



**QASA CLI**

# Web User Manual-L3

# Contents

- Getting Start .....9
- Web-based Switch Configuration.....12
- Console Port Interface .....13
- 1. System Config .....14
  - 1.1. System Homepage .....14
  - 1.2. Device Info .....15
  - 1.3. IP Config.....16
    - 1.3.1. IPv4 Config .....16
    - 1.3.2. IPv6 Config .....16
  - 1.4. Web Config .....17
    - 1.4.1. Web Timeout .....17
    - 1.4.2. HTTP .....17
    - 1.4.3. HTTPS .....17
    - 1.4.4. Security IP.....18
  - 1.5. User Management.....19
    - 1.5.1. User Management .....19
    - 1.5.2. Authentication Method .....20
  - 1.6. Firmware Upgrade .....21
    - 1.6.1. TFTP Service .....21
    - 1.6.2. FTP Service .....21
    - 1.6.3. HTTP Upgrade .....22
  - 1.7. Management Config.....22
    - 1.7.1. TFTP .....22
    - 1.7.2. HTTP .....23
  - 1.8. NTP .....23
    - 1.8.1. NTP Config .....23
    - 1.8.2. NTP Authentication Config.....24
  - 1.9. SNTP.....24
    - 1.9.1. Server Config .....24
    - 1.9.2. Time Zone Config .....25
  - 1.10. Device Management .....25
    - 1.10.1. Device Reboot/Reset .....25
    - 1.10.2. System Utilization.....26
    - 1.10.3. View System Config.....26

1.10.4. View Logging Buffer .....	27
1.10.5. View Logging Flash .....	27
2. Monitor Management .....	28
2.1. SSH Config .....	28
2.2. Telnet Config .....	28
2.3. Port Statistics .....	29
2.4. DDMI Status .....	30
2.5. Ping .....	30
2.6. Traceroute .....	31
2.7. Cable Diagnostics .....	31
2.8. SNMP Config .....	32
2.8.1. Global Config .....	32
2.8.2. User Config .....	32
2.8.3. Group Config .....	33
2.8.4. Community Config .....	34
2.8.5. Trap Config .....	34
2.8.6. View Config .....	35
2.8.7. Security IP Config .....	36
2.8.8. SNMP Statistics .....	36
2.9. RMON Config .....	36
2.9.1. RMON Statistics .....	36
2.9.2. RMON History Config .....	37
2.9.3. RMON Event Config .....	37
2.9.4. RMON Alarm Config .....	38
2.10. Onvif Config .....	39
2.10.1. Server Config .....	39
2.10.2. Detect Config .....	39
2.11. Loopback Detection .....	39
2.11.1. Port Mode .....	39
2.11.2. VLAN Loopback .....	40
2.11.3. Interval Time .....	40
2.11.4. Recovery Timeout .....	41
2.12. LLDP Config .....	41
2.12.1. Global Config .....	41
2.12.2. Port Config .....	42

2.12.3. TLV Config.....	43
2.12.4. Neighbor Info .....	43
3. Switch Config.....	44
3.1. Port Config.....	44
3.1.1. Port Config .....	44
3.1.2. Port 10G Mode (Specific).....	46
3.2. Port Mirror .....	46
3.3. Port Isolate.....	47
3.4. Port Channel.....	48
3.4.1. Port Channel Group .....	48
3.4.2. LACP .....	49
3.5. Jumbo Frame .....	49
3.6. Port Rate .....	50
3.7. Storm Control.....	51
3.8. MAC Address Config.....	52
3.8.1. Static MAC.....	52
3.8.2. Black Hole MAC .....	52
3.8.3. Aging-time.....	53
3.8.4. MAC Address List.....	54
3.9. AM .....	54
3.10. AAA.....	55
3.10.1. Radius.....	55
3.10.2. Radius Accounting .....	57
3.10.3. Tacacs.....	58
4. VLAN Config.....	61
4.1. VLAN Config.....	61
4.1.1. VLAN ID.....	61
4.1.2. Show VLAN.....	61
4.1.3. Port Config.....	62
4.2. GVRP Config .....	63
4.2.1. GVRP Config .....	63
4.2.2. GVRP Port .....	64
4.3. QINQ.....	64
4.3.1. Enable Dot1q Tunnel .....	64
4.3.2. Dot1q Tunnel TPID.....	65

4.4. Voice VLAN .....	65
4.4.1. VLAN Config .....	65
4.4.2. Port Config .....	66
4.5. MAC VLAN .....	67
4.5.1. VLAN Config .....	67
4.5.2. VLAN Member .....	67
4.5.3. Port Config .....	68
4.6. Protocol VLAN .....	68
4.7. Surveillance VLAN .....	69
4.7.1. VLAN Config .....	69
4.7.2. Port Config .....	70
5. Port Config .....	71
5.1 PoE Global Config .....	71
5.2. PoE Port Config .....	72
5.3. PD Alive .....	73
5.4. PoE Schedule .....	73
6. DHCP Config .....	74
6.1. DHCP Server .....	74
6.1.1. Global Config .....	74
6.1.2. Create Address Pool .....	74
6.1.3. Dynamic Pool .....	75
6.1.4. Manual Pool .....	76
6.1.5. Default Gateway .....	77
6.1.6. DNS Server .....	78
6.1.7. Excluded Address .....	79
6.1.8. Packet Statistics .....	79
6.1.9. Client List .....	80
6.2. DHCP Relay Config .....	80
6.2.1. DHCP Relay Config .....	80
6.3. DHCP Snooping .....	81
6.3.1. Global Config .....	81
6.3.2. VLAN Config .....	82
6.3.3. Static User Binding .....	82
6.3.4. Helper-server Config .....	83
6.3.5. Port Binding .....	84

6.3.6. Trust Port.....	84
7. ACL Config.....	85
7.1. Time Range Config .....	85
7.2. IP ACL .....	86
7.2.1. IP Standard ACL .....	86
7.2.2. IP Extended ACL.....	87
7.3. MAC ACL.....	88
7.3.1. MAC Standard ACL .....	88
7.3.2. MAC Extended ACL .....	89
7.4. MAC-IP Extended ACL.....	90
7.5. ACL Binding .....	92
7.5.1. Binding Port.....	92
7.5.2. Binding Vlan .....	93
8. Ring Network .....	94
8.1. Spanning-tree .....	94
8.1.1. Global Properties.....	94
8.1.2. Instance Mapping.....	95
8.1.3. Instance Properties .....	96
8.1.4. Port Config.....	96
8.1.5. Port Instance .....	97
8.1.6. Status .....	98
8.2. ERPS .....	98
8.2.1. ERPS Ring Config .....	98
8.2.2. ERPS Instance Config.....	100
8.2.3. View ERPS Statistics.....	101
9. Route Config.....	103
9.1. Static Route .....	103
9.2. RIP Route .....	104
9.2.1. Keychain .....	104
9.2.2. Basic Config.....	104
9.2.3. Network Config.....	105
9.2.4. Passive Interface .....	107
9.2.5. Neighbor Config .....	108
9.2.6. Interface Config.....	108
9.2.7. Redistribute Router .....	109

9.2.8. View RIP Information.....	110
9.3. OSPF Route.....	110
9.3.1. Basic Config .....	110
9.3.2. Network Config.....	111
9.3.3. Passive Interface .....	111
9.3.4. Area Config .....	112
9.3.5. Interface Config.....	113
9.3.6. Interface Authentication .....	115
9.3.7. Default Route Originate .....	116
9.3.8. Redistribute Router.....	117
9.3.9. View OSPF Information.....	118
9.4. BGP Route.....	118
9.4.1. Basic Config .....	118
9.4.2. Aggregate Address .....	119
9.4.3. Aggregate Address .....	120
9.4.4. Redistribute Router.....	120
9.4.5. Neighbor Config .....	121
9.4.6. BGP Correlative Config .....	121
9.4.7. Timer Config .....	122
9.4.8. View BGP Information .....	122
9.5. Routing Table .....	123
10 .Multicast Manage .....	124
10.1. IGMP Snooping Config.....	124
10.1.1. Basic Config .....	124
10.1.2. Static Router Port .....	124
10.1.3. VLAN Config.....	125
10.1.4. Querier Config.....	126
10.1.5. Multicast Table .....	126
10.2. MLD Snooping Config .....	127
10.2.1. Basic Config .....	127
10.2.2. Static Router Port .....	127
10.2.3. VLAN Config.....	128
10.2.4. Querier Config.....	129
10.2.5. Multicast Table .....	129
11. QoS Config .....	130

11.1. Port Config .....	130
11.1.1. Trust Config.....	130
11.1.2. Weight Config .....	130
11.1.3. CoS-To-IntP Config.....	133
11.1.4. DSCP-To-IntP Config .....	133
11.1.5. Policy Config .....	134
11.2. Class-Map Config .....	135
11.2.1. Class-Map Config.....	135
11.2.2. Class-Map Rule Config .....	135
11.3. Policy-Map Config.....	140
11.3.1. Policy Name Config.....	140
11.3.2. Policy Class Config.....	140
11.3.3. Policy Mark Config .....	141
11.3.4. Policy Bandwidth .....	142
11.3.5. Policy VLAN.....	143



# Getting Start

This section introduces the web-based configuration utility and covers the following topics:

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

## Powering on the device:

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 outline 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.



**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 behaviour.

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

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:

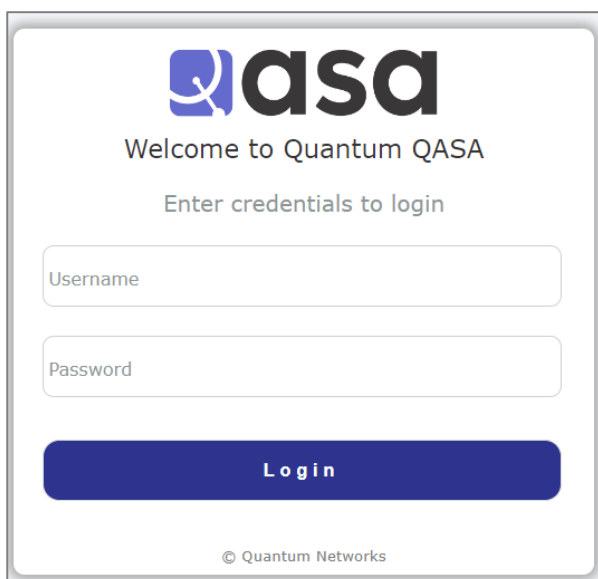
1. Open the Web browser.
2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.2.1) and then press Enter.



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 colour. 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.

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.



**Login Window**

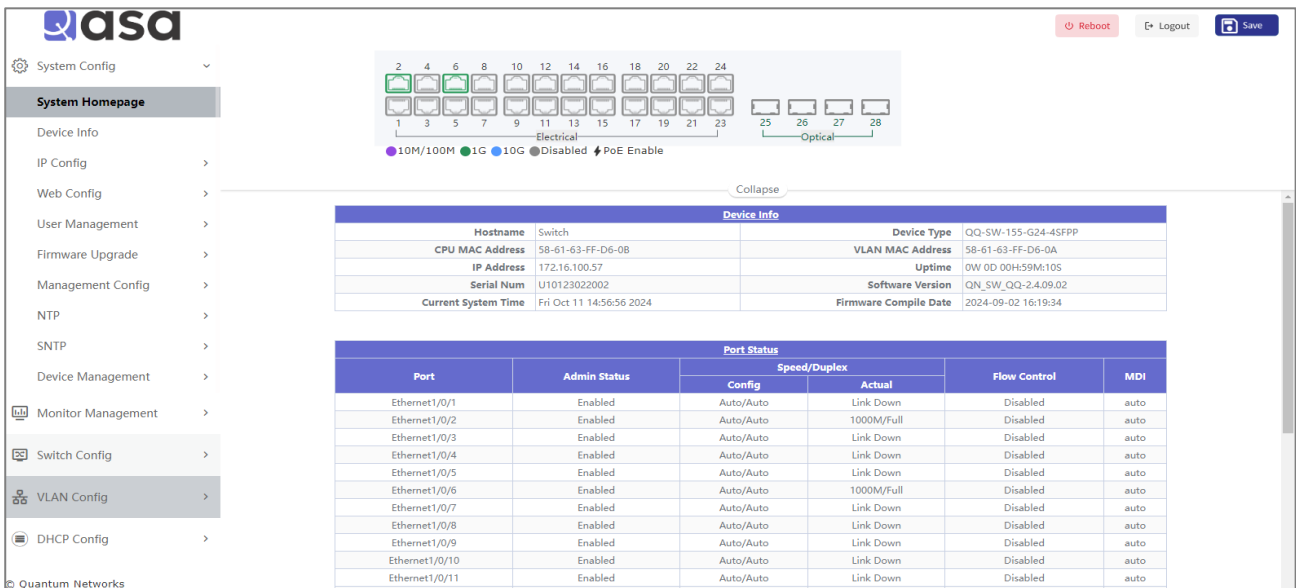
## Logging In

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 have logged in 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 as below.



The screenshot shows the ASA configuration utility interface. On the left is a navigation menu with options like System Config, Device Info, IP Config, Web Config, User Management, Firmware Upgrade, Management Config, NTP, SNTP, Device Management, Monitor Management, Switch Config, VLAN Config, and DHCP Config. The main area displays 'System Information' with a 'Collapse' button. At the top, there is a port status indicator showing 24 electrical ports (1-24) and 4 optical ports (25-28). Below this are two tables:

Device Info			
Hostname	Switch	Device Type	QQ-SW-155-G24-45FPP
CPU MAC Address	58-61-63-FF-D6-08	VLAN MAC Address	58-61-63-FF-D6-0A
IP Address	172.16.100.57	Uptime	0W 0D 00H:59M:10S
Serial Num	U10123022002	Software Version	QN_SW_QQ-2.4.09.02
Current System Time	Fri Oct 11 14:56:56 2024	Firmware Compile Date	2024-09-02 16:19:34

Port	Admin Status	Speed/Duplex		Flow Control	MDI
		Config	Actual		
Ethernet1/0/1	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/2	Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/3	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/4	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/5	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/6	Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/7	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/8	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/9	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/10	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/11	Enabled	Auto/Auto	Link Down	Disabled	auto

### System Information Window

If you enter 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.

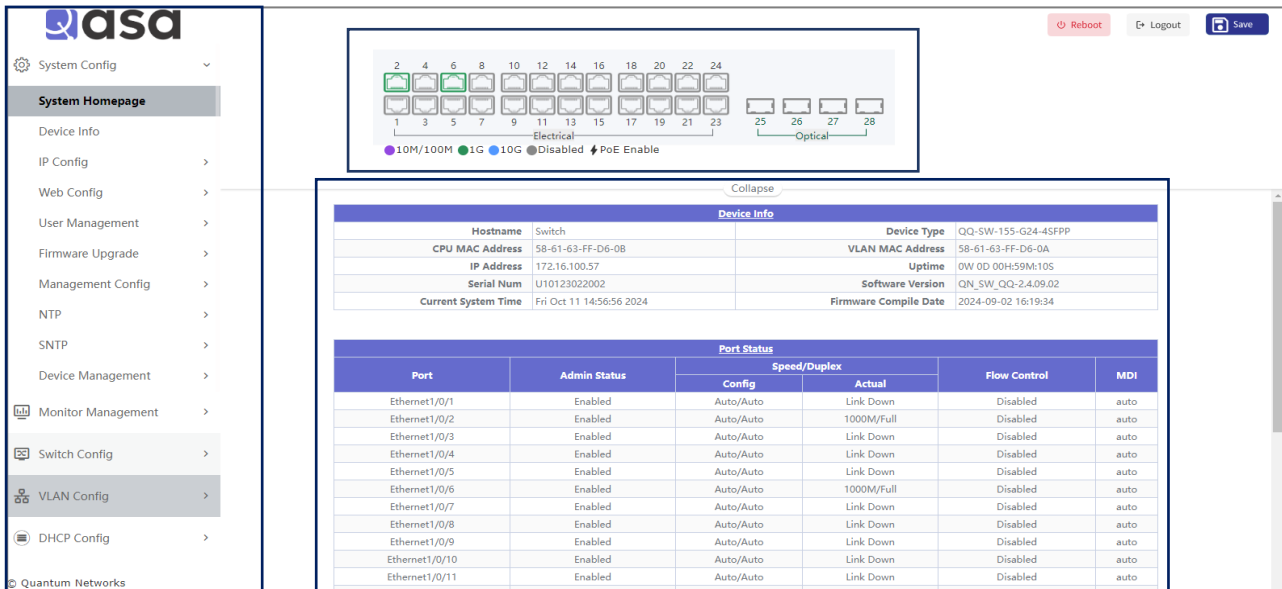
To logout, click Logout in the top right corner of any page. The system logs out of the device.

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 image:



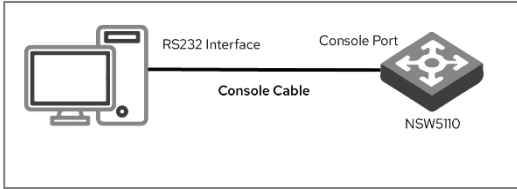
Device Info	
Hostname	Switch
Device Type	QQ-SW-155-G24-4SFPP
CPU MAC Address	58-61-63-FF-D6-0B
VLAN MAC Address	58-61-63-FF-D6-0A
IP Address	172.16.100.57
Uptime	0W 0D 00H:59M:10S
Serial Num	U10123022002
Software Version	QN_SW_QQ-2.4.09.02
Current System Time	Fri Oct 11 14:56:56 2024
Firmware Compile Date	2024-09-02 16:19:34

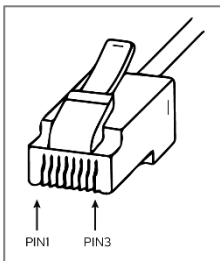
Port	Admin Status	Speed/Duplex		Flow Control	MDI
		Config	Actual		
Ethernet1/0/1	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/2	Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/3	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/4	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/5	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/6	Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/7	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/8	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/9	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/10	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/11	Enabled	Auto/Auto	Link Down	Disabled	auto

# 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:



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.



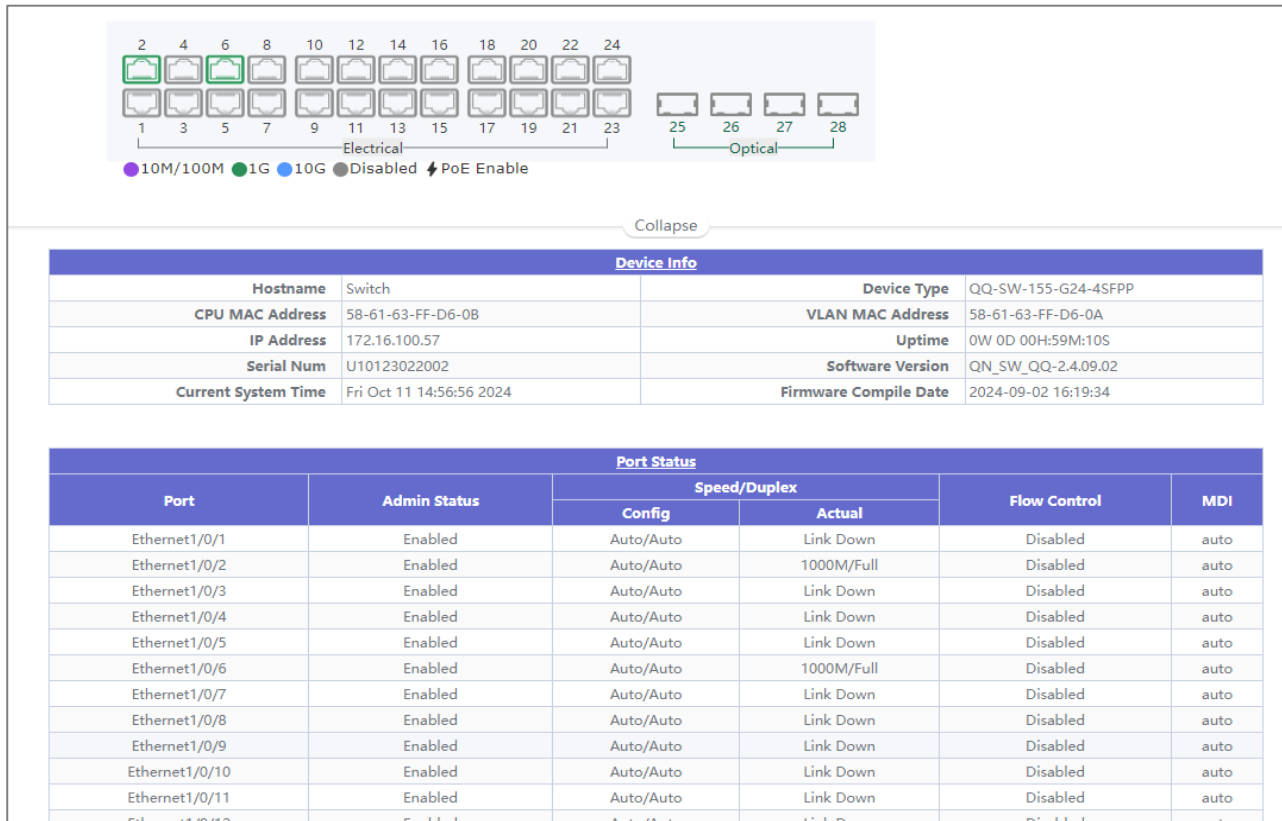
This cable is used to connect the console port of the switch to the external monitoring terminal. One end of the RJ45 eight-pin plug, the other end is a 25-hole plug (DB25) and 9-hole plug (DB9), RJ45 head into the switch’s console port socket, DB25 and DB9 can be used according to the requirements of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

RJ45	<====>	DB9
[ RTS 1 ~~~ 8 CTS ]		
[ DTR 2 ~~~ 6 DSR ]		
[ TXD 3 ~~~ 2 RXD ]		
[ GND 4 ~~~ 5 GND ]		
[ GND 5 ~~~ 5 GND ]		
[ RXD 6 ~~~ 3 TXD ]		
[ DSR 7 ~~~ 4 DTR ]		
[ CTS 8 ~~~ 7 RTS ]		

# 1. System Config

## 1.1. System Homepage

The system homepage contains **Device Info** and **Port Status** as shown in image below.



The screenshot displays a port status overview at the top, showing 28 ports arranged in two rows. The first row contains ports 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, and 24. The second row contains ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 26, 27, and 28. Ports 2, 4, 6, and 8 are highlighted in green, indicating 1G status. Ports 10, 12, 14, 16, 18, 20, 22, and 24 are highlighted in blue, indicating 10G status. Ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 26, 27, and 28 are highlighted in grey, indicating they are disabled. A legend below the port icons shows: 10M/100M (purple dot), 1G (green dot), 10G (blue dot), Disabled (grey dot), and PoE Enable (lightning bolt icon).

Below the port status overview is a "Collapse" button. The main content area is divided into two sections: "Device Info" and "Port Status".

Device Info			
Hostname	Switch	Device Type	QQ-SW-155-G24-4SFPP
CPU MAC Address	58-61-63-FF-D6-0B	VLAN MAC Address	58-61-63-FF-D6-0A
IP Address	172.16.100.57	Uptime	0W 0D 00H:59M:10S
Serial Num	U10123022002	Software Version	QN_SW_QQ-2.4.09.02
Current System Time	Fri Oct 11 14:56:56 2024	Firmware Compile Date	2024-09-02 16:19:34

Port Status					
Port	Admin Status	Speed/Duplex		Flow Control	MDI
		Config	Actual		
Ethernet1/0/1	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/2	Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/3	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/4	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/5	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/6	Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/7	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/8	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/9	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/10	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/11	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/12	Enabled	Auto/Auto	Link Down	Disabled	auto

Click on **Device Info** or **Port Status** to enter the corresponding page.

## 1.2. Device Info

The Device Info page allows you to view device information and also set the Hostname, Device Contact, device Location of the device and the Current System Time.

Device Info	
Hostname	<input type="text" value="Switch"/>
Device Contact	<input type="text" value="Default"/>
Device Location	<input type="text" value="Default"/>
Device Type	QQ-SW-155-G24-4SFPP
CPU MAC Address	58-61-63-FF-D6-0B
VLAN MAC Address	58-61-63-FF-D6-0A
IP Address	172.16.100.57
Client IP Address	192.168.13.101
Serial Num	U10123022002
Software Version	QN_SW_QQ-2.4.09.02
BootRom Version	V2.00
Firmware Compile Date	2024-09-02 16:19:34
Uptime	0W 0D 01H:45M:55S
Current System Time	<input type="text" value="15"/> Hour <input type="text" value="43"/> Min <input type="text" value="40"/> Sec <input type="text" value="2024"/> Year <input type="text" value="10"/> Month <input type="text" value="11"/> Day
<input type="button" value="Apply"/>	

<b>Hostname</b>	Fill in the new <b>Hostname</b> of the switch to be changed, 1-64 characters.
<b>Device Contact</b>	Fill in the new <b>Device Contact</b> of the switch to be changed, 0-255 characters.
<b>Device Location</b>	Fill in the new <b>Device Location</b> of the switch to be changed, 0-255 characters.
<b>Current System Time</b>	Manually changing the current system time, When the switch restart will invalidate.

## 1.3. IP Config

### 1.3.1. IPv4 Config

The page can be used to configure IP address and subnet mask for the VLAN interface. To display the "IPv4 Config" page, click System Config ->IP Config->IPv4 Config, click "Apply" to configure.

**IPv4 Config**

VLAN Interface	VLAN0001 <input type="button" value="v"/>		
IP Mode	Static IP <input type="button" value="v"/>		
IP Address	<input type="text"/>	Example:10.10.10.1	
Netmask	<input type="text"/>	Example:255.255.255.0	

Showing  Entries Showing 1 to 1 of 1 entries

	VLAN Interface	IP Mode	IP Address	Netmask
<input type="checkbox"/>	VLAN0001	Dynamic	172.16.100.57	255.255.255.0

<b>VLAN Interface</b>	VLAN ID of layer 3 interface created
<b>IP Mode</b>	Static IP: User self-configuration Dynamic: dhcp-client Automatic acquisition
<b>IP Address</b>	IP Address, e.g. A.B.C.D
<b>Netmask</b>	Netmask: for example :255.255.255.0
<b>Operation</b>	Action: Apply/Delete

### 1.3.2. IPv6 Config

The page can be used to configure IPv6 address and subnet mask for the VLAN interface. To display the "IPv6 Config" page, click System Config ->IP Config->IPv6 Config, click "Apply" to configure.

**IPv6 Config**

VLAN Interface	VLAN0001 <input type="button" value="v"/>		
IPv6 Address	<input type="text"/>	Example:2001::1234	
Prefix-length	<input type="text"/>	Example:48	

Showing  Entries Showing 0 to 0 of 0 entries

	No.	VLAN Interface	IPv6 Address
0 results found.			



<b>VLAN Interface</b>	VLAN ID of layer 3 interface created
<b>IPv6 Address</b>	IPv6 Address, Example:2001::1234
<b>Prefix-length</b>	Prefix length is 3 to 127, Example :48
<b>Operation</b>	Action: Apply/Delete

## 1.4. Web Config

### 1.4.1. Web Timeout

The page is used to configure Web Login Timeout time. By default it is 10 minutes.

**Login Timeout**

Login Timeout	10	(1-60 minutes)
<input type="button" value="Apply"/>		

<b>Web Login Timeout</b>	Web Login Timeout: 1-60 minutes, default 10 minutes
--------------------------	---

### 1.4.2. HTTP

HTTP Server Config module, the user can start or stop the HTTP service of the switch by using this module again. By default it is on.

**HTTP Server Config**

	HTTP Server Status <input checked="" type="checkbox"/>
--	--

### 1.4.3. HTTPS

HTTPS Server Config module, the user can start or stop the HTTPS service of the switch by using this module again. By default it is off.

**HTTPS Config**

	HTTPS Status <input type="checkbox"/>
--	---------------------------------------

---

**HTTPS Config**

HTTPS Status	<input checked="" type="checkbox"/>	
HTTPS Protocol Port	443	(1025-65535,default 443)
Encryption Type	<input type="radio"/> aes256-sha <input type="radio"/> ecdhe-rsa-aes256-sha <input checked="" type="radio"/> all	
<input type="button" value="Apply"/>		

<b>HTTPS Protocol Port</b>	HTTPS Protocol Port: 1025-65535 ,default 443
<b>Encryption Type</b>	Type: aes256-sha ecdhe-rsa-aes256-sha

### 1.4.4. Security IP

Login user security IP configuration module, where users can configure the security IPv4 address for login switch. Login methods include Telnet/HTTP/HTTPS.

**Login User Security IP Set**

To configure the trusted IP address for Telnet and SSH and HTTP/HTTPS login method

Security IP Address

Example:10.10.10.1

Apply

No.	Login user Security IPv4 List
■	Delete

<b>Security IP address</b>	Fill in the specified security IPv4 address	
<b>Operation</b>	Apply	Add address or list number
	Delete	Delete address or list number

### 1.4.5. ACL

Login user login access control list module, where users can configure the IPV4 access control list. Login methods include Telnet/SSH/Web.

**Login Access Control List Set**

Configure standard IP ACL protocol binding through Telnet/SSH/Web login

Access Control List

(1-64 string or number 1-299)

Binding Method
Web
▼

Apply

	Access Control List	Binding Method
■	Delete	Delete

<b>IPv4 access control list</b>	Standard access control list number, scope 1-64 characters or number 1-99	
<b>Binding Method</b>	Binding Method include web/ssh/telnet/all	
<b>Operation</b>	Apply	Add address or list number
	Delete	Delete address or list number

## 1.5. User Management

### 1.5.1. User Management

User Management module, users in this module can add or delete user operations.

**User Management**

<b>Username</b>	<input type="text"/>	(1-32 characters)
<b>Password</b>	<input type="text"/>	<input type="checkbox"/> Encrypted Text (Plain Text:1-32 characters)
<b>Priority</b>	<input type="text"/>	(number 1-15)

☐	No.	Username	Password	State	Priority
<input type="checkbox"/>	1	abs	abcd1234	Plain Text	1
<input type="checkbox"/>	2	_uni7	miniadmin	Plain Text	7
<input type="checkbox"/>	3	user2	user2	Plain Text	7
<input type="checkbox"/>	4	user1	user1	Plain Text	1
<input type="checkbox"/>	5	admin	admin	Plain Text	15

**WEB Privilege Config**

<b>Login Privilege Enable</b>	<input type="button" value="Disabled"/> ▼
-------------------------------	---

<b>Username</b>	User name to operate ,1-32 characters
<b>Password</b>	User password, choose the password encryption, otherwise no encryption 1-32 characters
<b>Priority</b>	Used to specify permission level.

WEB Privilege Config module, users can configure permissions for user accounts to login in the web.

**WEB Privilege Config**

<b>Login Privilege Enable</b>	<input type="button" value="Disabled"/> ▼
<b>Privilege Priority</b>	<input type="button" value="15"/> ▼

<b>Login Privilege Enable</b>	Change the way users log in into web pages with permissions, When the user priority is lower than the privilege priority, it changes from being unable to log in to being able to log in to the web page but do not configure information, and can only view the configuration. By default it is disable.
<b>Privilege Priority</b>	Used to specify permission level, default level 15, only the user with the level that is equal to or higher than can login in the switch by web.

## 1.5.2. Authentication Method

User Login Authentication Method Configure 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 is from left to right when the login method is combined in 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 .A AA 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.

**User Login Authentication Method Configure**

<b>Login Method</b>	Console <span style="float: right;">▼</span>
<b>Authentication Method1</b>	None <span style="float: right;">▼</span>
<b>Authentication Method2</b>	None <span style="float: right;">▼</span>
<b>Authentication Method3</b>	None <span style="float: right;">▼</span>
<b>Operation Type</b>	Configuration <span style="float: right;">▼</span>

Apply

Login Method	Authentication Method1	Authentication Method2	Authentication Method3
console	local	None	None
vty	local	None	None
web	local	None	None

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.

Only when the console authentication mode is 'none', can the login authentication mode be configured.

<b>Login Authentication</b>	Disabled <span style="float: right;">▼</span>
<b>Login Authentication Password</b>	<input style="width: 80%;" type="password"/> <span style="float: right; font-size: small;">Encrypted Text (Plain Text:1-32 characters)</span>

Apply

<b>Login Authentication</b>	Default is Disable.
<b>Login Authentication Password</b>	Login Authentication password, choose the password encryption, otherwise no encryption of 1-32 characters.

## 1.6. Firmware Upgrade

### 1.6.1. TFTP 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.

TFTP Service	
Server IP Address	<input type="text"/> Example:10.10.10.1
Server File Name	<input type="text"/> 1-100 characters, Example: nos.img
Operation Type	Upload <input type="button" value="v"/>
Transmission Type	binary <input type="button" value="v"/>
<input type="button" value="Apply"/>	

<b>Server IP address</b>	TFTP address IP peer server, point decimal	
<b>Server File name</b>	Source name to upload or download ,1-100 characters	
<b>Operation type</b>	Upload	Upload upgrade files from the switch to the TFTP server
	Download	Download upgrade files from TFTP server to switch
<b>Transmission type</b>	binary	Transfer files in binary format (default)
	ascii	Transfer files in ascii format

### 1.6.2. FTP 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 Service	
Server IP Address	<input type="text"/> Example:10.10.10.1
Username	<input type="text"/> 1-100 characters
Password	<input type="text"/> 1-100 characters
Server File Name	<input type="text"/> 1-100 characters, Example: nos.img
Operation Type	Upload <input type="button" value="v"/>
Transmission Type	binary <input type="button" value="v"/>
<input type="button" value="Apply"/>	

<b>Server IP Address</b>	FTP address IP peer server, point decimal	
<b>Username</b>	FTP server-to-server username ,1-100 characters	
<b>Password</b>	FTP server-side user password 1-100 characters	
<b>Server File Name</b>	Source name to upload or download ,1-100 characters	
<b>Operation Type</b>	Upload	Upload upgrade files from the switch to the TFTP server

	Download	Download upgrade files from TFTP server to switch
<b>Transmission Type</b>	binary	Transfer files in binary format (default)
	ascii	Transfer files in ascii format

### 1.6.3. HTTP Upgrade

HTTP Upgrade module, the user can select file by HTTP way, and can upgrade the firmware of the switch by this method.

**Local Upgrade**

[Select File](#)

Decompress the package and select the img file for upgrade.

## 1.7. Management Config

### 1.7.1. TFTP

TFTP module, the user can import or export switch configuration by TFTP.

**Import Configuration**

<b>Server IP Address</b>	<input type="text"/>	<small>Example:10.10.10.1</small>
<b>Config File Name</b>	<input type="text"/>	<small>1-100 characters, Example: startup.cfg</small>
<b>Transmission Type</b>	binary ▼	

[Apply](#)

**Export Configuration**

<b>Server IP Address</b>	<input type="text"/>	<small>Example:10.10.10.1</small>
<b>File Type</b>	Running Configuration ▼	
<b>Config File Name</b>	<input type="text"/>	<small>1-100 characters, Example: startup.cfg</small>

[Apply](#)

<b>Server IP Address</b>	TFTP address IP peer server, point decimal	
<b>Server File Name</b>	Source name to upload or download ,1-100 characters	
<b>Transmission Type</b>	binary	Transfer files in binary format (default)
	ascii	Transfer files in ascii format

## 1.7.2. HTTP

HTTP module, the user can Download or Upload switch Running Configuration or Startup Configuration by http.

<b>Operation Type</b>	Download	To download files
	Upload	To upload files
<b>File Type</b>	Running Configuration	Switch running configuration
	Startup Configuration	Switch startup configuration

## 1.8. NTP

### 1.8.1. NTP Config

NTP Global Config module, user can configure NTP service global switch operation.

**NTP Global Config**

NTP Global Config  Off

<b>NTP Global Config Operation</b>	Off	Close operation(default)
	On	Start

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

**NTP Global Config**

NTP Global Config  On

**NTP Server Config**

Server Address	<input type="text"/>	IP address type,for example:10.10.10.1
Version	<input type="text"/>	Version Range:1-4 Default:4
Key ID(optional)	<input type="text"/>	Key ID Range:1-4294967295

Showing  Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	No.	Server Address	Version	Key ID
0 results found.				

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

## 1.8.2. NTP Authentication Config

The user can configure the switch NTP authentication related items in this module.

**NTP Authentication Config**

<b>NTP Authentication Function</b>	<input type="text" value="Disabled"/>	
<b>Key ID</b>	<input type="text"/>	Key ID Range:1-4294967295
<b>MD5 For Key ID</b>	<input type="text"/>	1-16 Characters

Showing  Entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	No.	Key ID	MD5 For Key ID
0 results found.			

<b>NTP authentication Function</b>	Disable	Close NTP validation (default)
	Enable	Enable NTP validation
<b>Key ID</b>	Secret key value, range 1-4294967295	
<b>MD5 For Key ID</b>	The MD5 value of the secret key, which ranges from 1-16 of ascii code	
<b>Operation</b>	Apply	Add operations
	Delete	Delete operations

## 1.9. SNTP

### 1.9.1. Server Config

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

**SNTP Server Config**

<b>Server Address</b>	<input type="text"/>	IP address type,for example:10.10.10.1
<b>Version</b>	<input type="text"/>	Version Range:1-4

<input type="checkbox"/>	No.	Server Address	Version	State
0 results found.				

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



## 1.9.2. Time Zone Config

**Time Zone Config**

Time Zone	UTC <small>(1-16 character)</small>		
Time Difference	<input checked="" type="radio"/> After-utc <input type="radio"/> Before-utc		
Time Value	05	30	<small>Range:0-23,0-59</small>
Operation Type	Add ▼		

**Apply**

SNTP 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.

<b>Time zone</b>	Time zone name ,1-16 characters			
<b>Time difference</b>	After-UTC	Increased time zone behavior		
	Before-UTC	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	
		Default	Restore time zone default configuration	

## 1.10. Device Management

### 1.10.1. Device Reboot/Reset

Device Reboot/Reset module, the user can restart the switch by **Reboot** button, can also leave the factory initial settings restart by **Reset** button, but also can save the current set configuration by **Save** button.

**Device Management**

Reboot	<b>Reboot</b>	Reboot the switch.
Default	<b>Reset</b>	Restore factory configuration and reboot the switch.
Save	<b>Save</b>	Save current device configure.

## 1.10.2. System Utilization

This module displays current CPU usage of system, also displays the current system's memory resource usage.

Show cpu usage	
Last 5 second CPU usage	7%
Last 30 second CPU usage	7%
Last 1 minute CPU usage	7%
Last 5 minute CPU usage	7%
From running CPU usage	8%

Show memory usage	
The memory total	512 MB
Free	431607808 Bytes
Usage	19.61%

## 1.10.3. View System Config

This module displays configuration information in the current system run.

```

Current System Operation Configuration
!
no service password-encryption
!
hostname Switch
sysLocation Default
sysContact Default
!
enable password level 1 0 orchid
enable password level 15 7 6ad14ba9986e3615423dfca256d04e3f
multi config access
!
username admin privilege 15 password 0 admin
username orchid password 0 orchid
username user123 privilege 15 password 0 user123
!
authentication line console login local
!
!
!
!
logging flash level debugging
!

```

### 1.10.4. View Logging Buffer

This module displays system logging information in the current system run.

```

System Buffer Log

Current messages in SDRAM:53
53 %Oct 17 10:37:26.770 2024 <warnings> DEFAULT[tNetInput]:KEEPALIVE-
UPDOWN: Ethernet keepalive gateway 172.16.100.1 up! with interface Vlan1!
52 %Oct 17 10:37:07.130 2024 <warnings> DEFAULT[tiPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
51 %Oct 17 10:37:06.130 2024 <warnings> MODULE_PORT[tphyDaemon]:%PORT-5-UPDOWN: Interface Ethernet1/0/2, changed state to UP
50 %Oct 17 10:36:56.350 2024 <warnings> DEFAULT[tiPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN
49 %Oct 17 10:36:55.360 2024 <warnings> MODULE_PORT[tphyDaemon]:%PORT-5-UPDOWN: Interface Ethernet1/0/2, changed state to DOWN
48 %Oct 17 10:36:27.450 2024 <warnings> DEFAULT[tiPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
47 %Oct 17 10:36:26.460 2024 <warnings> MODULE_PORT[tphyDaemon]:%PORT-5-UPDOWN: Interface Ethernet1/0/2, changed state to UP
46 %Oct 17 10:36:24.440 2024 <warnings> DEFAULT[tiPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN
45 %Oct 17 10:36:23.440 2024 <warnings> MODULE_PORT[tphyDaemon]:%PORT-5-UPDOWN: Interface Ethernet1/0/2, changed state to DOWN
44 %Oct 17 10:35:38.820 2024 <warnings> DEFAULT[tiPTimer]:KEEPALIVE-
UPDOWN: Ethernet keepalive gateway 172.16.100.1 down! with interface Vlan1!
43 %Oct 16 16:57:38.140 2024 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin logout from 172.16.100.16:42314.
42 %Oct 16 16:56:24.630 2024 <warnings> MODULE_UTILS_TELNET[subTelnetd1]:Telnet: User admin login successfully from 172.16.100.16:42314.
41 %Oct 17 03:18:37.830 2024 <warnings> DEFAULT[tNetInput]:KEEPALIVE-
UPDOWN: Ethernet keepalive gateway 172.16.100.1 up! with interface Vlan1!
40 %Oct 17 03:18:29.760 2024 <warnings> DEFAULT[tiPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP

```

### 1.10.5. View Logging Flash

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

```

System Flash Log

Allowed max messages:655,Current messages:655
655 %Sep 02 05:31:25.870 2024 <critical> DEFAULT[zIM]:System cold restart...
654 %Sep 02 00:00:00.000 2024 <critical> DEFAULT[tUusrRoot]:Switch is start, software version is QN_SW_QQ-2.4.09.02
653 %Sep 02 05:31:25.880 2024 <critical> DEFAULT[zIM]:System warm restart...
652 %Sep 02 05:31:16.550 2024 <critical> MODULE_UTILS_FILESYSTEM[zIM]:fs_write_file 1728: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
651 %Sep 02 05:31:16.520 2024 <critical> MODULE_UTILS_FILESYSTEM[zIM]:fs_write_file 1710: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
650 %Sep 02 00:00:00.000 2024 <critical> DEFAULT[tUusrRoot]:Switch is start, software version is QN_SW_QQ-2.4.09.02
649 %Oct 11 19:16:54.810 2024 <critical> DEFAULT[zIM]:System will be rebooted (warm reboot), reason: reload via CLI by admin
648 %Oct 11 19:16:51.390 2024 <critical> MODULE_UTILS_FILESYSTEM[zIM]:fs_write_file 1728: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
647 %Oct 11 19:16:51.350 2024 <critical> MODULE_UTILS_FILESYSTEM[zIM]:fs_write_file 1710: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/startup.cfg
646 %Oct 11 19:16:38.590 2024 <critical> MODULE_UTILS_FILESYSTEM[zIM]:fs_write_file 1728: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/boot_password
645 %Oct 11 19:16:38.380 2024 <critical> MODULE_UTILS_FILESYSTEM[zIM]:fs_write_file 1710: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/boot_password
644 %Sep 02 05:31:25.560 2024 <critical> DEFAULT[zIM]:System warm restart...
643 %Sep 02 00:00:00.000 2024 <critical> DEFAULT[tUusrRoot]:Switch is start, software version is QN_SW_QQ-2.4.09.02
642 %Oct 11 19:13:23.090 2024 <critical> DEFAULT[zIM]:System will be rebooted (warm reboot), reason: reload via CLI by admin
641 %Sep 02 05:31:25.550 2024 <critical> DEFAULT[zIM]:System warm restart...

```

## 2. Monitor Management

### 2.1. SSH Config

SSH Config module, the user can configure the SSH status and SSH timeout.

**SSH Config**

Enabled  Off

**SSH Config**

Enabled  On

**SSH Server Configuration**

<b>Timeout Time</b>	<input type="text" value="180"/>	(10-600s, Default:180s)
<b>Maximum Connection Number</b>	<input type="text" value="5"/>	(1-16, Default:5)

<b>Enabled Operation</b>	Off: Close operation(default)	
	On: Start	
<b>Timeout Time</b>	Timeout of exit SSH login status ,10-600 seconds(default 180 s)	
<b>Maximum Connection</b>	Maximum number of connections logged in by SSH, range 1-16(default 5)	
<b>Operation</b>	Apply	Add operations and apply.

### 2.2. Telnet Config

Telnet server status module, where users can enable on or off login switches by Telnet. Telnet connect the maximum number module, the user can configure the maximum number of connections to the switch by Telnet.

**Telnet Server State**

Enabled  On

**Maximum Connection**

<b>Telnet Connection Number</b>	<input type="text" value="5"/>	(1-16, Default:5)
---------------------------------	--------------------------------	-------------------

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

## 2.3. Port Statistics

This page displays port statistics information.

Port Statistics																	
	PORT	Link Status	Rate(Bps) (R/T)	Rate(pps) (R/T)	unicast packets (R/T)	multicast packets (R/T)	broadcast packets (R/T)	input errors	output errors	CRC (R)	frame alignment (R)	overrun (R)	ignored (R)	abort (R)	length error (R)	undersize (R)	jabber (R)
<input type="checkbox"/>	Ethernet1/0/1	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/2	Connected	20741/5692	28/1	3554.0/4461.0	44393.0/51.0	2903.0/6.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/3	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/4	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/5	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/6	Connected	31/19981	0/27	163.0/142.0	2.0/44394.0	1.0/2908.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/7	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/8	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/9	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/10	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/11	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/12	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/13	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/14	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/15	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/16	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/17	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/18	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0

<b>Port</b>	physical ports
<b>Link Status</b>	Link Status: Connected; Disconnect
<b>Rate(bps) (R/T)</b>	Rate(bps): Received/Transmit;
<b>Rate(pps) (R/T)</b>	Rate(pps): Received/Transmit;
<b>Unicast packets(R/T)</b>	Unicast packets: Received/Transmit;
<b>multicast packets(R/T)</b>	multicast packets: Received/Transmit;
<b>broadcast packets(R/T)</b>	broadcast packets: Received/Transmit;
<b>Input errors</b>	Input errors
<b>output errors</b>	Output errors
<b>CRC(R)</b>	CRC(Cyclic Redundancy Check) Received;
<b>frame alignment (R)</b>	Frame Alignment Received;
<b>overrun (R)</b>	Overrun Received;
<b>ignored (R)</b>	Ignored Received;
<b>abort (R)</b>	Abort Received;

<b>length error (R)</b>	Length error Received;
<b>undersize (R)</b>	Undersize Received;
<b>jabber (R)</b>	Jabber Received;
<b>fragments (R)</b>	Fragments Received;
<b>collisions (T)</b>	Collisions Transmit;
<b>late collisions (T)</b>	Late Collisions Transmit;
<b>pause frame (R/T)</b>	Pause Frame Received/Transmit;
<b>Refresh</b>	Refresh Port Statistics
<b>Delete</b>	Select the port and click delete to clear Port Statistics

## 2.4. DDMI Status

This page displays fiber module information.

Port	Vendor Name	Module Type	Tx Power (dBm)	Send power reference value(dBm)	Rx Power (dBm)	Received power reference value(dBm)	Temperature (°C)	Temperature reference value(°C)	Voltage (V)	Voltage reference value(V)	Bias (mA)	Current reference value(mA)
Ethernet1/0/25	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
Ethernet1/0/26	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
Ethernet1/0/27	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
Ethernet1/0/28	N/A	N/A	N/A	N/A	N/A	N/A	N/A					

[Refresh](#)

<b>Port</b>	fiber ports
<b>Temperature (°C)</b>	Display the temperature of the fiber module
<b>Bias (mA)</b>	Display the Bias of the fiber module.
<b>RX Power (dBm)</b>	Display the RX Power of the fiber module.
<b>TX Power (dBm)</b>	Display the TX Power of the fiber module.

## 2.5. Ping

The user can run ping command.

**Ping**

Server address

[Apply](#)

**Ping Result**

## 2.6. Traceroute

The user can run route tracking command.

**Traceroute**

Server address

**Traceroute Result**

## 2.7. Cable Diagnostics

This chapter can be used to detect port link lines.

To display the "Cable Diagnostics" page, click Monitor Management ->Cable Diagnostics, click "Apply" to configure.

Cable Diagnostics				
■	Port	Test Result	Description	Cable Length(meters)
<input type="checkbox"/>	Ethernet1/0/1	-	-	-
<input type="checkbox"/>	Ethernet1/0/2	-	-	-
<input type="checkbox"/>	Ethernet1/0/3	-	-	-
<input type="checkbox"/>	Ethernet1/0/4	-	-	-
<input type="checkbox"/>	Ethernet1/0/5	-	-	-
<input type="checkbox"/>	Ethernet1/0/6	-	-	-
<input type="checkbox"/>	Ethernet1/0/7	-	-	-
<input type="checkbox"/>	Ethernet1/0/8	-	-	-
<input type="checkbox"/>	Ethernet1/0/9	-	-	-
<input type="checkbox"/>	Ethernet1/0/10	-	-	-
<input type="checkbox"/>	Ethernet1/0/11	-	-	-
<input type="checkbox"/>	Ethernet1/0/12	-	-	-
<input type="checkbox"/>	Ethernet1/0/13	-	-	-
<input type="checkbox"/>	Ethernet1/0/14	-	-	-
<input type="checkbox"/>	Ethernet1/0/15	-	-	-
<input type="checkbox"/>	Ethernet1/0/16	-	-	-
<input type="checkbox"/>	Ethernet1/0/17	-	-	-
<input type="checkbox"/>	Ethernet1/0/18	-	-	-
<input type="checkbox"/>	Ethernet1/0/19	-	-	-
<input type="checkbox"/>	Ethernet1/0/20	-	-	-

Cable Diagnostics				
■	Port	Test Result	Description	Cable Length(meters)
<input type="checkbox"/>	Ethernet1/0/1	Disconnect	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 1 (3, 6) 2 (4, 5) 2 (7, 8) 2
<input type="checkbox"/>	Ethernet1/0/2	Normal	Normal(Correctly terminated pair)	(1, 2) 1 (3, 6) 1 (4, 5) 1 (7, 8) 1
<input type="checkbox"/>	Ethernet1/0/3	Disconnect	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 2 (7, 8) 2
<input type="checkbox"/>	Ethernet1/0/4	Disconnect	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 1 (3, 6) 2 (4, 5) 2 (7, 8) 1
<input type="checkbox"/>	Ethernet1/0/5	Disconnect	Please check whether the network cable is connected(Open pair,no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 2 (7, 8) 2
<input type="checkbox"/>	Ethernet1/0/6	Normal	Normal(Correctly terminated pair)	(1, 2) 1 (3, 6) 1 (4, 5) 1 (7, 8) 1

## 2.8. SNMP Config

### 2.8.1. Global Config

SNMP network management function switch module, users can enable or disable SNMP functions. SNMP Agent State and Trap state default is disabled in Security IP state.

SNMP Management	
Agent State	Disabled ▼
RMON	Disabled ▼
Trap	Disabled ▼
Security IP	Disabled ▼
<input type="button" value="Save"/>	

### 2.8.2. User Config

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

Users						
Username	<input type="text"/> (1-32 characters)					
Group Name	<input type="text"/> (1-32 characters)					
Security Level	noAuthNoPriv ▼					
IPv4 Access Control List	<input type="text"/> (1-64 characters)					
IPv6 Access Control List	<input type="text"/> (1-64 characters)					
<input type="button" value="Apply"/>						
User Configuration Status Table						
Showing 10 ▼ Entries	Showing 0 to 0 of 0 entries					
Search <input type="text"/>						
Username	Group Name	Security Level	Authentication Protocol	Privacy Protocol	IPv4 Access Control List	IPv6 Access Control List
0 results found.						
<input type="button" value="Delete"/>						
<input type="button" value="First"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Last"/>						

<b>Username</b>	User name to operate ,1-32 characters	
<b>Group Name</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 3 DES 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	

### 2.8.3. Group Config

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

**Groups**

Group Name	<input type="text"/>	(1-32 characters)
Security Level	noAuthNoPriv	▼
Read View	<input type="text"/>	(1-32 characters)
Write View	<input type="text"/>	(1-32 characters)
Notify View	<input type="text"/>	(1-32 characters)

[Apply](#)

---

**Snmp Group Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	Group Name	Security Level	Read View	Write View	Notify View
0 results found.					

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Group Name</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>	Apply	Add SNMP groups
	Delete	Delete SNMP groups

## 2.8.4. Community Config

The community management module where users can configure SNMP community management.

**Community Managers**

Community Name	<input type="text" value=""/>	(1-255 characters)
Access Priority	Readonly <span style="font-size: small;">▼</span>	

Add

---

**Community Managers Status Table**

	Community Name	Access Priority
--	----------------	-----------------

Delete

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

## 2.8.5. Trap Config

The trap config, where users can configure trap management settings.

**TRAP Manager Config**

TRAP Receiver	<input type="text" value=""/>	Example:1.1.1.5
Version	V1 <span style="font-size: small;">▼</span>	
Community Name	<input type="text" value=""/>	

Add

---

**TRAP Manager Status Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	TRAP Receiver	Community Name	Version	Security Level	Username
0 results found.					

First Previous Next Last

Delete

<b>Trap Receiver</b>	Recipient IPv4/IPv6 address of Trap information	
<b>Community Name</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
	Delete	For Trap information receiver remove operation

## 2.8.6. View Config

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

**Views**

SNMP View	<input type="text" value=""/>	(1-32 characters)
OID	<input type="text" value=""/>	Example:1.3.6.1.2.1.1.1
Type	<input type="text" value="Include"/>	

---

**View Table**

Showing  Entries Showing 1 to 3 of 3 entries Search

	SNMP View	OID	Type
	v1defaultviewname	1.0.	Include
	v1defaultviewname	1.2.	Include
	v1defaultviewname	1.3.	Include

<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>	Apply	Add view
	Delete	Delete View

SNMP EngineID configuration module, where user can configure SNMP EngineID operation in this module.

**SNMP EngineID Configuration**

EngineID	<input type="text" value="18c3586163FFD60B"/>	Example:18c30125fa
Operation Type	<input type="text" value="Configuration"/>	

<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)

## 2.8.7. Security IP Config

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

**Manager Security IP Configuration**

Security IP Address

Security IP Address

## 2.8.8. SNMP Statistics

SNMP statistics module displays the SNMP function feedback information.

SNMP Statistics	
<b>SNMP packets input</b>	<b>0</b>
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
<b>SNMP packets output</b>	<b>0</b>
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	0

## 2.9. RMON Config

### 2.9.1. RMON Statistics

RMON statistics displays RMON statistics.

RMON Statistics																	
■	Port	Drop Events	Octets	Packets	Received packets												
					Broadcast Packets	Multicast Packets	CRC Alignment Errors	Undersize Packets	Oversize Packets	Fragments Packets	Jabbers Packets	Collisions	1-64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets
<input type="checkbox"/>	Ethernet1/0/1	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
<input type="checkbox"/>	Ethernet1/0/2	0	18003113	183582	11195	164237	0	0	0	0	0	0	65075	105416	13472	3774	3049
<input type="checkbox"/>	Ethernet1/0/3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/6	0	49006	484	1	2	0	0	0	0	0	0	56914	101888	12923	3290	1332
<input type="checkbox"/>	Ethernet1/0/7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	Ethernet1/0/10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

## 2.9.2. RMON History Config

**RMON History Config**

History ID	<input type="text" value=""/>	(1-65535)
Port	<input type="text" value="Ethernet1/0/1"/>	
History Buckets	<input type="text" value=""/>	(1-65535, Default:50) <input type="checkbox"/> ?
History Interval	<input type="text" value=""/>	(1-3600, Default:1800) <input type="checkbox"/> ?
Owner	<input type="text" value=""/>	(1-31 characters) <input type="checkbox"/> ?

---

**History Entry Table**

	History ID	Port	History Buckets	History Interval	Owner
<input type="checkbox"/>					

<b>History ID</b>	Add History ID : 1-65535
<b>Port</b>	Select Ethernet Port
<b>History Buckets</b>	The maximum number of buckets, default is 50.
<b>History Interval</b>	The number of seconds for each sample, default is 1800.
<b>Owner</b>	Owner name of event <1-31> character.

## 2.9.3. RMON Event Config

**RMON Event Config**

Event ID	<input type="text" value=""/>	(1-65535)
Event Type	<input type="text" value="None"/>	
Event Description	<input type="text" value=""/>	(1-127 characters) <input type="checkbox"/> ?
Owner	<input type="text" value=""/>	(1-31 characters) <input type="checkbox"/> ?

---

**Event Entry Table**

	Event ID	Event Type	Event Community	Event Description	Last Sent	Owner
0 results found.						

<b>Event ID</b>	Add Event ID : range: 1-65535
<b>Event Type</b>	Select Event Type
<b>Event Description</b>	Write Event Description, you can add characters to 127.
<b>Owner</b>	owner name of event <1-31> character

## 2.9.4. RMON Alarm Config

RMON Alarm Config	
Alarm ID	<input type="text" value=""/> (1-65535)
Port	Ethernet1/0/1 <input type="button" value="v"/>
Sample Variable	Drop-Events <input type="button" value="v"/>
Sample Interval	<input type="text" value=""/> (1-2147483647s)
Sample Type	absolute <input type="button" value="v"/>
Alarm Type	Rising <input type="button" value="v"/>
Rising Threshold	<input type="text" value=""/> (1-2147483647)
Rising Event	<input type="text" value=""/> (1-65535)
Falling Threshold	<input type="text" value=""/> (1-2147483647)
Falling Event	<input type="text" value=""/> (1-65535)
Owner	<input type="text" value=""/> (1-31 characters) <input type="checkbox"/> <input data-bbox="917 788 941 817" type="button" value="?"/>
<input type="button" value="Add"/>	

Alarm Entry Table											
<input type="checkbox"/>	Alarm ID	Port	Sample Variable	Sample Interval	Sample Type	Alarm Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Owner
0 results found.											
<input type="button" value="Delete"/>											

<b>Alarm ID</b>	Add alarm ID : 1-65535
<b>Port</b>	Ethernet Port.
<b>Sample Variable</b>	Select the sample variable
<b>Sample Interval</b>	Sample interval, In seconds
<b>Sample Type</b>	Select sample type
<b>Alarm Type</b>	Select alarm type
<b>Rising Threshold</b>	threshold of rising
<b>Rising Event</b>	event index of rising
<b>Falling Threshold</b>	threshold of falling
<b>Falling Event</b>	event index of falling
<b>Owner</b>	owner name of alarm <1-31> character

## 2.10. Onvif Config

### 2.10.1. Server Config

Onvif server global switch configuration module, user can Onvif server global switch operation.

**Server Config**

Server Config  Off

<b>Server config Operation</b>	Off: Close operation(default)
	On: Start

### 2.10.2. Detect Config

Onvif detect Config module, Click the **Send** button to send an Onvif detection packet to discover the device.

**Detect Config**

	MAC Address	IP Address	Port	Model	Description	Location
<input type="checkbox"/>						
<input type="button" value="Send Package"/>		<input type="button" value="Delete"/>				

## 2.11. Loopback Detection

### 2.11.1. Port Mode

The configuration of the page is used to set the loop detection control method. To display the "Port Mode" page , click Monitor Management ->Loopback Detection->Port Mode, click "Apply" to configure.

**Port Mode**

Port	--Please select --
Loopback-detection Mode	No <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Port	Loopback-detection Mode
Ethernet1/0/1	No
Ethernet1/0/2	No
Ethernet1/0/3	No
Ethernet1/0/4	No
Ethernet1/0/5	No
Ethernet1/0/6	No
Ethernet1/0/7	No
Ethernet1/0/8	No
Ethernet1/0/9	No
Ethernet1/0/10	No
Ethernet1/0/11	No
Ethernet1/0/12	No
Ethernet1/0/13	No

<b>Port</b>	Ethernet port name
<b>Loopback-detection mode</b>	Operation in case of loop: No: no control mode Shutdown: Disable port block : Block port
<b>Operation</b>	Operation of loop detection function: Apply: Configure control mode

### 2.11.2. VLAN Loopback

This page can be used to configure VLAN loop detection function enabled or disabled. To display the "VLAN Loopback" page, click Monitor Management ->Loopback Detection->VLAN Loopback, click "Apply" to configure.

**VLAN Loopback**

<b>Port</b>	<input type="text" value="--Please select --"/>
<b>VLAN List</b>	<input type="text" value="(1-4094, for example: 1;3-6)"/>

Port	VLAN List
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	
Ethernet1/0/9	
Ethernet1/0/10	
Ethernet1/0/11	
Ethernet1/0/12	
Ethernet1/0/13	

<b>Port</b>	Ethernet port name
<b>VLAN ID</b>	VLAN ID, range 1-4094
<b>Operation</b>	Apply: Set VLAN loop detection

### 2.11.3. Interval Time

This page can be used to configure the loop detection interval. To display the "Interval Time" page, click Monitor Management ->Loopback Detection->Interval Time, click "Apply" to configure.

**Interval Time**

<b>Loopback-detection Interval Time</b>	<input type="text" value="5"/>	<small>(5-300s, Default:5s)</small>
<b>No Loopback-detection Interval Time</b>	<input type="text" value="3"/>	<small>(1-30s, Default:3s)</small>



<b>Loopback-detection interval time</b>	Interval time between loops, size 5-300 seconds, default is 5.
<b>No Loopback-detection interval time</b>	No loop interval, size 1-30 seconds, default is 3.
<b>Operation</b>	Configuration: Set the test time by yourself. Default: Restore the default configuration, there is a loop detection interval of 35 seconds, there is no loop detection interval of 15 seconds.

### 2.11.4. Recovery Timeout

This page is used to configure loop detection to automatically return to an uncontrolled state. To display the "Recovery Timeout" page, click Monitor Management ->Loopback Detection-> Recovery Timeout, click "Apply" to configure.

**Recovery Timeout**

Recovery Switch Timeout  (0-3600s, Default:600s)

<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. Default is 600
--------------------------------	---

## 2.12. LLDP Config

### 2.12.1. Global Config

This page can be configured to enable or disable LLDP functionality, configure the interval between sending updates, configure the value of the message aging time multiplier, configure the sending delay time of the update message, configure the interval between sending Trap messages.

**Global Config**

This page is used to configure global properties of the LLDP function

Status	<input type="text" value="Enabled"/>	
Hello Message Sending Time	<input type="text" value="30"/>	(5-32768),Default:30
Aging Multiple	<input type="text" value="4"/>	(2-10),Default:4
Delay Time ?	<input type="text" value="2"/>	(1-8192),Default:2
Trap Interval ?	<input type="text" value="5"/>	(5-3600),Default:5
Operation Type	<input type="text" value="Apply"/>	

<b>Status(lldp enable)</b>	Enable: Global On LLDP Function Disable: Global Off LLDP Function
<b>Hello Message Sending Time</b>	Update message sending interval between 5-32768 seconds. The default configuration is 30 seconds.
<b>Aging Multiple</b>	Numerical magnitude between 2-10, the default configuration is 4.
<b>Delay Time</b>	Value between 1-8192 seconds, the default configuration is 2
<b>Trap Interval</b>	Value between 5 and 3600 seconds, the default configuration is 5.
<b>Operation Type</b>	Apply: User self-configuration Default: Restore default configuration

## 2.12.2. Port Config

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

**Trust Config**

This page is used to set port attributes for the LLDP function

<b>Port</b>	<input type="text" value="--Please select --"/>				
<b>LLDP Enable</b>	<input type="text" value="Enabled"/>				
<b>Trap Enable</b>	<input type="text" value="Disabled"/>				
<b>Agent State</b>	<input type="text" value="both"/>				
<b>Operation Type</b> <span style="color: orange;">?</span>	<input type="text" value="Discard"/>				
<b>Entry Max</b> <span style="color: orange;">?</span>	<input type="text" value="100"/>	<span style="color: orange;">(5-500,Default:100)</span>			

Port	LLDP Enable	Trap Enable	Agent State	Operation Type	Entry Max
Ethernet1/0/1	Enabled	Disabled	Both	Discard	100
Ethernet1/0/2	Enabled	Disabled	Both	Discard	100
Ethernet1/0/3	Enabled	Disabled	Both	Discard	100
Ethernet1/0/4	Enabled	Disabled	Both	Discard	100
Ethernet1/0/5	Enabled	Disabled	Both	Discard	100

<b>Port</b>	Ethernet port name
<b>LLDP port Enable type</b>	Enable or disable LLDP functions
<b>LLDP port Trap enable type</b>	Enable or disable Trap functions
<b>LLDP mode</b>	Agent State: Send; Receive; Both; Disable;
<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
<b>LLDP neighbors max-num value</b>	Remote table maximum save entry size 5-500

### 2.12.3. TLV Config

This page can configure port TLV properties.

#### TLV Config

This page is used to set the properties of TLV

<b>Port</b>	<input type="text" value="--Please select --"/>	
<b>TLV Config</b>	<input type="text" value="--Please select --"/>	
<b>IP Address</b>	<input type="text" value="0.0.0.0"/>	Example:10.10.10.1 (0.0.0.0 is considered as not setting management address)

[Apply](#)

Port	TLV Config
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	
Ethernet1/0/9	
Ethernet1/0/10	

<b>Port</b>	Ethernet port name
<b>LLDP Port Description</b>	Port description name information needs to be configured
<b>LLDP System Capability</b>	Information describing system capabilities
<b>LLDP System Description</b>	Message describing the system
<b>LLDP System Name</b>	System name information

### 2.12.4. Neighbor Info

This page can be used to view Neighbor information in Neighbor Table.

#### Neighbor Info

This page is used to view information about other neighbors

#### Neighbor Table

Showing  Entries Showing 0 to 0 of 0 entries Search

Number	Local Port	Neighbor Device Name	Neighbor Interface	Neighbor Interface Description	Neighbor MAC	Neighbor IP	System Description
0 results found.							

[First](#)
[Previous](#)
[Next](#)
[Last](#)

# 3. Switch Config

## 3.1. Port Config

### 3.1.1. Port Config

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

To display the "Port Config" page, click Switch Config->Port Config->Port Config, click "Apply" to configure.

**Port Config**

This page is used to configure basic port parameters.

<b>Ports</b>	Ethernet1/0/1 <span style="float: right;">▼</span>
<b>Description</b>	<input type="text"/> (1-200 character) <input type="checkbox"/> <span style="color: orange;">?</span>
<b>Admin Status</b>	Enabled <span style="float: right;">▼</span>
<b>Speed</b>	Auto <span style="float: right;">▼</span> <span style="color: orange;">?</span>
<b>Duplex</b>	Auto <span style="float: right;">▼</span>
<b>Flow Control</b>	Disabled <span style="float: right;">▼</span> <span style="color: orange;">?</span>
<b>MDI</b>	auto <span style="float: right;">▼</span> <span style="color: orange;">?</span>

Apply

<b>Ports</b>	Select physical ports
<b>Port Alias</b>	Set port alias name, value 1-200
<b>Admin status</b>	Port status: Enabled Disabled
<b>Speed</b>	Port Speed: Auto,10M,100M,1000M
<b>Duplex</b>	Port Duplex: Auto, Half, Full
<b>Flow Control</b>	Port Flow Control: Disabled, Enabled
<b>MDI</b>	MDI: auto, across, normal, default is auto.

Port	Description	Admin Status	Speed/Duplex		Flow Control	MDI
			Config	Actual		
Ethernet1/0/1		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/2		Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/3		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/4		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/5		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/6		Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/7		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/8		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/9		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/10		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/11		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/12		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/13		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/14		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/15		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/16		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/17		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/18		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/19		Enabled	Auto/Auto	Link Down	Disabled	auto

<b>Port</b>	physical ports
<b>Port Alias</b>	Port alias description
<b>Admin status</b>	Port status: Enabled Disabled
<b>Speed</b>	Port rate: 10: 10M 100: 100M 1000: 1000M Auto: Automatic negotiation rate
<b>Duplex</b>	Duplex: Auto: Automatic negotiation mode Half: Half duplex mode Full: Full duplex mode
<b>Flow control</b>	Port Flow Control Status:
<b>MDI</b>	MDI: auto, across, normal, default is auto.

### 3.1.2. Port 10G Mode (Specific)

This page is mainly used to configure the basic of 10G ports.

**Port 10G Mode**

This page is used to configure 10G port mode.

<b>Ports</b>	Ethernet1/0/25 ▼
<b>Port 10G Mode</b>	dac-50cm ▼

[Apply](#)

Ports	Port 10G Mode
Ethernet1/0/25	fiber-auto
Ethernet1/0/26	fiber-auto
Ethernet1/0/27	fiber-auto
Ethernet1/0/28	fiber-auto

<b>Port</b>	Select physical ports
<b>Port 10G Mode</b>	dac-50cm: DAC 50cm dac-100cm: DAC 100cm dac-300cm: DAC 300cm dac-500cm: DAC 500cm fiber-10g: Fiber forced 10G fiber-1g: Fiber forced 1G fiber-2500M: Fiber forced 2500M fiber-auto: Fiber Auto mode

### 3.2. Port Mirror

This section can be used for port mirroring function configuration.

To display the "Port Mirror" page, click Switch Config ->Port Mirror, click "Apply" to configure.

**Port Mirror**

This page is used to configure port mirror.

<b>Session ID</b>	1 ▼
<b>Destination Port</b>	Ethernet1/0/1 ▼
<b>Source Port</b>	--Please select --
<b>CPU Source</b>	Disabled ▼
<b>Access List</b>	<input type="text" value=""/> (1-7999)
<b>Mirror Direction</b>	rx ▼

[Apply](#)

Port Mirror Table					
■	Session ID	Destination Port	Source Port		Access List
			Tx	Rx	
<input type="checkbox"/>	1				
<input type="checkbox"/>	2				
<input type="checkbox"/>	3				
<input type="checkbox"/>	4				

[Delete](#)

<b>Session</b>	Mirror Session
<b>Destination port</b>	Mirror destination port
<b>Source port</b>	Mirror Source Port
<b>CPU Source</b>	CPU Source: Disabled Enabled
<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

### 3.3. Port Isolate

This page is mainly used to configure the port isolation.

Port Isolation Configuration			
This page is used to configure port isolate.			
<b>Isolate-Port Group Name</b>	<input type="text"/> (1-32 character)		
<b>Isolation Ports</b>	--Please select --		
<b>VLAN</b>	<input type="text"/> (1-4094, for example: 8,default not create in vlan)		
<a href="#">Add</a>			
Port Isolation Table			
■	VLAN	Isolate-Port Group Name	Isolation Ports
<a href="#">Delete</a>			

<b>Isolate-Port Group Name</b>	The name of isolate-port Group, value 1-32 characters
<b>Isolation Ports</b>	Select isolation ports to add isolate group

### 3.4. Port Channel

#### 3.4.1. Port Channel Group

This section can be used to create convergent groups.

To display the "Port Channel Group" page, click Port channel -> Port Channel Group, click "Apply" to configure.

**Port Channel**

This page is used to configure port channel.

Load Balance Alogorithm src-mac ▼

Apply

LAG	<input type="text"/>	(1-64)
Name	<input type="text"/>	(1-200 character)
Mode	<span style="border: 1px solid #ccc; padding: 2px 10px;">on</span> ▼	
State	<span style="border: 1px solid #ccc; padding: 2px 10px;">Enabled</span> ▼	
Member Port	<span style="border: 1px solid #ccc; padding: 2px 10px;">--Please select --</span>	

Apply

<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>src-dst-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> <p><b>ingress-port :</b> ingress port.</p>
<b>LAG</b>	To create a convergent group number, value 1-8.
<b>Name</b>	The name of LAG group, value 1-32 character
<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>
<b>State</b>	<p>Enabled</p> <p>Disabled</p>
<b>Member Port</b>	Ethernet port name



### 3.4.2. LACP

This page is available with setting system priority and port priority.  
To display the "LACP" page, click Switch Config -> Port channel->LACP,

LACP

This page is used to configure port channel LACP.

<b>System Priority</b>	<input type="text" value="32768"/>	(0-65535, default 32768)
------------------------	------------------------------------	--------------------------

<b>Port</b>	<input type="text" value="--Please select --"/>
-------------	---

<b>Port Priority</b>	<input type="text"/>	(0-65535, default 32768)
----------------------	----------------------	--------------------------

<b>Timeout</b>	<input type="text" value="long"/>
----------------	-----------------------------------

LACP Port Setting Table

	Port	Status	Port Priority	FLAG <span style="color: #a00; font-size: 0.8em;">?</span>
<input type="button" value="Delete"/>				

### 3.5. Jumbo Frame

This page is used to configure Jumbo Frame.

Jumbo Frame Configuration

This page is used to configure Jumbo Frame!

<b>Jumbo Frame Size</b>	<input type="text" value="1500"/>	1500-12270 (Unit: Bytes)
-------------------------	-----------------------------------	--------------------------

<b>Status</b>	Disabled(default) Enabled
<b>Jumbo Frame Size(Unit: Bytes)</b>	Size 1500-12270, default is 1500.

### 3.6. Port Rate

The page is configured for Port Rate.

To display the "Port Rate" page, click Switch Config -> Port Rate, click "Apply" to configure.

**Port Rate**

This page is used to configure port rate.

<b>Ports</b>	<input type="text" value="--Please select --"/>	
<b>Limit Type</b>	<input type="text" value="Ingress"/>	<input type="text" value="v"/>
<b>Status</b>	<input type="text" value="Disabled"/>	<input type="text" value="v"/>
<b>Rate(Kbps)</b>	<input type="text" value="No Limit"/>	1-1000000

<b>Ports</b>	Ethernet port name
<b>Limit Type</b>	Limit type: Egress: send Ingress : receive All: send and receive
<b>Status</b>	Disabled Enabled
<b>Rate</b>	Bandwidth control rate in the range of Kbps 1-1000000

Port	EgressRate(Kbps)	IngressRate(Kbps)
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
Ethernet1/0/9	1000000	1000000
Ethernet1/0/10	1000000	1000000
Ethernet1/0/11	1000000	1000000
Ethernet1/0/12	1000000	1000000
Ethernet1/0/13	1000000	1000000
Ethernet1/0/14	1000000	1000000
Ethernet1/0/15	1000000	1000000
Ethernet1/0/16	1000000	1000000
Ethernet1/0/17	1000000	1000000
Ethernet1/0/18	1000000	1000000
Ethernet1/0/19	1000000	1000000
Ethernet1/0/20	1000000	1000000

<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>Egress bandwidth threshold(Kb)</b>	Displays the bandwidth limit of the current sending data, ranging from 1-1000000kbps.

### 3.7. Storm Control

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

To display the "Storm Control" page, click Switch Config -> Storm Control, click "Apply" to configure.

**Storm Control**

This page is used to configure storm control.

<b>Ports</b>	--Please select --	
<b>Type</b>	Broadcast	▼
<b>Status</b>	Disabled	▼
<b>Rate(Kbits)</b>	No Limit	1-1000000

[Apply](#)

<b>Port</b>	Ethernet port name
<b>Type</b>	Broadcast/Multicast/Unicast
<b>Status</b>	Disabled: Disable Storm Control Enabled: Turn on the storm control function and configure the speed limit
<b>Rate</b>	storm control rate, ranging from 1-1000000 kbps or pps 1-1488095

Port	Broadcast	Unknown Multicast	Unknown Unicast
Ethernet1/0/1	Disabled	Disabled	Disabled
Ethernet1/0/2	Disabled	Disabled	Disabled
Ethernet1/0/3	Disabled	Disabled	Disabled
Ethernet1/0/4	Disabled	Disabled	Disabled
Ethernet1/0/5	Disabled	Disabled	Disabled
Ethernet1/0/6	Disabled	Disabled	Disabled
Ethernet1/0/7	Disabled	Disabled	Disabled
Ethernet1/0/8	Disabled	Disabled	Disabled
Ethernet1/0/9	Disabled	Disabled	Disabled
Ethernet1/0/10	Disabled	Disabled	Disabled
Ethernet1/0/11	Disabled	Disabled	Disabled
Ethernet1/0/12	Disabled	Disabled	Disabled
Ethernet1/0/13	Disabled	Disabled	Disabled
Ethernet1/0/14	Disabled	Disabled	Disabled
Ethernet1/0/15	Disabled	Disabled	Disabled
Ethernet1/0/16	Disabled	Disabled	Disabled
Ethernet1/0/17	Disabled	Disabled	Disabled
Ethernet1/0/18	Disabled	Disabled	Disabled
Ethernet1/0/19	Disabled	Disabled	Disabled
Ethernet1/0/20	Disabled	Disabled	Disabled

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

## 3.8. MAC Address Config

### 3.8.1. Static MAC

Configure Static MAC addresses, and establish the mapping relationship between MAC addresses and ports and VLANs.

**MAC Address Config**

<b>MAC Address</b>	<input type="text" value="00-00-00-00-00-00"/>
<b>VLAN ID</b>	<input style="border: none; border-bottom: 1px solid #ccc; background-color: #f0f0f0; width: 100%;" type="text" value="VLAN0001"/>
<b>Port</b>	<input style="border: none; border-bottom: 1px solid #ccc; background-color: #f0f0f0; width: 100%;" type="text" value="Ethernet1/0/1"/>

---

**Static MAC List**

Showing  Entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	No.	MAC Address	VLAN ID	Port
0 results found.				

<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</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

### 3.8.2. Black Hole MAC

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

**Black Hole MAC**

<b>MAC Address</b>	<input type="text" value="00-00-00-00-00-00"/>
<b>VLAN ID</b>	<input style="border: none; border-bottom: 1px solid #ccc; background-color: #f0f0f0; width: 100%;" type="text" value="VLAN0001"/>

---

**Black Hole MAC List**

Showing  Entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	No.	MAC Address	VLAN ID
0 results found.			

<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
	Delete	Delete the mapping relationship of the specified MAC address, VLAN, and port

Blackhole MAC list shows current existing MAC address, port, and VALN mapping relationship.

### 3.8.3. Aging-time

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.

**Aging-time**

Aging-time	300	(10-1000000)Second, default is 300, 0:No Aging
------------	-----	--

<b>MAC address Aging-time</b>	The aging time range is 10-1000000, 0 means no aging	
<b>Operation</b>	Apply	Set the aging time into the switch

### 3.8.4. MAC Address List

Quickly query the MAC address in the switch.

MAC Address List				
Showing	10	Entries	Showing 1 to 10 of 23 entries	Search <input type="text"/>
VLAN ID	MAC Address	Type	Creator	Port
1	00-45-E2-F7-EB-B1	DYNAMIC	Hardware	Ethernet1/0/2
1	08-8F-C3-B6-39-5F	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-00-1C-88	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-00-C1-61	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-00-C1-80	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-00-C6-C1	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-00-C6-E0	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-01-09-21	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-01-09-40	DYNAMIC	Hardware	Ethernet1/0/2
1	58-61-63-02-39-E5	DYNAMIC	Hardware	Ethernet1/0/2

<b>VLAN ID</b>	The created VLAN ID, showing the address in the VLAN
<b>MAC Address</b>	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx
<b>Type</b>	MAC address type
<b>Creator</b>	MAC address creator
<b>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.

### 3.9. AM

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

#### Access Manage(AM)

Through the port binding feature of AM access management, network administrators can bind legitimate user IP (MAC-IP) addresses to specified ports. After the binding operation, only messages sent by users with specified IP (MAC-IP) addresses can be forwarded through this port, enhancing users' monitoring of network security.

<b>Port</b>	<input type="text" value="--Please select --"/>
<b>Binding Type</b>	<input type="text" value="IP"/>
<b>IP Address</b>	<input type="text"/>
<b>Number</b> <span style="color: #e67e22;">?</span>	<input type="text" value="1"/>

---

#### AM Configuration Table

Showing	10	Entries	Showing 0 to 0 of 0 entries	Search <input type="text"/>	
<input type="checkbox"/>	Port	Binding Type	MAC Address	IP Address	Number
0 results found.					
<input type="button" value="Delete"/>					<input type="button" value="First"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Last"/>

<b>Port</b>	Designated port number
<b>Binding Type</b>	Select IP or MAC-IP method
<b>IP address</b>	Beginning IP address, decimal point
<b>Number</b>	Number of consecutive addresses after starting IP address ,1-32
<b>MAC address</b>	Source MAC address

### 3.10. AAA

#### 3.10.1. Radius

Radius Global Configuration module, users in this module can configure the global Radius function services.

**Radius Global Configuration**

The user priority for Radius authentication login is 1

<b>Key Type</b>	<input type="text" value="Plain Key"/>	
<b>Radius Global Key</b>	<input type="text"/>	1-64Characters
<b>System Recovery Time</b>	<input type="text" value="5"/>	Range:1-255(Min),Default:5
<b>Radius Retransmit Times</b>	<input type="text" value="3"/>	Range:0-100,Default:3
<b>Radius Server Timeout</b>	<input type="text" value="3"/>	Range:1-1000(Sec),Default:3

Radius Global Information				
Key Type	Radius Global Key	System Recovery Time	Radius Retransmit Times	Radius Server Timeout
Plain Key		5	3	3

<b>Key Type</b>	Plain Key: 1-64 character
	Cipher Key: 1-64 character, input plaintext application to encrypt cipher text.
<b>Radius Global Key</b>	Key string, 1-64 characters, select Use default and click Apply can set Radius Key default.
<b>System Recovery Time</b>	Radius service recovery time from downtime to accessibility, 1-255 minutes, and default is 5.
<b>Radius Retransmit Times</b>	Radius authentication packet retransmission time, 1-100 seconds, default is 3.
<b>Radius Server Timeout</b>	The corresponding time of the radius server, 1-1000 seconds, and default is 3.

Radius Authentication Configuration module, users in this module can configure the Radius authentication server.

### Radius Authentication Server Configuration

Authentication Server IP	<input type="text"/>	IPv4 or IPv6 address
Authentication Server Port(optional)	<input type="text"/>	Range:0-65535
Key Type	Plain Key <span style="float: right;">▼</span>	
Radius Key(optional)	<input type="text"/>	1-64Characters
Access Mode	None <span style="float: right;">▼</span>	
Primary Authentication Server	Non-primary authentication server <span style="float: right;">▼</span>	

[Apply](#)

Showing 10 Entries Showing 0 to 0 of 0 entries Search

NO.	Server IP Address	Port Number	Primary Server	Key Type	Radius Key	Access Mode
0 results found.						
<a href="#" style="background-color: #004a99; color: white; padding: 5px 15px; border-radius: 3px;">Delete</a>						
<a href="#" style="background-color: #004a99; color: white; padding: 2px 5px; border-radius: 3px;">First</a> <a href="#" style="background-color: #004a99; color: white; padding: 2px 5px; border-radius: 3px;">Previous</a> <a href="#" style="background-color: #004a99; color: white; padding: 2px 5px; border-radius: 3px;">Next</a> <a href="#" style="background-color: #004a99; color: white; padding: 2px 5px; border-radius: 3px;">Last</a>						

<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>Key Type</b>	Plain Key: 1-64 character	
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.	
<b>Radius Key</b>	Key string ,1-64 characters	
<b>Access Mode</b>	None: All services can use current RADIUS server by default	
	Telnet: RADIUS server only use telnet authentication	
	Dot1x: RADIUS server only use 802.1x authentication	
	Wireless: RADIUS server only use wireless authentication	
<b>Primary Authentication Server</b>	Primary authentication server	Specify radius server as primary accounting server
	Non-Primary authentication server	Specify radius server as non-primary accounting server



### 3.10.2. Radius Accounting

Radius authentication and accounting module, users in this module can configure the Radius billing server.

**Radius Accounting Server Configuration**

<b>Accounting Server IP</b>	<input type="text"/>	IPv4 or IPv6 address
<b>Authentication Server Port(optional)</b>	<input type="text"/>	Range:0-65535
<b>Key Type</b>	Plain Key <span style="float: right;">▼</span>	
<b>Radius Key(optional)</b>	<input type="text"/>	1-64Characters
<b>Primary Authentication Server</b>	Non-primary authentication server <span style="float: right;">▼</span>	

[Apply](#)

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	NO.	Server IP Address	port number	Key Type	Radius Key	Primary Server
0 results found.						

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<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>Key Type</b>	Plain Key: 1-64 character	
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.	
<b>Radius Key</b>	Key string ,1-64 characters	
<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

### 3.10.3. Tacacs

Tacacs global configuration module, users in this module can configure the global Tacacs function services.

#### Tacacs Global Configuration

The user priority for Tacacs authentication login is 1

<b>Key Type</b>	Plain Key <span style="font-size: small;">▼</span>	
<b>Tacacs Global Key</b>	<input type="text"/>	1-64 Characters
<b>Tacacs Server Global Timeout</b>	<input type="text" value="3"/>	Range:1-60(Sec),Default:3

[Apply](#)

Tacacs Global Information		
Key Type	Tacacs Global Key	Tacacs Server Global Timeout
Cipher Key	BZKXC9U5zUy7UPJV+x6UEA==	3

<b>Key Type</b>	Plain Key: 1-64 character Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.
<b>Tacacs Global Key</b>	Tacacs authentication global key ,1-64 characters
<b>Tacacs Server Global Timeout</b>	Tacacs authentication timeout ,1-60 seconds, default 3 seconds

Tacacs server configuration module, users in this module can configure the Tacacs authentication server.

#### Tacacs Authentication Server Configuration

<b>Authentication Server IP</b>	<input type="text"/>	IPv4 or IPv6 address
<b>Authentication Server Port(optional)</b>	<input type="text"/>	Range:0-65535
<b>Key Type</b>	Plain Key <span style="font-size: small;">▼</span>	
<b>Tacacs Key(optional)</b>	<input type="text"/>	1-64Characters
<b>Tacacs Server Timeout(optional)</b>	<input type="text"/>	Range:1-60(Sec),Default:3
<b>Primary Authentication Server</b>	Non-primary authentication server <span style="font-size: small;">▼</span>	

[Apply](#)

Showing  Entries
Showing 1 to 2 of 2 entries
Search

	NO.	Server IP Address	port number	Primary Server	Key Type	Tacacs Key	Tacacs Server Timeout
<input type="checkbox"/>	1	192.168.100.1	49	No	Cipher Key	BZKXC9U5zUy7UPJV+x6UEA==	
<input type="checkbox"/>	2	192.168.200.1	49	No	Cipher Key	BZKXC9U5zUy7UPJV+x6UEA==	

[Delete](#)

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

<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>Key Type</b>	Plain Key: 1-64 character	
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.	
<b>Tacacs Key</b>	Configure tacacs+ server encryption key 1-64 Characters	
<b>Tacacs Server Timeout</b>	Configure the tacacs+ server authentication time Interval <1-60> seconds. Default is 3.	
<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

### 3.10.4. Dot1x

**Dot1x Config**

Enable  Off

---

**Dot1x Config**

Enable  On

**Dot1x Port Config**

<b>Port</b>	<input type="text" value="--Please select --"/>
<b>Dot1x</b>	<input type="text" value="Disabled"/>
<b>Port Method</b>	<input type="text" value="Port"/>

Port	Dot1x	Port Method
Ethernet1/0/1	Disabled	Advanced User Access
Ethernet1/0/2	Disabled	Advanced User Access
Ethernet1/0/3	Disabled	Advanced User Access
Ethernet1/0/4	Disabled	Advanced User Access
Ethernet1/0/5	Disabled	Advanced User Access
Ethernet1/0/6	Disabled	Advanced User Access
Ethernet1/0/7	Disabled	Advanced User Access
Ethernet1/0/8	Disabled	Advanced User Access

<b>Port</b>	Ethernet Port Name.
<b>Dot1x</b>	Enable or Disable Dot1x.
<b>Port Method</b>	Select Port Method.

### 3.10.4. DNS Config

**DNS Config**

Enable  Off

**DNS Server Config**

<b>DNS Server Address</b>	<input type="text"/>	Example:10.10.10.1 or 2001::1234
<b>Priority</b>	<input type="text"/>	Priority:0-255

<input type="checkbox"/>	No.	DNS Server Address	Priority
<input type="button" value="Delete"/>			

<b>DNS Server Address</b>	Add DNS server address
<b>Priority</b>	Priority : 0-255

# 4. VLAN Config

## 4.1. VLAN Config

### 4.1.1. VLAN ID

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

**VLAN Configuration Management**

VLAN ID  (1-4094, for example: 1;3-6)

VLAN Name

**Add**

Showing  Entries

Showing 1 to 2 of 2 entries

Search

	No.	VLAN ID	VLAN Name
<input type="checkbox"/>	1	1	default
<input type="checkbox"/>	2	10	VLAN0010 ?

**Delete**

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

<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>Operation</b>	Add	Add VLAN
	Delete	Remove VLAN

### 4.1.2. Show VLAN

Show VLAN function module displays list of VLANs.

**Show VLAN List**

Showing  Entries

Showing 1 to 2 of 2 entries

Search

VLAN ID	Name	Type	Media	Ports
1	default	Static	ENET	Ethernet1/0/1, Ethernet1/0/2 Ethernet1/0/3, Ethernet1/0/4 Ethernet1/0/5, Ethernet1/0/6 Ethernet1/0/7, Ethernet1/0/8 Ethernet1/0/9, Ethernet1/0/10 Ethernet1/0/11, Ethernet1/0/12 Ethernet1/0/13, Ethernet1/0/14 Ethernet1/0/15, Ethernet1/0/16 Ethernet1/0/17, Ethernet1/0/18 Ethernet1/0/19, Ethernet1/0/20 Ethernet1/0/21, Ethernet1/0/22 Ethernet1/0/23, Ethernet1/0/24 Ethernet1/0/25, Ethernet1/0/26 Ethernet1/0/27, Ethernet1/0/28
10	VLAN0010	Static	ENET	

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

### 4.1.3. Port Config

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

**Port Mode Configure**

<b>Ports</b>	--Please select --	
<b>Mode</b>	Access ▼	
<b>Native Vlan</b>	VLAN0001 ▼	
<b>Ingress Check</b>	Enabled ▼	
<b>Tagged VLAN</b>	Range(1-4094)	Example 1-3;8
<b>UnTagged VLAN</b>	Range(1-4094)	Example 1-3;8

Apply

Port	Mode	Native Vlan	Ingress Check	Tag Vlan List	Untag Vlan List
Ethernet1/0/1	Access	VLAN0001	Enabled	-	-
Ethernet1/0/2	Access	VLAN0001	Enabled	-	-
Ethernet1/0/3	Access	VLAN0001	Enabled	-	-
Ethernet1/0/4	Access	VLAN0001	Enabled	-	-
Ethernet1/0/5	Access	VLAN0001	Enabled	-	-
Ethernet1/0/6	Access	VLAN0001	Enabled	-	-

<b>Port</b>	Port name	
<b>Mode</b>	Access	
	Trunk	
	Hybrid	
<b>Native Vlan</b>	Port PVID	
<b>Ingress Check</b>	Enabled	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
	Disabled	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
<b>Tagged VLAN</b>	Tag VLAN range 1-4094,example 1-3;8	
<b>Untagged VLAN</b>	Untag VLAN range 1-4094,example 1-3;8	

## 4.2. GVRP Config

### 4.2.1. GVRP Config

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

**GVRP Config**  
 Enabled  Off

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

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

**GVRP Config**

<b>Enabled</b>	<input checked="" type="radio"/>	
<b>Join Timer</b>	<input type="text" value="200"/>	Range:200-500 milli-second, default is 200
<b>Leave Timer</b>	<input type="text" value="600"/>	Range:500-1200 milli-second, default is 600
<b>Leaveall Timer</b>	<input type="text" value="10000"/>	Range:5000-60000 milli-second, default is 10000

<b>Join timer</b>	200-500ms	
<b>Leave timer</b>	500-1200ms	
<b>Leaveall timer</b>	500-60000ms	
<b>Operation</b>	Apply	Modify the value of the timer

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

**Enable GVRP On Port**

Enable the port will not be able to change the port mode!

**Ports**

Only display ports that enable gvrp.

Showing  Entries Showing 0 to 0 of 0 entries

	Port	GVRP Status
0 results found.		

## 4.2.2. GVRP Port

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

**Enable GVRP On Port**

Enable the port will not be able to change the port model!

Ports

[Apply](#)

Only display ports that enable gvrp.

Showing  Entries
Showing 0 to 0 of 0 entries
Search

<input type="checkbox"/>	Port	GVRP Status
0 results found.		

[First](#)
[Previous](#)
[Next](#)
[Last](#)

[Delete](#)

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

## 4.3. QINQ

### 4.3.1. Enable Dot1q Tunnel

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

**Enable Dot1q Tunnel**

Ports

[Apply](#)

Showing  Entries
Showing 0 to 0 of 0 entries
Search

<input type="checkbox"/>	Port	Status
0 results found.		

[First](#)
[Previous](#)
[Next](#)
[Last](#)

[Delete](#)

<b>Port</b>	Port name	
<b>Operation</b>	Apply	Enable dot1q tunnel
	Delete	Disable dot1q tunnel



### 4.3.2. Dot1q Tunnel TPID

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

**Configure Dot1q Tunnel TPID**

Only configure for QINQ disable port.

<b>Ports</b>	<input type="text" value="--Please select --"/>
<b>Protocol</b>	<input type="text" value="0x8100"/>
<b>Protocol ID</b>	<input type="text" value="Range:1-65535"/>

Port	Protocol
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	
Ethernet1/0/9	

<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	

## 4.4. Voice VLAN

### 4.4.1. VLAN Config

The voice vlan configure module, the user can select vlan to enable voice vlan.

**Voice VLAN Configure**

Voice VLAN

<b>Voice VLAN</b>	Select VLAN to enable voice VLAN
-------------------	----------------------------------

The voice OUI configure module, the user can set voice OUI.

### Voice VLAN Configure

Voice VLAN

VLAN0001

Apply

### Voice OUI Configure

MAC address	MAC Mask	Priority	Name
<input style="width: 90%;" type="text" value="00-00-00-00-00-00"/>	<input style="width: 90%;" type="text" value="FF-FF-FF-FF-FF-FF"/>	<input style="width: 90%;" type="text" value="Range:0-7"/>	<input style="width: 90%;" type="text" value="Up to 15 characters."/>

Add

Showing 10 Entries
Showing 0 to 0 of 0 entries
Search

	No.	Name	MAC address	MAC Mask	Priority
0 results found.					

Delete

First
Previous
Next
Last

<b>MAC Address</b>	The voice equipment MAC address, shown in xx-xx-xx-xx-xx-xx format.
<b>MAC Mask</b>	The last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, 0x0
<b>Priority</b>	The priority of the voice traffic, the valid range is 0-7
<b>Name</b>	The voice-name is the name of the voice equipment, which is to facilitate the equipment management

#### 4.4.2. Port Config

The voice vlan port Config module, the user can select port to enable voice vlan.

### Port Config

Ports

--Please select--

Status

Enabled

Apply

Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(A)	Enabled
Ethernet1/0/3(A)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/6(A)	Enabled
Ethernet1/0/7(A)	Enabled
Ethernet1/0/8(A)	Enabled
Ethernet1/0/9(A)	Enabled
Ethernet1/0/10(A)	Enabled
Ethernet1/0/11(A)	Enabled
Ethernet1/0/12(A)	Enabled
Ethernet1/0/13(A)	Enabled

<b>Port</b>	Port name	
<b>Status</b>	Enable	Enable voice vlan
	Disable	Disable voice vlan

## 4.5. MAC VLAN

### 4.5.1. VLAN Config

The vlan configure module, the user can select vlan to add mac vlan.

**VLAN Config**

MAC VLAN

[Add](#)

Showing  Entries Showing 0 to 0 of 0 entries Search

No.	MAC VLAN	VLAN Name
0 results found.		

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>MAC VLAN</b>	Select vlan to add mac vlan
-----------------	-----------------------------

### 4.5.2. VLAN Member

The MAC VLAN Configure module, the user can set mac vlan.

**MAC VLAN Configure**

<b>MAC address</b>	<input style="width: 100%;" type="text" value="00-00-00-00-00-00"/>
<b>MAC Mask</b>	<input style="width: 100%;" type="text" value="FF-FF-FF-FF-FF-FF"/>
<b>VLAN ID</b>	<input style="width: 100%;" type="text" value="VLAN0010"/>
<b>Priority</b>	<input style="width: 100%;" type="text" value="Range:0-7"/>

[Add](#)

Showing  Entries Showing 0 to 0 of 0 entries Search

No.	MAC address	MAC Mask	VLAN ID	Priority
0 results found.				

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>MAC address</b>	The voice equipment MAC address, shown in xx-xx-xx-xx-xx-xx format.
<b>MAC Mask</b>	The last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, 0x0
<b>Priority</b>	The priority of the voice traffic, the valid range is 0-7
<b>Name</b>	The voice-name is the name of the voice equipment, which is to facilitate the equipment management

### 4.5.3. Port Config

The mac vlan port Config module, the user can select port to enable mac vlan.

**Port Config**

<b>Ports</b>	--Please select --
<b>Status</b>	Enabled <span style="float: right;">▼</span>

[Apply](#)

Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(A)	Enabled
Ethernet1/0/3(A)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/6(A)	Enabled
Ethernet1/0/7(A)	Enabled
Ethernet1/0/8(A)	Enabled
Ethernet1/0/9(A)	Enabled
Ethernet1/0/10(A)	Enabled
Ethernet1/0/11(A)	Enabled

<b>Port</b>	Port name	
<b>Status</b>	Enable	Enable mac vlan
	Disable	Disable mac vlan

### 4.6. Protocol VLAN

The switch protocol vlan settings, the user can Config the protocol vlan.

**Protocol VLAN Configure**

<b>Mode</b>	ethernetII <span style="float: right;">▼</span>
<b>Ethernet Type</b>	Range:1536-65535
<b>VLAN Name</b>	VLAN0001 <span style="float: right;">▼</span>
<b>Priority</b>	Range:0-7

[Add](#)

Showing 10 Entries Showing 0 to 0 of 0 entries Search

No.	Protocol Type	VLAN Name	Priority
0 results found.			

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Mode</b>	ethernetII	Configure EthernetII Encapsulation
	snap	Configure LLC Encapsulation
	IIc	Configure SNAP Encapsulation
<b>Ethernet Type</b>	Packet protocol type, Configure Packet protocol type number, 1536-65535	
<b>VLAN Name</b>	Configure the VLAN ID.	
<b>Priority</b>	Configure priority value, 0-7	
<b>Operation</b>	Add	Add the protocol vlan
	Delete	Delete the protocol vlan

## 4.7. Surveillance VLAN

### 4.7.1. VLAN Config

**Surveillance VLAN Configure**

Surveillance VLAN	None ▼
Mode	Manual ▼

[Apply](#)

<b>Surveillance VLAN</b>	VLAN ID	
<b>Mode</b>	Manual	Allow Manually
	Auto	Allow Automatically

**Surveillance VLAN Configure**

Surveillance VLAN	VLAN0010 ▼
Mode	Manual ▼

[Apply](#)

**Surveillance OUI Configure**

MAC address	MAC Mask	Priority	Name
00-00-00-00-00-00	FF-FF-FF-FF-FF-FF	Range:0-7	Up to 15 characters.

[Add](#)

Showing 10 Entries Showing 0 to 0 of 0 entries

No.	Name	MAC address	MAC Mask	Priority
0 results found.				

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>MAC address</b>	The MAC address which is shown in the form of XX-XX-XX-XX-XX-XX
<b>MAC Mask</b>	The MAC address mask which is shown in the form of XX-XX-XX-XX-XX-XX
<b>VLAN ID</b>	Vlan-id is the ID of the VLAN with a valid range of 1-4094
<b>Priority</b>	Priority-id is the level of priority and is used in the VLAN tag with a valid range Of 0-7.

## 4.7.2. Port Config

The port Config module, the user can select port to enable mac vlan.

**Port Config**

Ports	Status
--Please select --	Enabled ▼

Apply

Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(A)	Enabled
Ethernet1/0/3(A)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/6(A)	Enabled
Ethernet1/0/7(A)	Enabled
Ethernet1/0/8(A)	Enabled
Ethernet1/0/9(A)	Enabled
Ethernet1/0/10(A)	Enabled
Ethernet1/0/11(A)	Enabled

<b>Port</b>	Port name	
<b>Status</b>	Enable	Enable mac vlan
	Disable	Disable mac vlan

# 5. Port Config

## 5.1 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, click "Apply" to configure.

PoE Global Config	
PoE Work Status	Online
PoE Port Max Number	48
PoE Support Type	802.3at/802.3af
PoE MCU Software Version	V1.1.3
PoE Power Available	<input type="text"/>
PoE Power Used	0 W
PoE Power Remaining	
PoE Main Voltage	54.4 V
PoE Police	Off <input type="button" value="v"/>
PoE Legacy	Off <input type="button" value="v"/>
PoE High-inrush Status	Enabled <input type="button" value="v"/>
PoE Reset Interval	5 <input type="text"/> (1-600 s)

<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 Reset Interval</b>	Port reset time range :1-600 per second

## 5.2. 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 Config , click "Apply" to configure.

**PoE Port Config**

<b>Port</b>	<input type="text" value="--Please select --"/>	
<b>Status</b>	<input type="text" value="Enable"/>	▼
<b>Priority</b>	<input type="text" value="Low"/>	▼
<b>Max Power</b>	<input type="text" value="32000"/>	(1-32000mW)

Port	Status	Oper	Power(mW)	Max Power(1-32000mW)	Current(mA)	Volt(V)	Priority	Class
Ethernet1/0/1	Enable	Off	0	32000	0	0	Low	N/A
Ethernet1/0/2	Enable	Off	0	32000	0	0	Low	N/A
Ethernet1/0/3	Enable	Off	0	32000	0	0	Low	N/A
Ethernet1/0/4	Enable	Off	0	32000	0	0	Low	N/A
Ethernet1/0/5	Enable	Off	0	32000	0	0	Low	N/A
Ethernet1/0/6	Enable	Off	0	32000	0	0	Low	N/A
Ethernet1/0/7	Enable	Off	0	32000	0	0	Low	N/A
Ethernet1/0/8	Enable	Off	0	32000	0	0	Low	N/A

<b>Port</b>	Current configured Ethernet ports
<b>Status</b>	Enable: Normal power supply Force: Forced power supply Disable: No power supply
<b>Priority</b>	Low: low priority High: high priority Critical: highest priority
<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



### 5.3. PD Alive

This page can be used to configure PoE PD alive under ports.

**PD Alive**

If not an integer multiple of 5, round up.

<b>PoE Monitor interval</b>	<input type="text" value="150"/>	(30-36000 s,default is 150)
<input type="button" value="Apply"/>		
<b>Port</b>	<input type="text" value="--Please select --"/>	
<b>Monitor Status</b>	<input type="text" value="Disabled"/>	
<input type="button" value="Apply"/>		

Port	Monitor Status
Ethernet1/0/1	Disabled
Ethernet1/0/2	Disabled
Ethernet1/0/3	Disabled
Ethernet1/0/4	Disabled
Ethernet1/0/5	Disabled

<b>Interface</b>	Current configured Ethernet ports
<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 Monitor Status</b>	Disabled: disable port monitoring Enabled: Enable port monitoring

### 5.4. PoE Schedule

**PoE Schedule**

<b>Port</b>	<input type="text" value="--Please select --"/>
<b>Time Range Name</b>	<input type="text" value="NULL"/>
<input type="button" value="Apply"/>	

Port	Time Range Name
Ethernet1/0/1	NULL
Ethernet1/0/2	NULL
Ethernet1/0/3	NULL

<b>Interface</b>	Current configured Ethernet ports
<b>Time range name</b>	The time range name defined by the switch

# 6. DHCP Config

## 6.1. DHCP Server

### 6.1.1. Global Config

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

**Global Config**

DHCP Server  Off

**Global Config**

DHCP Server  On

<b>DHCP server</b>	Off	Close DHCP server
	On	Open DHCP server

### 6.1.2. Create Address Pool

DHCP server address pool name configuration, user can add and delete the address pool name. DHCP Server Address Pool Table shows the address pool of the current DHCP server.

**Create Address Pool**

**Create Address Pool**

Address Pool Name  (1-32 character)

---

**DHCP Server Address Pool Table**

Showing  Entries

Showing 0 to 0 of 0 entries

Search

□	Address Pool Name
0 results found.	

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

### 6.1.3. Dynamic Pool

Switch DHCP address pool configuration, the user configures the DHCP address pool parameters. Dynamic Pool Config Table displays currently configured address pool.

**Dynamic Pool**

Address Pool Name	1 <input type="button" value="v"/>
Domain Name	<input type="text"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
DHCP Client Node Type	Default <input type="button" value="v"/>
Lease Time	Not Configured <input type="button" value="v"/>

---

**Dynamic Pool Config Table**

Showing  Entries Showing 0 to 0 of 0 entries

	Address Pool Name	Domain Name	IP Address/Netmask	DHCP Client Node Type	Lease Time
0 results found.					

<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.
	Delete	Restore the four parameters with check boxes to the default configuration, and the parameters without check boxes will not be operated.

## 6.1.4. Manual Pool

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

Manual Pool

<b>Address Pool Name</b>	1
<b>IP Address</b>	xxx.xxx.xxx.xxx
<b>Netmask</b>	xxx.xxx.xxx.xxx
<b>Binding Type</b>	Hardware Address
<b>ARP Hardware Type</b>	1(ethernet)
<b>MAC Address</b>	xx-xx-xx-xx-xx-xx

Static Pool Config Table

Showing 10 Entries
Showing 0 to 0 of 0 entries
Search

	Address Pool Name	MAC Address	IP Address/Netmask	Binding Type	ARP Hardware Type
0 results found.					

<b>Address Pool Name</b>	The name of the created address pool.	
<b>IP address</b>	IP address assigned by the DHCP server to the client.	
<b>Netmask</b>	The subnet mask assigned by the DHCP server to the client IP.	
<b>Binding Type</b>	Hardware Address Client identifier: The identifier of the client,	
<b>ARP Hardware Type</b>	The protocol type used by the client is rfc\ethernet\ieee802.  RFC ID: RFC protocol number, valid range is 1-255.	
<b>MAC address</b>	MAC address, for example: 44-11-22-33-44-55 (MAC address)	
<b>Operation</b>	Apply	Apply after selecting and adding data.
	Delete	Clear all data and restore to default.

### 6.1.5. Default Gateway

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

Default Gateway	
Address Pool Name	1
Gateway0	<input type="text"/>
Gateway1	<input type="text"/>
Gateway2	<input type="text"/>
Gateway3	<input type="text"/>
Gateway4	<input type="text"/>
Gateway5	<input type="text"/>
Gateway6	<input type="text"/>
Gateway7	<input type="text"/>
Operation	Add
<input type="button" value="Apply"/>	

<b>DHCP pool name</b>	The name of the created address pool.	
<b>Gateway 0-7</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 ignore 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.
	Delete	Clear all gateways and restore to the default state.

### 6.1.6. DNS Server

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

DNS Server	
Address Pool Name	1
DNS Server0	<input type="text"/>
DNS Server1	<input type="text"/>
DNS Server2	<input type="text"/>
DNS Server3	<input type="text"/>
DNS Server4	<input type="text"/>
DNS Server5	<input type="text"/>
DNS Server6	<input type="text"/>
DNS Server7	<input type="text"/>
Operation	Add

<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.
	Delete	Clear all DNS servers and restore to the default state.

### 6.1.7. Excluded Address

Excluding the dynamic allocation address configuration, the user configures the addresses that are not used for dynamic allocation. Excluded Address table displays the address range currently not used for dynamic allocation.

**Excluded Address**

Starting address	
Ending address	

[Apply](#)

---

**Exclude Address Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	Starting address	Ending address
0 results found.		

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<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>	Apply	Add the address range that is not used and dynamically allocated to the switch
	Delete	Delete the address range that is not used and dynamically allocated from the switch

### 6.1.8. Packet Statistics

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

Packet Statistics						
Address Pools	Database Agents	Automatic Bindings	Manual Bindings	Conflict Bindings	Expired Bindings	Malformed Message
1	0	0	0	0	0	0
<b>Message Received</b>						
BOOT REQUEST	DHCP Discover	DHCP Request	DHCP Decline	DHCP Release	DHCP Inform	
0	0	0	0	0	0	
<b>Message Send</b>						
BOOT Reply	DHCP Offer	DHCP ACK	DHCP NAK	DHCP Relay	DHCP Forward	
0	0	0	0	0	0	

[Clear Statistics](#)

It can be viewed in real time by clicking "Clear Statistics".

## 6.1.9. Client List

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.

Client List			
IP Address	Hardware Address	Lease Expiration	Type

<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	

## 6.2. DHCP Relay Config

### 6.2.1. DHCP Relay Config

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

**DHCP Relay Config**

DHCP Broadcast Suppress ?  Off

DHCP Relay Forwarding ?  Off

---

**DHCP Relay Config**

DHCP Broadcast Suppress ?  On

DHCP Relay Forwarding ?  On

Interface

VLAN0001 ▼

Helper-server Address

xxx.xxx.xxx.xxx

---

**DHCP Forward Protocol Table**

Showing 10 ▼ Entries
Showing 0 to 0 of 0 entries
Search

<input type="checkbox"/>	Forward Protocol	Interface	Helper-server Address
0 results found.			

<b>DHCP Broadcast Suppress</b>	On: Enable DHCP broadcast suppress function Off: Disable DHCP broadcast suppress function Default is off.
<b>DHCP Relay Forwarding</b>	On: Sets DHCP relay to forward UPD broadcast packets on the port Off: Disable DHCP Relay Forwarding



	Default is off.	
<b>Interface</b>	Established Layer 3 interface	
<b>Helper-server Address</b>	IP address of the Layer 3 interface	
<b>Operation</b>	Add	Add a Layer 3 interface for DHCP to forward UDP packets
	Delete	Delete the Layer 3 interface through which DHCP forwards UDP packets

## 6.3. DHCP Snooping

### 6.3.1. Global Config

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

**Global Config**

---

DHCP Snooping Status  Off

<b>DHCP Snooping status</b>	Off	Disable DHCP Snooping
	On	Enable DHCP Snooping

**Global Config**

---

DHCP Snooping Status  On

Action Num  (1-200,default 10)

Limit Rate  pps(0-100,default 100)

Displays the current DHCP Snooping status.

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

<b>DHCP Snooping action Num</b>	Set the maximum number of defense actions to avoid exhaustion of switch resources caused by attacks.	
<b>Limit Rate(Packet per second)</b>	Range: 0-100	
<b>Operation</b>	Apply	Configure the number of defense actions filled in above, default is 10, Configure the number of packets per second

Action Num, displays the current number of DHCP Snooping defense actions.

Limit Rate, displays the number of packets per second configured for the current DHCP Snooping.

### 6.3.2. VLAN Config

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

**VLAN Config**

<b>VLAN ID</b>	<input type="text" value="--Please select --"/>
<b>VLAN Enable</b>	Disabled <input type="button" value="v"/>

VLAN ID	VLAN Enable
VLAN0001	Disabled
VLAN0010	Disabled

<b>VLAN ID</b>	Select VLAN ID.	
<b>VLAN Enable</b>	Enable	Enable DHCP Snooping VLAN
	Disable	Disable DHCP Snooping VLAN

### 6.3.3. Static User Binding

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

**Static User Binding**

	<b>Binding Status</b> <input type="radio" value="Off"/>
--	---

**Static User Binding**

<b>Binding Status</b>	<input checked="" type="radio" value="On"/>
<b>MAC Address</b>	<input type="text"/>
<b>IP Address</b>	<input type="text"/>
<b>VLAN ID</b>	VLAN0001 <input type="button" value="v"/>
<b>Port</b>	Ethernet1/0/1 <input type="button" value="v"/>

---

**DHCP Snooping Binding Table**

Showing  Entries Showing 0 to 0 of 0 entries

☐	MAC Address	IP Address	Port	VLAN ID	Type
0 results found.					

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

<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>	Apply	Add DHCP Snooping binding user relationship
	Delete	Delete DHCP Snooping binding user relationship

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

**Helper-server Config**

<b>Helper-server Address</b>	<input type="text"/>
<b>Helper-server UDP Port</b>	9119 (1-65535,default 9119)
<b>Local IP Address</b>	<input type="text"/>
<b>Server Address Type</b>	Primary ▼

<input type="checkbox"/>	Helper-server Address	Helper-server UDP Port	Local IP Address	Server Address Type
--------------------------	-----------------------	------------------------	------------------	---------------------

<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>	Apply	Add HELPER server address
	Delete	Delete the HELPER server address, you can leave it blank when deleting

### 6.3.5. Port Binding

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.

**Port Binding**

<b>Port</b>	--Please select --
<b>Dot1x</b>	Disabled <span style="float: right;">▼</span>
<b>User</b>	Disabled <span style="float: right;">▼</span>

Apply

Port	Dot1x	User
Ethernet1/0/1	Disabled	Disabled
Ethernet1/0/2	Disabled	Disabled
Ethernet1/0/3	Disabled	Disabled
Ethernet1/0/4	Disabled	Disabled
Ethernet1/0/5	Disabled	Disabled
Ethernet1/0/6	Disabled	Disabled
Ethernet1/0/7	Disabled	Disabled
Ethernet1/0/8	Disabled	Disabled
Ethernet1/0/9	Disabled	Disabled
Ethernet1/0/10	Disabled	Disabled
Ethernet1/0/11	Disabled	Disabled

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

Displays the dot1x binding status of each DHCP Snooping port of the switch.

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.

### 6.3.6. Trust Port

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.

# 7. ACL Config

## 7.1. Time Range Config

Time Range configuration module, the user can add or delete the operation 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 no need to input the date including start and end time in the absolute-periodic.

You must input the weeks, start-time and end-time, but no need to 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 Config**

In the "Absolute" type, the start time and end time must be selected. If the start time and end time are the same time, only the start time can be work;In the "Absolute-period" type, a week value must be selected, including the start and end times, but cannot be the same;In the "Period" type, you must select a week value, including start and end times.

<b>Time Range Name</b>	<input type="text" value=""/>	(1-64 characters)
<b>Time Range Type</b>	Absolute <span style="font-size: x-small;">▼</span>	
<b>Start Time</b>	<input type="text" value="2024"/> - <input type="text" value="01"/> - <input type="text" value="01"/> <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/>	
<b>End Time</b>	<input type="text" value="2024"/> - <input type="text" value="01"/> - <input type="text" value="01"/> <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/>	

[Apply](#)

---

**Time Range Table**

Showing  Entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Time Range Name	Absolute	Periodic	Absolute-periodic
0 results found.				

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<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>	Apply	Add operations
	Delete	Delete operations

## 7.2. IP ACL

### 7.2.1. 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**

ACL Name	<input type="text"/>	(1-64 string or number 1-99)
ACL Action	<input type="text" value="Permit"/>	
Source Address Type	<input type="text" value="Any IP"/>	
TPID	<input type="text"/>	(0-65535,Optional configuration)
VLANID	<input type="text" value="Not Configured"/>	
DSCP	<input type="text" value="Not Configured"/>	

---

**IP Standard ACL Configuration Status Table**

Showing  Entries Showing 0 to 0 of 0 entries Search

	ACL Name	Source IP/Mask	TPID	VLANID/Mask	DSCP	ACL Action
0 results found.						

<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	

## 7.2.2. IP Extended ACL

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

**IP Extended ACL**

ACL Name	<input type="text"/>	<small>(1-64 string or number 100-299)</small>
Operation Type	ICMP	▼
ACL Action	Permit	▼
Fragment Packet	Disabled	▼
Source Address Type	Any IP	▼
Destination Address Type	Any IP	▼
IP Precedence	Not Configured	▼
TOS	Not Configured	▼
Time Range Name	Not Configured	▼
ICMP Type	Not Configured	▼
ICMP Code	Not Configured	▼

[Apply](#)

---

**IP Extended ACL Configuration Status Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Operation Type	Source IP/Mask	Destination IP/Mask	Fragment Packet	IP Precedence	TOS	Operation Type Parameter	Time Range Name	ACL Action
0 results found.										

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>List name</b>	Digital extensions IP access list numbers ,100-199	
<b>Operation type</b>	Extended operation type:ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IP.INIP.OSPF.IP.or Specified protocol	
<b>ACL Action</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

## 7.3. MAC ACL

### 7.3.1. 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**

<b>ACL Name</b>	<input type="text" value=""/>	(700-799)
<b>ACL Action</b>	Permit <span style="float: right;">▼</span>	
<b>Source Address Type</b>	Any MAC <span style="float: right;">▼</span>	

[Apply](#)

---

**MAC Standard ACL Configuration Status Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	ACL Name	Source MAC/Mask	ACL Action
0 results found.			

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>List name</b>	Digital Standard MAC Access List Number 700-799	
<b>ACL Action</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	



### 7.3.2. 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	
ACL Name	<input type="text"/> (1-64 string or number 1100-1199)
ACL Action	Permit <input type="button" value="v"/>
Source Address Type	Any MAC <input type="button" value="v"/>
Destination Address Type	Any MAC <input type="button" value="v"/>
Packet Type	None <input type="button" value="v"/>
Cos	Not Configured <input type="button" value="v"/>
Cos Mask	Not Configured <input type="button" value="v"/>
VLANID	Not Configured <input type="button" value="v"/>
EtherType	<input type="text"/> (1536-65535, Optional configure)
EtherType Mask	Not Configured <input type="button" value="v"/>
<input type="button" value="Apply"/>	

MAC Extended ACL Configuration Status Table								
Showing	10 <input type="button" value="v"/> Entries	Showing 0 to 0 of 0 entries			Search <input type="text"/>			
<input type="checkbox"/>	ACL Name	Source MAC/Mask	Destination MAC/Mask	Packet Type	Cos/Mask	VLANID/Mask	EtherType/Mask	ACL Action
0 results found.								
<input type="button" value="Delete"/>							<input type="button" value="First"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Last"/>	

<b>List name</b>	Digital Extension MAC-IP Access List Number ,3100-3199	
<b>ACL Action</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

## 7.4. 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

ACL Name	<input type="text"/>	(1-64 string or number 3100-3299)
Operation Type	<input type="text" value="ICMP"/>	
ACL Action	<input type="text" value="Permit"/>	
Source Address Type	<input type="text" value="Any MAC"/>	
Destination Address Type	<input type="text" value="Any MAC"/>	
Source Address Type	<input type="text" value="Any IP"/>	
Destination Address Type	<input type="text" value="Any IP"/>	
Paramer Options	<input type="text" value="Not Configured"/>	
TPID	<input type="text"/>	(0-65535,Optional configuration)
VLANID	<input type="text" value="Not Configured"/>	
Time Range Name	<input type="text" value="Not Configured"/>	
ICMP Type	<input type="text" value="Not Configured"/>	

ICMP Code	<input type="text" value="Not Configured"/>	
-----------	---	--

MAC-IP Extended ACL Configuration Status Table

Showing  Entries Showing 0 to 0 of 0 entries Search

☐	ACL Name	Operation Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Mask	Destination IP/Mask	TPID	VLANID/Mask	DSCP	IP Precedence	TOS	Operation Type Paramer	Time Range Name	ACL Action
0 results found.														

<b>List name</b>	Digital Extension MAC-IP Access List Number ,3100-3199	
<b>Operation type</b>	Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IP.INIP.OSPF.IP.or Specified_protocol	
<b>ACL Action</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>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>DSCP</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	

## 7.5. ACL Binding

### 7.5.1. Binding Port

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

**Binding Port**

<b>Port</b>	<input type="text" value="--Please select --"/>
<b>ACL Type</b>	<input type="text" value="IP"/>
<b>ACL Name</b>	<input type="text" value="ACL123"/>
<b>Attached Direction</b>	<input type="text" value="Ingress"/>

---

**Port Binding Status Table**

Showing  Entries
Showing 0 to 0 of 0 entries
Search

	Port	ACL Name	ACL Type	Attached Direction
0 results found.				

<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>	Apply	Add operations
	Delete	Delete operations

## 7.5.2. Binding Vlan

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

**Binding Vlan**

<b>VLAN Interface</b>	<input type="text" value="--Please select --"/>
<b>ACL Type</b>	<input type="text" value="IP"/>
<b>ACL Name</b>	<input type="text" value="ACL123"/>
<b>Attached Direction</b>	<input type="text" value="Ingress"/>

---

**VLAN Binding Status Table**

Showing  Entries
Showing 0 to 0 of 0 entries
Search

<input type="checkbox"/>	VLAN Interface	ACL Name	ACL Type	Attached Direction
0 results found.				

<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

# 8. Ring Network

## 8.1. Spanning-tree

### 8.1.1. Global Properties

This page uses the build tree function with global enable.

To display the "Global Properties" page, click Ring Network -> Spanning-tree ->Global Properties, click "Apply" to configure.

**Global Properties**

This page is used to configure the global basic parameters of the spanning tree.

Enabled

Off

<b>entry</b>	describe
<b>Operation</b>	On: enable spanning tree function Off: disables spanning tree functionality

**Global Properties**

This page is used to configure the global basic parameters of the spanning tree.

<b>Enabled</b>	<input checked="" type="radio"/> On
<b>Mode</b>	MSTP
<b>Cost Format</b>	dot1t
<b>Forward Time</b>	15 <small>Sec(4-30, default 15)</small>
<b>Hello Time</b>	2 <small>Sec(1-10, default 2)</small>
<b>Max Age Time</b>	20 <small>Sec(6-40, default 20)</small>
<b>Max Hop Time</b>	20 <small>(1-40, default 20)</small>
<b>Priority</b>	32768 <small>(0-61440, default 32768)</small>
<b>TC Flush</b>	Flush

Apply

<b>Mode</b>	Generating tree protocol type: Mstp.Stp.Rstp
<b>Cost Format</b>	Path cost format:Dot1t.Dot1d
<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>Hello Time</b>	Size range :1-10, in seconds,the following conditions shall be met: $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$
<b>Max Age Time</b>	Size range :6-40, in seconds,the following conditions shall be met: $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$

	Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)
<b>Max Hop Time</b>	Numerical range :1-40
<b>Priority</b>	Numerical range :0-61440, and an integer multiple of 4096

### 8.1.2. Instance Mapping

This page is used to configure the mapping relationship between the spanning tree instance and the VLAN.

**Instance Mapping**

This page is used to generate tree instance mapping vlan configuration.

**Instance Mapping Configuration**

<b>Instance</b>	0		
<b>Operation</b>	Add		
<b>VLAN List</b>	<input type="text"/>		(1-4094, for example: 1;3-6)
<b>Priority</b>	<input type="text"/>		(0-61440, default 32768)

[Apply](#)

---

**Instance Mapping Status**

Showing  Entries Showing 1 to 1 of 1 entries

Instance	VLAN List	Priority
0	1-4094	32768

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

<b>entry</b>	describe
<b>Instance name</b>	Generating tree instance ID, range 0-64
<b>Operation</b>	Add: Add the above configuration information Delete: Delete the above configuration information
<b>VLAN name</b>	VLAN ID, range : 1-4094

**Instance Mapping Status**

Showing  Entries Showing 1 to 1 of 1 entries

Instance	VLAN List	Priority
0	1-4094	32768

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

<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

### 8.1.3. Instance Properties

This page is used to configure MSTP domain name and MSTP revision level.

**Instance Properties**

This page is used for spanning tree instance parameter configuration.

**Instance Properties Configuration**

<b>Field Name</b>	<input type="text"/>	(1-32 characters, and cannot special char(!%#\$&< > + * ?), not entering indicates deletion)
<b>Revision-level</b>	<input type="text"/>	(0-65535)

Field Name	Revision-level
	0

<b>entry</b>	describe
<b>Field name</b>	MSTP domain name, the length is 1-32 characters
<b>Revision-level</b>	Range :0-65535
<b>Operation</b>	Apply added information.

### 8.1.4. Port Config

This page is used to configure and enable or disable the tree generation function under the port.

**Port Config**

This page is used to generate tree port parameter configuration.

<b>Port</b>	<input type="text" value="--Please select --"/>	
<b>Status</b>	Enabled	▼
<b>BPDU</b>	Disabled	▼ (Aggregation port not supported)
<b>Edge Port</b>	Disabled	▼
<b>Point-to-Point</b>	Auto	▼
<b>Packet Format</b>	Auto	▼
<b>Digest Snooping</b>	Disabled	▼
<b>TC Flush</b>	Default	▼ (Default to global TC FLUSH value)

Port	Status	BPDU	Edge Port	Point-to-Point	Packet Format	Digest Snooping	TC Flush
Ethernet1/0/1	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush

<b>Port</b>	Ethernet port name
<b>Status</b>	Enable: Port enable spanning tree function Disable: Port disables spanning tree functionality
<b>BPDU</b>	Disabled; VLAN:1-4094



<b>Edge Port</b>	Disabled; Enabled; BPDU Filter; BPDU Guard;
<b>Point-to-Point</b>	Auto; Disabled; Enabled;
<b>Packet Format</b>	Auto; Privacy; Standard;
<b>Digest Snooping</b>	Disabled; Enabled;
<b>TC Flush</b>	no Flush; Flush; Limit
<b>Operation</b>	Apply
	Protocol Migration Check

### 8.1.5. Port Instance

This page is used for configuration of instance port priority.

**Port Instance**

This page is used to generate tree port instance parameter configuration.

<b>Instance</b>	<input type="text" value="0"/>	<b>Port</b>	<input type="text" value="--Please select --"/>
<b>Path Cost</b>	<input type="text" value="0"/> (0-200000000)(0=>Auto)	<b>Priority</b>	<input type="text" value="128"/>
<b>Port Guard</b>	<input type="text" value="Auto"/>	<input type="button" value="Apply"/>	

Instance	Port	Path Cost	Priority	Port Guard
0	Ethernet1/0/1	Auto	128	Auto
0	Ethernet1/0/2	Auto	128	Auto
0	Ethernet1/0/3	Auto	128	Auto

<b>Instance name</b>	Generate tree instance name
<b>Port</b>	Ethernet port name
<b>Cost</b>	Size range :0-200000000
<b>Priority</b>	The size range is :0-240, multiple of 16
<b>Priority</b>	Auto; Root Guard; Loop Guard;
<b>Operation</b>	Configuration: Apply the above configuration

## 8.1.6. Status

This page is used to view information for the spanning-tree status.

Running Status Information									
MSTP Bridge Config Info									
Mode	Bridge MAC	Max Age Time	Hello Time	Forward Time	Force Version				
MSTP(IEEE 802.1s)	58:61:63:ff:d6:0b	20s	2s	15s	3				
Instance0									
Self Bridge ID					32768.58:61:63:ff:d6:0b				
Root ID					32768.58:61:63:00:c1:61				
Ext.RootPathCost					60000				
Region Root ID					this switch				
Int.RootPathCost					0				
Root Port ID					128.2				
Port	ID	Port Path Cost	Ext.RootPathCost	Int.RootPathCost	State	Role	DsgBridge	DsgPort	
Ethernet1/0/2	128.002	20000	40000	0	Forward	ROOT	32768.5861630239e5	128.003	
Ethernet1/0/6	128.006	20000	60000	0	Forward	DSGN	32768.586163ffd60b	128.006	

## 8.2. ERPS

### 8.2.1. ERPS Ring Config

This page is used for configuration of ERPS Ring.

### ERPS Ring Config

Create or delete ERPS ring.

Topology Change Propagation None ▼

Apply

Ring Name	<input type="text"/>	(1-64 character)
Version	V2 <span style="font-size: small;">▼</span>	
Ring-topo	major-ring <span style="font-size: small;">▼</span>	
Port1 Configure	Yes <span style="font-size: small;">▼</span>	
Port0	Ethernet1/0/1 <span style="font-size: small;">▼</span>	
Port1	Ethernet1/0/2 <span style="font-size: small;">▼</span>	
R-APS Virtual-Channel	Without <span style="font-size: small;">▼</span>	

Apply

### ERPS Configuration Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	Ring Name	Port0	Port1	Ring-topo	R-APS Virtual-Channel	Version	Instance Count
0 results found.							

Delete First Previous Next Last

<b>Topology Change Propagation</b>	None; ERPS; STP;
<b>Ring Name</b>	The ERPS ring name created,1-64 character
<b>Version</b>	If configured ERPS ring to support v1, this ring will not support multi-instance. ERPS ring instance does not support the management commands of MS, FS. If configured ERPS ring to support v2, the instance of this ring will deal with the ERPS packets according to the v1 format. Package the R-APS packets and resolve the fields according to v1 format. The fields defined by v2 will not be dealt. V1: Means to support v1 which is released in 2008-06 and the amendment (2009-04) V2: Means to support v2 which is released in 2010-03 and the amendment (2010-06)
<b>Ring-topo</b>	major-ring: Configure the ERPS ring as the major ring open-ring: Configure the ERPS ring as the open ring
<b>Port1 Configure</b>	No: Port1 is not allowed to be configured. Yes: Port1 is allowed to be configured.
<b>Port0</b>	Select port as Port 0 for ERPS
<b>Port1</b>	Select port as Port 1 for ERPS
<b>R-APS Virtual-Channel</b>	Configure if there is the R-APS virtual channel in ERPS ring according to the configuration. Inputting: Success or error. If there is not R-APS virtual channel on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R-APS channel and the data channel will be blocked at the same time. Without: The R-APS virtual channel is not existed in this ERPS ring. With: The R-APS virtual channel is existed in this ERPS ring.
<b>Operation</b>	Apply Delete

## 8.2.2. ERPS Instance Config

This page is used for configuration of ERPS Instance.

**ERPS Instance Config**

Ring Name	erps1	
Instance ID	1	
Control VLAN	VLAN0002	
Ring ID	1	
R-APS MEL	7	
Description		(1-64 characters)
Revertive Mode	Revertive	
Protected Instance		(0-64,use '-' and ';' splice,for example:1;3-6)
WTR Timer	5	(1-12min,default 5)
Guard Timer	50	(1-200ms,default 50)
Holdoff Timer	0	(0-10s,default 0)
Port0 Role	Common	

---

Port1 Role	Common	
------------	--------	--

[Apply](#)

**ERPS Configuration Status Table**

Showing 10 Entries Showing 1 to 1 of 1 entries Search

<input type="checkbox"/>	Ring Name	Instance ID	Control VLAN	Ring ID	R-APS MEL	Description	Revertive Mode	Protected Instance	WTR Timer	Guard Timer	Holdoff Timer	Port0 Role	Port1 Role
<input type="checkbox"/>	erps1	1	-	1	7		Revertive	-	5	50	0	Common	Common

[Delete](#)

[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

<b>Ring Name</b>	Select the ERPS ring you created
<b>Instance ID</b>	Create the ERPS ring instance ID, id of ERPS ring, the range is 1 to 16
<b>Control Vlan</b>	vlan id of R-APS packets, range is from 2 to 4094
<b>Ring ID</b>	ERPS ring id and the range is 1 to 64
<b>R-APS MEL</b>	The level value of APS packets, range is from 1 to 7
<b>Description</b>	ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines.
<b>Revertive Mode</b>	Configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, then cannot be configured. Only configured on the RPL owner node of the sub ring. Non-Reviertive; Reviertive;
<b>Protect ID</b>	The MSTP instance list protected by ERPS ring instance
<b>WTR Timer</b>	WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. The interval is 1min and the range is from 1 to 12min, default is 5min.

<b>Guard Timer</b>	The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. The interval is 10ms and the range is 10ms to 2s, default is 500ms.
<b>Holdoff Timer</b>	The interval is 1s and the range is 0 to 10s, default is 0s.
<b>Port0 Role</b>	Common is default config, it is the ordinary transmission node type. <ul style="list-style-type: none"> <li>• Owner</li> <li>• Neighbor</li> <li>• Common</li> </ul>
<b>Port1 Role</b>	
<b>Operation</b>	Apply
	Delete

### 8.2.3. View ERPS Statistics

View ERPS Statistics displays ERPS Statistics.

View ERPS Statistics																					
ERPS Instance Table																					
Showing 10 Entries		Showing 1 to 2 of 2 entries															Search <input type="text"/>				
Ring Name	Instance ID	Instance Port	Port Role	Port Status	Signal Status	Node Id	BPR	nrTx	nrRx	rbTx	rbRx	fsTx	fsRx	msTx	msRx	sfTx	sfRx	eventTx	eventRx	totalTx	totalRx
erps1	1	Port0	common	blocked	Non-failed	00-00-00-00-00-00	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
erps1	1	Port1	common	blocked	Non-failed	00-00-00-00-00-00	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

Ring Name	The ERPS ring name when you create
Instance ID	The ERPS ring instance ID when you create
Instance Port	The ERPS ring member ports
Port Role	ERPS ring node roles: RPL Owner, RPL neighbor, Common
Port States	Blocked: port is in block status forwarding: port is in forwarding status
Signal Status	ERPS ring port fault status: Non-failed: no fault Failed: fault happened
Last NodeID	The node ID information is the last bit of the MAC address
Last Bpr	The block link information carried by the receiving last R-APS saved by ERPS ring port, it is port0 or port1 which was blocked.
rbTX	RB transport statistics
rbRX	RB receive statistics

nrTX	NR transport statistics
nrRX	NR receive statistics
fsTX	FS transport statistics
fsRX	FS receive statistics
msTX	MS transport statistics
msRX	MS receive statistics
sfTX	SF transport statistics
sfRX	SF receive statistics
eventTX	Event transport statistics
eventRX	Event receive statistics
totalTX	Total transport statistics
totalRX	Total receive statistics

# 9. Route Config

## 9.1. Static Route

This page is used for the basic configuration of static routing.

**Static Route**

<b>Destination IP Address</b>	<input type="text"/>
<b>Mask Or Prefix-length</b>	<input type="text"/>
<b>Nexthop Or null0</b>	<input type="text"/>
<b>Distance</b>	1 <input type="text"/>

[Apply](#)

---

**Static Routing Configuration Status Table**

Showing  Entries
Showing 1 to 1 of 1 entries
Search

	Destination IP Address/Mask	Nexthop Or null0	Distance	State
<input type="checkbox"/>	0.0.0.0/0	172.16.100.1	1	Connected

[Delete](#)

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

<b>Destination IP address</b>	IP address, format :10.10.11.11
<b>Network mask or prefix-length</b>	Subnet mask in the following format :255.255.255.0; or mask length
<b>Nexthop or Interface null0</b>	IP address, format: 10.10.11.11. or null0
<b>Distance</b>	Range :1-255
<b>Operation type</b>	Apply: Add the above settings Delete: Delete the above

## 9.2. RIP Route

### 9.2.1. Keychain

This page is used for config keychain function.

#### Keychain

Keychain Name	<input type="text"/>	(1-80 characters)
Key ID	<input type="text"/>	(0-2147483647)
Key	<input type="text"/>	(1-256 character)

[Add](#)

---

#### Keychain Information Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	No.	Keychain Name	Key ID	Key
0 results found.				

[Delete Keychain](#)
[Delete Key ID](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Keychain Name</b>	Keychain Name, range 1-80 characters
<b>Key ID</b>	Key ID, range 0-2147483647
<b>Key</b>	Key, range 1-256 character.

### 9.2.2. Basic Config

This page is used to enable RIP function.

#### Basic Config

RIP Status  Off

---

#### Basic Config

RIP Status	<input checked="" type="radio"/> On	
Add Default Route	Disabled ▼	
Default Metric	1 ▼	
Version	V2 ▼	
Recv Buffer Size	<input type="text" value="0"/>	(8192-2147483647 Byte,default:0)
Update	<input type="text" value="30"/>	(5-2147483647 Sec)
Timeout	<input type="text" value="180"/>	(5-2147483647 Sec)
Garbage	<input type="text" value="120"/>	(5-2147483647 Sec)
Maximum Prefix	<input type="text" value="10000"/> <span style="color: red; font-size: small;">(1-65535)</span>	<input type="text" value="75%"/> ▼

[Apply](#)



<b>Add Default Route</b>	Control distribution of default route, distribute a default route.
<b>Default Metric</b>	Set a metric of redistribute routes, range is 1-16, default is 1.
<b>Version</b>	Config RIP version v1/v2, default is v2.
<b>Recv Buffer Size</b>	The RIP UDP receive buffer size value, default is 8192.
<b>Update</b>	Routing table update timer value in second. Default is 30.
<b>Timeout</b>	Routing information timeout timer. Default is 180.
<b>Garbage</b>	Garbage collection timer. Default is 120.
<b>Maximum Prefix</b>	Maximum number of RIP routes, default is 10000. Percentage of maximum routes to generate a warning (Default 75%)

### 9.2.3. Network Config

This page is used for RIP network config.

#### Network Config

Interface Type: VLAN ▼

Interface Value:  (1-4094)

Add

---

#### Network Config Table

Showing 10 ▼ Entries

Showing 0 to 0 of 0 entries

Search

No.	Network Interface Configured
0 results found.	

Delete

First
Previous
Next
Last

---

#### Network Config

Interface Type: Tunnel ▼

Interface Value:  (1-50)

Add

---

#### Network Config Table

Showing 10 ▼ Entries

Showing 0 to 0 of 0 entries

Search

No.	Network Interface Configured
0 results found.	

Delete

First
Previous
Next
Last

### Network Config

Interface Type	Loopback <span style="float: right;">▼</span>
Interface Value	<input type="text" value=""/> (1-1024)

[Add](#)

---

### Network Config Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	No.	Network Interface Configured
0 results found.		

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

### Network Config

Interface Type	IP Prefix <span style="float: right;">▼</span>
Interface Value	<input style="width: 40%;" type="text" value="IP Address"/> / <input style="width: 40%;" type="text" value="Prefix"/>

[Add](#)

---

### Network Config Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	No.	Network Interface Configured
0 results found.		

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Interface Type</b>	VLAN: vlan Tunnel: Tunnel interface Loopback: loopback IP Prefix: IP prefix <network>/<length>, e.g., 35.0.0.0/8
<b>Interface Value</b>	VLAN: interface name, 1-4094. Tunnel: Tunnel interface number, 1-50. Loopback: Loopback ID <1-1024> IP Prefix: IP prefix <network>/<length>, e.g., 35.0.0.0/8

## 9.2.4. Passive Interface

This page is used to configure RIP passive interface.

**Passive Interface**

The configured interface only receives and does not send data packets.

<b>Interface Type</b>	VLAN <span style="float: right;">▼</span>
<b>Interface Value</b>	VLAN0001 <span style="float: right;">▼</span>

[Add](#)

---

**Passive Interface Config Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	No.	Passive Interface
0 results found.		

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

**Passive Interface**

The configured interface only receives and does not send data packets.

<b>Interface Type</b>	Tunnel <span style="float: right;">▼</span>
<b>Interface Value</b>	<input style="width: 80%;" type="text"/> (1-50)

[Add](#)

---

**Passive Interface Config Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	No.	Passive Interface
0 results found.		

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Interface Type</b>	VLAN: vlan Tunnel: Tunnel interface
<b>Interface Value</b>	VLAN: interface name, 1-4094. Tunnel: Tunnel interface number, 1-50.

## 9.2.5. Neighbor Config

This page is used for RIP neighbor config.

### Neighbor Config

---

### Neighbor Config Table

Showing  Entries
Showing 0 to 0 of 0 entries
Search

No.	Neighbor Address
0 results found.	

<b>Neighbor Address</b>	Neighbor address: A.B.C.D
-------------------------	---------------------------

## 9.2.6. Interface Config

This page is used for RIP interface config.

### Interface Config

VLAN Interface	VLAN0001 <input type="button" value="v"/>
Send Version	Disabled <input type="button" value="v"/>
Send Packet	Enabled <input type="button" value="v"/>
Recv Version	Disabled <input type="button" value="v"/>
Recv Packet	Enabled <input type="button" value="v"/>
Authentication Mode	None <input type="button" value="v"/>
Compatible With Cisco	Disabled <input type="button" value="v"/>
Split Horizon	Poisoned <input type="button" value="v"/>

---

### Interface Config Table

Showing  Entries
Showing 0 to 0 of 0 entries
Search

No.	VLAN Interface	Send Version	Send Packet	Recv Version	Recv Packet	Authentication Mode	Key	Keychain Name	Compatible With Cisco	Split Horizon
0 results found.										

<b>VLAN Interface</b>	Select Interface VLAN
<b>Send Version</b>	Advertisement transmission 1: RIP version 1 1 2: RIP version 1 RIP version 2 1-compatible: RIPv1-compatible 2: RIP version 2 2 1: RIP version 2 RIP version 1

<b>Recv Version</b>	Advertisement reception 1: RIP version 1 2: RIP version 2
<b>Authentication Mode</b>	None: Not config MD5: Keyed message digest Plaintext: Clear text authentication
<b>Compatible With Cisco</b>	Compatible with cisco
<b>Split Horizon</b>	Poisoned: means configure the split horizon with poison reverse. Split Horizon with poison reverse by default.
	Enabled: enable split horizon
	Disabled: disable split horizon

### 9.2.7. Redistribute Router

This page is used for RIP Redistribute Router config.

**Redistribute Router**

<b>Routing Type</b>	Connected ▼
<b>Metric</b>	Not Configured ▼

[Add](#)

---

**Redistribute Router Table**

Showing 10 Entries Showing 0 to 0 of 0 entries Search

No.	Routing Type	OSPF Process ID	Metric
0 results found.			

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Routing Type</b>	Connected: redistribute connected routes
	Kernel: redistribute kernel routes
	OSPF Route: redistribute OSPF routes
	BGP Route: redistribute BGP routes
	Static Route: redistribute static routes
<b>Metric</b>	0-16, default is not configured
<b>OSPF Process ID</b>	Redistribute OSPF Process ID, 1-65535, No parameters indicate the default process

## 9.2.8. View RIP Information

This page is used for view RIP information.

**View RIP Information**

RIP Entries

**RIP Routing Information Table**

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,  
 B - BGP, a - aggregate, s - suppressed

Network	Next Hop	Metric	From	If	Time	Supplf
---------	----------	--------	------	----	------	--------

<b>RIP Entries</b>	RIP Information	Show the RIP related messages
	RIP Interface	Show the routes in the RIP route database
	RIP Protocol	Show the RIP process parameter and statistics information

## 9.3. OSPF Route

### 9.3.1. Basic Config

This page is used for OSPF basic config.

**Basic Config**

OSPF Process ID	<input type="text"/>	(0-65535)
Router ID	<input type="text" value="IP Address"/>	

[Add](#)

**OSPF Process ID Table**

Showing  Entries Showing 1 to 1 of 1 entries

	No.	OSPF Process ID	Router ID
<input type="checkbox"/>	1	10	172.16.100.57

[Delete](#)

[First](#)
[Previous](#)
1
[Next](#)
[Last](#)

<b>Process ID</b>	OSPF process ID, 0-65535.
<b>Router ID</b>	OSPF router-id in IP address format: A.B.C.D

### 9.3.2. Network Config

This page is used for OSPF network config.

**Network Config**

<b>OSPF Process ID</b>	<input type="text" value="10"/>	
<b>Network Address</b>	<input type="text" value="IP Address"/>	<input type="text" value="Prefix"/>
<b>Area Number</b>	<input type="text"/>	(0-4294967295 or IP)

**OSPF Area Network Table**

Showing  Entries
Showing 0 to 0 of 0 entries
Search

<input type="checkbox"/>	No.	OSPF Process ID	Network Address	Area Number
0 results found.				

<b>Process ID</b>	Select OSPF process ID.
<b>Network Address</b>	OSPF network prefix:A.B.C.D/M
<b>Area Number</b>	Set the OSPF area ID OSPF area ID as a decimal value:0-4294967295 OSPF area ID in IP address format: A.B.C.D

### 9.3.3. Passive Interface

This page is used for OSPF passive interface.

**Passive Interface**

The configured interface only receives and does not send data packets.

<b>OSPF Process ID</b>	<input type="text" value="10"/>	
<b>Interface</b>	<input type="text" value="Vlan1"/>	

**Passive Interface Config Table**

Showing  Entries
Showing 0 to 0 of 0 entries
Search

<input type="checkbox"/>	No.	OSPF Process ID	Interface
0 results found.			

<b>Process ID</b>	Select OSPF process ID.
<b>Interface Value</b>	Interface name

### 9.3.4. Area Config

This page is used for OSPF area config.

**Area Config**

OSPF Process ID	10
Area Number	
Operation Type	Authentication
Authentication Mode	None <span style="color: red; font-size: small;">?</span>

---

**OSPF Area Basic Config Table**

OSPF Process ID	Area Number	Authentication Mode	Cost
0 results found.			

---

**OSPF Area Range Config Table**

Showing  Entries
Showing 0 to 0 of 0 entries
Search

No.	OSPF Process ID	Area Number	Range Prefix	Type	Substitute Range Prefix
0 results found.					

<b>Process ID</b>	Select OSPF process ID.
<b>Area Number</b>	Select the OSPF area ID
<b>Operation Type</b>	Authentication: Enable authentication Default-Cost: Set the summary-default cost of a NSSA or stub area Range: Summarize routes matching address/mask (border routers only)
<b>Authentication Mode</b>	None: Not config MD5: Use message-digest authentication Plaintext: Use text authentication
<b>Cost</b>	Stub's advertised default summary cost, 0-16777215
<b>Range Prefix</b>	Area range prefix: A.B.C.D/M
<b>Type</b>	Advertise: Advertise this range (default) Not-Advertise: DoNotAdvertise this range Substitute: Announce area range as another prefix



### 9.3.5. Interface Config

This page is used for OSPF interface config.

Interface Config

<b>Interface Name</b>	Vlan1 <span style="color: #f00; font-size: 0.8em;">?</span>	<b>Disable OSPF</b>	Disabled
-----------------------	---	---------------------	----------

Basic Configuration of OSPF Interface

<b>Cost</b>	1 <span style="color: #f00; font-size: 0.8em;">(1-65535)</span>	<b>Priority</b>	1 <span style="color: #f00; font-size: 0.8em;">(0-255, default:1)</span>
<b>Hello Interval</b>	10 <span style="color: #f00; font-size: 0.8em;">(1-65535s,default:10s)</span>	<b>Transmit Delay</b>	1 <span style="color: #f00; font-size: 0.8em;">(1-3600s,default:1s)</span>
<b>Dead Interval</b>	40 <span style="color: #f00; font-size: 0.8em;">(1-65535s,default:40s)</span>	<b>Ignore MTU</b>	Disabled <span style="float: right;">▼</span>
<b>Retransmit Interval</b>	5 <span style="color: #f00; font-size: 0.8em;">(1-3600s,default:5s)</span>	<b>Database Filter</b>	Disabled <span style="float: right;">▼</span>
<b>MTU</b>	1500 <span style="color: #f00; font-size: 0.8em;">(576-65535)</span>	<b>Network Type</b>	Broadcast <span style="float: right;">▼</span>

Apply

<b>Interface Name</b>	Select Interface VLAN name
<b>Disable OSPF</b>	Enabled: Set Disable OSPF. Disabled: Set Enable OSPF.
<b>Cost</b>	Interface cost, <1-65535>
<b>Priority</b>	Router priority, <0-255>
<b>Hello Interval</b>	Time between HELLO packets, <1-65535> Seconds
<b>Transmit Delay</b>	Link state transmit delay <1-3600> Seconds
<b>Dead Interval</b>	Interval after which a neighbor is declared dead, <1-65535> Seconds
<b>Ignore MTU</b>	Ignores the MTU in DBD packets Disabled: Set disable ignore MTU Enabled: Set enable ignore MTU
<b>Retransmit Interval</b>	Time between retransmitting lost link state advertisements, <1-3600> Seconds
<b>Database Filter</b>	Filter OSPF LSA during synchronization and flooding Disabled: Set disable database filter. Enabled: Set enable database filter.
<b>MTU</b>	OSPF interface MTU, <576-65535> MTU size
<b>Network Type</b>	Network type Broadcast: Specify OSPF broadcast multi-access network non-broadcast: Specify OSPF NBMA network point-to-multipoint: Specify OSPF point-to-multipoint network point-to-point: Specify OSPF point-to-point network

OSPF Interface Status Table						
Link State	OSPF Process ID	Router ID	Area Number	Network Address	Hello	State
Up	1	10.10.10.1	0.0.0.0	172.16.100.57/24	Passive Interface	DROther
Neighbor/Adjacent	Hello(RX/TX)	DD(RX/TX)	LS-Req(RX/TX)	LS-Upd(RX/TX)	LS-Ack(RX/TX)	Sequence/Discarded
0/0	0/0	0/0	0/0	0/0	0/0	0/0
Designated Router						
No designated router on this network						
Backup Designated Router						
No backup designated router on this network						

<b>Link State</b>	Interface vlan link state
<b>Process ID</b>	OSPF process ID
<b>Router ID</b>	OSPF router ID
<b>Area Number</b>	OSPF interface area number
<b>Network Address</b>	OSPF interface network address
<b>Hello</b>	OSPF Hello due
<b>State</b>	OSPF interface state
<b>Neighbor/Adjacent</b>	OSPF interface Neighbor Count/ Adjacent neighbor count
<b>Hello(RX/TX)</b>	Hello received/sent
<b>DD(RX/TX)</b>	DD received/sent
<b>LS-Req(RX/TX)</b>	LS-Req received/sent
<b>LS-Upd(RX/TX)</b>	LS-Upd received/sent
<b>LS-Ack(RX/TX)</b>	LS-Ack received/sent
<b>Sequence/Discarded</b>	Crypt Sequence Number/Discarded
<b>Designated Router</b>	OSPF interface Designated Router
<b>Router ID</b>	Designated Router ID
<b>Network Address</b>	Designated Router Network Address
<b>Backup Designated Router</b>	OSPF interface Backup Designated Router
<b>Router ID</b>	Backup Designated Router ID
<b>Network Address</b>	Backup Designated Router Network Address

### 9.3.6. Interface Authentication

This page is used for OSPF interface authentication config.

**Interface Authentication**

Interface Name Vlan1

Interface Authentication Method

Authentication Method None

[Apply](#)

Key Config

Encryption Type Simple Key

Key Type Plain Key

Key  (1-8 characters)

[Apply](#)

**OSPF Interface Authentication Status Table**

Authentication Method	None
-----------------------	------

[Delete Simple Authentication Key](#)

---

OSPF Interface MD5 Key Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	No.	Key ID	Key Type	Key
0 results found.				

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Interface Name</b>	Select interface vlan name
<b>Authentication Method</b>	None: No Authentication
	Simple: Simple Authentication
	MD5: MD5 Authentication
<b>Simple Key</b>	Simple Authentication Key,1-8 characters
<b>MD5 Key</b>	MD5 Authentication Key,1-16 characters
<b>Plain key</b>	1-8 characters
<b>Cipher Key</b>	1-16 characters, input plaintext application to encrypt ciphertext
<b>Key ID</b>	MD5 Key ID, 1-255

### 9.3.7. Default Route Originate

This page is used for OSPF default route originate config.

Default Route Originate	
OSPF Process ID	10 ▼
Default-Information Originate	Disabled ▼
<input type="button" value="Apply"/>	

Default Route Originate	
OSPF Process ID	10 ▼
Default-Information Originate	Enabled ▼
Always	Disabled ▼
Metric Type	External Type 2 ▼
Metric	<input type="text" value=""/> (0-16777214, No parameter indicates no setting)
<input type="button" value="Apply"/>	

<b>Interface Name</b>	Select interface vlan name
<b>Authentication Method</b>	None: No Authentication
	Simple: Simple Authentication
	MD5: MD5 Authentication
<b>Simple Key</b>	Simple Authentication Key,1-8 characters
<b>MD5 Key</b>	MD5 Authentication Key,1-16 characters
<b>Plain key</b>	1-8 characters
<b>Cipher Key</b>	1-16 characters, input plaintext application to encrypt ciphertext
<b>Key ID</b>	MD5 Key ID, 1-255

### 9.3.8. Redistribute Router

This page is used for OSPF redistribute router config.

**Redistribute Router**

OSPF Process ID	10	
Routing Type	Connected	
Tag Value		(0-4294967295, Default is 0, No parameters indicates default value)
Metric Type	External Type 2	
Metric		(0-16777214, No parameter indicates no setting)

Add

---

**Redistribute Router Table**

Showing 10 Entries
Showing 1 to 1 of 1 entries
Search

	No.	Routing Type	Redistribute OSPF Process ID	Tag Value	Metric Type	Metric
<input type="checkbox"/>	1	system	-	-	External Type 2	-

Delete

First
Previous
1
Next
Last

<b>OSPF Process ID</b>	Select OSPF Process ID
<b>Default-Information Originate</b>	Create a default external route to OSPF route area, Enabled/Disabled
<b>Always</b>	Whether default route exist in the software or not, the default route is always advertised. Enabled/Disabled
<b>Metric Type</b>	External Type 1: Set the OSPF external type 1 metric value External Type 2: Set the OSPF External Type 2 metric value, default is External Type 2
<b>Metric</b>	Set the metric value for creating default route, Ranges between 0-16777214

### 9.3.9. View OSPF Information

This page is used for view OSPF Information config.

**View OSPF Information**

OSPF Entries
OSPF Information ▼

**OSPF Routing Information Table**

Routing Process "ospf 10" with ID 172.16.100.57  
 Process bound to VRF default  
 Process uptime is 1 day 0 hour 1 minute  
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled  
 Supports only single TOS(TOS0) routes  
 Supports opaque LSA  
 Supports Graceful Restart  
 Grace period for Graceful Restart 60 secs  
 Supports helper mode for Graceful Restart  
 This router is an ASBR (injecting external routing information)  
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs  
 Refresh timer 10 secs  
 Number of external LSA 0. Checksum Sum 0x000000  
 Number of opaque AS LSA 0. Checksum Sum 0x000000  
 Number of non-default external LSA 0  
 External LSA database is unlimited.  
 Number of LSA originated 0  
 Number of LSA received 0  
 Number of areas attached to this router: 0

<b>OSPF Entries</b>	OSPF Information	Display OSPF main messages
	OSPF Database	Display the OSPF link state data base messages
	OSPF Neighbor	Display the OSPF adjacent point messages

## 9.4. BGP Route

### 9.4.1. Basic Config

This page is used for BGP basic config.

**Basic Config**

**BGP Global Config**

Aggregate Nexthop Check	Disabled ▼
RFC1771 Path Select	Disabled ▼
RFC1771 Strict	Disabled ▼

Apply

**Create AS**

AS Number		(Number:1-4294967295)
-----------	--	-----------------------

Add

AS Table		
Showing 10 Entries	Showing 0 to 0 of 0 entries	Search
No.	AS Number	
0 results found.		
<a href="#">Delete</a>		<a href="#">First</a> <a href="#">Previous</a> <a href="#">Next</a> <a href="#">Last</a>

<b>Aggregate Nexthop Check</b>	Configures whether BGP checks all the route next-hop aggregating. When check is enabled, the aggregate will not performed if the next-hop of the covered routes are not accordance. When checking is disabled, all covered route will aggregated into the aggregate route. Default is disabled.
<b>RFC1771 Path Select</b>	After this attribute is set, path selecting will follow the way defined in RFC 1771, namely not checking the AS internal metric, when different AS exist, which should be perform without this attribute set Default is disabled
<b>RFC1771 Strict</b>	Set whether strictly follows the rfc1771 restrictions. With this attribute set, generation types of routes from protocols such as RIP, OSPF, ISIS, etc. will be regarded as IGP(internal generated),or else as incomplete.
<b>AS Number</b>	AS number, ranging from 1 to 4294967295, it can be shown in decimal notation(such as 6553700) or delimiter method (such as 100.100)

### 9.4.2. Aggregate Address

This page is used for BGP aggregate address config.

Network Config		
AS Number	<input type="text"/>	
IP Prefix	<input type="text"/> / <input type="text"/>	
BACKDOOR ?	<input type="text"/>	
<a href="#">Add</a>		
BGP Network Table		
Showing 10 Entries	Showing 0 to 0 of 0 entries	
Search		
No.	IP Prefix	BACKDOOR
0 results found.		
<a href="#">Delete</a>		<a href="#">First</a> <a href="#">Previous</a> <a href="#">Next</a> <a href="#">Last</a>

<b>AS Number</b>	AS Number
<b>IP Prefix</b>	Network prefix identify
<b>BACKDOOR</b>	back door parameters

### 9.4.3. Aggregate Address

This page is used for BGP aggregate address configuration.

#### Aggregate Address

<b>AS Number</b>	<input type="text"/>
<b>IP Prefix</b>	<input type="text"/> / <input type="text"/>
<b>Summary-Only</b> <span style="color: orange;">?</span>	<input type="text" value="Enabled"/>
<b>AS</b> <span style="color: orange;">?</span>	<input type="text" value="Enabled"/>

---

#### Address Aggregation Configuration Table

Showing  Entries Showing 0 to 0 of 0 entries

	No.	IP Prefix	Summary-Only	AS
0 results found.				

<b>AS Number</b>	AS Number
<b>IP Prefix</b>	IP address, length of mask.
<b>Summary-Only</b>	Send summary only ignoring specific route.
<b>AS</b>	Show AS on the path in list, each AS is shown once.

### 9.4.4. Redistribute Router

This page is used for BGP redistribute router config. Route from other ways will be distributed into the BGP route table.

#### Redistribute Router

<b>AS Number</b>	<input type="text"/>
<b>Routing Type</b>	<input type="text" value="Connected"/>

---

#### Redistribute Router Table

Showing  Entries Showing 0 to 0 of 0 entries

	No.	Routing Type	OSPF Process ID
0 results found.			

<b>AS Number</b>	AS Number	
<b>Routing Type</b>	Connected	redistribute connected route
	Kernel	Redistribute kernel route
	OSPF Route	redistribute OSPF Route
	RIP Route	redistribute RIP Route
	Static Route	redistribute Static Route



### 9.4.5. Neighbor Config

This page can be used for BGP neighbor configuration.

#### Neighbor Config

AS Number	<input type="text"/>	
Neighbor Address	<input type="text"/>	(IPV4/IPV6,exp:1.1.1.1 or 2112::1111)
Neighbor AS Number	<input type="text"/>	(Number:1-4294967295)

---

#### Neighbor Config Table

Showing  Entries Showing 0 to 0 of 0 entries

No.	Neighbor Address	Neighbor AS Number
0 results found.		

<b>AS Number</b>	AS Number
<b>Neighbor Address</b>	Neighbor IP address
<b>AS Number</b>	Neighbor AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100).

### 9.4.6. BGP Correlative Config

This page is used for BGP correlative config.

#### BGP Correlative Config

AS Number	<input type="text"/>
Command	<input type="text" value="always-compare-med"/>
Command Enabled	<input type="text" value="Enabled"/>

Command	Command Value
always-compare-med	
bestpath as-path ignore	
bestpath compare-confed-aspah	
bestpath compare-routerid	
client-to-client reflection	
cluster-id	
deterministic-med	
enforce-first-as	
fast-external-failover	
log-neighbor-changes	
network	

router-id	
scan-time	
graceful-restart	
graceful-restart restart-time	
graceful-restart stale-path-time	
selection-deferral-time	

### 9.4.7. Timer Config

This page is used for BGP Timer config.

**Timer Config**

<b>AS Number</b>	<input type="text"/>	
<b>Keepalive Interval</b>	<input type="text"/>	(0-65535s, Default:60s)
<b>Holdtime</b>	<input type="text"/>	(0-65535s, Default:240s)

<b>AS Number</b>	AS Number
<b>Keepalive Interval</b>	KEEPALIVE interval, default is 60s.
<b>Holdtime</b>	Hold Time, default is 240s.

### 9.4.8. View BGP Information

This page is used to view BGP Information.

**View BGP Information**

<b>BGP Entries</b>	<input type="text" value="BGP Information"/>
--------------------	--

**BGP Routing Information Table**

<b>BGP Entries</b>	BGP Routing Messages	For displaying the routing messages permitted by BGP
	BGP Neighbor	Show neighbor information of specified BGP or total BGP processes

## 9.5. Routing Table

This page is used to view for the basic status of routing table.

**Routing Table**

Routing-Table Entries
Status ▼

**Routing Status Table**

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP  
 O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
 \* - candidate default

Gateway of last resort is 172.16.100.1 to network 0.0.0.0  
 S\* 0.0.0.0/0 [1/0] via 172.16.100.1, Vlan1 tag:0  
 C 127.0.0.8 is directly connected, Loopback tag:0  
 C 172.16.100.0/24 is directly connected, Vlan1 tag:0  
 Total routes are : 3 item(s)

<b>Routing-Table Entries</b>	Status; Database; Connect Route; RIP Route; Static Route; Statistics; OSPF Route; Kernel Route; FIB;
------------------------------	--

# 10 .Multicast Manage

## 10.1. IGMP Snooping Config

### 10.1.1. Basic Config

Switch IGMP Snooping global switch, snooping IGMP messages. IGMP VLAN List displays the current existing VLAN interface and the running status of IGMP Snooping under the VLAN interface.

#### Basic Config

This page is used to configure the basic parameters of the IGMP SNOOPING function

<b>Status</b>	Disabled <span style="font-size: small;">▼</span>
<b>VLAN ID</b> <span style="color: #e67e22; font-size: small;">?</span>	--Please select --

[Apply](#)

---

#### IGMP VLAN List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	VLAN ID	Status
0 results found.		

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Switch on-off IGMP Snooping</b>	Enable	Turn on the global switch of IGMP Snooping on the switch
	Disable	Turn off the global switch of IGMP Snooping on the switch
<b>VLAN ID</b>	Created VLAN ID	

### 10.1.2. Static Router Port

IGMP Snooping mrouter port parameter configuration. VLAN Based Routing Port List displays current configuration information.

#### Static Router Port Config

This page is used to configure static routing ports and corresponding aging time

<b>VLAN ID</b>	--Please select --
<b>Static Router Port</b>	--Please select --
<b>Operation Type</b> <span style="color: #e67e22; font-size: small;">?</span>	Not Set <span style="font-size: small;">▼</span>
<b>Alive Time</b>	255 <span style="color: #e67e22; font-size: small;">(1-65535,Default:255)</span>

[Apply](#)

---

#### VLAN Based Routing Port List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Router Port	Alive Time
0 results found.		

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<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>	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

### 10.1.3. VLAN Config

Configure IGMP Snooping based on VLAN interface. IGMP VLAN Configuration List displays the configuration parameters of existing VLAN.

**VLAN Config**

This page is used to configure IGMP SNOOPING VLAN related parameters

<b>VLAN ID</b>	<input type="text" value="--Please select --"/>	
<b>Immediate leave</b>	<input type="text" value="Enabled"/> ▼	
<b>L2-general-Querier</b>	<input type="text" value="Enabled"/> ▼	
<b>Group number</b>	<input type="text" value="50"/>	(1-65535,Default:50)
<b>Source Table Number</b>	<input type="text" value="40"/>	(1-65535,Default:40)

---

**IGMP VLAN Configuration List**

Showing  Entries Showing 0 to 0 of 0 entries

VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
0 results found.				

<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</b>	Configuration	Configure the checked parameters into the selected VLAN

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).

### 10.1.4. Querier Config

IGMP Snooping query parameter configuration. Querier Configuration List displays current configuration information.

**Querier Config**

This page is used to configure query related parameters

<b>VLAN ID</b>	<input type="text" value="--Please select --"/>	
<b>Query-Interval</b>	<input type="text" value="125"/>	(1-65535,Default:125)
<b>Query-Mrsp-Max</b>	<input type="text" value="10"/>	(1-25,Default:10)
<b>Query-Robustness</b>	<input type="text" value="2"/>	(2-10,Default:2)
<b>Suppression-Query-Time</b> <span style="color: orange;">?</span>	<input type="text" value="255"/>	(1-65535,Default:255)

---

**Querier Configuration List**

Showing  Entries Showing 0 to 0 of 0 entries

VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time
0 results found.				

<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>	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

### 10.1.5. Multicast Table

The page displays multicast table information.

**Multicast Table**

This page is used to view the multicast table

**VLAN ID**

VLAN ID	Group IP	Source IP	Member Port
<input type="text" value="Not VLAN"/>	<input type="text" value="Example:224.1.1.1"/>	<input type="text" value="Example:10.10.10.1"/>	<input type="text" value="--Please select --"/>

---

**Multicast table**

Showing  Entries Showing 0 to 0 of 0 entries

Number	Group IP	Source IP	Member Port	Exptime	Source MAC	Verion
0 results found.						

## 10.2. MLD Snooping Config

### 10.2.1. Basic Config

Switch MLD Snooping global switch, MLD snooping messages. MLD VLAN List Display the current existing VLAN interface and the running status of IGMP Snooping under the VLAN interface.

#### Basic Config

This page is used to configure the basic parameters of the MLD SNOOPING function

<b>Status</b>	Enabled <span style="float: right;">▼</span>
<b>VLAN ID</b> <span style="color: orange;">?</span>	--Please select --

[Apply](#)

---

#### MLD VLAN List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	VLAN ID	Status
0 results found.		

[Delete](#) 
[First](#)
[Previous](#)
[Next](#)
[Last](#)

<b>Switch on-off IGMP Snooping</b>	Enable	Turn on the global switch of IGMP Snooping on the switch
	Disable	Turn off the global switch of IGMP Snooping on the switch
<b>VLAN ID</b>	Created VLAN ID	

### 10.2.2. Static Router Port

MLD Snooping mrouter port parameter configuration.

#### Static Router Port Config

This page is used to configure static routing ports and corresponding aging time

<b>VLAN ID</b>	--Please select --	
<b>Static Router Port</b>	--Please select --	
<b>Operation Type</b> <span style="color: orange;">?</span>	Not Set <span style="float: right;">▼</span>	
<b>Alive Time</b>	255	(1-65535,Default:255)

[Apply](#)

---

#### VLAN Based Routing Port List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Router Port	Alive Time
0 results found.		

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<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>	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

### 10.2.3. VLAN Config

Configure MLD Snooping based on VLAN interface.

**VLAN Config**

This page is used to configure MLD SNOOPING VLAN related parameters

<b>VLAN ID</b>	<input type="text" value="--Please select --"/>	
<b>Immediate leave</b>	<input type="text" value="Enabled"/> ▼	
<b>L2-general-Querier</b>	<input type="text" value="Enabled"/> ▼	
<b>Group number</b>	<input type="text" value="50"/>	(1-65535,Default:50)
<b>Source Table Number</b>	<input type="text" value="40"/>	(1-65535,Default:40)

---

**MLD VLAN Configuration List**

Showing  Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
0 results found.				

<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 to 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 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.

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).



## 10.2.4. Querier Config

MLD Snooping query parameter configuration.

**Querier Config**

This page is used to configure query related parameters

<b>VLAN ID</b>	<input type="text" value="--Please select --"/>	
<b>Query-Interval</b>	<input type="text" value="125"/>	(1-65535,Default:125)
<b>Query-Mrsp-Max</b>	<input type="text" value="10"/>	(1-25,Default:10)
<b>Query-Robustness</b>	<input type="text" value="2"/>	(2-10,Default:2)
<b>Suppression-Query-Time</b> <span style="color: orange;">?</span>	<input type="text" value="255"/>	(1-65535,Default:255)

**Querier Configuration List**

Showing  Entries Showing 0 to 0 of 0 entries

VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time
0 results found.				

<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>	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

## 10.2.5. Multicast Table

The page displays multicast table information.

**Multicast Table**

This page is used to view the multicast table

**VLAN ID**

VLAN ID	Group IP	Source IP	Member Port
Not VLAN	<input type="text" value="Example:ff01::1"/>	<input type="text" value="Example:2001::1234"/>	--Please select --

**Multicast table**

Showing  Entries Showing 0 to 0 of 0 entries

Number	Group IP	Source IP	Member Port	Exptime	Version
0 results found.					

# 11. QoS Config

## 11.1. Port Config

### 11.1.1. Trust Config

Trust Config Module is used to configure port trust rules.

**Trust Config**

This page is used to set port trust configuration

<b>Port</b>	<input type="text" value="--Please select --"/>
<b>Trust Class</b>	<input type="text" value="COS"/>
<b>Operation Type</b>	<input type="text" value="Add"/>

Port	Trust Class
Ethernet1/0/1	COS
Ethernet1/0/2	COS
Ethernet1/0/3	COS
Ethernet1/0/4	COS

<b>Port</b>	To configure the port name, click to expand the remaining ports	
<b>Trust class</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
	Delete	Remove a trust rule for the port

### 11.1.2. Weight Config

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

**Weight Config**

This page is used to set the port scheduling mode and queue weights

<b>Scheduling Type</b>	<input type="text" value="sp"/>	
<b>Port</b>	<input type="text" value="--Please select --"/>	
<b>Weight1</b>	<input type="text" value="1"/>	weight(0-127)
<b>Weight2</b>	<input type="text" value="2"/>	weight(0-127)
<b>Weight3</b>	<input type="text" value="3"/>	weight(0-127)
<b>Weight4</b>	<input type="text" value="4"/>	weight(0-127)
<b>Weight5</b>	<input type="text" value="5"/>	weight(0-127)
<b>Weight6</b>	<input type="text" value="6"/>	weight(0-127)
<b>Weight7</b>	<input type="text" value="7"/>	weight(0-127)
<b>Weight8</b>	<input type="text" value="8"/>	weight(0-127)

<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.

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

**Weight Config**

This page is used to set the port scheduling mode and queue weights

<b>Scheduling Type</b>	<input type="text" value="wrr"/>	
<b>Port</b>	<input type="text" value="--Please select --"/>	
<b>Weight1</b>	<input type="text" value="1"/>	weight(0-127)
<b>Weight2</b>	<input type="text" value="2"/>	weight(0-127)
<b>Weight3</b>	<input type="text" value="3"/>	weight(0-127)
<b>Weight4</b>	<input type="text" value="4"/>	weight(0-127)
<b>Weight5</b>	<input type="text" value="5"/>	weight(0-127)
<b>Weight6</b>	<input type="text" value="6"/>	weight(0-127)
<b>Weight7</b>	<input type="text" value="7"/>	weight(0-127)
<b>Weight8</b>	<input type="text" value="8"/>	weight(0-127)

<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>	Apply	Add the weight of each queue to the port, and fill in all the weights each queue before adding.

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
Ethernet1/0/9	1 2 3 4 5 6 7 8
Ethernet1/0/10	1 2 3 4 5 6 7 8
Ethernet1/0/11	1 2 3 4 5 6 7 8
Ethernet1/0/12	1 2 3 4 5 6 7 8

### Information feedback window

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.

**Weight Config**

This page is used to set the port scheduling mode and queue weights

<b>Scheduling Type</b>	<input type="text" value="wdr"/>	
<b>Port</b>	<input type="text" value="--Please select --"/>	
<b>Weight1</b>	<input type="text" value="1"/>	weight(0-127)
<b>Weight2</b>	<input type="text" value="2"/>	weight(0-127)
<b>Weight3</b>	<input type="text" value="4"/>	weight(0-127)
<b>Weight4</b>	<input type="text" value="8"/>	weight(0-127)
<b>Weight5</b>	<input type="text" value="16"/>	weight(0-127)
<b>Weight6</b>	<input type="text" value="32"/>	weight(0-127)
<b>Weight7</b>	<input type="text" value="64"/>	weight(0-127)
<b>Weight8</b>	<input type="text" value="64"/>	weight(0-127)

<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 4, the range is 0-32767	
<b>Weight4</b>	The weight value of queue 8, the range is 0-32767	
<b>Weight5</b>	The weight value of queue 16, the range is 0-32767	
<b>Weight6</b>	The weight value of queue 32, the range is 0-32767	
<b>Weight7</b>	The weight value of queue 64, the range is 0-32767	
<b>Weight8</b>	The weight value of queue 64, the range is 0-32767	
<b>Operation</b>	Apply	Add the weight of each queue to the port, and fill in all the weights of each queue before adding.

Port	Queue Weight
Ethernet1/0/1	1 2 4 8 16 32 64 64
Ethernet1/0/2	1 2 4 8 16 32 64 64
Ethernet1/0/3	1 2 4 8 16 32 64 64
Ethernet1/0/4	1 2 4 8 16 32 64 64
Ethernet1/0/5	1 2 4 8 16 32 64 64
Ethernet1/0/6	1 2 4 8 16 32 64 64
Ethernet1/0/7	1 2 4 8 16 32 64 64
Ethernet1/0/8	1 2 4 8 16 32 64 64
Ethernet1/0/9	1 2 4 8 16 32 64 64
Ethernet1/0/10	1 2 4 8 16 32 64 64
Ethernet1/0/11	1 2 4 8 16 32 64 64
Ethernet1/0/12	1 2 4 8 16 32 64 64
Ethernet1/0/13	1 2 4 8 16 32 64 64
Ethernet1/0/14	1 2 4 8 16 32 64 64

**Information feedback window**

### 11.1.3. CoS-To-IntP Config

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

**CoS-To-IntP Map**

This page is used to set the mapping relationship between COS and internal priority

CoS	0	1	2	3	4	5	6	7
IntP ?	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>

<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

Displays the execution process and the current mapping relationship.

### 11.1.4. DSCP-To-IntP Config

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

**DSCP-To-IntP Map**

This page is used to set the mapping relationship between DSCP and internal priority

<b>DSCP</b>	<input type="text" value="--Please select --"/>
<b>IntP ?</b>	<input type="text" value="0"/>

<b>DSCP value1-DSCP value8(optional)</b>	Up to eight DSCP values can be configured to the new IntP value, among which 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>	Apply	Configure DSCP to IntP value

DSCP	Internal Priority	DSCP	Internal Priority	DSCP	Internal Priority	DSCP	Internal Priority
0	0	16	2	32	4	48	6
1	0	17	2	33	4	49	6
2	0	18	2	34	4	50	6
3	0	19	2	35	4	51	6
4	0	20	2	36	4	52	6
5	0	21	2	37	4	53	6
6	0	22	2	38	4	54	6
7	0	23	2	39	4	55	6
8	1	24	3	40	5	56	7
9	1	25	3	41	5	57	7
10	1	26	3	42	5	58	7
11	1	27	3	43	5	59	7
12	1	28	3	44	5	60	7
13	1	29	3	45	5	61	7
14	1	30	3	46	5	62	7
15	1	31	3	47	5	63	7

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.

### 11.1.5. Policy Config

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

**Policy Config**

This page is used to set policy configuration on the port

<b>Port</b>	<input type="text" value="--Please select --"/>
<b>Policy-Map Name</b>	<input type="text" value=""/>
<b>Operation Type</b>	<input type="text" value="Add"/>

Port	Policy-Map Name
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

<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
	Delete	Delete port policy

## 11.2. Class-Map Config

### 11.2.1. Class-Map Config

Create and delete classification tables, view the currently configured classification tables. Class Map List displays the currently created class map name.

**Class-Map Config**

This page is used to set class map entries

Class-Map Name  (1-64 characters)

[Apply](#)

**Class-Map List**

Showing 10 Entries Showing 1 to 1 of 1 entries Search

	Entries	Class-Map Name	
<input type="checkbox"/>	1	Ipv6traffic	<a href="#" style="background-color: #0056b3; color: white; padding: 2px 5px;">First</a> <a href="#" style="background-color: #0056b3; color: white; padding: 2px 5px;">Previous</a> <a href="#" style="background-color: #0056b3; color: white; padding: 2px 5px;">1</a> <a href="#" style="background-color: #0056b3; color: white; padding: 2px 5px;">Next</a> <a href="#" style="background-color: #0056b3; color: white; padding: 2px 5px;">Last</a>

[Delete](#)

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

### 11.2.2. Class-Map Rule Config

Set the rules and corresponding parameters for classification matching.

**Class-Map Rule Config**

This page is used to set the matching rules for class map

Class-Map Name

Match Rule

ACL list name  (1-64 characters)

Operation Type

[Apply](#)

<b>Classification criteria rule</b>	access-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
	Del	Remove matching rules

**Class-Map Rule Config**

This page is used to set the matching rules for class map

<b>Class-Map Name</b>	Ipv6traffic	▼
<b>Match Rule</b>	COS	▼
<b>COS 0</b>	<input type="text"/>	(0-7)
<b>COS 1</b>	<input type="text"/>	(0-7)
<b>COS 2</b>	<input type="text"/>	(0-7)
<b>COS 3</b>	<input type="text"/>	(0-7)
<b>COS 4</b>	<input type="text"/>	(0-7)
<b>COS 5</b>	<input type="text"/>	(0-7)
<b>COS 6</b>	<input type="text"/>	(0-7)
<b>COS 7</b>	<input type="text"/>	(0-7)
<b>Operation Type</b>	Add	▼

<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
	Del	Remove matching rules



### Class-Map Rule Config

This page is used to set the matching rules for class map

<b>Class-Map Name</b>	Ipv6traffic	▼
<b>Match Rule</b>	VLAN	▼
VLAN 0	<input type="text"/>	(1-4094)
VLAN 1	<input type="text"/>	(1-4094)
VLAN 2	<input type="text"/>	(1-4094)
VLAN 3	<input type="text"/>	(1-4094)
VLAN 4	<input type="text"/>	(1-4094)
VLAN 5	<input type="text"/>	(1-4094)
VLAN 6	<input type="text"/>	(1-4094)
VLAN 7	<input type="text"/>	(1-4094)
<b>Operation Type</b>	Add	▼

<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>Vlan0-7</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
	Del	Remove matching rules

### Class-Map Rule Config

This page is used to set the matching rules for class map

<b>Class-Map Name</b>	Ipv6traffic	▼
<b>Match Rule</b>	IP DSCP	▼
IP DSCP 0	<input type="text"/>	(0-63)
IP DSCP 1	<input type="text"/>	(0-63)
IP DSCP 2	<input type="text"/>	(0-63)
IP DSCP 3	<input type="text"/>	(0-63)
IP DSCP 4	<input type="text"/>	(0-63)
IP DSCP 5	<input type="text"/>	(0-63)
IP DSCP 6	<input type="text"/>	(0-63)
IP DSCP 7	<input type="text"/>	(0-63)
<b>Operation Type</b>	Add	▼

<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 dscp0-7</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
	Del	Remove matching rules

**Class-Map Rule Config**

This page is used to set the matching rules for class map

Class-Map Name	Ipv6traffic	▼	
Match Rule	IP Precedence	▼	
IP Precedence 0	<input type="text"/>	(0-7)	
IP Precedence 1	<input type="text"/>	(0-7)	
IP Precedence 2	<input type="text"/>	(0-7)	
IP Precedence 3	<input type="text"/>	(0-7)	
IP Precedence 4	<input type="text"/>	(0-7)	
IP Precedence 5	<input type="text"/>	(0-7)	
IP Precedence 6	<input type="text"/>	(0-7)	
IP Precedence 7	<input type="text"/>	(0-7)	
Operation Type	Add	▼	

<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 precedence0-7</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
	Del	Remove matching rules

**Class-Map Rule Config**

This page is used to set the matching rules for class map

Class-Map Name	Ipv6traffic	▼	
Match Rule	IPV6 DSCP	▼	
IPV6 DSCP 0	<input type="text"/>	(0-63)	
IPV6 DSCP 1	<input type="text"/>	(0-63)	
IPV6 DSCP 2	<input type="text"/>	(0-63)	
IPV6 DSCP 3	<input type="text"/>	(0-63)	
IPV6 DSCP 4	<input type="text"/>	(0-63)	
IPV6 DSCP 5	<input type="text"/>	(0-63)	
IPV6 DSCP 6	<input type="text"/>	(0-63)	
IPV6 DSCP 7	<input type="text"/>	(0-63)	
Operation Type	Add	▼	

<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 dscp0-7</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
	Del	Remove matching rules

**Class-Map Rule Config**

This page is used to set the matching rules for class map

<b>Class-Map Name</b>	Ipv6traffic	▼
<b>Match Rule</b>	IPv6 Flowlabel	▼
<b>IPv6 Flowlabel 0</b>	<input type="text"/>	(0-1048575)
<b>IPv6 Flowlabel 1</b>	<input type="text"/>	(0-1048575)
<b>IPv6 Flowlabel 2</b>	<input type="text"/>	(0-1048575)
<b>IPv6 Flowlabel 3</b>	<input type="text"/>	(0-1048575)
<b>IPv6 Flowlabel 4</b>	<input type="text"/>	(0-1048575)
<b>IPv6 Flowlabel 5</b>	<input type="text"/>	(0-1048575)
<b>IPv6 Flowlabel 6</b>	<input type="text"/>	(0-1048575)
<b>IPv6 Flowlabel 7</b>	<input type="text"/>	(0-1048575)
<b>Operation Type</b>	Add	▼

<b>Classification criteria rule</b>	ipv6 Flowlabel	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 flowlabel0-7</b>	One or more IPv6 Flowlabel values can be set, ranging from 0 to 1048575;	
<b>Operation</b>	Add	Add matching rules
	Remove	Remove matching rules

**Class-Map matching rule table**

Showing 10 Entries Showing 1 to 1 of 1 entries Search

Class-Map Name	ACL list name	COS	VLAN	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
Ipv6traffic	none	none	none	none	none	none	none

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

## 11.3. Policy-Map Config

### 11.3.1. Policy Name Config

Create and delete policy tables, and collaborate with classification tables to create packet in and out rules. Policy-Map List displays currently created policy map.

#### Policy Name Config

This page is used to set policy map entries

Policy-Map Name  (1-64 characters)

[Apply](#)

---

#### Policy-Map List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	Entries	Policy-Map Name
0 results found.		

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

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

### 11.3.2. Policy Class Config

Apply the class-map to the policy-map. Policy Map Class List displays the association between the created policy table and the classification matching table.

#### Policy Class Config

This page is used to set policy classification rules

Policy-Map Name	<input style="width: 100%;" type="text"/>
Class-Map Name	<input style="width: 100%;" type="text" value="Ipv6traffic"/>
Inserted Before The Class-Map Name	<input style="width: 100%;" type="text" value="Ipv6traffic"/>

[Apply](#)

---

#### Policy-Map-Class List

Showing 10 Entries Showing 0 to 0 of 0 entries Search

	Policy-Map Name	Class-Map Name
0 results found.		

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

<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>	Apply	Apply values added or selected.

### 11.3.3. Policy Mark Config

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.

**Policy Mark Config**

This page is used to set policy tags

<b>Policy-Map Name</b>	<input type="text"/>
<b>Class-Map Name</b>	<input type="text" value="Ipv6traffic"/>
<b>Mark Type</b>	<input type="text" value="COS"/>
<b>COS</b>	<input type="text"/> (0-7)
<b>Operation Type</b>	<input type="text" value="Add"/>

---

**Policy Mark List**

Showing  Entries Showing 0 to 0 of 0 entries

Policy-Map Name	Class-Map Name	COS	IP DSCP	IP Precedence	Internal Priority	Drop Precedence
0 results found.						

<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 precedenc	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
<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>Operation</b>	Add	Add the priority and queue value associated with the strategy table and the classification matching table
	Delete	Remove the priority and queue value associated with the strategy table and the classification matching table

### 11.3.4. Policy Bandwidth

Configure the new aggregation strategy and the information rate and burst id of the aggregation strategy.

**Policy Bandwidth**

This page is used to set policy bandwidth configuration

Burst ID1	<input type="text" value="1024"/>	(1-8192)
Burst ID2	<input type="text" value="1024"/>	(1-8192)

Policy-Map Name	<input type="text"/>
Class-Map Name	<input type="text" value="Ipv6traffic"/>
Burst ID	<input type="text" value="1"/>
Bandwidth Rate	<input type="text"/> (1-10000000)
Operation Type	<input type="text" value="Add"/>

<b>Aggregate policy name</b>	New aggregate policy name, range: 1-64 character.	
<b>Committed Information Rate</b>	Information Rate, range: 1-10000000kbit/s	
<b>Policy burst id configuration</b>	Burst id configuration, range: 1-2	
<b>Operation</b>	Add	Add aggregate policy
	Remove	Remove aggregate policy

**Policy Bandwidth List**

Showing  Entries Showing 0 to 0 of 0 entries Search

Policy-Map Name	Class-Map Name	Burst ID	Bandwidth Rate(Kbps)
0 results found.			

### 11.3.5. Policy VLAN

Configure VLAN Association Policy.

**Policy VLAN**

This page is used to set policy configurations on VLANs

<b>Policy-Map Name</b>	<input type="text"/>	
<b>Vlan List</b> <span style="color: red; font-size: small;">?</span>	<input type="text"/>	(1-100 characters)
<b>Operation Type</b>	<input type="text" value="Add"/>	

---

**VLAN Policy List**

Showing  Entries Showing 0 to 0 of 0 entries Search

VLAN ID	Policy-Map Name
0 results found.	

<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