, the packet is rejected or allowed to be forwarded.

`source` : There are three input methods for source IP :

1)A.B.C.D wildcard can control the IP address from a network segment ;

2)any equivalent to A.B.C.D 255.255.255.255

3)host A.B.C.D equivalent to A.B.C.D 0.0.0.0

wildcard : decide which bits need to match , '0'means need to match , '1'means no need to match.

Extended IP rules : Extended IP rules are extensions of standard IP rules. You can control the forwarding of data packets by source IP, destination IP, IP protocol type, and service port.

Command form : `access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>`

Parameter Description :

`groupId` : access control list group number , extended IP ACL support from 100 to 199 groups or 2000 to 2699.

`deny/permit` : If there is an exact match, the packet is rejected or allowed to be forwarded.

`protocol` : Protocol types on the IP layer , like : tcp , udp etc. You can also enter the corresponding number 6(tcp). If you do not need to control these protocols, you can enter ip or 0.

source : There are three input methods for source IP :

- 1) A.B.C.D wildcard can control the IP address from a network segment ;
- 2) any equivalent to A.B.C.D 255.255.255.255
- 3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

srcPort : Is for the case where the protocol is tcp or udp , can control the source port of the packet, input method can be some familiar port service names , like : www also can be a number , like 80.

destination : there are three input methods for the destination IP :

- 1) A.B.C.D wildcard can control the IP address from a network segment ;
- 2) any equivalent to A.B.C.D 255.255.255.255
- 3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

destPort: For the case where the protocol is tcp or udp, the destination port of the data packet can be controlled. The input method is the same as srcPort.

tcp-flag: When the protocol is tcp. You can control the tcp field matching of the data packet. The optional parameters are ack, fin, psh, rst, syn, and urg.

IP MAC rule: The IP MAC group can control the source and destination MAC addresses and source and destination IP addresses of IP packets.

Command form : access-list <groupid> {deny | permit} <src-mac> ip <src-ip> <dst-ip>

Parameter Description :

groupid: access control list group number, extended IP 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.

There are three ways to enter the MAC address :

- 1) HHHH.HHHH.HHHH wildcard can control the MAC address from a segment ;
- 2) any equivalent to HHHH.HHHH.HHHH FFFF.FFFF.FFFF.
- 3) host A.B.C.D equivalent to HHHH.HHHH.HHHH 0000.0000.0000

src-ip : source IP address.

|

---

dst-ip : destination IP address.

There are three input methods for IP address :

- 1) A.B.C.D wildcard can control the IP address from a network segment ;
- 2) any equivalent to A.B.C.D 255.255.255.255
- 3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

ARP rule : The ARP group can control the operation type of the ARP packet, the sender MAC and the sender IP.

Command form : 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 : means any|reply|request , any is not to control the type of arp packet , reply is a response packet that controls arp , request is a request packet that controls the arp package.

sender-mac: MAC address of the sender of ARP packets.

There are three ways to enter the MAC address :

- 1)HHHH.HHHH.HHHH wildcard can control the MAC address from a segment ;
- 2)any equivalent to HHHH.HHHH.HHHH FFFF.FFFF.FFFF
- 3)host A.B.C.D equivalent to HHHH.HHHH.HHHH 0000.0000.0000

sender-ip: IP address of the sender of the ARP packet.

There are three input methods for IP address :

- 1) A.B.C.D wildcard can control the IP address from a network segment ;
- 2) any equivalent to A.B.C.D 255.255.255.255
- 3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

List of other commands :

show access-list [groupId]

Displays the list of rules configured in the current ACL. If groupId is entered, the list of rules for the current group ; Otherwise, display a list of all rules.

no access-list <groupId>

Delete the specified rule list. all rules of groupId group.

## 19.4 ACL based on time period

The time period is used to describe a special time range. Users may have such needs : Some ACL rules need to take effect within a certain period of time, but they are not used for packet filtering in other time periods, which is commonly referred to as filtering by time period. At this time, the user can first configure one or more time periods, and then refer to the time period by the time period name under the corresponding rule. This rule only takes effect within the specified time period, thereby realizing the ACL based on the time period filter.

If the time period referenced by the rule is not configured, the system gives a prompt message and allows such a rule to be created successfully, but the rule cannot take effect immediately until the user configures the referenced time period and the system time is within the specified time range ACL rule To take effect.

The configuration of the time period has the following two situations :

(1)Configure relative time period:Take the form of a certain time of a certain day to a certain time of a certain day ;

(2)Configure absolute time period : It takes the form of a certain year, a certain month, a certain day and a certain time to a certain year, a certain month, a certain day and a certain time.

Configure ACL based on time period :

| command  | description  | CLI mode                        |
|--|--|---------------------------------|
| time-range WORD<br>cycle-time from <0-23><br><0-59> to <0-23> <0-59> | configure a relative time period<br>including only hour and minutes<br>for a time period | Global<br>configuration<br>mode |

|   |  |                                 |
|---|--|---------------------------------|
| time-range WORD<br>cycle-time days from<br><0-6> to <0-6>   | Configure a relative time period<br>including only week for a time<br>period                                   | Global<br>configuration<br>mode |
| time-range WORD<br>cycle-time from <0-23><br><0-59> to <0-23> <0-59><br>days from <0-6> to <0-6>                                  | Configure a relative time period<br>including hour, minutes and week<br>for a time period                      | Global<br>configuration<br>mode |
| time-range WORD<br>utter-time from<br><2000-2100> <1-12><br><1-31> <0-23> <0-59> to<br><2000-2100> <1-12><br><1-31> <0-23> <0-59> | configure an absolute time period<br>including year, month, date, hour<br>and minutes for a time period        | Global<br>configuration<br>mode |
| no time-range WORD<br>cycle-time  | Delete all relative time periods in a<br>certain time period   | Global<br>configuration<br>mode |
| no time-range WORD<br>utter-time  | Delete all absolute time periods in<br>a certain time period   | Global<br>configuration<br>mode |
| no time-range WORD  | Delete a certain time period<br>(including deleting all relative<br>time periods and absolute<br>time periods) | Global<br>configuration<br>mode |
| no time-range   | Delete all time periods  | Global<br>configuration<br>mode |
| show time-range WORD<br>cycle-time  | Display all relative time periods of<br>a certain time period  | Privileged<br>mode              |
| show time-range WORD<br>utter-time  | Display all absolute time periods<br>of a certain time period  | Privileged<br>mode              |
| show time-range WORD  | Display certain time period<br>(including all absolute time<br>periods and relative time periods)              | Privileged<br>mode              |
| show time-range   | Show all time periods  | Privileged<br>mode              |
| time-acl  | ACL rules are applied for a  | Global                          |

|   |   |                           |
|---|---|---------------------------|
| (<1-99> <100-199> <1300-1999> <2000-2699> <700-799> <1100-1199>)<br>time-range WORD                   | certain time periods, and are applied when ACL is applied to the interface                | configuration mode        |
| no time-acl<br>(<1-99> <100-199> <1300-1999> <2000-2699> <700-799> <1100-1199>)<br>time-range (WORD ) | Cancel the application of a certain acl rule to a certain time period or all time periods | Global configuration mode |
| show time-acl<br>(<1-99> <100-199> <1300-1999> <2000-2699> <700-799> <1100-1199>)<br>time-range       | Show all time periods for a certain time which ACL rules are applied                      | Privileged mode           |
| show time-acl all<br>time-range   | Display the time period during which all ACL rules are applied                            | Privileged mode           |

Need to be note :

- (1) Configure multiple relative time periods for a certain time period, the relationship between the relative time periods is OR, the system time is in any relative time period, and the time period is in the activated state;
- (2) Configure multiple absolute time periods for a certain time period, the relationship between the absolute time periods is OR, the system time is in any absolute time period, and the time period is activated ;
- (3) If a certain time period is configured with a relative time period and an absolute time period at the same time, the relative time period and the absolute time period are related, and the system time is only active in the relative time period and the absolute time period at the same time ;
- (4) Up to 256 time periods can be defined ; Up to 256 relative time periods and absolute time periods can be configured for a time period ; An acl rule can apply up to 256 time periods ; When the ACL rule associated with the time period is applied to the interface, the time period becomes effective.

---

## 19.5 ACL filtering configuration

By default, all ports of the switch are not ACL filtered.

Command list :

```
access-group <groupId>
```

Mode: Layer 2 interface configuration mode

parameters :

groupId : ACL group number bound to the port

Function: Configure ACL port filtering.

Note: If the above command configuration fails or is invalid, there may be the following reasons:

There are too many rules in the ACL group or the hardware resources are exhausted or occupied by other applications.

Display ACL port filtering configuration

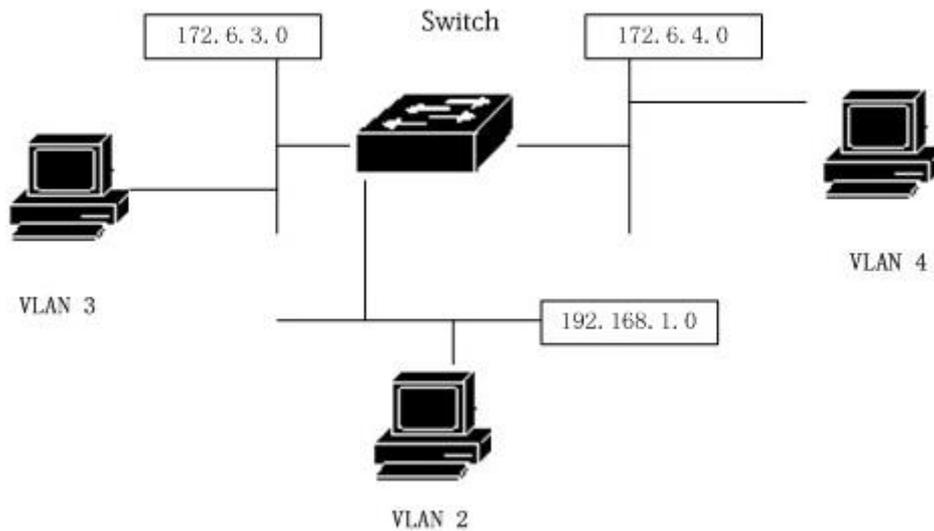
```
show access-group
```

Delete the configuration related to the current port and ACL port filtering

```
no acl- group <groupId>
```

## 19.6 ACL configuration example

One switch is connected to three subnets, ACL is designed, and the blocking source address is 192.168.1.0 network address. It allows traffic from other network addresses to pass through. The 192.168.1.0 network segment is connected to the 1/1 port of the switch.



Configure as follows on the switch :

```

Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3
Switch(config)#interface vlan3
Switch(config-vlan2)#ip add 172.16.3.1/24
Switch(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Switch(config)#access-list 10 permit any
Switch(config)#interface ge1/1
Switch(config-ge1/1)#access-group 10
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#access-group 10

```

---

## 19.7 ACL configuration troubleshooting

If ACL configuration fails, there may be the following reasons :

- 1、 Before configuring the access control list, make sure that all IPs are connected, and then add the access control list. This access control list is blocking the IP data flow of the source segment 192.168.1.0 through the switch. Pay attention to the writing of subnet reverse code. Use the show access-list command to list the access control list to view, be sure to pay attention to the source address and destination address do not write reverse. Then check the access control list. And the default access control list has an implicit deny any statement at the end. If you want to let all others 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、 DHCP SNOOPING protocol is enabled on the current interface.
- 4、 System CFP resources are exhausted.

---

## Chapter20 TCP/IP basic configuration

---

For a layer 2 switch with network management function, it is necessary to provide basic network configuration for the TCP/IP protocol to achieve communication with other devices.

This chapter mainly includes the following :

- Configure VLAN interface
- ARP configuration
- Configure static routing
- IP routing configuration example

---

## 20.1 Configure VLAN interface

In the switch, each layer 3 interface is attached to a certain VLAN, so the layer 3 interface is also called a VLAN interface. The creation and deletion of VLAN interfaces are done manually. Up to 4094 VLANs can be divided on the switch, but only up to 32 subnets can be established. The creation of the subnet interface can be created according to the needs of the user; the subnet interface can be manually deleted by the user, or can be deleted as the VLAN where the subnet is located is deleted.

Each VLAN interface has a name. The name of the VLAN interface is the string "vlan" followed by the VLAN ID number. For example, the name of the layer 3 interface of VLAN 1 is "vlan1", and the name of the layer 3 interface of VLAN 4094 is "vlan4094"

Like ports, VLAN interfaces also have management status and link status. At present, the switch does not provide the configuration of the management status of the VLAN interface. As long as the VLAN interface is created, the management status of the VLAN interface is always UP. The link status of the VLAN interface is related to the port included in the VLAN corresponding to the interface. As long as the link status of a port in the VLAN is RUNNING, the link status of the VLAN interface is RUNNING. If all the ports in the VLAN are If it is not RUNNING, the link status of the VLAN interface is not RUNNING.

You can configure an IP address on the VLAN interface and specify the network prefix of the network segment connected to this interface (which can be converted to a netmask). Currently, the switch only supports one IP address on one VLAN interface. Before configuring an IP address, users need to create a VLAN and add related ports to the VLAN. By default, the switch has a VLAN1 interface, and the IP address 10.10.10.1/24 is set on this interface. You can also modify the IP address of the VLAN1 interface. Interfaces of VLANs other than VLAN 1 have no IP address set by default.

The commands to configure the IP address of the VLAN interface are as follows :

| command                    | description             | CLI mode                  |
|----------------------------|-------------------------|---------------------------|
| Ip interface vlan <2-4094> | Create a VLAN interface | Global configuration mode |

|                                  |   |                              |
|----------------------------------|---|------------------------------|
| No ip interface vlan<br><2-4094> | Delete a VLAN interface   | Global configuration mode    |
| ip address <ip-prefix>           | Set the IP address on the VLAN interface. The parameters include the IP address of the interface and the network prefix of the connected network segment. If the IP address originally exists on the VLAN interface, delete the original IP address first, and then set the specified IP address. The format of the parameter is A.B.C.D/M. | Interface configuration mode |
| no ip address [ip-prefix]        | Delete the IP address of the VLAN interface. If a parameter is specified, the parameter must be the same as the parameter given during setup, otherwise this command is invalid. The format of the parameter is A.B.C.D/M.  | Interface configuration mode |

The commands to view the VLAN interface are as follows :

| command                  | description  | CLI mode                         |
|--------------------------|--|----------------------------------|
| show interface [if-name] | View the 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 parameter is specified, the information of all ports | Normal mode ,<br>Privileged mode |

|                     |   |                 |
|---------------------|---|-----------------|
|                     | and VLAN interfaces is checked.   |                 |
| show running-config | View the current configuration of the system, you can view the configuration of the VLAN interface. | Privileged mode |

For example :

Configure the subnet 193.1.1.0 on the VLAN3 interface, the subnet prefix is 24 (that is, the mask is 255.255.255.0), the IP address of the interface is 193.1.1.1, and view the information of the VLAN3 interface. The command is as follows :

```
switch(config)#interface vlan3
switch(config-vlan3)#ip address 193.1.1.1/24
switch(config-vlan3)#end
switch#show interface vlan3
```

## 20.2 ARP configuration

The ARP (Address Resolution Protocol) protocol is a protocol for mapping IP addresses to corresponding MAC addresses. When the source sends the Ethernet data frame to the destination in the same VLAN, the destination is determined based on the 48-bit Ethernet MAC address, and the destination determines whether it needs to receive this data based on the destination MAC address of the packet package.

Assume that hosts A and B on two adjacent network segments communicate through the switch. Before sending data to host B, host A first sends an ARP request message to the interface of the switch directly connected to host A, and sends the data after receiving an ARP reply. Packet to this interface. After receiving the data packet, the switch first broadcasts an ARP request message to host B. After receiving the ARP response message from host B, it sends the data packet to host B.

There is an ARP cache on the switch, called the ARP table, which stores the mapping records of IP addresses to MAC addresses in directly connected networks. Each entry in the ARP table has a survival time. The default is 20 minutes. When the switch does not receive an ARP request or response packet for the IP address during the lifetime, the ARP entry corresponding to the IP address will be deleted.

---

This section includes the following :

- Configure static ARP
- Configure ARP binding
- View ARP information

## 20.2.1 Configure static ARP

There are two different ARP entries in the ARP table, one is static ARP and the other is dynamic ARP. Static ARP is an ARP entry configured by the user through commands. The system will not automatically refresh and delete it. You need to manually complete it. Dynamic ARP is ARP that the system learns automatically according to the received ARP request or response packet. The system automatically creates and deletes, updates and maintains in real time, without user intervention, but users can manually delete dynamic ARP entries.

The switch is not configured with static ARP entries by default. It should be noted that when a VLAN interface is deleted or the IP of the subnet segment of the interface changes, the static and dynamic ARP entries in the original subnet segment are deleted. The commands for configuring static ARP are as follows:

| command                           | description   | CLI mode                  |
|-----------------------------------|---|---------------------------|
| arp <ip-address><br><mac-address> | Configure static ARP entries.<br>The first parameter is the IP address. The IP address must be within a subnet segment.<br>The second parameter is the MAC address. The MAC address must be a unicast MAC address. The format of the MAC address is HHHH.HHHH.HHHH, such as 0010.5cb1.7825. | Global configuration mode |

|                     |  |                           |
|---------------------|--|---------------------------|
| no arp <ip-address> | Delete ARP entries. Including deleting an IP ARP entry | Global configuration mode |
|---------------------|--|---------------------------|

## 20.2.2 View ARP information

The command to view ARP information is as follows :

| command             | description   | CLI mode                         |
|---------------------|---|----------------------------------|
| show arp            | View the ARP entry information in the ARP table, including all ARP entries,       | Normal mode ,<br>Privileged mode |
| show running-config | View the current configuration of the system, you can view the ARP configuration. | Privileged mode                  |

## 20.3 Configure static routing

A static route is a route defined by the user that allows a data packet to pass from a source address to a destination address through a specified path. You can configure a static route as the default route to send packets that cannot be routed to the default gateway.

The static route is manually configured by the administrator. It is suitable for networks with relatively simple networking structure. The administrator only needs to configure static routes to make the switch work normally. Static routes will not consume valuable network bandwidth because there will be no route updates.

The default route is also a static route. Simply put, the default route is the route that is used only when no matching route entry is found. That is, the default route is used only when there is no suitable route. In the routing table, the default route appears as a route to

the network 0.0.0.0/0 (with a mask of 0.0.0.0). If the destination of the packet is not in the routing table and there is no default route in the routing table, the packet will be discarded and an ICMP packet will be returned to the source indicating the destination address or network unreachable information. The default route is very useful in the network. In a typical network with hundreds of switches, running a dynamic routing protocol may consume a large amount of bandwidth resources. Using the default route can save the time occupied by routing and the bandwidth resources occupied by packet forwarding. Can meet the needs of a large number of users to communicate simultaneously to a certain extent.

The switch can be configured with multiple static routes to the same destination, but only one of the routes is activated for actual data forwarding. The switch is not configured with a static route by default.

The commands for configuring static routes are as follows :

| command  | description   | CLI mode                  |
|--|---|---------------------------|
| ip route <ip-prefix><br><nexthop-address>                    | Set up a static route. The first parameter specifies the network segment IP and network prefix length, and the second parameter specifies the next hop IP address.  | Global configuration mode |
| ip route <ip-address><br><mask-address><br><nexthop-address> | The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the IP address of the next hop.                    | Global configuration mode |
| no ip route <ip-prefix><br>[nexthop-address]                 | Delete the static route. The first parameter specifies the network segment IP and network prefix length, and the second parameter specifies the next hop IP address. If there is no second parameter, all routes matching the specified network segment will be deleted. If | Global configuration mode |

|   |   |                           |
|---|---|---------------------------|
|   | there is a second parameter, delete the route that matches both the specified network segment and the next hop.   |                           |
| no ip route <ip-address><br><mask-address><br>[nexthop-address] | The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the IP address of the next hop. If there is no third parameter, all routes matching the specified network segment will be deleted. If there is a third parameter, delete the route that matches both the specified network segment and the next hop. | Global configuration mode |

The command to view the route is as follows :

| command                                   | description  | CLI mode                     |
|---|--|------------------------------|
| show ip route [<ip-address>   <ip-prefix> | View the information of the activated route, you can choose to view all routes, a route, a route of a network segment, and a static route. | Normal mode, Privileged mode |
| show ip route database                    | View all routing information (including activated and inactive routes), you can choose to view all routes.                                 | Normal mode, Privileged mode |

|                     |   |                 |
|---------------------|---|-----------------|
| show running-config | View the current configuration of the system, you can view the configuration of the static route. | Privileged mode |
|---------------------|---|-----------------|

For 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 Switch(config)#ip route 200.1.1.0/24 10.1.1.2

Delete the static route whose destination IP address is 200.1.1.0, subnet mask is 255.255.255.0, and next hop is 10.1.1.2.

The configuration command is :

Switch(config)#no ip route 200.1.1.0/24

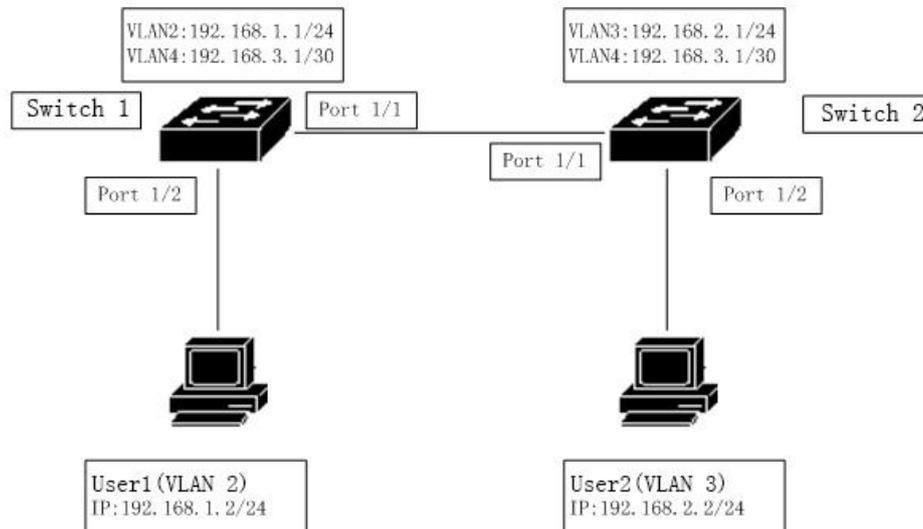
Or Switch(config)#no ip route 200.1.1.0/24 10.1.1.2

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

---

## 20.4 TCP/IP Basic configuration example



In the figure, switch 1 is a layer 2 switch, and switch 2 is a layer 3 switch.

### 20.4.1 Layer 3 interface

Configure the Layer 3 interface corresponding to VLAN 2 on Switch 1, and assign an IP address of 192.168.1.1/24.

The configuration is as follows :

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switch access vlan 2
Switch(config)#ip interface vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
```

Verification: User 1 can ping the IP address of the Layer 3 interface corresponding to VLAN 2 of switch 1.

---

## 20.4.2 Static routing

To access switch 1, user 2 must access switch 1 through the routing function of switch 2.

Switch 1 is configured as follows :

```
Switch#config t
Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
```

Switch 2 is configured as follows :

```
Switch#config t
Switch(config)#ip route 192.168.1.0/24 192.168.3.1
```

Verification: User 2 can ping General Switch 1.

## 20.4.3 ARP

Configure static ARP for user 1 to allow only user 1 to access from VLAN 2. Assume that the MAC address of user 1 is 00:00:00:00:00:01.

Switch 1 is configured as follows :

```
Switch#config t
Switch(config)#arp 192.168.1.2 0000.0000.0001
```

Verification: User 1 can ping the IP address of the Layer 3 interface corresponding to VLAN 2 of switch 1.

---

# Chapter21 **SNMP** **configuration**

---

The switch provides SNMP for remote management of the switch. This chapter describes how to configure SNMP, mainly including the following :

This chapter mainly includes the following :

- SNMP introduction
- SNMP configuration
- SNMP configuration example

---

## 21.1 SNMP introduction

SNMP is a simple network management protocol, is currently the most widely used network management protocol, it has five major 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).

There are four major elements of the SNMP network management protocol: management workstation, management agent, management information base, and network management protocol. The management agent is on the switch, which is the server end of the management station to access the switch. The information of the management station to access the network management agent is organized in the form of MIB to form a management information database.

SNMP has three major operations: GET operation, SET operation, TRAP operation. The GET operation enables the management station to obtain the value of the object in the agent. SET operation enables the management station to set the value of the object in the agent. TRAP operation enables agents to notify the management station of events.

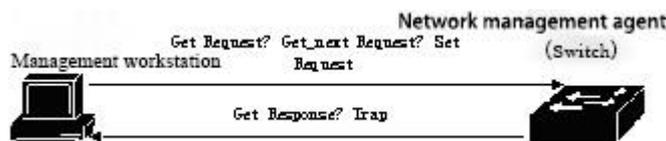
TRAP messages are actively sent to the management station when an event occurs on the switch. These messages include cold start, hot start, port link up and link down, common body name authentication failure, STP state switching, etc.

At present, there are three versions of SNMP: SNMPV1, SNMPV2, and SNMPV3. The later version is an upgraded version of the front, with enhanced functions and improved security. The switch supports all three SNMP versions, and can parse the SNMP protocol packages of the three versions. When sending TRAP messages, you can use any of SNMPV1, SNMPV2 and SNMPV3 to send.

The switch supports RFC, BRIDGE and private MIB objects, and the switch can be fully managed through SNMP. The following lists some MIBs supported by the switch: RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2573, RFC 2574, RFC 2575, RFC 2674 and other common MIBs.

The figure is an example of the SNMP protocol interaction between the management

station and the management agent. The management station can access the switch management agent by sending SNMP messages of Get Request, GetNext Request, GetBulk Request, and Set Request to obtain or set the value of the MIB object of the switch. The switch management agent returns the SNMP message of Get Response to the management station. When some events occur on the switch, the management agent of the switch actively sends SNMP TRAP messages to the management station.



SNMP protocol interaction between management station and management agent

## 21.2 SNMP configuration

The SNMP configuration includes the community configuration of the switch, the TRAP workstation, and the configuration of the snmp system information. The switch has a read-only community by default, the community name is public, and the switch can be configured with up to 8 communities. The switch does not configure TRAP workstations by default.

SNMP commands are as follows :

| command                                      | description  | CLI mode                  |
|--|--|---------------------------|
| snmp community<br><community-name> {ro   rw} | Configure the community name to access the NMS. This is an interactive command. During configuration, the user can enter the name of the created community and read/write permissions according to the prompt. | Global configuration mode |
| no snmp community<br><community-name>        | Delete the specified SNMP community name.  | Global configuration mode |

|  |   |                             |
|--|---|-----------------------------|
| snmp trap <notify-name><br>host <ipaddress> version {1<br>  2c   3}            | Add or modify the sending destination of snmp trap. This is an interactive command. The notify name is unique. If you modify the existing name, you can modify the trap to send the target item. host is the destination address to send trap; version is sent by snmpV1, snmpV2c or snmpV3. This command configures the target port as 162 by default. | Global configuration mode   |
| no snmp trap <notify-name>   | Delete the specified SNMP trap.   | Global configuration mode   |
| snmp system information<br><contact   location   name><br><information-string> | Configure system information. Configurable system information includes: contact, location and name.   | Global configuration mode   |
| no snmp system information<br><contact   location   name >                     | Delete a system configuration information.  | Global configuration mode   |
| show snmp community  | Display all current public body names and corresponding read and write permission information.  | Normal mode/privileged mode |
| show snmp trap   | Display all current trap names and the target IP address and version information sent by the corresponding trap.  | Normal mode/privileged mode |
| show snmp system information   | Displays the system information set by SNMP.  | Normal mode/privileged mode |

|



|  |  |      |
|--|--|------|
|  |  | mode |
|--|--|------|

## 21.3 SNMP configuration example

### 21.3.1 configuration

Configure a community name named "private" to operate with read and write permissions.

Configure an SNMP trap named test and send the destination IP to 10.10.10.10; the SNMP version used is 1.

The specific content of the contact to configure the system is :

E-mail:networks@acb.com。

The specific content of the location of the configuration system is : Shenzhen。

The specific content of the configuration system name is : switch。

The configuration of the switch is as follows :

```
Switch#config t
Switch(config)#snmp community private rw
Switch(config)#snmp system information contact E-mail:networks@abc.com
Switch(config)#snmp system information location Shenzhen
Switch(config)#snmp system information name switch
```

---

# Chapter22 RMON configuration

---

This chapter mainly includes the following :

- RMON introduction
- RMON configuration
- RMON configuration example

## 22.1 RMON introduction

RMON (Remote Monitoring, remote network monitoring) is a standard monitoring specification, mainly used to monitor the data traffic in a network segment or even the entire network, and is one of the widely used network management standards. The RMON specification is extended from the SNMP MIB, so it is also a MIB and the most important enhancement to the MIB II standard. RMON makes SNMP more effective and proactive to monitor remote devices.

The RMON monitoring system consists of two parts: a detector (agent or monitor) and a management station. RMON agents store network information in RMON MIB, and they are directly implanted into network devices (such as routers, switches, etc.). The management station uses SNMP to obtain RMON data information.

This device supports the 4 most commonly used groups in RMON :

(1)Statistics (statistics): provides statistical data for each interface, most of which are counters, recording the information collected by the monitor from the interface.

(2) History: save the data sampled on the specified interface at fixed intervals.

(3)Alarm group (alarm): Samples the specified data of all interfaces at a fixed time interval, and compares with the set threshold, triggers the corresponding event when the conditions are met.

(4) Event group (event): set the event, you can choose to record logs or send Trap.

---

## 22.2 RMON configuration

RMON command includes 4 groups of configuration, view configuration and view data :

| command   | description   | CLI mode                |
|---|---|-------------------------|
| rmon statistics <1-100> (owner WORD)                                | Enable the configuration of the statistical group with the specified serial number for this port. This is an interactive command. The configuration is that the user can input the serial number and owner according to the prompt, and the owner is optional (the same below). The serial number is the number configured by the statistics group, and the value ranges from 1 to 100.   | Port configuration mode |
| no rmon statistics <1-100>  | Cancel the configuration of the statistical group with the specified serial number.   | Port configuration mode |
| rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD) | It is an interactive command to configure the history group parameter of specified serial number for this port. The configuration user can enter the serial number, number of request buckets, time interval and owner according to the prompt. The serial number is the configuration number of the historical group, and the value range is 1 to 100; the number of request buckets is the maximum number of saved data, the value range is 1 to 100; | Port configuration mode |

|   |  |                           |
|---|--|---------------------------|
|   | the sampling interval is in seconds, and the value range is 1 to 3600.   |                           |
| no rmon history <1-100>   | Cancel the configuration of the historical group with the specified serial number.   | Port configuration mode   |
| rmon alarm <1-60> WORD<br><1-3600> (absolute delta)<br>rising-threshold <1-2147483647><br><1-60> falling-threshold<br><1-2147483647> <1-60> (owner WORD ) | Configure the alarm group parameters of the specified serial number. This is an interactive command. The configuration user can enter the serial number, monitoring object, time interval, comparison method, upper limit threshold, upper limit event serial number, lower limit threshold, lower limit time piece serial number and owner according to the prompt. The serial number is the number of the alarm group configuration, the value range is 1 to 60; the monitoring object is the OID of a MIB node, the sampling interval is in seconds, and the value range is 1 to 3600; the comparison mode can be selected absolute or delta, respectively Represents the absolute value (the value of each sampling) and the relative value (the increment of each sampling relative to the previous sampling); the upper and lower threshold values range from 1 to 2147483647; the event must be configured in advance, and the number value range is 1 to 60. | Global configuration mode |
| no rmon alarm <1-60>  | Cancel the configuration of  | Global                    |

|  |  |                           |
|--|--|---------------------------|
|  | the alarm group with the specified serial number.  | configuration mode        |
| rmon event <1-60> (log log-trap WORD none trap WORD) (description WORD ) (owner WORD ) | It is an interactive command to configure the event group parameters of the specified serial number. The configuration user can input the serial number, event type, community name, description and owner according to the prompt. The sequence number is the number of the event group configuration, and the value range is 1 to 60; the event type can be selected from log (record log), log-trap (record log and send Trap), none (no action) and trap (issue Trap), When selecting log-trap or trap, you must also specify the community name (the community name configuration is ignored in this device). | Global configuration mode |
| no rmon event <1-60>   | Cancel the configuration of the event group with the specified serial number.  | Global configuration mode |
| show rmon (statistics history-control alarm event) config                              | View RMON configuration information, this is an interactive command. The configuration user can input the viewing object according to the prompt.  | 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 historical group data, the configuration user must enter the interface name.  | Global configuration mode |

---

## 22.3 RMON configuration example

Enable statistics group configuration on port ge1/1, serial number is 10, and owner is tereco.

Enable historical group data collection on port ge1/8, serial number 2, save up to 80 data, sampling interval is 1 minute, no owner.

Configure the event with sequence number 1 to record logs without owner.

Configure the event with sequence number 3, send Trap, the community name is public, and there is no owner.

Enable the alarm group with sequence number 5 to monitor the number of bytes received on each port. When the number of bytes per half minute is greater than 1000, a Trap alarm is issued, and when it is less than 10, a log is recorded. No owner.

The switch configuration is as follows :

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#rmon statistics 10 owner tereco
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/8
Switch(config-ge1/8)#rmon history 2 buckets 80 interval 60
Switch(config-ge1/8)#exit
Switch(config)#rmon event 1 log
Switch(config)#rmon event 3 trap public
Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3
falling-threshold 10 1
```

---

# Chapter23 Cluster configuration

---

The switch provides a cluster management function, which can realize a group of network devices managed by a single device. This chapter describes how to configure cluster management, mainly including the following :

- Introduction to cluster management
- Configuration management equipment
- Configure member devices
- Cluster management display and maintenance
- Typical configuration examples of cluster management

## 23.1 Introduction to cluster management

### 23.1.1 Cluster definition

A cluster is a collection of network devices that can be managed as a single device. The purpose of cluster management: to solve the centralized management of a large number of scattered network devices.

Cluster advantages: save public network IP addresses; simplify configuration management tasks. The network administrator only needs to configure the public network IP address on one switch in the cluster to manage and maintain the other switches in the cluster.

---

The switch that configures the public network IP address and performs management functions is the command switch, and the other managed switches are member switches. The command switch and the member switches form a "cluster".

The cluster configures and manages the switches inside the cluster through the following three protocols.

- NDP ( Neighbor Discovery Protocol )
- NTDP ( Neighbor Topology Discovery Protocol )
- Cluster ( Cluster Management Protocol )

The working process of the cluster includes 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 cluster is established. The working principle is as follows :

- All devices obtain the information of neighboring devices through NDP, including the software version, host name, MAC address and port name of neighboring devices.
- The management device uses NTDP to collect the device information within the hop range specified by the user and the connection information of each device, and determines the candidate devices of the cluster from the collected topology information.
- The management device completes the operations of adding the candidate device to the cluster and the member device leaving the cluster according to the candidate device information collected by NTDP.

The packets of the cluster are all Layer 2 Ethernet packets. For the specific format and interaction process, see the national standard "YDT 1692-2007 Ethernet Switch Cluster Management Technical Requirements."»

### **23.1.2 Cluster Role**

According to the different positions 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 IP address.

- Command switch to create a cluster ;

|

---

- The command switch collects NDP (Neighbor Discovery Protocol) and NTDP (Neighbor Topology Discovery Protocol) information to discover and determine candidate switches ;

- Command switches control the maintenance of the cluster, you can add candidate switches to the cluster or delete member switches from the cluster ;

- After the cluster is established, the command switch provides the management channel for the cluster.

## 2 ) Member switch

Managed switches in the cluster.

Member switches are candidate switches before joining the cluster.

Member switches do not set public IP ;

The management of member switches is done through the command switch agent.

## 3 ) Candidate switch

A switch that has the ability to join the cluster, but has not joined any cluster.

4 ) The switch must be a candidate switch before it can become a member switch.

## 5 ) Independent switch

Switch without cluster function.

Various roles can be converted according to certain rules :

- While creating a cluster on the candidate device, the user designates the current candidate device as the cluster management device. Each cluster must specify one (and only one) management device. After the management device is designated, the management device discovers and determines candidate devices by collecting relevant information. Users can add candidate devices to the cluster through corresponding configuration.

- After the candidate device joins the cluster, it becomes a member device.

- After a member device in the cluster is deleted, it will be restored as a candidate device.

- The management device can only be restored as a candidate device when the cluster is deleted.

---

### 23.1.3 NDP introduction

NDP is used to obtain information about directly connected neighbor devices, including connection port, device name, software version, etc. The working principle is as follows :

- A device running NDP periodically sends NDP messages to neighbors. The NDP message contains NDP information (including the device name, software version, and connection port of the current device) and the aging time of the NDP information on the receiving device. At the same time, it will also receive but not forward NDP messages sent by neighboring devices.

The devices running NDP will store and maintain the NDP neighbor information table, and create an entry for each neighbor device in the NDP neighbor information table. If a new neighbor is discovered and the NDP message sent by it is received for the first time, an entry is added to the NDP neighbor information table; if the NDP information received from the neighbor device is different from the old information, the NDP is updated. If the corresponding data items in the table are the same, only the aging time is updated. If the NDP information sent by the neighbor is not received after the aging time, the corresponding neighbor entry will be automatically deleted.

### 23.1.4 NTDP introduction

NTDP is used to collect information about each device and connection information between devices within a certain network. NTDP provides the device information that can join the cluster for the management device and collects the topology information of the devices within the specified hop count.

NDP provides adjacency table information for NTDP. NTDP sends and forwards the NTDP topology collection request based on the adjacency information to collect NDP information of each device within a certain network range and its connection information with all neighbors. After collecting this information, the management device or network management can use this information as needed to complete the required functions. When the NDP on the member device discovers that the neighbor has changed, it informs the management device of the neighbor change through a handshake message. The management device can start NTDP to collect the specified topology, so that NTDP can reflect the network topology change in time.

The management device can periodically perform topology collection in the network, and the user can also initiate a topology collection through manual configuration commands. The process of the management device collecting topology information is as follows :

- The management device periodically sends NTDP topology collection request

packets from the NTDP-enabled port.

- The device that receives the request message immediately sends a topology response message to the management device, and copies the request message on the NTDP-enabled port and sends it to the neighboring device; the topology response message contains the basic information of the device and all neighbors Device NDP information.

- The neighboring device will perform the same operation after receiving the request message, until the topology collection request message spreads to all devices within the specified hop range.

When topology collection request packets are diffused in the network, a large number of network devices simultaneously receive topology collection requests and simultaneously send topology response packets. In order to avoid network congestion and busy management device tasks, the following measures can be taken to control the topology collection request packet proliferation speed :

- After receiving the topology collection request, the device does not immediately forward the topology collection request packet, but waits for a certain period of time before it starts to forward the topology collection request packet on the NTDP-enabled port.

- On the same device, except for the first port, each NTDP-enabled port will send a topology collection request packet to the previous port after a certain time delay before forwarding the topology collection request packet.

## **23.1.5 Cluster management and maintenance**

### 1) Candidate device joins the cluster

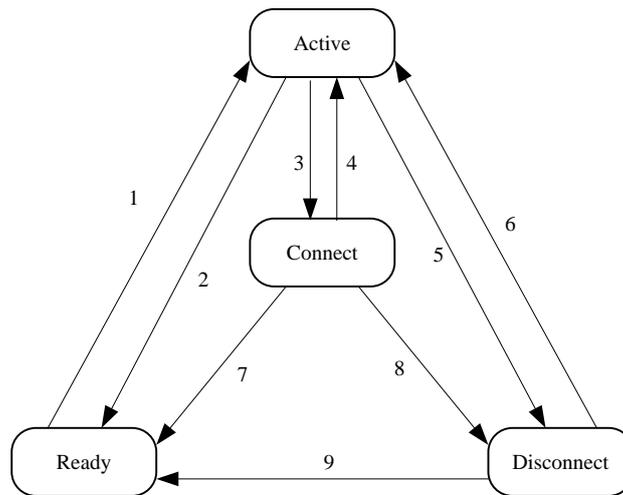
The user should first specify the management device before establishing the cluster. The management device discovers and determines candidate devices through the NDP and NTDP protocols, automatically adds the candidate devices to the cluster, or can manually add the candidate devices to the cluster.

After the candidate device successfully joins the cluster, it will obtain the cluster member serial number and cluster management assigned to it by the management device Private IP address used, etc.

### 2) Communication within the cluster

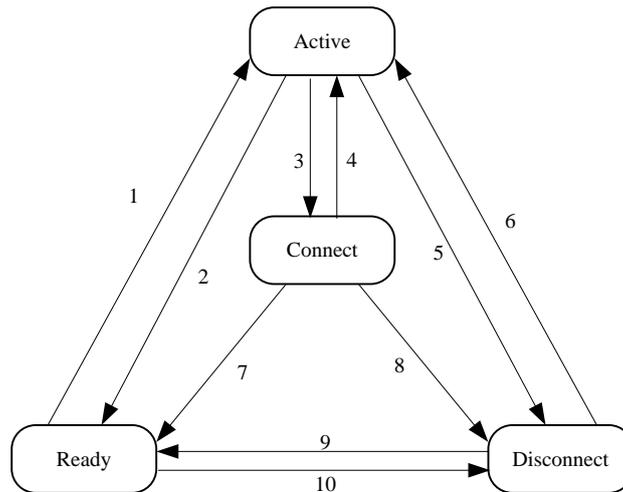
Within the cluster, the management device and member devices communicate in real time through handshake messages to maintain the

Connection status, the connection status of the management device and member devices is shown in the figure below.



- 1 Member join
- 2 Member deletion
- 3 Can't receive handshake signal for three consecutive times
- 4 Receive handshake signal
- 5 Recover request received
- 6 Interrupt recovery, re-register through
- 7 Member deletion
- 8 The state remains longer than the specified time
- 9 Member deletion

**Command switch state transition diagram**



- 1 Join the cluster
- 2 Exit the cluster
- 3 Can't receive handshake signal for three consecutive times
- 4 Receive handshake signal
- 5 Received join request
- 6 Interrupt recovery, re-register through
- 7 Exit the cluster
- 8 The state stays longer than the specified time or receives the join request message
- 9 Exit the cluster
- 10 Configuration recovery

**Member switch state transition diagram**

The command switch collects the basic information of the device, identifies a device as a candidate switch, and is initially in the Ready state.

In any state, the operation of deleting a member will migrate the state of the member switch back to the Ready state, and identify it as a candidate switch.

- After the cluster is established successfully, after the candidate device joins the cluster and becomes a member device, the management device saves the status

---

information of the member device locally, and marks the member status as Active, and the member device also saves its own status information locally, and identifies its own status Active.

- The management device and member devices periodically send handshake messages to each other. After receiving the handshake message from the member device, the management device does not respond and keeps the member device in the Active state; the member device also does not reply and keeps its state as Active.

- If the management device does not receive the handshake message sent by the member device within the triple handshake message sending interval after sending the handshake message to the member device, the state of the member device saved locally will be migrated from Active to Connect; the same If the member device does not receive the handshake message sent by the management device within three times of the handshake message transmission interval after sending the handshake message to the management device, its own state will also transition from Active to Connect.

- If the management device receives the handshake message or management message sent by the member device in the Connect state within the effective retention time, it will migrate the state of the member device back to Active, otherwise it will be migrated to Disconnect, and the management device will consider this The member is disconnected; if the member device in the Connect state receives the handshake message or management message sent by the management device within the effective retention time, it will migrate its state to Active, otherwise it will migrate to Disconnect.

- When the interrupted communication between the management device and the member device is restored, the member device in the Disconnect state will rejoin the cluster. After joining successfully, the member device's management device and local status will return to Active.

If a topology change is found, the member device also transmits the change information to the management device through a handshake message.

## **23.1.6 Management vlan**

The management VLAN limits the scope of cluster management. By configuring the management VLAN, the following functions can be achieved :

- The management messages of the cluster (including NDP, NTDP messages, and handshake messages) will be restricted to the management VLAN and isolated from other messages, increasing security.

- Management device and member device realize internal communication through management VLAN.

Cluster management requires that the ports connecting the management device and the member/candidate device, including the cascade port (when the candidate device is connected to the management device through another candidate device, the ports connected to each other between the candidate devices are called cascade ports) Management VLAN is allowed to pass, so :

- If the port does not allow the management VLAN to pass, the device connected to the port cannot join the cluster. Therefore, before the cluster, make sure that the port connecting the candidate device and the management device includes a cascade port to allow the management VLAN to pass.
- Only when the default VLAN ID of the port connecting the management device to the member/candidate device and the cascade port is the management VLAN, the packets configured with the management VLAN are allowed to pass without a label, otherwise the packets of the management VLAN must be The label passes.

For more information about VLAN, please refer to "Configuring VLAN".

## 23.2 Introduction to cluster configuration

Before configuring a cluster, users need to clarify the roles and functions of each device in the cluster, and also configure related functions to plan communication with devices in the cluster.

| Configuration tasks                |   |
|------------------------------------|---|
| Configuration management equipment | Enable the NDP function of the system and port  |
|                                    | Configure NDP parameters                        |
|                                    | Enable the NTDP function of the system and port |
|                                    | Configure NTDP parameters                       |
|                                    | Configure to manually collect NTDP information  |
|                                    | Enable the cluster function                     |
|                                    | Establish a cluster                             |
|                                    | Configure member interaction within the cluster |
|                                    | Configure cluster member management             |

|  |   |
|--|---|
| Configure member devices               | Enable the NDP function of the system and port  |
|  | Enable the NTDP function of the system and port |
|  | Configure to manually collect NTDP information  |
|  | Enable the cluster function                     |
| Configure cluster member mutual access |   |
|  |   |
|  |   |

*Note :*

*After the cluster is established, after the NDP or NTDP function is turned off on the management device and member devices, the cluster will not be disbanded, but it will affect the normal operation of the established cluster.*

## 23.3 Configuration management equipment

### 23.3.1 Enable the NDP function of the system and port

| command           | description  | CLI mode                     |
|-------------------|--|------------------------------|
| ndp global enable | Enable the global NDP function. By default, it is turned off globally.       | Configuration mode           |
| ndp enable        | Enable the NDP function of the port. NDP is disabled by default on all ports | Interface configuration mode |

*Note :*

- *The NDP function of the global and port must be enabled at the same time for NDP to function properly.*
- *NDP function does not support aggregation ports.*
- *In order to prevent the management device from collecting topology information of devices that do not need to join the cluster during topology collection and adding it to*

the cluster, it is recommended to turn off the NDP function on the ports connected to devices that do not need to join the cluster.

### 23.3.2 Configure NDP parameters

| command                      | description  | CLI mode           |
|------------------------------|--|--------------------|
| ndp aging-timer <aging-time> | Configure the aging time of NDP packets sent by this device on the receiving device. The default is 180 seconds. | Configuration mode |
| ndp hello-timer <hello-time> | Configure the interval for sending NDP packets. The default is 60 seconds.                                       | Configuration mode |

*Note:*

The aging time of NDP packets on the receiving device should generally not be less than the NDP sending interval, otherwise it will cause the instability of the NDP port neighbor information table.

### 23.3.3 Enable the NTDP function of the system and interface

| command            | description   | CLI mode                     |
|--------------------|---|------------------------------|
| ntdp global enable | Enable the global NTDP function. By default, it is turned off globally.       | Configuration mode           |
| ntdp enable        | Enable the NTDP function of the port. NDP is disabled by default on all ports | Interface configuration mode |

*Note :*

- The NTDP function of the global and port must be enabled at the same time for NTDP to function properly.

- NTDP function does not support aggregation ports

- In order to prevent the management device from collecting topology information of devices that do not need to join the cluster during topology collection and add it to the cluster, it is recommended to disable the NTDP function on the ports connected to devices that do not need to join the cluster.

---

## 23.3.4 Configure NTDP parameters

| command                      | description   | CLI mode           |
|------------------------------|---|--------------------|
| ntdp hop <hop-value>         | Configure the scope of topology collection. By default, in the collected topology, the farthest device is 3 hops away from the topology collection device.      | Configuration mode |
| ntdp timer <interval-time>   | Configure the interval for collecting topology information periodically. The default is 1 minute.   | Configuration mode |
| ntdp timer hop-delay <time>  | Configure the time that the collected device waits before forwarding the topology collection request packet on the first port. The default is 200 milliseconds. | Configuration mode |
| ntdp timer port-delay <time> | Configure the port delay time for the current device to forward the topology collection request. The default is 20 milliseconds.                                | Configuration mode |

## 23.3.5 Configure to manually collect NTDP information

After the cluster is established, the management device will periodically collect topology information. In addition, users can manually collect NTDP information through configuration (regardless of whether the cluster is established) or not, and initiate a NTDP information collection process, so as to more effectively manage and monitor the device in real time.

| command      | description                            | CLI mode                     |
|--------------|--|------------------------------|
| ntdp explore | Collect topology information manually. | Normal mode, privileged mode |

## 23.3.6 Enable the cluster function

| command        | description  | CLI mode           |
|----------------|--|--------------------|
| cluster enable | Enable the cluster function. The default cluster function is turned off. | Configuration mode |

## 23.3.7 Establish a cluster

The management VLAN limits the scope of cluster management. By configuring the management VLAN, the following functions can be achieved :

- The management messages of the cluster (including NDP, NTDP messages, and handshake messages) will be restricted to the management VLAN and isolated from other messages, increasing security.
- Management device and member device realize internal communication through management VLAN.

| command                           | description  | CLI mode           |
|-----------------------------------|--|--------------------|
| cluster management-vlan <vlan-id> | Specify the management VLAN. The default management VLAN is VLAN1. | Configuration mode |

### **Note :**

*If the current device is in a cluster, management VLAN modification is not allowed.*

*When not in a cluster :*

- 1 ) Check if the vlan exists, if there is no direct failure, if there is, continue to the next step.*
- 2 ) Check all the interfaces again. If the VLAN where the interface is located and the management VLAN are not the same VLAN, turn on the global switches of ndp and ntdp and do the corresponding shutdown and clear operation, and then reopen.*
- 3 ) Find the Layer 3 interface to be configured with VLAN. If not found, create a Layer 3 interface corresponding to VLAN. If the creation fails, the management VLAN configuration is successful. You can use ndp and ntdp, but you cannot join the cluster.*
- 4) Set the current layer 3 interface mac to dev\_id. If the vlan is set successfully and the*

*new layer 3 interface fails to be created, use the vlan1 mac as the dev\_id. If the management VLAN has been configured, but the user deletes the vlan directly in the vlan database, the management VLAN is automatically set to vlan1, and the opened ndp, ntdp and global switches of the cluster are all turned off and the corresponding closing and clearing operations are performed.*

Before establishing a cluster, the user must first set the private IP address range used by the member devices in the cluster. When the candidate device is added, the management device dynamically allocates a private IP address that can be used within the cluster range and issues it to the candidate device. Communication within the cluster to realize the management and maintenance of member devices by the management device.

| command                   | description  | CLI mode           |
|---------------------------|--|--------------------|
| cluster ip-pool <IP/MASK> | Configure the private IP address range used by the member devices in the cluster on the device to be set as the management device. | Configuration mode |

**Note :**

- *The IP addresses of the VLAN interfaces of the management device and member devices and the cluster address pool cannot be configured on the same network segment, otherwise the cluster will not work properly.*
- *Can be configured only when the device is not in the cluster.*
- *Use the management VLAN to find whether there is a corresponding Layer 3 port. If there is no Layer 3 port, directly return failure. (This device cannot be a cluster command switch) If there is a Layer 3 interface, configure the base address of IP-POOL to the Layer 3 port. If the configuration fails, IP-POOL also fails to configure.*

By default, the device is not a management device, and the cluster is established :

| command              | description  | CLI mode           |
|----------------------|--|--------------------|
| cluster build <name> | Manually establish a cluster, configure the current device as a management device, and | Configuration mode |

|                              |   |                    |
|------------------------------|---|--------------------|
|                              | assign a cluster name.  |                    |
| cluster auto-build <name>    | Automatically establish a cluster.<br>The automatic cluster function automatically adds all candidate devices discovered within the specified hop range to the created cluster.                                   | Configuration mode |
| cluster delete <name>        | Delete the cluster.   | Configuration mode |
| cluster stop auto-add member | Under the automatic cluster configuration, stop automatically joining member switches. This operation can only stop joining new devices. Devices that have already joined the cluster will remain in the cluster. | Configuration mode |

Note :

- *The user can only specify the management VLAN before establishing the cluster. After the device has joined the cluster, the user cannot modify the management VLAN. If 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 management VLAN as the default VLAN ID of the port connecting the management device to the member device and the cascade port.*
- *Only when the ports connecting the management device and member devices and the default VLAN IDs of all cascade ports are management VLANs, can the packets of the management VLAN be allowed to pass without a label, otherwise the ports connecting the management device and member devices must be configured. And all the cascade ports allow tags of management VLAN to pass through. For specific configuration, please refer to "VLAN".*
- *The private IP address range of member devices in the cluster can only be configured when the cluster has not been established, and can only be configured on the management device. If the cluster has been established, the system does not allow*

*modification of the IP address range.*

### **23.3.8 Configure member interaction within the cluster**

Within the cluster, the management device and member devices communicate in real time through handshake messages to maintain the connection status between them. You can configure the time interval for sending handshake messages and the effective retention time of the device on the management device. All member devices in the cluster take effect simultaneously.

| command                       | description  | CLI mode           |
|-------------------------------|--|--------------------|
| cluster timer <interval-time> | Configure the interval at which handshake packets are 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 |

### **23.3.9 Configure cluster member management**

The user can manually specify the candidate devices to join the cluster on the management device, or manually delete the specified member devices in the cluster. Join/delete operations of cluster members must be performed on the management device, otherwise an error message will be returned.

| command   | description                             | CLI mode           |
|---|---|--------------------|
| cluster add member mac-address <mac-address>    | Add candidate devices to the cluster.   | Configuration mode |
| cluster delete member mac-address <mac-address> | Remove member devices from the cluster. | Configuration mode |

## **23.4 Configure member devices**

### **23.4.1 Enable the NDP function of the system and port**

See Enabling the NDP function of the system and port

---

## 23.4.2 Enabling the NTDP function of the system and port

See Enabling the NTDP function of the system and port

## 23.4.3 Configure to manually collect NTDP information

See Configuring Manually Collecting NTDP Information

## 23.4.4 Enable the cluster function

See Enabling the cluster function

## 23.5 Configuring access to cluster members

After the NDP, NTDP, and cluster functions are correctly configured, the member devices in the cluster can be configured, managed, and monitored through the management device. You can switch to the specified member device operation interface on the management device to configure and manage the member device.

| command                                  | description   | CLI mode                     |
|--|---|------------------------------|
| cluster switch-to member <member-number> | Switch from the management device operation interface to the member device operation interface. | Normal mode, privileged mode |

*note :*

*Telnet connection is used for the mutual switching between the cluster management device and the member devices. Pay attention when switching :*

- *Before performing the switch, the peer device needs to execute the "telnet server enable" command to enable the telnet function, otherwise the switch will fail.*

*Switch from the management device to the member device, if the member number n does not exist, an error message will be displayed.*

*If the Telnet user of the device requested to log in is full, the switch will fail.*

---

## 23.6 Cluster management display and maintenance

| command   | description  | CLI mode                     |
|---|--|------------------------------|
| show ndp[interface <ifname> ]                         | Display NDP configuration information  | Normal mode, privileged mode |
| reset ndp statistics [interface <ifname>]             | Clear NDP statistics   | Configuration view           |
| show ntdp   | Display system NTDP information  | Normal mode, privileged mode |
| show ntdp device-list                                 | Display device information collected by NTDP                                 | Normal mode, privileged mode |
| show ntdp single-device mac-address <mac-address>     | Display detailed NTDP information of the specified device                    | Normal mode, privileged mode |
| show cluster  | Display the status and statistics of the cluster to which the device belongs | Normal mode, privileged mode |
| show cluster topology                                 | Display cluster topology information   | Normal mode, privileged mode |
| show cluster candidates [ mac-address <mac-address> ] | Display candidate device information   | Normal mode, privileged mode |
| show cluster members [ <member-number>]               | Display cluster member information.  | Normal mode, privileged mode |

## 23.7 Typical example of cluster management configuration

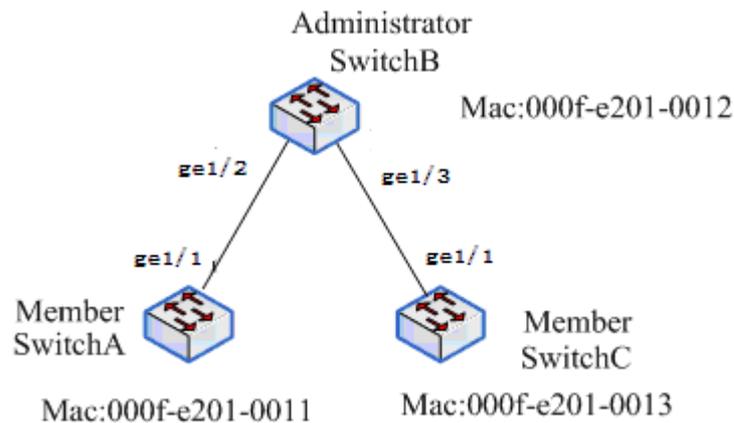
1、Networking requirements :

The cluster abc is composed of three switches, and its management VLAN is VLAN 10. Among them, Switch B is the management device.

( Administrator ) ; Switch A and Switch C are member devices ( Member ) 。

The base address IP of the entire cluster address pool is 10.0.0.1, supporting 8 devices.

2、 Network diagram :



3、 Configuration steps :

Configure member devices SwitchA

# configure management VLAN。

```
[SwitchA] cluster management-vlan 10
```

```
[SwitchA] interface ge1/1
```

```
[SwitchA-ge1/1] switch access vlan 10
```

# Enable the global NDP function and the NDP function on port ge1/1。

```
[SwitchA] ndp global enable
```

```
[SwitchA] interface ge1/1
```

```
[SwitchA-ge1/1] ndp enable
```

# Enable the global NTDP function and the NTDP function on port ge1/1。

```
[SwitchA] ntdp global enable
```

```
[SwitchA] interface ge1/1
```

```
[SwitchA-ge1/1] ntdp enable
```

# Enable the cluster function。

```
[SwitchA] cluster enable
```

Configure member devices SwitchC

Because the configuration of the member devices is the same, the configuration on Switch C is similar to Switch A, and the configuration process is omitted.

Configure management equipment SwitchB

# configure management VLAN。

|

---

```
[SwitchB] cluster management-vlan 10
[SwitchB] interface ge1/2
[SwitchB-ge1/2] switch access vlan 10
[SwitchB] interface ge1/3
[SwitchB-ge1/3] switch access vlan 10
# Enable global NDP and NTDP functions, and 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
# Set the aging time of NDP packets sent by the device on the receiving device to 200
seconds.
```

```
[SwitchB] ndp timer aging 200
# Set the interval for sending NDP packets to 70 seconds.
[SwitchB] ndp timer hello 70
# Configure the maximum hop count for topology collection to 2 hops.
[SwitchB] ntdp hop 2
# Configure the delay time for the first port of the collected device to forward topology
collection request packets to 150ms.
```

```
[SwitchB] ntdp timer hop-delay 150
# Configure the delay time for other ports on the collected device to forward topology
collection request packets to 15ms.
```

```
[SwitchB] ntdp timer port-delay 15
# Configure the topology collection interval to 3 minutes.
```

```
[SwitchB] ntdp timer 3
```

```
# Enable the cluster function.
```

```
[SwitchB] cluster enable
```

|

---

# Configure the private IP address of member devices range from 10.0.0.1 ~ 10.0.0.9.

```
[SwitchB] cluster ip-pool 10.0.0.1 8
```

# Configure the current device as a management device, and establish a cluster named abc, members automatically join the cluster.

```
[SwitchB] cluster autobuild abc
```

#When you have added all the switches you want to add, you can turn off the automatic join cluster function.

```
[SwitchB]cluster stop auto-add member
```

---

## Chapter24 **SNTP** **configuration**

---

This chapter mainly includes the following :

- introduction
- SNTP configuration
- Display SNTP

---

## 24.1 SNTP introduction

At present, the Internet generally uses communication protocols to achieve network time synchronization, that is, NTP (Network Time Protocol), and there is another protocol that is a simplified version of NTP protocol, that is, SNTP (Simple Network Time Protocol).

The NTP protocol can span various platforms and operating systems and uses very sophisticated algorithms, so it is almost not affected by the delay and jitter of the network, and can provide 1-50ms accuracy. NTP also provides an authentication mechanism with a high level of security. However, the NTP algorithm Complex, high requirements on the system.

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 high. The accuracy can generally reach about 1 second, which can basically meet the needs of most occasions..

Since the SNTP message and the NTP message are completely the same, the SNTP Client implemented by this switch is fully compatible with the NTP Server.

## 24.2 SNTP configuration

### 24.2.1 Default SNTP settings

| project                            | Default value                |
|------------------------------------|------------------------------|
| SNTP status                        | Disable disable SNTP service |
| NTP Server                         | none                         |
| SNTP synchronization time interval | 1800 seconds                 |
| Local time zone                    | +8, UTC/GMT+08:00            |

Enable and disable SNTP

The configuration is as follows:

Switch# configure terminal

Enter global configuration mode  
Switch(config)# sntp enable  
Enable SNTP  
Switch(config)# sntp disable  
Disable SNTP

## 24.2.2 Configuring the SNTP Server Address

Since the SNTP message and the NTP message are exactly the same, the SNTP Client is fully compatible with the NTP Server. There are many NTP Servers on the network, you can choose one with less network delay as the NTP on the switch Server.

The specific NTP server address can be obtained from <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 up to three server addresses. The switch uses the first server address to synchronize time. If synchronization fails, the second server address is used, and so on.

The configuration for adding a Server address is as follows :

```
Switch# configure terminal
Enter global configuration mode
Switch(config)# sntp server 210.72.145.44
```

Increase the SNTP server IP. If there are already three Server addresses on the switch, the increase will fail. You need to delete the address and add it

The configuration for deleting the server address is as follows :

```
Switch(config)# no sntp server
Delete all Server addresses
Switch(config)# no sntp server 210.72.145.44
Delete a server address
```

## 24.2.3 Configure SNTP clock synchronization interval

The SNTP Client needs to synchronize the clock with the NTP Server regularly, so that the clock can be corrected regularly.

The configuration is as follows:

```
Switch# configure terminal
Switch(config)# sntp interval 60
```

Set the interval of the timing synchronization clock, the unit is second, the range is 60 seconds-65535 seconds. The default value is 1800 seconds, here is set to 60 seconds

```
Switch(config)# no sntp interval
```

The interval of the timing synchronization clock is restored to the default of 1800 seconds.

## 24.2.4 Configure local time zone

The time obtained after communicating through the SNTP protocol is Greenwich Mean Time (GMT). In order to prepare for the hunting of local time, it is necessary to set up the local area to adjust the standard time. By default, the switch sets the local time zone to eighth zone, which is also the time zone of China.

The configuration is as follows:

```
Switch# configure terminal
```

```
Switch(config)# sntp time-zone -8
```

```
Set local time zone to west eight
```

```
Switch(config)# no sntp time-zone
```

The local time zone is restored to the East Eight District

## 24.3 SNTP information display

The configuration is as follows:

```
Switch# show sntp
```

```
Switch# show running-config
```

---

# Chapter25 RIP configuration

---

This chapter mainly includes the following :

- RIP introduction
- RIP configuration
- RIP configuration example

## 25.1 RIP introduction

RIP (Routing Information Protocol) is a dynamic routing protocol developed earlier. It uses the distance vector algorithm and is mostly used in small networks. RIP protocol packets are encapsulated in UDP packets, using UDP port 520. The main idea of RIP is to use hops to measure the distance to the host, and the number of hops increases by 1 every time a router passes through, to calculate the routing metric and select the route. RIP stipulates that the maximum number of hops is 15, and the number of hops 16 is marked as unreachable. RIP broadcasts the entire routing table to allow routers in the network to synchronize routing information and update the message every 30 seconds. If a certain routing entry does not receive an update message from a neighbor within 180 seconds, then Mark it as unreachable, delete the route if no valid update is received after 120 seconds.

RIP is easy to implement because of its simple idea, but it also brings about

---

corresponding routing loop problems. To prevent routing loops, RIP introduces a split horizon mechanism to avoid spoofing between routers. Split horizon means that routing updates will not be published from the received interface. Split horizon with poisonous reverse is to advertise routing updates from the received interface, but the weight is marked as unreachable, which allows neighbor routers to quickly identify loops without waiting for the weight to increase to unreachable.

The routing entry in the routing table should contain the destination address (host or network) next hop address, forwarding interface, routing weight, timer (the timer is reset when a routing update is received) routing tag.

When RIP starts, it immediately sends a full-table request message 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 routing table in response to the message. . After receiving the response message, the router will process the routes one by one and modify its own routing table. When there is a new route, it will immediately generate a trigger update message. After a series of update processes, eventually RIP converges, and each router in the network maintains the latest and consistent routing information. After the network is stable, RIP still broadcasts the local routing table to neighbors every 30 seconds, and each router maintains its own routing information according to the received routing update message and performs the most optimal route. RIP uses a timeout mechanism to process routing entries that have not been updated for a long time to ensure that the routing is correct in real time.

RIP is mostly used in campus networks and more continuous regional networks with simple structures, and complex large-scale networks are difficult to handle.

## 25.2 RIP configuration

After starting the RIP protocol, you can configure the RIP functions and attributes. RIP configuration is mostly in RIP configuration mode and interface configuration mode.

RIP configuration includes :

- Start RIP and enter RIP configuration mode
- Enable RIP interface
- Configure unicast message transmission
- Configure the working status of the interface
- Configure default routing metric

- 
- Configure management distance
  - Configure timer
  - Configuration version
  - Import external routes
  - Configure route filtering
  - Configure additional routing metric
  - Configure the RIP version of the interface
  - Configure the sending and receiving status of the interface
  - Configure split horizon
  - Message authentication
  - Configure interface metric

### 25.2.1 Start RIP and enter RIP configuration mode

Mode: Global configuration mode

command : router rip

Start rip and enter rip configuration mode

command : no router rip

Close rip agreement

Default: do not run rip protocol

### 25.2.2 Enable RIP interface

When RIP works, you can specify some interfaces, configure the network where it is located as a RIP network, and you can send and receive RIP protocol packets on it. .

Mode: RIP configuration mode

command : network <network-address>

Enable 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 A.B.C.D. The former one

specifies the network ip and mask length, and the latter one specifies the network ip and mask length.

Default: RIP protocol is disabled on all interfaces after startup

After the RIP protocol is started, the working network segment must be specified. 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 RIP view, the interfaces that are not in the specified network segment do not exist. The parameter network-address is an enabled or disabled network address, which can be configured as an interface ip address. The network command enables the interface of the network segment at this address. For example: the IP address of an interface is 192.160.1.1, use the command network 192.160.1.1/24, use the show running-config command to see the network 192.160.1.0/24.

### **25.2.3 Configure unicast messaging**

RIP protocol version 1 uses broadcast exchange messages, and version 2 uses multicast (224.0.0.9) to exchange messages. When running the RIP protocol on a link that does not support broadcasting, you need to specify a specific unicast address to exchange messages.

Mode: RIP configuration mode

command : neighbor <ip-address>

Configure the peer unicast IP address

command : no neighbor <ip-address>

Cancel the setting of the peer unicast IP address

Parameters: ip-address is the specified unicast ip address

Default: RIP protocol does not send messages to any unicast address

### **25.2.4 Configure the working status of the interface**

The RIP protocol runs on some networks and may only require RIP interface routing, and does not want to broadcast RIP routes on this interface. Use the network command to

specify the interface to send and receive RIP protocol packets, and you can learn the interface route. Use the passive-interface command to only learn the route of the interface and block the broadcast of the interface.

Mode: RIP configuration mode

command : passive-interface <if-name>

Configure the interface to be passive

command : no passive-interface <if-name>

Cancel interface passive state

Parameters: if-name is the agreed layer 3 interface name (for example: vlan1  
vlan2 ...)

Default: none of the enabled RIP interfaces are in passive state

## 25.2.5 Configure the default routing metric

When importing external routes, you need to specify a routing metric; when the routing metric is not specified, the default routing metric is used.

Mode: RIP configuration mode

command : default-metric <metric>

Set the default route metric when importing external routes

command : no default-metric [metric]

When importing external routes, the default route metric is 1

Parameter: metric value is between 1~16, greater than 1, less than 16.

Default: the metric value is 1, use the no default-metric command to restore to the default value.

## 25.2.6 Configure management distance

Each protocol has an agreed priority, and the management distance is the priority of the route selected when the routing strategy is used. When there are two identical routes (from different routing protocols) to the same destination, the smaller the administrative

distance, the route of the protocol is preferred.

Mode: RIP configuration mode

command : distance <distance>

Set management distance value

command : no distance [distance]

Restore the management distance to the default value

Parameter: distance value is between 1~255

Default: distance value is 120, use no distance command to restore to default value.

## 25.2.7 Configure Timer

The RIP protocol has three timers. One is that the complete routing table is broadcast to all RIP interfaces every 30 seconds. The second is that each route in the RIP routing table is marked with a metric of 16 if no update is received for 180 seconds. The third is RIP. Each route in the routing table is deleted from the routing table if the metric is 16 and it has not been effectively updated for 120 seconds.

Mode: RIP configuration mode

command : timers basic <update> <timeout> <garbage>

Set three timer values

command : no timers basic

Restore timer to default

Parameters: The first parameter update is the timer for updating the entire RIP routing table regularly , The second parameter timeout is the timer that is not updated when each route times out , The third parameter garbage is that each route is marked as invalid and the timer needs to be deleted after timeout; The value range of the three timers is  $5\sim(2^{31}-1)$ .

Default: update is updated every 30 seconds; timeout is marked as invalid for 180 seconds; garbage is deleted for 120 seconds.

---

## 25.2.8 Configuration version

RIP protocol currently has version 1 (RFC1058) and version 2 (RFC2453), the configured version value will be reflected in the version field of the protocol packet.

Mode: RIP configuration mode

command : version <version>

Set RIP protocol to version 1 or version 2

command : no version [version]

Restore RIP protocol version to default

Parameter: version can take the value 1 or 2

Default: version 2

## 25.2.9 Import external routes

RIP allows users to import routing information of other protocols into the routing table of RIP. The routing protocols (types) that RIP can import include: connected, static, OSPF, IS-IS, BGP.

Mode: RIP configuration mode

command : redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> |

route-map <route-map-name>]

Import other protocol routes

command : no redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> | route-map <route-map-name>]

Cancel imported routes

Parameters: The first parameter is the name of introducing other protocols, which can be directly connected, static, ospf, is-is, bgp ; The second parameter is the weight set at the time of introduction, ranging from 1~16之间 ; The third parameter is the name of the referenced route-map. Route-map is configured in the global configuration mode, please refer to the command manual.

Default: RIP protocol does not introduce any external protocol

---

## 25.2.10 Configure route filtering

RIP provides route filtering function, through the specified access control list and address prefix list, to filter received routes and advertised routes, configure policy rules to filter.

Mode: RIP configuration mode

command : `distribute-list <acl-name> {in | out} [if-name]`

Use the access-list to filter the input and output of the interface

command : `no distribute-list <acl-name> {in | out} [if-name]`

Cancel access-list filtering

Parameters: `acl-name` indicates the name of the referenced access-list ; `if-name` indicates the RIP interface to which it is applied ; `in` and `out` indicate whether the application is in the direction of receiving the route or the direction of publishing the route.

command : `distribute-list prefix <pre-name> {in | out} [if-name]`

Use prefix-list filtering

command : `no distribute-list prefix <pre-name> {in | out} [if-name]`

Cancel the use of prefix-list filtering

Parameters: `pre-name` indicates the name of the referenced prefix-list ; `if-name` indicates the RIP interface to which it is applied ; `in` and `out` indicate whether the application is in the direction of receiving the route or the direction of publishing the route.

Default: RIP protocol does not filter any received and sent routes

`access-list` and `prefix-list` are configured in global configuration mode, please refer to the command manual.

## 25.2.11 Configure additional routing metric

The additional routing weight is an offset value added to the input and output of the routing weight of the RIP protocol. It does not directly change the routing weight in the

routing table, but adds an offset when the interface receives and sends routes.

Mode: RIP configuration mode

command : `offset-list <acl-name> {in | out} <offset> [if-name]`

Use access-list to add an offset to the weight of the input and output routes of the interface

command : `no offset-list <acl-name> {in | out} <offset> [if-name]`

Cancel the weight offset of the input and output routes

Parameters: `acl-name` indicates the name of the referenced access-list ; `in` and `out` indicate whether the application is in the input or output direction ; `offset` represents the value of the offset , ranging from 0~16 ; `if-name` indicates the RIP interface to which it is applied.

Default: The additional weight of each route is 1 when receiving a message, and the additional weight of each route is 0 when sending a message.

## 25.2.12 Configure the RIP version of the interface

RIP is divided into two versions: RIP-1 and RIP-2. You can specify the version of the RIP packets it processes on the enabled RIP protocol interface. The receiving direction can be divided into receiving only RIP-1 messages, receiving only RIP-2 messages, and receiving both RIP-1 and RIP-2 messages. In the sending direction, it can be divided into sending RIP-1 messages, sending RIP-2 messages (by broadcast), sending RIP-2 messages (by multicast), both sending RIP-1 and sending RIP-2 message. RIP-2 has two methods of sending messages, broadcast and multicast. Using multicast can not only prevent hosts on the same network that are not running RIP from receiving RIP broadcast messages, but also prevent RIP-1 hosts from handling RIP errors. -2 routing with subnet mask.

Mode: Interface configuration mode

command : `ip rip receive version {1 | 2}`

Set the interface to receive only version 1 packets or only version 2 packets

Parameter: Version 1 or Version 2

command : `ip rip receive version {1 2 | 2 1}`

Set the interface to receive both version 1 and version 2 messages

Parameter: Can be written 1 2 or 2 1

command : no ip rip receive version [1 | 2 | 1 2 | 2 1]

Restore the interface receiving packets to the default value

Default: version 2 multicast mode

command : ip rip send version {1 | 2 | 1-compatible}

Set the interface to send only version 1 messages or only version 2 messages

Parameters: version 1 or version 2; 1-compatible means that the version 2 interface sends out a version 1 compatible message, that is, a broadcast message instead of a 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 1 2 or 2 1

command : no ip rip send version [1 | 2 | 1-compatible | 1 2 | 2 1]

Restore the interface sending packets to the default value

Default: version 2 multicast mode

## 25.2.13 Configure the transceiver status of the interface

After the network command is used to enable the RIP interface in RIP mode, you can also specify the status of sending and receiving protocol packets in interface mode, whether to receive protocol packets or whether to send protocol packets.

Mode: Interface configuration mode

command : ip rip receive-packet

Configure the interface to receive protocol packets

command : no ip rip receive-packet

Configure the interface not to receive protocol packets

command : ip rip send-packet

Configure the interface to send protocol packets

|

---

command : no ip rip send-packet

Configure the interface not to send protocol packets

Default: enable receiving and sending protocol packets

Note the difference. The network command starts a network to run the RIP protocol, and sends and receives protocol packets on the interface within the network. The interface route is included in the routing table. The passive-interface command prevents the interface from sending and receiving protocol packets after the network command takes effect, but the interface route is still included in the routing table. The ip rip receive-packet and ip rip send-packet commands also specify whether the interface receives or sends protocol packets after the network command takes effect.

## 25.2.14 Configure split horizon

Split horizon means that routes received from this interface are not sent out from this interface. Split horizon with poisonous inversion means that the route received from this interface is still sent from this interface, but its metric value is marked as 16. Horizontal segmentation can avoid loops to a certain extent. Horizontal segmentation with toxic inversion is more efficient than ordinary horizontal segmentation, and direct marking is not reachable. But on the NBMA network, it is necessary to prohibit split horizon to obtain the correct route.

Mode: Interface configuration mode

command : ip rip split-horizon [poisoned]

Enable interface split function or with poison reverse

command : no ip rip split-horizon

Disable the split horizon function of the interface

Parameter: No poisoned parameter means to start the ordinary horizontal split function , Poisoned parameter indicates that the split horizon function with poison reverse is enabled.

Default: split horizon with toxic reversal.

---

## 25.2.15 Message authentication

RIP-1 does not support message authentication, and RIP-2 supports message authentication. There are two authentication methods, plaintext authentication and MD5 authentication. The unencrypted authentication data in plaintext authentication is transmitted along with the message, which cannot provide security and cannot be applied to networks with high security requirements. There are two types of password settings: common key and key chain. The common key stores independent character strings, and the key chain manages the key's id, content, received lifetime, and sent lifetime. See the Command Reference Manual for details of keychain management.

Mode: Interface configuration mode

command : ip rip authentication mode {text | md5}

Set authentication mode plain text or md5

command : no ip rip authentication mode [text | md5]

Cancel certification

Parameters: text for plain text authentication, md5 authentication.

Default: no authentication

command : ip rip authentication string <password>

Set authentication password string

command : no ip rip authentication string [password]

Cancel authentication password string

Parameters: 16-byte authentication password

command : ip rip authentication key-chain <key-chain-name>

Set authentication key-chain

command : no ip rip authentication key-chain [key-chain-name]

Cancel the key-chain of authentication

Parameters: the name of the referenced key-chain ; key-chain is configured in global configuration mode , See the command manual.

## 25.2.16 Configure interface metric

Mode: Interface configuration mode

mode : ip rip metric <metric>

Configure interface metric

command : no ip rip metric

Restore interface metric to default metric

Parameter: The value of metric ranges from 1 to 16, which indicates the metric of the route entry learned by this interface.

Default: 1

## 25.2.17 Display information

mode : Normal mode or privileged mode

command : show ip protocols

Display information about all running protocols

command : show ip protocols rip

Display RIP protocol information

command : show ip rip

Show RIP routing

command : show ip rip database

Show RIP database

command : show ip rip database count

Display the number of RIP database entries

command : show ip rip interface [if-name]

Display RIP interface information

Parameters: if-name is the agreed layer 3 interface name

Mode: Privileged mode

command : show running-config

Display the current configuration of the switch, including RIP configuration.

command : show running-config rip

Display the current configuration of the RIP protocol.

---

## 25.3 RIP configuration example

### (1) configuration

The three switches are connected in pairs, each with 6 network segments, and the rip protocol is enabled, so that the three PCs can communicate with each other.

On switch 1 :

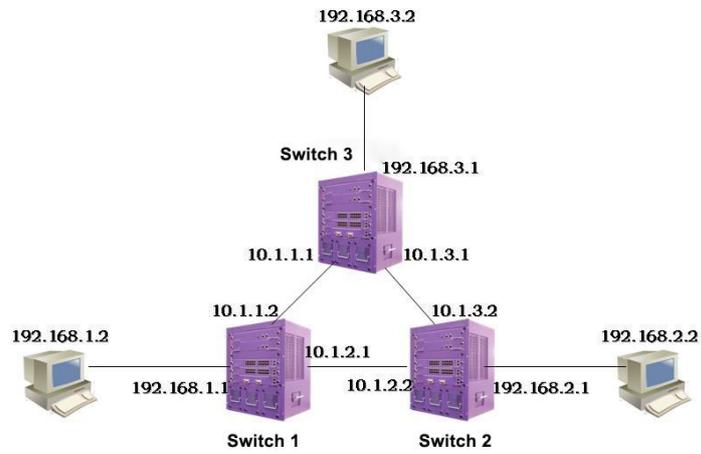
```
Switch# configure terminal
Switch(config)#router rip
Switch(config-rip)#network 192.168.1.0/24
Switch(config-rip)#network 10.1.1.0/24
Switch(config-rip)#network 10.1.2.0/24
```

On switch 2 :

```
Switch# configure terminal
Switch(config)#router rip
Switch(config-rip)#network 192.168.2.0/24
Switch(config-rip)#network 10.1.2.0/24
Switch(config-rip)#network 10.1.3.0/24
```

On switch 3 :

```
Switch# configure terminal
Switch(config)#router rip
Switch(config-rip)#network 192.168.3.0/24
Switch(config-rip)#network 10.1.1.0/24
Switch(config-rip)#network 10.1.3.0/24
```



## (2) verification

Use the following command to view RIP information :

```
show ip protocols rip  
show ip rip database  
show ip rip interface
```

---

## Chapter26 **OSPF** **configuration**

---

This chapter mainly includes the following :

- OSPF introduction
- OSPF configuration
- OSPF configuration example

---

## 26.1 OSPF introduction

OSPF (Open Shortest Path First) is a protocol based on link state algorithm, which can support larger-scale networks and has faster convergence speed.

Routers running the OSPF protocol each maintain a link state database (LSDB), which describes the topology of the entire autonomous system as if it were a map. After the databases of all routers are 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 the topology changes in the network, the router only needs to encapsulate the changed link state in the link state update (LSU) message and broadcast it. 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, which forms the topology description LSDB of the entire network and converts it into a weighted directed graph, you can use the SPF algorithm to calculate the routing table.

In the broadcast network, each router needs to broadcast its own status information to other routers, which will establish multiple pairwise adjacencies, which will bring a lot of unnecessary message transmission. To this end, OSPF has appointed a designated router (DR) and a backup designated router (BDR). The router sends the link information to the DR, which is collected by the DR and then sent to all routers. Effectively reduces the number of adjacencies between routers on the broadcast network.

OSPF supports five protocol packets :

The HELLO message is broadcast periodically to neighbors, used to discover and maintain the neighbors, conduct DR elections, and contains some interface attribute values. Some parameters in the HELLO message must be consistent to establish a neighbor.

DD message (Database Description) uses the DD message to describe its own LSDB during the synchronization process, including the head of each LSA. The LSA head can uniquely determine an LSA, and the peer router can determine whether it has this LSA; None, then request the complete LSA.

LSR message (Link State Request) After two routers exchange DD messages, they will know which LSAs of the peer router are missing locally. At this time, they need to send

---

LSR messages to request the complete LSA. Only LSA head is needed when requesting.

LSU message (Link State Update) is a collection of multiple LSAs.

LSAck message (Link State Acknowledgement) is to confirm the received LSU message to ensure reliable transmission of link information. Confirm with LSA head.

Router-id concept: the unique identifier of the router in the autonomous system.

Area: If OSPF is running on a larger network, the LSDB will be very large due to the large increase in the number of routers, and the synchronization time and routing calculation time will increase, taking up a lot of storage space and CPU resources. And the larger the network, the more frequent the topology changes, so that the network is often in flux. Routers need to spend a lot of time to transmit packets to calculate routes, which unnecessarily takes up network bandwidth. Therefore, OSPF introduces the concept of area and divides the router into different areas. LSDB only synchronizes in the area and calculates routes in the area. The routing interaction between areas is completed by the border router (ABR). In this way, the number of routers in the area will be limited, and the LSDB will be limited to a small capacity. The time to calculate the route will be greatly reduced, and the convergence will be fast when the topology changes. The concept of area effectively groups a large-scale network and undertakes a small-scale routing function within each area. Routes between areas interact on the backbone area (area with area ID 0). Therefore, all non-backbone areas must be connected to the backbone area, that is, at least one interface of the ABR connects to the backbone area. If the network is planned and there is a non-backbone area that cannot communicate with the backbone area, you must configure a virtual link to establish a logical path, that is, an ABR in the backbone area and an ABR in the non-backbone area through a transmission area establishment point to Point link. Then the inter-domain routing information in the backbone area will also be advertised to the non-backbone area through the virtual link.

## 26.2 OSPF configuration

After the OSPF protocol is started, enter the OSPF configuration mode to set the corresponding attributes and functions. OSPF configuration commands are mostly in OSPF configuration mode and interface configuration mode.

OSPF configuration includes :

- Start OSPF and enter OSPF mode

- 
- Enable interface
  - Designated host
  - Configure router ID
  - Configure adjacency points
  - Prohibit the interface from sending packets
  - Configure SPF timer
  - Configure management distance
  - Import external routes
  - Configure the network type of the interface
  - Configure the interval for sending hello messages
  - Configure the neighbor router failure time
  - Configure retransmission interval
  - Configure interface delay
  - Configure the priority of the interface in DR election
  - Configure the cost of sending packets on the interface
  - Configure whether the interface sends DD packets with MTU value
  - Configure interface packet authentication
  - Configure area virtual links
  - Configure regional route aggregation
  - Configure regional message authentication
  - Configure stub area
  - Configure nssa area
  - Configure external route aggregation
  - Configure the default metric of external routes

## 26.2.1 Start OSPF and enter OSPF mode

The OSPF protocol can run multiple copies, using the process ID (process-id) to identify; when starting the OSPF protocol, it is necessary to indicate which process ID is started; if there is no parameter, the process number is 0.

Mode: Global configuration mode

command : router ospf [process-id]

Start the OSPF process with process ID process-id and enter its mode

command : no router ospf [process-id]

Close the OSPF process with process ID process-id

Parameter: The value of process-id ranges from  $1\sim(2^{16}-1)$  , indicating the OSPF process ID started ; Without the parameter process-id, start OSPF with process number 0.

Default: do not run OSPF protocol

## 26.2.2 Enable interface

The valuable aspect of the OSPF protocol is that it introduces a layered idea and divides a complete autonomous system into different regions in order to establish a conceptual hierarchical network model. The area is logical, and the routers in the autonomous system are artificially grouped. When different interfaces of a router belong to different areas, that is, across areas, it is called a border router ABR. For each network segment that starts the OSPF protocol, it can only belong to a specific area, that is, each interface running the OSPF protocol on the router must belong to the specified area. Areas are identified by area numbers (area-id), and the area with area number 0 is the backbone area. Routing information between different areas is passed through the border router. Different from RIP protocol, you must specify the area to which OSPF protocol runs on the interface.

Mode: OSPF configuration mode

command : network <network-address> area <area-id>

Designated area designated interface running OSPF protocol

command : no network <network\_address> area <area-id>

Shut down OSPF on a specific interface in a specific area

Parameters: network-address has two forms: A.B.C.D/M and A.B.C.D A.B.C.D. The former one specifies the network ip and mask length, and the latter one specifies the network ip and mask length. area-id also has two forms A.B.C.D and integer, the former uses dotted decimal format, the latter takes values between  $0\sim(2^{32}-1)$ .

Default: The interface is not enabled after the OSPF protocol is started

---

## 26.2.3 Designated host

Mode: OSPF configuration mode

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

Parameters: ip-address uses A.B.C.D format to indicate a designated host in a certain area, which is of stub type on the link representation of the router. The area-id is described in the network command. cost indicates the cost of specifying the link, which is an optional parameter.

Default: if the cost is not configured, the default is 0

## 26.2.4 Configure router ID

The router ID is a 32-bit unsigned integer, which is the unique identifier of a router in an autonomous system. The router ID can be manually configured. When configuring, ensure that the IDs of any two routers in the autonomous system are different. If not configured, the router uses the IP address of the loopback interface; if loopback has no IP, select the highest address from the current interface's IP address as the ID. In order to ensure the stable operation of OSPF, the router ID should be divided and manually configured during network planning.

Mode: OSPF configuration mode

command : ospf router-id <router-id>

Configure router ID

command : no ospf router-id

Cancel router ID

command : router-id <router-id>

command : no router-id [router-id]

Parameter: router-id uses A.B.C.D format

Default: After the OSPF protocol is started, the router ID is automatically generated according to the rules. The rules are as follows: first select the router-id configured by this command; if not, choose the IP address of the loopback; if not, choose the highest IP address of the current interface; if not, then 0.0.0.0.

Both sets of commands have the same function.

## 26.2.5 Configure adjacency

The OSPF protocol interactive protocol packets use the multicast address 224.0.0.5 or 224.0.0.6 through multicast. When the OSPF protocol runs on a link that does not support broadcasting, such as NBMA, some configuration must be performed to use unicast to exchange protocol packets. At this time, you can manually specify the peer IP address and the corresponding attribute value.

Mode: OSPF configuration mode

command : neighbor <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>]

Specify peer adjacency points and set properties

command : no neighbor <ip-address> [priority <prio> | poll-interval <deadtime> | cost <cost>]Cancel the peer adjacency point and attribute settings

Parameters: IP address of the peer end of ip-address, in A.B.C.D format ; prio is the peer priority, ranging from 0~255 ,deadtime is the timing when the peer is considered to be down , If the timer expires, no more hello messages will be sent to the peer , ranging from 1~(2<sup>16</sup>-1) ; cost is the cost of the link to the peer , ranging from 1~(2<sup>16</sup>-1).

Default: priority is 1 (0 does not participate in DR election); poll-interval is 120 seconds; cost is 10.

---

## 26.2.6 Disable the interface from sending packets

In a simple network, the interface of the OSPF protocol only represents a network segment between two devices, just to transmit data, then set the interface to passive state, blocking the broadcast of hello messages on its link, This does not affect learning about the interface route.

Mode: OSPF configuration mode

command : `passive-interface <if-name>`

Configure the interface to be passive

command : `no passive-interface <if-name>`

Cancel interface passive state

Parameters: if-name is the name of the layer 3 interface (for example: `vlan1` `vlan2...`)

Default: The interfaces enabled after OSPF protocol start are not in passive state

If the interface running the OSPF protocol is designated as passive, the directly connected routes of the interface can still be advertised, but OSPF packets on the interface will be blocked and the interface cannot establish neighbor relationships. In some networking situations, it can effectively save network resources.

## 26.2.7 Configure SPF calculation time

When the OSPF link state database LSDB changes, the shortest path needs to be recalculated. If the shortest path is calculated immediately after each change, it will occupy a lot of resources and affect the efficiency of the router. By configuring the delay and hold values to adjust the SPF calculation interval, you can suppress the excessively frequent SPF calculations caused by frequent network changes, thereby avoiding the concentration of a large amount of system resources at a time and affecting the router's operating efficiency.

The SPF calculation has a timer, and each time the next calculation is started according to the suppression time. When the timer expires and the SPF calculation needs to be started, recalculate the last SPF calculation to this suppression time. If the configured suppression time has been exceeded, the configured delay time is used to

|

---

start the timer. If the configured suppression time has not been exceeded, the configured suppression time is used to calculate the required delay time. If the delay time is less than the configured delay time, the configured delay time is used, otherwise the SPF calculation is started directly using the calculated delay time.

Mode: OSPF configuration mode

command : `timers spf <delay> <hold>`

Configure the delay and hold values of the SPF calculation interval

command : `no timers spf`

Restore to default

Parameters: delay means the time to delay when calculating SPF; hold means the time to be suppressed between two SPF calculations.

Default: delay is 5s; hold is 10 seconds

## 26.2.8 Configure management distance

The router can run multiple routing protocols at the same time. How to select among the routing information learned by multiple routing protocols requires the use of administrative distance. When different protocols find the same route, the administrative distance is small, which is preferred.

Mode: OSPF configuration mode

command : `distance <distance>`

Configure management distance

command : `no distance <distance>`

Restore the management distance to the default value

command : `distance ospf {intra-area <distance> | inter-area <distance> | external <distance>}`

Configure different types of management distance

|

---

command : no distance ospf

Restore the three types of management distance to default values

Parameters: The distance values range from 1~255 ; intra-area indicates the administrative distance of intra-area routing ; inter-area indicates the administrative distance of inter-domain routing ; external indicates the management distance of the external route.

Default: The management distance of OSPF protocol is 110 ; The management distance of intra-domain routing, inter-domain routing, and external routing is 0.

## 26.2.9 Import external routes

Multiple dynamic routing protocols can be run on the router, and routing information can be shared between different routing protocols. OSPF regards the routes learned by other routing protocols as routes outside the autonomous system and is introduced by the ASBR, the border router of the autonomous system. When importing external routes, attributes such as weight and weight type can be specified.

There are four types of OSPF routing, one is intra-domain routing, the other is inter-domain routing, both types of routes are within the autonomous system; the third is type-1 external routing, and the fourth is type-2 external routing Routing, these two types of routing describe routes to destinations outside the autonomous system. Type-1 routes are routes from other IGPs. OSPF believes that the credibility is relatively high and is comparable to the routing weights in the autonomous system. Therefore, the cost of this type of external routing is the cost of the router itself to ASBR and ASBR. The total cost to the destination. Type-2 routes are routes from other EGPs. OSPF believes that its credibility is not very high, and its cost is much greater than the routing cost in the autonomous system, which is not comparable. Therefore, the cost of this type of external routing only uses ASBR to the destination The cost of the ground, and ignore the cost of the router itself to the ASBR.

Mode: OSPF configuration mode

command : redistribute {kernel | connected | static | rip | isis | bgp} [metric <metric> |

|

---

metric-type <type> | route-map <route-map-name> | tag <tag>]

command : no redistribute {kernel | connected | static | rip | isis | bgp} [metric <metric>  
| metric-type <type> | route-map <route-map-name> | tag <tag>]

Parameters: The first required parameter is the type of external routes that can be imported, including direct connection, static, RIP, IS-IS, BGP ;The second parameter is the weight set when importing external routes, ranging from  $0\sim(2^{24}-1)$  ; the third parameter is the imported two types of external routes, divided into type-1 and type-2 , type-1 Route for IGP , type-2 is EGP routing ;The third parameter is the name of the referenced route-map. Route-map is configured in the global configuration mode, please refer to the command manual ; The fourth parameter is tag, with a value between  $0\sim(2^{32}-1)$  , which is an external routing attribute.

Default: do not import any external routing protocol

## 26.2.10 Configure the network type of the interface

The OSPF protocol is viewed from the perspective of its own router. Each router describes its adjacent network topology and passes it to other routers. OSPF divides the network types of interface links into four types according to the link layer protocol type: one is the broadcast type (the link layer protocol is Ethernet, FDDI etc); the second is the NBMA non-broadcast multiple access type (the link layer protocol is FR, ATM, HDLC, X.25 etc); The third is the point-to-multipoint type, and no link layer protocol will be considered as a point-to-multipoint type by default. The point-to-multipoint type must be forcedly configured by other network types. The most common approach is to change the non-fully connected NBMA to a point-to-multipoint network. Four is point-to-point type (link layer protocols are PPP, LAPB, POS)。

On a broadcast network without multiple access capabilities, the interface can be configured to NBMA type. When not all routers are directly reachable in the NBMA network, the interface can be configured as a point-to-multipoint type.

The NBMA network agreed in the OSPF protocol is fully connected, non-broadcast, and reachable at multiple points. Point-to-multipoint networks are not necessarily fully

|

---

connected. NBMA requires DR selection. There is no DR in point-to-multipoint networks. NBMA network multicasts packets by point-to-multipoint network by specifying neighbor unicast packets.

Mode: Interface configuration mode

command : ip ospf network <type>

Configure the network type of the interface link

command : no ip ospf network

Restore the network type of the interface link to the default

parameters : type can choose broadcast 、 non-broadcast 、 point-to-point 、 point-to-multipoint [non-broadcast] ; The first type is a broadcast network, and the second type is a non-broadcast network, which is NBMA , The third type is a point-to-point network , The fourth type is a point-to-multipoint network ; Point-to-multipoint networks are divided into broadcast and non-broadcast networks , Non-broadcast neighbors cannot be automatically discovered, and neighbors must be specified.

Default: broadcast network

## **26.2.11 Configure the interval for sending hello packets**

Hello messages are used to periodically send to neighbor routers, discover and maintain neighbor relationships, and elect DR and BDR. Hello message interval can be manually configured, but care should be taken to keep the hello timer interval between neighbors in the network the same. The value of the Hello timer is inversely proportional to the router convergence speed and network load.

Mode: Interface configuration mode

command : ip ospf hello-interval <seconds>

Configure the interval of the hello timer

|

---

command : no ip ospf hello-interval

Restore the hello timer interval to the default value

Parameter: The value of seconds ranges from 1~( $2^{16}-1$ ), indicating the time interval between two hello message transmissions.

Default: hello interval is 10 seconds on broadcast network and point-to-point network; hello interval is 30 seconds on NBMA network and point-to-multipoint network.

## 26.2.12 Configure the neighbor router expiration time

Mode: Interface configuration mode

command : ip ospf dead-interval <seconds>

Configure neighbor expiration time

command : no ip ospf dead-interval

Restore the neighbor failure time to the default value

Parameter: The value of seconds is between 1~( $2^{16}-1$ ), which means that the neighbor's hello message is not received after the second time, the neighbor is considered invalid; each time the hello message is received, the neighbor's dead timer is updated.

Default: neighbor failure time on broadcast networks and point-to-point networks is 40 seconds; neighbor failure time on NBMA networks and point-to-multipoint networks is 120 seconds; When the network type is modified, the default values for hello interval and dead interval will be used.

## 26.2.13 Configure retransmission time

OSPF is a reliable link-state protocol. The LSU packets that it interacts with require an LSU-ack from the peer. When the confirmation message is received, the party considers that the link status update is received. If no confirmation message is received within the retransmission interval, the LSA will be retransmitted to the neighbor. The retransmission interval can be manually configured. It needs to be longer than the time for

a packet to be transmitted between two routers. If the setting is too small, it will cause unnecessary retransmissions.

Mode: Interface configuration mode

command : ip ospf retransmit-interval <seconds>

Configure the interface retransmission interval

command : no ip ospf retransmit-interval

Restore the retransmission interval to the default value

Parameter: The value of seconds ranges from 1~( $2^{16}-1$ ), indicating the interval between retransmissions when the LSA is not received by the peer.

Default: retransmission interval 5s

## 26.2.14 Configure interface delay

Each link state broadcast LSA in the link state update message LSU has an age time field. It is necessary to increase the transmission delay of the sending interface before transmission. This parameter mainly considers the time required for the interface to send packets, especially on low-speed networks, it is necessary to consider configuring this parameter.

Mode: Interface configuration mode

command : ip ospf transmit-delay <seconds>

Set the transmission delay of the interface

command : no ip ospf transmit-delay

Restore the transmission delay of the interface to the default value

Parameter: The value of seconds ranges from 1~( $2^{16}-1$ ), indicating that the age field of the LSA sent on this interface needs to increase this delay value.

Default: the transmission delay of the interface is 1s

---

## 26.2.15 Configure the priority of the interface in DR election

In order to avoid repeated point-to-point transmission of link information in the broadcast network, it is necessary to elect designated routers DR and BDR to be responsible for link information within the broadcast network segment. The priority of an interface indicates its qualifications for DR election. When there is a conflict in the election, the highest priority is considered first. The priority of 0 does not participate in the election, the priority is greater than 0 are candidates, each router contains its own priority information and DR in its own hello message, broadcast in the broadcast network, and finally choose the priority Become DR. If the priority is equal, the router ID with the highest priority will take precedence.

When the DR fails, the router in the network needs to go through a process of re-election of DR, which takes a period of time and will cause routing calculation errors during this period. The concept of BDR is to smoothly transition to the new DR. BDR is a backup of DR. It is selected at the same time in DR election. It also establishes adjacency relationship with other routers in the network. However, the information collection and publishing node in the network is in DR instead of BDR. BDR only maintains the synchronization of adjacency. When the DR fails, the BDR will immediately become the DR, which is responsible for collecting information within the network segment, and at this time, a new process will be initiated to elect the BDR, but the election of the BDR does not affect the calculation of the route.

Mode: Interface configuration mode

command : ip ospf priority <prio>

Configure the priority of the interface in DR election

command : no ip ospf priority

Restore interface priority to default

Parameters: The value of prio ranges from 0~255 , which indicates the priority in DR selection.

Default: priority is 1

---

## 26.2.16 Configure the cost of sending packets on the interface

The network controls traffic by configuring different costs for different links. The cost of an interface represents the cost of sending packets from that interface. If not manually configured, OSPF will automatically calculate the interface cost based on the interface baud rate.

Mode: Interface configuration mode

command : ip ospf cost <cost>

command : no ip ospf cost

Parameters: cost ranges from 1~( $2^{16}-1$ ), indicating the substitute value of packets sent on this interface.

Default: interface cost 10

## 26.2.17 Configure whether the interface sends DD packets to fill the MTU field

Mode: Interface configuration mode

command : ip ospf mtu-ignore

Set not to check mtu value in DD message

command : no ip ospf mtu-ignore

Cancel do not check mtu value in DD message

Default: check mtu value in DD message

## 26.2.18 Configure interface packet authentication

OSPF protocol packet authentication on the interface supports plain text mode and MD5 mode.

Mode: Interface configuration mode

|

---

command : ip ospf authentication <mode>

Configure authentication mode

command : no ip ospf authentication

Cancel certification

Parameter: No parameter means clear text authentication;message-digest means MD5 authentication;null means no authentication

command : ip ospf authentication-key <password>

Configure clear text authentication password string

command : no ip ospf authentication-key

Cancel clear text authentication password string

Parameters: password represents the password string for clear text authentication

command : ip ospf message-digest-key <key-id> md5 <password>

Configure MD5 authentication password

command : no ip ospf message-digest-key <key-id>

Cancel MD5 authentication password

Parameters: The value of key-id is between 1~255, which is used to sort in the key chain; password represents the password string.

Default: no authentication is configured

## 26.2.19 Configure area virtual links

The OSPF protocol uses a hierarchical idea to divide the routers in the autonomous system into different groups. These groups are called areas. All areas are not equal, but have a hierarchical relationship. Among them, the 0.0.0.0 area is the most special and is the backbone area. In other non-backbone areas, inter-domain routes must be exchanged through the backbone area. Therefore, all non-backbone areas must be connected to the backbone area, that is, at least one interface on the ABR is in area 0. If due to network topology limitations, some areas cannot guarantee physical access to the backbone area,

then a virtual link needs to be configured to ensure logical access. Both ends of the virtual link are ABR, and the middle passes a non-backbone area, which is called the transit area. When configuring a virtual link, you need to specify the ID of the transmission area and the ID of the peer ABR, and they must be configured on the ABR at both ends to take effect.

When the routing of the transmission area is calculated, the virtual link is activated, which is logically equivalent to forming a point-to-point connection between the two endpoints, so you can configure interface parameters and start authentication on its physical interface Features.

Unicast messages are transmitted between ABRs. Routers that forward the unicast messages in the transmission area treat them as ordinary IP packets to forward. Therefore, it can only be understood that a logical link is provided in the transmission area. Two ABRs Protocol messages can be exchanged between.

Mode: OSPF configuration mode

command : area <area-id> virtual-link <router-id>

Configure the transmission area and peer ID of the virtual link

[authentication <mode> |

Configure the authentication mode of the virtual link

authentication-key <password> |

Configure the clear text authentication password for the virtual link

message-digest-key <key-id> md5 <password> |

Configure virtual link MD5 authentication password

hello-interval <seconds> |

Configure the hello interval of the virtual link

dead-interval <seconds> |

Configure Virtual Link Neighbor Failure Time

retransmit-interval <seconds> |

Configure the virtual link retransmission interval

transmit-delay <seconds> |

Configure the virtual link interface delay

command : no area <area-id> virtual-link <router-id>

[authentication <mode> |

authentication-key <password> |

message-digest-key <key-id> md5 <password> |

hello-interval <seconds> |

dead-interval <seconds> |

retransmit-interval <seconds> |  
transmit-delay <seconds>]

Cancel virtual link settings

Parameters: area-id indicates the ID of the transmission area. You can use the dotted decimal format A.B.C.D, or you can use the integer format, ranging from 0~( $2^{32}-1$ ).  
router-id indicates the ID of the peer router of the virtual link, using the A.B.C.D format. Both authentication and sending interface attributes are optional, please refer to the relevant command description.

Default: no virtual link is configured

## 26.2.20 Configure regional route aggregation

Mode: OSPF configuration mode

command : area <area-id> range <ip-prefix> [advertise | not-advertise]

Configure aggregation scope

command : no area <area-id> range <ip-prefix> [advertise | not-advertise]

Cancel aggregation

Parameters: area-id indicates the area ID, which specifies the aggregation of the routes in the area, you can use the dotted decimal format A.B.C.D, or you can use the integer format, ranging from 0~( $2^{32}-1$ ).ip-prefix uses the prefix format A.B.C.D/M to indicate the aggregation range. The optional parameters advertise and not-advertise indicate whether to broadcast the aggregation range, that is, ip-prefix. The original network route will be broadcast.

## 26.2.21 Configure regional message authentication

The authentication types of all routers in an area must be consistent. The authentication password strings of all routers in a network segment must be consistent. The configuration area authentication only starts the authentication function (clear text or MD5), and the password uses the corresponding configuration value of the interface. Refer to interface message authentication configuration.

Mode: OSPF configuration mode

|

---

command : area <area-id> authentication [message-digest]

Configure regional authentication mode

command : no area <area-id> authentication

Cancel regional certification

Parameters: area-id indicates the area ID and specifies the area to be authenticated; dotted decimal format A.B.C.D can be used, or integer format can be used, ranging from 0~(2<sup>32</sup>-1).

The optional parameter none indicates plain text authentication, and message-digest indicates MD5 authentication.

Default: Do not start regional authentication

## 26.2.22 Configure stub area

Mode: OSPF configuration mode

command : area <area-id> stub [no-summary]

Configure the router in the stub area

command : no area <area-id> stub [no-summary]

Cancel the attribute of the router in the stub area

command : area <area-id> default-cost <cost>

Configure the default cost of the ABR broadcast route connected in the stub area

command : no area <area-id> default-cost

Restore the default cost to the default value

Parameters: area-id indicates the area ID, indicating which area attribute is a stub; you can use the dotted decimal format A.B.C.D, or you can use the integer format, the value is between 0~(2<sup>32</sup>-1).no-summary means not to inject inter-domain routes into the stub area.

The first set of commands is to configure the router located in the stub area, and the second set of commands is to configure the ABR with the interface connected to the stub area.

Default: no stub area is configured

---

## 26.2.23 Configuring the nssa area

Mode: OSPF configuration mode

command : area <area-id> nssa [options]

Configure nssa attributes

command : no area <area-id> nssa [options]

Cancel nssa area attribute

Parameters: area-id indicates the area ID. For options, see the command manual.

Default: Do not configure nssa area

## 26.2.24 Configure external route aggregation

Routes imported from other protocols are broadcast one by one in the type-5 LSU. Use the aggregation command to specify a prefix range. The routes covered in this range are suppressed, and only the aggregated route is broadcast. When the number of external routes is huge, it can effectively reduce the size of LSDB.

Mode: OSPF configuration mode

command : summary-address <ip-prefix> [not-advertise | tag <tag>]

Configure aggregation scope and attributes

command : no summary-address <ip-prefix> [not-advertise | tag <tag>]

Cancel external route aggregation

Parameters: ip-prefix uses the address prefix format ABCD/M to indicate the range of routes that need to be aggregated; not-advertise indicates that the aggregated route will not be broadcast; tag is the set tag value, which ranges from 0~(2<sup>32</sup>-1), The default is 0.

Default: Do not aggregate external imported routes

## 26.2.25 Configuring the Default Weight of External Routes

When importing external routes, if the redistribute command does not specify a metric value, the default weight value is used.

Mode: OSPF configuration mode

command : default-metric <metric>

Configure the default metric when importing external routes

command : no default-metric [metric]

When importing external routes, the default weight is the default value

Parameter: metric value is between  $0 \sim (2^{24} - 1)$

Default: The default weight is 1

## 26.2.26 Display information

Mode: normal mode or privileged mode

command : show ip protocols

command : show ip protocols ospf

Display OSPF protocol information

command : show ip ospf [process-id]

Display OSPF process information

Parameters: instance-id is the process ID,

The value ranges from  $0 \sim (2^{16} - 1)$

command : show ip ospf border-routers

Display ABR information

command : show ip ospf database <type>

Display LSDB information

Parameters: type is LSA of various types and summary information, please refer to the command manual for details.

command : show ip ospf interface [if-name]

Display OSPF interface information

Parameters: if-name is the agreed layer 3 interface name

command : show ip ospf route [count]

Display OSPF routing table

Parameter: count indicates the total number of entries in the routing table.

command : show ip ospf virtual-links

Display OSPF virtual link information

command : show ip ospf neighbor [options]

Display OSPF neighbor information

Parameters: options see command manual

Mode: Privileged mode

mode : show running-config

Display the current configuration of the switch, including OSPF configuration.

command : show running-config ospf

Display the current configuration of the OSPF protocol,

## 26.3 OSPF configuration example

### (1) configuration

The three switches are connected in pairs, and each has 6 network segments, all of which enable the OSPF protocol, so that the three PCs can communicate with each other. The interface is required to be in the same area area 0.

On switch 1上 :

```
Switch#configure terminal
```

```
Switch(config)#router ospf 100
```

```
Switch(config-ospf-100)#network 10.1.1.0/24 area 0
```

```
Switch(config-ospf-100)#network 10.1.2.0/24 area 0
```

```
Switch(config-ospf-100)#network 192.168.1.0/24 area 0
```

On switch 2 :

```
Switch#configure terminal
```

```
Switch(config)#router ospf 100
```

```
Switch(config-ospf-100)#network 10.1.2.0/24 area 0
```

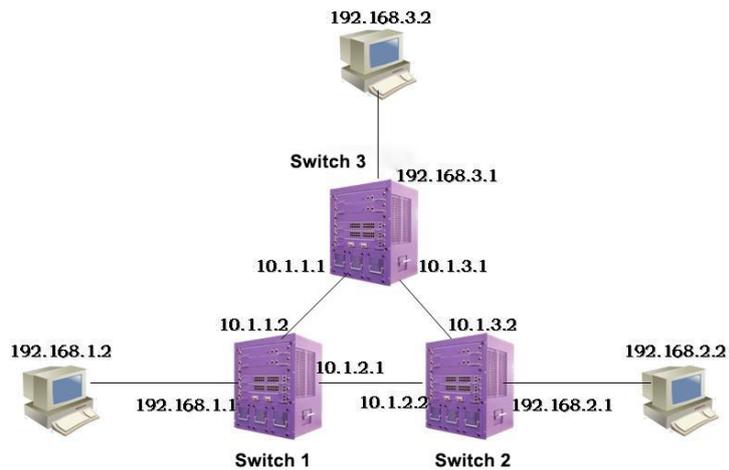
```
Switch(config-ospf-100)#network 10.1.3.0/24 area 0
```

```
Switch(config-ospf-100)#network 192.168.2.0/24 area 0
```

On switch 3 :

```
Switch#configure terminal
```

```
Switch(config)#router ospf 100
Switch(config-ospf-100)#network 10.1.1.0/24 area 0
Switch(config-ospf-100)#network 10.1.3.0/24 area 0
Switch(config-ospf-100)#network 192.168.3.0/24 area 0
```



## (2) verification

```
show ip ospf database
show ip ospf interface
show ip ospf neighbor
show ip route ospf
show ip ospf route
```

---

# Chapter27 VRRP configuration

---

This chapter mainly includes the following: :

- VRRP introduction
- VRRP configuration
- VRRP configuration example

## 27.1 VRRP introduction

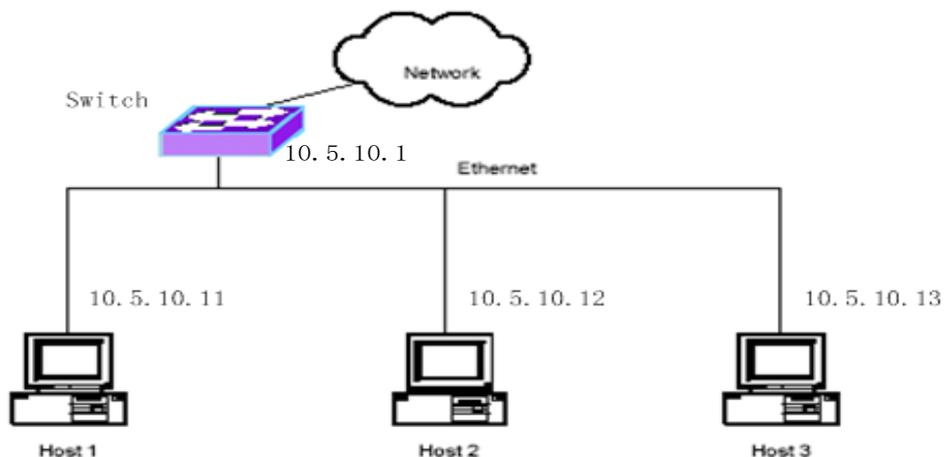
VRRP is the abbreviation of Virtual Router Redundancy Protocol and is an important Layer 3 reliability protocol used for redundant backup of the default gateway. This section gives a detailed description of the VRRP protocol, mainly including the following :

- VRRP Overview
- VRRP terminology
- VRRP protocol interaction
- Virtual master router election
- Virtual router status

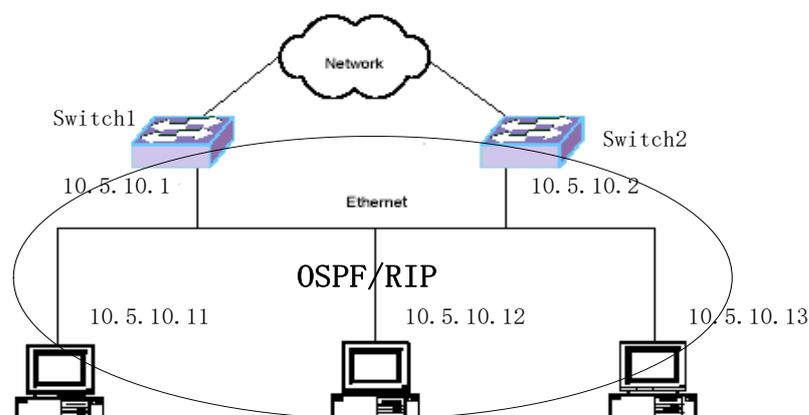
- VRRP tracking

## 27.1.1 VRRP Overview

The following figure is a typical intranet networking solution. One interface of the switch is connected to the external network, and 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 hosts 1, 2, and 3 are all configured with IP addresses, all on the network segment 10.5.10.0/24. A default gateway is configured on hosts 1, 2, and 3, the next hop points to the switch, and the IP address of the next hop is 10.5.10.1. In this way, the host sends a packet whose destination IP address is not in this network segment will match the default route and send it to the switch. The switch then forwards the packet out, and the switch also forwards the packet sent from the external network to the corresponding host. This allows the host to 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. When the switch fails, all the hosts are interrupted from the outside. In order to solve this problem, there is a solution to expand a switch to two or more switches, running the dynamic routing protocol OSPF or RIP between the host and the switch, as shown below.



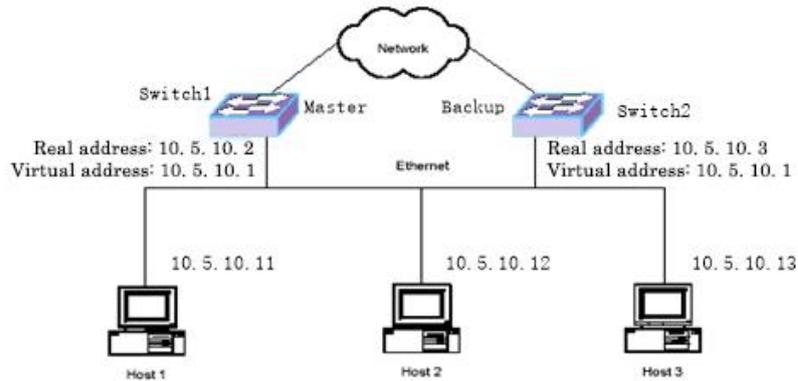
|

---

After the host runs the dynamic routing protocol, the host can learn all the routes of the external network. When communicating with the external network, the host searches for the route according to the destination IP address of the packet and obtains the next hop to determine whether the packet is sent to switch1. Still switch2. When one of the switches fails, the route in the host can be re-learned within a short time, and the next hop of the route will point to the router without the failure, so that the communication between the host and the external network will not be interrupted.

However, it is unrealistic to implement a dynamic routing protocol on the host. For hosts, the load of running dynamic routing protocols is too large. For the network, running dynamic routing protocols on the hosts will cause excessive unnecessary data traffic on the network, and some hosts do not support dynamic routing protocols at all.

In order to fundamentally solve this single point of failure, the VRRP protocol is the best choice. The VRRP protocol was specifically proposed for this problem. As shown in the following figure, Switch1 and Switch2 form a virtual router. The real IP addresses of the interfaces of the two switches are different, but there is a common virtual IP address 10.5.10.1, and the default gateway of the host is set to the virtual IP address 10.5. 10.1. When Switch1 is a virtual master switch, the communication between the host and the external network is forwarded through Switch1, but when Switch1 fails, Switch2 takes over Switch1 as the virtual master switch, and the communication between the host and the external network is forwarded through Switch2. Using VRRP protocol, the host only needs to set the default gateway, and does not need to run other protocols on the host, the load of the host is small, and only a small amount of VRRP protocol flow needs to be added on the network.



## 27.1.2 VRRP terminology

Here are a few frequently used terms :

### 1 ) VRRP

Abbreviation of Virtual Router Redundancy Protocol, which is a fault-tolerant protocol of the default gateway, which can improve the reliability of the network.

### 2 ) Virtual Router

Virtual router, an abstract object, based on the subnet interface, including a virtual router identifier (VRID) and an IP address, this IP address(s) is also called a virtual IP address, and the virtual IP address is used as the default gateway of the host.

### 3 ) VRRP Router

VRRP router, that is, a router running the VRRP protocol, a VRRP router can be added to a virtual router.

### 4 ) IP Address Owner

IP address owner, VRRP router whose virtual IP address is the same as the real IP address of the interface.



|

---

Source MAC address: The virtual MAC address of the virtual router is 00-00-5e-00-01-{VRID}, VRID is the virtual router identifier. For example, the VRID of the virtual router is 1, and the virtual MAC address is 00-00-5e-00-01-01.

Destination MAC address: VRRP multicast MAC address, which is 01-00-5e-00-00-12.

## 2 ) IP header field of VRRP packet

Source IP address: The primary IP address of the interface that sends VRRP packets.

Destination IP address: The multicast IP address is 224.0.0.18 and cannot be forwarded at Layer 3.

TTL: 255, in order to prevent remote VRRP packet attacks.

Protocol: 112.

## 3 ) VRRP header field

Version : 2.

Type: The type of VRRP packet. Only one type is supported: 1 --- ADVERTISEMENT, VRRP notification packet.

VRID: Identifies a virtual router.

Priority: For this virtual router, the priority of the VRRP router sent.

Count IP Adrs: The number of virtual IP addresses. A virtual router can have multiple virtual IP addresses.

Auth Type: An authentication method between VRRP routers in a virtual router.

Advertisement Interval: Advertisement interval, the default is 1 second.

Checksum: Checksum, calculated from the Version of the VRRP header.

IP Address(es): One or more virtual IP addresses.

Authentication Data: authentication data.

## 4 ) VRRP priority

Each VRRP router in a virtual router needs to be configured with a priority. The priority ranges from 0 to 255, of which 0 and 255 have special purposes. The configurable priority ranges from 1 to 254, and the default is 100. The larger the priority value, the higher the

priority, and the more likely it becomes a virtual master router.

When a VRRP router is the IP address owner in a virtual router, its priority is 255.

When the virtual master router needs to notify other backup routers that it is no longer the master, it sends a VRRP packet with a priority of 0 to the other backup routers, which can quickly trigger other backup routers to become virtual master routers.

#### 5 ) VRRP certification

The VRRP protocol provides three authentication methods. In actual use, different authentication methods can be selected according to the security requirements of the network.

0 --- No Authentication

No certification

1 --- Simple Text Password

Simple password authentication

2 --- IP Authentication Header

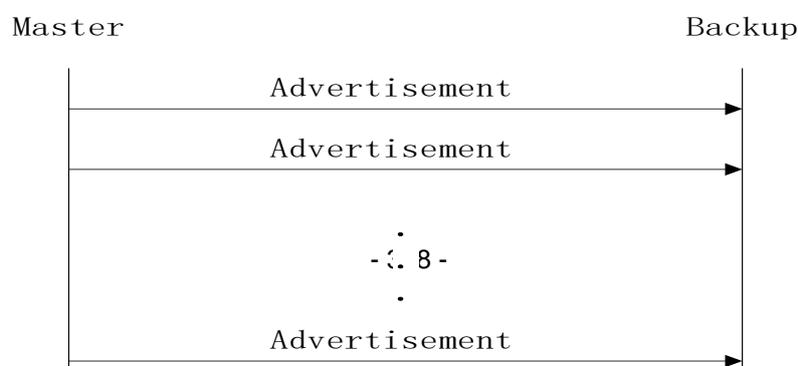
IP authentication header, through the HMAC-MD5 method to calculate the message digest.

You can use no authentication or simple password authentication method in the network with low security, HMAC authentication method in the network with high security.

For the 0 and 2 authentication methods, the Authentication Data field is filled with 0, and for the 1 authentication method, the Authentication Data field is filled with the password. For the 2 authentication method, the message digest is filled in the IP Authentication Header field, which means that the AH field is added to the IP header.

#### 6 ) VRRP packet interaction

The VRRP protocol has only one type of packet, the ADVERTISEMENT announcement packet. In a virtual router, the virtual master router sends an advertisement packet every Advertisement Interval time (default is 1 second). The virtual backup router decides whether state transition is required based on the received VRRP advertisement packet. The interaction between the master and backup protocol is shown in the figure below:



---

## 27.1.4 Election of Virtual Master Router

The selection of a 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 is working properly, it is the virtual master router.

- VRRP priority

The VRRP router with the highest priority working properly becomes the virtual master router. The configurable priority range is from 1 to 254. The priority of the IP address owner's router is 255. When the virtual master router informs the virtual backup router that it is no longer the master, a priority of 0 is given in the VRRP packet.

- The actual IP address size of the interface. When the priority is the same, the VRRP router with the larger actual IP address of the interface becomes the virtual master router.

In the following cases, the master-slave switchover will occur in the virtual router:

1 ) When the virtual master router fails, there will be a master-slave switchover. In this case, there are two possibilities:

- If the virtual master router is still active, it will send a VRRP packet with priority 0. After receiving this packet, the backup router will switch to the virtual master router if it does not receive the VRRP packet of the virtual master router within `Skew_Time`. In this case, the switching speed is relatively fast, and the switching can be achieved within 1 second.

- If the virtual master router cannot be active, the virtual backup router will switch to the virtual master router after not receiving the VRRP packet of the virtual master router within the Master Down Interval time.

$$\text{Master\_Down\_Interval} = (3 * \text{Advertisement\_Interval}) + \text{Skew\_Time}$$

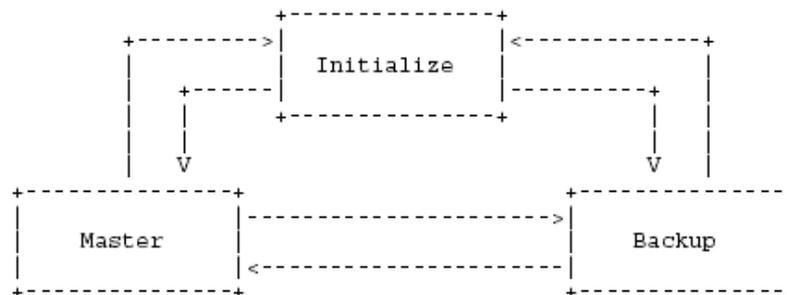
$$\text{Skew\_Time} = ((256 - \text{Priority}) / 256)$$

2 ) When the virtual master router is not the IP address owner, and now a router with the IP address owner joins the network, this router will become the virtual master router, and the master-standby switchover will occur.

3 ) When a VRRP router joins the network, if the priority of the router is higher than the virtual master router and is in preemptive mode (the configuration variable Preempt\_Mode is TRUE), the router will become the virtual master router, and the master-standby switchover occurs.

## 27.1.5 Status of Virtual Router

Each VRRP router in a virtual router executes a state machine. The migration of the state machine is as follows:



### 1 ) Initialize status

The Initialize state is the initial state of a virtual router. In this state, it waits for the startup event. If the Startup event is received in this state, the processing is as follows :

- If the priority of this VRRP router is 255 (that is, the IP address owner), the router becomes the virtual master router and moves to the Master state.

Otherwise, the router becomes a virtual backup router and moves to the Backup state.

After the router moves to the Master state, the actions are as follows :

- Send a VRRP announcement packet.
- Broadcast an ARP request, including virtual IP address and corresponding virtual MAC address.

- Set the Advert\_Timer timer, the interval is Advertisement\_Interval.

The actions that the router does after moving to the Backup state are as follows :

- Set the Master\_Down\_Timer timer, the timing interval is Master\_Down\_Interval.

## 2 ) Backup status

The purpose of the backup state is to monitor the availability and status of the virtual master router and take over the work of the virtual master router at any time.

If a Shutdown event is received, cancel the Master\_Down\_Timer timer and return to the Initialize state.

If the Master\_Down\_Timer expires, it becomes a virtual master router and transitions to the Master state.

If you receive a VRRP announcement packet, there are the following situations:

- If the priority field in the VRRP packet is 0, set Master\_Down\_Timer, and the timing interval is Skew\_Time.
- Otherwise, if the preemption mode (Preempt\_Mode) is FALSE or the priority in the VRRP packet  $\geq$  the priority of the VRRP router, reset the Master\_Down\_Timer and the timing interval to Master\_Down\_Interval.
- Otherwise, discard the VRRP packet.

## 3 ) Master status

The VRRP router in the Master state is responsible for forwarding Layer 3 data packets passing through the virtual router.

If a Shutdown event is received, cancel the Advert\_Timer timer, send a VRRP notification packet with priority 0, and move to the Initialize state.

If the Adver\_Timer timer expires, send a VRRP announcement packet to reset the Adver\_Timer timer.

If you receive a VRRP announcement packet, there are the following situations:

- If the priority in the packet is 0, send a VRRP announcement packet and reset the Advert\_Timer.
- Otherwise, if the priority in the packet is greater than the priority or the same priority of the VRRP router, but the IP address of the packet is greater than the main IP address of the interface of the VRRP router, cancel the Adver\_Timer timer, set the

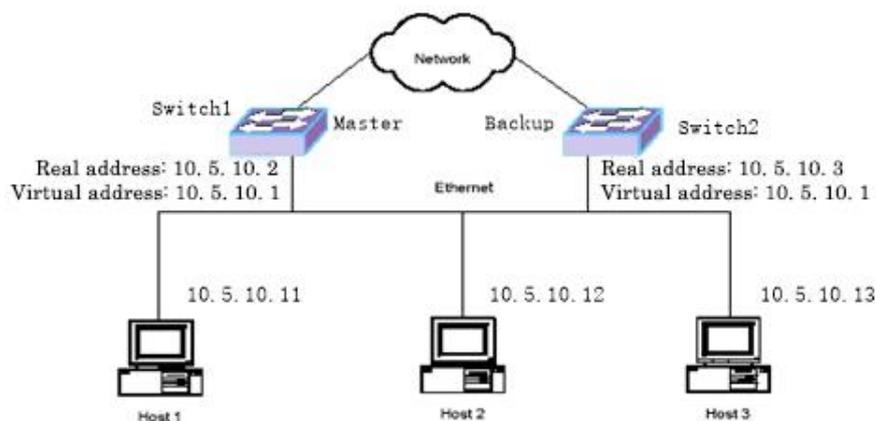
Master\_Down\_Timer, and move to the Backup state.

- Otherwise, discard the VRRP advertisement packet.

## 27.1.4 VRRP tracking

The VRRP protocol itself can only detect failures inside the virtual router, such as the interface where the virtual router is located, LINK DOWN, or the VRRP router crashes, etc., but cannot detect failures outside the virtual router. When a fault occurs outside the virtual router, the virtual router cannot select the virtual master router based on these faults, which will cause interruption of network data. VRRP tracking can solve this problem. The VRRP router tracks the specified external events. When an external failure occurs, the VRRP router changes its running priority and reselects the virtual master router to ensure that the network data is not interrupted.

As shown in the figure below, when the external interface of the virtual master router Switch1 is LINK DOWN, if VRRP tracking is not enabled, Switch1 continues to be the virtual master router, and the host cannot access the external network. If the VRRP tracking function is enabled, Switch1 can detect external faults, and modify its own running priority, re-select the virtual master router, Switch1 changes to a virtual backup router, Switch2 changes to a virtual master router, so that the host can continue to access the external network.



VRRP tracking includes three types: interface tracking, route tracking and PING tracking. Interface tracking is that the VRRP router tracks the external interface of the virtual router. If a tracked interface is LINK DOWN, it indicates that an external fault has occurred. Route tracking is that the VRRP router tracks the routes in the routing table that it has learned. If the route does not exist or the route exists but is not active, it indicates that an external fault has occurred. PING tracking is a device where the VRRP router has

been PING being tracked. If there is no PING response within the specified time, it indicates that an external fault has occurred. The virtual router can track the interface, routing and PING at the same time. For each type of tracking, it can also track multiple events. As long as one of the tracked events fails, it indicates that the virtual router has an external failure, and only all of them are tracked. The event is normal, only to indicate that the virtual router has no external faults.

## 27.2 VRRP configuration

VRRP configuration includes the following: :

- Create and delete virtual routers
- Configure the virtual IP address of the virtual router
- Configure the parameters of the virtual router
- Configure VRRP tracking
- Start and close the virtual router
- View VRRP information

### 27.2.1 Create and delete virtual routers

The virtual router is built on the subnet interface and needs to specify a VRID. The system does not create a virtual router by default.

When a virtual router is no longer needed, the virtual router can be deleted. If the virtual router has already been started, the virtual router will be shut down first, and then the virtual router will be deleted.

The commands to create and delete virtual routers are as follows:

| command            | description   | CLI mode                  |
|--------------------|---|---------------------------|
| router vrrp <vrid> | Create a virtual router and enter the VRRP configuration mode. If the virtual router already exists, enter the VRRP configuration mode directly. The parameter is VRID, | Global configuration mode |

|                       |  |                           |
|-----------------------|--|---------------------------|
|                       | ranging from 1 to 255.                         |                           |
| no router vrrp [vrid] | Delete a virtual router, the parameter is VRID | Global configuration mode |

## 27.2.2 Configure the virtual IP address of the virtual router

A virtual IP address must be configured on the virtual router. In theory, one or more virtual IP addresses can exist in a virtual router, but a virtual router only supports one virtual IP address when the switch is implemented. By default, the switch is not configured with a virtual IP address.

The command to configure the virtual IP address of the virtual router is as follows :

| command                                      | description  | CLI mode                |
|--|--|-------------------------|
| virtual-ip <virtual-ip><br><backup   master> | Set the virtual IP address of the virtual router.    | VRRP configuration mode |
| no virtual-ip                                | Delete the virtual IP address of the virtual router. | VRRP configuration mode |

note :

- The configuration of the virtual IP address of the virtual router must be successful when the virtual router has been shut down, but cannot be configured successfully when the virtual router is started.
- The virtual IP address must be on the same network segment as the main IP address of the interface, otherwise the configuration is unsuccessful.

## 27.2.3 Configure the parameters of the virtual router

The parameters of the virtual router include priority, preemption mode, advertisement interval, authentication method and authentication data. These parameters have default values, as shown in the following table :

| Parameter             | Default          |
|-----------------------|------------------|
| Priority              | 100              |
| Preemption mode       | TRUE             |
| Notification interval | 1 second         |
| Authentication method | No certification |
| Authentication data   | none             |

During configuration, for the virtual router, the advertisement interval, authentication method and authentication data must be configured the same, and the priority and preemption mode parameters can be configured the same.

The priority is divided into configuration priority and operation priority. In most cases, the operation priority uses the configuration priority, but when the VRRP router is the IP address owner, the operation priority is 255, and the configuration priority is not used. level.

As for the authentication method, the switch currently only implements two methods of no authentication and simple password authentication, but not the IP authentication header method.

The commands to configure the parameters of the virtual router are as follows:

| command                           | description   | CLI mode                |
|-----------------------------------|---|-------------------------|
| priority < priority-value >       | Set the priority of the virtual router. The priority ranges from 1 to 254.                        | VRRP configuration mode |
| preempt-mode {false   true}       | Set the preemption mode of the virtual router, TRUE means preemption, FALSE means not preemption. | VRRP configuration mode |
| advertisement-interval <interval> | Set the advertisement interval of the virtual router, ranging from 1 to 255, in seconds.          | VRRP configuration mode |
| authentication none               | Set the authentication method of the virtual router   | VRRP configuration mode |

|   |  |                         |
|---|--|-------------------------|
|   | to no authentication.  |                         |
| authentication<br>simple-password <key> | Set the authentication method of the virtual router to simple password authentication, and set the authentication data, that is, the password. | VRRP configuration mode |

mote :

- The configuration of the virtual router's parameters must be successful when the virtual router has been shut down, but cannot be successfully configured when the virtual router is started.

## 27.2.4 Configure VRRP tracking

At present, the switch only implements the VRRP interface tracking function. The VRRP router can track an interface, and the interface can be a Layer 2 interface or an aggregate interface. The switch does not configure the tracked interface by default.

If the VRRP router is the IP address owner, the administrator can configure VRRP tracking, but in reality VRRP tracking will not take effect, which means that even if the virtual router has an external failure, it will not re-select the virtual master router. If you want to use the VRRP tracking function, do not configure the virtual router as the IP address owner.

When the administrator configures VRRP tracking, specifies the one to be tracked, and starts the virtual router, VRRP tracking starts to take effect. When the VRRP router finds a tracked interface LINK DOWN, it is considered that an external failure has occurred, and the virtual router's operation priority is set to the source priority minus the priority-value value. Through the interaction of the VRRP protocol package, the virtual master can be reselected router. When the tracked interfaces are all LINK UP, the fault is recovered, and the operation priority of the virtual router is reset to the configuration priority.

The commands to configure VRRP tracking are as follows:

| command                    | description  | CLI mode                |
|----------------------------|--|-------------------------|
| circuit-failover <if-name> | Set the interface to be tracked by the virtual router. | VRRP configuration mode |

|                     |  |                         |
|---------------------|--|-------------------------|
| <priority-value>    |  |                         |
| no circuit-failover | Clear the tracked interface of the virtual router. | VRRP configuration mode |

note:

Configuring VRRP tracking must be successful when the virtual router has been turned off, but cannot be successfully configured when the virtual router is started.

## 27.2.5 Start and shut down the virtual router

After the virtual router is created and the virtual IP address and parameters are set, the virtual router is not actually running and is still in the Initialize state. Starting the virtual router will start the operation of the protocol, send a Startup event to the protocol, and the state machine transitions to the Master state or the Backup state. Shutting down the virtual router will shut down the operation of the protocol, send a Shutdown event to the protocol, and the state transitions back to the Initialize state.

Before starting the virtual router, you must ensure that the virtual IP address has been configured. When the virtual router is started, if you need to modify the virtual IP address or parameters, you must first shut down the virtual router and then configure it. After the configuration is complete, start the virtual router.

The commands to start and close the virtual router are as follows :

| command | description                  | CLI mode                |
|---------|------------------------------|-------------------------|
| enable  | Start the virtual router.    | VRRP configuration mode |
| disable | Turn off the virtual router. | VRRP configuration mode |

## 27.2.6 View VRRP information

You can view the running status information and configuration information of VRRP through commands. The commands to view VRRP information are as follows :

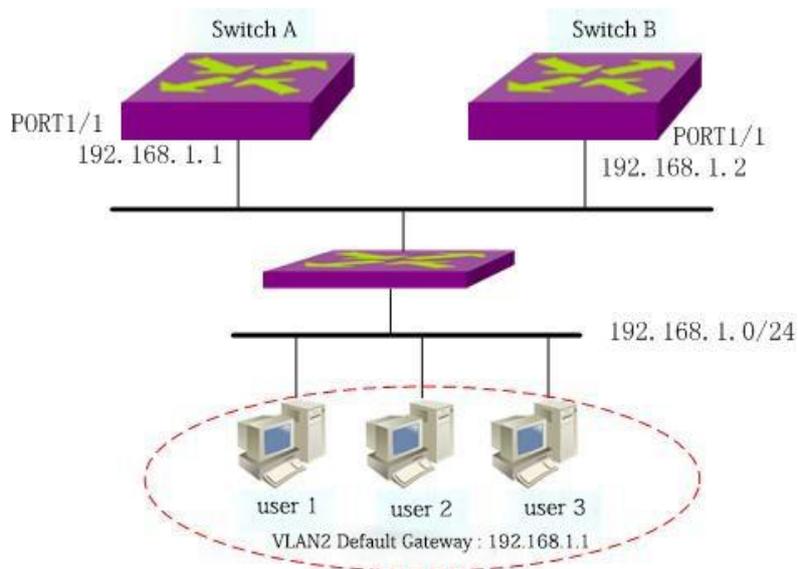
| command | description | CLI mode |
|---------|-------------|----------|
|---------|-------------|----------|

|                     |  |                                 |
|---------------------|--|---------------------------------|
| show vrrp [vrid]    | If no parameters are entered, all virtual router information is displayed.         | Normal mode,<br>Privileged mode |
| show running-config | View the current configuration of the system, you can view the VRRP configuration. | Privileged mode                 |

## 27.3 VRRP configuration example

### (1) configuration

Enable the VRRP function on the two switches to provide users in the LAN with a three-layer routing redundancy function to eliminate routing failures in the network, set switch 1 as the master switch, and switch 2 as the 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-ip 192.168.1.1 master
Switch(config-vrrp)#enable
```

Configuration on Switch B :

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#ip interface vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.2/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 backup
Switch(config-vrrp)#enable vrrp
```

## **(2) verification:**

Use the following command to view VRRP information :

```
show running-config
show vrrp
show vrrp 1
```

---

## Chapter28 **Configure VLLP**

---

This chapter mainly includes the following:

- VLLP introduction
- VLLP configuration
- VLLP configuration example

---

## 28.1 VLLP introduction

VLLP (VRRP Layer-2 Loop Protect Protocol) is a private protocol proposed to solve the problem of Layer 2 loops in the application of VRRP protocol. When using two Layer 3 switches to implement virtual routing redundancy backup, a loop will be formed between the Layer 3 switch and the Layer 2 switch. The VLLP protocol communicates with each other through the message to notify each other of the port status on their respective links and calculates The loop cuts the loop by setting the status of a specific port to block. The port set to the block state will be reset to the forward state if the timer expires. The VLLP protocol monitors and maintains the loop status of the port by immediately notifying the port status change and timer timeout, and ensures that the loop is cut off in time. The VLLP protocol uses query-response to collect port status information. When two Layer 3 switches running the VLLP protocol are started, they will automatically elect one in the sender state and the other in the receiver state. The sender is responsible for sending the query message regularly, and the receiver sends back the reply message after receiving the query message. When the receiver has a port state change, it needs to actively send a link state change message to notify the sender to make the corresponding change. The VLLP protocol needs to work in conjunction with the VRRP protocol to start and maintain the relevant port status in the VLAN. The VLLP protocol only needs to run on the VRRP switch, while the Layer 2 switch does not need to run any loop protection protocol.

Basic concepts of VLLP protocol:

VLLP device: A VLLP protocol entity running on a vlan is called a VLLP device.

VLLP port: a port that participates in VLLP protocol interaction in the vlan corresponding to the VLLP device.

VLLP device status: VLLP device has two states: sender and receiver.

Sender: The VLLP device in the sender state actively sends VLLP query messages periodically.

Receiver: The VLLP device in the receiver state answers the query message; when the link state changes, it actively sends the VLLP link state change message.

VLLP port status: VLLP port has three STP statuses: disable, block and forward.

Main port: When the VLLP device is in the sender state, it elects a VLLP port as the main port; a VLLP sender has only one main port. A VLLP port with a high priority and a mapping relationship can be preempted and become the master port.

VLLP port mapping relationship: There are VLLP ports that exchange VLLP protocol packets with the peer switch.

VLLP equipment receiver election principles:

1. The recipient with the highest priority becomes the receiver;
2. The priority is the same, and the MAC address with the largest becomes the receiver.

Principles for selecting the main port:

1. The port must be link up
2. There must be a mapping relationship between VLLP ports

If there is no VLLP port that meets the condition, the main port does not exist;

If there are multiple VLLP ports that meet the conditions, the one with the highest priority is selected as the master port; if the priority is the same, the earliest established mapping relationship is selected as the master port.

Principles for determining the status of VLLP ports:

VLLP device is the sender, then the state of the main port must be forward;

The VLLP device is the sender, the link state is link up, and the state of the VLLP port where there is no mapping relationship is forward

The VLLP device is the sender, the link state is link up and the state of the mapped VLLP port is block;

The VLLP device is the receiver and the link status is link up. The VLLP port status is forward;

The status of the VLLP port whose link status is link down is disabled.

VLLP protocol packets are encapsulated in MAC frames

|                                   |             |                |                   |
|-----------------------------------|-------------|----------------|-------------------|
| Destination MAC Address (6 bytes) |             |                |                   |
| Source MAC Address (6 bytes)      |             |                |                   |
| 0x8100                            |             | Prio           | Vlan ID (12 bits) |
| Ethernet Type (2 bytes)           |             |                |                   |
| Version                           | Type        | Port1(2 bytes) |                   |
| Priority                          | Query Inter | Main port      |                   |
| Reserved (4 bytes)                |             |                |                   |
| Port2                             |             | Link state     | STP state         |

There are three types of VLLP protocol messages

Link status query message LQ

Link status response message LA

Link state change message LC

Value range of each field in the message format:

Des MAC: fixed at 00:09:ca:ff:ff:ff

Src MAC: MAC of vlan sending VLLP protocol packets

Ethernet Type: fixed at 0x268e

Version: currently 1

Type: LQ is 1; LA is 2; LC is 3;

Port1: Index value of the port that sends VLLP protocol packets

Priority: VLLP device priority, value 1~255;

Query Interval: VLLP sender query timer interval, the default is 5 seconds;

Main port: VLLP sender main port index value, only in LQ message;

Reserved: reserved field is zero

Port2: the index value of the port where the status change occurs in the LC message, and port2 and port1 in the LQ and LA message are the same;

Link state: link state of port2, link up is 1, link down is 2;

STP state: STP state of port2, disable is 1, block is 2, and forward is 3.

VLLP protocol principle:

Configure the VLLP device in a vlan and start the VLLP protocol, and configure the VLLP device in the corresponding vlan of the peer switch and start the VLLP protocol. At this time, the VLLP protocol entity (VLLP device) running on the vlan constitutes a pair of sender and receiver. When the protocol starts, both parties are senders and both send LQ messages to the other party. When the VLLP device receives the LQ message, it will elect the receiver according to the priority carried in the message and the peer MAC address, and the winner One party becomes the receiver and no longer sends the LQ message but responds to the sender's LQ message. When the receiver's timer expires and the LQ message has not been received, the receiver will return to the sender state and start to send the LQ message.

In a vlan with the VLLP protocol enabled, the ports participating in the VLLP protocol packet interaction need to be configured as VLLP ports. VLLP ports can be valid Layer 2 ports (including trunk groups), but trunk members are not allowed to be configured as VLLP ports. VLLP protocol messages are sent and received through the VLLP port. The VLLP port and the corresponding VLLP port configured in the VLAN of the VLLP protocol corresponding to the peer switch form a pair of mapping relationships. They determine the mapping relationship with the peer port by sending a query message to receive a response message or changing the message. , And calculate the possible loops in the network according to this mapping relationship and its own link status, and maintain the STP status of the port according to the principle of VLLP port status determination, thereby preventing loops in the topology.

---

Multiple VLLP ports can be activated in the vlan with the VLLP protocol enabled. They may or may not be physically connected to the peer switch. When a port belongs to multiple VLANs, the same VLLP port will also appear in multiple VLLP devices. The VLLP protocol will dynamically collect information about the link status change of the VLLP port and the STP status of the peer VLLP port to calculate the loop in time and effectively prevent the occurrence of loops in the network.

When there are multiple VLANs, the internal port configuration is exactly the same, but the VLLP protocol needs to be enabled on multiple VLANs, and each Layer 2 port needs to send and receive multiple VLLP protocol packets running on different VLANs, which causes the burden on the switch. Propose the concept of affiliated VLAN. That is, the VLANs with the same port configuration only run the VLLP protocol on one VLAN, that is, the master VLAN, and the remaining VLANs are added as subordinate VLANs to the instance of the master VLAN. The status of the port in the instance is written by the result of the loop calculation by the VLLP protocol on the main VLAN. It should be noted that when configuring an auxiliary VLAN, ensure that the VLLP ports of the main VLAN are in the auxiliary VLAN, and all the ports of the auxiliary VLAN are in the main VLAN. When the secondary VLAN is configured and a Layer 2 port is added to the secondary VLAN, if the port is also in the primary VLAN, the primary VLAN will manage the port status in a unified manner; if the port is not in the primary VLAN, the port status cannot be managed. Alarm information.

## 28.2 VLLP configuration

After starting the VLLP protocol, relevant attribute configuration and port creation can be performed, and all related commands are in the VLLP configuration mode.

VLLP configuration includes :

- Create a vllp device on the Layer 3 interface
- Enable vllp device
- Create a vllp port on the Layer 2 interface
- Configure the priority of vllp devices
- Configure VLLP device query timer interval
- Configure affiliate VLAN
- Configure the priority of vllp port

---

## 28.2.1 Create a vllp device on the layer 3 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

Parameters: if-name is the agreed layer 3 interface name (for example: vlan1 vlan2...)

Default: do not start vllp protocol

## 28.2.2 Enable vllp device

Mode: VLLP configuration mode

Command: vllp enable enable vllp device

Command: vllp disable disable vllp device

Default: vllp device is not started after it is created

## 28.2.3 Create a vllp port on the Layer 2 interface

Mode: VLLP configuration mode

Command: vllp port <if-name> create vllp port

Command: no vllp port <if-name> delete vllp port

Parameters: if-name is the agreed layer 2 interface name (for example: ge1/1 trunk1...)

Default: vllp protocol is not applied on the layer 2 port. When the Layer 2 interface is a trunk member, the vllp protocol cannot be applied.

## 28.2.4 Configuring VLLP Device Priority

Mode: VLLP configuration mode

Command: vllp priority <priority> configure vllp device priority

Command: no vllp priority [priority] restore vllp device priority to default

Parameters: priority ranges from 1 to 255. The priority is used by the vllp device to elect the recipient.

Default: 100

---

## 28.2.5 Configure the 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 the query timer interval to the default value

Parameter: interval is between 1 and 255. The configuration values will take effect when the vllp device is the sender or when migrating back to the sender.

default: 5 seconds

## 28.2.6 Configure affiliate VLAN

Mode: VLLP configuration mode

Command: vllp dependency <if-name> configure auxiliary vlan

Command: no vllp dependency <if-name> delete subordinate vlan

Parameters: if-name is the agreed layer 3 interface name (for example: vlan1 vlan2...)

Default: no auxiliary VLAN is configured

## 28.2.7 Configure vllp port priority

mode : VLLP configuration mode

command : vllp port <if-name> priority <priority> Configure vllp port priority

command : no vllp port <if-name> priority [priority] Restore the priority of the vllp port to the default value

parameter :if-name is the agreed layer 2 interface name (for example: ge1/1 trunk1...); priority ranges from 1 to 255. The priority is used by the vllp sender to elect the main port.

default : 100

## 28.2.8 Display information

Mode: normal mode or privileged mode

command : show vllp

Show vllp protocol vllp device list

commad : show vllp <if-name>

Display detailed information of a vllp device

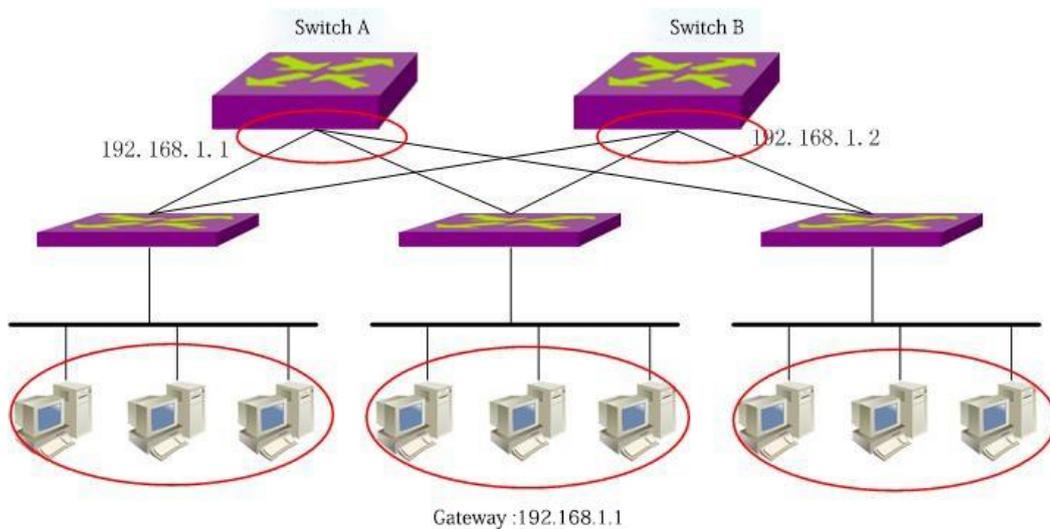
Parameters: if-name is the agreed layer 3 interface name (for example: vlan1  
vlan2...)

command : show vllp map

Display the mapping relationship of each vllp port in the vllp protocol

## 28.3 VLLP configuration example

### (1) configuration



Configuration on Switch A :

```
Switch#configure terminal
```

```
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#ip interface vlan 2
```

```
Switch(config)#interface ge1/1
```

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

|

---

```
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 master
Switch(config-vrrp)#enable
Switch(config-vrrp)#exit
Switch(config)#router vllp vlan2
Switch(config-vllp)#vllp 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)#vllp port ge1/1
Switch(config-vllp)#vllp port ge1/2
Switch(config-vllp)#vllp port ge1/3
Switch(config-vllp)# enable
```

## **(2) verification**

Use the following command to view VLLP information :

```
show vllp
show vllp <if-name>
show vllp map
```

---

## Chapter29 **Configure policy routing**

---

This chapter mainly includes the following: :

- Introduction of policy routing
- Policy routing configuration
- Policy routing configuration example

---

## 29.1 Introduction to policy routing

Policy routing (policy-based-route) is a mechanism for routing based on user-defined policies. Unlike simply looking up the routing table for forwarding based on the destination address of an IP message, policy routing is set based on certain attributes in the message information, such as destination address, source address, and other information for flexible routing. Rich router routing knowledge.

## 29.2 Policy routing configuration

The configuration includes the following :

- Create a new policy route
- Insert a policy route
- Delete a policy route
- Move a policy route
- View policy routing information

### 29.2.1 Create a new policy route

The following command creates a new policy route in global configuration mode :

```
policy route <ID> <SIP> <DIP> <next-hop>
```

ID : ID of the newly created policy routing rule, range 1-100.

SIP, DIP : There are three input methods for source and destination IP :

1)A.B.C.D wildcard Can control the IP address from a network segment ;

2)any Equivalent to A.B.C.D 255.255.255.255

3)host A.B.C.D Equivalent to A.B.C.D 0.0.0.0

wildcard : Decide which bits need to match, '0' means need to match, '1' means need not to match.

---

next-hop : Represents the next-hop host address, the format is A.B.C.D

## 29.2.2 Insert a policy route

The following command inserts a new policy route in global configuration mode :

```
policy route insert <ID> <SIP> <DIP> <next-hop> before <EXIST_ID>
```

ID : ID of the newly inserted policy rule, range 1-100.

SIP, DIP : There are three input methods for source and destination IP :

1)A.B.C.D wildcard Can control the IP address from a network segment ;

2)any Equivalent to A.B.C.D 255.255.255.255

3)host A.B.C.DEquivalent 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 to match.

next-hop : Represents the next-hop host address, the format is A.B.C.D

EXIST\_ID : Indicate before which rule to insert, range 1-100.

## 29.2.3 Delete a policy route

The following command deletes a policy route in global configuration mode :

```
no policy route <ID>
```

ID : ID of the policy rule to be deleted, range 1-100.

## 29.2.4 Move 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 : Rules that need to be moved.

(before|after) : Indicates before or after moving target rule :

## 29.2.5 View policy routing information

The following command is executed in normal mode or privileged mode to view all policy routing information :

```
show policy route
```

## 29.3 Policy routing configuration example

Configure the source IP address as 192.168.3.100 and use the gateway of 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 as 192.168.10.100 and use the gateway of 192.168.2.1.

```
Switch#configure terminal
```

```
Switch#(config)#policy route 2 any host 192.168.10.100 192.168.2.1
```

Configure the source IP address as 192.168.3.100, the destination IP address as 10.10.10.100, and take the gateway of 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
```

---

# Chapter30 Configure System Log

---

This chapter mainly includes the following:

- System log introduction
- System log configuration

## 30.1 Introduction to System Log

The system log module is an important part of the switch. It is used to record the operation status, abnormal behavior and user's operation behavior of the entire system, helping administrators to understand and monitor the working status of the system in time. The system log module manages all the log information from the running modules of the system, collects, classifies, stores and displays the log information.

In the logging system, there is also an important debugging function. The cooperation of system logs and debugging can help administrators or other technical personnel to monitor the operation of the network and debug and diagnose faults in the network. Administrators can easily select the content that needs to be debugged, and observe the log information output by debugging to locate and solve the fault of the device or network. This section mainly includes the following: :

- Format of log information
- Log storage
- Log display
- Debugging tool

### 30.1.1 Log information format

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. An example of the format of the log information is as follows:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

In this log message, the timestamp is 2006/05/20 13:56:34; the priority is Warning; the module name is MSTP; and the log content is Port up notification received for port ge1/2.

### 1 ) Timestamp

The format of the time stamp: year/month/day hour:minute:second.

Hours are in 24-hour format, from 0 to 23.

The timestamp records the time when this log information was generated, and uses the system time of the switch. The system time has been set when the switch was shipped from the factory, and the administrator can also modify it. After the device is powered off, the system time can still run.

### 2 ) priority

The priority records the importance of the log information. The log information is divided into four levels according to the importance of the log information. The order of priority from high to low is Critical, Warning, Informational, and Debugging. The priority is described in the following table:

| priority      | description  |
|---------------|--|
| Critical      | Serious mistake                                      |
| Warning       | General errors, warnings, very important tips        |
| Informational | Important tips, general tips, diagnostic information |
| Debugging     | Debug information                                    |

### 3 ) Module name

The module name records the module generated by this log message. The following table lists some major modules that generate log information:

| Module name | description                                  |
|-------------|--|
| CLI         | Command line interface module                |
| MSTP        | Multi-instance spanning tree protocol module |

---

|      |                      |
|------|----------------------|
| VLAN | VLAN function module |
| ARP  | ARP protocol module  |
| IP   | IP protocol module   |
| ICMP | ICMP protocol module |
| UDP  | UDP protocol module  |
| TCP  | TCP protocol module  |

#### 4 ) Log content

The log content is a phrase or sentence, which represents the content of the log information. The administrator can know what happened to the system by reading the log content.

### 30.1.2 Storage of logs

There are generally three ways to store logs, which are :

- The log is stored in memory.
- Logs are stored in NVM.
- Logs are stored in the server.

There are four log tables in memory according to the priority of the logs. Each table stores log information of a priority. That is, the logs are divided into four types according to the priority of the logs. Each type of log exists in a separate log table. Each log table has 1K entries, which can store 1K log messages. When the log table is full, the logs behind it cover the log messages with the longest time. There is a problem with this storage method. After the system restarts, these log messages are gone. The administrator cannot see the log messages when the system crashes, and cannot locate the problem.

For important log information, such as the priority and Critical log information, you can store these log information in the system's NVM. In this storage method, after the system restarts, the log information in the NVM can also be retained, which is convenient for the administrator to locate the problem when the system crashes. However, one problem with this storage method is that due to the limited capacity of NVM, the log information entries stored in NVM are very limited.

Another better way is to store the log information in the server, which can be achieved using the SYSLOG protocol. The log information can be sent to the server in real time,

---

and the server saves the log information and displays it on an interface. This storage method is not only convenient for users to view log information, but also has a huge capacity. It can store a large amount of log information on the server.

Currently, the system only supports storing log information in memory, and does not support storing log information in NVM or servers.

### **30.1.3 Log display**

There are two ways to display the log: manual display and real-time display. Manual display means that the user displays the log information by inputting commands, and real-time display means that when the log information is generated, the log information is directly output to the terminal, and the user can see it in time.

For the manual display mode, the user can view all the log information. The display order of the log information is that the last generated log information is placed at the front, so that the user can first see the recent operating status of the switch.

For the real-time display mode, the user must turn on the terminal real-time display switch. If the switch is turned on, the generated log information is not only written to the log table, but also the log information is output to the terminal. If the switch is turned off, the log information will not be displayed on the terminal in real time. Currently, the system can only output log information to the Console terminal in real time. It does not support output of log information to Telnet terminals.

### **30.1.4 debugging tool**

Debugging is a diagnostic tool for devices and networks. It can track data packets sent and received by the system and modules, and changes in the state machine of the module. It can allow administrators to understand and monitor the operation of the system and modules. The situation can be tracked through the debugging tool.

The debugging tool provides a wealth of switches. By controlling these switches, the administrator can track what he is interested in. When an abnormality occurs on the device or network, the administrator can turn on the debugging switch related to this abnormality and find the problem by tracking the execution process of the system and modules.

When a debugging switch is turned on, the system will generate related log information, which will be written to the corresponding log table. In general, the priority of

---

the log information generated by debugging is Informational. When the terminal real-time display switch is turned on, these log information will be output to the terminal in real time. When the debugging switch is turned off, the system will not generate related log information.

## 30.2 System log configuration

The system log configuration includes the following:

- Configure terminal real-time display switch
- View log information
- Configure debugging switch
- View debugging information

### 30.2.1 Configure terminal real-time display switch

By default, the real-time display switch of the terminal is turned off, and the log information generated by the system is written to the log table, but it will not be displayed on the terminal in real time. There are also some log messages in the system that are not restricted by this switch. These log messages are always output to the Console terminal in real time.

At present, the switch can only display log information in real time on the Console terminal, and cannot display log information in real time on the Telnet terminal.

When the user uses the write command to store the current configuration of the system in the configuration file, the terminal real-time display switch configuration will not be stored in the system configuration file. When the system restarts, these configurations will be lost and need to be reconfigured.

The command to configure the terminal real-time display switch is as follows:

| command       | description                                  | CLI mode                  |
|---------------|--|---------------------------|
| log stdout    | Open the terminal real-time display switch.  | Global configuration mode |
| no log stdout | Close the terminal real-time display switch. | Global configuration mode |

---

## 30.2.2 Set log level

The command to set the log level is as follows :

| command   | description   | CLI mode                     |
|---|---------------|------------------------------|
| log trap<br><[alerts  <br>critical  <br>debugging  <br>emergencies<br>  errors  <br>informational<br> <br>notifications<br>  warnings]> | Set log level | Global<br>configuration mode |

## 30.2.3 View log information

The command to view the log information is as follows :

| command  | description                     | CLI mode                     |
|----------|---------------------------------|------------------------------|
| show log | Display all log<br>information. | Global<br>configuration mode |

## 30.2.4 Configure debugging switch

The system provides a variety of debugging switches, involving multiple modules, here only lists the schematic commands of each module, for the complete format of the command, see the command manual.

When the user uses the write command to store the current configuration of the system to the configuration file, the configuration of the debugging switch is not stored in the configuration file of the system. When the system is restarted, these configurations will

be lost and need to be reconfigured.

The schematic commands for configuring the debugging switch are as follows:

| command              | description   | CLI mode        |
|----------------------|---|-----------------|
| debug ip ...         | Turn on the debugging switch for the system to send and receive IP packets.         | Privileged mode |
| no debug ip ...      | Turn off the debugging switch for sending and receiving IP packets in the system.   | Privileged mode |
| debug ip icmp ...    | Turn on the debugging switch that the system sends and receives ICMP packets.       | Privileged mode |
| no debug ip icmp ... | Turn off the debugging switch for sending and receiving ICMP packets in the system. | Privileged mode |
| debug ip arp ...     | Turn on the debugging switch for the system to send and receive ARP packets.        | Privileged mode |
| no debug ip arp ...  | Turn off the debugging switch for the system to send and receive ARP packets.       | Privileged mode |
| debug ip udp ...     | Turn on the debugging switch for the system to send and receive UDP packets.        | Privileged mode |
| no debug ip udp ...  | Turn off the debugging switch for sending and receiving UDP packets in the system.  | Privileged mode |
| debug ip tcp ...     | Turn on the debugging   | Privileged      |

|                            |   |                 |
|----------------------------|---|-----------------|
|                            | switch that the system sends and receives TCP packets.                        | mode            |
| no debug ip tcp ...        | Turn off the debugging switch that the system sends and receives TCP packets. | Privileged mode |
| debug mstp ...             | Turn on the debugging switch for MSTP protocol diagnosis.                     | Privileged mode |
| no debug mstp ...          | Turn off the related debugging switch for MSTP protocol diagnosis.            | Privileged mode |
| debug igmp snooping ...    | Turn on the relevant debugging switch for IGMP SNOOPING function diagnosis.   | Privileged mode |
| no debug igmp snooping ... | Turn off the relevant debugging switch for IGMP SNOOPING function diagnosis.  | Privileged mode |
| debug dhcp snooping ...    | Turn on the debugging switch for DHCP SNOOPIN protocol diagnosis              | Privileged mode |
| no debug dhcp snooping ... | Disable debugging related to DHCP SNOOPIN protocol diagnosis                  | Privileged mode |
| no debug all               | Turn off all debugging switches in the system.                                | Privileged mode |

### 30.2.5 View debugging information

The command to view debugging information is as follows :

| command  | description  | CLI mode                     |
|--|--|------------------------------|
| show debugging [dhcp snooping   erps   igmp snooping   ip   mstp   rip ] | Check the debugging switch configuration. If no parameters are entered, view the debugging switch configuration of all modules. If only one of the parameters is entered, only one module's debugging switch configuration is viewed. If the input parameter is ip, the debugging switch configuration of the IP, ICMP, ARP, UDP, and TCP modules will be checked. | Normal mode, Privileged mode |

### 30.3 SYSLOG configuration

SYSLOG includes the following :

- SYSLOG introduction
- SYSLOG configuration
- SYSLOG configuration example

#### 30.3.1 SYSLOG introduction

SYSLOG is a standard protocol for the management of device log information, and it has gained great application due to its concise design. In the SYSLOG system, it is divided into three parts. One is to define each sub-module in order to distinguish the log information generated by different modules; define different levels of log information in order to observe the operation status of the device. Various log information of the device is collected according to this agreement. The second is the configuration file, which defines how to process the collected log information, which

can be saved locally, can be sent to a specified server on the network, can be distributed to the specified logged-in users, etc.; the configuration file determines how to save the device generated Log information. The third is to send SYSLOG protocol messages according to the message format defined by RFC. It can be seen that in our switch system, the entire SYSLOG work contract is the system log module. The first part of the SYSLOG protocol is completed by each functional sub-module in the switch, and sends each level of log information to the system log module. Four levels of log tables are maintained in the system log module. The second part of the SYSLOG protocol is the unified distribution of log information by the system log module. One is real-time or manual display on the serial terminal through the terminal display switch; the second is to save four levels of log tables in memory; the third is to save high-level on NVM Log information at the same level to avoid losing important log records in the event of a power failure; the fourth is to send the logs to a remote server for storage, collection, and sorting through SYSLOG messages. The SYSLOG submodule in the system log module only implements the third part of the function, and transmits the system log to the server.

### 30.3.2 SYSLOG configuration

SYSLOG configuration commands include:

- Open the syslog server address
- Close the syslog server address
- Open the syslog protocol

| command                 | description  | CLI mode                  |
|-------------------------|--|---------------------------|
| syslog open <server-ip> | Open the syslog server address; the parameter server-ip is the server IP address | Global configuration mode |
| syslog close            | Close syslog server address  | Global configuration mode |
| log syslog              | Open the syslog protocol   | Global configuration mode |

---

### 30.3.3 SYSLOG configuration example

#### ( 1 ) Configuration

Configure the IP address of the syslog server as 192.168.0.201, and configure the switch as follows:

```
Switch#configure terminal
```

```
Switch(config)#syslog open 192.168.0.201
```

```
Switch(config)# log syslog
```

#### ( 2 ) 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
```