



# **L3 Switch Series (PoE)**

## **User Manual**

# Table of Contents

<b>Getting Started</b> .....	<b>12</b>
Power.....	12
Connecting to Power.....	12
Connecting to the Network.....	12
Starting the Web-based Configuration Utility.....	13
Logging In.....	14
Logging Out.....	14
<b>Web-based Switch Configuration</b> .....	<b>15</b>
<b>Console Port Interface</b> .....	<b>15</b>
<b>1. Switch basic configuration</b> .....	<b>16</b>
1.1 Switch basic configuration.....	16
1.1.1 Login user configuration.....	16
1.1.2 Login user authentication method configuration.....	17
1.1.3 Logging user Security IP management.....	17
1.1.4 Basic configuration.....	18
1.1.5 Save current running-configuration.....	19
1.2 SNMP authentication.....	20
1.2.1 SNMP authentication.....	20
1.2.1.1 User.....	20
1.2.1.2 Groups.....	21
1.2.1.3 Views.....	21
1.2.1.4 SNMP engineid configuration.....	22
1.2.2 SNMP management.....	22
1.2.3 Community managers.....	23
1.2.4 Configure snmp manager security IP.....	24
1.2.5 SNMP statistics.....	24
1.3 SSH management.....	24
1.3.1 Switch on-off SSH.....	24
1.3.2 SSH management.....	25
1.4 Firmware update.....	25
1.4.1 TFTP service.....	25
1.4.1.1 TFTP client service.....	25
1.4.1.2 TFTP server service.....	26
1.4.2 FTP service.....	26
1.4.2.1 FTP client service.....	26
1.4.2.2 FTP server service.....	27
1.5 Telnet server configuration.....	28
1.5.1 Telnet server state.....	28
1.5.2 Max numbers of telnet access connection.....	28
1.6 Maintenance and debugging command.....	29
1.6.1 Debug command.....	29
1.6.2 show clock.....	29
1.6.3 show cpu usage.....	30
1.6.4 show memory usage.....	30
1.6.5 show flash.....	30
1.6.6 show running-config.....	30
1.6.7 show switchport interface.....	30
1.6.8 show tcp.....	31

1.6.9 show udp.....	31
1.6.10 show telnet login.....	31
1.6.11 show version.....	31
<b>2. Module management.....</b>	<b>32</b>
2.1 Show boot-files.....	32
2.2 Set Boot IMG and Startup-Config.....	32
<b>3. Port configuration.....</b>	<b>32</b>
3.1 Ethernet port configuration.....	32
3.1.1 Port layer 1 attribution configuration.....	33
3.1.2 Bandwidth control configuration.....	35
3.1.3 Switchport description.....	36
3.1.4 Port combo forced mode config.....	37
3.1.5 port scan mode.....	38
3.2 VLAN interface configuration.....	38
3.2.1 Add interface VLAN.....	38
3.2.2 L3 interface IP address mode configuration.....	38
3.3 SPAN configuration.....	39
3.4 Loopback-detection configuration.....	42
3.4.1 Port Loopback-detection mode configuration.....	42
3.4.2 VLAN Loopback-detection configuration.....	44
3.4.3 Loopback-detection interval-time configuration.....	44
3.4.4 Loopback-detection control recovery configuration.....	45
3.5 Isolate-port configuration.....	45
3.5.1 Isolate-port group configuration.....	45
3.5.2 Interface join group config.....	46
3.5.3 show isolate-port group.....	46
3.6 Port storm-control config.....	47
3.6.1 Port storm-control config.....	47
3.6.2 storm-control bypass configuration.....	48
3.7 Port rate-violation config.....	49
3.7.1 rate-violation configuration.....	49
3.8 Port virtual-cable-test config.....	49
3.8.1 virtual-cable-test configuration.....	49
3.9 Port debug and maintenance.....	50
3.9.1 Show port information.....	50
3.9.2 Show entire traffic information.....	51
3.9.3 Show rate violation port.....	51
3.10 uldp configuration.....	51
3.10.1 uldp enable config.....	51
3.10.2 uldp Hello message config.....	52
3.10.3 uldp recovery time config.....	53
3.10.4 show uldp configuration.....	53
3.11 LLDP configuration.....	54
3.11.1 LLDP configuration.....	54
3.11.2 LLDP port status config.....	55
3.11.3 LLDP tx-interval config.....	55
3.11.4 LLDP msgTxHold config.....	56
3.11.5 LLDP transmit delay config.....	56
3.11.6 LLDP notification interval config.....	57
3.11.7 LLDP neighbors max-num config.....	57

3.11.8 LLDP too many neighbors config.....	58
3.11.9 LLDP transmit optional tlv config.....	59
3.11.10 show LLDP configuration.....	59
3.12 LED shutoff configuration.....	61
3.12.1 Time Range configuration.....	61
3.12.2 LED shutoff config.....	62
3.13 Jumbo packet forwarding configuration.....	62
<b>4. MAC address table configuration.....</b>	<b>63</b>
4.1 MAC address table configuration.....	63
4.1.1 MAC address aging-time configuration.....	63
4.1.2 Configure MAC address.....	63
4.1.3 Delete MAC address.....	65
4.1.4 MAC address query.....	65
<b>5. VLAN configuration.....</b>	<b>66</b>
5.1 VLAN configuration.....	66
5.1.1 Create/Remove VLAN.....	66
5.1.2 Assign ports for VLAN.....	67
5.1.3 Port type configuration.....	68
5.1.4 Hybrid port configuration.....	69
5.1.5 Trunk port configuration.....	70
5.1.6 Private-vlan configuration.....	71
5.2 GVRP configuration.....	72
5.2.1 Enable global GVRP.....	72
5.2.2 Enable GVRP on port.....	72
5.2.3 GARP configuration.....	73
5.3 VLAN-translation configuration.....	73
5.3.1 Enable/Disable VLAN-translation.....	73
5.3.2 Add/Delete VLAN-translation.....	74
5.3.3 VLAN-translation miss drop configuration.....	75
5.3.4 show VLAN-translation.....	75
5.4 dynamic VLAN configuration.....	76
5.4.1 VLAN protocol configuration.....	76
5.5 Dot1q tunnel configuration.....	77
5.5.1 Enable dot1q tunnel.....	77
5.5.2 dot1q tunnel tpid configuration.....	77
<b>6. IGMP Snooping configuration.....</b>	<b>78</b>
6.1 Switch on-off IGMP Snooping.....	78
6.2 IGMP Snooping port enable.....	78
6.3 IGMP Snooping configuration.....	79
6.4 IGMP Snooping mrouter configuration.....	80
6.5 IGMP Snooping query configuration.....	80
<b>7. MLD Snooping configuration.....</b>	<b>81</b>
7.1 Switch on-off MLD Snooping.....	81
7.2 MLD Snooping port enable.....	82
7.3 MLD Snooping configuration.....	82
7.4 MLD Snooping mrouter port configuration.....	83
7.5 MLD Snooping query configuration.....	83
<b>8. Time Range configuration.....</b>	<b>84</b>
8.1 Time Range configuration.....	84

<b>9. ACL configuration.....</b>	<b>85</b>
9.1 Numeric ACL.....	85
9.1.1 Standard numeric ACL.....	85
9.1.1.1 IP standard ACL.....	85
9.1.1.2 MAC standard ACL.....	86
9.1.2 Extended numeric ACL.....	87
9.1.2.1 IP extended ACL.....	87
9.1.2.2 MAC-IP extended ACL.....	88
9.1.3 Delete Numeric ACL.....	90
9.2 Name ACL.....	91
9.2.1 Standard name ACL.....	91
9.2.1.1 IP standard ACL.....	91
9.2.2 Extended name ACL.....	92
9.2.2.1 IP extended ACL.....	92
9.2.2.2 MAC extended ACL.....	93
9.2.2.3 MAC-IP extended ACL.....	94
9.2.3 Delete name ACL.....	96
9.3 Filter configuration.....	97
9.3.1 Firewall configuration.....	97
9.4 Show ACL configuration.....	97
9.4.1 Show access list.....	97
9.4.2 Show firewall.....	97
9.4.3 Show time range.....	98
9.5 ACL binding configuration.....	98
9.5.1 Attach ACL to port.....	98
9.5.2 Show access group.....	98
9.5.3 Clear Pacl Statistic.....	99
9.5.4 Attach ACL to vlan.....	99
9.5.5 show vacl configuration.....	100
9.5.6 clear vlan acl statistic.....	100
<b>10. IPv6 ACL configuration.....</b>	<b>100</b>
10.1 IPv6 standard access-list configuration.....	100
10.2 IPv6 name access-list configuration.....	101
10.3 Show IPv6 access list.....	102
10.4 Attach IPv6 ACL to port.....	102
10.5 Attach IPv6 ACL to vlan.....	102
<b>11. AM configuration.....</b>	<b>103</b>
11.1 AM global configuration.....	103
11.1.1 Enable/Disable AM.....	103
11.2 AM port configuration.....	103
11.2.1 Enable/Disable AM port.....	103
11.2.2 AM IP-Pool configuration.....	104
11.2.3 AM MAC-IP-Pool configuration.....	104
11.3 Show AM port configuration.....	105
11.3.1 Show AM port configuration.....	105
11.3.2 Clear port AM Pool.....	105
<b>12. Port channel configuration.....</b>	<b>105</b>
12.1 LACP port group configuration.....	105
12.2 Delete port group.....	106

12.3 Show port group info.....	107
12.4 Show interface port-channel.....	108
12.5 Add member port.....	108
12.6 Del member port.....	109
12.7 Set lacp port priority.....	110
12.8 Set lacp system priority.....	110
<b>13. DHCP configuration.....</b>	<b>111</b>
13.1 DHCP management.....	111
13.1.1 Enable DHCP.....	111
13.2 DHCP server configuration.....	112
13.2.1 Dynamic pool configuration.....	112
13.2.1.1 Dynamic address pool configuration.....	112
13.2.1.2 client's default gateway configuration.....	113
13.2.1.3 Client DNS server configuration.....	114
13.2.1.4 Client WINS server configuration.....	115
13.2.1.5 DHCP file server address configuration.....	116
13.2.1.6 DHCP network parameter configuration.....	117
13.2.1.7 Excluded address configuration.....	118
13.2.2 Manual DHCP IP pool configuration.....	118
13.2.2.1 Static address pool configuration.....	118
13.2.3 Address pool name configuration.....	120
13.2.4 DHCP packet statistics.....	121
13.3 DHCP relay configuration.....	121
13.3.1 DHCP relay configuration.....	121
13.4 DHCP debugging.....	122
13.4.1 Delete record.....	122
13.4.1.1 Delete binding log.....	122
13.4.1.2 Delete conflict log.....	122
13.4.1.3 Delete DHCP server statistics log.....	123
13.4.2 show IP-MAC binding.....	123
13.4.3 show conflict-logging.....	124
<b>14. DHCP Snooping configuration.....</b>	<b>124</b>
14.1 DHCP Snooping global configuration.....	124
14.1.1 Enable/Disable DHCP Snooping.....	124
14.1.2 DHCP Snooping binding configuration.....	124
14.1.3 DHCP Snooping binding user configuration.....	125
14.1.4 DHCP Snooping action count config.....	126
14.1.5 DHCP Snooping limit-rata config.....	126
14.1.6 DHCP Snooping helper-server config.....	127
14.2 DHCP Snooping port configuration.....	128
14.2.1 Enable/Disable DHCP Snooping binding dot1x.....	128
14.2.2 Enable/Disable DHCP Snooping binding user.....	128
14.2.3 Enable/Disable DHCP Snooping trust.....	129
14.2.4 DHCP Snooping action config.....	130
14.3 show DHCP Snooping configuration.....	131
14.3.1 show DHCP Snooping configuration.....	131
<b>15. SNTP configuration.....</b>	<b>131</b>
15.1 SNTP server configuration.....	132
15.2 Request interval configuration.....	132

15.3 Time difference configuration.....	132
15.4 Show snmp.....	133
<b>16. NTP configuration.....</b>	<b>133</b>
16.1 NTP global configuration.....	133
16.1.1 NTP global switch configuration.....	133
16.1.2 NTP server configuration.....	134
16.1.3 NTP broadcast or multicast address count configuration.....	134
16.1.4 NTP access group configuration.....	135
16.1.5 NTP authenticate configuration.....	135
16.2 NTP interface configuration.....	136
16.2.1 NTP interface switch configuration.....	136
16.3 NTP configuration display.....	136
16.3.1 NTP status display.....	136
<b>17. QOS port configuration.....</b>	<b>136</b>
17.1 QOS port configuration.....	136
17.1.1 QOS port trust state configuration.....	136
17.1.2 QOS port COS parameters configuration.....	137
17.1.3 QOS port select queue schedule algorithm configuration.....	138
17.1.4 QOS port wrr algorithm queue weight configuration.....	139
17.1.5 QOS port wdr algorithm queue weight configuration.....	140
17.1.6 QOS service policy configuration.....	141
17.2 QOS class-map configuration.....	141
17.2.1 Class map-configuration.....	141
17.2.2 classification criteria configuration.....	142
17.3 QoS policy configuration.....	147
17.3.1 QoS policy configuration.....	147
17.4 QOS policy-map configuration.....	147
17.4.1 policy-map configuration.....	147
17.4.2 Class-map use to policy-map config.....	148
17.5 QoS policy-class-map configuration.....	148
17.5.1 Policy-class-map accounting configuration.....	148
17.5.2 Aggregate policy configuration.....	149
17.5.3 Policy-class-map policy configuration.....	150
17.5.4 Policy-class-map set configuration.....	151
17.6 QoS mapping configuration.....	152
17.6.1 COS-to-IntP mapping.....	152
17.6.2 COS-to-DP mapping.....	153
17.6.3 DSCP-to-DSCP mapping.....	153
17.6.4 DSCP-to-IntP mapping.....	154
17.6.5 DSCP-to-DP mapping.....	155
17.6.6 EXP-to-IntP mapping.....	156
17.6.7 EXP-to-DP mapping.....	156
17.6.8 IntP-to-DSCP mapping.....	157
17.6.9 IntP-to-EXP mapping.....	157
17.7 QoS aggregate policy configuration.....	158
17.8 QoS service policy configuration.....	158
<b>18. L3 forward configuration.....</b>	<b>159</b>
18.1 IP route Aggregation configuration.....	159
18.1.1 Route aggregate configuration.....	159

18.2 ARP configuration.....	160
18.2.1 ARP configuration.....	160
18.2.2 Clear ARP cache.....	160
18.2.3 Show ARP.....	161
18.3 Gratuitous arp config.....	161
18.3.1 gratuitous-arp interval time configuration.....	161
18.3.2 interface gratuitous-arp interval time configuration.....	161
18.3.3 show gratuitous-arp configuration.....	162
18.4 ARP protection configuration.....	162
18.4.1 ARP GUARD configuration.....	162
18.4.1.1 ARP GUARD configuration.....	162
18.4.2 ANTI-ARPSCAN configuration.....	163
18.4.2.1 ANTI-ARPSCAN on-off configuration.....	163
18.4.2.2 ANTI-ARPSCAN port-based threshold configuration.....	163
18.4.2.3 ANTI-ARPSCAN IP-based threshold configuration.....	164
18.4.2.4 ANTI-ARPSCAN trust port configuration.....	165
18.4.2.5 ANTI-ARPSCAN trust IP configuration.....	165
18.4.2.6 ANTI-ARPSCAN recovery on-off configuration.....	166
18.4.2.7 ANTI-ARPSCAN recovery time configuration.....	166
18.4.2.8 Show ANTI-ARPSCAN information.....	167
18.5 Show IP Traffic.....	167
<b>19. Route configuration.....</b>	<b>168</b>
19.1 Policy based routing.....	168
19.2 Static route configuration.....	168
19.2.1 Static route configuration.....	168
<b>20. IPv6 Route configuration.....</b>	<b>169</b>
20.1 IPv6 configuration.....	169
20.1.1 IPv6 basic configuration.....	169
20.1.2 IPv6 ND configuration.....	170
20.1.3 Show IPv6 neighbor.....	172
20.2 Show IPv6 route.....	174
20.2.1 Show IPv6 route database.....	174
20.2.2 Show IPv6 NSM route.....	175
20.2.3 Show IPv6 FIB.....	176
20.2.4 Show IPv6 route statistics.....	178
<b>21. DCSCM configuration.....</b>	<b>178</b>
21.1 DCSCM Source-control enable/disable configuration.....	178
21.2 DCSCM destination-control enable/disable configuration.....	179
21.3 DCSCM Source-control access-group configuration.....	179
21.4 DCSCM destination-control access-group configuration.....	180
21.5 DCSCM destination-control access-group configuration (sip).....	180
21.6 DCSCM destination-control access-group configuration (vMAC).....	181
21.7 Multicast policy configuration.....	182
21.8 ACL multicast source control.....	183
<b>22. Spanning-tree configuration.....</b>	<b>185</b>
22.1 Spanning-tree field configuration.....	185
22.1.1 Instance configuration.....	185
22.1.2 Field name configuration.....	186
22.1.3 Revision-level configuration.....	186



22.2 Spanning-tree Port configuration.....	187
22.2.1 PortFast configuration.....	187
22.2.2 Port priority configuration.....	188
22.2.3 Port cost configuration.....	189
22.2.4 Spanning-tree port mode.....	189
22.2.5 Link-type configuration.....	190
22.2.6 Spanning-tree agreement port configuration.....	191
22.3 Spanning-tree global configuration.....	191
22.3.1 Spanning-tree global agreement port configuration.....	191
22.3.2 Forward-time configuration.....	192
22.3.3 Hello-time configuration.....	192
22.3.4 Max age time configuration.....	193
22.3.5 Max hop time configuration.....	194
22.3.6 Spanning tree mode configuration.....	195
22.3.7 Spanning tree cost-format configuration.....	195
22.3.8 Priority configuration.....	196
22.4 Show spanning-tree.....	196
22.4.1 Instance information.....	196
22.4.2 Revision-Level information.....	197
<b>23. MRPP configuration.....</b>	<b>197</b>
23.1 MRPP global configuration.....	197
23.1.1 MRPP global switch configuration.....	197
23.1.2 MRPP poll time configuration.....	198
23.1.3 MRPP domain id configuration.....	199
23.2 MRPP port configuration.....	199
23.2.1 MRPP port property configuration.....	199
23.3 MRPP domain configuration.....	200
23.3.1 MRPP control vlan config.....	200
23.3.2 MRPP node mode config.....	201
23.3.3 MRPP hello timer config.....	202
23.3.4 MRPP fail timer config.....	203
23.3.5 MRPP domain switch config.....	204
23.4 MRPP configuration display.....	204
23.4.1 MRPP display.....	204
23.4.2 MRPP statistics display.....	205
23.4.3 Clear MRPP statistics.....	205
<b>24. ULPP configuration.....</b>	<b>206</b>
24.1 ULPP global configuration.....	206
24.1.1 ULPP group configuration.....	206
24.2 ULPP port configuration.....	207
24.2.1 ULPP port property configuration.....	207
24.3 ULPP group configuration.....	207
24.3.1 ULPP group description configuration.....	207
24.3.2 ULPP group property configuration.....	208
24.4 ULPP configuration display.....	210
24.4.1 ULPP group configuration display.....	210
24.4.2 ULPP port statistics display.....	210
24.4.3 ULPP port property display.....	210
24.4.4 ULPP port statistics clear.....	211

<b>25. ULSM configuration.....</b>	<b>211</b>
25.1 ULSM global configuration.....	211
25.1.1 ULSM group configuration.....	211
25.2 ULSM port configuration.....	212
25.2.1 ULSM port property configuration.....	212
25.3 ULSM configuration display.....	213
25.3.1 ULSM display.....	213
<b>26. Authentication configuration.....</b>	<b>213</b>
26.1 RADIUS client configuration.....	213
26.1.1 RADIUS global configuration.....	213
26.1.2 RADIUS authentication configuration.....	214
26.1.3 RADIUS accounting configuration.....	215
26.2 TACACS server configuration.....	216
26.2.1 TACACS global configuration.....	216
26.2.2 TACACS server host configuration.....	216
26.3 802.1x configuration.....	217
26.3.1 802.1x Global configuration.....	217
26.3.2 802.1x port authentication configuration.....	218
26.3.3 802.1x port MAC configuration.....	218
26.3.4 802.1x port status list.....	219
26.4 MAB configuration.....	219
26.4.1 MAB ENABLE configuration.....	219
26.4.2 MAB Authentication configuration.....	220
26.4.3 MAB parameter configuration.....	220
26.4.4 MAB show.....	222
<b>27. PoE Config.....</b>	<b>222</b>
27.1 PoE Global Config.....	223
27.1.1 PoE Global Config.....	223
27.2 PoE Port Config.....	223
27.2.1 PoE Port Config.....	223
<b>28. DOS attack protection configuration.....</b>	<b>225</b>
28.1 Source IP equal destination IP DOS attack protection configuration.....	225
28.2 Source port equal destination port DOS attack protection configuration.....	226
28.3 TCP DOS attacks on invalid flags configuration.....	226
28.4 ICMP DOS attack protection configuration.....	226
28.5 ICMP packet-size configuration.....	227
28.6 First fragment IP packet DOS attack protection configuration.....	227
<b>29. SSL config.....</b>	<b>227</b>
29.1 IP HTTP server configuration.....	227
29.2 SSL global configuration.....	228
29.3 SSL server monitor port configuration.....	228
29.4 SSL secure-ciphersuite configuration.....	229
<b>30. sFlow configuration.....</b>	<b>229</b>
30.1 sFlow collector global address configuration.....	229
30.2 sFlow collector port address configuration.....	230
30.3 sFlow agent address configuration.....	230
30.4 sFlow priority configuration.....	231
30.5 sFlow header length configuration.....	231

30.6 sFlow data length configuration.....	232
30.7 sFlow rate configuration.....	233
30.8 sFlow counter interval configuration.....	233
30.9 sFlow analyzer configuration.....	234
<b>31. IPv6 security ra configuration.....</b>	<b>234</b>
31.1 IPv6 security ra global configuration.....	234
31.2 IPv6 security ra port configuration.....	235
31.3 show IPv6 security ra.....	235
<b>32. Device log message.....</b>	<b>236</b>
32.1 Show device log message.....	236
32.2 Clear logging in logbuff channel.....	236

# Getting Started

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device.
- Connecting to the network.
- Starting the web-based configuration utility.

## Power

### Connecting to Power

Power down and disconnect the power cord before servicing or wiring a switch.

Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch.

Disconnect the power cord before installation or cable wiring.

The switch is powered by the AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source.

Connect the AC power connector on the back panel of the switch to the external power source with the included power cord, and check the power LED is on.



Figure 1. Rear View AC Power Socket.

### Connecting to the Network

To connect the switch to the network:

1. Connect an Ethernet cable to the Ethernet port of a computer.
2. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. The LED of the port lights if the device connected is active.
3. Repeat Step 1 and Step 2 for each device to connect to the switch.



We strongly recommend using CAT-5E or better cable to connect network devices. When connecting network devices, do not exceed the maximum cabling distance of 100 meters (328 feet). It can take up to one minute for attached devices or the LAN to be operational after it is connected. This is normal behavior.

Connect the switch to end nodes using a standard Cat 5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as shown in the illustration below.

Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which the switch is connected.

## Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility. Be sure to disable any pop-up blocker.

Browser Restrictions:

- If you are using older versions of Internet Explorer, you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.
2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.2.1) and then press Enter.



When the device is using the factory default IP address, its power LED flashes continuously. When the device is using a DHCP assigned IP address or an administrator-configured static IP address, the power LED is lit a solid color. Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address, your computer's IP address can be in the following range: 192.168.2.x (whereas x is a number from 2 to 254).

After a successful connection, the login window displays.

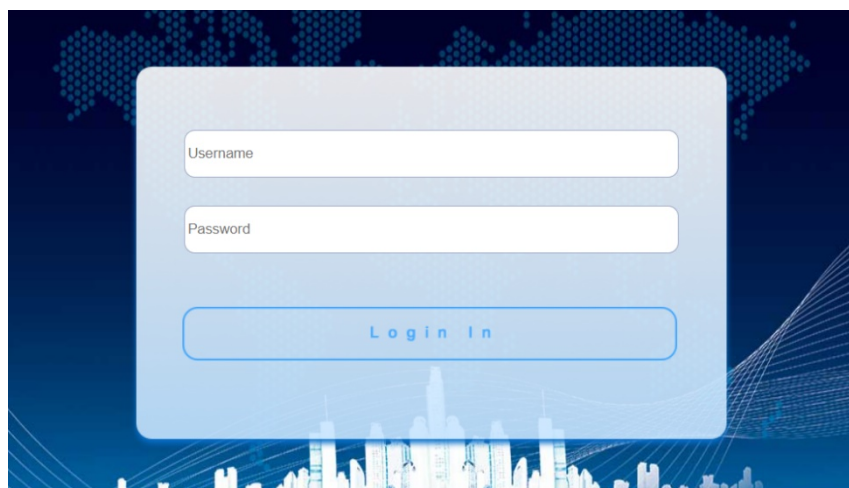


Figure 2. Login Window

## Logging In

The default username is admin and the default password is admin. The first time that you log in with the default username and password, you are required to enter a new password.

To log in to the device configuration utility:

1. Enter the default user ID (admin) and the default password (admin).
2. If this is the first time that you logged on with the default user ID (admin) and the default password (admin) it is recommended that you change your password immediately.

When the login attempt is successful, the System Information window displays.



Figure 3. System Information.

If you entered an incorrect username or password, an error message appears and the Login page remains displayed on the window. If you are having problems logging in, please see the Launching the Configuration Utility section in the Administration Guide for additional information.

## Logging Out

By default, the application logs out after ten minutes of inactivity.

To logout, click Logout in the top right corner of any page. The system logs out of the device.

When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears, with a message indicating the logged-out state. After you log in, the application returns to the initial page.

# Web-based Switch Configuration

The smart switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features.

For the purposes of this manual, the user interface is separated into four sections, as shown in the following figure:

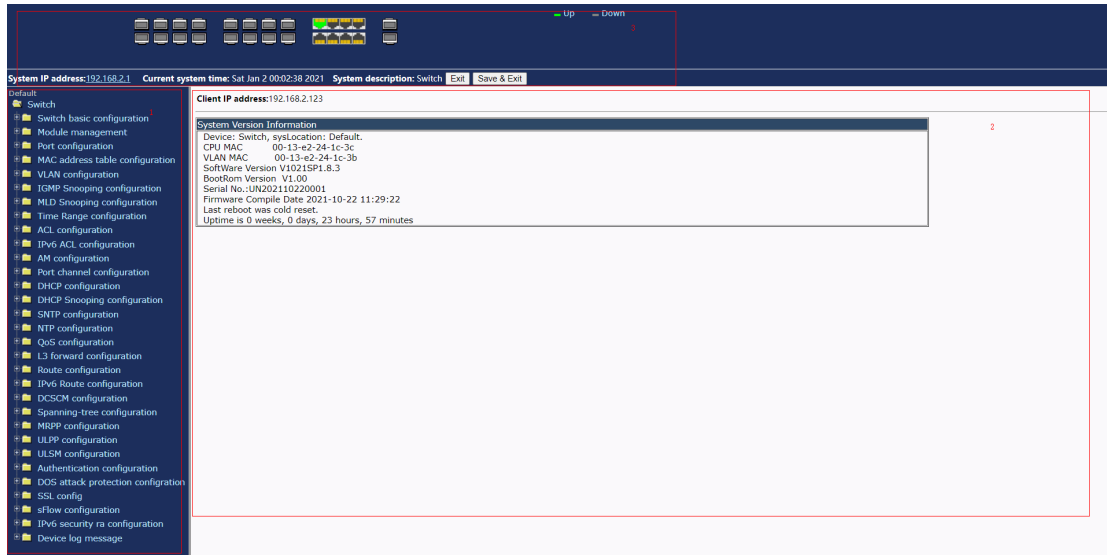


Figure 4. User Interface.

# Console Port Interface

The PoE smart switch has a monitor port (Console port). Rate 9600bps, standard RJ45 plug. Use a dedicated monitoring cable to lead the port to the PC serial port connection, as follows:

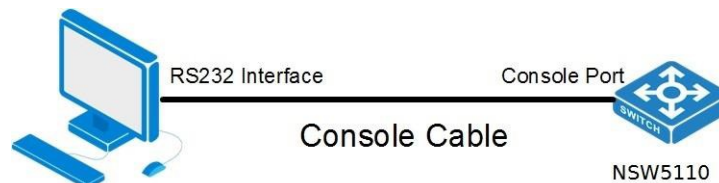


Figure 5.

The RJ45 connector used by the Console port is shown in the figure below, and the RJ45 plug corresponds to the RJ45 socket, from left to right numbered from 1 to 8.

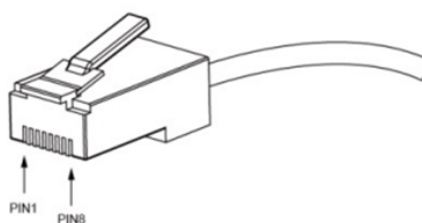


Figure 6.

This cable is used to connect the console port of the switch to the external monitoring terminal. One end of the RJ45 eight-pin plug, the other end is a 25-hole plug(DB25) and 9-hole plug(DB9), RJ45 head into the switch's console port socket, DB25 and DB9 can be used according to the requirements of the terminal serial port, the cable internal connection schematic as follows:

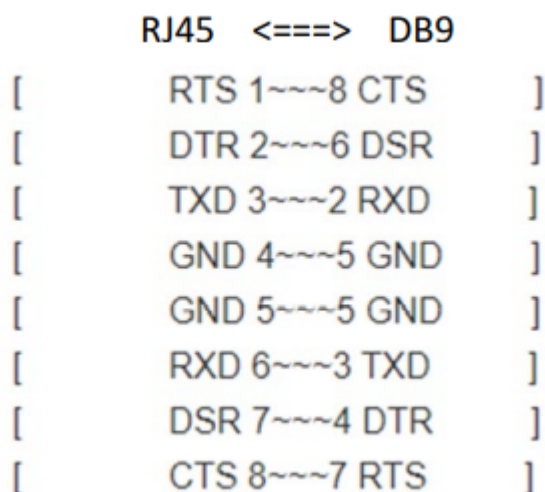


Figure 7.

## 1. Switch basic configuration

### 1.1 Switch basic configuration

#### 1.1.1 Login user configuration

Login user management module, users in this module can add or delete user operations.

Login username and password configuration	
User	<input style="width: 80%;" type="text"/>
Password	<input style="width: 80%;" type="password"/> <input type="checkbox"/> Encrypted text
Priority	<input style="width: 80%;" type="text"/>
Operation	Remove <input type="button" value="v"/>
<input type="button" value="Apply"/>	

User			
User name	Password	State	Priority
admin	admin	Plain text	15

Figure 8.

<b>User</b>	User name to operate, 1-32 characters.	
<b>Password</b>	User password, choose the password encryption, otherwise no encryption of 1-32 characters.	
<b>Priority</b>	Used to specify permission level, default level 15.	
<b>Operation</b>	Add	Create new users.



	Remove	Delete the specified user (password and priority can not be entered).
--	--------	---

### 1.1.2 Login user authentication method configuration

Login user authentication method configuration module, the user can configure console.vty.web authentication method used in login, authentication method can be any one or combination of Local.RADIUS and TACACS.preferences from left to right when the login method is combined configuration. If the user has passed the authentication method, the authentication method of the lower preference is ignored. As long as you pass an authentication method, the user can log in. AAA functions and RADIUS servers should be configured before using RADIUS authentication. If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.

Login user authentication method configuration	
Login method	Console ▾
Authentication method1	None ▾
Authentication method2	None ▾
Authentication method3	None ▾
<input type="button" value="Apply"/> <input type="button" value="Default"/>	

Login user authentication method				
Login method	Authentication method1	Authentication method2	Authentication method3	
console	None	None	None	None
vty	local	None	None	None
web	local	None	None	None

Figure 9.

Login method	Authentication method	
<b>console</b>	<b>local</b>	Authentication using the local user account database.
<b>vty</b>	<b>radius</b>	Authentication using remote Radius server.
<b>web</b>	<b>tacacs</b>	Authentication using remote Tacacs server.
<b>Default</b>		Default console no authentication, vty and web local authentication.

### 1.1.3 Logging user Security IP management

Login user security IP configuration module, where users can configure the security IP. IPv6 address for login switch, or configure access control list.

Login user Security IP Set	
Security IP address	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Login Access control list Set	
Ipv4 access control list <input type="button" value="v"/>	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Login user Security IPv4 List
end of security IPv4
Login user Security IPv6 List
end of security IPv6
Login Ipv4 access control list
end of ipv4 access list
Login Ipv6 access control list
end of ipv6 access list

Figure 10.

<b>Security IP address</b>	Fill in the specified security IP or IPv6 address (the access control list is valid until the IPv6 address is filled in).	
<b>IPv4/IPv6 access control list</b>	Standard access control list number, scope 1-64.	
<b>Operation</b>	Add	Add address or list number.
	Remove	Delete address or list number.

#### 1.1.4 Basic configuration

Basic configuration module, in which users can configure switch current time, exit privilege mode timeout and switch name respectively.

Basic clock configuration	
HH:MM:SS	<input type="text"/>
YYYY.MM.DD	<input type="text"/>
Apply	<input type="button" value="Apply"/>

Configure exec timeout	
Timeout(minute)	<input type="text"/>
Timeout(second)	<input type="text"/>
Operation	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Switch name configuration	
Switch name	<input type="text"/>
Operation	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 11.

<b>HH:MM:SS</b>	Current time, format: hours:minutes:seconds.
<b>YYYY.MM.DD</b>	Current date, format: Year.Month.Day.

<b>Timeout (minute)</b>	Exit privilege mode timeout score 0-35791.	
<b>Timeout (second)</b>	Seconds of exit privilege mode timeout (not set separately), 0-59 seconds.	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Restore default (default timeout: 10 minutes).

<b>Switch name</b>	Fill in the new name of the switch to be changed, 1-64 characters.	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Do recovery default (default name: Switch).

### 1.1.5 Save current running-configuration

Save the current configuration module, the user can save the current set configuration, can also leave the factory initial settings restart, but also choose whether to save the current set configuration before restart.

Save current running-configuration	
<input type="text"/>	
<input type="button" value="Apply"/>	

Reboot with the default configuration	
<input type="text"/>	
<input type="button" value="Apply"/>	

Save current configuration before reboot?	
Yes <input type="button" value="v"/>	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 12.

## 1.2 SNMP authentication

### 1.2.1 SNMP authentication

#### 1.2.1.1 User

SNMP user management module, users can add or delete SNMP user operations in this module.

Users	
SNMP username	<input type="text"/>
SNMP group	<input type="text"/>
Security level	noAuthNoPriv ▼
Authentication protocol:	MD5 ▼
Authentication password:	<input type="password"/>
Privacy protocol:	DES ▼
Privacy password:	<input type="password"/>
Ipv4 access control list	<input type="text"/>
Ipv6 access control list	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Figure 13.

<b>SNMP username</b>	User name to operate, 1-32 characters.	
<b>SNMP group</b>	User group to join, 1-32 characters.	
<b>Security level</b>	noAuthNoPriv	Uncertified non-encrypted level.
	authNoPriv	Authentication but not encryption level.
	authpriv	Authentication and encryption level.
<b>Authentication protocol:</b>	MD5	HMAC MD5 algorithm for authentication.
	SHA	Authentication uses HMAC SHA algorithms.
<b>Authentication password:</b>	Password for authentication.	
<b>Privacy protocol:</b>	DES	Encryption DES algorithm.
	AES	Encryption AES algorithm.
	3DES	Encryption with 3DES algorithm.
<b>Privacy password:</b>	Password for encryption.	
<b>Ipv4 access control list</b>	Standard IPv4 access control list number, range: 1-64 characters.	
<b>Ipv6 access control list</b>	Standard IPv6 access control list number, range: 1-64 characters.	

<b>Operation</b>	Add	Add SNMP users.
	Remove	Delete SNMP users.

### 1.2.1.2 Groups

SNMP group management module in which users can add or delete SNMP group operations.

Groups	
SNMP group	<input type="text"/>
Security level	noAuthNoPriv ▼
Read SNMP view	<input type="text"/>
Write SNMP view	<input type="text"/>
Notify SNMP view	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Figure 14.

<b>SNMP group</b>	User group name to operate, 1-32 characters.	
<b>Security level</b>	noAuthNoPriv	Uncertified non-encrypted level.
	authNoPriv	Authentication but not encryption level.
	authpriv	Authentication and encryption level.
<b>Read SNMP view</b>	Name of readable view, including 1-32 characters.	
<b>Write SNMP view</b>	Name of writable view, including 1-32 characters.	
<b>Notify SNMP view</b>	Notice the name of the view, including 1-32 characters.	
<b>Operation</b>	Add	Add SNMP groups.
	Remove	Delete SNMP groups.

### 1.2.1.3 Views

SNMP view management module in which users can add or delete SNMP view operations.

Views		
SNMP view	<input type="text"/>	
OID	<input type="text"/>	
Type:	Include ▼	
Operation	Add ▼	
<input type="button" value="Apply"/>		
SNMP view	OID	Type
v1defaultviewname	1.0.	Include
v1defaultviewname	1.2.	Include
v1defaultviewname	1.3.	Include

Figure 15.

<b>SNMP view</b>	User view name to operate, 1-32 characters.	
<b>OID</b>	OID number to operate, decimal.	
<b>Type:</b>	Include	Include this OID.
	Exclude	Exclude this OID.
<b>Operation</b>	Add	Add view.
	Remove	Delete view.

#### 1.2.1.4 SNMP engineid configuration

SNMP Engineid configuration module, the user can configure SNMP Engineid operation in this module.

The figure shows a configuration window titled "SNMP engineid configuration". It contains two main input fields: "Engineid" and "Operation". The "Operation" field is a dropdown menu currently set to "Configuration". Below these fields is an "Apply" button. Below the configuration area is a list box showing the current "Engineid" value as "18c308c6b3c91aab".

Figure 16.

<b>Engineid</b>	Engine id, Hex, 1-32 characters.	
<b>Operation</b>	configuration	Configuration operations.
	Default	Restore default (default is company ID plus local MAC address).

#### 1.2.2 SNMP management

SNMP network management function switch module, users can enable or disable SNMP functions.

The figure shows a configuration window titled "SNMP management". It contains four state selection fields: "SNMP Agent state", "RMON state", "Trap state", and "Security IP state". Each field has a dropdown menu currently set to "Open". Below these fields is an "Apply" button.

Figure 17.

### 1.2.3 Community managers

The group string management module where users can SNMP group string management and configure TRAP management settings.

The image shows two screenshots of configuration forms. The top form is titled 'Community managers' and contains the following fields: 'Community string' (text input), 'Access priority' (dropdown menu with 'Read only' selected), and 'Operation' (dropdown menu with 'Add' selected). Below these fields is an 'Apply' button. The bottom form is titled 'TRAP manager configuration' and contains the following fields: 'Trap receiver' (text input), 'Community string' (text input), 'Version' (dropdown menu with '1' selected), 'Security level' (dropdown menu with 'noAuthNoPriv' selected), and 'Operation' (dropdown menu with 'Add' selected). Below these fields is an 'Apply' button.

Figure 18.

<b>Community string</b>	Community string name, 1-255 characters.	
<b>Access priority</b>	Read only	Read-only permission level.
	Read and write	Read and write permission level.
<b>Operation</b>	Add	Do Community string add operations.
	Remove	Do Community string delete operations.

<b>Trap receiver</b>	Recipient IPv4/IPv6 address of Trap information.	
<b>Community string</b>	Community string name, V1/V2 version: 1-255 characters, V3 version: 1-24 characters.	
<b>Version</b>	Three versions: V1/V2C/V3.	
<b>Security level (V3 version support only)</b>	noAuthNoPriv	Uncertified non-encrypted level.
	authNoPriv	Authentication but not encryption level.
	authpriv	Authentication and encryption level.
<b>Operation</b>	Add	For Trap information receiver add operation.
	Remove	For Trap information receiver remove operation.

### 1.2.4 Configure snmp manager security IP

The administrator IP the address setting module, where the user can add or delete the SNMP manager's safe IP address.

Figure 19.

<b>Security IP address</b>	SNMP Management Security IPv4/IPv6 Address.	
<b>Operation</b>	Add	Add a Security IP.
	Remove	Remove a Security IP.

### 1.2.5 SNMP statistics

SNMP statistical information module, users in this module can view the SNMP function feedback information.

```

Information feedback window
SW1# show snmp
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors (Max packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Get-response PDUs
  0 SNMP trap PDUs
  
```

Figure 20.

## 1.3 SSH management

### 1.3.1 Switch on-off SSH

SSH function switch module in which the user can enable or disable switches by SSH.

Figure 21.



### 1.3.2 SSH management

SSH management configuration module, the user can configure the SSH timeout, SSH authentication times and SSH RSA secret key modulus, and can also view the user login status of the SSH server.

The screenshot shows three configuration panels for SSH management:

- SSH timeout management:** Includes fields for 'SSH timeout' and 'Operation' (set to 'Configuration'), with an 'Apply' button.
- SSH reauthentication management:** Includes fields for 'SSH reauthentication' and 'Operation' (set to 'Configuration'), with an 'Apply' button.
- Create SSH RSA key:** Includes a field for 'SSH RSA key' (set to '1024') and an 'Apply' button.

Below these panels is a table titled 'Show SSH Server's State' with the following columns:

Num	Version	Status	SSH username

Figure 22.

<b>SSH timeout</b>	Timeout of exit SSH login status, 10-600 seconds.	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Recovery default (default 180 s).
<b>SSH reauthentication</b>	SSH number of re-authentications when logged in, 1-10.	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Restore default (default re-authentication 3 times).
<b>SSH RSA key</b>	A module for calculating RSA keys, ranging from 768-2048, default 1024.	

## 1.4 Firmware update

### 1.4.1 TFTP service

#### 1.4.1.1 TFTP client service

TFTP client service module, the user can upload or download files by TFTP way, and can upgrade the firmware of the switch by this method.

The screenshot shows the 'TFTP client service' configuration panel with the following fields:

- Server IP address
- Local file name
- Server file name
- Operation type: Upload (dropdown menu)
- Transmission type: binary (dropdown menu)

An 'Apply' button is located at the bottom right of the panel.

Figure 23.

<b>Server IP address</b>	TFTP address IP peer server, point decimal.	
<b>Local file name</b>	Name of destination file to upload or download, 1-100 characters.	
<b>Server file name</b>	Source name to upload or download, 1-100 characters.	
<b>Operation type</b>	Upload	To upload files.
	Download	To download files.
<b>Transmission type</b>	binary	Transfer files in binary format (default).
	ascii	Transfer files in ascii format.

#### 1.4.1.2 TFTP server service

TFTP server-side service module, users can configure the TFTP server settings in this module.

Figure 24.

<b>Server state</b>	Open	Enable TFTP server functionality.
	Close	Disable TFTP server functionality (default).
<b>TFTP Timeout</b>	TFTP service exit timeout, range 5-3600 s (default 600 s).	
<b>TFTP Retransmit times</b>	TFTP number of retransmissions after transmission failure, range 1-20 (default 5).	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Restore default.

#### 1.4.2 FTP service

##### 1.4.2.1 FTP client service

FTP client service module, the user can upload or download files by FTP way, and can upgrade the firmware of the switch by this method.

FTP client service	
Server IP address	<input type="text"/>
User	<input type="text"/>
Password	<input type="text"/>
Local file name	<input type="text"/>
Server file name	<input type="text"/>
Operation type	Upload <input type="button" value="v"/>
Transmission type	binary <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 25.

<b>Server IP address</b>	FTP address IP peer server, point decimal.	
<b>User</b>	FTP server-to-server username, 1-100 characters.	
<b>Password</b>	FTP server-side user password, 1-100 characters.	
<b>Local file name</b>	Name of destination file to upload or download, 1-100 characters.	
<b>Server file name</b>	Source name to upload or download, 1-100 characters.	
<b>Operation type</b>	Upload	To upload files.
	Download	To download files.
<b>Transmission type</b>	binary	Transfer files in binary format (default).
	ascii	Transfer files in ascii format.

#### 1.4.2.2 FTP server service

FTP server service module, the user can configure various settings of FTP server.

FTP server service	
FTP server State	Close <input type="button" value="v"/>
FTP Timeout	<input type="text" value="600"/>
Operation	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

FTP user name and password setting	
User	<input type="text"/>
Password	<input type="text"/>
State	Plain text <input type="button" value="v"/>
Operation type	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 26.

<b>FTP server state</b>	Open	Enable FTP server functionality.
	Close	Disable FTP server functionality (default).

<b>FTP Timeout</b>	FTP service exit timeout, range 5-3600 s (default 600 s).	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Restore default.

<b>User</b>	FTP service username to operate, 1-32 characters.	
<b>Password</b>	FTP service user password to operate, 1-16 characters.	
<b>State</b>	Plain text	Do not encrypt FTP service password.
	Encrypted	Encryption of FTP service passwords.
<b>Operation type</b>	Add	Add operations.
	Remove	Delete operations.

## 1.5 Telnet server configuration

### 1.5.1 Telnet server state

Telnet server status module, where users can enable or disable login switches by Telnet.

Telnet server state	
Telnet server state	Open ▾
Apply	

Figure 27.

### 1.5.2 Max numbers of telnet access connection

Telnet connect the maximum number module, the user can configure the maximum number of connections to the switch by Telnet.

Max numbers of telnet access connection	
Telnet access connection number	<input type="text"/>
Operation	Configuration ▾
Apply	

Information feedback window	
Telnet access connection number	5

Figure 28.

<b>Telnet access connection number</b>	Maximum number of connections logged in by Telnet, range 1-16 (default 5).	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Restore default.

## 1.6 Maintenance and debugging command

### 1.6.1 Debug command

Maintenance and debugging command module. the user can configure the mapping relationship between host and IP, also can run ping command and route tracking command.

The figure shows three configuration windows. The 'Basic host configuration' window has fields for 'Host name', 'IP address', and 'Operation' (with a dropdown menu set to 'Add'), and an 'Apply' button. The 'PING' window has fields for 'Host name' and 'IP address', and an 'Apply' button. The 'Traceroute' window has fields for 'IP address', 'Host name', 'Hops', and 'timeout', and an 'Apply' button.

Figure 29.

<b>Host name</b>	Host name for mapping, 1-64 characters.	
<b>IP address</b>	IP address for mapping, point decimal.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

<b>Host name</b>	To ping the host name, configure the mapping relationship between the host and the IP.
<b>IP address</b>	IP address to ping, decimal.

<b>IP address</b>	IP address for routing tracing, point decimal.
<b>Host name</b>	Host name for routing tracing, 1-64 characters.
<b>Hops</b>	Number of hops, route, range 1-255.
<b>timeout</b>	Tracking timeout, 100-10000.

### 1.6.2 show clock

This module is used to display the current system time and date.

```
Information feedback window
SW1# show clock
Current time: Wed Jan 01 01:03:21 2020 [UTC]
```

Figure 30.

### 1.6.3 show cpu usage

This module is used to display resource usage cpu current system.

```
Information feedback window
SW1# show cpu usage
Last 5 second CPU IDLE: 83%
Last 30 second CPU IDLE: 92%
Last 5 minute CPU IDLE: 92%
From running CPU IDLE: 91%
```

Figure 31.

### 1.6.4 show memory usage

This module is used to display the current system memory resource usage.

```
Information feedback window
SW1# show memory usage
The memory total 128 MB , free 68009984 bytes , usage is 49.33%
```

Figure 32.

### 1.6.5 show flash

This module is used to display the current system flash storage resource usage.

```
Information feedback window
SW1# show flash
total 22789K
-rw- 10817705 mantest.img
-rw- 12514223 nos.img
-rw- 1384 startup.cfg
-rw- 1361 test1.cfg
Drive : flash:
Size:30.0M Used:23.5M Available:6.5M Use:78%
```

Figure 33.

### 1.6.6 show running-config

This module is used to display configuration information in the current system run.

```
Information feedback window
SW1# show run
!
no service password-encryption
!
hostname SW1
sysLocation Russia, Moscow, Ryabinovaya st, 26 bld 2
sysContact +7(495)797-3311
!
username admin privilege 15 password 0 admin
!
!
!
ssh-server enable
ssh-server timeout 600
!
!
web language english
!
snmp-server enable
snmp-server enable traps
!
!
```

Figure 34.

### 1.6.7 show switchport interface

This module is used to display the port information of the current switch.

```

Information feedback window
SW1# show switchport interface
Ethernet1/0/1
Type :Universal
Mode :Trunk
Port VID :1
Trunk allowed Vlan: 1-4094
Ethernet1/0/2
Type :Universal
Mode :Trunk
Port VID :1
Trunk allowed Vlan: 1-4094

```

Figure 35.

### 1.6.8 show tcp

This module is used to display tcp connection information for the current switch.

```

Information feedback window
SW1# show tcp

```

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State	IF	VRF
192.168.2.1	80	192.168.2.200	54216	ESTABLISHED	0	0
127.0.0.1	2650	127.0.0.1	32785	ESTABLISHED	0	0
127.0.0.1	32785	127.0.0.1	2650	ESTABLISHED	0	0
0.0.0.0	80	0.0.0.0	0	LISTEN	0	0
0.0.0.0	22	0.0.0.0	0	LISTEN	0	0
0.0.0.0	23	0.0.0.0	0	LISTEN	0	0
127.0.0.1	2650	0.0.0.0	0	LISTEN	0	0

Figure 36.

### 1.6.9 show udp

This module is used to display udp connection information for the current switch.

```

Information feedback window
SW1# show udp

```

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	161	0.0.0.0	0	CLOSE
0.0.0.0	3071	0.0.0.0	0	CLOSE

Figure 37.

### 1.6.10 show telnet login

This module is used to display the user information that is currently logged in to the switch by telnet.

```

Information feedback window
SW1# show telnet login
Authenticate login by local.
Login user:

```

Figure 38.

### 1.6.11 show version

This module is used to display the user information that is currently logged in to the switch by telnet.

Client IP address:192.168.2.200

System Version Information	
Device:	Switch, sysLocation: Russia, Moscow, Ryabinovaya st, 26 bld 2.
CPU MAC	08-c6-b3-c9-1a-ab
VLAN MAC	08-c6-b3-c9-1a-ac
SoftWare Version	8.101.30
BootRom Version	2011.12.16
HardWare Version	1.2
CPLD Version	N/A
Serial No.:	7135070820200001
Last reboot	was cold reset.
Uptime is	0 weeks, 0 days, 1 hours, 9 minutes

Figure 39.

## 2. Module management

### 2.1 Show boot-files

This module is used to display system firmware and configuration files for the next restart of the switch.

Information feedback window	
Booted files on switch	
The primary img file at the next boot time:	flash:/nos.img
The backup img file at the next boot time:	flash:/nos.img
Current booted img file:	flash:/nos.img
The startup-config file at the next boot time:	flash:/startup.cfg
Current booted startup-config file:	flash:/startup.cfg

Figure 40.

### 2.2 Set Boot IMG and Startup-Config

This module is used to configure the system firmware and configuration files for the next restart of the switch.

Set boot files in Active Master		
Primary IMG	<input type="text"/>	Set
Backup IMG	<input type="text"/>	Set
Startup-config	<input type="text"/>	Set
<input type="text"/>		

Figure 41.

<b>Primary IMG</b>	System firmware first boot item when switch restarts.
<b>Backup IMG</b>	System firmware second boot item when switch restarts.
<b>Startup-config</b>	Start configuration file on switch restart.

## 3. Port configuration

### 3.1 Ethernet port configuration

This chapter mainly configures the related port function of Ethernet port.



### 3.1.1 Port layer 1 attribution configuration

This page is mainly used to configure the basic properties of physical ports.

To display the "Port layer 1 attribution configuration" page, click Port configuration -> Ethernet port configuration -> Port layer 1 attribution configuration, click "Apply" to configure.

Port configuration		
Port	Ethernet1/0/1 ▾	
mdi	auto ▾	<input type="checkbox"/>
Admin status	no shutdown ▾	<input type="checkbox"/>
Speed/Duplex status	Auto ▾	<input type="checkbox"/>
Module type	auto-detected ▾	<input type="checkbox"/>
1000M Mode	▾	<input type="checkbox"/>
Fiber portMode	Auto ▾	<input type="checkbox"/>
Flow control status	Invalid flow control ▾	<input type="checkbox"/>
Loopback	no loopback ▾	<input type="checkbox"/>
		<input type="button" value="Apply"/>

Figure 42.

entry	describe
<b>Mdi</b>	Invalid settings.
<b>Admin status</b>	Port status: Shutdown: enable no shutdown: disable
<b>Speed/Duplex status</b>	Port rate and Working mode.
<b>Module type</b>	Port types such as Ethernet port, Gigabit optical port, etc.
<b>1000M Mode</b>	Mode configuration in Gigabit port configuration.
<b>Fiber portMode</b>	Invalid settings.
<b>Flow control status</b>	Port Flow Control.
<b>Loopback</b>	Port loop detection: Loopback: enable No Loopback: disable
<b>Port rate</b>	Port rate: 10:10M 100:100M 1000:1000M Auto: Automatic negotiation rate
<b>Working mode</b>	Working mode:

	Auto: Automatic negotiation mode Half: Half duplex mode Full: Full duplex mode
--	--

Port list								
Port	mdi	managementStatus	Speed	Mode	1000M Mode	Fiber portMode	Flow control	loopback
Ethernet1/0/1	auto	No Shutdown	10M	full	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/2	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/3	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/4	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/5	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/6	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/7	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/8	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback

Figure 43.

<b>entry</b>	describe
<b>Mdi</b>	Invalid settings.
<b>managementStatus</b>	Port enable status: Shutdown: enable no shutdown: disable
<b>Speed</b>	Port rate: 10:10M 100:100M 1000:1000M Auto: Automatic negotiation rate
<b>Mode</b>	Working mode: Auto: Automatic negotiation mode Half: Half duplex mode Full: Full duplex mode
<b>1000M Mode</b>	Mode configuration in Gigabit port configuration.

<b>Fiber portMode</b>	Invalid settings.
<b>Flow control</b>	Port Flow Control.
<b>Loopback</b>	Port loop detection: Loopback: enable No Loopback: disable

### 3.1.2 Bandwidth control configuration

The page is configured for bandwidth control.

To display the "Bandwidth control configuration" page, click Port configuration -> Ethernet port configuration -> Bandwidth control configuration, click "Apply" to configure.

Bandwidth control configuration			
Port	Bandwidth control level	Control type	Operation
Ethernet1/0/1 ▾		Transmit ▾	Configuration ▾
			Apply

Figure 44.

<b>entry</b>	describe
<b>Bandwidth control level</b>	Bandwidth control rate in the range of Kbps 1-1000000.
<b>Control type</b>	Control type: Transmit:send receive:receive Both: send and receive
<b>Operation</b>	Configuration: User-defined configuration Default: Restore default configuration

Port list		
Port	Ingress bandwidth threshold(Kb)	Engress bandwidth threshold(Kb)
Ethernet1/0/1	1000000	1000000
Ethernet1/0/2	1000000	1000000
Ethernet1/0/3	1000000	1000000
Ethernet1/0/4	1000000	1000000
Ethernet1/0/5	1000000	1000000
Ethernet1/0/6	1000000	1000000
Ethernet1/0/7	1000000	1000000
Ethernet1/0/8	1000000	1000000

Figure 45.

<b>Port</b>	Ethernet port name.
-------------	---------------------

<b>Ingress bandwidth threshold(Kb)</b>	Displays the current received data bandwidth limit in the range of Kbps 1-1000000.
<b>Engress bandwidth threshold(Kb)</b>	Displays the bandwidth limit of the current sending data, ranging from 1-1000000kbps.

### 3.1.3 Switchport description

The page can be used to set the port name.

To display the "Switchport description" page, click Port configuration -> Ethernet port configuration -> Switchport description, click "Apply" to configure.

Switchport description	
Port	Ethernet1/0/1 ▾
Description	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 46.

<b>Port</b>	Ethernet port name.
<b>Description</b>	Port description name, length 1-200 characters.
<b>Operation</b>	Configuration: User-defined configuration Default: Restore default configuration

Port list	
Port	Description
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	

Figure 47.

<b>Port</b>	Ethernet port name.
<b>Description</b>	Port description name, length 1-200 characters.

### 3.1.4 Port combo forced mode config

This page can be used to configure the combo port interface type to switch.

To display the "Port combo forced mode config" page, click Port configuration -> Ethernet port configuration -> Port combo forced mode config, click "Apply" to configure.

Port combo forced mode config	
Port	Ethernet1/0/1 ▾
forced mode	copper-forced ▾
<b>Apply</b>	

Figure 48.

<b>Port</b>	Ethernet port name.
<b>forced mode</b>	Configure combo port current interface type: Copper-forced: copper Sfp-forced: fiber sfp-preferred-auto: Automatic switching

Information feedback window	
Port	forced mode
Ethernet1/0/1	no support
Ethernet1/0/2	no support
Ethernet1/0/3	no support
Ethernet1/0/4	no support
Ethernet1/0/5	no support
Ethernet1/0/6	no support
Ethernet1/0/7	no support
Ethernet1/0/8	no support

Figure 49.

<b>Port</b>	Ethernet port name.
<b>forced mode</b>	Configure combo port current interface type:

	Copper-forced: copper Sfp-forced: fiber sfp-preferred-auto: Automatic switching
--	---

### 3.1.5 port scan mode

This function switch is not supported for the time being.

## 3.2 VLAN interface configuration

This chapter mainly realizes the creation of VLAN interface and the configuration of interface address.

### 3.2.1 Add interface VLAN

This page is mainly used to create VLAN interfaces.

To display the "add interface VLAN" page, click Port configuration -> VLAN interface configuration -> add interface VLAN, click "Apply" to configure.

Add interface VLAN	
VLAN ID	1 ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 50.

entry	describe
VLAN ID	VLAN ID created.
Operation	Action: Add/Remove

Vlan ID	State
Vlan1	Layer 3 interface
Vlan5	Non layer 3 interface

Figure 51.

entry	describe
VLAN ID	VLAN ID added.
State	Is VLAN a layer 3 interface.

### 3.2.2 L3 interface IP address mode configuration

The page can be used to configure IP address and subnet mask for the VLAN interface.

To display the "L3 interface IP address mode configuration" page, click Port configuration -> VLAN interface configuration -> L3 interface IP address mode configuration, click "Apply" to configure.

L3 interface IP address mode configuration	
VLAN interface	Vlan1 ▾
IP mode	Specify IP address ▾
Interface IP address	<input type="text"/>
Interface network mask	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 52.

<b>entry</b>	describe
<b>VLAN interface</b>	VLAN ID of layer 3 interface created.
<b>IP mode</b>	Access to interface IP address: bootp-client: bootp-client Automatic acquisition dhcp-client: dhcp-client Automatic acquisition Specify IP address: User self configuration
<b>Interface IP address</b>	IP address, e.g. A.B.C D.
<b>Interface network mask</b>	Network mask: for example: 255.255.255.0.
<b>Operation</b>	Action: Add/Remove

### 3.3 SPAN configuration

This section can be used for port mirroring function configuration.

To display the "SPAN configuration" page, click Port configuration -> VLAN interface configuration -> SPAN configuration, click "Apply" to configure.

Destination port (SPAN) configuration	
Session	1 ▾
Destination port (SPAN)	1/0/1 ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 53.

<b>entry</b>	describe
<b>Session</b>	Mirror Session.
<b>Destination port (SPAN)</b>	Mirror destination port.

<b>Operation</b>	Action: Add/Remove
------------------	--------------------

SPAN configuration	
Session	Destination port (SPAN)
1	Ethernet1/0/1

Figure 54.

<b>entry</b>	describe
<b>Session</b>	Mirror Session.
<b>Destination port (SPAN)</b>	Mirror destination port.

Source port (SPAN) configuration	
Session	1 ▾
Source port (SPAN) list	1/0/1 ▾
CPU to be used for source port	<input type="checkbox"/>
Access list	
Mirror direction	both ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 55.

<b>entry</b>	describe
<b>Session</b>	Mirror Session.
<b>Source port (SPAN) list</b>	Mirror Source Port.
<b>CPU to be used for source port</b>	CPU used as the source of data.
<b>Access list</b>	The access control list set for the mirror source port.
<b>Mirror direction</b>	What kind of data is needed to filter to the destination port: Both: Sending and receiving Rx: receive Tx: send
<b>Operation</b>	Add: Add configuration for the corresponding operation Remove: Delete the corresponding configuration



Rspan vlan configuration	
VLAN ID	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 56.

<b>entry</b>	describe
<b>VLAN ID</b>	VLAN ID.
<b>Operation</b>	Add: Add configuration for the corresponding operation Remove: Delete the corresponding configuration

reflector port (SPAN) configuration	
Session	1 <input type="button" value="v"/>
Port	Ethernet1/0/1 <input type="button" value="v"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 57.

<b>entry</b>	describe
<b>Session</b>	Mirroring Session.
<b>Port</b>	Ethernet port number.
<b>Operation</b>	Add: Add configuration for the corresponding operation Remove: Delete the corresponding configuration

remote vlan configuration	
Session	1 <input type="button" value="v"/>
VLAN ID	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 58.

<b>entry</b>	describe
<b>Session</b>	Mirroring Session.
<b>VLAN ID</b>	VLAN ID.
<b>Operation</b>	Add: Add configuration for the corresponding operation Remove: Delete the corresponding configuration

sample rate configuration	
Session	1 ▾
rate	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 59.

<b>entry</b>	describe
<b>Session</b>	Mirroring Session.
<b>rate</b>	It indicates how many packets are mirrored to the destination port.

Source port (SPAN) list							
session 1		session 2		session 3		session 4	
Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 60.

<b>entry</b>	describe
<b>Session</b>	Mirroring Session.
<b>Tx/Rx</b>	Direction of source port mirror data.
<b>Ethernet1/0/10</b>	Mirror Source Port for Session.

### 3.4 Loopback-detection configuration

This chapter is mainly for port loop detection function configuration.

#### 3.4.1 Port Loopback-detection mode configuration

The configuration of the page is used to set the loop detection control method.

To display the "Port Loopback-detection mode configuration" page, click Port configuration -> Port Loopback-detection configuration -> Port Loopback-detection mode configuration, click "Apply" to configure.

Port Loopback-detection mode configuration	
Port	Ethernet1/0/1 ▾
Loopback-detection mode	shutdown ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 61.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Loopback-detection mode</b>	Operation in case of loop: Shutdown: Disable port block: Block port
<b>Operation</b>	Operation of loop detection function: Add: Open loop detection and configure control mode Remove: Disable loop detection

Information feedback window	
Port	Loopback-detection mode
Ethernet1/0/1	no control mode
Ethernet1/0/2	no control mode
Ethernet1/0/3	no control mode
Ethernet1/0/4	no control mode
Ethernet1/0/5	no control mode
Ethernet1/0/6	no control mode
Ethernet1/0/7	no control mode
Ethernet1/0/8	no control mode

Figure 62.

<b>entry</b>	describe
--------------	----------

<b>Port</b>	Ethernet port name.
<b>Loopback-detection mode</b>	Shutdown: Disable port block: Block port no control mode: Disable port loop detection

### 3.4.2 VLAN Loopback-detection configuration

This page can be used to configure VLAN loop detection function enabled or disabled.

To display the "VLAN Loopback-detection configuration" page, click Port configuration -> Port Loopback-detection configuration -> VLAN Loopback-detection configuration, click "Apply" to configure.

VLAN Loopback-detection configuration	
Port	Ethernet1/0/1 ▾
VLAN ID	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 63.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>VLAN ID</b>	VLAN ID, range 1-4094.
<b>Operation</b>	Add: Enable VLAN loop detection Remove: Disable VLAN loop detection

### 3.4.3 Loopback-detection interval-time configuration

This page can be used to configure the loop detection interval.

To display the "Loopback-detection interval-time configuration" page, click Port configuration -> Port Loopback-detection configuration -> Loopback-detection interval-time configuration, click "Apply" to configure.

Loopback-detection interval-time configuration	
Loopback-detection interval time	<input type="text"/>
no Loopback-detection interval time	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 64.

<b>entry</b>	describe
<b>Loopback-detection interval time</b>	Interval time between loops, size 5-300 seconds.
<b>no Loopback-detection interval time</b>	No loop interval, size 1-30 seconds.
<b>Operation</b>	Configuration: Set the test time by yourself. Default: Restore the default configuration, there is a loop detection interval of 5 seconds, there is no loop detection interval of 3 seconds.

### 3.4.4 Loopback-detection control recovery configuration

This page is used to configure loop detection to automatically return to an uncontrolled state.

To display the "Loopback-detection control recovery configuration" page, click Port configuration -> Port Loopback-detection configuration -> Loopback-detection control recovery configuration, click "Apply" to configure.

Figure 65.

<b>entry</b>	describe
<b>Recovery switch timeout</b>	When a port is disabled or blocked due to a loop, it automatically recovers to an uncontrolled time, the size range is 0-3600 seconds. When it is configured as 0, the auto recovery function is disabled.

## 3.5 Isolate-port configuration

This section can set up port isolation related functions.

### 3.5.1 Isolate-port group configuration

This page can be used to add or delete isolated groups.

To display the "Isolate-port group configuration" page, click Port configuration -> Isolate-port configuration -> Isolate-port group configuration, click "Apply" to configure.

Figure 66.

<b>entry</b>	describe
<b>Group name</b>	Isolation group name, example: aaaa.
<b>Operation</b>	Add: Create an isolation group Remove: Delete an isolation group

### 3.5.2 Interface join group config

This page can be used to add ports for isolation groups.

To display the "Interface join group config" page, click Port configuration -> Isolate-port configuration -> Interface join group config, click "Apply" to configure.

Figure 67.

<b>entry</b>	describe
<b>Group name</b>	Created isolation group name, example: aaaa.
<b>Port</b>	Ethernet port name.
<b>Operation</b>	Add: Add ports to the isolation group Remove: Delete ports in isolation groups

### 3.5.3 show isolate-port group

This page is used to display isolation group information.

To display the "show Isolate-port group" page, click Port configuration -> Isolate-port configuration -> show Isolate-port group, click "Apply" to view.

Figure 68.

<b>entry</b>	describe
<b>Group name</b>	Created isolation group name, example: aaaa.

### 3.6 Port storm-control config

This chapter can set up storm control related functions.

#### 3.6.1 Port storm-control config

This page can be configured for the storm control function of the port.

To display the "Port storm-control config" page, click Port configuration -> Port storm-control config -> Port storm-control config, click "Apply" to configure.

storm-control configuration	
Port	Ethernet1/0/1 ▾
storm-control type	broadcast ▾
storm-control value	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 69.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>storm-control type</b>	Broadcast/Multicast/Unicast
<b>storm-control value</b>	Storm control rate, ranging from 1-1000000 kbps or 1-1488095 pps.
<b>Operation</b>	Add: Turn on the storm control function and configure the speed limit Remove: Disable Storm Control

Information feedback window	
Port	storm-control type
Ethernet1/0/1	None
Ethernet1/0/2	None
Ethernet1/0/3	None
Ethernet1/0/4	None
Ethernet1/0/5	None
Ethernet1/0/6	None
Ethernet1/0/7	None
Ethernet1/0/8	None

Figure 70.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>storm-control type</b>	Broadcast/Multicast/Unicast

### 3.6.2 storm-control bypass configuration

This page can configure storm control unit, filter protocol, filter protocol status and other functions.

To display the "storm-control bypass configuration" page, click Port configuration -> Port storm-control config -> storm-control bypass configuration, click "Apply" to configure.

storm-control configuration	
storm-control type:	bypass ▾
storm-control bypass protocol:	arp ▾
storm-control bypass protocol status:	disable ▾
Apply	

Figure 71.

<b>entry</b>	describe
<b>storm-control type</b>	Bypass: Bypass Protocol Kbps: Storm control rate units pps: Storm control rate units
<b>storm-control bypass protocol</b>	Broadcast Storm Filter Agreement
<b>storm-control bypass protocol status</b>	Disable: Disable protocol filtering Enable: Enable protocol filtering



### 3.7 Port rate-violation config

This chapter is mainly used for the configuration of rate limiting functions.

#### 3.7.1 rate-violation configuration

This page is mainly used to configure the rate limit function.

To display the "rate-violation configuration" page, click Port configuration -> Port rate-violation config -> rate-violation configuration, click "Apply" to configure.

Port rate-violation config	
Port	Ethernet1/0/1 ▾
rate-violation type	all ▾
rate-violation value	
rate-violation sub type	shutdown ▾
rate-violation recover time	
Operation	Add ▾
Apply	

Figure 72.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>rate-violation type</b>	Type of breach: All/Broadcast/Multicast/Unicast/ Control: Operation violation
<b>rate-violation value</b>	Limit rate, range 200-2000000.
<b>rate-violation sub type</b>	Overspeed operation: Shutdown: Disable port Block: Block port
<b>rate-violation recover time</b>	The time when the port overspeed is automatically resumed after it is disabled, if the size is 0-86400 seconds, configuring 0 seconds means no automatic recovery.
<b>Operation</b>	Add: Function Enable Remove: Function disabled

### 3.8 Port virtual-cable-test config

This chapter can be used to detect port link lines.

#### 3.8.1 virtual-cable-test configuration

This chapter can be used to detect port link lines.

To display the "virtual-cable-test configuration" page, click Port configuration -> Port virtual-cable-test config -> virtual-cable-test configuration, click "Apply" to configure.

**virtual-cable-test configuration**

Port Ethernet1/0/1 ▼

Apply

**Information feedback window**

```

Switch# virtual-cable-test interface Ethernet1/0/14
Interface Ethernet1/0/14:
-----
Cable pairs      Cable status      Length (meters)
-----
(1, 2)           well              13
(3, 6)           well              13
(4, 5)           well              13
(7, 8)           well              13
    
```

Figure 73.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.

### 3.9 Port debug and maintenance

This section is mainly used to view port, overall traffic statistics, port rate violation configuration and other information view.

#### 3.9.1 Show port information

This page can be used to view port details.

To display the "Show port information" page, click Port configuration -> Port debug and maintenance -> Show port information, click "Apply" to view.

Please select port: Ethernet1/0/1 ▼

**Information feedback window**

```

Interface brief:
 Ethernet1/0/1 is down, line protocol is down
 Ethernet1/0/1 is layer 2 port, alias name is (null), index is 1
 Hardware is Gigabit-TX, address is 00-1f-ce-10-b0-1b
 PVID is 1
 MTU 1500 bytes, BW 10000 Kbit
 Time since last status change: 0w-0d-0h-36m-32s (2192 seconds)
 Encapsulation ARPA, Loopback not set
 Auto-duplex , Auto-speed
 FlowControl is off, MDI type is auto
    
```

Figure 74.

### 3.9.2 Show entire traffic information

This page can be used to view statistics of overall traffic.

To display the "Show entire traffic information" page, click Port configuration -> Port debug and maintenance -> Show entire traffic information, click "Apply" to view.

Show entire traffic information										
Port	Receiving statistics					Transmitting statistics				
	Total packets	Error packets	Dropped packets	5 minute rate(packets/sec)	Last 5 second rate(packets/sec)	Total packets	Error packets	Dropped packets	5 minute rate(packets/sec)	Last 5 second rate(packets/sec)
Ethernet1/0/1	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/2	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/3	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/4	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/5	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/6	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/7	0	0	0	0	0	0	0	0	0	0
Ethernet1/0/8	0	0	0	0	0	0	0	0	0	0

Figure 75.

### 3.9.3 Show rate violation port

This page can be used to view port rate violation function configuration information.

To display the "Show rate violation port" page, click Port configuration -> Port debug and maintenance -> Show rate violation port, click "Apply" to view.

Rate-violation port state information		
Port	Port rate-violation control mode	Rate-violation port state
Ethernet1/0/1	shutdown	down

Figure 76.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Port rate-violation control mode</b>	Shutdown: Disable port Block: Block port
<b>Rate-violation port state</b>	Status of current port: Down: Not connected Up: Connected Forwarding: forward Block: block

## 3.10 uldp configuration

This chapter is mainly used for the configuration of single link detection function.

### 3.10.1 uldp enable config

This page can be used to enable or disable single link detection protocols.

To display the "uldp enable config" page, click Port configuration -> uldp configuration -> uldp enable config, click "Apply" to configure.

uldp global enable configuration	
uldp global enable type	uldp enable ▾
Operation	Enable ▾
Apply	

Figure 77.

<b>entry</b>	describe
<b>uldp global enable type</b>	<p>uldp enable: Turn on the ULDP function of all ports that support ULDP functions.</p> <p>uldp aggressive-mode: Configure all ports ULDP working mode for positive mode.</p> <p>uldp manual shutdown: global close auto disable port, switch to manual close port.</p>
<b>Operation</b>	<p>Enable: Function Enable</p> <p>Disable: Function Disable</p>

uldp port enable configuration	
Port	Ethernet1/0/1 ▾
uldp port enable type	uldp port enable ▾
Operation	Enable ▾
Apply	

Figure 78.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>uldp global enable type</b>	<p>Uldp port enable: Turn on the ULDP function of the specified port.</p> <p>uldp port aggressive-mode: Configure the specified port ULDP working mode to positive mode.</p>
<b>Operation</b>	<p>Enable: Function Enable</p> <p>Disable: Function Disable</p>

### 3.10.2 uldp Hello message config

This page is used to Hello the message sending interval.

To display the "uldp Hello message config" page, click Port configuration -> uldp configuration -> uldp Hello message config, click "Apply" to configure.

Figure 79.

<b>entry</b>	describe
<b>uldp Hello message time</b>	Message sending interval, range 5-100 seconds.
<b>Operation</b>	Configuration: User self-configuration Default: Restore the default configuration, the default configuration is 10 seconds.

### 3.10.3 uldp recovery time config

This page can be used to configure ULDP auto recovery time.

To display the "uldp recovery time config" page, click Port configuration -> uldp configuration -> uldp recovery time config, click "Apply" to configure.

Figure 80.

<b>entry</b>	describe
<b>uldp Hello message time</b>	Automatic recovery time after the port is disabled, ranging from 30-86400 seconds to 0 seconds without automatic recovery.
<b>Operation</b>	Configuration: User self-configuration Default: Restore default configuration, default configuration is 0 seconds.

### 3.10.4 show uldp configuration

This page can be used to view port ULDP configuration information.

To display the "uldp recovery time config" page, click Port configuration -> uldp configuration -> uldp recovery time config, click "Apply" to view.

**show uldp configuration**

Port

**Information feedback window**

```
Switch# show uldp
uldp enable
uldp hello interval is          10
uldp shut down mode is         AUTO
uldp global work mode is       NORMAL
the total number of the port is 4
```

---

PortName	PhyLink	LineProto	WorkMode	PortState	NeighborNum
Ethernet1/0/25	UP	DOWN	NORMAL	INACTIVE	0
Ethernet1/0/26	UP	DOWN	NORMAL	INACTIVE	0
Ethernet1/0/27	UP	DOWN	NORMAL	INACTIVE	0
Ethernet1/0/28	UP	DOWN	NORMAL	INACTIVE	0

Figure 81.

### 3.11 LLDP configuration

This chapter can be used to configure LLDP related functions.

#### 3.11.1 LLDP configuration

This page can be configured to enable or disable LLDP functionality.

To display the "LLDP configuration" page, click Port configuration -> LLDP configuration -> LLDP configuration, click "Apply" to configure.

**LLDP global enable configuration**

lldp enable

Figure 82.

<b>entry</b>	describe
<b>lldp enable</b>	Enable: Global On LLDP Function Disable: Global Off LLDP Function

LLDP port enable configuration	
Port	Ethernet1/0/1 ▾
LLDP port enable type	LLDP port enable ▾
Operation	Enable ▾
Apply	

Figure 83.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>LLDP port enable type</b>	Enable or disable LLDP functions.
<b>Operation</b>	Turn on or off LLDP function.

### 3.11.2 LLDP port status config

This page can configure port status.

To display the "LLDP port status config" page, click Port configuration -> LLDP configuration -> LLDP port status config, click "Apply" to configure.

LLDP port status config	
Port	Ethernet1/0/1 ▾
LLDP port status	send ▾
Apply	

Figure 84.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>LLDP port status</b>	Send: Send only data Receive: Receive only data Both: Sending and receiving data simultaneously Disable: Both sending and receiving are prohibited

### 3.11.3 LLDP tx-interval config

This page can configure the interval between sending updates.

To display the "LLDP tx-interval config" page, click Port configuration -> LLDP configuration -> LLDP tx-interval config, click "Apply" to configure.

LLDP tx-interval config	
LLDP Hello message time	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 85.

<b>entry</b>	describe
<b>LLDP Hello message time</b>	Update message sending interval between 5-32768 seconds.
<b>Operation</b>	Configuration: User self-configuration Default: Restore the default configuration, the default configuration is 30 seconds.

### 3.11.4 LLDP msgTxHold config

This page can configure the value of the message aging time multiplier.

To display the "LLDP msgTxHold config" page, click Port configuration -> LLDP configuration -> LLDP msgTxHold config, click "Apply" to configure.

LLDP msgTxHold config	
LLDP msgTxHold value	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 86.

<b>entry</b>	describe
<b>LLDP msgTxHold value</b>	Numerical magnitude between 2-10.
<b>Operation</b>	Configuration: User self-configuration Default: Restore default configuration, default configuration is 4.

### 3.11.5 LLDP transmit delay config

This page can configure the sending delay time of the update message.



To display the "LLDP transmit delay config" page, click Port configuration -> LLDP configuration -> LLDP transmit delay config, click "Apply" to configure.

Figure 87.

<b>entry</b>	describe
<b>LLDP transmit delay value</b>	Value between 1-8192 seconds.
<b>Operation</b>	Configuration: User self-configuration Default: Restore default configuration for 2 seconds

### 3.11.6 LLDP notification interval config

This page can configure the interval between sending Trap messages.

To display the "LLDP notification interval config" page, click Port configuration -> LLDP configuration -> LLDP notification interval config, click "Apply" to configure.

Figure 88.

<b>entry</b>	describe
<b>LLDP notification interval value</b>	Value between 5 and 3600 seconds.
<b>Operation</b>	Configuration: User self-configuration Default: Restore default configuration for 5 seconds

### 3.11.7 LLDP neighbors max-num config

This page can be used to Remote Table the settings for save entries.

To display the "LLDP neighbors max-num config" page, click Port configuration -> LLDP configuration -> LLDP neighbors max-num config, click "Apply" to configure.

LLDP neighbors max-num config	
Port	Ethernet1/0/1 ▾
LLDP neighbors max-num value	
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 89.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>LLDP neighbors max-num value</b>	Remote table maximum save entry size 5-500.
<b>Operation</b>	Configuration: User self-configuration Default: Restore default configuration, default configuration is 100

### 3.11.8 LLDP too many neighbors config

This page can be used to set up operations after Remote Table is full.

To display the "LLDP too many neighbors config" page, click Port configuration -> LLDP configuration -> LLDP too many neighbors config, click "Apply" to configure.

LLDP neighbors max-num config	
Port	Ethernet1/0/1 ▾
LLDP neighbors max-num value	
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 90.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>LLDP too many neighbors value</b>	Discard: Discard new neighbor information Delete: Delete the neighbor information with the least aging time in the remote table, and then

	add new neighbor information
--	------------------------------

### 3.11.9 LLDP transmit optional tlv config

This page can configure port TLV properties.

To display the "LLDP transmit optional tlv config" page, click Port configuration -> LLDP configuration -> LLDP transmit optional tlv config, click "Apply" to configure.

LLDP transmit optional tlv config	
Port	Ethernet1/0/1 ▾
LLDP Port description	<input type="checkbox"/>
LLDP System capability	<input type="checkbox"/>
LLDP System description	<input type="checkbox"/>
LLDP System name	<input type="checkbox"/>
Apply	

Figure 91.

entry	describe
Port	Ethernet port name.
LLDP Port description	Port description name information needs to be configured.
LLDP System capability	Information describing system capabilities.
LLDP System description	Message describing the system.
LLDP System name	System name information.

### 3.11.10 show LLDP configuration

This page can be used to view LLDP configuration messages.

To display the "show LLDP configuration" page, click Port configuration -> LLDP configuration -> show LLDP configuration, click "Apply" to view.

show LLDP configuration	
LLDP too many neighbors value	show LLDP ▾
Port	all ▾
Apply	

### Information feedback window

```
Switch# show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been disabled globally.
LLDP enabled port : NULL
LLDP interval :30
LLDP txTTL :120
LLDP NotificationInterval :5
LLDP txDelay :2
LLDP-MED FastStart Repeat Count :4
-----END-----
```

show LLDP configuration	
LLDP too many neighbors value	show LLDP port ▾
Port	Ethernet1/0/14 ▾
<input type="button" value="Apply"/>	

### Information feedback window

```
Switch# show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been disabled globally.
LLDP enabled port : NULL
LLDP interval :30
LLDP txTTL :120
LLDP NotificationInterval :5
LLDP txDelay :2
LLDP-MED FastStart Repeat Count :4
-----END-----
```

show LLDP configuration	
LLDP too many neighbors value	show LLDP ▾
Port	all ▾
<input type="button" value="Apply"/>	

Information feedback window							
Switch# show lldp traffic							
PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized
Ethernet1/0/14	0	0	0	0	0	0	0

show LLDP configuration	
LLDP too many neighbors value	show LLDP <input type="button" value="v"/>
Port	all <input type="button" value="v"/>
<input type="button" value="Apply"/>	

```

Information feedback window
Switch# show lldp neighbors interface Ethernet1/0/14
Port name : Ethernet1/0/14
Port Remote Counter : 1
TimeMark :3596
ChassisIdSubtype :4
ChassisId :00-0e-c6-bf-ad-7a
PortIdSubtype :MAC address
PortId :00-0e-c6-bf-ad-7a
*****:

```

Figure 92.

### 3.12 LED shutoff configuration

This chapter can be used to set the timing of led lights out.

#### 3.12.1 Time Range configuration

This page can be used to set the time range for led lights to go out.

To display the "Time Range configuration" page, click Port configuration -> LED shutoff configuration -> Time Range configuration, click "Apply" to configure.

Time range configuration	
Time range name	<input type="text"/>
Time range type	absolute <input type="button" value="v"/> <input type="checkbox"/>
Start Time	
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
End Time	
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
Operation type	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 93.

<b>entry</b>	describe
<b>Time range name</b>	Time range name, length 1-64 characters.
<b>Time range type</b>	Absolute: Absolute time range, date required

	Absolute-periodic: Absolute cycle time range Periodic: Period Time Range
<b>Week</b>	Range: 1-7
<b>Time</b>	Time format: 14:00
<b>Date</b>	Date Scope: 2001.1.1-2038.12.31

### 3.12.2 LED shutoff config

This page can be used for LED timing extinguishing configuration.

To display the "LED shutoff config" page, click Port configuration -> LED shutoff configuration -> LED shutoff config, click "Apply" to configure.

Figure 94.

<b>entry</b>	describe
<b>Time range name</b>	With the configured time range name.
<b>LED state</b>	LED lamp status.
<b>Operation</b>	Configuration: User self-configuration Default: Function disabled

### 3.13 Jumbo packet forwarding configuration

This section can be used for the configuration of super packet forwarding.

This page can be used to set the time range for led lights to go out.

To display the "LED shutoff config" page, click Port configuration -> LED shutoff configuration -> LED shutoff config, click "Apply" to configure.

Jumbo packet forwarding configuration	
Jumbo packet size	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 95.

entry	describe
Jumbo packet size	Range: 1500-12270
Operation	Configuration: User self-configuration Default: Function disabled

## 4. MAC address table configuration

### 4.1 MAC address table configuration

#### 4.1.1 MAC address aging-time configuration

Each time the switch learns a MAC address, it will store the address and set the aging time. When the time is over, the address will be removed from the switch.

MAC address aging-time configuration	
MAC address aging-time	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 96.

MAC address aging-time	The aging time range is 10-1000000, 0 means no aging.	
Operation	Configuration	Set the aging time into the switch.
	Default	Restore the aging time of the switch to the default state.

MAC address aging-time
300

Figure 97. Display the current MAC address aging time.

#### 4.1.2 Configure MAC address

Configure static or Blackhole MAC addresses, and establish the mapping relationship between MAC addresses and ports and VLANs.

Configure static MAC address	
MAC address	<input type="text"/>
VLAN ID	1 ▾
Port list	Ethernet1/0/1 ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 98.

<b>MAC address</b>	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx.	
<b>VLAN ID</b>	Created VLAN ID.	
<b>Port list</b>	Mapped port.	
<b>Operation</b>	Add	The mapping relationship between MAC address and port and VLAN will be added.
	Remove	Delete the mapping relationship of the specified MAC address, VLAN, and port.

Configure blackhole MAC address	
MAC address	<input type="text"/>
VLAN ID	1 ▾
Blackhole based type	▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 99.

<b>MAC address</b>	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx, packets with this address will be discarded and will not be forwarded to the network by the switch.	
<b>VLAN ID</b>	Created VLAN ID.	
<b>Blackhole based type</b>	source	Source based on source address filter.
	destination	Target based on target address filter.
	both	Both are based on source address and destination address filters, the default value is both.
<b>Operation</b>	Add	The mapping relationship between MAC address and port and VLAN will be added.
	Remove	Delete the mapping relationship of the specified MAC address, VLAN, and port.



MAC address	VLAN ID	Port
00-11-22-cc-bb-dd	1	Ethernet1/0/1
00-11-55-cc-bb-df	1	Blackhole

Figure 100. Display current existing MAC address, port, VLAN mapping relationship.

### 4.1.3 Delete MAC address

Quickly delete the MAC address in the switch.

Delete MAC address		
Port status	Static ▼	
Delete by VLAN ID	1 ▼	<input type="checkbox"/> Select
Delete by MAC		<input type="checkbox"/> Select
Delete by port	Ethernet1/0/1 ▼	<input type="checkbox"/> Select
		<input type="button" value="Delete"/>

Figure 101.

<b>Port status</b>	Static	User-created and assigned MAC address.
	Dynamic	The MAC address automatically learned by the switch through the message.
	Blackhole	The user creates the assigned MAC address, but the packet of this address will not be forwarded by the switch.
<b>Delete by VLAN ID</b>	The created VLAN ID, delete the selected address type in the VLAN.	
<b>Delete by MAC</b>	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx.	
<b>Delete by port</b>	Delete all MAC addresses under the port.	

MAC address	VLAN ID	Status
00-1a-33-44-de-fd	1	Ethernet1/0/1
10-55-df-98-77-55	1	Blackhole

Figure 102. Display the current mapping relationship between MAC address, VLAN ID, and port.

### 4.1.4 MAC address query

Quickly query the MAC address in the switch.

MAC address query		
Port status	Static ▼	<input type="checkbox"/> Select
Query by MAC	<input type="text"/>	<input type="checkbox"/> Select
Query by VLAN ID	1 ▼	<input type="checkbox"/> Select
Query by port	Ethernet1/0/1 ▼	<input type="checkbox"/> Select
		<input type="button" value="Apply"/>

Figure 103.

<b>Port status</b>	Static	User-created and assigned MAC address.
	Dynamic	The MAC address automatically learned by the switch through the message.
	Blackhole	The user creates the assigned MAC address, but the packet of this address will not be forwarded by the switch.
<b>Query by VLAN ID</b>	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx.	
<b>Query by MAC</b>	The created VLAN ID, showing the address in the VLAN.	
<b>Query by port</b>	Find the MAC address by port.	

Note: Check the small box at the back to make the condition take effect. By default, there is no condition. When there is no condition, all MAC address information will be displayed.

反馈信息窗口				
Read mac address table....				
Vlan	Mac Address	Type	Creator	Ports
1	00-0e-c6-c7-93-15	STATIC	App	Ethernet1/0/8
1	10-f0-13-f1-72-3a	STATIC	System	CPU
2	00-11-33-55-88-66	STATIC	User	Ethernet1/0/4

Figure 104. Display the results of the query.

## 5. VLAN configuration

### 5.1 VLAN configuration

#### 5.1.1 Create/Remove VLAN

VLAN configuration function module, users add or delete VLANs in this module.

VLAN ID configuration	
VLAN ID	<input type="text"/>
VLAN Name	<input type="text"/>
VLAN Type	<input type="text" value="▼"/>
Operation	Add <input type="text" value="▼"/>
<input type="button" value="Apply"/>	

Figure 105.

<b>VLAN ID</b>	The serial number of the VLAN, range: 2-4094.	
<b>VLAN name</b>	By default, the default is VLAN plus four-digit serial number, range: 1-64 characters.	
<b>VLAN type</b>	Private vlan (isolated). Private vlan (community). Private vlan (primary). universal vlan; There are three dedicated VLANs in the Primary port: Primary VLAN, Isolated VLAN and Community VLAN can communicate with the ports of the Isolated VLAN and Community VLAN related to this Primary VLAN; the ports in the Isolated VLAN are isolated from each other and are only related to it. The ports in the Primary VLAN communicate with each other; the ports in the Community VLAN can communicate with each other or with the related Primary VLAN ports; there is no communication between the ports in the Community VLAN and the ports in the Isolated VLAN. There is no communication between the ports in the Community VLAN and the ports in the Isolated VLAN.	
<b>Operation</b>	Add	Add VLAN.
	Remove	Remove VLAN.

VLAN ID information		
VLAN ID	VLAN Name	VLAN Type
1	default	universal vlan

Figure 106.

### 5.1.2 Assign ports for VLAN

Assign ports to the VLAN, and users add and remove ports in the VLAN in this module.

Assign ports for VLAN	
VLAN ID	1 <input type="text" value="▼"/>
Port	Ethernet1/0/1 <input type="text" value="▼"/>
Operation	Add <input type="text" value="▼"/>
<input type="button" value="Apply"/>	

Figure 107.

<b>VLAN ID</b>	Created VLAN.	
<b>Port</b>	Port name.	
<b>Operation</b>	Add	Add port to VLAN.
	Remove	Remove the port from the VLAN port list.

### 5.1.3 Port type configuration

Switch port type setting, the user can change the switch port type in this module.

Figure 108.

<b>Port</b>	Port name.	
<b>Type</b>	access	
	trunk	
	hybrid	
<b>State</b>	Enable VLAN ingress check	When a data packet enters the switch, the VLAN ingress filter checks whether the ingress port of the data packet belongs to the given (forwarded) VLAN.
	Disable VLAN ingress check	When a data packet enters the switch, the VLAN ingress filter does not check whether the ingress port of the data packet belongs to the given (forwarded) VLAN.

Port mode configuration		
Port	Type	State
Ethernet1/0/1	access	Open
Ethernet1/0/2	access	Open
Ethernet1/0/3	access	Open
Ethernet1/0/4	access	Open
Ethernet1/0/5	access	Open
Ethernet1/0/6	access	Open
Ethernet1/0/7	access	Open
Ethernet1/0/8	access	Open

Figure 109.

### 5.1.4 Hybrid port configuration

Switch Hybrid port VLAN configuration, the user changes the attributes of the switch's Hybrid port type in this module.

Set hybrid native VLAN	
Port	Ethernet1/0/4 ▼
Hybrid native VLAN	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Figure 110.

<b>Port</b>	Port name.	
<b>Hybrid native VLAN</b>	PVID of the port, VLAN TAG tag when the port is sending and receiving data frames.	
<b>Operation</b>	Add	Add port to VLAN.
	Remove	Remove the port from the VLAN port list.

Set hybrid allow VLAN	
Port	Ethernet1/0/4 ▼
Hybrid allowed VLAN list	<input type="text"/>
Operation	Add all ▼
Tagged	Untag ▼
<input type="button" value="Apply"/>	

Figure 111.

<b>Port</b>	Port name.	
<b>Hybrid allowed VLAN list</b>	List of allowed VLANs, connected with "-" and ";".	
<b>Operation</b>	Add all	Add port to all VLANs, 1-4094.
	Add	Add a VLAN to the list of existing passed VLANs.
	Except add	Add the port to all VLANs outside the specified VLAN.
	Cover add	Clear the original passed VLAN list, and then add the specified VLAN list to the VLAN list.
	Remove	Remove the specified VLAN list from the existing passed VLAN list.
<b>Tagged</b>	Untag method to join.	
	Tag way to join.	

Port	Hybrid native VLAN	Hybrid Tagged allowed VLAN list	Hybrid UnTagged allowed VLAN list
Ethernet1/0/4	1		

Figure 112. Display detailed information of Hybrid port.

### 5.1.5 Trunk port configuration

Switch trunk port VLAN configuration, the user can change the attributes of the trunk port type of the switch in this module.

**Set trunk native VLAN**

Port	Ethernet1/0/6 ▼
Trunk native VLAN	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Figure 113.

<b>Port</b>	Port name.	
<b>Trunk native VLAN</b>	PVID of the port, VLAN TAG tag when the port is sending and receiving data frames.	
<b>Operation</b>	Add	Add port to VLAN.
	Remove	Remove the port from the VLAN port list.

Set trunk allow VLAN	
Port	Ethernet1/0/6 ▾
Trunk allowed VLAN list	<input type="text"/>
Operation	Add all ▾
<input type="button" value="Apply"/>	

Figure 114.

<b>Port</b>	Port name.	
<b>Trunk allowed VLAN list</b>	List of allowed VLANs, connected with "-" and ";"	
<b>Operation</b>	Add	Add port to all VLANs, 1-4094.
	Remove	Add a VLAN to the list of existing passed VLANs.
	Except add	Add the port to all VLANs outside the specified VLAN.
	Cover add	Clear the original passed VLAN list, and then add the specified VLAN list to the VLAN list.
	Remove	Remove the specified VLAN list from the existing passed VLAN list.

Port	Trunk native VLAN	Trunk allowed VLAN list
Ethernet1/0/6	1	1-4094

Figure 115. Display the detailed information of the trunk port.

### 5.1.6 Private-vlan configuration

Switch Private-vlan binding operation, the user binds the private-vlan relationship in this module.

Private-vlan association	
Designate Primary-vlan	▾
Association VLAN list	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 116.

<b>Designate Primary-vlan</b>	Created Primary-vlan.
-------------------------------	-----------------------

<b>Association VLAN list</b>	The secondary VLAN associated with the Primary-vlan, the secondary VLAN includes private vlan (isolated), private vlan (community).	
<b>Operation</b>	Configuration	Associate the secondary VLAN with the primary VLAN.
	Default	Clear the primary-vlan association.

Primary-vlan	Association VLAN list
2	4

Figure 117. Display the related information of Primary-vlan.

## 5.2 GVRP configuration

### 5.2.1 Enable global GVRP

The switch starts the global GVRP setting, and the user turns on or off the global GVRP.

Enable global GVRP	
Enable/Disable global GVRP	Disable ▾
Apply	

Figure 118.

<b>Enable/Disable global GVRP</b>	Enable	Start the global GVRP module function.
	Disable	Disable the global GVRP module function.

Enable global GVRP	
GVRP status	Disable

Figure 119.

### 5.2.2 Enable GVRP on port

The switch port starts GVRP settings, and the user opens or closes the port GVRP.

Enable GVRP on port	
Port	Ethernet1/0/4 ▾
Enable/Disable GVRP	Enable ▾
Apply	

Figure 120.

<b>Port</b>	Port name.	
<b>Enable/Disable</b>	Enable	Start the port GVRP module function.



<b>GVRP</b>	Disable	Disable the port GVRP module function.
-------------	---------	--

Port	GVRP Status
Ethernet1/0/4	Disable
Ethernet1/0/6	Disable

Figure 121. Display the GVRP status of each port.

### 5.2.3 GARP configuration

The switch configures GARP parameters, and the user sets the value of various timers to manage GARP.

GARP parameters configuration	
Join timer	<input type="text" value="200"/>
Leave timer	<input type="text" value="600"/>
Leaveall timer	<input type="text" value="10000"/>
Operation	<input type="text" value="Configuration"/>
<input type="button" value="Apply"/>	

Figure 122.

<b>Join timer</b>	200-500ms.	
<b>Leave timer</b>	500-1200ms.	
<b>Leaveall timer</b>	500-60000ms.	
<b>Operation</b>	configuration	Modify the value of the timer.
	default	Restore the timer value to the default configuration.

## 5.3 VLAN-translation configuration

### 5.3.1 Enable/Disable VLAN-translation

The switch port starts the VLAN-translation setting, and the user opens or closes the port VLAN-translation.

Enable/Disable VLAN-translation	
Port	<input type="text" value="Ethernet1/0/1"/>
Enable/Disable VLAN-translation	<input type="text" value="Enable"/>
<input type="button" value="Apply"/>	

Figure 123.

<b>Port</b>	Port name	
<b>Enable/Disable VLAN-translation</b>	Enable	Enable the VLAN-translation function of the port.
	Disable	Disable the VLAN-translation function of the port.

Port	VLAN-translation Status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable

Figure 124. Display the VLAN-translation status of each port.

### 5.3.2 Add/Delete VLAN-translation

Switch VLAN-translation conversion settings, the user sets the VLAN-translation conversion relationship.

Add/Delete VLAN-translation	
Port	Ethernet1/0/1 ▾
source vlan ID	Vlan1 ▾
destination vlan ID	Vlan1 ▾
dirction	in ▾
Operation	Add ▾
Apply	

Figure 125.

<b>Port</b>	Port name.	
<b>Source vlan ID</b>	Configured VLAN.	
<b>Destination vlan ID</b>	Configured VLAN.	
<b>dirction</b>	in	Configure the conversion direction of VLAN-translation as the ingress conversion function.
	out	Configure the conversion direction of VLAN-translation as the egress conversion function.
<b>Operation</b>	Add	Add VLAN-translation conversion relationship.
	Remove	Remove VLAN-translation conversion relationship.

### 5.3.3 VLAN-translation miss drop configuration

When the switch VLAN-translation fails to find the translation relationship, the packet loss settings are set. The user sets the direction of the packet loss configuration when the VLAN-translation finds the translation relationship.

VLAN-translation miss drop configuration	
Port	Ethernet1/0/1 ▾
dirction	both ▾
Operation	Configuration ▾
Apply	

Figure 126.

<b>Port</b>	Port name.	
<b>dirction</b>	both	The port performs VLAN-translation search and translation relationship configuration for packet loss at both the egress and the ingress.
	in	Packet loss configuration when the port performs VLAN-translation lookup translation relationship at the ingress.
	out	Packet loss configuration when the port performs VLAN-translation lookup translation relationship at the egress.
<b>Operation</b>	Configuration	Add VLAN-translation to find the packet loss configuration when searching for translation relations.
	Cancel	Delete the configuration of packet loss when searching for translation relationship in VLAN-translation.

### 5.3.4 show VLAN-translation

The display of switch VLAN-translation related configuration, the user can check the switch VLAN-translation configuration.

show VLAN_translation	
Apply	

Figure 127.

<b>Apply</b>	Confirm that you want to view VLAN-translation related configuration information.
--------------	---

```

Information feedback window
Switch# show vlan-translation
Interface Ethernet1/0/1:
    vlan-translation is enable, miss drop is not set

```

Figure 128. Display VLAN-translation related configuration information.

## 5.4 dynamic VLAN configuration

### 5.4.1 VLAN protocol configuration

Switch VLAN protocol table entry configuration, user configuration protocol VLAN parameters to generate VLAN.

protocol vlan mode configuration	
VLAN interface	Vlan1 ▾
protocol mode	ethernetII ▾
protocol mode ID	<input type="text"/>
SSAP ID	<input type="text"/>
priority ID	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 129.

<b>VLAN interface</b>	Created VLAN.	
<b>Protocol mode</b>	ethernetII	VLAN is divided according to data packets in ethernetII format.
	snap	VLAN is divided according to data packets in snap format.
	llc	VLAN is divided according to data packets in the LLC format.
	all	Used when cancel operation, restore all protocol VLAN to static VLAN.
<b>Protocol mode ID</b>	The ID range of ethernetII and snap is 1536-65535, and the ID range of llc is 0-255.	
<b>SSAP ID</b>	It is only set in the llc protocol, range: 0-255.	
<b>Priority ID</b>	Queue priority, range: 0-7.	
<b>Operation</b>	configuration	Modify VLAN parameters and configure to dynamic protocol VLAN.
	cancel	Restore VLAN from dynamic VLAN to static.

```

Information feedback window
Switch# config
Switch(config)# protocol-vlan mode ethernetII etype 1536 vlan 1 priority 0

```

Figure 130. Display configuration info.

## 5.5 Dot1q tunnel configuration

### 5.5.1 Enable dot1q tunnel

Switch dot1q tunnel configuration, the user configures the port to enable the dot1q tunnel function.

Enable dot1q tunnel	
Port	Ethernet1/0/1 ▾
Operation	Enable ▾
Apply	

Figure 131.

<b>Port</b>	Port name.	
<b>Operation</b>	Enable	Enable dot1q tunnel.
	Disable	Disable dot1q tunnel.

```

Information feedback window
Switch# config
Switch(config)# interface Ethernet1/0/1
Switch(config-if-ethernet1/0/1)# dot1q-tunnel enable

```

Figure 132. Display the execution process and results.

### 5.5.2 dot1q tunnel tpid configuration

Switch port dot1q tunnel tpid configuration, users configure port dot1q tunnel tpid parameters.

Dot1q tunnel tpid configuration	
Port	Ethernet1/0/1 ▾
protocol	0x8100 ▾
protocol ID	<input type="text"/>
Apply	

Figure 133.

<b>Port</b>	Port name.	
<b>Protocol</b>	0x8100	Set the outer TPID to 0x8100.
	0x9100	Set the outer TPID to 0x9100.

	0x9200	Set the outer TPID to 0x9200
	protocol ID	Set a custom TPID.
<b>Protocol ID</b>	The value of the custom TPID.	

```

Information feedback window
Switch# config
Switch(config)# interface Ethernet1/0/1
Switch(config-if-ethernet1/0/1)# dot1q-tunnel tpid 0x8100
QinQ enabled in Ethernet1/0/1, please disable it first!
ERROR: set dot1q-tunnel tpid on Ethernet1/0/1 error

```

Figure 134. Display the execution process and results.

## 6. IGMP Snooping configuration

### 6.1 Switch on-off IGMP Snooping

Switch IGMP Snooping global switch, snooping IGMP messages.

Figure 135.

<b>Switch on-off IGMP Snooping</b>	Open	Turn on the global switch of IGMP Snooping on the switch.
	Close	Turn off the global switch of IGMP Snooping on the switch.

Figure 136. Display the current global status of IGMP Snooping.

### 6.2 IGMP Snooping port enable

Configure IGMP Snooping port switch.

Figure 137.

<b>VLAN ID</b>	Created VLAN ID.
----------------	------------------

<b>Operation type</b>	Open	Open VLAN interface IGMP Snooping.
	Close	Close VLAN interface IGMP Snooping.

IGMP Snooping VLAN config	
VLAN ID	Operation type
1	OPEN

Figure 138. Display the current existing VLAN interface and the running status of IGMP Snooping under the VLAN interface.

### 6.3 IGMP Snooping configuration

Configure IGMP Snooping based on VLAN interface.

Igmp Snooping Configuration		
VLAN ID	vlan 1 ▾	<input type="checkbox"/>
Immediate leave configuration	immediate leave ▾	<input type="checkbox"/>
L2-general-querier configuration	L2-general-querier ▾	<input type="checkbox"/>
Group number	<input type="text"/>	<input type="checkbox"/>
Source table number	<input type="text"/>	<input type="checkbox"/>
Operation	Configuration ▾	<input type="checkbox"/>
		<input type="button" value="Apply"/>

Figure 139.

<b>VLAN ID</b>	Created VLAN ID.	
<b>Immediate leave configuration</b>	IGMP fast leave function in VLAN.	
<b>L2-general-querier configuration</b>	Used to send regular queries regularly to help switches in this network segment learn the mrouter port.	
<b>Group number</b>	The upper limit of the total number of groups. When the number of joined groups reaches the limit, the newly joined groups will be rejected to prevent hostile attacks. The default is 50, and the range: 1-65535.	
<b>Source table number</b>	The maximum number of source entries in each group, including include sources and exclude sources. The default is 40, and the range: 1-65535.	
<b>Operation type</b>	Configuration	Configure the checked parameters into the selected VLAN.
	Default	Restore the checked parameters to the default state.

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are

unified functions, so the two function parameters will take effect together (when one parameter is set, the other will be set to the default value).

VLAN ID	Immediate leave configuration	L2-general-querier configuration	Group number	Source table number
1	Disable	Disable	50	40

Figure 140. Display the configuration parameters of the existing VLAN.

## 6.4 IGMP Snooping mrouter configuration

IGMP Snooping mrouter port parameter configuration.

IGMP Snooping mrouter port configuration	
VLAN ID	vlan 1 ▾
Mrouter port	Ethernet1/0/1 ▾ <input type="checkbox"/>
MRouter port alive time	<input type="text"/> <input type="checkbox"/>
Operation type	Add ▾
<input type="button" value="Apply"/>	

Figure 141.

<b>VLAN ID</b>	Created VLAN ID.	
<b>Mrouter port</b>	Port name.	
<b>Mrouter port alive time</b>	Time to live of the port, range: 1-65535.	
<b>Operation type</b>	Add	Add the mrouter port parameter configuration checked under the selected VLAN.
	Remove	Delete the mrouter port parameter configuration checked under the selected VLAN.

VLAN ID	Mrouter port	MRouter port alive time
1		255

Figure 142. Display current configuration information.

## 6.5 IGMP Snooping query configuration

IGMP Snooping query parameter configuration.



IGMP Snooping query configuration		
VLAN ID	vlan 1 ▼	
Query-Interval	<input type="text"/>	<input type="radio"/>
Query-mrsp configuration	<input type="text"/>	<input type="radio"/>
Query-robustness configuration	<input type="text"/>	<input type="radio"/>
Suppression-query-time configuration	<input type="text"/>	<input type="radio"/>
Operation type	Add ▼	
		<input type="button" value="Apply"/>

Figure 143.

<b>VLAN ID</b>	Created VLAN ID.	
<b>Query-Interval</b>	IGMP Snooping query interval, range: 1-65535.	
<b>Query-mrsp configuration</b>	Maximum response time for group query.	
<b>Query-robustness configuration</b>	IGMP Snooping robustness, range: 2-10.	
<b>Suppression-query-time configuration</b>	Prohibited query time, range: 1-65535.	
<b>Operation type</b>	Add	Add the mrouter port parameter configuration checked under the selected VLAN.
	Remove	Delete the mrouter port parameter configuration checked under the selected VLAN.

VLAN ID	Query-Interval	Query-mrsp configuration	Query-robustness configuration	Suppression-query-time configuration
1	125	10	2	255

Figure 144. Display current configuration information.

## 7. MLD Snooping configuration

### 7.1 Switch on-off MLD Snooping

Configure MLD Snooping global status switch.

Switch on-off MLD Snooping	
Switch on-off MLD Snooping	Open ▼
<input type="button" value="Apply"/>	

Figure 145.

<b>Switch on-off MLD Snooping</b>	Open	Turn on the global switch of MLD Snooping on the switch.
	Close	Turn off the global switch of MLD Snooping on the switch.

## 7.2 MLD Snooping port enable

Configure MLD Snooping port switch.

Figure 146.

<b>VLAN ID</b>	Created VLAN ID.	
<b>Operation type</b>	Open	Open VLAN interface MLD Snooping.
	Close	Close VLAN interface MLD Snooping.

## 7.3 MLD Snooping configuration

MLD Snooping configuration based on VLAN interface.

Figure 147.

<b>VLAN ID</b>	Created VLAN ID.
<b>Immediate leave configuration</b>	MLD fast leave function in VLAN.
<b>L2-general-querier configuration</b>	Used to send regular queries regularly to help switches in this network segment learn the mrouter port.
<b>Group number</b>	The upper limit of the total number of groups. When the number of joined groups reaches the limit, the newly joined groups will be rejected to prevent hostile attacks. The default is 50, and the range: 1-65535.

<b>Source table number</b>	The maximum number of source entries in each group, including include sources and exclude sources. The default is 40, and the range: 1-65535.	
<b>Operation</b>	Configuration	Configure the checked parameters into the selected VLAN.
	Default	Restore the checked parameters to the default state.

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are unified functions, so the two function parameters will take effect together (when one parameter is set, the other will be set to the default value).

## 7.4 MLD Snooping mrouter port configuration

MLD Snooping MRouter port parameter configuration.

MLD Snooping mrouter port configuration		
VLAN ID	vlan 1 ▾	
Mrouter port	Ethernet1/0/1 ▾	<input type="checkbox"/>
MRouter port alive time		<input type="checkbox"/>
Operation type	Add ▾	
		Apply

Figure 148.

<b>VLAN ID</b>	Created VLAN ID.	
<b>Mrouter port</b>	Port name.	
<b>Mrouter port alive time</b>	Time to live of the port, range: 1-65535.	
<b>Operation type</b>	Add	Add the mrouter port parameter configuration checked under the selected VLAN.
	Remove	Delete the mrouter port parameter configuration checked under the selected VLAN.

## 7.5 MLD Snooping query configuration

MLD Snooping query parameter configuration.

MLD Snooping query configuration		
VLAN ID	vlan 1 ▾	
Query-Interval	<input type="text"/>	<input type="radio"/>
Query-mrsp configuration	<input type="text"/>	<input type="radio"/>
Query-robustness configuration	<input type="text"/>	<input type="radio"/>
Suppression-query-time configuration	<input type="text"/>	<input type="radio"/>
Operation type	Add ▾	
		<input type="button" value="Apply"/>

Figure 149.

<b>VLAN ID</b>	Created VLAN ID.	
<b>Query-Interval</b>	MLD Snooping query interval, range: 1-65535.	
<b>Query-mrsp configuration</b>	Maximum response time for group query.	
<b>Query-robustness configuration</b>	MLD Snooping robustness, range: 2-10.	
<b>Suppression-query-time configuration</b>	Prohibited query time, range: 1-65535.	
<b>Operation type</b>	Add	Add the mrouter port parameter configuration checked under the selected VLAN.
	Remove	Delete the mrouter port parameter configuration checked under the selected VLAN.

## 8. Time Range configuration

### 8.1 Time Range configuration

Time Range configuration module, the user can add or delete the operation of in this module, which can be applied to various ACL.

In the absolute mode you must input the start-time , end-time is not necessary.

You must input the weeks, start-time and end-time, but need not input the date including start and end time in the absolute-periodic. You must input the weeks, start-time and end-time, but need not input the date including start and end time, and may input multi-week values,separate them with ",", such as:1-7:monday-sunday;31:daily;96:weekdays;127:weekend.

Input date format: YYYY.MM.DD.Input week format: number (1:Monday etc.),if input multi-week values,separate them with ",",such as:1,2 identify monday&tuesday..Input time format: HH:MM:SS.

Time range configuration	
Time range name	<input type="text"/>
Time range type	absolute <input type="checkbox"/>
Start Time	
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
End Time	
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
Operation type	Add <input type="checkbox"/>
<input type="button" value="Apply"/>	

Figure 150.

<b>Time range name</b>	Time period names must begin with alphabetic or numeric characters, 1-64 characters.	
<b>Time range type</b>	absolute	Absolutely
	absolute-periodic	Absolute-periodic
	periodic	periodic
<b>Week</b>	Start or end weeks, "1-7":"monday-sunday"; "31":"daily"; "96":"weekdays"; "127":"weekend".	
<b>Time</b>	Start or end time, HH:MM:SS.	
<b>Date</b>	Start or end date, YYYY.MM.DD, range2001.1.1-2038.12.31.	
<b>Operation type</b>	Add	Add operations.
	Remove	Delete operations.

## 9. ACL configuration

### 9.1 Numeric ACL

#### 9.1.1 Standard numeric ACL

##### 9.1.1.1 IP standard ACL

The digital standard IP access list configuration module, where users can create or modify parameters for the digital standard IP access list.

IP standard ACL(Number)	
List name	
Rule	permit ▼
Source address type	Any IP ▼
Source IP	
Reverse network mask	
tpid	
VLANID	
VLANID mask	
dscp	
Apply	

Figure 151.

<b>List name</b>	Digital Standard IP Access List Number 1-99.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.
<b>Source address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Source IP</b>	Source IP address, decimal point.	
<b>Reverse network mask</b>	Source IP address mask, decimal point.	
<b>tpid</b>	Label Protocol Identification, 0-65535.	
<b>VLANID</b>	VLAN ID, 1-4094.	
<b>VLANID mask</b>	VLAN mask , 0-4095	
<b>dscp</b>	IP message priority, 0-63.	

### 9.1.1.2 MAC standard ACL

The digital standard MAC access list configuration module, where users can create or modify parameters for the digital standard MAC access list.

MAC standard ACL(Number)	
List name	
Rule	permit ▼
Source address type	Any MAC ▼
Source MAC	
Reverse network mask	
Apply	

Figure 152.

<b>List name</b>	Digital Standard MAC Access List Number, 700-799.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.
<b>Source address type</b>	Any MAC	Match any MAC address.
	Specified MAC	Match MAC specified address.
	Host MAC	Match the specified host MAC.
<b>Source IP</b>	Source MAC address.	
<b>Reverse network mask</b>	Source MAC address inverse mask.	

### 9.1.2 Extended numeric ACL

#### 9.1.2.1 IP extended ACL

The digital extension IP access list configuration module, where users can create or modify parameters for the digital extension IP access list.

IP extended ACL(Number)	
Operation type	ICMP
List name	
Rule	permit
Fragment packet	<input type="checkbox"/>
Source address type	Any IP
Source IP	
Reverse network mask	
Destination address type	Any IP
Destination IP	
Reverse network mask	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
Apply	

Figure 153.

<b>Operation type</b>	Extended operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol.	
<b>List name</b>	Digital extensions IP access list numbers, 100-199.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.

<b>Fragment packet</b>	Optional whether long messages are transmitted in pieces.	
<b>Source address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Source IP</b>	Source IP address, decimal point.	
<b>Reverse network mask</b>	Source IP address mask, decimal point.	
<b>Destination address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Destination IP</b>	Destination IP, decimal points.	
<b>Reverse network mask</b>	Destination IP address mask, decimal point.	
<b>IP precedence</b>	IP priority, 0-7.	
<b>TOS</b>	Service type, 0-15.	
<b>Time range name</b>	Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters.	
<b>ICMP type</b>	ICMP message type, 0-255.	
<b>ICMP code</b>	ICMP message code, 0-255.	

### 9.1.2.2 MAC-IP extended ACL

Digital extension MAC-IP access list configuration module, where users can create or modify parameters for the digital extension MAC-IP access list.



MAC-IP extended ACL(Number)	
Operation type	ICMP
List name	
Rule	permit
Source address type	Any MAC
Source MAC	
Reverse network mask	
Destination address type	Any MAC
Destination MAC	
Reverse network mask	
Source address type	Any IP
Source IP	
Reverse network mask	
Destination address type	Any IP
Destination IP	
Reverse network mask	
tpid	
VLANID	
VLANID mask	
dscp	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
Apply	

Figure 154.

<b>Operation type</b>	Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol.	
<b>List name</b>	Digital Extension MAC-IP Access List Number, 3100-3199.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.
<b>Source address type</b>	Any MAC	Match any MAC address.
	Specified MAC	Match MAC specified address.
	Host MAC	Match the specified host MAC.
<b>Source MAC</b>	Source MAC address.	
<b>Reverse network mask</b>	Source MAC address inverse mask.	
<b>Destination address</b>	Any MAC	Match any MAC address.

<b>type</b>	Specified MAC	Match MAC specified address.
	Host MAC	Match the specified host MAC.
<b>Destination MAC</b>	Destination MAC.	
<b>Reverse network mask</b>	Destination MAC address inverse mask.	
<b>Source address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Source IP</b>	Source IP address, decimal point.	
<b>Reverse network mask</b>	Source IP address mask, decimal point.	
<b>Destination address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Destination IP</b>	Destination IP address, decimal point.	
<b>Reverse network mask</b>	Destination IP address mask, decimal point.	
<b>tpid</b>	Label Protocol Identification, 0-65535.	
<b>VLANID</b>	VLAN ID, 1-4094.	
<b>VLANID mask</b>	VLAN mask, 0-4095.	
<b>dcsp</b>	IP message priority, 0-63.	
<b>IP precedence</b>	IP priority, 0-7.	
<b>TOS</b>	Service type, 0-15.	
<b>Time range name</b>	Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters.	
<b>ICMP type</b>	ICMP message type, 0-255.	
<b>ICMP code</b>	ICMP message code, 0-255.	

### 9.1.3 Delete Numeric ACL

Delete the digital access list module, where the user can delete the specified digital access list.

Delete Numeric ACL		
List name	<input type="text"/>	<input type="text"/>
		Apply

Figure 155.

<b>List name</b>	Specify numeric access list numbers, 1-3199.
------------------	--

## 9.2 Name ACL

### 9.2.1 Standard name ACL

#### 9.2.1.1 IP standard ACL

Naming standard IP access list configuration module, where users can create or modify parameters for naming standard IP access list.

IP standard ACL	
List name	
Rule	permit ▼
Source address type	Any IP ▼
Source IP	
Reverse network mask	
tpid	
VLANID	
VLANID mask	
dscp	
Apply	

Figure 156.

<b>List name</b>	Nomenclature criteria IP access list names, strings must start with letters, 1-64 characters.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.
<b>Source address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Source IP</b>	Source IP address, decimal point.	
<b>Reverse network mask</b>	Source IP address mask, decimal point.	
<b>tpid</b>	Label Protocol Identification, 0-65535.	
<b>VLANID</b>	VLAN ID, 1-4094.	
<b>VLANID mask</b>	VLAN mask, 0-4095	
<b>dscp</b>	IP message priority, 0-63.	

## 9.2.2 Extended name ACL

### 9.2.2.1 IP extended ACL

Name extension IP access list configuration module, where users can create or modify parameters for named extension IP access list.

IP extended ACL	
Operation type	ICMP
List name	
Rule	permit
Source address type	Any IP
Source IP	
Reverse network mask	
Destination address type	Any IP
Destination IP	
Reverse network mask	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
Apply	

Figure 157.

<b>Operation type</b>	Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol.	
<b>List name</b>	Name extensions IP access list names, strings must start with letters, 1-64 characters.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.
<b>Fragment packet</b>	Optional whether long messages are transmitted in pieces.	
<b>Source address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Source IP</b>	Source IP address, decimal point.	
<b>Reverse network mask</b>	Source IP address mask, decimal point.	
<b>Destination address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.

	Host IP	Match the specified host IP.
<b>Destination IP</b>	Destination IP, decimal points.	
<b>Reverse network mask</b>	Destination IP address mask, decimal point.	
<b>IP precedence</b>	IP priority, 0-7.	
<b>TOS</b>	Service type, 0-15.	
<b>Time range name</b>	Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters.	
<b>ICMP type</b>	ICMP message type, 0-255.	

### 9.2.2.2 MAC extended ACL

Name extension MAC access list configuration module, where users can create or modify parameters for named extension MAC access list.

MAC extended ACL	
List name	<input type="text"/>
Rule	permit <input type="button" value="v"/>
Source address type	Any MAC <input type="button" value="v"/>
Source MAC	<input type="text"/>
Reverse network mask	<input type="text"/>
Destination address type	Any MAC <input type="button" value="v"/>
Destination MAC	<input type="text"/>
Reverse network mask	<input type="text"/>
Packet type	none <input type="button" value="v"/>
cos	<input type="text"/>
cos mask	<input type="text"/>
VLANID	<input type="text"/>
VLANID mask	<input type="text"/>
etherType	<input type="text"/>
etherType mask	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 158.

<b>List name</b>	Digital Extension MAC-IP Access List Number, 3100-3199.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.
<b>Source address type</b>	Any MAC	Match any MAC address.
	Specified MAC	Match MAC specified address.
	Host MAC	Match the specified host MAC.
<b>Source MAC</b>	Source MAC address.	

<b>Reverse network mask</b>	Source MAC address inverse mask.	
<b>Destination address type</b>	Any MAC	Match any MAC address.
	Specified MAC	Match MAC specified address.
	Host MAC	Match the specified host MAC.
<b>Destination MAC</b>	Destination MAC address.	
<b>Reverse network mask</b>	Destination MAC address inverse mask.	
<b>Packet type</b>	none	none
	tagged-802-3	Format of marked Ethernet 802-3 packets.
	tagged-eth2	Format of marked Ethernet II packets.
	untagged-802-3	Format of unmarked Ethernet 802-3 packets.
	untagged-eth2	Format of unmarked Ethernet II packets.
<b>cos</b>	cos, 0-7.	
<b>cos mask</b>	cos mask, 0-7.	
<b>VLANID</b>	VLAN ID, 1-4094.	
<b>VLANID mask</b>	VLAN mask, 0-4095.	
<b>etherType</b>	Ethernet type field value, 1536-65535.	
<b>etherType mask</b>	Ethernet type field value mask, 0-65535.	

### 9.2.2.3 MAC-IP extended ACL

Name extension MAC-IP access list configuration module, where users can create or modify parameters for named extension MAC-IP access list.

MAC-IP extended ACL	
Operation type	ICMP
List name	
Rule	permit
Source address type	Any MAC
Source MAC	
Reverse network mask	
Destination address type	Any MAC
Destination MAC	
Reverse network mask	
Source address type	Any IP
Source IP	
Reverse network mask	
Destination address type	Any IP
Destination IP	
Reverse network mask	
tpid	
VLANID	
VLANID mask	
dscp	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
Apply	

Figure 159.

<b>Operation type</b>	Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol.	
<b>List name</b>	Digital Extension MAC-IP Access List Number, 3100-3199.	
<b>Rule</b>	permit	Rule permit.
	deny	Rule deny.
<b>Source address type</b>	Any MAC	Match any MAC address.
	Specified MAC	Match MAC specified address.
	Host MAC	Match the specified host MAC.
<b>Source MAC</b>	Source MAC address.	
<b>Reverse network mask</b>	Source MAC address inverse mask.	
<b>Destination address</b>	Any MAC	Match any MAC address.

<b>type</b>	Specified MAC	Match MAC specified address.
	Host MAC	Match the specified host MAC.
<b>Destination MAC</b>	Destination MAC address.	
<b>Reverse network mask</b>	Destination MAC address inverse mask.	
<b>Source address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Source IP</b>	Source IP address, decimal point.	
<b>Reverse network mask</b>	Source IP address mask, decimal point.	
<b>Destination address type</b>	Any IP	Match any IP address.
	Specified IP	Match IP specified address.
	Host IP	Match the specified host IP.
<b>Destination IP</b>	Destination IP, decimal points.	
<b>Reverse network mask</b>	Destination IP address mask, decimal point.	
<b>tpid</b>	Label Protocol Identification, 0-65535.	
<b>VLANID</b>	VLAN ID, 1-4094.	
<b>VLANID mask</b>	VLAN mask, 0-4095.	
<b>dcsp</b>	IP message priority, 0-63.	
<b>IP precedence</b>	IP priority, 0-7.	
<b>TOS</b>	Service type, 0-15.	
<b>Time range name</b>	Time period names to be applied must begin with alphabetic or numeric characters, 1-64 characters.	
<b>ICMP type</b>	ICMP message type, 0-255.	
<b>ICMP code</b>	ICMP message code, 0-255.	

### 9.2.3 Delete name ACL

Delete the named access list module, where users can delete the specified named access list.

Delete Name ACL		
List name	<input type="text"/>	<input type="text"/>
		Apply



Figure 160.

<b>List name</b>	String must start with a letter, 1-64 characters.
------------------	---

## 9.3 Filter configuration

### 9.3.1 Firewall configuration

Firewall ACL configuration module in which users can operate switch firewall configuration.

Figure 161.

<b>Packet filtering</b>	open	open
	close	close
<b>Firewall default action</b>	permit	Rule permit.
	deny	Rule deny.

## 9.4 Show ACL configuration

### 9.4.1 Show access list

The access control list module is displayed in which the user can display ACL specified information or all ACL information.

Figure 162.

<b>Access list</b>	Specify the ACL name or number to display ALL display all ACL.
--------------------	--

### 9.4.2 Show firewall

Display packet filtering function configuration information module, user in this module can display firewall status information.

Figure 163.

### 9.4.3 Show time range

Display time range function configuration information module, where users can display configured custom time information.

Figure 164.

<b>Time-range name</b>	Specifies the time period name to display, ALL displays all time period information.
------------------------	--

## 9.5 ACL binding configuration

### 9.5.1 Attach ACL to port

ACL port binding module, the user can bind and delete the access list of the specified port.

Figure 165.

<b>Port</b>	Designated port number.	
<b>ACL type</b>	IP	IP type.
	MAC	MAC type.
	MAC-IP	MAC-IP type.
<b>List name</b>	Specify access list name, 1-64 characters.	
<b>ACL Attached Direction</b>	in	Application ACL only.
	in and traffic-statistics	Application ACL and flow monitoring.
<b>Operation type</b>	Add	Add operations.
	Remove	Delete operations.

### 9.5.2 Show access group

The configuration information module on ACL display port, where the user can display the ACL binding information of the specified port or all ports.

Show access group	
Port	ALL
ACL Attached Direction	in
Apply	

Figure 166.

<b>Port</b>	Specifies the port number to display the information ALL displays all port information.	
<b>ACL Attached Direction</b>	in	Application ACL only.
	in and traffic-statistics	Application ACL and flow monitoring.

### 9.5.3 Clear Pacl Statistic

The statistical information module ACL the port, where the user can clear the ACL statistics of the specified port.

Clear Pacl Statistic	
Port or Interface name	Ethernet1/0/1
ACL Attached Direction	in
Apply	

Figure 167.

<b>Port or Interface name</b>	Specifies the port number to clear statistics.	
<b>ACL Attached Direction</b>	in	Application ACL only.
	in and traffic-statistics	Application ACL and flow monitoring.

### 9.5.4 Attach ACL to vlan

ACL vlan binding module, where users can bind and delete access lists to specified VLAN.

Attach ACL to vlan	
VLAN interface	Vlan1
ACL type	IP
List name	
ACL Attached Direction	in
Operation type	Add
Apply	

Figure 168.

<b>VLAN interface</b>	Specifies the VLAN number to operate on.
<b>ACL type</b>	Specifies the type of ACL to bind: IP.MAC.MAC-IP.
<b>List name</b>	Specify access list name, 1-64 characters.

<b>ACL Attached Direction</b>	in	Application ACL only.
	in and traffic-statistics	Application ACL and flow monitoring.
<b>Operation type</b>	Add	Add operations.
	Remove	Delete operations.

### 9.5.5 show vacl configuration

The vlan acl configuration information module is displayed in which the user can display ACL binding information for the specified VLAN or all VLAN.

show vacl configuration	
VLAN interface	Vlan1 ▾
ACL Attached Direction	in ▾
Apply	

Figure 169.

### 9.5.6 clear vlan acl statistic

Clear the VLAN acl statistical information module, where the user can clear the ACL statistics of the specified VLAN.

clear vlan acl statistic	
VLAN interface	Vlan1 ▾
ACL Attached Direction	in ▾
Apply	

Figure 170.

<b>VLAN interface</b>	Specifies the VLAN number to clear statistics.	
<b>ACL Attached Direction</b>	in	Application ACL only.
	in and traffic-statistics	Application ACL and flow monitoring.

## 10. IPv6 ACL configuration

### 10.1 IPv6 standard access-list configuration

IPv6 standard access list configuration module, users can create, delete or modify parameters for digital standard IPv6 access lists.

IPv6 standard access-list configuration	
Access list number	
Rule	permit ▾
Source address type	host-source ▾
IPv6 address	
Operation	Add ▾
Apply	

Figure 171.

<b>Access list number</b>	Digital Standard IPv6 Access List Number, 500-599.	
<b>Rule</b>	Permit	Rule permit.
	Deny	Rule deny.
<b>Source address type</b>	Specifies IPv6 source host	Matches IPv6 specified source host.
	All IPv6 source hosts	Match any IPv6 source host.
	IPv6 source address	Match IPv6 specified source address.
<b>IPv6 address</b>	IPv6 address to operate.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 10.2 IPv6 name access-list configuration

IPv6 named access table configuration module, the user can create, delete, or modify parameters on the named standard IPv6 access list.

Figure 172.

<b>IPv6 name access-list</b>	Name of access list.	
<b>Rule</b>	Permit	Rule permit.
	Deny	Rule deny.
<b>Source address type</b>	Specifies IPv6 source host	Matches IPv6 specified source host.
	All IPv6 source hosts	Match any IPv6 source host.
	IPv6 source address	Match IPv6 specified source address.
<b>IPv6 address</b>	IPv6 address to operate.	
<b>Operation</b>	Add	Add operations.

	Remove	Delete operations.
--	--------	--------------------

### 10.3 Show IPv6 access list

Show IPv6 access control list module where users can display IPv6 access list to create, delete, or modify parameters.

Figure 173.

<b>List name</b>	Specifies the ACL name or number to display, 0-64 characters.
------------------	---

### 10.4 Attach IPv6 ACL to port

IPv6 ACL port binding module, the user can bind and delete the IPv6 access list on the specified port.

Figure 174.

<b>Port</b>	Designated port number.	
<b>List name</b>	Specify access list name, 1-64 characters.	
<b>ACL Attached Direction</b>	in	Application ACL only.
	in and traffic-statistics	Application ACL and flow monitoring.
<b>Operation type</b>	Add	Add operations.
	Remove	Delete operations.

### 10.5 Attach IPv6 ACL to vlan

IPv6 ACL VLAN binding module, the user can bind and delete the IPv6 access list to the specified VLAN.

Figure 175.

<b>VLAN interface</b>	VLAN number specified.	
<b>List name</b>	Specify access list name, 1-64 characters.	
<b>ACL Attached Direction</b>	in	Application ACL only.
	in and traffic-statistics	Application ACL and flow monitoring.
<b>Operation type</b>	Add	Add operations.
	Remove	Delete operations.

## 11. AM configuration

### 11.1 AM global configuration

#### 11.1.1 Enable/Disable AM

AM switch configuration module, the user can start or close the global AM function in this module.

The figure shows two screenshots from a network configuration interface. The top screenshot is titled 'Enable/Disable AM' and contains a form with 'AM status' set to 'Enable' in a dropdown menu and an 'Apply' button. The bottom screenshot is titled 'Information feedback window' and shows the 'AM status' as 'Enable'.

Figure 176.

### 11.2 AM port configuration

#### 11.2.1 Enable/Disable AM port

AM port switch configuration module, where the user can start or close the AM function of the specified port.

The figure shows two screenshots from a network configuration interface. The top screenshot is titled 'Enable/Disable AM port' and contains a form with 'Port' set to 'Ethernet1/0/1' in a dropdown menu and 'AM port status' set to 'Enable' in another dropdown menu, with an 'Apply' button. The bottom screenshot is titled 'Information feedback window' and displays a table with the following data:

Port	AM port status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable

Figure 177.

<b>Port</b>	Specifies the port number.
-------------	----------------------------

<b>AM port status</b>	Enable or disable.
-----------------------	--------------------

### 11.2.2 AM IP-Pool configuration

AM IP-Pool configuration module, the user can set up an AM IP segment on the specified port, allowing / rejecting messages within the segment to be forwarded through the port.

AM IP-Pool configuration	
Port	Ethernet1/0/1 <input type="button" value="v"/>
IP address	<input type="text"/>
Count	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 178.

<b>Port</b>	Designated port number.	
<b>IP address</b>	Beginning IP address, decimal point.	
<b>Count</b>	Number of consecutive addresses after starting IP address, 1-32.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

### 11.2.3 AM MAC-IP-Pool configuration

AM MAC-IP-Pool configuration module, the user can set up an AM MAC-IP segment on the specified port, allowing / rejecting messages from within the segment to be forwarded through the port.

AM MAC-IP-Pool configuration	
Port	Ethernet1/0/1 <input type="button" value="v"/>
IP address	<input type="text"/>
MAC address	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 179.

<b>Port</b>	Designated port number.	
<b>IP address</b>	Beginning IP address, decimal point.	
<b>MAC address</b>	Source MAC address.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.



## 11.3 Show AM port configuration

### 11.3.1 Show AM port configuration

The AM port configuration module is displayed in which the user can display the AM function configuration information of the specified port.

Figure 180.

<b>Port</b>	Designated port number.
-------------	-------------------------

### 11.3.2 Clear port AM Pool

AM Pool address pool cleanup module, where users can configure the specified AM Pool to clear.

Figure 181.

<b>Operation</b>	all	Clear all AM Pool.
	ip-pool	Clear ip-pool only.
	mac-ip-pool	Clear mac-ip-pool only.

## 12. Port channel configuration

Configure port related features settings using the Port Channel configuration page.

### 12.1 LACP port group configuration

This section can be used to create convergent groups.

To display the “LACP port group configuration” page, click Port channel configuration -> LACP port group configuration, click “Apply” to configure.

Figure 182.

<b>entry</b>	describe
<b>Group number</b>	Range: 1-128.
<b>Load balance mode</b>	<p><b>src-mac:</b> Execute load balancing according to source MAC.</p> <p><b>dst-mac:</b> Execute load balancing according to target MAC.</p> <p><b>dst-src-mac:</b> Execute load balancing based on source and target MAC.</p> <p><b>src-ip:</b> Execute load balancing according to source IP.</p> <p><b>dst-ip:</b> Execute load balancing according to target IP.</p> <p><b>dst-src-ip:</b> Execute load balancing according to target IP source.</p> <p><b>dst-src-mac-ip:</b> Perform load balancing based on target and source Mac and source IP.</p>

Port group table			
Group number	Group member size	Load balance	Operation
1	0	src-mac	<a href="#">Add member</a> <a href="#">Remove member</a> <a href="#">Show interface</a>

Figure 183.

<b>entry</b>	describe
<b>Group number</b>	Convergence group created, size range: 1-128.
<b>Group member size</b>	Number of members in convergent groups.
<b>Load balance mode</b>	<p><b>src-mac:</b> Execute load balancing according to source MAC.</p> <p><b>dst-mac:</b> Execute load balancing according to target MAC.</p> <p><b>dst-src-mac:</b> Execute load balancing based on source and target MAC.</p> <p><b>src-ip:</b> Execute load balancing according to source IP.</p> <p><b>dst-ip:</b> Execute load balancing according to target IP.</p> <p><b>dst-src-ip:</b> Execute load balancing according to target IP source.</p> <p><b>dst-src-mac-ip:</b> Perform load balancing based on target and source Mac and source IP.</p>
<b>Operation</b>	Click on the entry in the corresponding action bar and jump to the corresponding settings page.

## 12.2 Delete port group

This page can be used to delete created convergent groups.

To display the “Delete port group” page, click Port channel configuration -> Delete port group, click “Apply” to configure.

Port group table			
Group number	Group member size	Load balance	Operation
1	0	src-mac	Delete

Figure 184.

<b>entry</b>	describe
<b>Group number</b>	Range: 1-128.
<b>Group member size</b>	Number of members in convergent groups.
<b>Load balance</b>	<p><b>src-mac:</b> Execute load balancing according to source MAC.</p> <p><b>dst-mac:</b> Execute load balancing according to target MAC.</p> <p><b>dst-src-mac:</b> Execute load balancing based on source and target MAC.</p> <p><b>src-ip:</b> Execute load balancing according to source IP</p> <p><b>dst-ip:</b> Execute load balancing according to target IP.</p> <p><b>dst-src-ip:</b> Execute load balancing according to target IP source.</p> <p><b>dst-src-mac-ip:</b> Perform load balancing based on target and source Mac and source IP.</p>

### 12.3 Show port group info

This page can view the information of the convergent group configuration.

To display the “Show port group info” page, click Port channel configuration -> Show port group info, click “Apply” to view.

```

Information feedback window
Switch# config
Switch(config)# show port-group brief
ID: port group number; Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
       the first is selected ports number, the second is standby ports number, and
       the third is unselected ports number.
ID   Mode   Partner ID   Ports   Load-balance
-----
1                               src-mac
Switch(config)# show port-group detail
Flags: A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
Port-group number: 1, Mode: , Load-balance: src-mac
Port-group detail information:
System ID: 0x8000,00-1f-ce-10-b0-1b
Local:
  Port           Status      Priority Oper-Key Flag
-----
Remote:
  Actor          Partner    Priority Oper-Key SystemID      Flag
-----

```

Figure 185.

## 12.4 Show interface port-channel

This page can view the information of the convergent group port.

To display the “Show interface port-channel” page, click Port channel configuration -> Show interface port-channel, click “Apply” to view.

```

Information feedback window
Switch# show interface port-channel 1
Interface brief:
  Port-Channell is down, line protocol is down
  Port-Channell is layer 2 port, alias name is (null), index is 53
  Port-Channell is LAG port, member is :
    Hardware is EtherChannel, address is 00-1f-ce-10-b0-1b
  PVID is 1
  MTU 1500 bytes, BW 10000 Kbit
  Time since last status change:0w-0d-3h-21m-9s (12069 seconds)
  Encapsulation ARPA, Loopback not set
  Force half-duplex, Auto-speed
  FlowControl is off, MDI type is auto
Statistics:
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  The last 5 second input rate 0 bits/sec, 0 packets/sec
  The last 5 second output rate 0 bits/sec, 0 packets/sec
Input packets statistics:
  0 input packets, 0 bytes, 0 no buffer
  0 unicast packets, 0 multicast packets, 0 broadcast packets
  0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
  0 abort, 0 length error, 0 undersize 0 jabber, 0 fragments, 0 pause frame
Output packets statistics:
  0 output packets, 0 bytes, 0 underruns
  0 unicast packets, 0 multicast packets, 0 broadcast packets
  0 output errors, 0 collisions, 0 late collisions, 0 pause frame

```

Figure 186.

## 12.5 Add member port

This page can be used to add port members to a convergence group.

To display the “Add member port” page, click Port channel configuration -> Add member port, click “Apply” to configure.

Port group add port	
Group number	1 ▾
Port list	Ethernet1/0/1 ▾
mode	on ▾
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Figure 187.

<b>entry</b>	describe
<b>Group number</b>	To create a convergent group number.
<b>Port list</b>	Ethernet port name.
<b>mode</b>	<p>On: force port to join port channel without LACP enabled.</p> <p>Active: Enable the LACP on the port and set it to Active mode.</p> <p>Passive: Enable LACP on the port and set it to passive mode.</p>

Port group port list	
Index	Port Name
1	Ethernet1/0/1

Figure 188.

<b>entry</b>	describe
<b>Index</b>	To create a convergent group numb.
<b>Port Name</b>	Ethernet port name added to convergence group.

## 12.6 Del member port

This page can be used to delete port members within the convergence group.

To display the “Del member port” page, click Port channel configuration -> Del member port, click “Apply” to configure.

Port group remove port	
Group number	1 ▾
Port list	Ethernet1/0/1 ▾
<input type="button" value="Remove"/> <input type="button" value="Reset"/>	

Figure 189.

<b>entry</b>	describe
<b>Group number</b>	To create a convergent group number.
<b>Port list</b>	Ethernet port name.

## 12.7 Set lacp port priority

This page is available with setting port priority.

To display the “Set lacp port priority” page, click Port channel configuration -> Set lacp port priority, click set to set, click Reset to restore default settings.

Set lacp port priority	
Group number	1 ▾
Port list	Ethernet1/0/1 ▾
Lacp port priority	
<input type="button" value="set"/> <input type="button" value="Reset"/>	

Figure 190.

<b>entry</b>	describe
<b>Group number</b>	To create a convergent group number.
<b>Port list</b>	Ethernet port name added to convergence group.
<b>Lacp port priority</b>	Range: 0-65535.

## 12.8 Set lacp system priority

This page is available with setting system priorities.

To display the “Set lacp system priority” page, click Port channel configuration -> Set lacp system priority, click set to set, click Reset to restore default settings.

Set lacp system priority	
Lacp system priority	<input type="text"/>
<input type="button" value="set"/>	<input type="button" value="Reset"/>

Figure 191.

entry	describe
Lacp system priority	Range: 0-65535.

## 13. DHCP configuration

### 13.1 DHCP management

#### 13.1.1 Enable DHCP

DHCP status configuration and query, the user configures the DHCP server status and address conflict log status in this module, and checks the DHCP server status and address conflict log status.

Enable DHCP	
DHCP server status	Close ▾
Conflict logging status	Open ▾
<input type="button" value="Apply"/>	

Figure 192.

<b>DHCP server status</b>	Close	Close DHCP server.
	Open	Open DHCP server.
<b>Conflict logging status</b>	Close	Close address conflict logging.
	Open	Open address conflict logging.
<b>Apply</b>	Apply the currently selected configuration to the switch to make the configuration effective.	

Information feedback window	
DHCP server status	Conflict logging status
Close	Open

Figure 193.

<b>DHCP server status</b>	Close	The current DHCP server is off.
	Open	The current DHCP server is on.

<b>Conflict logging status</b>	Close	The current address conflict log is off.
	Open	The current address conflict log is open.

## 13.2 DHCP server configuration

### 13.2.1 Dynamic pool configuration

#### 13.2.1.1 Dynamic address pool configuration

Switch DHCP address pool configuration, the user configures the DHCP address pool parameters.

DHCP IP address pool configuration		
DHCP pool name	▼	
DHCP pool domain name		<input type="checkbox"/>
Address range	IP address:	<input type="text"/>
	Network mask:	<input type="text"/>
DHCP client node type	b-node ▼	<input type="checkbox"/>
Address lease timeout	<input type="radio"/> Infinite <input checked="" type="radio"/> Specified	
	Day:	<input type="text"/>
	Hour:	<input type="text"/>
	Minute:	<input type="text"/>
Operation	Add ▼	
		<input type="button" value="Apply"/>

Figure 194.

<b>DHCP pool name</b>	The name of the created address pool.	
<b>DHCP pool domain name</b>	The domain name of the currently selected address pool. After configuration, you need to tick the box at the back to apply the domain name to the switch during application.	
<b>Address range</b>	IP address	Network number of the address pool.
	Network mask	Netmask of the address pool.
<b>DHCP client node type</b>	b-node	Broadcast node.
	p-node	For point-to-point nodes.
	m-node	Used for hybrid nodes to perform point-to-point communication after broadcasting.
	h-node	Hybrid nodes that broadcast after peer-to-peer communication.
	Designate	Hexadecimal node type, from 0 to 255.



<b>Address lease timeout</b>	Infinite	The lease period of the address is unlimited, and the number of days/hours/minutes below do not need to be filled in.
	Specified	There is a time limit for the lease of the address. You can rent it according to the lease time filled in below, and it will be automatically recovered if the time is exceeded.
<b>Operation</b>	Add	Add the above four parameters with check boxes to the switch, the parameters without check boxes will not be operated.
	Remove	Restore the four parameters with check boxes to the default configuration, and the parameters without check boxes will not be operated.

```

Information feedback window
Switch# show ip dhcp pool config
dhcp pool 1
    Lease  day:1, hour: 0, minute :0

```

Figure 195. Information display of the currently configured address pool.

### 13.2.1.2 client's default gateway configuration

The switch DHCP client default gateway configuration, the user configures the gateway parameters of the DHCP address pool.

Client's default gateway configuration	
DHCP pool name	1 ▾
Gateway 0	<input type="text"/>
Gateway 1	<input type="text"/>
Gateway 2	<input type="text"/>
Gateway 3	<input type="text"/>
Gateway 4	<input type="text"/>
Gateway 5	<input type="text"/>
Gateway 6	<input type="text"/>
Gateway 7	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 196.

<b>DHCP pool name</b>	The name of the created address pool.
<b>Gateway0-7</b>	Gateway IP address in dotted decimal format. Gateway 0 has the highest

	priority. The smaller the number, the higher the priority. The gateway can be set to zero or more, but the setting must start with 0 and no vacancies can appear in the middle, otherwise the gateway will be Ignored the following parameters, such as setting gateway 0-1 and gateway 7, only gateway 0-1 takes effect.	
<b>Operation</b>	Add	Add the gateway effectively set above to the currently selected DHCP address pool.
	Remove	Clear all gateways and restore to the default state.

```

Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# default-router 1.1.1.1

```

Figure 197. Information display after application.

### 13.2.1.3 Client DNS server configuration

The switch DHCP client DNS server configuration, the user configures the DNS server parameters of the DHCP address pool.

Client DNS server configuration	
DHCP pool name	1 ▾
DNS server 0	1.1.1.1
DNS server 1	
DNS server 2	
DNS server 3	
DNS server 4	
DNS server 5	
DNS server 6	
DNS server 7	
Operation	Add ▾
Apply	

Figure 198.

<b>DHCP pool name</b>	The name of the created address pool.
<b>DNS server 0-7</b>	For the IP address in dotted decimal format, DNS server 0 has the highest priority. The smaller the number, the higher the priority. The DNS server can be set to zero or more, but the setting must start from 0 and there can be no vacancies in the middle, otherwise the DNS server The following parameters will be ignored, such as setting DNS server 0-1 and DNS server 7, only DNS

	server 0-1 takes effect.	
<b>Operation</b>	Add	Add the DNS server effectively set above to the currently selected DHCP address pool.
	Remove	Clear all DNS servers and restore to the default state.

```

Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# dns-server 1.1.1.1

```

Figure 199. Information display after application.

### 13.2.1.4 Client WINS server configuration

The switch DHCP client WINS server configuration, the user configures the WINS server parameters of the DHCP address pool.

Client WINS server configuration	
DHCP pool name	1 ▾
WINS server 0	<input type="text"/>
WINS server 1	<input type="text"/>
WINS server 2	<input type="text"/>
WINS server 3	<input type="text"/>
WINS server 4	<input type="text"/>
WINS server 5	<input type="text"/>
WINS server 6	<input type="text"/>
WINS server 7	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 200.

<b>DHCP pool name</b>	The name of the created address pool.	
<b>WINS server 0-7</b>	The WINS server IP address in dotted decimal format. WINS server 0 has the highest priority. The smaller the number, the higher the priority. The WINS server can be set to zero or more, but the setting must start from 0 and there can be no vacancies in the middle, otherwise WINS server will ignore the following parameters, such as setting WINS server 0-1 and WINS server 7, only WINS server 0-1 takes effect.	
<b>Operation</b>	Add	Add the WINS server effectively set above to the currently selected DHCP address pool.
	Remove	Clear all WINS servers and restore them to the default

		state.
--	--	--------

```

Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# netbios-name-server 1.1.1.1

```

Figure 201. Information display after application.

### 13.2.1.5 DHCP file server address configuration

The switch client import file stores the address configuration, and the user configures the parameters of the DHCP address pool client import file.

DHCP file server address configuration	
DHCP pool name	1 ▾
DHCP client bootfile name	123. cfg
File server 0	1. 1. 1. 1
File server 1	
File server 2	
File server 3	
File server 4	
File server 5	
File server 6	
File server 7	
Operation	Add ▾
Apply	

Figure 202.

<b>DHCP pool name</b>	The name of the created address pool.	
<b>DHCP client bootfile name</b>	Specify the name of the file to be imported for the client. Usually used for diskless workstations, these workstations need to download configuration files from the server at startup.	
<b>File server 0-7</b>	The IP address in dotted decimal format has the highest priority for importing file server 0. The smaller the number, the higher the priority. The importing file server can be set to zero or more, but the setting must start from 0 and there should be no vacancies in the middle, otherwise Importing file server will ignore the following parameters, such as setting import file server 0-1 and import file server 7, only import file server 0-1 takes effect.	
<b>Operation</b>	Add	Add the imported file server effectively set above to the currently selected DHCP address pool.

	Remove	Clear all imported file servers and restore to the default state.
--	--------	---

```

Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# bootfile 123.cfg
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# next-server 1.1.1.1

```

Figure 203. Information display after application.

### 13.2.1.6 DHCP network parameter configuration

Switch network parameter configuration, the user configures the network parameters of the DHCP address pool.

DHCP network parameter configuration	
DHCP pool name	1 ▾
Code	
Network parameter value type	IP ADDRESS ▾
Network parameter value(ASCII,HEX or IP)	
Operation type	Add ▾
Apply	

Figure 204.

<b>DHCP pool name</b>	The name of the created address pool.	
<b>Code</b>	The code range of network parameters is 0-254, and each code corresponds to a different function in DHCP. The definition of option codes is described in detail in RFC2123.	
<b>Network parameter value type</b>	There are three types of network parameter values: ASCII, HEX, and IP ADDRESS.	
<b>Network parameter value (ASCII, HEX or IP)</b>	ASCII string, up to 255 characters; Hexadecimal value, not greater than 510, and must be an even number; IP address in decimal format, up to 63 IP addresses can be configured.	
<b>Operation</b>	Add	Add the network parameters of the selected address pool to the switch.
	Remove	Clear the network parameters filled in the selected address pool (delete according to the code of the network

		parameter).
--	--	-------------

```

Information feedback window
Switch# config t
Switch(config)# ip dhcp pool 1
Switch(dhcp-1-config)# option 82 ip 192.168.2.1
DHCPD: Option 82 has been added to pool 1

```

Figure 205. Information display after application.

**13.2.1.7 Excluded address configuration**

Excluding the dynamic allocation address configuration, the user configures the addresses that are not used for dynamic allocation.

Address allocation configuration		
Starting address	<input type="text"/>	<input type="text"/>
Ending address	<input type="text"/>	<input type="text"/>
Operation type	Add <input type="button" value="v"/>	<input type="text"/>
		<input type="button" value="Apply"/>

Figure 206.

<b>Starting address</b>	Start address not used for dynamic allocation.	
<b>Ending address</b>	End address not used for dynamic allocation.	
<b>Operation type</b>	Add	Add the address range that is not used and dynamically allocated to the switch.
	Remove	Delete the address range that is not used and dynamically allocated from the switch.

Address list	
Starting address	Ending address
1.1.1.1	1.1.1.25
end of list	

Figure 207. Display the address range currently not used for dynamic allocation.

**13.2.2 Manual DHCP IP pool configuration**

**13.2.2.1 Static address pool configuration**

Switch static address pool configuration, and manually bind client parameters.

Hardware address	
DHCP pool name	1 ▾
Parameter choose	ethernet ▾
Hardware address	00-11-22-33-44-55
Operation	Add ▾
Apply	

Figure 208.

<b>DHCP pool name</b>	The name of the created address pool.	
<b>Parameter choose</b>	The protocol type used by the client is rfc\ethernet\ieee802. RFC ID: RFC protocol number, valid range is 1-255.	
<b>Hardware address</b>	Hardware address.	
<b>Operation</b>	Add	Add manually bound hardware address and protocol type.
	Remove	Remove the manually bound hardware address and protocol type.

Client pool configuration	
Client pool configuration	1
Client IP address	
Client network mask	
Operation	Add ▾
Apply	

Figure 209.

<b>Client pool configuration</b>	The name of the created address pool (modify the selection through the address pool name of the user's hardware address).	
<b>Client IP address</b>	IP address assigned by the DHCP server to the client.	
<b>Client network mask</b>	The subnet mask assigned by the DHCP server to the client IP.	
<b>Operation</b>	Add	Add manually bound IP address and subnet mask.
	Remove	Delete the manually bound IP address and subnet mask.

User name	
DHCP pool name	1
User	
Client identifier	
Operation	Add ▼
Apply	

Figure 210.

<b>DHCP pool name</b>	The name of the created address pool (modify the selection through the address pool name of the user's hardware address).	
<b>user</b>	Client user name.	
<b>Client identifier</b>	The identifier of the client, for example: 44-11-22-33-44-55 (MAC address).	
<b>Operation</b>	Add	Add manually bound client identifier and user name.
	Remove	Delete the manually bound client identifier and user name.

### 13.2.3 Address pool name configuration

DHCP server address pool name configuration, user settings add and delete the address pool name.

Address pool name configuration	
DHCP pool name	
Operation type	Add pool ▼
Apply	

Figure 211.

<b>DHCP pool name</b>	The name of the created address pool.	
<b>Operation type</b>	Add pool	Add the address pool of the DHCP server.
	Remove pool	Delete the address pool of the DHCP server.

```

Information feedback window
Switch# show ip dhcp pool config
dhcp pool 1
Lease day:1, hour: 0, minute :0

```

Figure 212. Display the address pool of the current DHCP server.



### 13.2.4 DHCP packet statistics

DHCP server data packet statistics, users can view DHCP data packets.

DHCP packet statistics	
Address pool number	1
Proxy database	0
Dynamical assignment address	0
Manual binded address	0
Address conflict	0
Binding exceeding lease time	0
Errors	0
Received DHCP packet statistics	
Received	0
DHCP DISCOVER	0
DHCP REQUEST	0
DHCP DECLINE	0
DHCP RELEASE	0
DHCP INFORM	0
Transmitted DHCP packet statistics	
Transmitted	0
DHCP OFFER	0
DHCP ACK	0
DHCP NAK	0
DHCP RELAY	0
DHCP FORWARD	0
<input type="button" value="Clear"/> <input type="button" value="Show"/>	

Figure 213. It can be viewed in real time by clicking “Clear and” “Show”.

## 13.3 DHCP relay configuration

### 13.3.1 DHCP relay configuration

The switch DHCP relay configuration, the user configures the port range, and the switch sends UDP broadcast messages to the port.

DHCP forward UDP configuration	
Range	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Port
67

Figure 214.

<b>Range</b>	Port used by DHCP to forward UDP packets.	
<b>Operation</b>	Add	Add the port used by DHCP to forward UDP packets.
	Remove	Delete the port through which DHCP forwards UDP

		packets.
--	--	----------

DHCP help-address configuration		IP address	L3 Interface
IP address	<input type="text"/>	192.168.2.1	Vlan1
L3 Interface	Vlan1 <input type="button" value="v"/>		
Operation	Add <input type="button" value="v"/>		
		<input type="button" value="Apply"/>	

Figure 215.

<b>IP address</b>	IP address of the Layer 3 interface.	
<b>L3 Interface</b>	Established Layer 3 interface.	
<b>Operation</b>	Add	Add a Layer 3 interface for DHCP to forward UDP packets.
	Remove	Delete the Layer 3 interface through which DHCP forwards UDP packets.

## 13.4 DHCP debugging

### 13.4.1 Delete record

#### 13.4.1.1 Delete binding log

DHCP binding record deletion, users can delete all binding records or delete specified binding records, static binding records need to be deleted in the static address pool configuration.

Delete DHCP binding log	
Delete binding area	Delete all binding log <input type="button" value="v"/>
IP Address	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 216.

<b>Delete binding area</b>	Delete all binding log.	Delete all binding records, no need to fill in the IP address below.
	Delete specify binding log.	Delete the specified binding record, fill in the deleted IP in the IP address below.
<b>IP Address</b>	IP address in dotted decimal notation.	

#### 13.4.1.2 Delete conflict log

The DHCP conflict record is deleted, and the user can delete all conflict records or delete the specified conflict record.

Delete conflict log	
Delete conflict address area	Delete all conflict log ▼
IP Address	
Apply	

Figure 217.

<b>Delete conflict log</b>	Delete all conflict log	Delete all conflict records, no need to fill in the IP address below.
	Delete specify binding log	Delete the specified conflict record, fill in the deleted IP in the IP address below.
<b>IP Address</b>	IP address in dotted decimal notation.	

### 13.4.1.3 Delete DHCP server statistics log

Deleting the statistics records of the DHCP server, the user can delete all the statistics records of the DHCP server.

Delete DHCP server statistics log
Apply

Figure 218. After deleting the statistical record of the DHCP server, the statistical information of the DHCP packet will be cleared.

### 13.4.2 show IP-MAC binding

The DHCP server's IP and MAC binding status, the user can view the binding entries and the relationship between the bound IP and MAC.

```

Information feedback window
Switch# clear ip dhcp server statistics
Switch# show ip dhcp binding
Total dhcp binding items: 0, the matched: 0
IP address      Hardware address  Lease expiration  Type
  
```

Figure 219.

<b>IP address</b>	Client's IP address.	
<b>Hardware address</b>	The hardware address or MAC address of the client.	
<b>Lease expiration</b>	Client IP expiration time.	
<b>Type</b>	Manual	Manual binding.
	Dynamic	Dynamic allocation.

### 13.4.3 show conflict-logging

The conflict record of the DHCP server, the user can view the conflict situation.

```
Information feedback window
Switch# show ip dhcp conflict
IP Address      Detection method  Detection Time
```

Figure 220.

<b>Display info</b>	Description.
<b>IP Address</b>	Conflicting IP address.
<b>Detection method</b>	The conflicting method was detected.
<b>Detection Time</b>	The time when the conflict was detected.

## 14. DHCP Snooping configuration

### 14.1 DHCP Snooping global configuration

#### 14.1.1 Enable/Disable DHCP Snooping

With the enabling and disabling of the DHCP Snooping module, users can view and operate the status of DHCP Snooping.

Figure 221.

<b>DHCP Snooping status</b>	Disable	Disable DHCP Snooping.
	Enable	Enable DHCP Snooping.

Figure 222. Display the current DHCP Snooping status.

#### 14.1.2 DHCP Snooping binding configuration

When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

Figure 223.

<b>DHCP Snooping binding status</b>	Disable	Disable DHCP Snooping binding function.
	Enable	Enable DHCP Snooping binding function.

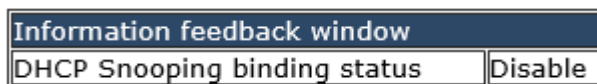


Figure 224. Shows whether the current DHCP Snooping binding status function is enabled.

### 14.1.3 DHCP Snooping binding user configuration

When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

DHCP Snooping binding user configuration	
MAC address	<input type="text"/>
User IP address	<input type="text"/>
User mask	<input type="text"/>
VLAN ID	<input type="text"/>
Port	Ethernet1/0/1 <input type="button" value="v"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 225.

<b>MAC address</b>	The MAC address of the statically bound user is the only index of the bound user.	
<b>User IP address</b>	Statically bind the user's IP address.	
<b>User mask</b>	Statically bind the user's subnet mask.	
<b>VLAN ID</b>	Statically bind the VLAN ID of the user.	
<b>Port</b>	Bind the user's access port statically, the port is associated with the VLAN ID, and the port is required to allow the VLAN to pass.	
<b>Operation</b>	Add	Add DHCP Snooping binding user relationship.
	Remove	Delete DHCP Snooping binding user relationship.

```

Information feedback window
Switch# config t
Switch(config)# no Ip dhcp snooping binding user 00-22-33-44-55-66 interface Ethernet1/0/1 vlan 1
Please enable dhcp snooping binding in global first!
    
```

Figure 226. Display the process and error messages or results generated during application execution.

#### 14.1.4 DHCP Snooping action count config

DHCP Snooping defense action number configuration, if the number of alarm messages is greater than the set number, it will force the restoration of the earliest defense measures to send new defense measures.

DHCP Snooping action count config	
DHCP Snooping action count	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 227.

<b>DHCP Snooping action count</b>	Set the maximum number of defense actions to avoid exhaustion of switch resources caused by attacks.	
<b>Operation</b>	Add	Configure the number of defense actions filled in above.
	Remove	Reduce the number of defense actions to 10.

Information feedback window	
DHCP Snooping action count	10

Figure 228. Display the current number of DHCP Snooping defense actions.

#### 14.1.5 DHCP Snooping limit-rate config

DHCP Snooping packet receiving rate limit sets the number of DHCP messages sent per second.

DHCP Snooping limit-rate config	
Packet per second	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 229.

<b>Packet per second</b>	Range: 0-100.	
<b>Operation</b>	Add	Configure the number of packets per second.
	Remove	Restore the default number of packets per second, the default is 100.

Information feedback window	
Packet per second	100

Figure 230. Display the number of packets per second configured for the current DHCP Snooping.

### 14.1.6 DHCP Snooping helper-server config

DHCP SNOOPING will send the monitored binding information to HELPER SERVER for storage. If the switch starts abnormally, you can recover the bound data from the HELPER SERVER.

DHCP Snooping helper-server config	
Helper-server address	<input type="text"/>
Helper-server UDP port	<input type="text"/>
Local IP address	<input type="text"/>
Second address	<input type="text"/> <input type="button" value="v"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 231.

<b>Helper-server address</b>	HELPER server address.	
<b>Helper-server UDP port</b>	DHCP SNOOPING and HELPER SERVER use UDP protocol for communication, the port range is 1-65535.	
<b>Local IP address</b>	The effective management IP address of the switch.	
<b>Second address</b>	Two HELPER server addresses are allowed, DHCP SNOOPING will first try to connect to the PRIMARY server. Only when the PRIMARY server cannot be accessed, the switch HELPER server will connect to the SECONDARY server. Set the PRIMARY server before setting up the SECONDARY server.	
<b>Operation</b>	Add	Add HELPER server address.
	Remove	Delete the HELPER server address, you can leave it blank when deleting.

Information feedback window	
Switch#	config t
Switch(config)#	no ip user helper-address

Figure 232.

Display the process and error messages or results generated during application execution.

## 14.2 DHCP Snooping port configuration

### 14.2.1 Enable/Disable DHCP Snooping binding dot1x

DHCP SNOOPING will notify the DOT1X module of the binding information captured by the user controlled by the DOT1X. DHCP Snooping port binding dot1x function needs to enable DHCP Snooping binding configuration first.

Enable/Disable DHCP Snooping binding dot1x	
Port	DHCP Snooping binding dot1x status
Ethernet1/0/1 ▾	Enable ▾
Apply	

Figure 233.

Port	Port name.	
<b>DHCP Snooping binding dot1x status</b>	Enable	Enable the dot1x status of DHCP Snooping port binding.
	Disable	Disable the dot1x binding status of the DHCP Snooping port.

Information feedback window	
Port	DHCP Snooping binding dot1x status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable

Figure 234. Display the dot1x binding status of each DHCP Snooping port of the switch.

### 14.2.2 Enable/Disable DHCP Snooping binding user

When this function is enabled on the port, DHCP SNOOPING will treat the captured binding information as a trusted user who is allowed to access all resources. The DHCP Snooping port binding user status function needs to enable the DHCP Snooping binding configuration first.

Enable/Disable DHCP Snooping binding user	
Port	DHCP Snooping binding user status
Ethernet1/0/1 ▾	Enable ▾
Apply	

Figure 235.

Port	Port name.
------	------------



<b>DHCP Snooping binding user status</b>	Enable	Enable DHCP Snooping port binding user status.
	Disable	Disable DHCP Snooping port binding user status.

Information feedback window	
Port	DHCP Snooping binding user status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable

Figure 236. Display the status of users bound to each DHCP Snooping port of the switch.

### 14.2.3 Enable/Disable DHCP Snooping trust

When a port changes from an untrusted port to a trusted port, the original defense action of the port will be automatically deleted; all security history records will be cleared.

Enable/Disable DHCP Snooping trust	
Port	DHCP Snooping binding trust status
Ethernet1/0/1 ▾	Enable ▾
Apply	

Figure 237.

<b>Port</b>	Port name.	
<b>DHCP Snooping binding trust status</b>	Enable	Enable DHCP Snooping port trust attribute status.
	Disable	Disable the trust attribute status of the DHCP Snooping port.

Information feedback window	
Port	DHCP Snooping binding trust status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable

Figure 238. Display the trust attribute status of each DHCP Snooping port of the switch.

#### 14.2.4 DHCP Snooping action config

Automatic port defense action, the port will detect the fake DHCP server, and the trusted port will not detect the fake DHCP server, so the corresponding defense action will never be triggered. When a port changes from an untrusted port to a trusted port, the original defense action of the port will be automatically deleted.

DHCP Snooping action config	
Port	Ethernet1/0/1 ▾
DHCP Snooping action	shutdown ▾
DHCP Snooping recovery time	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 239.

<b>Port</b>	Port name.	
<b>DHCP Snooping action</b>	shutdown	Automatically close the port.
	blackhole	Block traffic from fake DHCP server based on MAC.
<b>DHCP Snooping recovery time</b>	The user can set the recovery after performing automatic defense operations.	
<b>Operation</b>	Add	Add DHCP Snooping port automatic defense configuration.
	Remove	Delete DHCP Snooping port automatic defense configuration.

Information feedback window		
Port	DHCP Snooping action	DHCP Snooping recovery time
Ethernet1/0/1	none	0
Ethernet1/0/2	none	0
Ethernet1/0/3	none	0
Ethernet1/0/4	none	0
Ethernet1/0/5	none	0
Ethernet1/0/6	none	0
Ethernet1/0/7	none	0
Ethernet1/0/8	none	0

Figure 240. Display the automatic defense configuration of each DHCP Snooping port.

## 14.3 show DHCP Snooping configuration

### 14.3.1 show DHCP Snooping configuration

Display detailed configuration of DHCP Snooping.

**Show DHCP Snooping configuration**

DHCP Snooping show object  ▼

Figure 241.

<b>DHCP Snooping show object</b>	All	All ports are displayed.
	Ethernet1/0/1-28	Only display information about one port.

```

Information feedback window
Switch# show ip dhcp snooping interface Ethernet1/0/1
interface Ethernet1/0/1 user config:
trust attribute: untrust
action: none
binding dot1x: disabled
binding user: disabled
binding mab guard: disabled
recovery interval:0(s)
Driver user number 0 : Max user number 1024
Alarm info: 0
Binding info: 0
Static Binding info: 0
Static Binding info from shell: 0
Static Binding info from server: 0
flag: D - Dynamic ; U - already upload server ;
S - static binding info from shell; R - static binding info from server;
O - dhcp ack has option82; X - notify dot1x ok;
L - notify driver ok; E - notify dot1x error
P - binding protect;
Expired Binding: 0
Request Binding: 0

```

Figure 242. Select Ethernet1/0/1, only display the DHCP Snooping information of Ethernet1/0/1.

## 15. SNTP configuration

## 15.1 SNTP server configuration

SNTP the server settings module, the user can add or delete the specified time server as the clock source.

The figure shows two screenshots. The top one is a configuration form titled "SNTP server and version configuration" with fields for "Server address", "Version", and "Operation" (set to "Add"), and an "Apply" button. The bottom one is an "Information feedback window" showing a terminal-style output: "SW1# config t", "SW1(config)# show sntp", and a table with columns "server address", "version", and "last receive".

Figure 243.

<b>Server address</b>	The specified time server address decimal point.	
<b>Version</b>	Version number, range 1-4, default 4.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 15.2 Request interval configuration

Send request interval setting module, where the user can set the interval SNTP the client sends a request to the NTP/SNTP. By default, the interval is 64 seconds.

The figure shows two screenshots. The top one is a configuration form titled "Request interval from SNTP client to SNTP server" with fields for "Interval", "Operation" (set to "Configuration"), and an "Apply" button. The bottom one is a display window titled "Interval" showing a table with "Interval" and the value "64".

Figure 244.

<b>Interval</b>	Duration value, range 16-16284 s.	
<b>Operation</b>	Configuration	Configuration operations.
	Default	Do recovery default (default 64 s).

## 15.3 Time difference configuration

SNTP the time zone and UTC time difference setting module where the client is located, the user can set the switch's current time zone and name it.

Time difference configuration	
Time zone	<input type="text"/>
Time difference	<input checked="" type="radio"/> After-utc <input type="radio"/> Before-utc
Time value	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 245.

<b>Time zone</b>	Time zone name, 1-16 characters.	
<b>Time difference</b>	Add	Increased time zone behavior.
	Reduce	Reduced time zone behavior.
<b>Time value</b>	Time zone specific change hours 0-23.	Time zone specific change minute value 0-59.
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 15.4 Show sntp

Display SNTP module, where users can view the current information status SNTP the switch.

```

Information feedback window
SW1# config t
SW1(config)# show sntp
server address                version last receive

```

Figure 246.

## 16. NTP configuration

### 16.1 NTP global configuration

#### 16.1.1 NTP global switch configuration

NTP service global switch configuration module, user can NTP service global switch operation.

NTP global switch configuration	
Operation	Disable <input type="button" value="v"/>
<input type="button" value="Apply"/>	

NTP global switch configuration	
NTP global configuration	disable

Figure 247.

<b>Operation</b>	Disable	Close operation.
	Enable	Start (default).

### 16.1.2 NTP server configuration

NTP the server configuration module, the user can configure the specified time server of the switch time source in this module.

NTP server and version configuration	
Server address	<input type="text"/>
Version	<input type="text"/>
Key	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

```

Information feedback window
SW1# config t
SW1(config)# show ntp session
ntp peer doesn't exist!
    
```

Figure 248.

<b>Server address</b>	The specified time server address decimal point.	
<b>Version</b>	Version number, range 1-4, default 4.	
<b>Key</b>	Secret key value, range 1-4294967295.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

### 16.1.3 NTP broadcast or multicast address count configuration

NTP service address number configuration module, the user can configure the maximum number of broadcast or multicast servers supported by the switch NTP client.

NTP broadcast or multicast address count configuration	
Address max count	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

```

Address max count
Address max count 50
    
```

Figure 249.

<b>Address max count</b>	Maximum number of broadcast or multicast servers supported NTP clients, 1-100 (default 50).	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

### 16.1.4 NTP access group configuration

NTP access control list configuration module, where users can configure switch NTP access control list.

NTP access group configuration	
Access list	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 250.

<b>Access list</b>	IPv4: 1-99; IPv6: 50-599.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

### 16.1.5 NTP authenticate configuration

NTP verification configuration module, the user can configure the switch NTP authentication related items.

NTP authenticate configuration	
NTP authenticate switch	Disable <input type="button" value="v"/>
Key type	none <input type="button" value="v"/>
Key	<input type="text"/>
MD5	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 251.

<b>NTP authenticate switch</b>	Disable	Close NTP validation (default).
	Enable	Enable NTP validation.
<b>Key type</b>	none	none
	authentication-key	Authentication secret key.
	trusted-key	Trust key.
<b>Key</b>	Secret key value, range 1-4294967295.	
<b>Md5</b>	The MD5 value of the secret key, which ranges from 1-16 of ascii code.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 16.2 NTP interface configuration

### 16.2.1 NTP interface switch configuration

NTP service interface switch configuration module, the user can specify the NTP service interface switch operation.

NTP interface configuration	
VLAN interface	Vlan1 ▾
NTP interface configuration	Disable ▾
NTP interface client	none ▾
Apply	

Figure 252.

<b>VLAN interface</b>	VLAN1	VLAN interface for current switch configurable.
<b>NTP interface configuration</b>	Disable	Close operation.
	Enable	Start-up operation.
<b>NTP interface client</b>	none	Interface NTP client type.
	broadcast	
	no broadcast	
	multicast	
	no multicast	
	ipv6 multicast	
	no ipv6 multicast	

## 16.3 NTP configuration display

### 16.3.1 NTP status display

NTP status display module, where users can view NTP service current status information.

```

Information feedback window
SW1# show ntp status
ntp clock status: unsynchronized
    
```

Figure 253.

## 17. QOS port configuration

### 17.1 QOS port configuration

#### 17.1.1 QOS port trust state configuration

Configure port trust rules.



QoS port trust state configuration	
Port	Ethernet1/0/1 ▾
Packet class rule	COS ▾
Operation	Add ▾
Apply	

Figure 254.

<b>Port</b>	To configure the port name, click to expand the remaining ports.	
<b>Packet class rule</b>	COS	Cos to int mapping based on intp field.
	DSCP	Intp field based on dscp to intp mapping.
<b>Operation</b>	Add	Add a trust rule for the port.
	Remove	Remove a trust rule for the port.

Information feedback window	
Port	Trust class
Ethernet1/0/1	COS
Ethernet1/0/2	COS
Ethernet1/0/3	COS
Ethernet1/0/4	COS
Ethernet1/0/5	COS
Ethernet1/0/6	COS
Ethernet1/0/7	COS
Ethernet1/0/8	COS

Figure 255.

### 17.1.2 QOS port COS parameters configuration

Configure the COS value of the port, regardless of whether the trust rule of the current port is trusted.

QoS port cos parameters configuration	
Port	Ethernet1/0/1 ▾
Port related COS value	<input type="text"/>
Operation	Add ▾
Apply	

Figure 256.

<b>Port</b>	To configure the port name, click to expand the remaining ports.
<b>Port related</b>	The default COS value of the port, range: 0-7.

<b>COS value</b>		
<b>Operation</b>	Add	Add the COS value of the port.
	Remove	Delete the COS value of the port and restore it to 0.

Information feedback window	
Port	Port related COS value
Ethernet1/0/1	0
Ethernet1/0/2	0
Ethernet1/0/3	0
Ethernet1/0/4	0
Ethernet1/0/5	0
Ethernet1/0/6	0
Ethernet1/0/7	0
Ethernet1/0/8	0

Figure 257.

### 17.1.3 QoS port select queue schedule algorithm configuration

Configure the port to process the priority of packets according to different queue scheduling algorithms.

QoS port select queue schedule algorithm configuration	
Port	Ethernet1/0/1 ▼
Queue schedule algorithm	sp ▼
Apply	

Figure 258.

<b>Port</b>	To configure the port name, click to expand the remaining ports.	
<b>Queue schedule algorithm</b>	sp	Strict queuing priority, packet transmission in order of priority.
	wrr	Weighted round-robin scheduling. Rotate scheduling between queues to ensure that each queue gets a certain amount of service time.
	wdr	Weighted difference round-robin scheduling, based on message length transmission, based on the combined effect of weight and K value to generate the length of transmission in the message queue.

Information feedback window	
Port	Trust class
Ethernet1/0/1	sp
Ethernet1/0/2	wdr
Ethernet1/0/3	wrr
Ethernet1/0/4	wrr
Ethernet1/0/5	wrr
Ethernet1/0/6	wrr
Ethernet1/0/7	wrr
Ethernet1/0/8	wrr

Figure 259. Display the queue scheduling algorithm trusted by the current port.

### 17.1.4 QoS port wrr algorithm queue weight configuration

Configure the weight value of the eight queues of each port, and allocate the number of packets according to the weight value.

QoS port wrr algorithm queue weight configuration	
Port	Ethernet1/0/1 ▼
Weight1	<input type="text"/>
Weight2	<input type="text"/>
Weight3	<input type="text"/>
Weight4	<input type="text"/>
Weight5	<input type="text"/>
Weight6	<input type="text"/>
Weight7	<input type="text"/>
Weight8	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Figure 260.

<b>Port</b>	To configure the port name, click to expand the remaining ports.
<b>Weight1</b>	The weight value of queue 1, the range is 0-127.
<b>Weight2</b>	The weight value of queue 2, the range is 0-127.
<b>Weight3</b>	The weight value of queue 3, the range is 0-127.
<b>Weight4</b>	The weight value of queue 4, the range is 0-127.
<b>Weight5</b>	The weight value of queue 5, the range is 0-127.
<b>Weight6</b>	The weight value of queue 6, the range is 0-127.
<b>Weight7</b>	The weight value of queue 7, the range is 0-127.
<b>Weight8</b>	The weight value of queue 8, the range is 0-127.

<b>Operation</b>	Add	Add the weight of each queue to the port, and fill in all the weights of each queue before adding.
	Remove	To restore the weight of each queue of the port to the default, you need to add the value of eight queues.

Information feedback window	
Port	Queue weight
Ethernet1/0/1	1 2 3 4 5 6 7 8
Ethernet1/0/2	1 2 3 4 5 6 7 8
Ethernet1/0/3	1 2 3 4 5 6 7 8
Ethernet1/0/4	1 2 3 4 5 6 7 8
Ethernet1/0/5	1 2 3 4 5 6 7 8
Ethernet1/0/6	1 2 3 4 5 6 7 8
Ethernet1/0/7	1 2 3 4 5 6 7 8
Ethernet1/0/8	1 2 3 4 5 6 7 8

Figure 261. Information feedback window.

### 17.1.5 QoS port wrr algorithm queue weight configuration

Configure the weight value of the eight queues of each port, transmit based on the length of the message, and generate the transmission length in the message queue based on the combined action of the weight and the K value.

QoS port wrr algorithm queue weight configuration	
Port	Ethernet1/0/1 ▾
Weight1	<input type="text"/>
Weight2	<input type="text"/>
Weight3	<input type="text"/>
Weight4	<input type="text"/>
Weight5	<input type="text"/>
Weight6	<input type="text"/>
Weight7	<input type="text"/>
Weight8	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 262.

<b>Port</b>	To configure the port name, click to expand the remaining ports.
<b>Weight1</b>	The weight value of queue 1, the range is 0-32767.
<b>Weight2</b>	The weight value of queue 2, the range is 0-32767.

<b>Weight3</b>	The weight value of queue 3, the range is 0-32767.	
<b>Weight4</b>	The weight value of queue 4, the range is 0-32767.	
<b>Weight5</b>	The weight value of queue 5, the range is 0-32767.	
<b>Weight6</b>	The weight value of queue 6, the range is 0-32767.	
<b>Weight7</b>	The weight value of queue 7, the range is 0-32767.	
<b>Weight8</b>	The weight value of queue 8, the range is 0-32767.	
<b>Operation</b>	Add	Add the weight of each queue to the port, and fill in all the weights of each queue before adding.
	Remove	To restore the weight of each queue of the port to the default, you need to add the value of eight queues.

### 17.1.6 QOS service policy configuration

Configure the port's policy table, and the port will process packets according to the rules of the classification table in the policy table.

Figure 263.

<b>Port</b>	To configure the port name, click to expand the remaining ports.	
<b>Policy map name</b>	The name of the policy table, added by the policy table configuration.	
<b>Operation</b>	Add	Policy for adding ports.
	Remove	Delete port policy.

## 17.2 QOS class-map configuration

### 17.2.1 Class map-configuration

Create and delete classification tables, view the currently configured classification tables.

Figure 264.

<b>Class-map name</b>	Class-map name, range: 1-64 character.	
<b>Operation</b>	Add	Add Class-map.
	Remove	Remove Class-map.

Information feedback window	
Class-map name	1

Figure 265. Display the currently created class-map name.

### 17.2.2 classification criteria configuration

Set the rules and corresponding parameters for classification matching.

Classification criteria configuration	
Classification criteria rule	access-group ▾
Class-map name	1 ▾
ACL list name	
Operation	Add ▾
Apply	

Figure 266.

<b>Classification criteria rule</b>	accesss-group	Match the specified IP ACL, MAC ACL or IPv6 standard ACL or MAC-IP ACL.
<b>Class-map name</b>	The name of the created class-matching table, select by clicking the drop-down.	
<b>ACL list name</b>	Created ACL name, 1-64 characters.	
<b>Operation</b>	Add	Add matching rules.
	Remove	Remove matching rules.

Classification criteria configuration	
Classification criteria rule	ip dscp ▾
Class-map name	1 ▾
IP dscp0	
IP dscp1	
IP dscp2	
IP dscp3	
IP dscp4	
IP dscp5	
IP dscp6	
IP dscp7	
Operation	Add ▾
Apply	

Figure 267.

<b>Classification criteria rule</b>	ip dscp	Match the specified DSCP value, this parameter is the DSCP list.
<b>Class-map name</b>	The name of the created class-matching table, select by clicking the drop-down.	
<b>IP dscp 0-7</b>	One or more DSCP values can be set, up to 8 DSCP values can be set, the range is 0~63.	
<b>Operation</b>	Add	Add matching rules.
	Remove	Remove matching rules.

Classification criteria configuration	
Classification criteria rule	ip precedence ▾
Class-map name	1 ▾
IP precedence0	
IP precedence1	
IP precedence2	
IP precedence3	
IP precedence4	
IP precedence5	
IP precedence6	
IP precedence7	
Operation	Add ▾
Apply	

Figure 268.

<b>Classification criteria rule</b>	ip precedence	Match the specified ip priority, this parameter is the IP priority list.
<b>Class-map name</b>	The name of the created class-matching table, select by clicking the drop-down.	
<b>IP precedence 0-7</b>	One or more ip priority values can be set, the list contains up to 8 IP priority values, and the valid range is 0~7.	
<b>Operation</b>	Add	Add matching rules.
	Remove	Remove matching rules.

Classification criteria configuration	
Classification criteria rule	vlan <input type="button" value="v"/>
Class-map name	1 <input type="button" value="v"/>
Vlan0	<input type="text"/>
Vlan1	<input type="text"/>
Vlan2	<input type="text"/>
Vlan3	<input type="text"/>
Vlan4	<input type="text"/>
Vlan5	<input type="text"/>
Vlan6	<input type="text"/>
Vlan7	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 269.

<b>Classification criteria rule</b>	vlan	Match the specified vlan, this parameter is a list of vlan id.
<b>Class-map name</b>	The name of the created class-matching table, select by clicking the drop-down.	
<b>Vlan 0-7</b>	One or more VLAN IDs can be set, including 8 VLAN IDs at most, ranging from 1 to 4094.	
<b>Operation</b>	Add	Add matching rules.
	Remove	Remove matching rules.



Classification criteria configuration	
Classification criteria rule	cos <input type="button" value="v"/>
Class-map name	1 <input type="button" value="v"/>
Cos0	<input type="text"/>
Cos1	<input type="text"/>
Cos2	<input type="text"/>
Cos3	<input type="text"/>
Cos4	<input type="text"/>
Cos5	<input type="text"/>
Cos6	<input type="text"/>
Cos7	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 270.

<b>Classification criteria rule</b>	cos	Match the specified CoS value, this parameter is a list of vlan id.
<b>Class-map name</b>	The name of the created class-matching table, select by clicking the drop-down.	
<b>Cos 0-7</b>	One or more cos values can be set, the parameter is a CoS list composed of up to 8 CoS, the range is 0~7.	
<b>Operation</b>	Add	Add matching rules.
	Remove	Remove matching rules.

Classification criteria configuration	
Classification criteria rule	ipv6 dscp <input type="button" value="v"/>
Class-map name	1 <input type="button" value="v"/>
IPv6 dscp0	<input type="text"/>
IPv6 dscp1	<input type="text"/>
IPv6 dscp2	<input type="text"/>
IPv6 dscp3	<input type="text"/>
IPv6 dscp4	<input type="text"/>
IPv6 dscp5	<input type="text"/>
IPv6 dscp6	<input type="text"/>
IPv6 dscp7	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 271.

<b>Classification criteria rule</b>	ipv6 dscp	Match the specified ipv6 DSCP value, this parameter is the ipv6 DSCP list.
<b>Class-map name</b>	The name of the created class-matching table, select by clicking the drop-down.	
<b>IPv6 dscp 0-7</b>	One or more ipv6 DSCP values can be set, up to 8 DSCP values can be set, the range is 0~63.	
<b>Operation</b>	Add	Add matching rules.
	Remove	Remove matching rules.

Classification criteria configuration	
Classification criteria rule	ipv6 flowlabel ▾
Class-map name	1 ▾
IPv6 flowlabel0	
IPv6 flowlabel1	
IPv6 flowlabel2	
IPv6 flowlabel3	
IPv6 flowlabel4	
IPv6 flowlabel5	
IPv6 flowlabel6	
IPv6 flowlabel7	
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 272.

<b>Classification criteria rule</b>	ipv6 flow label	Match the specified IPv6 flow label, this parameter is the value of the IPv6 flow label DSCP list.
<b>Class-map name</b>	The name of the created class-matching table, select by clicking the drop-down.	
<b>IPv6 flow label 0-7</b>	One or more IPv6 flow label values can be set, ranging from 0 to 1048575.	
<b>Operation</b>	Add	Add matching rules.
	Remove	Remove matching rules.

```

反馈信息窗口
Switch# config t
Switch(config)# class-map c1
Switch(config-classmap-c1)# match access-group 1

```

Figure 273. Display configuration application execution process and return result.

## 17.3 QoS policy configuration

### 17.3.1 QoS policy configuration

Configure the policy table burst-group, provide the policy class-map to use.

policy configuration	
policy burst id configuration:	1 ▾
policy burst size configuration	
Apply	

Figure 274.

<b>Policy burst id configuration</b>	There are only two IDs, 1 and 2.
<b>Policy burst size configuration</b>	The default is 1024, the range that can be set: 1-8192.

## 17.4 QOS policy-map configuration

### 17.4.1 policy-map configuration

Create and delete policy tables, and collaborate with classification tables to create packet in and out rules.

Policy-map configuration	
Policy-map name	
Operation	Add ▾
Apply	

Figure 275.

<b>Policy-map name</b>	Policy-map name, range: 1-64 character.	
<b>Operation</b>	Add	Add policy-map.
	Remove	Remove policy-map.

Information feedback window	
Policy-map name	p1

Figure 276. Display the currently created policy-map.

## 17.4.2 Class-map use to policy-map config

Apply the class-map to the policy-map.

Class-map use to policy-map configuration	
Policy-map name	p1 ▾
Class-map name	
Inserted before the class-map name	
Operation	Add ▾
Apply	

Figure 277.

<b>policy-map name</b>	The name of the created policy-map.	
<b>class-map name</b>	The name of the classification table created by the classification matching table, this table will be applied to the policy-map.	
<b>Inserted before the class-map name</b>	Prior to the insertion of the classification matching table, the name of the classification table that has been applied to the strategy table, and the priority of the newly applied classification matching table is increased.	
<b>Operation</b>	Add	Add an association between the strategy table and the classification table.
	Remove	Remove an association between the strategy table and the classification table.

Information feedback window	
Policy-map name	Class-map name
p1	1

Figure 278. Display the association between the created policy table and the classification matching table.

## 17.5 QoS policy-class-map configuration

### 17.5.1 Policy-class-map accounting configuration

Configure the statistics switch of the strategy table and the classification matching table, and display the association between the strategy table and the classification matching table.

Policy-class-map accounting configuration	
Policy-map name	p1 ▾
Class-map name	c1 ▾
Accounting switch	Disable ▾
Apply	

Figure 279.

<b>Policy-map name</b>	The name of the policy-map that has been created.	
<b>Class-map name</b>	The name of the classification matching table that has been created.	
<b>Accounting switch</b>	Disable	Disable the traffic statistics function associated with the policy-map and class-map, and automatically establish an association if there is no association.
	Enabled	Start the traffic statistics function associated with the policy-map and class-map, and automatically establish an association if there is no association.

Information feedback window		
Policy-map name	Class-map name	Accounting switch
p1	c1	Enable

Figure 280. Display the traffic statistics switch information of the associated policy-map and class-map table.

### 17.5.2 Aggregate policy configuration

Configure the set strategy of the associated policy table and classification matching table. The policy mapping refers to the aggregation policy, and the aggregation policy is applied to the classified traffic. The same policy set can be referenced by different policy class mappings.

Aggregate policy configuration	
Policy-map name	p1 ▾
Class-map name	c1 ▾
Aggregate policy name	
Operation	Add ▾
Apply	

Figure 281.

<b>Policy-map name</b>	Name of the created policy table.
------------------------	-----------------------------------

<b>Class-map name</b>	Classification match table created.	
<b>Aggregate policy name</b>	The name of the aggregation strategy, 1-64 characters in length.	
<b>Operation</b>	Add	Start the set strategy associated with the strategy table and the classification matching table, and automatically establish the association if there is no associated strategy table and the classification matching table.
	Remove	Close the set strategy associated with the strategy table and the classification matching table, and automatically establish the association between the strategy table and the classification matching table without association.

Information feedback window		
Policy-map name	Class-map name	Aggregate policy name
p1	c1	a1

Figure 282. Display the set policy information of the associated policy table and the classification matching table.

### 17.5.3 Policy-class-map policy configuration

Configure the information rate in the policy mapping configuration mode.

Policy-class-map policy configuration	
Policy-map name	p1 ▾
Class-map name	c1 ▾
Committed information rate	
Committed burst id:	1 ▾
Operation	Add ▾
Apply	

Figure 283.

<b>Policy-map name</b>	Name of the created policy table.
<b>Class-map name</b>	Classification match table created.
<b>Committed information rate</b>	Committed Information Rate-CIR (Committed Information Rate), in Kbps, ranging from 1 to 10,000,000.
<b>Committed burst ID</b>	The burst ID range is 1 and 2, and the main commitment is the burst size.

<b>Operation</b>	Add	Add the strategy information rate and burst size associated with the strategy table and the classification matching table, and automatically establish the association if there is no associated strategy table and the classification matching table.
	Remove	Delete the policy information rate and burst size associated with the policy table and the classification matching table, and automatically establish the association if there is no associated policy table and the classification matching table.

### 17.5.4 Policy-class-map set configuration

Configure the priority of packets in the policy mapping configuration mode. Assign a new DSCP and IP priority to the classified traffic. Only the classified traffic that meets the matching criteria will be assigned a new value.

Figure 284.

<b>Classification criteria rule</b>	ip dscp	Set the DSCP value again according to the rules defined in the policy-map and class-map.
	ip precedence	Set the IP priority again according to the rules defined in the policy-map and class-map.
	drop-precedence	Set the discarding priority again according to the rules defined in the policy-map and class-map.
	internal-priority	Set the internal priority again according to the rules defined by the policy-map and class-map.
	cos	Set the COS value again according to the rules defined by the policy table and the classification matching table.
	ipv6 default next hop vrf	Set the default next hop address again according to the rules defined in the policy table and classification matching table.
<b>Policy-map name</b>	The name of the created policy table.	
<b>Class-map name</b>	Created classification match table.	
<b>DSCP</b>	DSCP value, range: 0-63.	

<b>Precedence</b>	IP priority, range: 0-7.	
<b>Drop-precedence</b>	Drop priority, range: 0-2.	
<b>Internal-priority</b>	Internal priority, range: 0-7.	
<b>COS</b>	COS value, range: 0-7.	
<b>Vrf</b>	Vrf value, range: 0-252.	
<b>IPv6 Address (X:X::X:X)</b>	IPv6 default next hop address.	
<b>Operation</b>	Add	Add the priority and queue value associated with the strategy table and the classification matching table.
	Remove	Remove the priority and queue value associated with the strategy table and the classification matching table.

## 17.6 QoS mapping configuration

### 17.6.1 COS-to-IntP mapping

Configure the value mapped from the COS value to the internal priority (queue).

CoS-to-IntP mapping								
CoS value	0	1	2	3	4	5	6	7
IntP value	0	1	2	3	4	5	6	7
Operation type	Configuration ▾							
								Apply

Figure 285.

<b>CoS value</b>	The COS value carried in the message or the default COS value assigned when entering.	
<b>IntP value</b>	The value of the internal priority (queue) to which the COS value will be mapped.	
<b>Operation type</b>	Configuration	Configure the value of COS to IntP.
	Default	Restore the mapping relationship to the default state.

```

反馈信息窗口
Switch# config t
Switch(config)# mls qos map cos-intp 2 1 2 3 4 5 6 7

Ingress COS-TO-Internal-Priority map:
COS:  0  1  2  3  4  5  6  7
-----
INTP: 2  1  2  3  4  5  6  7

```



Figure 286. Display the execution process and the current mapping relationship.

### 17.6.2 COS-to-DP mapping

Configure the value mapped from the COS value to the drop priority (queue).

CoS-to-DP mapping								
CoS value	0	1	2	3	4	5	6	7
DP value	0	0	0	0	0	0	0	0
Operation type	Configuration ▾							
								Apply

Figure 287.

<b>CoS value</b>	The COS value carried in the message or the default COS value assigned when entering.	
<b>IntP value</b>	The value of the drop priority (queue) to which the COS value will be mapped.	
<b>Operation type</b>	Configuration	Configure COS to drop priority value.
	Default	Restore the mapping relationship to the default state.

反馈信息窗口

```
Ingress COS-TO-Drop-Precedence map:
COS:  0  1  2  3  4  5  6  7
-----
DP:   0  0  0  0  0  0  0  0
```

Figure 288. Display the execution process and the current mapping relationship.

### 17.6.3 DSCP-to-DSCP mapping

Configure the mapping from DSCP value to DSCP value.

DSCP-to-DSCP mapping		
DSCP value1		
DSCP value2(optional)		
DSCP value3(optional)		
DSCP value4(optional)		
DSCP value5(optional)		
DSCP value6(optional)		
DSCP value7(optional)		
DSCP value8(optional)		
DSCP value		
Operation type	Configuration ▾	
		Apply

Figure 289.

<b>DSCP value1-DSCP value8 (optional)</b>	Up to eight DSCP values can be configured to the new DSCP value, among which DSCP value1 is required, DSCP value2-8 is optional, range: 0-63.	
<b>DSCP value</b>	New DSCP value, range: 0-63.	
<b>Operation type</b>	Configuration	Configure DSCP to DSCP value.
	Default	Restore the mapping relationship to the default state.

```

反馈信息窗口
Switch# config t
Switch(config)# mls qos map dscp-dscp 63 60          to 1

Ingress DSCP-TO-DSCP map:
d1 : d2  0  1  2  3  4  5  6  7  8  9
0:      0  1  2  3  4  5  6  7  8  9
1:     10 11 12 13 14 15 16 17 18 19
2:     20 21 22 23 24 25 26 27 28 29
3:     30 31 32 33 34 35 36 37 38 39
4:     40 41 42 43 44 45 46 47 48 49
5:     50 51 52 53 54 55 56 57 58 59
6:      1 61 62  1
    
```

Figure 290. Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

### 17.6.4 DSCP-to-IntP mapping

Configure the value mapped from the DSCP value to the IntP value.

DSCP-to-IntP mapping	
DSCP value1	<input type="text"/>
DSCP value2(optional)	<input type="text"/>
DSCP value3(optional)	<input type="text"/>
DSCP value4(optional)	<input type="text"/>
DSCP value5(optional)	<input type="text"/>
DSCP value6(optional)	<input type="text"/>
DSCP value7(optional)	<input type="text"/>
DSCP value8(optional)	<input type="text"/>
IntP value	<input type="text"/>
Operation type	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 291.

<b>DSCP value1-</b>	Up to eight DSCP values can be configured to the new IntP value, among which
---------------------	--

<b>DSCP value8 (optional)</b>	DSCP value1 is required, DSCP value2-8 is optional, range: 0-63.	
<b>IntP value</b>	New IntP value, range: 0-7.	
<b>Operation type</b>	Configuration	Configure DSCP to IntP value.
	Default	Restore the mapping relationship to the default state.

```

反馈信息窗口
Switch# config t
Switch(config)# mls qos map dscp-intp 60 50 31      to 2

Ingress DSCP-TO-Internal-Priority map:
d1 : d2  0  1  2  3  4  5  6  7  8  9
0:      0  0  0  0  0  0  0  0  0  0  1  1
1:      1  1  1  1  1  1  1  1  2  2  2  2
2:      2  2  2  2  2  3  3  3  3  3  3  3
3:      3  2  4  4  4  4  4  4  4  4  4  4
4:      5  5  5  5  5  5  5  5  5  5  6  6
5:      2  6  6  6  6  6  6  7  7  7  7  7
6:      2  7  7  7  7

```

Figure 292. Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

### 17.6.5 DSCP-to-DP mapping

Configure the value mapped from the DSCP value to the DP value.

DSCP-to-DP mapping	
DSCP value1	<input type="text"/>
DSCP value2(optional)	<input type="text"/>
DSCP value3(optional)	<input type="text"/>
DSCP value4(optional)	<input type="text"/>
DSCP value5(optional)	<input type="text"/>
DSCP value6(optional)	<input type="text"/>
DSCP value7(optional)	<input type="text"/>
DSCP value8(optional)	<input type="text"/>
DP value	<input type="text"/>
Operation type	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 293.

<b>DSCP value1-DSCP value8 (optional)</b>	Up to eight DSCP values can be configured to the new DP value, among which DSCP value1 is required, DSCP value2-8 is optional, range: 0-63.
---	---

<b>DP value</b>	New DP value, range: 0-2.	
<b>Operation type</b>	Configuration	Configure DSCP to DP value.
	Default	Restore the mapping relationship to the default state.

```

反馈信息窗口
Ingress DSCP-TO-Drop-Precedence map:
d1 : d2  0  1  2  3  4  5  6  7  8  9
0:      0  0  0  0  0  0  0  0  0  0
1:      0  0  0  0  0  0  0  0  0  0
2:      0  0  0  0  0  0  0  0  0  0
3:      0  0  0  0  0  0  0  0  0  0
4:      0  0  0  0  0  0  0  0  0  0
5:      0  0  0  0  0  0  0  0  0  0
6:      0  0  0  0  0  0  0  0  0  0

```

Figure 294. Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

### 17.6.6 EXP-to-IntP mapping

Configure the value mapped from EXP value to IntP.

EXP-to-IntP mapping								
EXP value	0	1	2	3	4	5	6	7
IntP value	0	1	2	3	4	5	6	7
Operation type	Configuration ▼							
								Apply

Figure 295.

<b>EXP value</b>	EXP value carried in the message, range: 0-7.	
<b>IntP value</b>	New IntP value, range: 0-7.	
<b>Operation type</b>	Configuration	Configure DSCP to IntP value.
	Default	Restore the mapping relationship to the default state.

### 17.6.7 EXP-to-DP mapping

Configure the value mapped from EXP value to DP.

EXP-to-DP mapping								
EXP value	0	1	2	3	4	5	6	7
DP value	0	0	0	0	0	0	0	0
Operation type	Configuration ▼							
								Apply

Figure 296.

<b>EXP value</b>	EXP value carried in the message, range: 0-7.	
<b>DP value</b>	New DP value, range: 0-2.	
<b>Operation type</b>	Configuration	Configure EXP to DP value.
	Default	Restore the mapping relationship to the default state.

### 17.6.8 IntP-to-DSCP mapping

Configure the value mapped from IntP value to DSCP.

IntP-to-DSCP mapping								
IntP value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56
Operation type	Configuration ▾							
								Apply

Figure 297.

<b>IntP value</b>	The value of the internal priority of the message, range: 0-7.	
<b>DSCP value</b>	New DSCP value, range: 0-63.	
<b>Operation type</b>	Configuration	Configure IntP to DSCP value.
	Default	Restore the mapping relationship to the default state.

### 17.6.9 IntP-to-EXP mapping

Configure the value mapped from IntP value to EXP.

IntP-to-EXP mapping								
IntP value	0	1	2	3	4	5	6	7
EXP value	0	1	2	3	4	5	6	7
Operation type	Configuration ▾							
								Apply

Figure 298.

<b>IntP value</b>	The value of the internal priority of the message, range: 0-7.	
<b>EXP value</b>	New EXP value, range: 0-7.	
<b>Operation type</b>	Configuration	Configure IntP to EXP value.
	Default	Restore the mapping relationship to the default state.

## 17.7 QoS aggregate policy configuration

Configure the new aggregation strategy and the information rate and burst id of the aggregation strategy.

QoS aggregate policy configuration	
Aggregate policer name	<input type="text"/>
Committed Information Rate	<input type="text"/>
policy burst id configuration:	1 <input type="button" value="v"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 299.

<b>Aggregate policer name</b>	New aggregate policer name, range: 1-64 character.	
<b>Committed Information Rate</b>	Information Rate, range: 1-10000000 kbit/s.	
<b>Policy burst id configuration</b>	Burst id configuration, range: 1-2.	
<b>Operation</b>	Add	Add aggregate policer.
	Remove	Remove aggregate policer.

```

Information feedback window
Switch# config t
Switch(config)# mls qos aggregate-policy agg1 10000 burst-group 1
    
```

Figure 300. Display the configuration process and results, no error will be reported after normal configuration.

## 17.8 QoS service policy configuration

Configure VLAN Association Policy.

QoS service policy configuration	
Policy-map name	p1 <input type="button" value="v"/>
Vlan List	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 301.

<b>Policy-map name</b>	The name of the created strategy, select by clicking the drop-down.	
<b>VLAN List</b>	VLAN ID, range: 1-4094.	
<b>Operation</b>	Add	Add VLAN-based policy.
	Remove	Remove VLAN-based policy.

```
反馈信息窗口
Switch# config t
Switch(config)# service-policy input p1 vlan 2
```

Figure 302. Display the configuration process and results, no error will be reported after normal configuration.

## 18. L3 forward configuration

### 18.1 IP route Aggregation configuration

#### 18.1.1 Route aggregate configuration

This page is used for enabled or disabled configuration of routing aggregation.

To display the “Route aggregate configuration” page, click L3 forward configuration -> IP route Aggregation configuration -> Route aggregate configuration, click “Apply” to configure.

**Enable route aggregation**

Enable route aggregation Disable ▾

Apply

Figure 303.

entry	describe
<b>Enable route aggregation</b>	Enable: Enable routing aggregation. Disable: Disable routing aggregation.

**Route aggregation status**

Route aggregation status disable

Figure 304.

entry	describe
<b>Routing aggregation state</b>	Enable: Enable routing aggregation. Disable: Disable routing aggregation.

## 18.2 ARP configuration

### 18.2.1 ARP configuration

This page is used to configure ARP static entries.

To display the “ARP configuration” page, click L3 forward configuration -> ARP configuration -> ARP configuration, click “Apply” to configure.

ARP configuration	
IP address	<input type="text"/>
MAC address	<input type="text"/>
Operation type	Add <input type="button" value="v"/>
VLAN interface	Vlan1 <input type="button" value="v"/>
Port	Ethernet1/0/1 <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 305.

<b>entry</b>	describe
<b>IP address</b>	IP address, e.g .1.1.1.1.
<b>MAC address</b>	MAC address.
<b>Operation type</b>	Add: Apply the above settings. Remove: Delete the above.
<b>VLAN interface</b>	VLAN id created.
<b>Port</b>	Ethernet port name.

### 18.2.2 Clear ARP cache

This page is used to clear ARP statistics.

To display the “Clear ARP cache” page, click L3 forward configuration -> ARP configuration -> Clear ARP cache, click “Apply” to configure.

Clear ARP cache	
<input type="button" value="Apply"/>	

Figure 306.



### 18.2.3 Show ARP

This page is used to view the information of the ARP table.

To display the “Clear ARP cache” page, click L3 forward configuration -> ARP configuration -> Clear ARP cache.

ARP list				
Binding IP	Binding MAC	Interface	Port	flag
192.168.2.74	00-0e-c6-bf-ad-7a	Vlan1	Ethernet1/0/14	dynamic
Number of ARP entry				
Number of ARP entry			1	
				Refresh

Figure 307.

## 18.3 Gratuitous arp config

### 18.3.1 gratuitous-arp interval time configuration

This page is used to configure the global free ARP send time interval.

To display the “gratuitous-arp interval time configuration” page, click L3 forward configuration -> Gratuitous arp config -> gratuitous-arp interval time configuration, click “Apply” to configure.

gratuitous-arp interval time configuration	
interval time	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 308.

entry	describe
interval time	Range: 5-1200 seconds.
Operation	Add: Apply the above settings. Remove: Recovery default interval 300 seconds.

### 18.3.2 interface gratuitous-arp interval time configuration

This page is used to set vlan interface free ARP send interval configuration.

To display the “interface gratuitous-arp interval time configuration” page, click L3 forward configuration -> Gratuitous arp config -> interface gratuitous-arp interval time configuration, click “Apply” to configure.

interface gratuitous-arp interval time configuration	
Vlan ID	1 ▾
interval time	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 309.

<b>entry</b>	describe
<b>VLAN ID</b>	Vlan ID created.
<b>interval time</b>	Range: 5-1200 seconds.
<b>Operation</b>	Add: Apply the above settings. Remove: Recovery default interval 300 seconds.

### 18.3.3 show gratuitous-arp configuration

This page is used to view ARP free configuration information.

To display the “show gratuitous-arp configuration” page, click L3 forward configuration -> Gratuitous arp config -> show gratuitous-arp configuration, click “Apply” to view.

gratuitous-arp interval time configuration	
Vlan ID	▾
<input type="button" value="Apply"/>	

```

Information feedback window
Switch# show ip gratuitous-arp
Gratuitous ARP send is Global disabled
Gratuitous ARP send enabled interface vlan information:
Name          Interval-Time(seconds)

```

Figure 310.

## 18.4 ARP protection configuration

### 18.4.1 ARP GUARD configuration

#### 18.4.1.1 ARP GUARD configuration

This page is used for ARP GUARD configuration.

To display the “ARP GUARD configuration” page, click L3 forward configuration -> ARP protection configuration -> ARP GUARD configuration -> ARP GUARD configuration, click “Apply” to configure.

ARP GUARD configuration	
Port	Ethernet1/0/1 ▾
IP address	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 311.

entry	describe
Port	Ethernet port name.
IP address	IP address, e.g .1.1.1.1.
Operation	Add: Apply the above settings. Remove: Delete the above.

## 18.4.2 ANTI-ARPSCAN configuration

### 18.4.2.1 ANTI-ARPSCAN on-off configuration

This page is used to configure the anti ARP scan function switch.

To display the “ARP GUARD configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN on-off configuration, click “Apply” to configure.

ANTI-ARPSCAN on-off configuration	
ANTI-ARPSCAN on-off status	Disable ▾
<input type="button" value="Apply"/>	

ANTI-ARPSCAN on-off status	
ANTI-ARPSCAN on-off status	Disable

Figure 312.

entry	describe
ANTI-ARPSCAN on-off status	Enable: Function Enable. Disable: Function disabled.

### 18.4.2.2 ANTI-ARPSCAN port-based threshold configuration

This page is available for port-based configuration of anti-scan ARP thresholds.

To display the “ANTI-ARPSCAN port-based threshold configuration” page, click L3 forward configuration ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN port-based threshold configuration, click “Apply” to configure.

ANTI-ARPSCAN port-based threshold configuration	
Range of threshold	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 313.

entry	describe
Range of threshold	Size range: 2-200, unit pack/s.
Operation	Configuration: Application settings. Default: Restore default 10 packs/s.

ANTI-ARPSCAN port-based threshold configuration	
Range of threshold	16

Figure 314.

entry	describe
Range of threshold	Current configured threshold, size range: 2-200, unit pack/second.

#### 18.4.2.3 ANTI-ARPSCAN IP-based threshold configuration

This page is used to configure the IP-based anti ARP scan threshold.

To display the “ANTI-ARPSCAN IP-based threshold configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN IP-based threshold configuration, click “Apply” to configure.

ANTI-ARPSCAN IP-based threshold configuration	
Range of threshold	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 315.

entry	describe
-------	----------

<b>Range of threshold</b>	Size range: 2-200, unit pack/s.
<b>Operation</b>	Configuration: Application settings. Default: Restore default 6 packs/s.

ANTI-ARPSCAN IP-based threshold configuration	
Range of threshold	8

Figure 316.

<b>entry</b>	describe
<b>Range of threshold</b>	Current configured threshold, size range: 2-200, unit pack/second.

#### 18.4.2.4 ANTI-ARPSCAN trust port configuration

This page is used to set the port to anti ARP scan trust port.

To display the “ANTI-ARPSCAN trust port configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN trust port configuration, click “Apply” to configure.

ANTI-ARPSCAN trust port configuration	
Port	Ethernet1/0/1 ▾
Port trust status	trust-port ▾
Operation	Add ▾
Apply	

Figure 317.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Port trust status</b>	trust-port: Trust port. supertrust-port: Super trust port. iptrust-port: IP trust port.
<b>Operation</b>	Add: Application settings. Remove: Delete the corresponding settings.

#### 18.4.2.5 ANTI-ARPSCAN trust IP configuration

This page can be used to prevent ARP scanning trust IP configuration.

To display the “ANTI-ARPSCAN trust IP configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN trust ip configuration, click “Apply” to configure.

ANTI-ARPSCAN trust IP configuration	
IP address	<input type="text"/>
Network mask	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 318.

entry	describe
IP address	IP address, e.g .1.1.1.1.
Network mask	Corresponding IP address mask.
Operation	Add: Application settings. Remove: Delete the corresponding settings.

#### 18.4.2.6 ANTI-ARPSCAN recovery on-off configuration

This page can be used to prevent ARP scanning automatic recovery switch configuration.

To display the “ANTI-ARPSCAN recovery on-off configuration” page, click L3 forward configuration ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN recovery on-off configuration, click “Apply” to configure.

ANTI-ARPSCAN recovery on-off configuration	
ANTI-ARPSCAN recovery on-off status	Enable <input type="button" value="v"/>
<input type="button" value="Apply"/>	

ANTI-ARPSCAN recovery on-off status	
ANTI-ARPSCAN recovery on-off status	Enable

Figure 319.

entry	describe
ANTI-ARPSCAN recovery on-off status	Enable: Enable automatic recovery function. Disable: Disable automatic recovery function.

#### 18.4.2.7 ANTI-ARPSCAN recovery time configuration

This page can be used to configure the automatic recovery time against ARP scanning.

To display the “ANTI-ARPSCAN recovery time configuration” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> ANTI-ARPSCAN recovery time configuration, click “Apply” to configure.

The figure shows two screenshots of the configuration page. The top screenshot is the initial state with empty input fields. The bottom screenshot shows the 'Recovery time' field populated with the value '300'.

Figure 320.

<b>entry</b>	describe
<b>Recovery time</b>	Size range: 5-86400 per second.
<b>Operation</b>	Configuration: Apply the above settings. Default: Recovery default auto recovery 300 seconds.

#### 18.4.2.8 Show ANTI-ARPSCAN information

This page is used to view anti ARP scan run information.

To display the “Show ANTI-ARPSCAN information” page, click L3 forward configuration -> ARP protection configuration -> ANTI-ARPSCAN configuration -> Show ANTI-ARPSCAN information, click “Apply” to view.

```

Information feedback window
Switch# show anti-arpscan
Total port: 28
Name                Port-property  beShut  shutTime(seconds)
Ethernet1/0/1       untrust       N       0
Ethernet1/0/2       untrust       N       0
Ethernet1/0/3       untrust       N       0
Ethernet1/0/4       untrust       N       0
Ethernet1/0/5       untrust       N       0
Ethernet1/0/6       untrust       N       0
Ethernet1/0/7       untrust       N       0
Ethernet1/0/8       untrust       N       0
  
```

Figure 321.

### 18.5 Show IP Traffic

This page can be used to view statistics for IP packets.

To display the “Show IP Traffic” page, click L3 forward configuration -> ARP protection configuration -> Show IP Traffic, click “Apply” to view.

```

Information feedback window
Switch# show ip traffic
IP statistics:
  Rcvd: 134947 total, 135005 local destination
        0 header errors, 0 address errors
        0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
        0 fragment rcvd, 0 fragment dropped
        0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent: 138810 generated, 0 forwarded
        0 dropped, 0 no route
ICMP statistics:
  Rcvd: 0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
  Sent: 0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
  TcpActiveOpens          6,  TcpAttemptFails          0
  TcpCurrEstab           3,  TcpEstabResets          3
  TcpInErrs              0,  TcpInSegs             135005
  TcpMaxConn             264,  TcpOutRsts             0
  TcpOutSegs            138868,  TcpPassiveOpens       1738
  TcpRetransSegs        167,  TcpRtoAlgorithm        1
  TcpRtoMax             120000,  TcpRtoMin              200
UDP statistics:
  UdpInDatagrams         0,  UdpInErrors            0
  UdpNoPorts             0,  UdpOutDatagrams        0

```

Figure 322.

## 19. Route configuration

### 19.1 Policy based routing

The directory function is to be developed.

### 19.2 Static route configuration

#### 19.2.1 Static route configuration

This page can be used for the basic configuration of static routing.

To display the “Static route configuration” page, click Route configuration -> Static route configuration -> Static route configuration, click “Apply” to configure.



Static IP route configuration	
Destination IP address	<input type="text"/>
Network mask or prefix-length	<input type="text"/>
Nextthop or Interface null0	<input type="text"/>
preference(optional)	<input type="text"/>
Operation type	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 323.

entry	describe
Destination IP address	IP address, format: 10.10.11.11.
Network mask or prefix-length	Subnet mask in the following format: 255.255.255.0; or mask length.
Nextthop or Interface null0	IP address, format: 10.10.11.11. or null0.
Preference (optional)	Range: 1-255.
Operation type	Add: Add the above settings. Remove: Delete the above.

## 20. IPv6 Route configuration

### 20.1 IPv6 configuration

#### 20.1.1 IPv6 basic configuration

This page is used to vlan the ipv6 address of the interface and the configuration of ipv6 routing.

If you want to display the "IPv6 Basic Configuration" page, click IPv6 Route configuration -> IPv6 configuration -> IPv6 basic configuration, click "Apply" to configure.

IPv6 basic configuration	
command	ipv6 address <input type="button" value="v"/>
VLAN interface	Vlan1 <input type="button" value="v"/>
IPv6 address(X:X::X:X/M)	<input type="text"/>
EUI-64	<input type="button" value="v"/>
Operation	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 324.

<b>entry</b>	describe
<b>IPv6 address</b>	Vlan interface ipv6 address configuration.
<b>VLAN interface</b>	Vlan created.
<b>IPv6 address</b>	Example: 2001:3f:ed8::99/64.
<b>EUI-64</b>	IPv6 address is automatically generated based on the eui64 interface identifier of the interface.
<b>Operation</b>	Configure: User self-configuration. Default: Restore default configuration.

IPv6 basic configuration	
command	ipv6 route ▾
IPv6 Destination address(X:X::X:X/M)	<input type="text"/>
IPv6 nexthop address(X:X::X:X)	<input type="text"/>
VLAN interface	▾
IPv6 tunnel number	<input type="text"/>
Precedence	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 325.

Note: the switch does not support ipv6 routing configuration, the configuration of this page is not effective.

### 20.1.2 IPv6 ND configuration

This page is used for settings that can be used for neighbor discovery related functions.

If you display the “IPv6 ND Configuration” page, click IPv6 Route configuration -> IPv6 configuration -> IPv6 ND Configuration, click “Apply” to configure.

IPv6 ND configuration	
command	dad attempts ▾
VLAN interface	Vlan1 ▾
IPv6 dad-attempts	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 326.

<b>entry</b>	describe
<b>Data attempts</b>	During duplicate address detection, the neighbor request message number continuously sent by the interface is set.
<b>VLAN interface</b>	Vlan created.
<b>IPv6 dad-attempts</b>	Range: 0-10.
<b>Operation</b>	Configuration: Apply the above settings. Default: Default request message number is 1.

IPv6 ND configuration	
command	ns-interval ▾
VLAN interface	Vlan1 ▾
IPv6 ns-interval	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 327.

<b>entry</b>	describe
<b>ns-interval</b>	Time interval setting for neighbor request messages.
<b>VLAN interface</b>	Vlan created.
<b>IPv6 ns-interval</b>	Size range: 1-3600, per second.
<b>Operation</b>	Configuration: Apply the above settings. Default: Default request message number is 1 second.

IPv6 ND configuration	
command	neighbor ▾
VLAN interface	Vlan1 ▾
IPv6 address	<input type="text"/>
MAC address	<input type="text"/>
Port	Ethernet1/0/1 ▾
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 328.

<b>entry</b>	describe
<b>Neighbor</b>	Set the Static Neighbor Table Item.
<b>VLAN interface</b>	Vlan created.
<b>IPv6 address</b>	Static Neighbor IPv6 Address.
<b>MAC address</b>	Static Neighbor MAC Address.
<b>Port</b>	Ethernet port name.
<b>Operation</b>	Configuration: Apply the above settings. Default: Delete the corresponding static neighbor table item.

IPv6 ND configuration	
command	clear ipv6 neighbors ▾
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 329.

<b>entry</b>	describe
<b>Clear ipv6 neighbor</b>	Clear neighbor table items, but can not delete static neighbor table items.
<b>Operation</b>	Configuration: Delete neighbor table item. Default: Delete Neighbor Table Item.

### 20.1.3 Show IPv6 neighbor

This page is used to view ipv6 neighbor information.

To display the “Show IPv6 neighbor” page, click IPv6 Route configuration -> IPv6 configuration -> Show IPv6 neighbor, click “Apply” to view.

Show IPv6 neighbor	
Parameter choose	Address ▾
IPv6 address	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 330.

<b>entry</b>	describe
--------------	----------

<b>Address</b>	Based on address.
<b>IPv6 address</b>	IPv6 address.

**Show IPv6 neighbor**

Parameter choose	Count ▾
<input type="button" value="Apply"/>	

Figure 331.

<b>entry</b>	describe
<b>Count</b>	Display counter information.

**Show IPv6 neighbor**

Parameter choose	Vlan ▾
VLAN ID	<input style="width: 90%;" type="text"/>
<input type="button" value="Apply"/>	

Figure 332.

<b>entry</b>	describe
<b>Vlan</b>	Vlan Based Interface.
<b>Vlan id</b>	Vlan id created.

**Show IPv6 neighbor**

Parameter choose	Ethernet ▾
Ethernet port	<input style="width: 90%;" type="text"/>
<input type="button" value="Apply"/>	

Figure 333.

<b>entry</b>	describe
<b>ethernet</b>	Based on Ethernet port.
<b>Ethernet port</b>	Physical Port Name.

## 20.2 Show IPv6 route

### 20.2.1 Show IPv6 route database

This page is used to view IPv6 routing table database information.

To display the “Show IPv6 route database” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 route database, click “Apply” to view.

Show IPv6 route database	
Parameter choose	destination ▾
IPv6 address	<input type="text"/>
Apply	

Figure 334.

<b>entry</b>	describe
<b>Destination</b>	Based on ipv6 address.
<b>IPv6 address</b>	IPv6 address in the routing table.

Show IPv6 route database	
Parameter choose	prefix ▾
IPv6 address(X:X::X:X/M)	<input type="text"/>
Apply	

Figure 335.

<b>entry</b>	describe
<b>Prefix</b>	Based on ipv6 address.
<b>IPv6 address</b>	IPv6 address in the routing table.

Show IPv6 route database	
Parameter choose	database ▾
Apply	

Figure 336.

<b>entry</b>	describe
--------------	----------

<b>database</b>	Routing table database information.
-----------------	-------------------------------------

### 20.2.2 Show IPv6 NSM route

This page is used to view IPv6 NSM routing table information.

To display the “Show IPv6 NSM route” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 NSM route, click “Apply” to view.

**Show IPv6 route database**

Parameter choose	<input style="width: 90%; border: none;" type="text" value="v"/>
<input type="button" value="Apply"/>	

**Information feedback window**

```

Switch# show ipv6 route database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
       > - selected route, * - FIB route, p - stale info
Timers: Uptime
C*> ::1/128 via ::, Loopback, 03:55:41 tag:0

```

Figure 337.

<b>entry</b>	describe
<b>connected</b>	IPv6 routing table information from NSM.

**Show IPv6 NSM route**

Parameter choose	<input style="width: 90%; border: none;" type="text" value="database"/>
Parameter choose	<input style="width: 90%; border: none;" type="text" value="connected"/>
<input type="button" value="Apply"/>	

**Information feedback window**

```

Switch# show ipv6 route nsm database connected
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
       > - selected route, * - FIB route, p - stale info
Timers: Uptime
C*> ::1/128 via ::, Loopback, 03:57:50 tag:0

```

Figure 338.

<b>entry</b>	describe
<b>database</b>	IPv6 Routing Table Database.

connected	Route table information.
-----------	--------------------------

### 20.2.3 Show IPv6 FIB

This page is used to view IPv6 forward information.

To display the “Show IPv6 FIB” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 FIB, click “Apply” to view.

**Show IPv6 FIB**

Parameter choose ▼

**Information feedback window**

```

Switch# show ipv6 route fib
Total IPv6 routes: 2 entries
Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
C   fe80::/64   via ::,   Vlan1   0
C   ff00::/8    via ::,   Vlan1   0

```

Figure 339.

entry	describe
Blank parameters	Forwarding Information Database.

**Show IPv6 FIB**

Parameter choose local ▼

**Information feedback window**

```

Switch# show ipv6 route fib local
Total IPv6 routes: 3 entries
::1/128   via ::,   Loopback
fe80::21f:ceff:fe10:b01a/128   via ::,   Loopback

```

Figure 340.

entry	describe
Local	Local table.



Show IPv6 FIB	
Parameter choose	vrf ▾
VRF ID(0-255)	<input type="text"/>
<input type="button" value="Apply"/>	

```

反馈信息窗口
Switch# show ipv6 route fib vrf 0 statistics
Route statistics:
Total routes are : 4 item(s)
Total unspec routes are : 0 item(s)
Total boot routes are : 2 item(s)
Total kernel routes are : 2 item(s)
Total connected routes are : 0 item(s)
Total static routes are : 0 item(s)
Total rip routes are : 0 item(s)
Total bgp routes are : 0 item(s)
Total ospf routes are : 0 item(s)
Total ospf external routes are : 0 item(s)
Total dvmrp routes are : 0 item(s)
Total unknown routes are : 0 item(s)

```

Figure 341.

<b>entry</b>	describe
<b>Vrf</b>	Virtual routing transponder.
<b>VRF ID (0-255)</b>	Virtual Route Forwarder Number.

Show IPv6 FIB	
Parameter choose	statistics ▾
<input type="button" value="Apply"/>	

```

Information feedback window
Switch# show ipv6 route fib statistics
Route statistics:
Total routes are : 4 item(s)
Total unspec routes are : 0 item(s)
Total boot routes are : 2 item(s)
Total kernel routes are : 2 item(s)
Total connected routes are : 0 item(s)
Total static routes are : 0 item(s)
Total rip routes are : 0 item(s)
Total bgp routes are : 0 item(s)
Total ospf routes are : 0 item(s)
Total ospf external routes are : 0 item(s)
Total dvmrp routes are : 0 item(s)
Total unknown routes are : 0 item(s)

```

Figure 342.

<b>entry</b>	describe
<b>statistics</b>	Routing table statistics.

## 20.2.4 Show IPv6 route statistics

This page is used to view IPv6 routing statistics.

To display the “Show IPv6 route statistics” page, click IPv6 Route configuration -> Show IPv6 route -> Show IPv6 route statistics, click “Apply” to view.

```

Information feedback window
Switch# show ipv6 route statistics
Route statistics:
Total routes are : 1 item(s)
Total default routes are : 0 item(s)
Total kernel routes are : 0 item(s)
Total connected routes are : 1 item(s)
Total static routes are : 0 item(s)
Total rip routes are : 0 item(s)
Total bgp routes are : 0 item(s)
Total ospf routes are : 0 item(s)
Total ospf intra area routes are : 0 item(s)
Total ospf inter area routes are : 0 item(s)
Total ospf nssa type 1 routes are : 0 item(s)
Total ospf nssa type 2 routes are : 0 item(s)
Total ospf external type 1 routes are : 0 item(s)
Total ospf external type 2 routes are : 0 item(s)

```

Figure 343.

Note: the corresponding function of parameter vrf has not been realized.

## 21. DCSCM configuration

### 21.1 DCSCM Source-control enable/disable configuration

Configure Dcscm multicast source control configuration and view the configuration status.

Figure 344.

<b>Dcscm Source-control enable/disable configuration</b>	Enable	Enable dcscm multicast source control configuration.
	Disable	Disable dcscm multicast source control configuration.

DCSCM Source-control state	
DCSCM Source-control state	Disable

Figure 345. Display the current configuration status.

## 21.2 DCSCM destination-control enable/disable configuration

Configure Dcscm multicast destination control configuration and view configuration status.

DCSCM destination-control enable/disable configuration	
DCSCM destination-control enable/disable configuration	Enable ▾
Apply	

Figure 346.

<b>Dcscm destination-control enable/disable configuration</b>	Enable	Enable dcscm multicast destination control configuration.
	Disable	Disable dcscm multicast destination control configuration.

DCSCM destination-control enable/disable state	
DCSCM destination-control enable/disable state	Disable

Figure 347. Display the current configuration status.

## 21.3 DCSCM Source-control access-group configuration

Configure Dcscm multicast source control list configuration and view the configuration status of the configuration list.

DCSCM Source-control access-group configuration	
Port	Ethernet1/0/1 ▾
DCSCM Source-control access-group number	
Operation	Add ▾
Apply	

Figure 348.

<b>Port</b>	Port name	
<b>DCSCM destination-control access-group number</b>	Match the multicast data message imported from the interface according to the configured source control list number. The source control list number is derived from the ACL multicast source control configuration of ACL multicast control, range: 5000-5099.	
<b>Operation</b>	Add	Add source control list number under port.
	Remove	Delete the source control list from the port.

DCSCM Source-control access-group	
Port	DCSCM Source-control access-group number
Ethernet1/0/1	5000

Figure 349. Display the currently configured port and the corresponding source control list number (there is no port configured by default).

## 21.4 DCSCM destination-control access-group configuration

Configure Dcscm multicast destination control list configuration and view configuration list configuration status.

DCSCM destination-control access-group configuration	
Port	Ethernet1/0/1 <input type="button" value="v"/>
DCSCM destination-control access-group number	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 350.

<b>Port</b>	Port name	
<b>DCSCM destination-control access-group number</b>	Match the multicast data message imported from the interface according to the configured destination control list number. The destination control list number is derived from the ACL multicast destination control configuration of ACL multicast control, range: 6000-7999.	
<b>Operation</b>	Add	Add the destination control list number under the port.
	Remove	Delete the destination control list from the port.

DCSCM destination-control access-group	
Port	DCSCM destination-control access-group number
Ethernet1/0/1	6000

Figure 351. Display the currently configured port and the corresponding destination control list number (there is no port configured by default).

## 21.5 DCSCM destination-control access-group configuration

### (sip)

Configure the IP-based Dcscm port multicast destination control list configuration and view the configuration list configuration status.

DCSCM destination-control access-group configuration(sip)	
DCSCM destination-control IP-address/mask	
DCSCM destination-control access-group number	
Operation	Add ▼
<input type="button" value="Apply"/>	

Figure 352.

<b>DCSCM destination-control IP-address/mask</b>	Determine the members of the multicast group according to the specified network end and mask. When the multicast group member matches the control list number, the interface can be added, otherwise the interface is not added.	
<b>DCSCM destination-control access-group number</b>	Match the multicast data message imported from the specified network according to the configured destination control list number. The destination control list number is configured from the ACL multicast destination control configuration of ACL multicast control, range: 6000-7999.	
<b>Operation</b>	Add	Add the destination control list number under the designated network terminal.
	Remove	Delete the destination control list from the specified network segment.

DCSCM destination-control access-group(sip)	
DCSCM destination-control IP-address/mask	DCSCM destination-control access-group number
10.0.0.0/24	6000

Figure 353.

Display the current configured destination IP address and the corresponding destination control list number (there is no configured port by default).

## 21.6 DCSCM destination-control access-group configuration (vMAC)

Configure VLAN-MAC based Dcscm multicast source control list configuration and view the configuration list configuration status.

DCSCM destination-control access-group configuration(vMAC)	
VLAN interface	Vlan1 ▼
MAC address	
DCSCM destination-control access-group number	
Operation	Add ▼
<input type="button" value="Apply"/>	

Figure 354.

<b>VLAN interface</b>	VLAN interface.	
<b>MAC address</b>	Transmit the source MAC address of IGMP-REPORT, the format is “xx-xx-xx-xx-xx-xx”.	
<b>DCSCM destination-control access-group number</b>	Match the multicast data message imported from the interface according to the configured destination control list number. The destination control list number is derived from the ACL multicast destination control configuration of ACL multicast control, range: 6000-7999.	
<b>Operation</b>	Add	Add the destination control list number to the host corresponding to the MAC address in the VLAN.
	Remove	Delete the destination control list from the corresponding MAC address host under the VLAN.

DCSCM destination-control access-group(vMAC)		
VLAN interface	MAC address	DCSCM destination-control access-group number
1	01-00-22-33-44-55	6000

Figure 355. Display the mac host and the corresponding destination control list number under the currently configured vlan (there is no configured port by default).

## 21.7 Multicast policy configuration

Configure multicast policy and view configuration status.

Multicast policy configuration	
Source IP-address/mask	<input type="text"/>
Destination IP-address/mask	<input type="text"/>
DCSCM priority	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 356.

<b>Source IP-address/mask</b>	The source IP address range of multicast data packets, format: 192.168.2.0/24.	
<b>Destination address/mask</b>	<b>IP-</b>	The destination IP address range of multicast data packets, format: 224.0.0.0/8.
<b>DCSCM priority</b>	Specify priority, range: 0-7.	
<b>Operation</b>	Add	Configure the switch matching priority of multicast data packets in a specified range to be modified to a specified value, and TOS is also specified to the same value.
	Remove	Delete the priority policy of multicast data in the specified

	range.
--	--------

```

Multicast policy
ip multicast-policy 192.168.2.0/24 224.168.2.0/24 cos 1

```

Figure 357. Display the currently configured multicast policy.

## 21.8 ACL multicast source control

Configure ACL access rules and view the configuration status of the configuration list.

ACL multicast source control	
ACL number	<input type="text"/>
Rule	permit <input type="button" value="v"/>
Source address type	Any IP <input type="button" value="v"/>
Multicast source address	<input type="text"/>
Multicast source wildcard	<input type="text"/>
Source address type	Any IP <input type="button" value="v"/>
Multicast destination address	<input type="text"/>
Multicast destination wildcard	<input type="text"/>
Operation type	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 358.

<b>ACL number</b>	ACL number, range: 5000-5099.	
<b>Rule</b>	permit	Allow the following rules to pass.
	deny	Reject the following rules to pass.
<b>Source address type</b>	Specified address	An address range determined by IP addresses and address wildcards.
	Any IP	Any host address.
	Host Address	A specified address (set in the multicast source/destination IP address).
<b>Multicast source/destination address</b>	The address type is the host address and the IP address set when specifying the address, for example: 10.1.1.0 or 192.168.5.1.	
<b>Multicast source/destination wildcard</b>	The address type is the wildcard set when specifying the address, for example: 0.0.0.255.	
<b>Operation type</b>	Add	Add the set rules to the ACL number, and other functions use the source control list number to use these rules.

	Remove	Delete the rule of ACL number.
--	--------	--------------------------------

ACL multicast destination control	
ACL number	<input type="text"/>
Rule	permit ▾
Source address type	Any IP ▾
Multicast source address	<input type="text"/>
Multicast source wildcard	<input type="text"/>
Source address type	Any IP ▾
Multicast destination address	<input type="text"/>
Multicast destination wildcard	<input type="text"/>
Operation type	Add ▾
<input type="button" value="Apply"/>	

Figure 359.

<b>ACL number</b>	ACL number, range: 5000-5099.	
<b>Rule</b>	permit	Allow the following rules to pass.
	deny	Reject the following rules to pass.
<b>Source address type</b>	Specified address	An address range determined by IP addresses and address wildcards.
	Any IP	Any host address.
	Host Address	A specified address (set in the multicast source/destination IP address).
<b>Multicast source/destination address</b>	The address type is the host address and the IP address set when specifying the address, for example: 10.1.1.0 or 192.168.5.1.	
<b>Multicast source/destination wildcard</b>	The address type is the wildcard set when specifying the address, for example: 0.0.0.255.	
<b>Operation type</b>	Add	Add the set rules to the ACL number, and other functions use the source control list number to use these rules.
	Remove	Delete the rule of ACL number.

```

Information feedback window
Switch# show ip multicast source-control access-list
access-list 5000 permit ip any-source any-destination
access-list 5093 permit ip any-source any-destination
Switch# show ip multicast destination-control access-list
access-list 6000 permit ip any-source any-destination

```



Figure 360. Display the currently configured multicast source control list number and multicast destination control list number rules.

## 22. Spanning-tree configuration

### 22.1 Spanning-tree field configuration

#### 22.1.1 Instance configuration

This page can be used to configure the mapping relationship between the spanning tree instance and the VLAN.

To display the “Instance configuration” page, click Spanning-tree configuration -> Spanning-tree field configuration -> Instance configuration, click “Apply” to configure.

Instance configuration	
Instance name	<input type="text"/>
VLAN name	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 361.

<b>entry</b>	describe
<b>Instance name</b>	Generating tree instance ID, range 0-64.
<b>VLAN name</b>	VLAN ID, range: 1-4094.
<b>Operation</b>	Add: Add the above configuration information. Remove: Delete the above configuration information.

Instance configuration	
Instance name	VLAN name
0	1-4094

Figure 362.

<b>entry</b>	describe
<b>Instance name</b>	Generating tree instance ID, size range 0-64.
<b>VLAN name</b>	VLAN ID, range: 1-4094.

### 22.1.2 Field name configuration

This page can be used to configure MSTP domain name.

To display the "Instance configuration" page, click Spanning-tree configuration -> Spanning-tree field configuration -> Field name configuration, click "Apply" to configure.

Field name configuration	
Field name	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Field name	
Field name	name

Figure 363.

<b>entry</b>	describe
<b>Field name</b>	MSTP domain name, the length is 1-32 characters.
<b>Operation</b>	Configuration: Use the above configuration. Default: Default does not match domain name.

### 22.1.3 Revision-level configuration

This page can be used to configure MSTP revision level.

To display the "Instance configuration" page, click Spanning-tree configuration -> Spanning-tree field configuration -> Revision-level configuration, click "Apply" to configure.

Revision-level configuration	
Revision-level	<input type="text"/>
Operation	Default ▾
<input type="button" value="Apply"/>	

Figure 364.

<b>entry</b>	describe
<b>Revision-level</b>	Range :0-65535.
<b>Operation</b>	Configuration: Use the above configuration. Default: Restore default configuration 0.

Revision-level	
Revision-level	0

Figure 365.

<b>entry</b>	describe
<b>Revision-level</b>	MSTP revision level with configuration, size range: 0-65535.

## 22.2 Spanning-tree Port configuration

### 22.2.1 PortFast configuration

This page can be used for the configuration of edge ports.

To display the "PortFast configuration" page, click Spanning-tree configuration -> Spanning-tree Port configuration -> PortFast configuration, click "Apply" to configure.

PortFast configuration	
Port	Ethernet1/0/1 ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Figure 366.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Operation</b>	Add: Configure the above port type to an edge port. Remove: Configure the above port type to be a non-edge port.

PortFast configuration	
Port	PortType(1/0)
Ethernet1/0/1	0
Ethernet1/0/2	0
Ethernet1/0/3	0
Ethernet1/0/4	0
Ethernet1/0/5	0
Ethernet1/0/6	0
Ethernet1/0/7	0
Ethernet1/0/8	0

Figure 367.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>PortType(1/0)</b>	1: Represents an edge port. 0: Represents a non-edge port.

### 22.2.2 Port priority configuration

This page can be used for configuration of instance port priority.

To display the "PortFast configuration" page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Port priority configuration, click "Apply" to configure.

Port priority configuration	
Port	Ethernet1/0/1 <input type="button" value="v"/>
Instance name	<input type="text"/>
Priority	<input type="text"/>
Operation	Default <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 368.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Instance name</b>	Generate tree instance name.
<b>Priority</b>	The size range is: 0-240, multiple of 16.
<b>Operation</b>	Configuration: Apply the above configuration.

	Default: Restore default priority 32768.
--	--

<b>Port priority configuration</b>	
Ethernet1/0/1 of Instance 0	Operation port path cost 20000, Port priority 32, Port Identifier 032.001

Figure 369.

### 22.2.3 Port cost configuration

This page can be used to configure port path costs.

To display the “Port cost configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Port cost configuration, click “Apply” to configure.

Port cost configuration	
Port	Ethernet1/0/1 ▾
Instance name	
Cost	
Operation	Default ▾
<input type="button" value="Apply"/>	

Figure 370.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Instance name</b>	Generate tree instance name.
<b>Cost</b>	Size range: 0-2000000000.
<b>Operation</b>	Configuration: Apply the above configuration. Default: Recovery port default path cost.

### 22.2.4 Spanning-tree port mode

This page can be used to configure the spanning tree running mode where the port is located.

To display the “Spanning-tree port mode” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Spanning-tree port mode, click “Apply” to configure.

Spanning-tree port mode	
Port	Ethernet1/0/1 ▾
<input type="button" value="Apply"/>	

Figure 371.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.

### 22.2.5 Link-type configuration

This page can be used to configure port link types.

To display the “Link-type configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Link-type configuration, click “Apply” to configure.

Link-type configuration	
Port	Ethernet1/0/1 ▾
Link type	auto ▾
Operation	Default ▾
<input type="button" value="Apply"/>	

Figure 372.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Link type</b>	Auto: Automatic consultations. Force-true: Point-to-point type. Force-false: Non-point-to-point type.
<b>Operation</b>	Configuration: Apply the above configuration. Default: Auto is the default link type for the recovery port.

Link-type configuration	
Port	Link type
Ethernet1/0/1	auto
Ethernet1/0/2	auto
Ethernet1/0/3	auto
Ethernet1/0/4	auto
Ethernet1/0/5	auto
Ethernet1/0/6	auto
Ethernet1/0/7	auto
Ethernet1/0/8	auto

Figure 373.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Link type</b>	Auto: Automatic consultations. Force-true: Point-to-point type. Force-false: Non-point-to-point type.

### 22.2.6 Spanning-tree agreement port configuration

This page can be used to configure enable or disable the tree generation function under the port.

To display the “Spanning-tree agreement port configuration” page, click Spanning-tree configuration -> Spanning-tree Port configuration -> Spanning-tree agreement port configuration, click “Apply” to configure.

Figure 374.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>Operation</b>	Enable: Port enable spanning tree function. Disable: Port disables spanning tree functionality.

## 22.3 Spanning-tree global configuration

### 22.3.1 Spanning-tree global agreement port configuration

This page uses the build tree function with global enable.

To display the “Spanning-tree global agreement port configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning-tree global agreement port configuration, click “Apply” to configure.

Figure 375.

<b>entry</b>	describe
--------------	----------

<b>Operation</b>	Enable: enable spanning tree function. Disable: disable spanning tree functionality.
------------------	---

### 22.3.2 Forward-time configuration

This page can be used to configure forwarding delay time.

To display the "Forward-time configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Forward-time configuration, click "Apply" to configure.

Forward-time configuration	
Forward-time	<input type="text"/>
Operation	Default <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 376.

entry	describe
<b>Forward-time</b>	Size range: 4-30, in seconds, the following conditions shall be met: $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$ .
<b>Operation</b>	Configuration: Configure the above settings. Default: Restore default 15s.

Forward-time configuration	
Forward-time configuration	15

Figure 377.

entry	describe
<b>Forward-time configuration</b>	Configuration of current forwarding delay time.

### 22.3.3 Hello-time configuration

This page can be used to bpdu the configuration of the sending interval.

To display the "Hello-time configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Hello-time configuration, click "Apply" to configure.



Hello-time configuration	
Bridge hello time	<input type="text"/>
Operation	Default <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 378.

entry	describe
Bridge hello time	Size range: 1-10, in seconds, the following conditions shall be met: $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$ .
Operation	Configuration: Configure the above settings. Default: Restore default 2s.

Hello-time configuration	
Bridge hello time	2

Figure 379.

entry	describe
Bridge hello time	Current HELLO Maximum Survival Time Configuration.

### 22.3.4 Max age time configuration

This page can be used to configure the maximum aging time of BPDU messages.

To display the "Max age time configuration" page, click Spanning-tree configuration -> Spanning-tree global configuration -> Max age time configuration, click "Apply" to configure.

Max age time configuration	
Max age time	<input type="text"/>
Operation	Default <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 380.

entry	describe
-------	----------

<b>Max age time</b>	Size range: :6-40, in seconds, the following conditions shall be met: $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$ .
<b>Operation</b>	Configuration: Configure the above settings. Default: Restore default 20s.

Max age time configuration	
Max age time	20

Figure 381.

<b>entry</b>	describe
<b>Max age time</b>	Configuration of current maximum aging time.

### 22.3.5 Max hop time configuration

This page can be used to BPDU the maximum number of hops that packets are forwarded in the spanning tree domain.

To display the “Max hop time configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Max hop time configuration, click “Apply” to configure.

Max hop time configuration	
Max hop time	<input type="text"/>
Operation	Default <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 382.

<b>entry</b>	describe
<b>Max hop time</b>	Numerical range: 1-40.
<b>Operation</b>	Configuration: Configure the above settings. Default: Restore default 20s.

Max hop time configuration	
Max hop time	20

Figure 383.

<b>entry</b>	describe
<b>Max hop time</b>	Maximum number of hops currently configured.

### 22.3.6 Spanning tree mode configuration

This page is used to set the running mode of the switch spanning tree.

To display the “Spanning tree mode configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning tree mode configuration, click “Apply” to configure.

Spanning tree mode configuration	
Mode	Mstp ▾
Operation	Default ▾
Apply	

Figure 384.

<b>entry</b>	describe
<b>Mode</b>	Generating tree protocol type: Mstp.Stp.Rstp
<b>Operation</b>	Configuration: Configure the above settings. Default: Restore default configuration mode to mstp.

Spanning tree mode configuration	
Mode	mstp

Figure 385.

<b>entry</b>	describe
<b>Mode</b>	Current run spanning tree protocol type.

### 22.3.7 Spanning tree cost-format configuration

This page is used to set the global configuration path cost format.

To display the “Spanning tree cost-format configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Spanning tree cost-format configuration, click “Apply” to configure.

Spanning tree cost-format configuration	
Mode	dot1t ▾
Apply	

Figure 386.

<b>entry</b>	describe
<b>Mode</b>	Path cost format: Dot1t.Dot1d.

### 22.3.8 Priority configuration

This page is used to set the bridge priority of the spanning tree instance.

To display the “Priority configuration” page, click Spanning-tree configuration -> Spanning-tree global configuration -> Priority configuration, click “Apply” to configure.

Figure 387.

<b>entry</b>	describe
<b>Instance name</b>	Generate tree instance name.
<b>Priority</b>	Numerical range: 0-61440, and an integer multiple of 4096.
<b>Operation</b>	Configuration: Configure the above settings. Default: Restore default configuration priority 32768.

## 22.4 Show spanning-tree

### 22.4.1 Instance information

This page can be used to view information for the specified instance.

To display the “Instance information” page, click Spanning-tree configuration -> Show spanning-tree -> Instance information, click “Apply” to view.

Figure 388.

entry	describe
Instance name	Generate tree instance name.

```

Information feedback window
Switch# show spanning-tree mst 0 detail
***** Process 0 *****
##### Instance 0 #####
vlans mapped: 1-4094
Root Id      : this switch
Root Times   : Max Age 20, Hello Time 2, Forward Delay 15, Max hops 20
Port 14 (Ethernet1/0/14) of Instance 0 is DSGN forwarding
Port info:   port id 128.14 priority 128 cost 0
Designated root has priority 32768, address 001f.ce10.b01b
Designated bridge has priority 32768, address 001f.ce10.b01b
BPDU: sent   2348(TCN 0, CONFIG 0, MST 2348)
      received 0(TCN 0, CONFIG 0, MST 0)

```

Figure 389.

## 22.4.2 Revision-Level information

This page can be used to view configuration information for the spanning tree domain.

To display the “Revision-Level information” page, click Spanning-tree configuration -> Show spanning-tree -> Revision-Level information, click “Apply” to view.

```

Information feedback window
Switch# show spanning-tree mst config
Name          name
Revision      0
Instance      Vlans Mapped
-----
00            1-4094
-----

```

Figure 390.

## 23. MRPP configuration

### 23.1 MRPP global configuration

#### 23.1.1 MRPP global switch configuration

This page is used to enable or disable MRPP protocols.

To display the “MRPP global switch configuration” page, click MRPP configuration -> MRPP global configuration -> MRPP global switch configuration, click “Apply” to configure.

MRPP global switch configuration	
Operation	Disable ▾
Apply	

Figure 391.

entry	describe
Operation	Enable: Enable MRPP protocol functionality. Disable: Close MRPP Protocol Function.

MRPP global switch configuration	
MRPP global configuration	disable

Figure 392.

entry	describe
MRPP global configuration	Disable: Current mrpp protocol status is closed. Enable: Current mrpp protocol status opens.

### 23.1.2 MRPP poll time configuration

This page can be used to configure MRPP query time.

To display the “MRPP poll time configuration” page, click MRPP configuration -> MRPP global configuration -> MRPP poll time configuration, click “Apply” to configure.

MRPP poll time configuration	
MRPP poll time	
Operation	Default ▾
Apply	

Figure 393.

entry	describe
MRPP poll time	Range: 20-200, unit milliseconds.
Operation	Configuration: Apply the above settings. Default: Restore default ms 100.

MRPP poll time configuration	
MRPP poll time	100

Figure 394.

entry	describe
MRPP poll time	Current configured query time.

### 23.1.3 MRPP domain id configuration

This page is used to set the ID number of the MRPP domain.

To display the “MRPP domain id configuration” page, click MRPP configuration -> MRPP global configuration -> MRPP domain id configuration, click “Apply” to configure.

MRPP domain id configuration	
MRPP domain	<input type="text"/>
Operation	Remove <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 395.

entry	describe
MRPP domain	ID range: 1-4096.
Operation	Configuration: Apply the above settings. Default: Delete configured domain ID.

MRPP domain id configuration	
Index	Domain ID

Figure 396.

entry	describe
Domain ID	Domain ID range: 1-4096.

## 23.2 MRPP port configuration

### 23.2.1 MRPP port property configuration

This page can be used to configure the primary and secondary ports of the MRPP ring.

To display the “MRPP port property configuration” page, click MRPP configuration -> MRPP port configuration -> MRPP port property configuration, click “Apply” to configure.

MRPP port property configuration	
Port	Ethernet1/0/1 ▾
MRPP domain	
MRPP port property	primary ▾
Operation	Remove ▾
Apply	

Figure 397.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>MRPP domain</b>	MRPP domain ID, range: 1-4096.
<b>MRPP port property</b>	Primary: Main port. Secondary: Secondary port.
<b>Operation</b>	Add: Apply the above configuration. Remove: Delete the above configuration.

MRPP port property configuration			
Index	Domain ID	Port Name	Property

Figure 398.

<b>entry</b>	describe
<b>Domain ID</b>	MRPP domain ID, range: 1-4096.
<b>Port Name</b>	Ethernet port.
<b>Property</b>	Primary: Main port. Secondary: Secondary port.

## 23.3 MRPP domain configuration

### 23.3.1 MRPP control vlan config

This page can be used to configure control VLAN for MRPP rings.

To display the “MRPP control vlan configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP control vlan configuration, click “Apply” to configure.



MRPP control vlan config	
MRPP domain	▼
VLAN ID	
Operation	Remove ▼
Apply	

Figure 399.

entry	describe
MRPP domain	MRPP domain ID, range created: 1-4096.
VLAN ID	VLAN ID, range: 1-4094.
Operation	Configuration: Apply the above configuration. Remove: Delete the above configuration.

MRPP control vlan config		
Index	Domain ID	Control-VLAN

Figure 400.

entry	describe
Domain ID	MRPP domain ID, range: 1-4096.
Operation	Scope of control VLAN, for current MRPP domain configuration: 1-4094.

### 23.3.2 MRPP node mode config

This page can be used to configure MRPP nodes.

To display the “MRPP node mode configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP node mode configuration, click “Apply” to configure.

MRPP node mode config	
MRPP domain	▼
MRPP node mode	master ▼
Apply	

Figure 401.

entry	describe
-------	----------

<b>MRPP domain</b>	MRPP domain ID, range: 1-4096.
<b>MRPP node mode</b>	Master: Master node. Transit: Transmission node.

MRPP node mode config		
Index	Domain ID	Node mode

Figure 402.

<b>entry</b>	describe
<b>Domain ID</b>	MRPP domain ID, range: 1-4096.
<b>Node mode</b>	Master: Master node. Transit: Transmission node.

### 23.3.3 MRPP hello timer config

This page can be used to MRPP Hello the configuration of message sending intervals.

To display the “MRPP hello timer configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP hello timer configuration, click “Apply” to configure.

MRPP hello timer config	
MRPP domain	<input type="text" value="v"/>
MRPP hello timer range	<input type="text"/>
Operation	Remove <input type="text" value="v"/>
<input type="button" value="Apply"/>	

Figure 403.

<b>entry</b>	describe
<b>MRPP domain</b>	MRPP domain ID, range: 1-4096.
<b>MRPP hello timer range</b>	Interval time range: 1-100 seconds.
<b>Operation</b>	Configuration: Apply the above configuration. Remove: Delete the above configuration and restore the default configuration to 1 second.

MRPP hello timer config		
Index	Domain ID	Hello-Timer

Figure 404.

<b>entry</b>	describe
<b>Domain ID</b>	MRPP domain ID, range: 1-4096.
<b>Hello-Timer</b>	Hello message sending interval when the current configuration takes effect.

### 23.3.4 MRPP fail timer config

This page is used MRPP configure the health message receive timeout.

To display the “MRPP fail timer configuration” page, click MRPP configuration -> MRPP domain configuration -> MRPP fail timer configuration, click “Apply” to configure.

Figure 405.

<b>entry</b>	describe
<b>MRPP domain</b>	MRPP domain ID, range: 1-4096.
<b>MRPP fail timer range</b>	Interval time range: 1-300 seconds.
<b>Operation</b>	Configuration: Apply the above configuration. Remove: Delete the above configuration and restore the default configuration to 3 second.

Figure 406.

<b>entry</b>	describe
<b>Domain ID</b>	MRPP domain ID, range: 1-4096.
<b>FAIL-Timer</b>	Receive timeout when the current configuration takes effect.

### 23.3.5 MRPP domain switch config

This page can be used to enable or disable MRPP rings.

To display the “MRPP domain switch config” page, click MRPP configuration -> MRPP domain configuration -> MRPP domain switch config, click “Apply” to configure.

MRPP domain switch config	
MRPP domain	▼
Operation	Disable ▼
Apply	

Figure 407.

entry	describe
MRPP domain	MRPP domain ID, range: 1-4096.
Operation	Enable: Enable the corresponding MRPP ring. Disable: Disable the corresponding MRPP ring.

MRPP domain switch configuration		
Index	Domain ID	Flag

Figure 408.

entry	describe
Domain ID	MRPP domain ID, range: 1-4096.
Flag	The enable state disable or enable of the currently configured active MRPP domain.

## 23.4 MRPP configuration display

### 23.4.1 MRPP display

This page can be used to view configuration information for MRPP domains.

To display the “MRPP display” page, click MRPP configuration -> MRPP domain configuration -> MRPP display, click “Apply” to view.

MRPP display	
MRPP domain	all ▾
Apply	

Information feedback window
Switch# show mrpp
Poll time : 100 (ms)

Figure 409.

entry	describe
Domain ID	MRPP domain ID, range: 1-4096.

### 23.4.2 MRPP statistics display

This page can be used to view statistics of MRPP domain data and status changes.

To display the “MRPP statistics display” page, click MRPP configuration -> MRPP domain configuration -> MRPP statistics display, click “Apply” to view.

MRPP statistics display	
MRPP domain	all ▾
Apply	

Information feedback window
Switch# show mrpp statistics
Poll time : 100 (ms)

Figure 410.

entry	describe
Domain ID	MRPP domain ID, range: 1-4096.

### 23.4.3 Clear MRPP statistics

This page can be used to clear statistics for MRPP domains.

To display the “Clear MRPP statistics” page, click MRPP configuration -> MRPP domain configuration -> Clear MRPP statistics, click “Apply” to configure.

Clear MRPP statistics	
MRPP domain	all ▾
Apply	

Figure 411.

## 24. ULPP configuration

### 24.1 ULPP global configuration

#### 24.1.1 ULPP group configuration

This page can be used to add or delete ULPP groups.

To display the “ULPP group configuration” page, ULPP configuration -> ULPP global configuration -> ULPP group configuration, click “Apply” to configure.

ULPP group configuration	
ULPP group	
Operation	Add ▾
Apply	

Figure 412.

<b>entry</b>	describe
<b>ULPP group</b>	Group ID size range: 1-48.
<b>Operation</b>	Add: Add ULPP groups. Remove: Delete ULPP groups.

ULPP group configuration	
ULPP group	1

Figure 413.

<b>entry</b>	describe
<b>ULPP group</b>	ULPP groups created.

## 24.2 ULPP port configuration

### 24.2.1 ULPP port property configuration

This page can be used to set the port as the master-slave port of the ulpp group. It can also enable or disable receiving MAC address and ARP update packets, can also configure a control VLAN for the port.

To display the “ULPP port property configuration” page, ULPP configuration -> ULPP port configuration -> ULPP port property configuration, click “Apply” to configure.

ULPP port property configuration	
Port	Ethernet1/0/1 ▾
ULPP port flush mode	mac ▾ <input type="checkbox"/>
ULPP port control vlan	<input type="text"/> <input type="checkbox"/>
ULPP group	1 ▾
ULPP port mode	master ▾ <input type="checkbox"/>
Operation	Remove ▾
<input type="button" value="Apply"/>	

Figure 414.

entry	describe
Port	Ethernet port name.
ULPP port flush mode	Mac: Receive mac update packets. Arp: Receive arp more packets.
ULPP port control vlan	Vlan created.
ULPP group	ULPP groups created.
ULPP port mode	Master: Main port. Slave: Slave port.
Operation	Configuration: Apply the above configuration. Remove: Delete the above configuration.

## 24.3 ULPP group configuration

### 24.3.1 ULPP group description configuration

This page can be used to configure the description name for ULPP group.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP group configuration -> ULPP group description configuration, click “Apply” to configure.

ULPP group description configuration	
ULPP group	1 ▾
ULPP group description	
Operation	Remove ▾
<input type="button" value="Apply"/>	

Figure 415.

<b>entry</b>	describe
<b>ULPP group</b>	ULPP groups created.
<b>ULPP group description</b>	1-128 characters in length.
<b>Operation</b>	Configuration: Apply the above configuration. Remove: Delete the above configuration.

ULPP group description configuration	
ULPP group	ULPP group description
1	

Figure 416.

<b>entry</b>	describe
<b>ULPP group</b>	ULPP groups created.
<b>ULPP group description</b>	Description of ULPP groups currently set.

### 24.3.2 ULPP group property configuration

This page can be used to configure the ulpp group properties of preemption mode, preemption delay, protection VLAN, control VLAN, flush mode, etc.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP group configuration -> ULPP group property configuration, click “Apply” to configure.



ULPP group property configuration		
ULPP group	1 ▾	
ULPP group preemption mode	on ▾	<input type="checkbox"/>
ULPP group preemption delay		<input type="checkbox"/>
ULPP group control vlan		<input type="checkbox"/>
ULPP group protect vlan		<input type="checkbox"/>
ULPP group flush mode	mac ▾	<input type="checkbox"/>
Operation	Remove ▾	
		Apply

Figure 417.

entry	describe
<b>ULPP group</b>	ULPP groups created.
<b>ULPP group preemption mode</b>	On: Preemptive mode enabled. Off: Disable Preemptive Mode.
<b>ULPP group preemption delay</b>	Delay time range: 1-600, per second.
<b>ULPP group control vlan</b>	Created VLAN, VLAN ID between 1-4094.
<b>ULPP group protect vlan</b>	MSTP instance list, value range: 1-4094.
<b>ULPP group flush mode</b>	Mac: Send mac update packet. Arp: Send arp update packet.
<b>Operation</b>	Configuration: Apply the above configuration. Remove: Delete the above configuration.

ULPP group property configuration				
ULPP group	ULPP group preemption mode	ULPP group preemption delay	ULPP group control vlan	ULPP group flush mode
1	OFF	30	1	ALL

Figure 418.

entry	describe
<b>ULPP group</b>	ULPP group created.
<b>ULPP group preemption mode</b>	On: Preemptive mode enabled. Off: Disable Preemptive Mode.

<b>ULPP group preemption delay</b>	Delay time for current configuration.
<b>ULPP group control vlan</b>	ULPP group control VLAN currently set.
<b>ULPP group protect vlan</b>	MSTP instance list, value range: 1-4094.
<b>ULPP group flush mode</b>	Mac: Send mac update packet. Arp: Send arp update packet. ALL: Send mac and arp update packet.

## 24.4 ULPP configuration display

### 24.4.1 ULPP group configuration display

This page can be used to view configuration information for ULPP groups.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP group configuration display, click “Apply” to view.

**ULPP group configuration display**

ULPP group  all

---

**Information feedback window**

```
Switch# show ulpp group
ULPP group 1 information:
Description:
Preemption mode: OFF
Preemption delay: 30s
Control VLAN: 1
Flush packet: MAC ARP
Protected VLAN: Reference Instance
Member      Role      State      Track-cfm-level
-----
-----
```

Figure 419.

### 24.4.2 ULPP port statistics display

This page can be used to view ULPP port statistics.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP port statistics display, click “Apply” to view.

**ULPP port statistics display**

Port  Ethernet1/0/1

Figure 420.

### 24.4.3 ULPP port property display

This page can be used to view ULPP port configuration information.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP port property display, click “Apply” to view.

```

Information feedback window
Switch# show ulpp flush-receive-port
ULPP flush-receive portlist:
Portname          Type          Control Vlan
-----

```

Figure 421.

### 24.4.4 ULPP port statistics clear

This page can be used to clear statistics of ULPP related data on the port.

To display the “ULPP group description configuration” page, ULPP configuration -> ULPP configuration display -> ULPP port statistics clear, click “Apply” to view.

**ULPP port statistics clear**

Port  ▼

Figure 422.

## 25. ULSM configuration

### 25.1 ULSM global configuration

#### 25.1.1 ULSM group configuration

This page can be used to create or delete ULSM groups.

To display the “ULSM group configuration” page, click ULSM configuration -> ULSM global configuration -> ULSM group configuration, click “Apply” to configure.

**ULSM group configuration**

ULSM group

Operation  ▼

Figure 423.

<b>entry</b>	describe
<b>ULSM group</b>	Group ID range: 1-32.
<b>Operation</b>	Add: Create a ULSM group.

	Remove: Removing ULSM groups of corresponding ID.
--	---

ULSM group configuration	
ULSM group	1

Figure 424.

entry	describe
ULSM group	ULSM groups created.

## 25.2 ULSM port configuration

### 25.2.1 ULSM port property configuration

This page can be used to add uplink or downlink ports for ULSM groups that have been created.

To display the “ULSM group configuration” page, click ULSM configuration -> ULSM port configuration -> ULSM port property configuration, click “Apply” to configure.

ULSM port property configuration	
Port	Ethernet1/0/1 ▾
ULSM group	1 ▾
ULSM port property	downlink ▾
Operation	Remove ▾
Apply	

Figure 425.

entry	describe
Port	Ethernet port name.
ULSM group	ULSM groups created.
ULSM port property	Uplink: Uplink port. Downlink: Downlink port.
Operation	Configuration: Apply the above settings. Remove: Delete the above.

ULSM port property		
Port	ULSM group	ULSM port property
Ethernet1/0/1	1	uplink

Figure 426.

<b>entry</b>	describe
<b>Port</b>	Ethernet port name.
<b>ULSM group</b>	ULSM groups created.
<b>ULSM port property</b>	Current ULSM groups correspond to configured upper and lower ports. Uplink: Uplink port. Downlink: Downlink port.

## 25.3 ULSM configuration display

### 25.3.1 ULSM display

This page can be used to view the current status of the ULSM group and the status of the upper and lower ports within the group.

To display the “ULSM group configuration” page, click ULSM configuration -> ULSM port configuration -> ULSM port property configuration, click “Apply” to view.

The screenshot shows the 'ULSM display' configuration page. It features a text input field for 'ULSM group', a dropdown menu set to 'all', and an 'Apply' button. Below this is an 'Information feedback window' displaying the command 'Switch# show ulsm group' and its output: 'ULSM group 1 state: Down'. A table follows, showing the status of the Uplink port (Ethernet1/0/1) as 'Down'.

Port	Role	State	ShutDown-by-ULSM
Ethernet1/0/1	UpLink	Down	

Figure 427.

## 26. Authentication configuration

### 26.1 RADIUS client configuration

#### 26.1.1 RADIUS global configuration

RADIUS global configuration module, the users in this module can configure the global RADIUS function services.

RADIUS configuration	
Authentication status	Disable ▾
Accounting	Disable ▾
Radius key operation	▾
RADIUS key	<input type="text"/>
System recovery time	5
RADIUS Retransmit times	3
RADIUS server timeout	3
<input type="button" value="Apply"/>	

AAA server status	
the status of the aaa	disable
the status of the radius accounting	disable
radius-server timeout	3
radius-server retransmit	3
radius-server dead-time	5
radius-server authentication host	192.168.2.200 port:23 primary

Figure 428.

<b>Authentication status</b>	Enable	Enable RADIUS certification services.
	Disable	Disabling RADIUS certification services.
<b>Accounting</b>	Enable	Enable RADIUS billing services.
	Disable	Disabling RADIUS billing services.
<b>Radius key operation</b>	Add	Add RADIUS key.
	Remove	Delete RADIUS key.
<b>RADIUS key</b>	Key string, 1-64 characters.	
<b>System recovery time</b>	Radius service recovery time from downtime to accessibility, 1-255 minutes.	
<b>RADIUS Retransmit times</b>	Radius authentication packet retransmission time, 1-100 seconds.	
<b>RADIUS server timeout</b>	The corresponding time of the radius server, 1-100 seconds.	

### 26.1.2 RADIUS authentication configuration

RADIUS authentication configuration module, the users in this module can configure the RADIUS authentication server.

RADIUS authentication server configuration		
Authentication server IP	<input type="text"/>	
Authentication server port(optional)	<input type="text"/>	
Primary authentication server	Primary authentication server ▼	
Operation	Add ▼	
<input type="button" value="Apply"/>		

RADIUS server configuration list		
Server IP	Port num	Primary server

Figure 429.

<b>Authentication server IP</b>	The address of IPv4 or IPv6 of the radius authentication server.	
<b>Authentication server port</b>	Port number of radius authentication server(optional), 0-65535.	
<b>Primary authentication server</b>	Primary authentication server	Specify radius server as primary authentication server.
	Non-Primary authentication server	Specify radius server as non-primary authentication server.
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

### 26.1.3 RADIUS accounting configuration

Radius authentication and accounting module, the users in this module can configure the RADIUS billing server.

RADIUS accounting server configuration		
Accounting server IP	<input type="text"/>	
Accounting server port(optional)	<input type="text"/>	
Primary accounting server	Primary accounting server ▼	
Operation	Add ▼	
<input type="button" value="Apply"/>		

RADIUS accounting server configuration list		
Server IP	Port num	Primary server

Figure 430.

<b>Accounting server IP</b>	Radius authentication server IPv4 or IPv6 address.
<b>Accounting server port</b>	Radius authentication server port number (optional), 0-65535.

<b>Primary accounting server</b>	Primary accounting server	Specify radius server as primary accounting server.
	Non-Primary accounting server	Specify radius server as non-primary accounting server.
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 26.2 TACACS server configuration

### 26.2.1 TACACS global configuration

TACACS global configuration module, the users in this module can configure the global TACACS function services.

TACACS configuration	
TACACS key	<input type="text"/>
TACACS server timeout	<input type="text" value="3"/>
Operation	Remove <input type="button" value="v"/>
<input type="button" value="Apply"/>	

TACACS server status	
the status of the tacacs	
tacacs-server timeout	<input type="text" value="3"/>

Figure 431.

<b>TACACS key</b>	TACACS authentication key, 1-16 characters.	
<b>TACACS server timeout</b>	TACACS authentication timeout, 1-60 seconds, default 3 seconds.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

### 26.2.2 TACACS server host configuration

TACACS server configuration module, the users in this module can configure the TACACS authentication server.

TACACS server configuration	
Authentication server IP	<input type="text"/>
Authentication server port(optional)	<input type="text"/>
Primary authentication server	Primary authentication server <input type="button" value="v"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 432.



<b>Authentication server IP</b>	TACACS authentication server IPv4 address, decimal point.	
<b>Authentication server port</b>	TACACS authentication server port number (optional), 0-65535.	
<b>Primary authentication server</b>	Primary accounting server	Specify TACACS server as primary accounting server.
	Non-Primary accounting server	Specify TACACS server as non-primary accounting server.
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 26.3 802.1x configuration

### 26.3.1 802.1x Global configuration

802.1x Global Configuration Module, the users in this module can configure the global 802.1x function services.

802.1x configuration	
802.1x status	Disable ▾
Maximum retransmission times of EAP-request/identity	2
Reauthenticate client periodically	Disable ▾
Holddown time for authentication failure	10
Reauthenticate client interval	3600
Resending EAP-request/identity interval	30
EAP relay authentication mode	forbid ▾
Private client	forbid ▾
MAC filtering	forbid ▾
802.1x unicast	Disable ▾
<input type="button" value="Apply"/>	

Figure 433.

<b>802.1x status</b>	Boot or turn off 802.1x function.
<b>Maximum retransmission times of EAP-request/identity</b>	Scope 1-10.
<b>Reauthenticate client periodically</b>	Start or close periodic recertification.
<b>Holddown time for authentication failure</b>	Range 1-65535 seconds, default 10 seconds.
<b>Reauthenticate client interval</b>	Range 1-65535 seconds, default 3600 seconds.
<b>Resending EAP-request/identity interval</b>	Range 1-65535 seconds, default 30 seconds.

<b>EAP relay authentication mode</b>	Ban or permit EAP relay authentication.
<b>Private client</b>	Prohibit or allow private clients.
<b>MAC filtering</b>	Ban or permit MAC address filtering.
<b>802.1x unicast</b>	Disable or enable 802.1x unicast teleport function.

### 26.3.2 802.1x port authentication configuration

802.1x port authentication configuration module, in this module the users can configure the 802.1x function of the specified port.

802.1x port configuration	
Port	Ethernet1/0/1 ▾
802.1x status	Disable ▾
Authentication type	force-unauthorized ▾
Authentication mode	Port-based ▾
Port maximum user	1
Guest VLAN ID	0
Apply	

Figure 434.

<b>Port</b>	Designated port number.	
<b>802.1x status</b>	Boot or close 802.1x on this port.	
<b>Authentication type</b>	force-unauthorized	Mandatory unauthorized.
	force-authorized	Mandatory authorization.
	Auto (802.1x)	automatism (802.1x authorization).
<b>Authentication mode</b>	Port-based	Based on port.
	Mac-based	Based on MAC.
<b>Port maximum user</b>	Maximum number of users allowed to connect to the ports, 1-256, default 1.	
<b>Guest VLAN ID</b>	Guest VLAN, 0-4094, default 0.	

### 26.3.3 802.1x port MAC configuration

802.1x port MAC configuration module, the users in this module can add or delete port 802.1x functions MAC specified ports.

802.1x port MAC configuration	
Port	Ethernet1/0/1 ▾
Mac	<input type="text"/>
Operation	Add MAC filter entry ▾
<input type="button" value="Apply"/>	

Figure 435.

<b>Port</b>	Specifies the port number.
<b>MAC</b>	MAC address to operate.
<b>Operation</b>	Add or delete port MAC address filter table items.

### 26.3.4 802.1x port status list

802.1x port MAC status list, the user can view 802.1 status information on x specified port and authenticate 802.1x in this module.

802.1x port status list	
Port	Ethernet1/0/1 ▾
802.1x status	Disable
Authentication type	NULL
Authentication status	Unauthenticated
Authentication mode	No authentication mode
<input type="button" value="Reauthenticate"/>	

Figure 436.

## 26.4 MAB configuration

### 26.4.1 MAB ENABLE configuration

MAB enable configuration module, the users in this module can MAB the function of global enable and specified port enable operation.

MAB global enable configuration	
MAB global enable	Enable ▾
Apply	

MAB port enable configuration	
Port	Ethernet1/0/1 ▾
MAB port enable	Enable ▾
Apply	

Figure 437.

<b>MAB global enable</b>	Global enable or disable MAB function.
<b>Port</b>	Specifies the port number.
<b>MAB port enable</b>	Function on or off MAC specified port.

### 26.4.2 MAB Authentication configuration

MAB user authentication configuration module, the users in this module can configure the MAB user authentication mode.

MAB Authentication configuration	
MAB Authentication TYPE	MAC address ▾
username	
password	
Apply	

Figure 438.

<b>MAB Authentication TYPE</b>	Mac address	Authentication based on MAC address.
	Username and password	Authentication based on username and password (to be configured).
<b>username</b>	user name for authentication, 1-32 characters.	
<b>password</b>	password for authentication, 1-32 characters.	

### 26.4.3 MAB parameter configuration

MAB parameter configuration module, the users in this module can configure the parameters of the MAB function.

MAB parameter configuration	
Port	Ethernet1/0/1 ▾
parameter type	guest vlan range ▾
value	<input type="text"/>
Enable ▾	
<input type="button" value="Apply"/>	

Figure 439.

<b>Port</b>	Specify port name.	
<b>parameter type</b>	Guest vlan range	VLAN operation for guest.
	Max binding value	Operation of maximum binding on ports.
<b>value</b>	After the parameter type is selected, the corresponding parameter value range can be set.	
<b>Enable Disable</b>	Boot or close port MAB parameter configuration.	

MAB parameter configuration	
parameter type	reauth-period ▾
value	<input type="text"/>
Enable ▾	
<input type="button" value="Apply"/>	

Figure 440.

<b>parameter type</b>	Reauth period	MAB time interval for re-authentication after failed authentication.
	Offline-detect	Detect the scan time of each port online status, 0 does not detect.
	Quiet-period	Configure the silence time after MAB authentication failure.
	Stale-period	Configure the time to delete bound users after the MAB port is closed.
	Linkup-period	Configure the restart time range after MAB port shutdown.
<b>value</b>	After the parameter type is selected, the corresponding parameter value can be set.	
<b>Enable Disable</b>	Boot or close global MAB parameter configuration.	

authentication mab	
check type	radius ▾
Enable ▾	
Apply	

Figure 441.

<b>Check type</b>	MAC address authentication uses radius or none to verify user login.
<b>Enable Disable</b>	Start or close validation mode configuration.

spoofing-garp-check	
spoofing-garp-check	Enable ▾
Apply	

Figure 442.

<b>spoofing-garp-check</b>	Activate or close check fake free ARP configuration.
----------------------------	--

### 26.4.4 MAB show

MAB display module, the users can display mAb status of specified port or all ports in this module.

MAB show	
Port	all ▾
Apply	

Information feedback window			
Switch# show mac-authentication-bypass			
The Number of all binding is 0			
MAC	Interface	Vlan ID	State
-----			

Figure 443.

<b>Port</b>	Displays information MAB the specified port or all ports.
-------------	---

## 27. PoE Config

## 27.1 PoE Global Config

### 27.1.1 PoE Global Config

This page can be used to globally configure PoE properties and view PoE global property information.

To display the "PoE Global Config" page, click PoE Config -> PoE Global Config -> PoE Global Config, click "Apply" to configure.

PoE Global Config	
PoE Work Status	online
PoE Port Max Number	24
PoE Support Type	802.3at/802.3af
PoE MCU Software Version	V2.1
PoE Power Available(37-370 W)	370
PoE Power Used	0 W
PoE Power Remaining	370 W
PoE Main Voltage	54.4 V
PoE Min Voltage	44 V
PoE Max Voltage	57 V
PoE Police	Off ▾
PoE Legacy	Off ▾
PoE High-inrush Status	Enable ▾
PoE Monitor interval(30-36000 s)	150
PoE Reset Interval(1-600 s)	5
Apply	

Figure 444.

entry	describe
<b>PoE Power Available</b>	Maximum power supported by current switches.
<b>PoE Police</b>	Enable status of priority power supply policy: Off: disable On: enable
<b>PoE Legacy</b>	Current status of standard PD detection function: Off: disable On: enable
<b>PoE High-inrush Status</b>	Enable/Disable.
<b>PoE Monitor interval</b>	Check whether the PD connected to the current port is in the detection interval of normal communication, range: 30-36000 seconds.
<b>PoE Reset Interval</b>	Port reset time range: 1-600 per second.

## 27.2 PoE Port Config

### 27.2.1 PoE Port Config

This page can be used to configure PoE properties under ports.

To display the "PoE Port Config" page, click PoE Config -> PoE Port Global Config -> PoE Port Config, click "Apply" to configure.

PoE Port Config			
Interface	Status	Priority	PoE Monitor Status
Ethernet1/0/1 ▾	auto ▾	low ▾	off ▾
			Apply

Figure 445.

<b>entry</b>	describe
<b>Interface</b>	Current configured Ethernet ports.
<b>Status</b>	Auto: Normal power supply Static: Forced power supply Disable: No power supply
<b>Priority</b>	Low: low priority High: high priority Critical: highest priority
<b>PoE Monitor Status</b>	Off: Disable port monitoring ON: Enable port monitoring

Max Power	
Interface	Max Power(1-32000mW)
Ethernet1/0/1 ▾	32000 mW
Apply	

Figure 446.

<b>entry</b>	describe
<b>Interface</b>	Current configured Ethernet ports.
<b>Max Power</b>	Sets the maximum output power supported by the current port, size range: 1-32000, unit mW; For example: 100, 200, 3000.

Time range name	
Interface	Time range name
Ethernet1/0/1 ▾	▾
Apply	



Time range name	
Interface	Time range name
Ethernet1/0/1 ▾	▾
Apply	

Figure 447.

<b>entry</b>	describe
<b>Interface</b>	Current configured Ethernet ports.
<b>Time range name</b>	The time range name defined by the switch.

Unset Time range name	
Interface	Ethernet1/0/1 ▾
Default	

Figure 448.

<b>entry</b>	describe
<b>Interface</b>	Current configured Ethernet ports.
<b>Default</b>	

## 28. DOS attack protection configuration

### 28.1 Source IP equal destination IP DOS attack protection configuration

Source IP equal to destination IP anti DoS attack configuration module, the user can start or turn off the DOS attack function IP equal to the destination in this module.

Source IP equal destination IP DOS attack protection configuration	
DOS attack protection status	Disable ▾
Apply	

DOS attack protection status	
DOS attack protection status	Disable

Information feedback window	
Switch# config t	
Switch(config)# no dosattack-check srcip-equal-dstip enable	

Figure 449.

## 28.2 Source port equal destination port DOS attack protection configuration

Source port equal to destination port anti DoS attack configuration module, the users in this module can start or close the source port equal to the destination port DOS attack function.

Source port equal destination port DOS attack protection configuration	
DOS attack protection status	Disable ▾
<input type="button" value="Apply"/>	

DOS attack protection status	
DOS attack protection status	Disable

Information feedback window	
Switch# config t	
Switch(config)# no dosattack-check srcport-equal-dstport enable	

Figure 450.

## 28.3 TCP DOS attacks on invalid flags configuration

TCP DoS attack invalid flag bit configuration module, the users in this module can start or close the DOS attack function to check unauthorized TCP tags.

TCP DOS attacks on invalid flags configuration	
DOS attack protection status	Disable ▾
<input type="button" value="Apply"/>	

DOS attack protection status	
DOS attack protection status	Disable

Information feedback window	
Switch# config t	
Switch(config)# no dosattack-check tcp-flags enable	

Figure 451.

## 28.4 ICMP DOS attack protection configuration

ICMP anti DoS attack configuration module, the user can start or turn off the DOS attack check function of the anti-ICMP fragment in this module.

ICMP DOS attack protection configuration	
DOS attack protection status	Enable ▾
<input type="button" value="Apply"/>	

DOS attack protection status	
DOS attack protection status	Enable

Information feedback window	
Switch# config t	
Switch(config)# dosattack-check icmp-attacking enable	

Figure 452.

## 28.5 ICMP packet-size configuration

The maximum ICMP message configuration module is allowed, the users can configure the maximum net length of icmpv4 packets in this module.

ICMP packet-size configuration	
Packet-size	64
Apply	

Packet-size	
Packet-size	64

Information feedback window	
Switch# config t	
Switch(config)# dosattack-check icmpV4-size 64	

Figure 453.

<b>Packet-size</b>	Maximum net length of allowed ICMPv4 packets, 64-1023, default 512.
--------------------	---

## 28.6 First fragment IP packet DOS attack protection configuration

The first IP packet fragment anti DoS attack configuration module, the user can start or turn off the DOS attack function against the first IP message fragment in this module.

First fragment IP packet DOS attack protection configuration	
DOS attack protection status	Enable ▾
Apply	

DOS attack protection status	
DOS attack protection status	Enable

Information feedback window	
Switch# config t	
Switch(config)# dosattack-check ipv4-first-fragment enable	

Figure 454.

## 29. SSL config

### 29.1 IP HTTP server configuration

HTTP server configuration module, the user can start or stop the HTTP service of the switch by using this module again.

IP HTTP server configuration	
IP HTTP server status	Enable ▾
Apply	

Information feedback window	
IP HTTP server status	Enable

Information feedback window	
Switch# config t	
Switch(config)# ip http server	
web server has worked	

Figure 455.

## 29.2 SSL global configuration

SSL function switch configuration module, the users in this module can start or close the switch SSL service function.

SSL global configuration	
SSL status	Enable ▾
Apply	

Information feedback window	
SSL status	Enable

Information feedback window	
Switch# config t	
Switch(config)# ip http secure-server	
web server is on	

Figure 456.

## 29.3 SSL server monitor port configuration

SSL server monitor port number start configuration module, the users can configure SSL server listening port number in this module.

SSL server monitor port configuration	
port number	<input type="text"/>
Operation	Add ▾
Apply	

Information feedback window	
port number	443

Figure 457.

<b>Port</b>	Specifies the port number.	
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 29.4 SSL secure-ciphersuite configuration

SSL encryption suite configuration module, the users can configure the encryption suite type of SSL service in this module.

Figure 458.

<b>secure-ciphersuite type</b>	aes256-sha	aes256-sha encryption is used.
	ecdhe-rsa-aes256-sha	ecdhe-rsa-aes256-sha encryption is used.
<b>Operation</b>	Add	Add operations.
	Remove	Delete operations.

## 30. sFlow configuration

### 30.1 sFlow collector global address configuration

This page can be used to configure the global sFlow analyzer address.

To display the “sFlow collector global address configuration” page, sFlow configuration -> sFlow collector global address configuration, click “Apply” to configure.

Figure 459.

<b>entry</b>	describe
--------------	----------

<b>IP address</b>	sFlow Analyzer Address.
<b>destination port NO.</b>	Range between 1025 and 65535.
<b>Operation</b>	Configuration: User self-configuration. Default: Restore default configuration.

### 30.2 sFlow collector port address configuration

This page can be used to configure port sFlow analyzer address.

To display the “sFlow collector port address configuration” page, sFlow configuration -> sFlow collector port address configuration, click “Apply” to configure.

sFlow collector port address configuration	
Port	Ethernet1/0/1 ▾
IP address	<input type="text"/>
destination port NO.	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 460.

<b>entry</b>	describe
<b>Port</b>	Ethernet port number.
<b>IP address</b>	sFlow Analyzer Address.
<b>destination port NO.</b>	Range between 1025 and 65535.
<b>Operation</b>	Configuration: User self-configuration. Default: Restore default configuration.

### 30.3 sFlow agent address configuration

This page can be used for sFlow agent configuration.

To display the “sFlow agent address configuration” page, sFlow configuration -> sFlow agent address configuration, click “Apply” to configure.

sFlow agent address configuration	
IP address	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 461.

<b>entry</b>	describe
<b>IP address</b>	sFlow agent address.
<b>Operation</b>	Configuration: User self-configuration. Default: Restore default configuration.

### 30.4 sFlow priority configuration

This command is used to set the priority of the sample message.

To display the “sFlow priority configuration” page, sFlow configuration -> sFlow priority configuration, click “Apply” to configure.

sFlow priority configuration	
agent priority value	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 462.

<b>entry</b>	describe
<b>agent priority value</b>	Range: 0-3.
<b>Operation</b>	Configuration: User self-configuration. Default: Restore default configuration.

### 30.5 sFlow header length configuration

This page can be used to configure the length of header packets copied in sFlow data sampling.

To display the “sFlow header length configuration” page, sFlow configuration -> sFlow header length configuration, click “Apply” to configure.

sFlow header length configuration	
Port	Ethernet1/0/1 ▾
header length	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 463.

entry	describe
Port	Ethernet port name.
header length	Length range: 32-256.
Operation	Configuration: User self-configuration. Default: Restore default configuration.

### 30.6 sFlow data length configuration

This page is used to configure sflow packet length.

To display the “sFlow header length configuration” page, sFlow configuration -> sFlow data length configuration, click “Apply” to configure.

sFlow data length configuration	
Port	Ethernet1/0/1 ▾
data length	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 464.

entry	describe
Port	Ethernet port name.
data length	Length range: 500-1470.
Operation	Configuration: User self-configuration. Default:



	Restore default configuration, default value is 1400.
--	---

### 30.7 sFlow rate configuration

This page can be used to configure port hardware sampling rates.

To display the “sFlow rate configuration” page, sFlow configuration -> sFlow rate configuration, click “Apply” to configure.

sFlow rate configuration	
Port	Ethernet1/0/1 ▾
direction	input ▾
rate value	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 470.

entry	describe
Port	Ethernet port name.
direction	Input: receive data. Output: send data.
rate value	Rate range: 1000-16383500.
Operation	Configuration: User self-configuration. Default: Restore default configuration.

### 30.8 sFlow counter interval configuration

This page can be used to configure sFlow statistical sampling intervals.

To display the “sFlow counter interval configuration” page, sFlow configuration -> sFlow counter interval configuration, click “Apply” to configure.

sFlow counter interval configuration	
Port	Ethernet1/0/1 ▾
counter interval	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 466.

entry	describe
Port	Ethernet port name.
counter interval	Sampling interval range: 20-120.
Operation	Configuration: User self-configuration. Default: Restore default configuration.

### 30.9 sFlow analyzer configuration

This page can be used for globally enabled sFlow analyzers.

To display the “sFlow analyzer configuration” page, sFlow configuration -> sFlow analyzer configuration, click “Apply” to configure.

sFlow analyzer configuration	
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Figure 467.

entry	describe
Operation	Configuration: Function Enable. Remote: Function disabled.

## 31. IPv6 security ra configuration

### 31.1 IPv6 security ra global configuration

Launch the global IPv6 security RA module, the user can start or close the global IPv6 security RA function in this module.

IPv6 security ra global configuration	
Operation	Enable ▾
Apply	

Information feedback window
Switch# config
Switch(config)# ipv6 security-ra enable

Figure 468.

### 31.2 IPv6 security ra port configuration

Start port IPv6 security RA module, the user can start or close the security RA function IPv6 the specified port in this module.

IPv6 security ra port configuration	
Port	Ethernet1/0/1 ▾
Operation	Enable ▾
Apply	

Information feedback window
Switch# config
Switch(config)# interface Ethernet1/0/1
Switch(config-if-ethernet1/0/1)# ipv6 security-ra enable

Figure 469.

<b>Port</b>	Specifies the port number.	
<b>Operation</b>	Enable	Start operation.
	Disable	Close operation.

### 31.3 show IPv6 security ra

Show IPv6 security RA configuration module, the user can display the specified port or global IPv6 security RA function configuration information in this module.

show IPv6 security ra	
Port	Ethernet1/0/1 ▾
<input type="button" value="Apply"/>	

```

Information feedback window
Switch# config
Switch(config)# show ipv6 security-ra interface Ethernet1/0/1
IPv6 security RA information:
Global IPv6 Security RA State: enabled
IPv6 Security RA State: Yes
Switch# config
Switch(config)# show ipv6 security-ra interface Ethernet1/0/1
IPv6 security RA information:
Global IPv6 Security RA State: enabled
IPv6 Security RA State: Yes
    
```

Figure 470.

<b>Port</b>	Specifies the port number ALL represents all.
-------------	---

## 32. Device log message

### 32.1 Show device log message

View device log information module, where the users can view system key logs and warning logs.

Show device log message	
Level	critical ▾
Begin	<input type="text"/>
End	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 471.

<b>Level</b>	critical	Key-level log information.
	warnings	Warning Level Log Information.
<b>Begin</b>	To see where the log information starts.	
<b>End</b>	To see the end location of the log information.	

### 32.2 Clear logging in logbuff channel

Clears all log message modules in the buffer, the users in this module can clear all log messages in the buffer.

<b>Clear logging in logbuff channel</b>	
Clear logging in logbuff channel?	
	<input type="button" value="Apply"/>

---

<b>Information feedback window</b>
Switch# clear logging sdram

Figure 472.