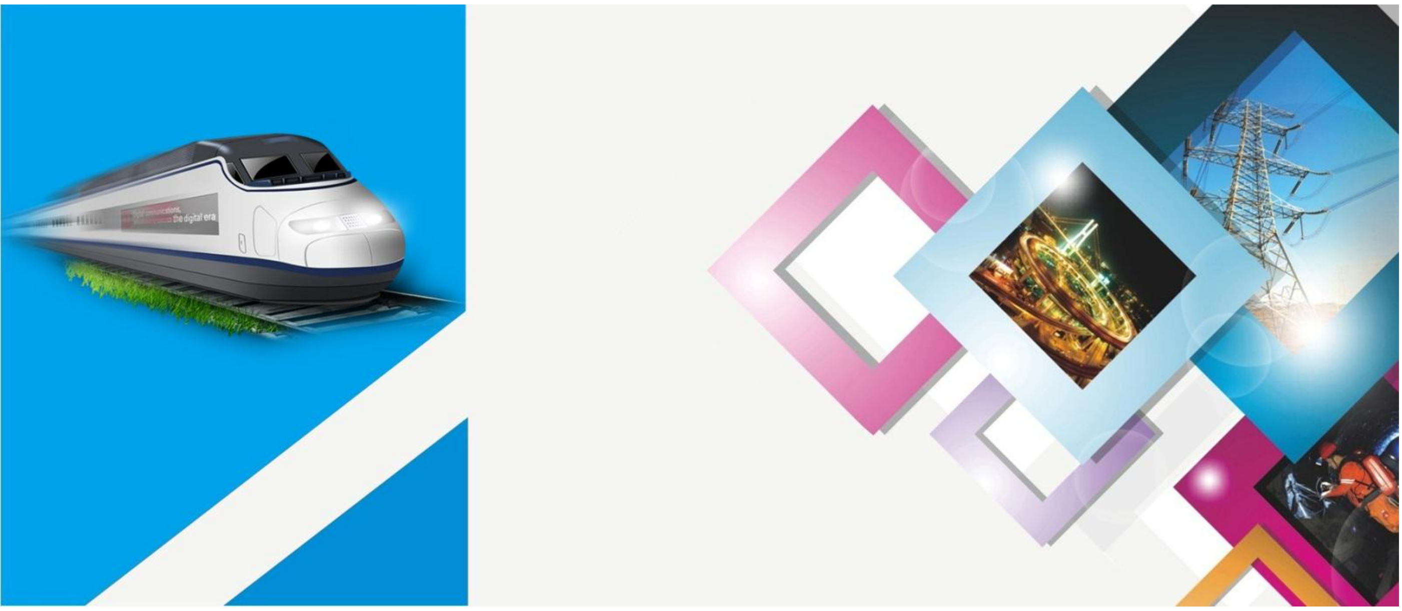


IES6312 Series

Managed Industrial PoE/non-PoE Ethernet Switch

User Manual

Version 01

Issue Date: 2019-01-21

Industrial Ethernet Communication Solutions Expert 3onedata Co., Ltd.

Trademark statement

3onedata, 3onedata® and 3One data® are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Notes

Purchased product, service or features should be constrained by 3ondedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata
Make network communication more reliable

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology support:	tech-support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

Managed Industrial PoE/non-PoE Ethernet Switch User Manual has introduced this switch:

- Product feature
- Network management method
- Network management relative principle overview

Readers

This manual mainly suits for engineers as follows:

- Network administrator responsible for network configuration and maintenance
- On-site technical support and maintenance staff
- Hardware engineer

Text Format Convention

Format	Description
“”	Words with "" represent the interface words. e.g.: "The port number".
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	Represent the words click to achieve hyperlink. Font color as: "Light blue".
About This Chapter	The "About This Chapter" section provides links to each section and corresponding principles / operating chapters in this chapter.

Icon Convention

Format	Description
⚠ Notice	Reminder the announcements in the operation, improper

Format	Description
	operation may result in data loss or equipment damage.
⚠ Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
Note	Make a necessary supplementary instruction for operation description.
Key	Configuration, operation, or tips for device usage.
Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version NO.	Revision Date	Revision Description
01	2019-01-21	Product release

Content

The First Part: Operation

1 Log in the Web Interface

1.1 WEB Browsing System Requirements

While using managed industrial Ethernet switches, the system should meet the following conditions.

Hardware and Software	System Requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	Above 256 color
Browser	Above Internet Explorer 6.0
Operating System	Windows XP Windows 7

1.2 Setting IP Address of PC

The switch default management as follows:

IP Setting	Default Value
IP Address	192.168.1.254
Subnet Mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and switch is reachable.
- Before local configuration, please make sure the computer IP address is on the same subnet as the one of switch.

Notes:
While first configuring the switch, if it is a local configuration mode, please make sure that the network segment of current PC is 1.

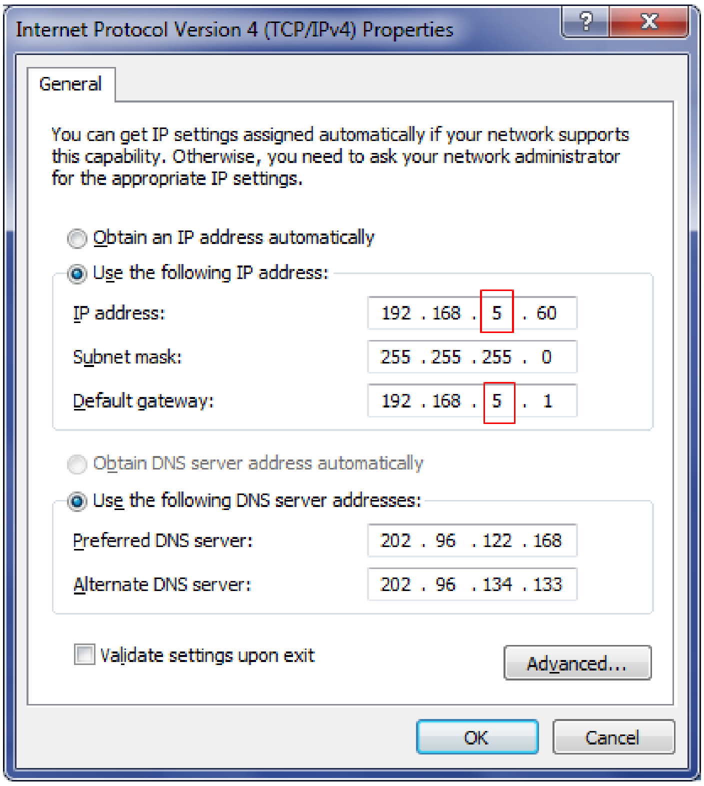
E.g.: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follows:

Step 1 Open "Control Panel > Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2 Change the selected "5" in red frame of the picture below to "1".



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 5 . 60
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 5 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 202 . 96 . 122 . 168
Alternate DNS server: 202 . 96 . 134 . 133

□ Validate settings upon exit

Step 3 Click “OK”, IP address modifies successfully.

Step 4 End.

⚠ Notice

In windows system, if user adopts the advanced configuration function of IP address and accesses the switch device via setting IP dummy address, the following managed functions can't be achieved: IEEE 802.1x polling.

1.3 Log in the Web Configuration Interface

Operation Steps

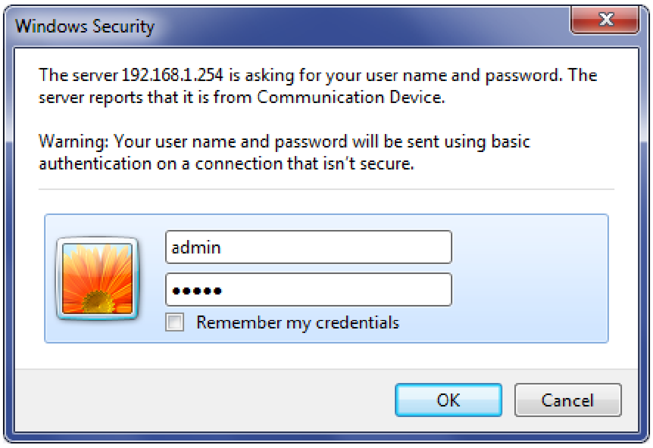
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 On the browser's address bar, type in the switch addresses "http://192.168.1.254 ".

Step 3 Click the “Enter” key.

Step 4 Pop-up a window as the figure below, enter the user name and password on the login window.



Windows Security

The server 192.168.1.254 is asking for your user name and password. The server reports that it is from Communication Device.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

admin

•••••

□ Remember my credentials

Notes:

- The default username and password are “admin”, please strictly distinguish capital and small letter while entering.
- Default username and password have the administrator privileges.

Step 5 Click "OK".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.

Notes:

After login in the device, modify the switch IP address for usage convenience.

2 System Configuration

2.1 System Information

Function Description

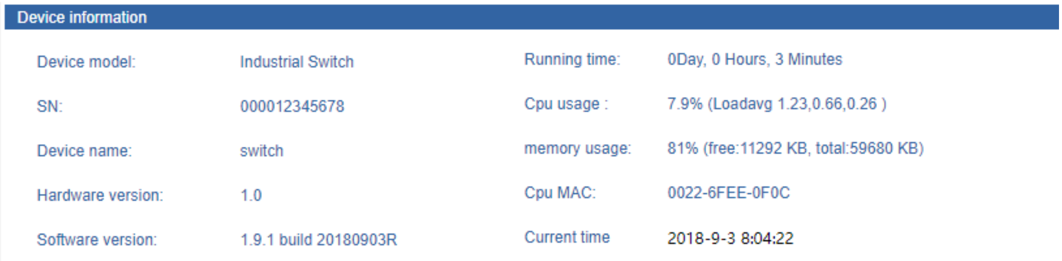
In "System Information" page, user can check "Device Information" and "Port Info".

Operation Path

Open in order: "Main Menu > System Config > System Information".

Interface Description

Device information interface as follows:



Device information

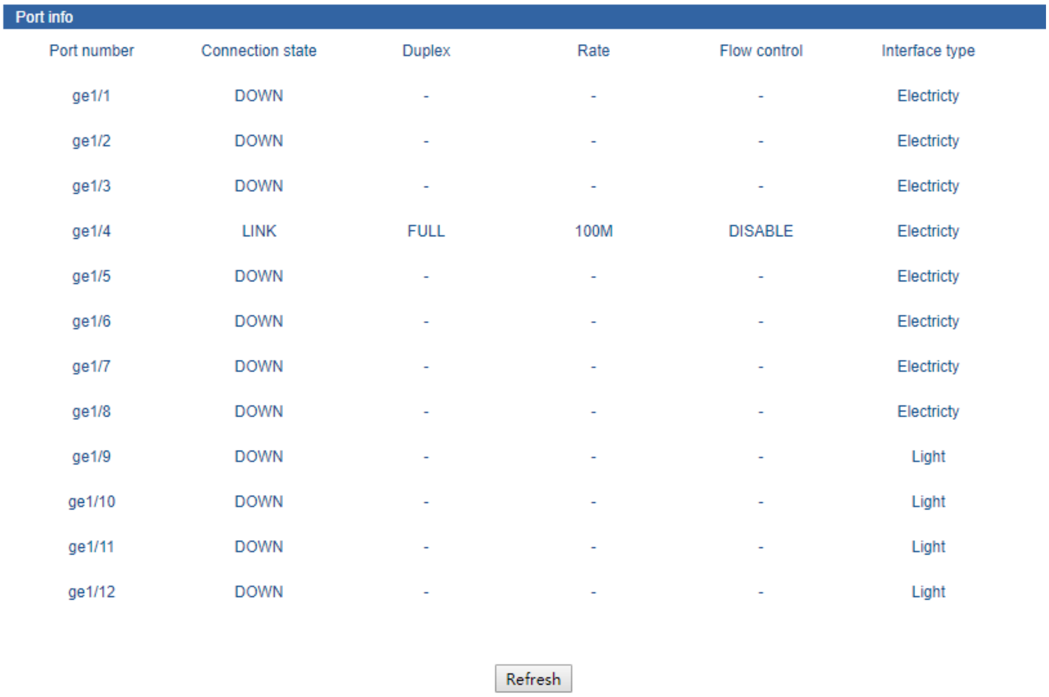
Device model:	Industrial Switch	Running time:	0Day, 0 Hours, 3 Minutes
SN:	000012345678	Cpu usage :	7.9% (Loadavg 1.23,0.66,0.26)
Device name:	switch	memory usage:	81% (free:11292 KB, total:59680 KB)
Hardware version:	1.0	Cpu MAC:	0022-6FEE-0F0C
Software version:	1.9.1 build 20180903R	Current time	2018-9-3 8:04:22

The main element configuration description of device information interface:

Interface Element	Description
Device model	The batch number used by the device to facilitate the management of device tags.
SN	SN code, product serial number.
Device name	The network identity of the device
Hardware Version	Current hardware version information, pay attention to the hardware version limits in software version.

Interface Element	Description
Software Version	Current using software version information, updated software version has more functions.
Running time	Current device running time after power on.
CPU usage	Current device CPU utilization ratio.
Memory usage	Current device memory utilization ratio.
CPU MAC	Hardware address of device factory configuration.
Current time	The information display of current data and time

Port information interface as follows:



Port info

Port number	Connection state	Duplex	Rate	Flow control	Interface type
ge1/1	DOWN	-	-	-	Electricty
ge1/2	DOWN	-	-	-	Electricty
ge1/3	DOWN	-	-	-	Electricty
ge1/4	LINK	FULL	100M	DISABLE	Electricty
ge1/5	DOWN	-	-	-	Electricty
ge1/6	DOWN	-	-	-	Electricty
ge1/7	DOWN	-	-	-	Electricty
ge1/8	DOWN	-	-	-	Electricty
ge1/9	DOWN	-	-	-	Light
ge1/10	DOWN	-	-	-	Light
ge1/11	DOWN	-	-	-	Light
ge1/12	DOWN	-	-	-	Light

The main element configuration description of port information interface.

Interface Element	Description
Port number	The port name that the device's Ethernet port corresponds to
Connection state	Port connection state, display state as follows: ● "LINK" represents connected port; ● "DOWN" represents disconnected port.
Duplex	Port duplex state, display state as follows: ● "HALF" represents the corresponding port is in half-duplex state;

Interface Element	Description
	● "FULL" represents corresponding port is in full duplex state.
Rate	Current port link rate, valid after port connection, display speed as follows: ● 10M; ● 100M; ● 1000M.
Flow control	Port flow control state, it shows as below: ● DISABLE: disable ● tx: enable port flow control of data sending ● rx: enable port flow control of data receiving ● both: enable port flow control of both data sending and receiving
Interface type	Interface type, display port type as follows: ● electricity; ● Light.

2.2 Configure Network

Function Description

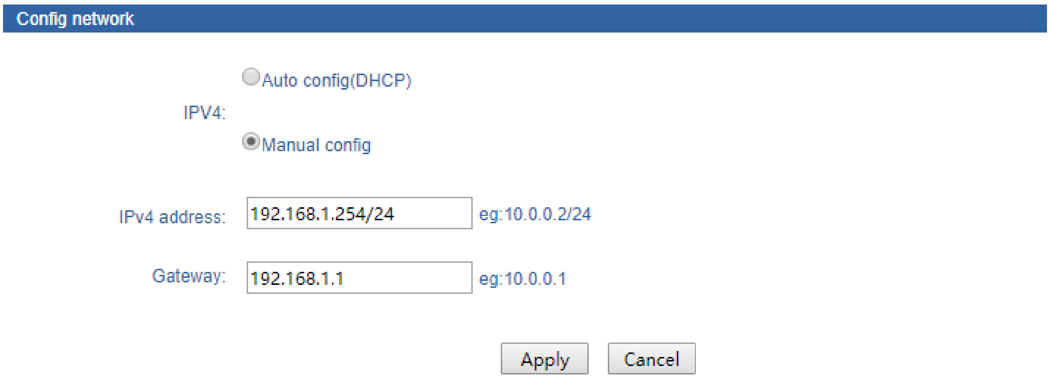
On the "Network Setting" page, configure the device IP address and gateway. Network configuration supports two models, automated acquisition (DHCP) and manual configuration.

Operation Path

Open in order: "Main Menu > System Configuration > Network Setting".

Interface Description

Network Setting interface as follows:



IPV4: ○ Auto config(DHCP) ● Manual config

IPv4 address: 192.168.1.254/24 eg:10.0.0.2/24

Gateway: 192.168.1.1 eg:10.0.0.1

The main element configuration description of network setting interface.

Interface Element	Description
IPV4	IPv4 address access method, manual configuration and automatic acquisition. ● "Automatic Acquisition (DHCP)", automatic acquisition is open DHCP function; obtain the IP address of the device through HyperTerminal. Connect to INTERNET function to use NTP, please fill in the correct gateway and DNS address. ● "Manual Configuration", fill in the static IP address, user needs to manually fill in the IPV4 address and gateway.
IPv4 address	Manually enter device IP address and subnet mask information, such as: 10.0.0.2/24.
Gateway	Fill in the gateway address information of device, e.g.: 10.0.0.1.

2.3 User Configuration

Function Description

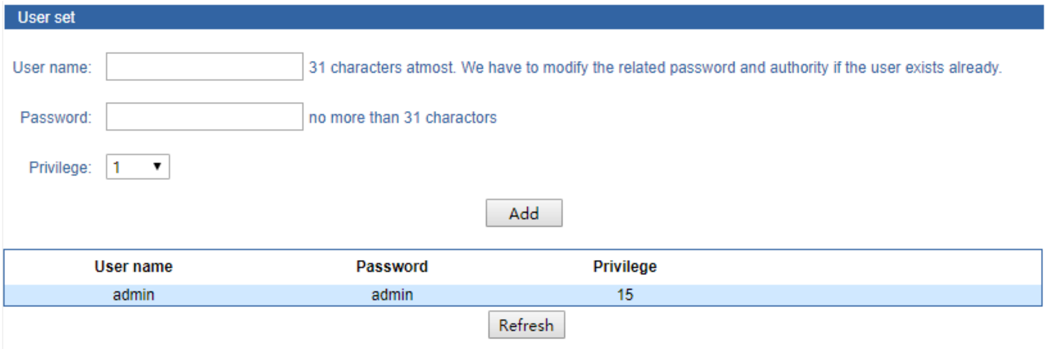
On the "User Configuration" page, user is free to add and delete username, user needs to enter username and password to access the device, the initial username and password are: admin.

Operation Path

Open in order: "Main Menu > System Config > User Config".

Interface Description

User configuration interface as follows:


User set

User name: 31 characters atmost. We have to modify the related password and authority if the user exists already.

Password: no more than 31 charactors

Privilege: 1

User name	Password	Privilege
admin	admin	15

The main element configuration description of user configuration interface:

Interface Element	Description
User name	Visitor’s identification, it can't be empty. Notes: Maximum 31 characters, if the user has existed in system, user should modify relative password and privilege.
Password	Password used by visitor, it can't be empty, maximum 31 characters.
Privilege	The visitor's privilege is 1-15. Notes: Privilege 1-2: Only conduct read-only operation in the command line; Privilege 3-15: It can conduct all operations. In this device, these privileges only work when user adopts Telnet or HyperTerminal to access the device. Any privilege in the WEB interface can perform all operations.

2.4 Log Information

Function Description

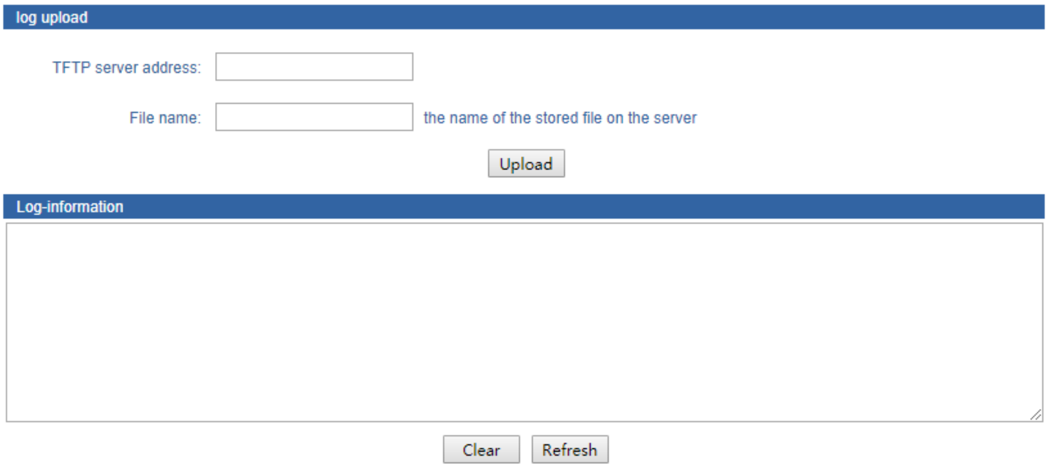
On the "Log Information" page, user can view the log information of the device and upload the log information to the tftp server.

Operation Path

Open in order: " Main menu > System configuration > Log information".

Interface Description

Log information interface as follows:



log upload

TFTP server address:

File name: the name of the stored file on the server

The main element configuration description of log information interface.

Interface Element	Description
TFTP server	Upload log TFTP server IP address.
File name	Log stored file name, its path is decided by TFTP server.

2.5 SSHD Configuration

Function Description

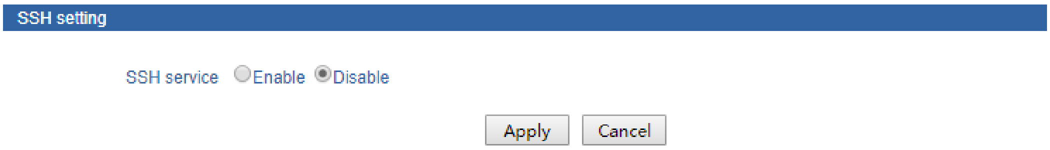
On the "SSHD Config" page, enable/disable the SSH service function. The full English name of SSH is Secure Shell. SSH is the security protocol based on the application layer and transport layer. SSH is a currently reliable protocol that provides security protocol for remote login sessions and other web services. SSH protocol can effectively prevent the information leakage in the process of remote management issues, and DNS and IP spoofing. In addition, the transmitted data is compressed so that the transmission speed can be increased.

Operation Path

Open in order: "Main Menu > System Config > SSHD Config".

Interface Description

SSHD configuration interface as follows:



SSH service ○Enable ●Disable

The main element configuration description of SSHD configuration interface.

Interface Element	Description
SSH service	SSH service function status, the options are as follows: • Enable; • Disable.

2.6 TELNET Configuration

Function Description

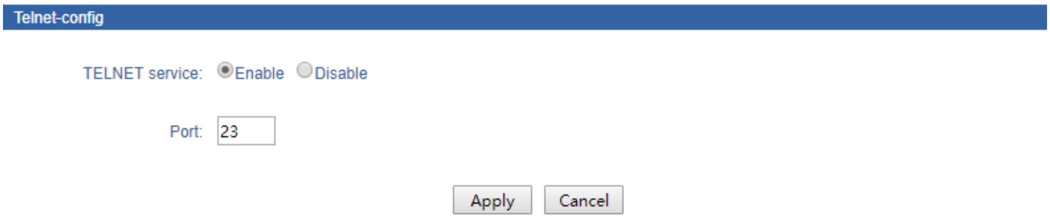
On the "TELNET Config" page, user can enable TELNET service. TELNET terminal can be connected to the switch through the Telnet PC client.

Operation Path

Open in order: "Main Menu > System Config > TELNET Config".

Interface Description

TELNET configuration interface as follows:



TELNET service: ●Enable ○Disable

Port: 23

The main element configuration description of TELNET configuration interface.

Interface Element	Description
TELNET service	TELNET service function status, the options are as follows: • Enable; • Disable.
Port	Telnet service port number, default port number is 23.

2.7 HTTPS Setting

Function Description

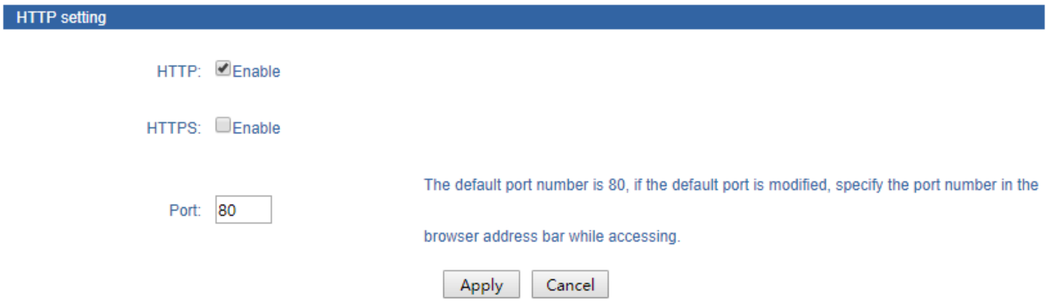
On the "HTTPS Setting" page, enable the HTTP or HTTPS protocol, PC can use browser to access the switch. HTTPS (Full name: Hypertext Transfer Protocol over Secure Socket Layer), is the HTTP channel which takes safety as the goal, is simply a safe version of HTTP. HTTPS provides data encryption services to prevent the attacker to intercept the transmitted message between the Web browser and web server, obtain some sensitive information, such as credit card numbers, passwords, etc.

Operation Path

Open in order: "Main Menu > System Config > HTTPS Config".

Interface Description

HTTPS configuration interface as follows:



HTTP setting

HTTP: ☑Enable

HTTPS: ☐Enable

Port: 80

The default port number is 80, if the default port is modified, specify the port number in the browser address bar while accessing.

The main element configuration description of HTTPS configuration interface:

Interface Element	Description
HTTP	Device HTTP protocol function status, enable checkbox. Notes: HTTP access format is: HTTP://192.168.1.254, Address is corresponding switch IP address.
HTTPS	Device HTTP protocol function status, enable checkbox. Notes: HTTPS access format is : HTTPS://192.168.1.254, Address is corresponding switch IP address.
Port	HTTP protocol service port number, the default port number is 80, if the default port is modified, specify the port number in the browser address bar while accessing.

2.8 Diagnostic Test

2.8.1 Ping

Function Description

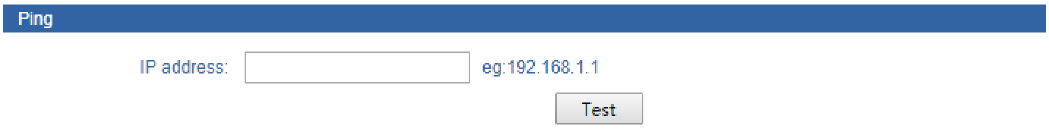
On the "Ping" page, Ping is used to check whether the network is open or network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether two network machines are connected and communicated, and confirm the time delay.

Operation Path

Open in order: "Main Menu > System Config > Diagnostic Test > Ping".

Interface Description

Ping information interface as follows:



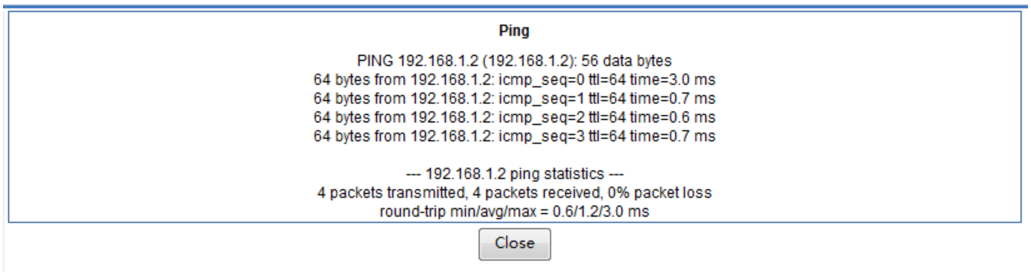
The main element configuration description of Ping configuration interface.

Interface Element	Description
IP Address	The IP address of the detected device, that is, the destination address. The device can check the network intercommunity to other devices via the ping command.

Ping Configuration Steps:

Step 1 Fill in the needed IP address in the IP address text box;

Step 2 Click the "Test" to see the Ping results;



Ping

```
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=3.0 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.7 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.6 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.7 ms

--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.6/1.2/3.0 ms
```

Step 3 End.

2.8.2 TRACEROUTE

Function Description

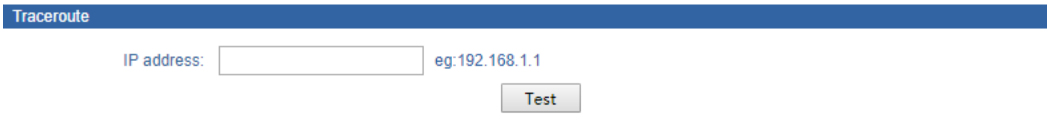
In the "TRACEROUTE" page, users can test the network situation between the switch and the target host. Traceroute sends the data packet to destination device and measure the cost time. Each Traceroute will measure a route for three times. Output result includes each test time (ms), device name (if exists) and the IP address.

Operation Path

Open in order: "Main Menu > System Config > Diagnostic Test > Traceroute".

Interface Description

TRACEROUTE interface as follows:



Traceroute

IP address: eg:192.168.1.1

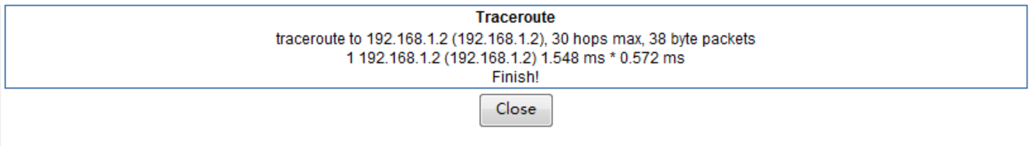
The main element configuration description of TRACEROUTE interfaces:

Interface Element	Description
IP Address	Destination device IP address, fill in the opposite device IP address that needs test.

TRACEROUTE Configuration Steps:

Step 1 Fill in the destination IP address in the "IP address" text box;

Step 2 Click the "Test" to see the results, as the picture below.



Traceroute

```
traceroute to 192.168.1.2 (192.168.1.2), 30 hops max, 38 byte packets
1 192.168.1.2 (192.168.1.2) 1.548 ms * 0.572 ms
Finish!
```

Notes:

The picture above shows the time from device to IP address 192.168.1.2, after a jump, the three times were 2991.014ms, 2995.141ms and 3006.380ms.

Step 3 End.

2.8.3Port Loopback

Function Description

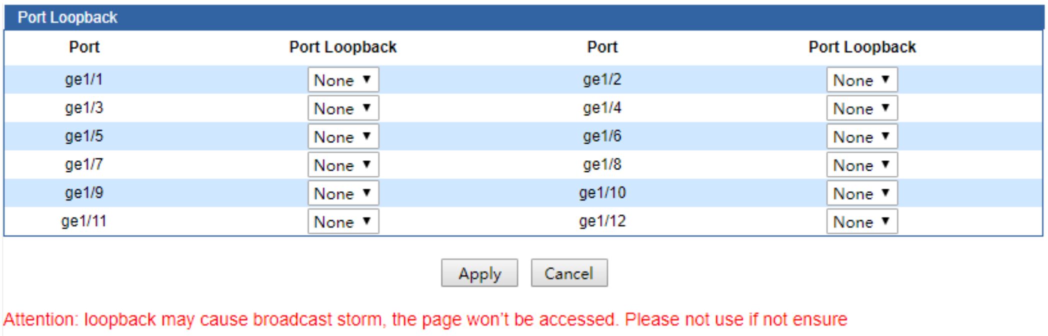
On "Port Loopback" page, user can measure the loopback situation of the switch port PHY or MAC for the convenience of troubleshooting. Port loopback is a common method for the maintenance and troubleshooting of communication port line. Connect the sending end of tested device or line to its receiving end, then the tested device can judge whether the line or port exists breakpoint by receiving the signal sent by it. The test instrument hanged on the loopback route can also test the transmission quality of the loopback route.

Operation Path

Open in order: "Main Menu > System Config > Diagnostic Test > Port Loopback".

Interface Description

Port loopback interface as follows:



Port Loopback

Port	Port Loopback	Port	Port Loopback
ge1/1	None ▼	ge1/2	None ▼
ge1/3	None ▼	ge1/4	None ▼
ge1/5	None ▼	ge1/6	None ▼
ge1/7	None ▼	ge1/8	None ▼
ge1/9	None ▼	ge1/10	None ▼
ge1/11	None ▼	ge1/12	None ▼

Attention: loopback may cause broadcast storm, the page won't be accessed. Please not use if not ensure

The main element configuration description of port loopback interface:

Interface Element	Description

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Port Loopback	Port loopback method, options as follows: ● None: that is the port disable port loopback function; ● MAC: Data is looped back after transmitted to the MAC layer of Ethernet; ● PHY: Data is looped back after transmitted to the physical layer of Ethernet. Notes: After test, please restore the port loopback mode to default None to ensure the normal communication of ports.

3 Port Configuration

3.1 Port Setting

Function Description

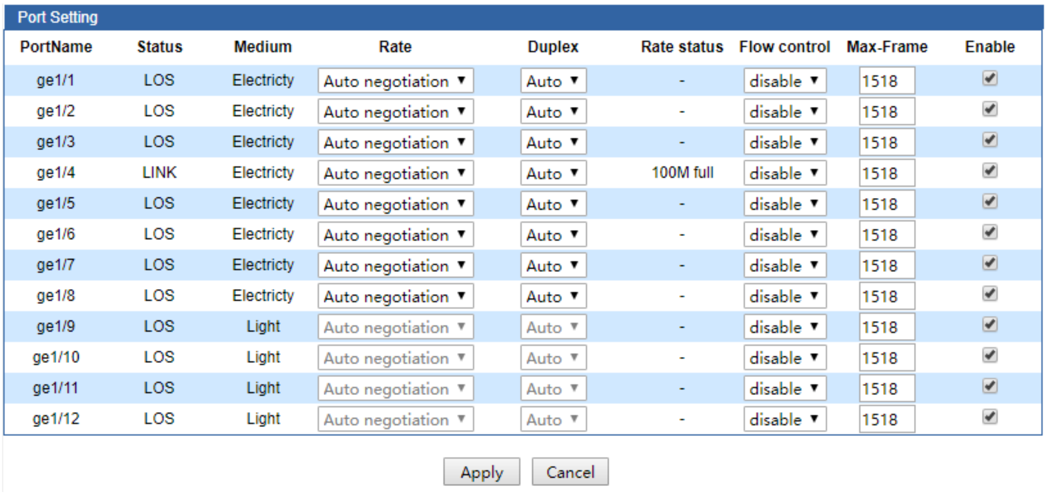
On the "Port Setting" page, user can check port type, rate and connection state, set rate mode, duplex mode, port enable, flow control and other parameters.

Operation Path

Open in order: " Main Menu > Port Config > Port Setting".

Interface Description

Port setting interface as follows:



PortName	Status	Medium	Rate	Duplex	Rate status	Flow control	Max-Frame	Enable
ge1/1	LOS	Electricty	Auto negotiation	Auto	-	disable	1518	☑
ge1/2	LOS	Electricty	Auto negotiation	Auto	-	disable	1518	☑
ge1/3	LOS	Electricty	Auto negotiation	Auto	-	disable	1518	☑
ge1/4	LINK	Electricty	Auto negotiation	Auto	100M full	disable	1518	☑
ge1/5	LOS	Electricty	Auto negotiation	Auto	-	disable	1518	☑
ge1/6	LOS	Electricty	Auto negotiation	Auto	-	disable	1518	☑
ge1/7	LOS	Electricty	Auto negotiation	Auto	-	disable	1518	☑
ge1/8	LOS	Electricty	Auto negotiation	Auto	-	disable	1518	☑
ge1/9	LOS	Light	Auto negotiation	Auto	-	disable	1518	☑
ge1/10	LOS	Light	Auto negotiation	Auto	-	disable	1518	☑
ge1/11	LOS	Light	Auto negotiation	Auto	-	disable	1518	☑
ge1/12	LOS	Light	Auto negotiation	Auto	-	disable	1518	☑

The main element configuration description of port setting interface.

Interface Element	Description

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
State	Ethernet port connection status, display status as follows: ● LOS: represent the port is disconnected; ● LINK: represent the port is connected.
Medium	Ethernet port connection type, display medium as follows: ● Copper port; ● Fiber port.
Rate	Ethernet port working speed, optional speed as follows: ● Auto negotiation: 10/100/1000 M speed self-adaption; ● 10M only; ● 100M only; ● 1000 M only.
Duplex	The duplex mode of Ethernet mode, options are: ● Auto-negotiation: full/half duplex self-adaption; ● Full; ● Half.
Rate status	Port rate and duplex mode, status as follows: ● -: port has no connection ● 1000M full: gigabit full duplex; ● 100M full: 100M full duplex; ● 100M half: 100M half duplex; ● 10M full: 10M full duplex; ● 10M half: 10M half duplex..
Flow control	Port flow control status, options as follows: ● Disable: Disable; ● Tx: Enable port data sending flow control; ● Rx: Enable port data receiving control; ● Both: Enable port data sending or receiving flow control.
Max-Frame	Ethernet port transmitted maximum data frame length, input range 64-16356.
Enable	Enable Ethernet port. Note: If user doesn't check the port "Enable" checkbox, the port won't be connected to use.

3.2 Storm Control

Function Description

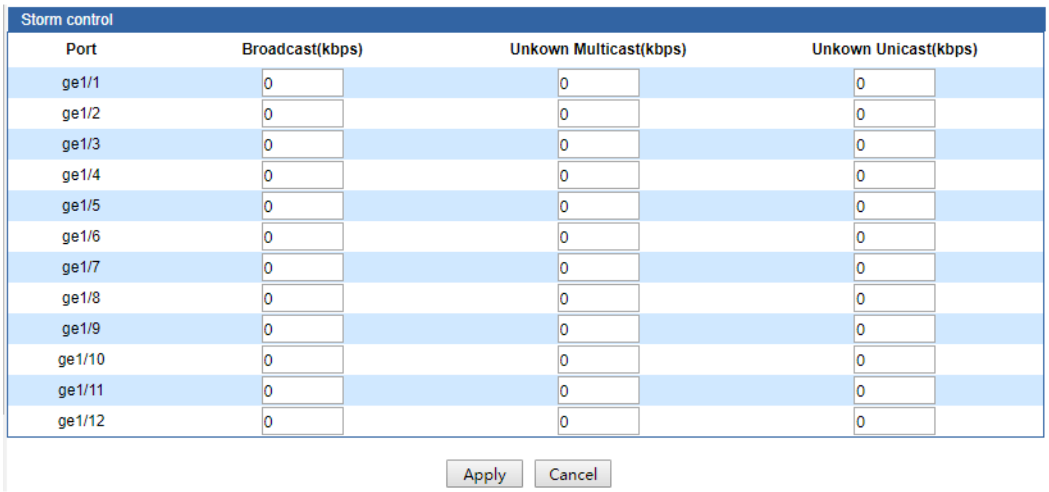
On the "Storm Control" page, user can set the maximum broadcast, multicast or unknown unicast packet flow the port allows. When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast or unknown unicast flow limit, so that the proportion of overall broadcast, unknown multicast or unknown unicast flow can be reduced to limited range, ensuring the normal operation of network business.

Operation Path

Open in order: "Main Menu > Port Config > Storm control".

Interface Description

Storm control interface as follows:



Storm control

Port	Broadcast(kbps)	Unkown Multicast(kbps)	Unkown Unicast(kbps)
ge1/1	0	0	0
ge1/2	0	0	0
ge1/3	0	0	0
ge1/4	0	0	0
ge1/5	0	0	0
ge1/6	0	0	0
ge1/7	0	0	0
ge1/8	0	0	0
ge1/9	0	0	0
ge1/10	0	0	0
ge1/11	0	0	0
ge1/12	0	0	0

The main element configuration description of storm control interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Broadcast (kbps)	The port control for broadcast packet transmission speed, input value range of 100M port is 0-100000, input value range of 1000M port is 0~1000000. Notes: Broadcast packet, that is the destination address is

Interface Element	Description
	FF-FF-FF-FF-FF-FF data frame.
Unknown Multicast (kbps)	The port control for unknown multicast data packet transmission speed, input value range of 100M port is 0-100000, input value range of 1000M port is 0~1000000. Notes: Multicast packet, that is destination address is XX-XX-XX-XX-XX-XX data frame, the second X is odd number, such as: 1, 3, 5, 7, 9, B, D, F, other X represents arbitrary number.
Unknown Unicast (kbps)	The port control for unknown unicast data packet transmission speed, input value range of 100M port is 0-100000, input value range of 1000M port is 0~1000000. Notes: Unknown unicast packet, that is the MAC address of the data frame doesn't exist in the MAC address table of the device, which needs to be forwarded to all ports.

3.3 Port Rate Limit

Function Description

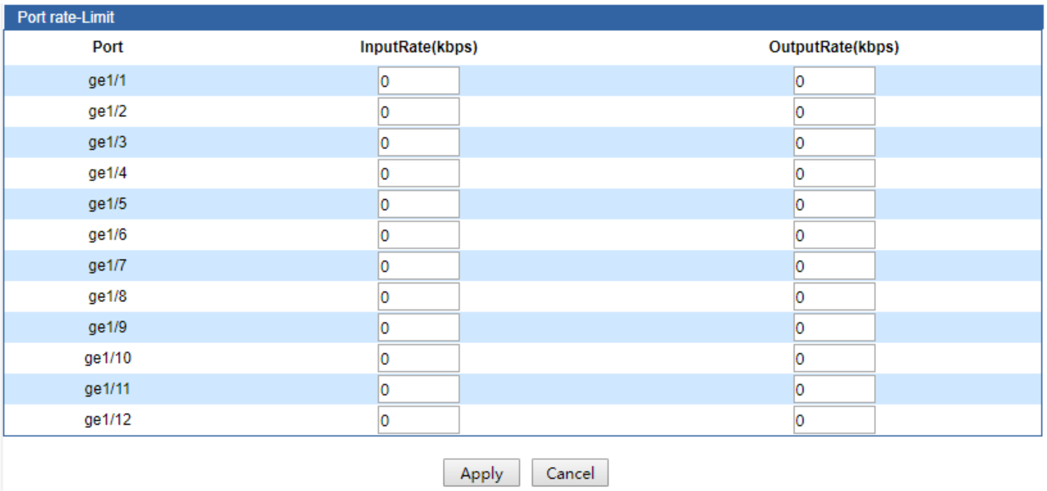
On the "Port rate-Limit" page, User can limit the communication flow of each port or cancel the port flow limit. The device provides port speed limit, including entrance and exit speed limit. User can select a fixed speed, its range is: 0kbps-100Mbps (100M), 0kbps-1000Mbps (Gigabit), the device will discard the packet or adopt flow control to limit the transmission speed or receiving speed of opposite device according to the flow control is enabled or not.

Operation Path

Open in order: "Main menu > Port Config > Port rate-Limit".

Interface Description

Port rate limit interface as follows:



Port rate-Limit

Port	InputRate(kbps)	OutputRate(kbps)
ge1/1	0	0
ge1/2	0	0
ge1/3	0	0
ge1/4	0	0
ge1/5	0	0
ge1/6	0	0
ge1/7	0	0
ge1/8	0	0
ge1/9	0	0
ge1/10	0	0
ge1/11	0	0
ge1/12	0	0

The main element configuration description of port rate limit interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Input Rate(kbps)	The port limit for all input data transmission speed, input value range of 100M port is 0-100000, input value range of 1000M port is 0~1000000.
Output Rate(kbps)	The port control for all output data transmission speed, input value range of 100M port is 0-100000, input value range of 1000M port is 0~1000000.

Note

- When using the port rate limit, flow control should be enabled, otherwise the rate between devices will no longer be a smooth curve;
- When using the port rate limit, packet loss should not occur unless the flow control is disabled. The fast or slow transmission speed represents packet loss;
- Port rate limit has a high quality requirement to network cable; otherwise there will occur a lot of conflict and broken packets.

3.4 Mirror

Function Description

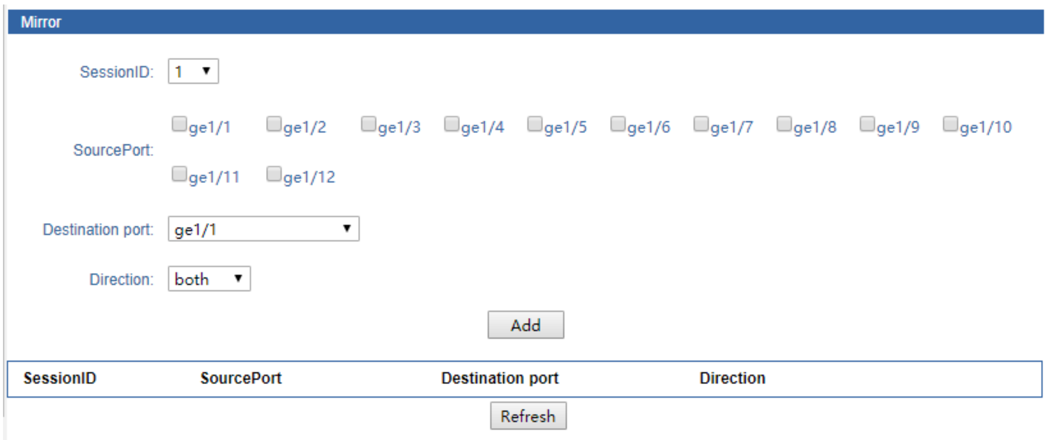
On the "Mirror" page, user can copy the data from the origin port to appointed port for data analysis and monitoring.

Operation Path

Open in order: "Main menu > Port Config > Mirror".

Interface Description

Mirror interface as follows:


Mirror

SessionID: 1

SourcePort: □ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8 □ge1/9 □ge1/10 □ge1/11 □ge1/12

Destination port: ge1/1

Direction: both

SessionID	SourcePort	Destination port	Direction

The main element configuration description of mirror interface:

Interface Element	Description
Session ID	Device mirror ID number, value is 1~4. Notes: The device supports maximum 4-way mirror sessions.
Source port	A set of monitored ports, which will collect data from these ports in the specified direction, and the mirror port can be one or more.
Destination	A port for monitoring, and the device outputs data from the port to the specified direction.

Interface Element	Description
Direction	This parameter specifies the direction of the monitoring port data, a total of "ingress", "egress", "both" three options. Monitor can choose according to their own needs. ● ingress: import data, the packet received by the port will be mirrored to the destination port; ● egress: export data, the message sent by the port will be mirrored to the destination port; ● Both: all data, mirror the port receiving and sending packets at the same time.

Note

- The function must be shut down in normal usage, otherwise all senior management functions based on port are not available, such as RSTP, IGMP-Snooping, etc.
- Mirror function only deals with FCS normal packet; it cannot handle the wrong data frame

3.5 Alarm Settings

Function Description

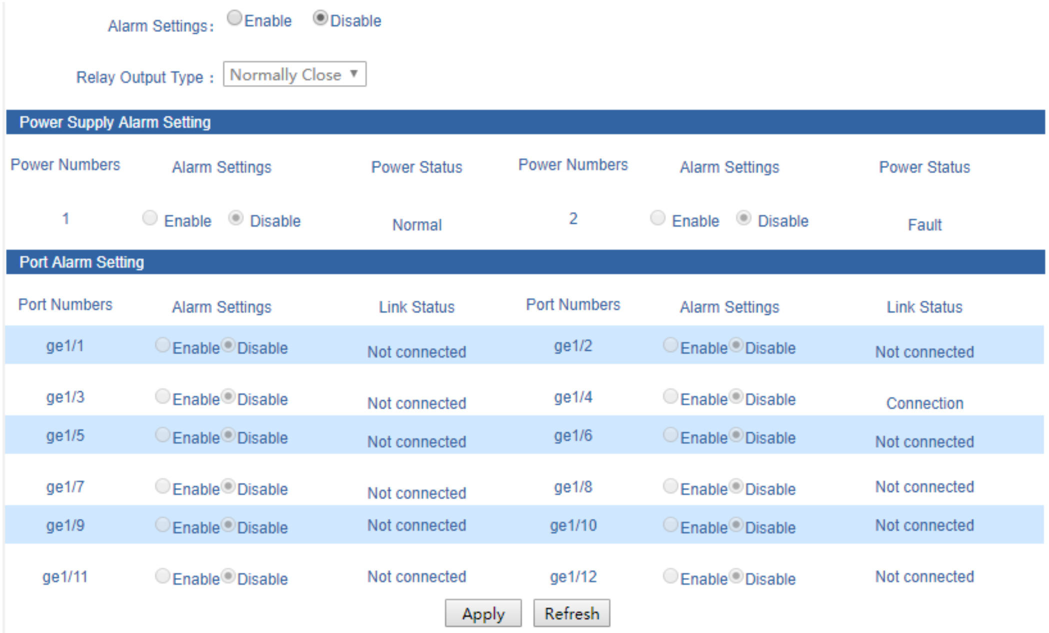
On the "Alarm Settings" page, user can set power supply alarm, port alarm function; when the equipment is in abnormal state, it can promptly notify the administrator, and quickly repair the equipment status to avoid excessive losses.

Operation Path

Open in order: "Main Menu > Port Config > Alarm Settings".

Interface Description

Alarm settings interface as follows:



Alarm Settings: ○Enable ●Disable

Relay Output Type : Normally Close ▼

Power Supply Alarm Setting

Power Numbers	Alarm Settings	Power Status	Power Numbers	Alarm Settings	Power Status
1	○ Enable ● Disable	Normal	2	○ Enable ● Disable	Fault

Port Alarm Setting

Port Numbers	Alarm Settings	Link Status	Port Numbers	Alarm Settings	Link Status
ge1/1	○Enable●Disable	Not connected	ge1/2	○Enable●Disable	Not connected
ge1/3	○Enable●Disable	Not connected	ge1/4	○Enable●Disable	Connection
ge1/5	○Enable●Disable	Not connected	ge1/6	○Enable●Disable	Not connected
ge1/7	○Enable●Disable	Not connected	ge1/8	○Enable●Disable	Not connected
ge1/9	○Enable●Disable	Not connected	ge1/10	○Enable●Disable	Not connected
ge1/11	○Enable●Disable	Not connected	ge1/12	○Enable●Disable	Not connected

The main element configuration description of alarm setting interface.

Interface Element	Description
Alarm Settings	power supply and port alarm function status, options: • Enable; • Disable.
Relay Output Type	Relay output type status, options as follows: • Normally open: Relay is open circuit status in normal no alarm, when there is an alarm, the alarm lamp is bright, and the relay is in a closed state. • Normally closed: Relay is closed status in normal no alarm, when there is an alarm, the alarm light is bright, the relay is in the open state.
Power Supply Alarm Setting	**Power supply alarm setting**
Power Numbers	Power supply name corresponding to device power supply, "1" represents power supply PWR1, "2" represents power supply PWR2.
Alarm Settings	Power supply alarm function status, options as follows: • Enable; • Disable. Notes: DC provides 2-way power supply (AC without power supply alarm), when 1-way power supply goes wrong, another power

Interface Element	Description
	supply operates soon, double power supply hot standby. After enable power supply alarm, the device will output alarm signal to hint power supply abnormal operation when power supply status is abnormal.
Power Status	The device power supply working status, display items as follows: ● Fault; ● Normal.
Port Alarm Setting	**Port alarm setting**
Port Numbers	The corresponding port name of the device Ethernet port.
Alarm Settings	Port alarm function status, options as follows: ● Enable; ● Disable. Notes: After enable port alarm, when port occurs abnormal status, such as connection break down, the device will output a signal to hint the abnormal operation of device.
Link status	Port link status, display items as follows: ● No connection; ● Connected.

3.6 Link Aggregation

Link aggregation is the shorter form of Ethernet link aggregation; it binds multiple Ethernet physical links into a logical link, achieving the purpose of increasing the link bandwidth. At the same time, these bundled links can effectively improve the link reliability by mutual dynamic backup.

The Link Aggregation Control Protocol (LACP) protocol based on the IEEE802.3ad standard is a protocol for implementing dynamic link aggregation. Devices running this protocol exchange LACPDUs (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit) to exchange link aggregation related information.

Based on the enabling or disabling of LACP protocol, the link aggregation can be divided into two modes, static aggregation and dynamic aggregation.

3.6.1Static Configuration

Function Description

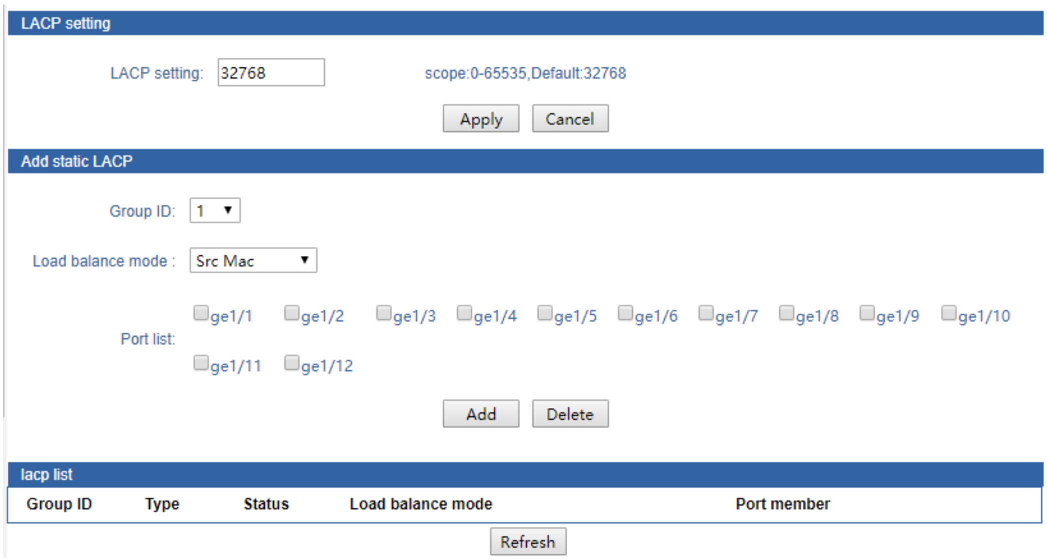
Under static aggregation mode, the member port in aggregation group disables LACP protocol, its port status is maintained manually.

Operation Path

Open in order: "Main Menu > Port Config > Link Aggregation > Static Config".

Interface Description

Static configuration interface as follows:



LACP setting

LACP setting: 32768 scope:0-65535,Default:32768

Add static LACP

Group ID: 1

Load balance mode : Src Mac

Port list: □ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8 □ge1/9 □ge1/10 □ge1/11 □ge1/12

lacp list

Group ID	Type	Status	Load balance mode	Port member

The main element configuration description of static configuration interface.

Interface Element	Description
LACP setting	**LACP setting column.**
LACP setting	LACP priority level setting, LACP setting range 0-65535, defaults to 32768. Notes: The smaller of interface LACP priority level value is, the higher priority level is, which is used for distinguishing the priority degree of selecting different ports as active port.
Add static LACP	**Add static aggregation group setting column.**
Group ID	Static aggregation link ID number, support maximum 16 groups, each group can configure 8 ports to join aggregation.
Load balance	Load balance mode is the flow load balance in aggregation

Interface Element	Description
mode	group, there exist 3 options: ● Src Mac: Conduct load balance according to the message MAC address, messages with the same source MAC addresses pass via the same port when , otherwise, messages pass via different ports; ● Dst Mac: Conduct load balance according to the message destination MAC address, messages with the same destination MAC addresses pass via the same port, otherwise, messages pass via different ports; ● Src&Dst Mac: Conduct load balance according to the message source and destination MAC address, messages with the same source and destination MAC addresses pass via the same port, otherwise, messages pass via different ports;
Port list	Device port list, check the port to join aggregation group.
LACP list	**LACP list column.**
Group ID	Added port aggregation group ID number.
Type	Aggregation group mode: ● Manual: Static aggregation; ● LACP: Dynamic aggregation.
State	Aggregation group connection state: ● UP: Port member is connected; ● DOWN: Port member is disconnected.
Load balance mode	Load balance mode: ● Src Mac; ● Dst Mac; ● Src&Dst Mac.
Port member	Port member in the aggregation group.

3.6.2 LACP Configuration

Function Description

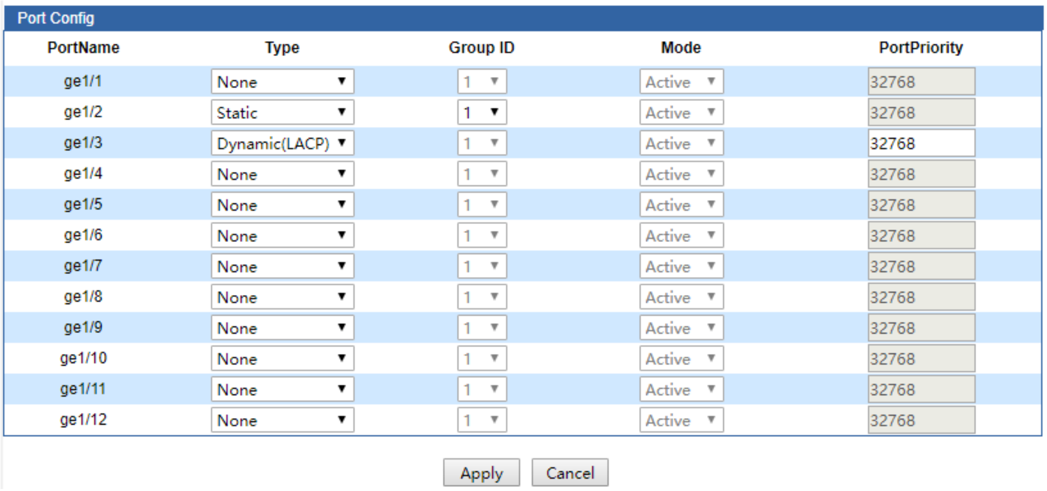
Dynamic aggregation is an aggregation method that system automatically creates or deletes aggregation group, the port addition and deleting in the dynamic aggregation group is done automatically by LACP protocol. Only ports connected to the same device with same rate, duplex property, and basic configuration can create a dynamic aggregation. Even one port can also create dynamic aggregation, at this time, its single port aggregation. In dynamic aggregation, port LACP protocol is in enable state.

Operation Path

Open in order: "Main Menu > Port Config > Link Aggregation > LACP Config".

Interface Description

LACP configuration interface as follows:



Port Config

PortName	Type	Group ID	Mode	PortPriority
ge1/1	None	1	Active	32768
ge1/2	Static	1	Active	32768
ge1/3	Dynamic(LACP)	1	Active	32768
ge1/4	None	1	Active	32768
ge1/5	None	1	Active	32768
ge1/6	None	1	Active	32768
ge1/7	None	1	Active	32768
ge1/8	None	1	Active	32768
ge1/9	None	1	Active	32768
ge1/10	None	1	Active	32768
ge1/11	None	1	Active	32768
ge1/12	None	1	Active	32768

The main element configuration description of LACP configuration interface:

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Type	Setting port aggregation function: ● None: Represent the port disabling link aggregation function; ● Static: Represent the port is static aggregation mode; ● Dynamic (LACP): Represent the port is dynamic aggregation mode.
Group ID	Group ID, the range is 1~16.
Mode	Mode refers to LACP negotiation mode, it's divided into: ● Active: The port sends LACP message periodically; ● Passive: The port doesn't send LACP message in normal time, once receiving the LACP message of

Interface Element	Description
	opposite terminal, it will normally send LACP message.
Port Priority	Dynamic LACP port priority, defaults to 32768.

3.7 Isolate-port

Function Description

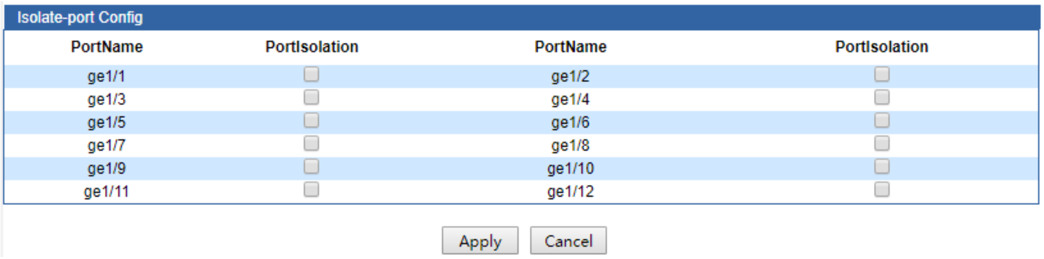
Isolate-port is for achieving layer-2 isolation between messages, it can add different ports to different VLAN, but won't waste limited VLAN sources. Adopting isolate-port characteristics can achieve isolation of ports within the same VLAN. After adding the ports to isolation group, user can achieve the layer 2 data isolation of ports within isolation group. Port isolation function has provided safer and more flexible networking scheme for users.

Operation Path

Open in order: "Main Menu > Port Configuration > Isolate-port Config".

Interface Description

Isolate-port configuration interface as follows:



Isolate-port Config

PortName	PortIsolation	PortName	PortIsolation
ge1/1	□	ge1/2	□
ge1/3	□	ge1/4	□
ge1/5	□	ge1/6	□
ge1/7	□	ge1/8	□
ge1/9	□	ge1/10	□
ge1/11	□	ge1/12	□

The main element configuration description of isolate-port config interface.

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Isolate-port	Check the port isolation optional box to enable the port isolation function within the same VLAN.

3.8 Port Statistics

3.8.1 Port Stats

Function Description

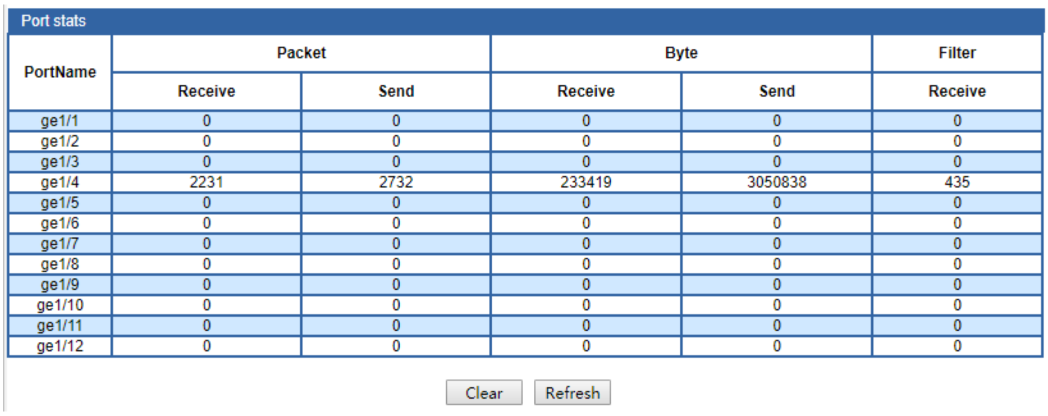
On the "Port Stats" page, user can check the data packet and byte number that each port sends or receives,

Operation Path

Open in order: "Main Menu > Port Config > Port Statistics > Port Stats".

Interface Description

Port stats interface as follows:



PortName	Packet		Byte		Filter
	Receive	Send	Receive	Send	Receive
ge1/1	0	0	0	0	0
ge1/2	0	0	0	0	0
ge1/3	0	0	0	0	0
ge1/4	2231	2732	233419	3050838	435
ge1/5	0	0	0	0	0
ge1/6	0	0	0	0	0
ge1/7	0	0	0	0	0
ge1/8	0	0	0	0	0
ge1/9	0	0	0	0	0
ge1/10	0	0	0	0	0
ge1/11	0	0	0	0	0
ge1/12	0	0	0	0	0

3.8.2 Detail Port Stats

Function Description

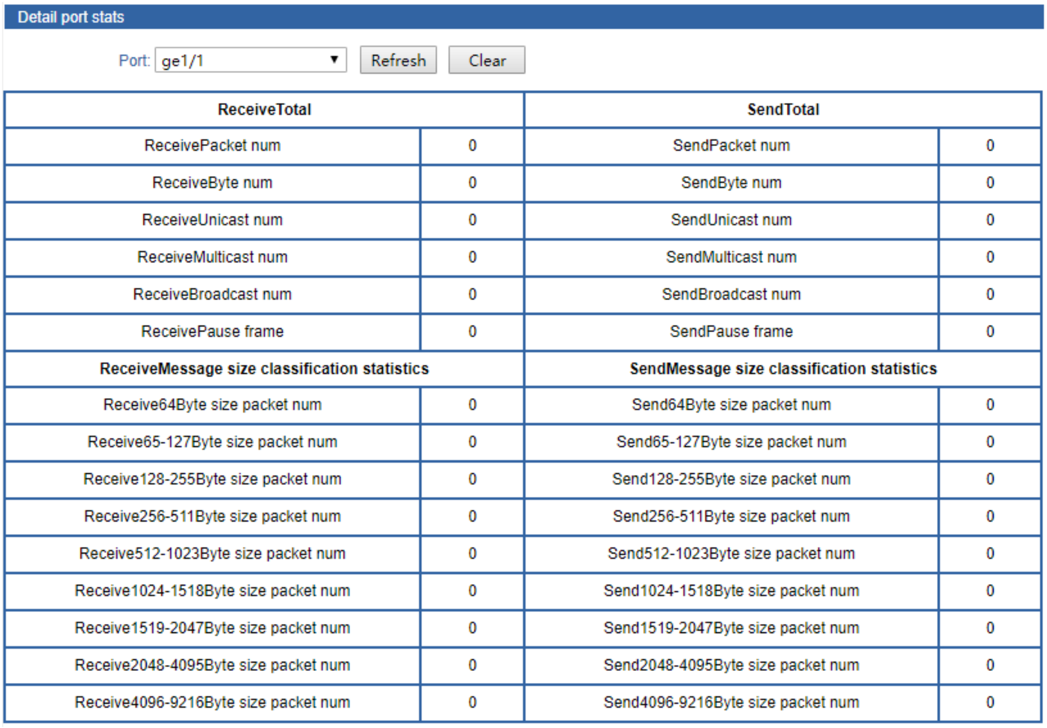
On the "Detail Port Stats" page, user can check the data sum and message size classified statistic that each port sends or receives.

Operation Path

Open in order: "Main Menu > Port Config > Port Statistics > Detail Port Stats".

Interface Description

Detail port stats interface as follows:



Detail port stats

Port: ge1/1 ▾ Refresh Clear

ReceiveTotal		SendTotal	
ReceivePacket num	0	SendPacket num	0
ReceiveByte num	0	SendByte num	0
ReceiveUnicast num	0	SendUnicast num	0
ReceiveMulticast num	0	SendMulticast num	0
ReceiveBroadcast num	0	SendBroadcast num	0
ReceivePause frame	0	SendPause frame	0
ReceiveMessage size classification statistics		**SendMessage size classification statistics**	
Receive64Byte size packet num	0	Send64Byte size packet num	0
Receive65-127Byte size packet num	0	Send65-127Byte size packet num	0
Receive128-255Byte size packet num	0	Send128-255Byte size packet num	0
Receive256-511Byte size packet num	0	Send256-511Byte size packet num	0
Receive512-1023Byte size packet num	0	Send512-1023Byte size packet num	0
Receive1024-1518Byte size packet num	0	Send1024-1518Byte size packet num	0
Receive1519-2047Byte size packet num	0	Send1519-2047Byte size packet num	0
Receive2048-4095Byte size packet num	0	Send2048-4095Byte size packet num	0
Receive4096-9216Byte size packet num	0	Send4096-9216Byte size packet num	0

4 Layer 2 Configuration

4.1 VLAN Configuration

VLAN is Virtual Local Area Network. VLAN is the data switching technology that logically (note: not physically) divides the LAN device into each network segment (or smaller LAN) to achieve the virtual working group (unit).

VLAN advantages mainly include:

- Port isolation. Ports in different VLAN, even in the same switch, can't intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLAN can't directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. Changing the network user belongs to needn't to change ports or connection; only need change the firmware configuration.

That is, ports within the same VLAN can intercommunicate; otherwise, ports can't communicate with each other. A VLAN is identified with VLAN ID, and ports with the same VLAN ID belong to a same VLAN.

4.1.1PVlan Configuration

Function Description

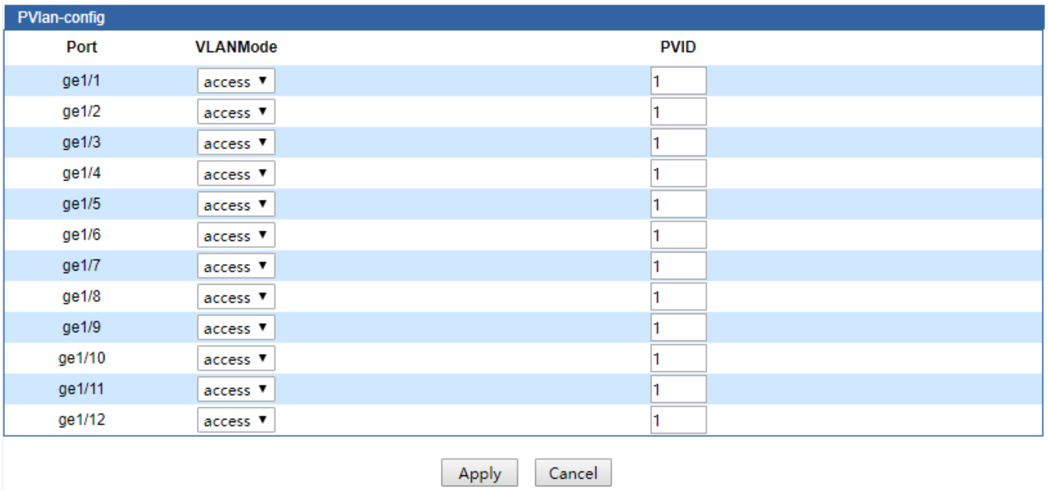
On the "PVlan-config" page, user can configure the port VLAN mode (access, trunk), and VLAN ID: PVID.

Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > PVlan-Config".

Interface Description

PVlan configuration interface as follows:



PVlan-config

Port	VLANMode	PVID
ge1/1	access	1
ge1/2	access	1
ge1/3	access	1
ge1/4	access	1
ge1/5	access	1
ge1/6	access	1
ge1/7	access	1
ge1/8	access	1
ge1/9	access	1
ge1/10	access	1
ge1/11	access	1
ge1/12	access	1

The main element configuration description of PVlan configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
VLAN Mode	Two port link types that the switch supports: ● Access: Port can only belong to 1 VLAN, which is generally used to connect user device. All default ports belong to access port. ● Trunk: Ports can belong to multiple VLAN, receive and send multiple VLAN messages, generally used in the connection between network devices.
PVID	Port0base Vlan ID is the port virtual LAN ID number, which is relative to the VLAN TAG mark when the port receives and sends data frame.

4.1.2 Trunk Configuration

Function Description

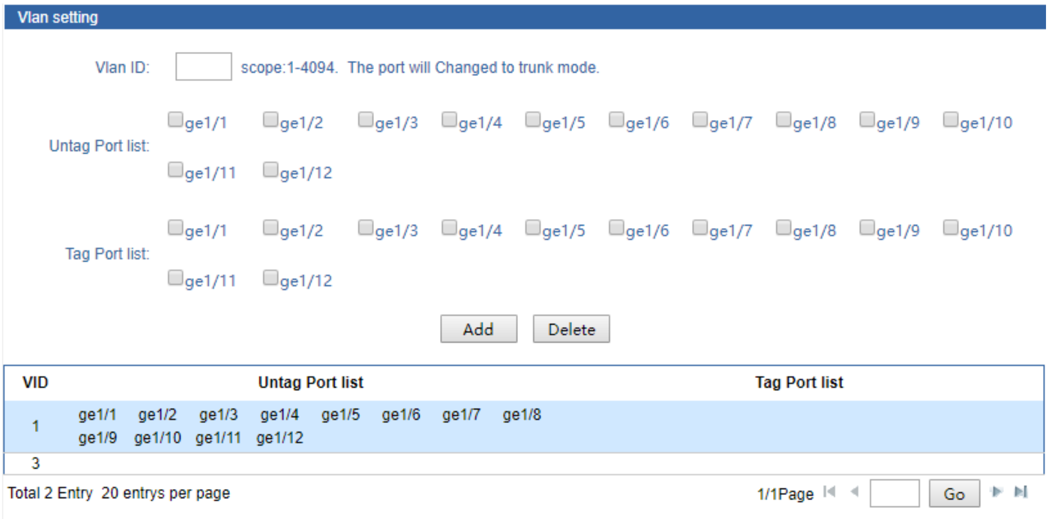
On the "Trunk-config" page, user can configure the port Untagged and Tag port list.

Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > Trunk-config".

Interface Description

Trunk configuration interface as follows:



Vlan setting

Vlan ID: scope:1-4094. The port will Changed to trunk mode.

Untag Port list: □ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8 □ge1/9 □ge1/10 □ge1/11 □ge1/12

Tag Port list: □ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8 □ge1/9 □ge1/10 □ge1/11 □ge1/12

VID	Untag Port list	Tag Port list
1	ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12	
3		

Total 2 Entry 20 entrys per page

The main element configuration description of Trunk configuration interface.

Interface Element	Description
Vlan ID	VLAN ID number, value range is 1-4094.
Untag Port list	Check untagged port member to conduct untagged process to sending data frame.
Tag Port list	Check tag port member to conduct tagged process to sending data frame.

Process for Port Receiving and Sending Message

Port Type	Process for Receiving Message	
	When Receiving the untagged message	When Receiving Tagged Message
Access Port	Label the message with corresponding VLAN Tag of port default VLAN ID.	Keep VLAN ID unchanged, without replacing.
Trunk Port	Label the message with corresponding VLAN Tag of	Keep VLAN ID unchanged, without replacing.

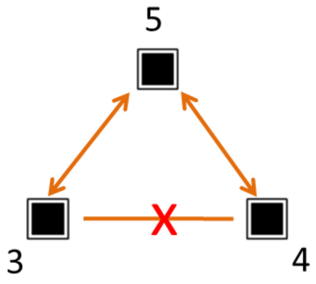
Port Type	Process for Receiving Message	
	When Receiving the untagged message	When Receiving Tagged Message
	port default VLAN ID.	

Port Type	Process for Sending Message
Untag	Forward the untagged message during forwarding
Tag	Forward the tagged message during forwarding

Access port type can only be Untagged, Trunk port type can be Untagged or Tag.

Example: Typical VLAN Configuration

Suppose that the switch port 3, 4 and 5 have the following requirements: Port 3 and Port 5 communicate with each other. Port 4 and Port 5 communicate with each other. Port 3 and Port 4 cannot communicate with each other, as the picture below. Do not consider other ports, how to set the VLAN?



Example Analysis

Port3, Port 4 and Port 5 are set with different forwarding entries, and forwarding entries enable the communication between the ports.

Analyze the port forwarding entries design as below:

- Port3

  Port3 and Port5 communicate with each other. Port3 forwarding entries include Port3 and Port5. Therefore, a forwarding entry PVID2 is designed, including Port 3 and Port 5. Plan port 3 and port 5 as "Untag Port List".

- Port4

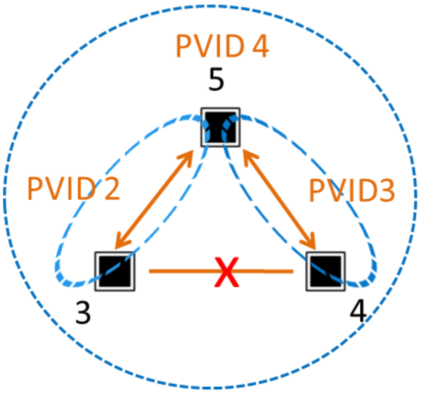
  Port4 and Port5 communicate with each other. Port3 forwarding entries include

Port4 and Port5. Therefore, a forwarding entry PVID3 is designed, including Port 4 and Port 5. Plan Port4 and Port5 as "Untag Port List".

- Port5

  Port5 and Port3, Port4 communicate with each other, Port5 forwarding entries include Port3, Port4 and Port5. Therefore, design a forwarding entry PVID4, including Port3, Port 4 and Port 5. Plan port 3, port 4 and port 5 as "Untag Port List".

According to Port3, Port 4 and Port 5 forwarding entry analysis, the forwarding entry design picture as follows:



Operation Steps

Step 1 Access "Main Menu > Layer 2 Config > VLAN Config > Trunk-config".

Step 2 Establish forwarding entry PVID2.

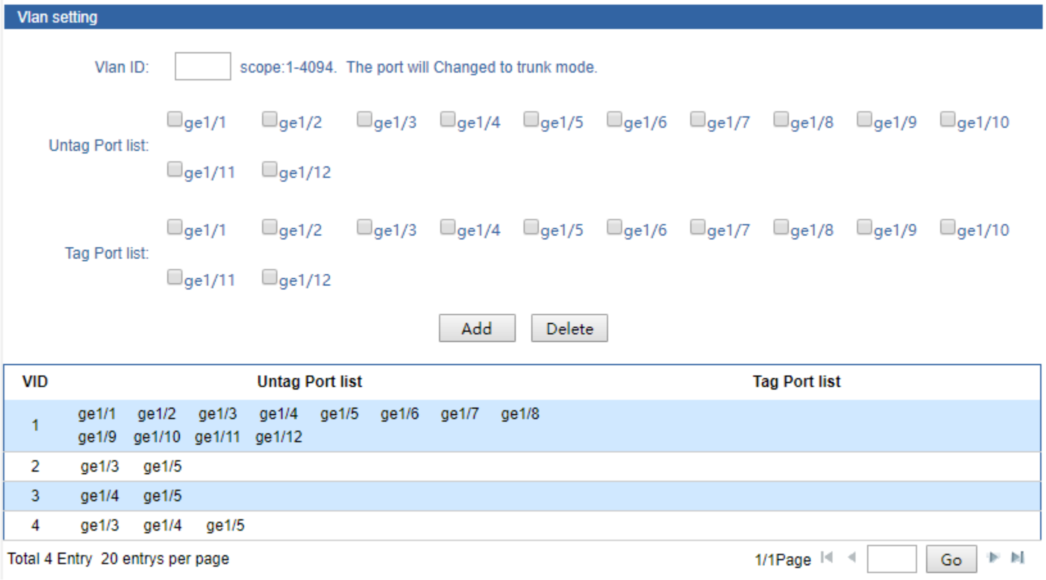
1. Enter 2 in "Vlan ID" text box;
2. Select the ports "ge1/3" and "ge1/5" checkbox under "Untag Port List";
3. Click "add" button.

Step 3 Establish forwarding entry PVID3.

1. Enter 3 in "Vlan ID" text box;
2. Select the ports "ge1/4" and "ge1/5" checkbox under "Untag Port List";
3. Click "add" button.

Step 4 Establish forwarding entry PVID4.

1. Enter 4 in "Vlan ID" text box;
2. Select the port "ge1/3", "ge1/4" and "ge1/5" checkbox under "Untag Port List";
3. Click "add" button, as the picture below.



Vlan setting

Vlan ID: scope:1-4094. The port will Changed to trunk mode.

Untag Port list: □ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8 □ge1/9 □ge1/10 □ge1/11 □ge1/12

Tag Port list: □ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8 □ge1/9 □ge1/10 □ge1/11 □ge1/12

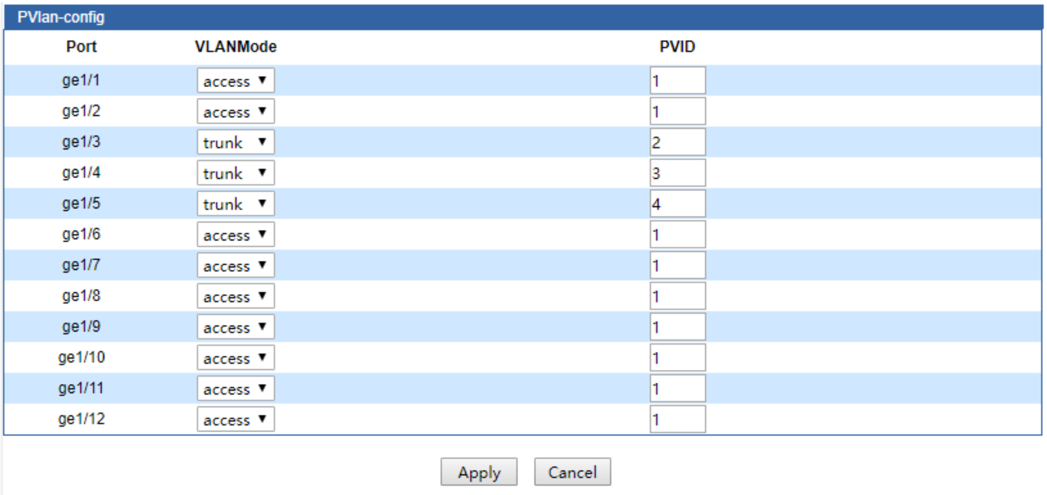
VID	Untag Port list	Tag Port list
1	ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12	
2	ge1/3 ge1/5	
3	ge1/4 ge1/5	
4	ge1/3 ge1/4 ge1/5	

Total 4 Entry 20 entrys per page 1/1Page

Step 5 Access "Main Menu > Layer 2 Config > VLAN Config > PVlan Config".

Step 6 Port corresponding forwarding entry PVID;

1. Enter 2 in the "PVID" text box in "ge1/3" configuration bar of the port;
2. Enter 3 in the "PVID" text box in the "ge1/4" configuration bar of the port;
3. Enter 4 in the "PVID" text box in "ge1/5" configuration bar of the port;
4. Click "Apply" button, as the picture below.



PVlan-config

Port	VLANMode	PVID
ge1/1	access	1
ge1/2	access	1
ge1/3	trunk	2
ge1/4	trunk	3
ge1/5	trunk	4
ge1/6	access	1
ge1/7	access	1
ge1/8	access	1
ge1/9	access	1
ge1/10	access	1
ge1/11	access	1
ge1/12	access	1

Step 7 End.

4.1.3 VLAN Configuration

Function Description

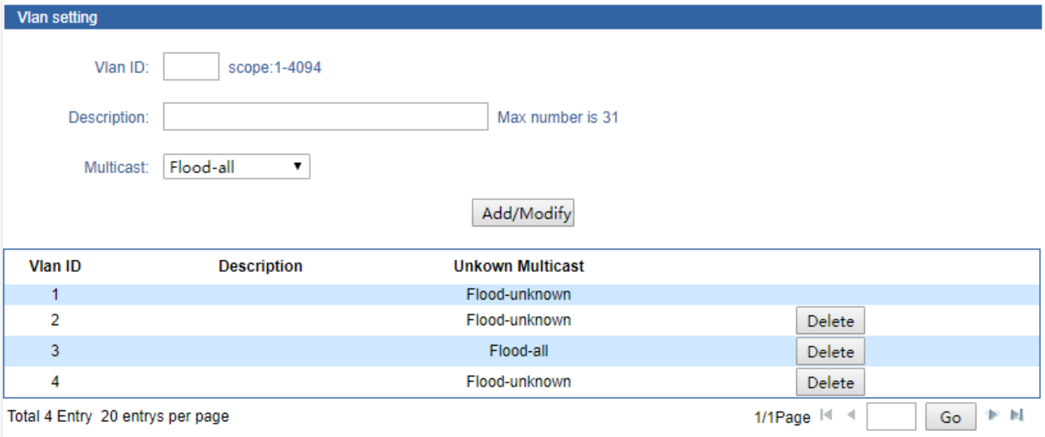
On the "Vlan-config" page, user can configure the VLAN ID description.

Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > Vlan-config".

Interface Description

Vlan configuration interface as follows:



Vlan setting

Vlan ID: scope:1-4094

Description: Max number is 31

Multicast: Flood-all

Vlan ID	Description	Unkown Multicast	
1		Flood-unknown	
2		Flood-unknown	Delete
3		Flood-all	Delete
4		Flood-unknown	Delete

Total 4 Entry 20 entrys per page 1/1Page

The main element configuration description of Vlan configuration interface.

Interface Element	Description
Vlan ID	VLAN ID number, value range is 1-4094.
Description	Vlan ID description, maximum 31 characters.
Multicast	Multicast process method; ● Flood-all: Flooding all multicast packets; ● Flood-unknow: Flooding unknown multicast packets; ● Drop: Drop the multicast packets.

4.1.4 Vlan Setting

Function Description

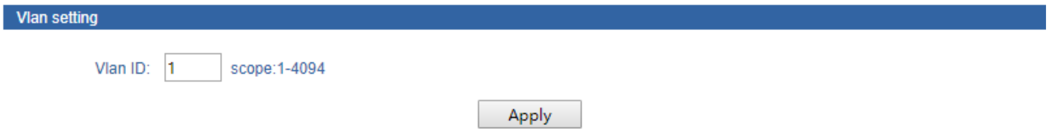
On the “Vlan setting” page, user can configure and manage Vlan ID number.

Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > Manage Vlan".

Interface Description

Manage Vlan interface as follows:


Vlan setting

Vlan ID: 1 scope:1-4094

The main element configuration description of Vlan configuration interface.

Interface Element	Description
Vlan ID	User can log in to switch via managing the port of VLAN to implement central network management over devices. Manage VLAN ID number, value range is 1-4094.

4.2 MAC-VLAN

Function Description

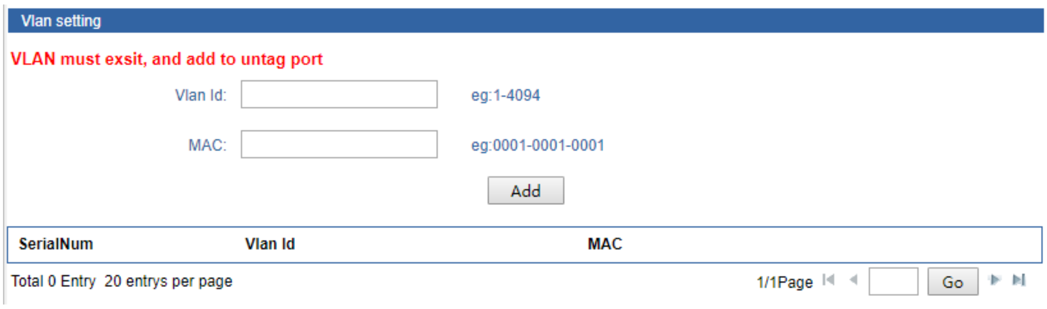
On the "mac-vlan" page, user can configure MAC and divide VLAN. It defines the VLAN member according to the message source MAC address, and sends the appointed message after adding the VLAN Tag.

Operation Path

Open in order: "Main Menu > Layer 2 Config > mac-vlan".

Interface Description

Mac-vlan interface as follows:


Vlan setting

VLAN must exsit, and add to untag port

Vlan Id: eg:1-4094

MAC: eg:0001-0001-0001

SerialNum	Vlan Id	MAC

Total 0 Entry 20 entrys per page

The main element configuration description of Vlan configuration interface.

Interface Element	Description
Vlan ID	VLAN ID number, value range is 1-4094. Note: VLAN must exist, and join in ports that need links via untag.
MAC	Source MAC address of sending data message, like 0001-0001-0001.

4.3 MAC Configuration

MAC (Media Access Control) address is the hardware identity of network device; the switch forwards the message according to MAC address. MAC address has uniqueness, which has guaranteed the correct retransmission of message. Each switch is maintaining a MAC address table. In the table, MAC address is corresponding to the switch port. When the switch receives data frame, it filters the data frame or forwards it to corresponding port of the switch according to MAC address table. MAC address is the foundation and premise that switch achieves fast forwarding.

4.3.1MAC Configuration

Each port in the switch is equipped with automatic address learning function, it stores the frame source address (source MAC address, switch port number) that port sends and receives in the address table. Ageing time is a parameter influencing the switch learning process; the default value is 300 seconds. When the timekeeping starts after an address record is added to the address table, if each port doesn't receive the frame whose source address is the MAC address within the ageing time, then these addresses will be deleted from dynamic forwarding address table (source MAC address, destination MAC address and their corresponding switch port number).

Function Description

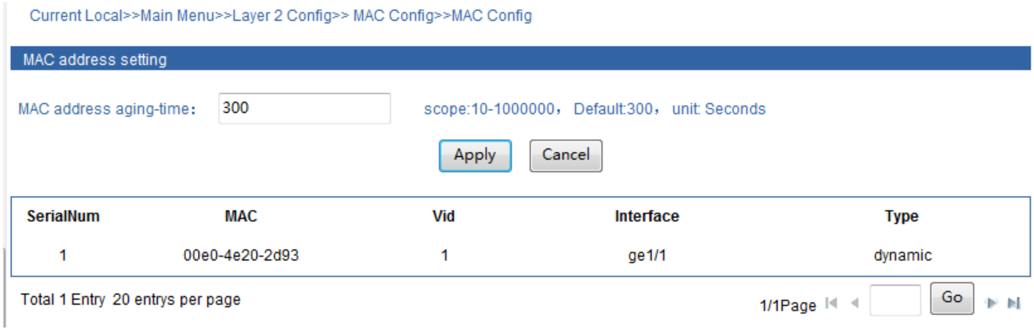
On the "MAC address setting" page, user can configure the ageing time of dynamic MAC address and check static and dynamic MAC address information.

Operation Path

Open in order: "Main Menu > Layer 2 Config > MAC Config > MAC Config".

Interface Description

MAC configuration interface as follows:



Current Local>>Main Menu>>Layer 2 Config>> MAC Config>>MAC Config

MAC address setting

MAC address aging-time: 300 scope:10-1000000, Default:300, unit: Seconds

SerialNum	MAC	Vid	Interface	Type
1	00e0-4e20-2d93	1	ge1/1	dynamic

Total 1 Entry 20 entrys per page

The main element configuration description of MAC configuration interface.

Interface Element	Description
MAC address aging-time	MAC address aging-time, unit is second, default value is 300, range is 10-1000000.
SerialNum	MAC table size serial number.
MAC	Access the device MAC address.
VID	VLAN ID number the data MAC address sending belongs to.
Interface	Corresponding port number of the MAC address.
Type	MAC address type, dynamic MAC and static MAC address, display as follows: ● Dynamic; ● Static.

4.3.2 Static MAC

Function Description

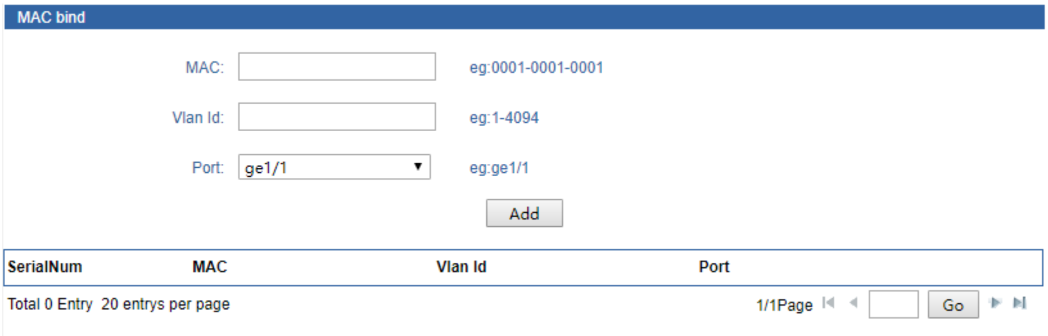
On the "Static MAC" page, user can manually configure the static MAC address and bind the source MAC address without aging.

Operation Path

Open in order: "Main Menu > Layer 2 Config > MAC Config > Static MAC".

Interface Description

Static MAC interface as follows:



MAC bind

MAC: eg:0001-0001-0001

Vlan Id: eg:1-4094

Port: ge1/1 eg:ge1/1

Add

SerialNum	MAC	Vlan Id	Port

Total 0 Entry 20 entrys per page 1/1Page Go

The main element configuration description of static MAC interface.

Interface Element	Description
MAC	Fill in the MAC address that needs to bind the interface, such as 0001-0001-0001.
Vlan ID	VLAN ID number the data MAC address sending belongs to, such as 1-4094. Notes: Input Vlan ID is the existing ID.
Port	Select the binding port number via the drop-down arrow.

Note

- The function is a sort of security mechanism, please carefully confirm the setting, otherwise, part of the devices won't be able to communicate;
- Please don't adopt multicast address as the entering address;
- Please don't enter reserved MAC address, such as the local MAC address.

4.4 Spanning-tree Configuration

Spanning-tree protocol is a sort of layer 2 management protocol; it can eliminate the network layer 2 circuit via selectively obstructing the network redundant links. At the same time, it has link backup function. Here are two kinds of spanning-tree protocols:

- STP (Spanning Tree Protocol);
- RSTP (Rapid Spanning Tree Protocol);

Spanning-tree protocol has two main functions:

- First function is utilizing spanning-tree algorithm to establish a spanning-tree that takes a port of a switch as the root to avoid ring circuit in Ethernet.
- Second function is achieving the convergence protection purpose via spanning-tree protocol when Ethernet topology changes.

4.4.1 Bridge Settings

Function Description

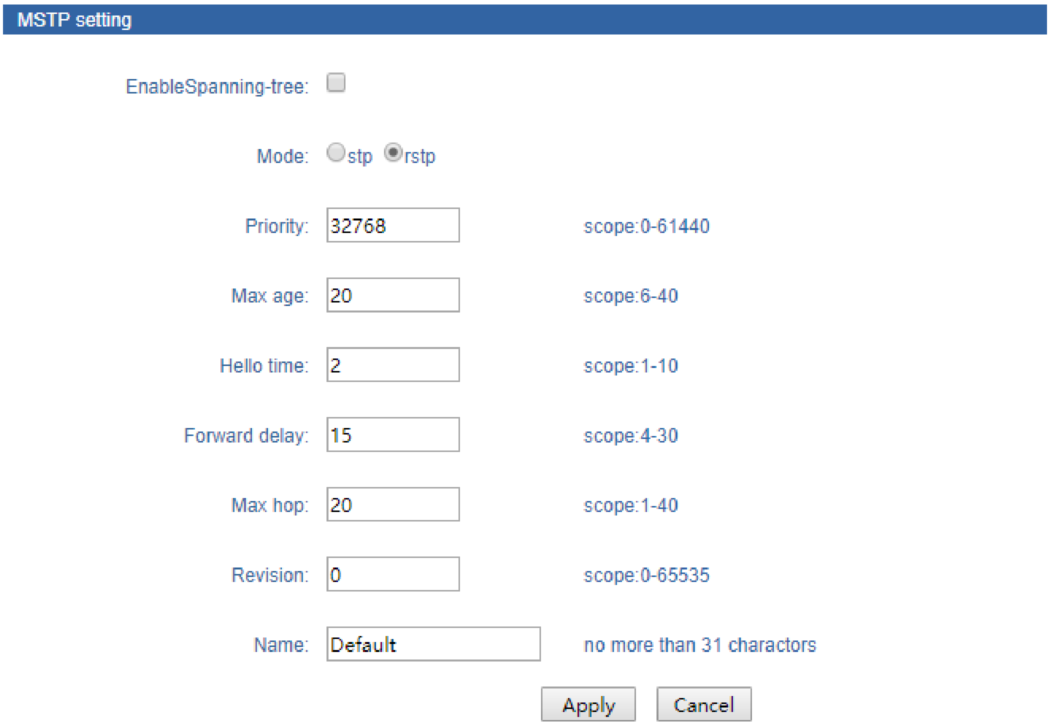
On the "Bridge Settings" page, user can configure relative parameters of spanning-tree.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Bridge Settings".

Interface Description

Bridge settings interface as follows:



MSTP setting

EnableSpanning-tree: ☐

Mode: ○stp ●rstp

Priority: 32768 scope:0-61440

Max age: 20 scope:6-40

Hello time: 2 scope:1-10

Forward delay: 15 scope:4-30

Max hop: 20 scope:1-40

Revision: 0 scope:0-65535

Name: Default no more than 31 charactors

The main element configuration description of bridge settings interface.

Interface Element	Description
Enable Spanning-tree	Enable Spanning-tree.
Mode	Two modes for spanning-tree protocol choice: ● STP: Spanning-tree; ● RSTP: Rapid spanning tree.
Priority	Bridge priority level, value range is 0-61440. Notes: Smaller the priority level value is, higher the priority level is.
Max age	The maximum lifetime of the message in the device, range is 6-40. It's used to determine whether the configuration message times out.
Hello time	Message sending cycle, value range is 1-10. Notes: The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty.
Forward delay	Port state transition delay, value range is 4-30.
Max hop	The maximum hop in multiple spanning tree region, value range is 1-40. Notes:

Interface Element	Description
	The maximum hop in multiple spanning tree region has limited the size of multiple spanning tree region. The maximum hop configured on a domain root will be used as the maximum hop in multiple spanning tree region.
Revision	multiple spanning tree revision level, value range is 0-65535. Notes: When the multiple spanning tree region name, revision level, instance-to-VLAN mapping relation are the same, the two or more bridges will belong to a same multiple spanning tree region.
Name	multiple spanning tree domain name, up to 31 characters.

4.4.2 Bridge Ports

Function Description

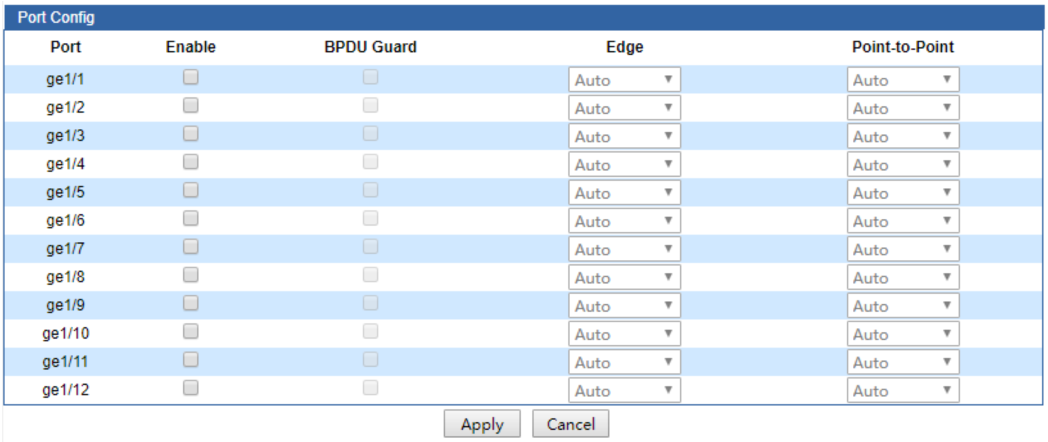
On the "Bridge Port" page, user can enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Bridge Ports".

Interface Description

Bridge ports interface as follows:



Port Config

Port	Enable	BPDU Guard	Edge	Point-to-Point
ge1/1	□	□	Auto	Auto
ge1/2	□	□	Auto	Auto
ge1/3	□	□	Auto	Auto
ge1/4	□	□	Auto	Auto
ge1/5	□	□	Auto	Auto
ge1/6	□	□	Auto	Auto
ge1/7	□	□	Auto	Auto
ge1/8	□	□	Auto	Auto
ge1/9	□	□	Auto	Auto
ge1/10	□	□	Auto	Auto
ge1/11	□	□	Auto	Auto
ge1/12	□	□	Auto	Auto

The main element configuration description of bridge ports interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.

Interface Element	Description
Enable	Enable checkbox to participate in spanning-tree.
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function.
Edge	Configure port type: ● Auto: Automatic system detection; ● Force True: Edge port; ● Force False: No edge port.
Point-to-Point	Port link type: ● Auto: Automatic system detection; ● Force True: Point-to-point link; ● Force False: Non point-to-point link.

4.5 ERPS Configuration

Ethernet Ring Protection Switching (ERPS) is the Ethernet Ring Network Link Layer Technology with high reliability and stability. It can prevent the broadcast storm caused by data loop when the Ethernet ring is intact. When the Ethernet ring link failure occurs, it has high convergence speed that can rapidly recover the communication path between each node in the ring network.

4.5.1Ring Configuration

Function Description

On the "Ring Configuration" page, user could configure ring network.

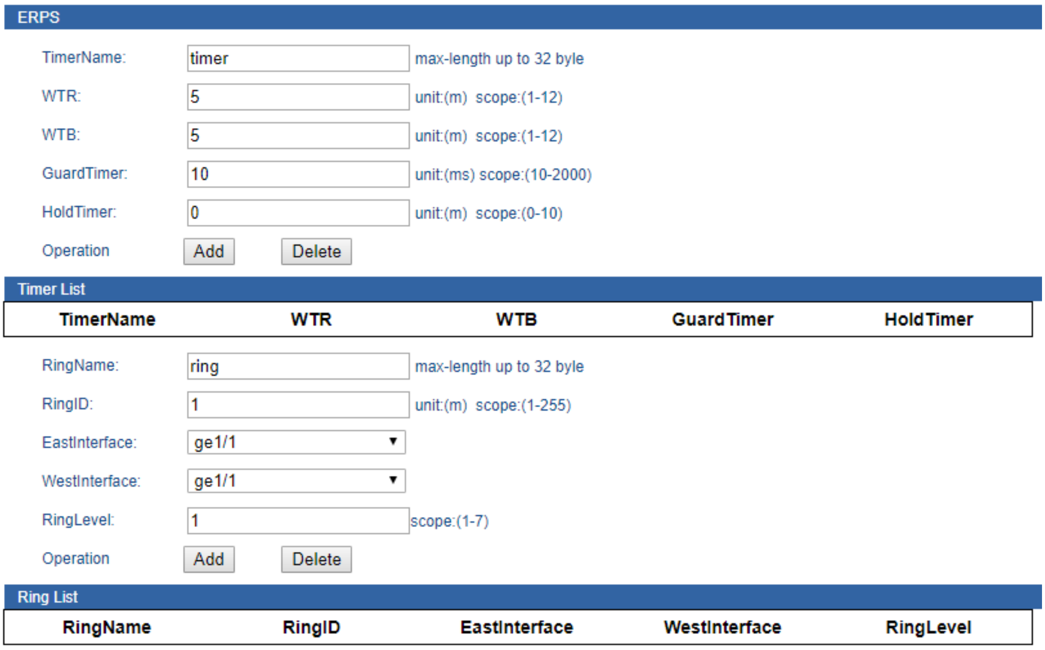
An Ethernet network topology connected in ring is called a ERPS Ring. It could be divided into main ring and subring. Every device in the ERPS ring is a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

Operation Path

Open in order: "Main Menu > Layer 2 Config >ERPS Config > Ring Config”.

Interface Description

Ring configuration interface as follows:



ERPS

TimerName: timer max-length up to 32 byle

WTR: 5 unit:(m) scope:(1-12)

WTB: 5 unit:(m) scope:(1-12)

GuardTimer: 10 unit:(ms) scope:(10-2000)

HoldTimer: 0 unit:(m) scope:(0-10)

Operation Add Delete

Timer List

TimerName	WTR	WTB	GuardTimer	HoldTimer

RingName: ring max-length up to 32 byle

RingID: 1 unit:(m) scope:(1-255)

EastInterface: ge1/1 ▼

WestInterface: ge1/1 ▼

RingLevel: 1 scope:(1-7)

Operation Add Delete

Ring List

RingName	RingID	EastInterface	WestInterface	RingLevel

The main element configuration description of ring configuration interface.

Interface Element	Description
ERPS	**ERPS configuration**
Timer Name	The default name of timer is timer, which is up to 32 bytes.
WTR	WTR(Wait To Restore)timer, its value range is 1-12 minutes. Under revertive mode, the timer starts when the owner node in protection state receives NR packet. The owner node blocks the RPL port and unblocks the fault port after the timer expires.
WTB	WTB（Wait To Block）timer, its value range is 1-12 minutes. Under revertive mode, when the owner node is in MS (Manual Switch) or FS (Forced Switch) status, WTB timer will start if user carries out clean command on the owner node. After the timer expires, the owner node will block the RPL port and unblock temporary blocking port.
Guard Timer	Guard timer, its value range is 10-2000ms. The timer starts when the port detects the link restoration, before the timer expires, the port won’t deal with R-APS (Ring Automatic Protection Switching) packet.
Hold Timer	Hold timer, its value range is 0-10ms. The timer starts when the port detects the link restoration, delay the fault report speed. When the link fails, the timer should report the fault if it

Interface Element	Description
	exists after Hold timer expires.
Operation	Click the button to operate: ● Add ● Delete
Timer List	**Added timer would display in this list**
Ring Name	The default name of ring network is ring, which is up to 32 bytes
Ring ID	The ID of ring network, its value range is 1-255
East Interface	Ring network 1, its value range is 1-port number
West Interface	Ring network 2, its value range is 1-port number
Ring Level	The higher the ring network level is, the greater the value is, its value range is 1-7
Operation	Click the button to operate: ● Add ● Delete
Ring List	**Added ring would display in this list**

4.5.2 Instance Configuration

Function Description

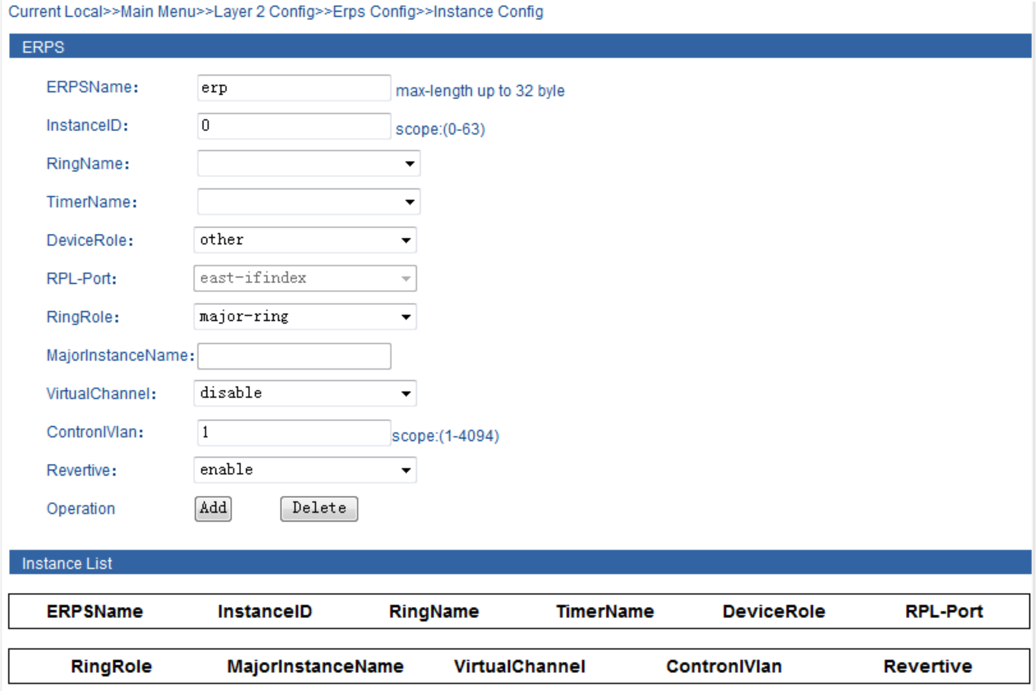
On the "Instance Configuration” page, user could configure instance.

Operation Path

Open in order: "Main Menu > Layer 2 Config >ERPS Config > Instance Config”.

Interface Description

Instance configuration interface as follows:



Current Local>>Main Menu>>Layer 2 Config>>Erps Config>>Instance Config

ERPS

ERPSName: erp max-length up to 32 byle

InstanceID: 0 scope:(0-63)

RingName:

TimerName:

DeviceRole: other

RPL-Port: east-ifindex

RingRole: major-ring

MajorInstanceName:

VirtualChannel: disable

ControlVlan: 1 scope:(1-4094)

Revertive: enable

Instance List

ERPSName	InstanceID	RingName	TimerName	DeviceRole	RPL-Port

RingRole	MajorInstanceName	VirtualChannel	ControlVlan	Revertive

The main element configuration description of instance configuration interface:

Interface Element	Description
ERPS	**ERPS Configuration**
ERPS Name	The default name of ERPS is erp, which is up to 32 bytes
Instance ID	The ID of instance, its value range is 0-63
Ring Name	The default name of ring network is the ring name that has been added in the ring network list
Timer Name	The default name of timer is the name that has been added in the timer list
Device Role	Each device in ERPS ring is called a node. The node role is decided by user configuration, they are divided into following types: ● RPL-Owner: owner node is responsible for blocking and unblocking the port in RPL of the node to prevent loop forming and conduct link switching. ● RPL-Neighbor: neighbor node is connected to Owner node on RPL. Cooperating to the Owner node, it blocks and unblocks the ports on RPL of the node and conduct link switching. ● Interconnection: interconnected node is the node to

Interface Element	Description
	connect multiple rings in the multi-loop model, it belongs to the subring, and the primary ring has no interconnected node. In the link protocol packet upload mode between the two subring interconnected nodes, the subring protocol packet ends in the interconnected node, but the data packet won't end. ● Other: normal node is the other node in addition to the above three nodes. Normal node is responsible for receiving and forwarding the protocol packet and data packet in the link.
RPL-Port	RPL (Ring Protection Link) port is the appointed ring network port for Owner node to establish RPL.
Ring Role	Options of ring role drop-down box: ● Major-ring: main ring network ● Sub-ring: subring network
Major Instance Name	The major instance name could be set and need to be set as ERPS instance name only when the ring role is Sub-ring
Virtual Channel	After enable virtual channel, the subring protocol packet could transmit across the primary ring; otherwise, the subring protocol packet can only transmit in the ring. Options: ● enable ● disable
Control VLAN	The VLAN channel of protocol packet, its value range is 1-4094
Revertive	Options: ● Enable: In revertive mode, WTR timer starts when the owner node receives the link recovery packet after the clearing of fault. The timer will change from fault link protection status to idle status after expiring. ● Disable: Irreversible mode: Owner node doesn't conduct any action after receiving the link recovery packet and keeps the port status set before.

4.6 IGMP-snooping

IP host applies for joining (or leaving) multicast group to nearby routers through the Internet Group Management Protocol (IGMP). IGMP Snooping is a multicast suppression mechanism that manages and controls multicast group by listening and analyzing IGMP messages exchanged between host and multicast devices.

The working process of IGMP Snooping is: The switch intercepts the messages exchanged between the host and router, and traps the multicast information and requested port. When the switch intercepts the IGMP Report (request) sent by the host toward router, the switch adds the port to multicast forwarding table. When the switch intercepts the IGMP Leave message sent by the host, the router sends a Group-Specific Query message of the port. If other hosts need the multicast, they will respond with the IGMP Report message. If the router can't receive any response from the host, the switch deletes the port from the multicast forwarding table. The router sends IGMP Query messages periodically. After receiving the IGMP Query messages, the switch deletes the port from the multicast table if the device does not receive IGMP Report messages from the host within a certain period of time.

4.6.1IGMP-snooping

Function Description

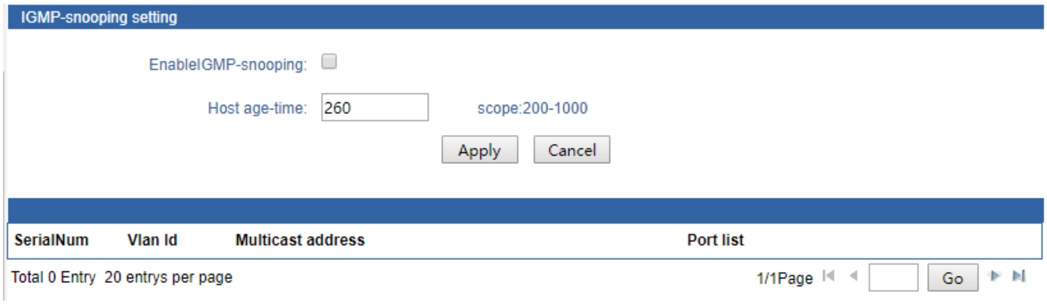
On the "IGMP-snooping Configuration" page, users can enable / disable IGMP and configure the host aging time.

Operation Path

Open in order: "Main Menu > Layer 2 Config > IGMP-snooping Config > IGMP-snooping Config".

Interface Description

IGMP-snooping configuration interface as follows:



IGMP-snooping setting

EnableIGMP-snooping: □

Host age-time: 260 scope:200-1000

SerialNum	Vlan Id	Multicast address	Port list

Total 0 Entry 20 entrys per page 1/1Page

The main element configuration description of IGMP-snooping port configuration interface.

Interface Element	Description
Enable IGMP-snooping	Enable IGMP-snooping configuration checkbox.
Host aging time	Host aging time, value range is 200-1000s.
SerialNum	IGMP-Snooping list serial number.
Vlan Id	Port number VLAN ID number.
multicast source	Multicast source IP address.
multicast addr	Multicast IP address.
Port list	The corresponding port name of the device Ethernet port.

4.6.2 Static Multicast

Function Description

On the "Static Multicast" page, user can add or delete static multicast.

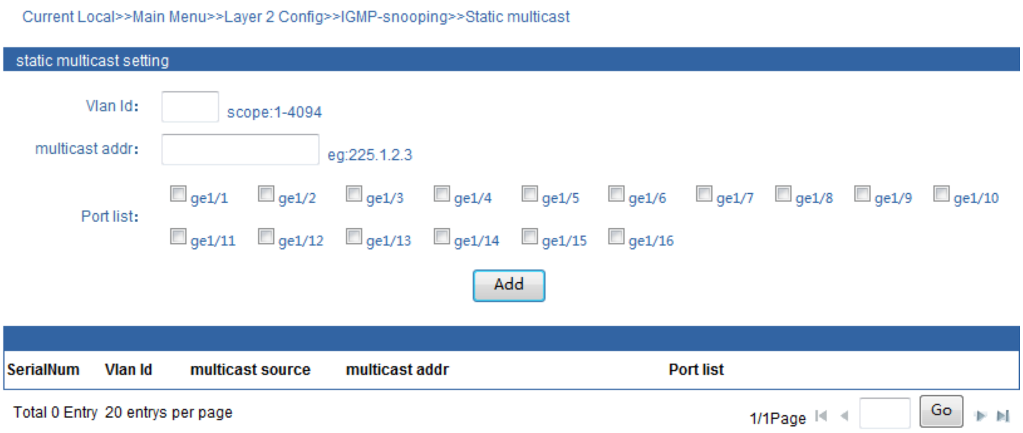
Main function of static multicast: Add certain ports to a multicast group; these ports can receive data when data is sent to this multicast address.

Operation Path

Open in order: "Main Menu > Layer 2 Config > IGMP-snooping > Static multicast".

Interface Description

Static multicast interface as follows:



Current Local>>Main Menu>>Layer 2 Config>>IGMP-snooping>>Static multicast

static multicast setting

Vlan Id: scope:1-4094

multicast addr: eg:225.1.2.3

Port list: □ ge1/1 □ ge1/2 □ ge1/3 □ ge1/4 □ ge1/5 □ ge1/6 □ ge1/7 □ ge1/8 □ ge1/9 □ ge1/10 □ ge1/11 □ ge1/12 □ ge1/13 □ ge1/14 □ ge1/15 □ ge1/16

SerialNum	Vlan Id	multicast source	multicast addr	Port list

Total 0 Entry 20 entrys per page

1/1Page

The main element configuration description of static multicast interface.

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
multicast addr	Multicast IP address information, such as: 225.1.2.3.
Port list	Check the box and select the device port to form a multicast group.

4.6.3 Router Port Configuration

Function Description

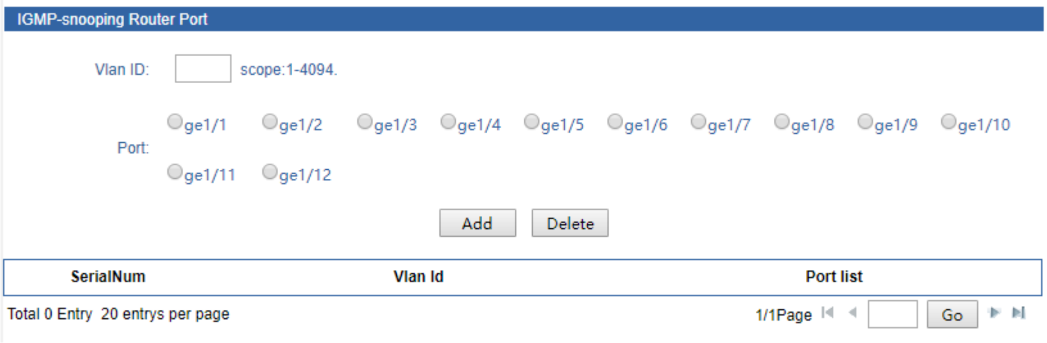
On the "Router Port Configuration" page, user can configure multicast router port..

Operation Path

Open in order: "Main Menu > Layer 2 Config > IGMP-Snooping > Global Router Port Config".

Interface Description

Router port configuration interface as follows:



IGMP-snooping Router Port

Vlan ID: scope:1-4094.

Port: ○ge1/1 ○ge1/2 ○ge1/3 ○ge1/4 ○ge1/5 ○ge1/6 ○ge1/7 ○ge1/8 ○ge1/9 ○ge1/10 ○ge1/11 ○ge1/12

SerialNum	Vlan Id	Port list

Total 0 Entry 20 entrys per page

The main element configuration description of router port configuration interface:

Interface Element	Description
VLAN ID	VLAN ID, value range is 1-4094.
Port list	Check the box of port list and choose device port as the static router port that connects router.

4.7 Ring Configuration

Ring provides automatic recovery and reconnection mechanism for the disconnected Ethernet network, which has link redundancy and self-recovery ability in case of network interruption or network failure.

The core of Ring technology is without master station setting. In a multi-ring network of up to 250 switches, the network self-recovery time is less than 20 milliseconds. Each port in this series of switches can be used as a ring port and connected with other switches. When an interruption occurs in the network connection, the relay for fault alarm will be activated and the Ring redundant mechanism enables the backup link to quickly recover the network communication.

4.7.1Global Configuration

Function Description

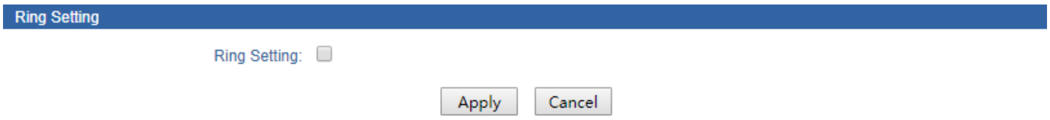
On the "Local Configuration" page, user can enable/disable the ring network.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Ring Config > Global Config".

Interface Description

Global configuration interface as follows:



Ring Setting

Ring Setting: ☐

The main element configuration description of global configuration interface.

Interface Element	Description
Ring Setting	Ring setting checkbox, enable Ring network function after checking.

4.7.2 Node Configuration

Function Description

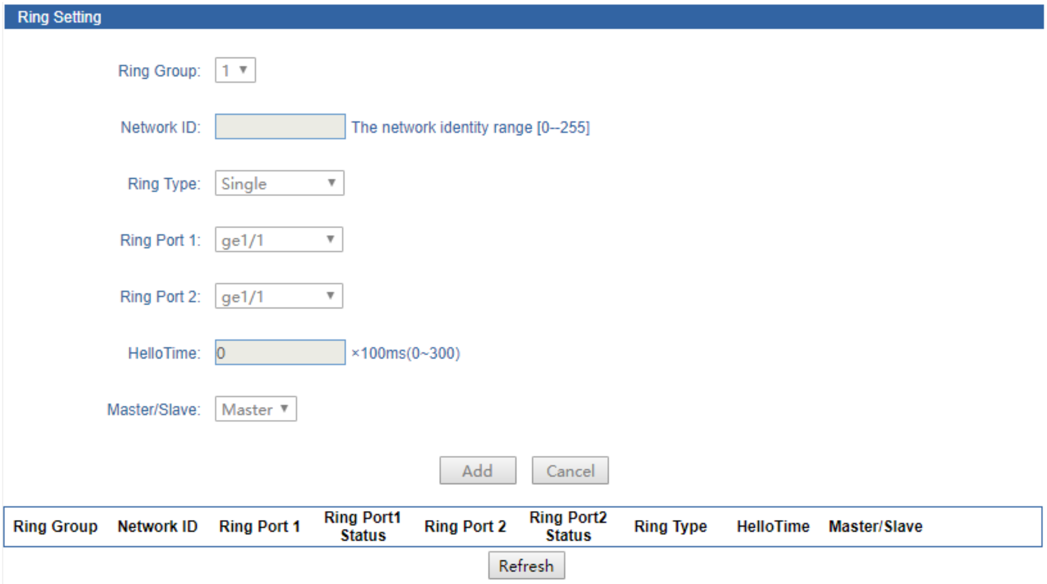
On the "Node Configuration" page, user can enable/disable the ring network.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Ring Config > Node Config".

Interface Description

Node configuration interface as follows:



Ring Setting

Ring Group: 1

Network ID: The network identity range [0--255]

Ring Type: Single

Ring Port 1: ge1/1

Ring Port 2: ge1/1

HelloTime: 0 ×100ms(0~300)

Master/Slave: Master

Ring Group	Network ID	Ring Port 1	Ring Port1 Status	Ring Port 2	Ring Port2 Status	Ring Type	HelloTime	Master/Slave

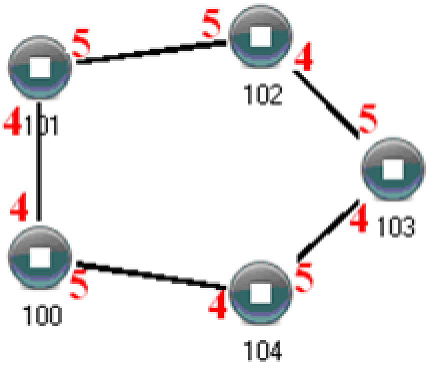
The main element configuration description of node configuration interface.

Interface Element	Description
Ring Group	Support ring group 1-4, it can create 4 ring networks at the same time.
Network ID	When multiple switch devices constitute a ring network, the current ring identification of the ring is network identification; the network identifications of different ring network are different.
Ring Type	According to the scene environment requirement, choose different ring type. ● Single: Single ring, it adopts a continuous ring to connect each device together. ● Couple: Coupling ring is a redundant structure proposed to connect two independent networks. ● Chain: The chain, it enhances the flexibility that user builds any type of redundant network topology structure via a kind of advanced software technology. ● Dual-homing: Two adjacent rings share a switch; users can carry the same switch on two different networks or two different switching devices on the same network.
Ring port 1	The network port 1 on the switch device used to form the ring network. Note: When the ring type is "Couple", coupling port is a port connecting different network identifications.
Ring port 2	Network port 2 on the switch device that is used to form the ring network. Note: When the ring type is "Couple", coupling port is a port connecting different network identifications.
Hello Time	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not.
Maser/slave	The master/slave mode of ring network, options are: Master: ring network master device

Interface Element	Description
	Slave: ring network slave device. Note: Single ring has master device and slave device options. One-master multiple-slave mode is recommended in a single ring. When the device is master device, one end of it in the ring is backup link. It can enable backup link from master station to ensure the normal operation of network when the ring network has failures.

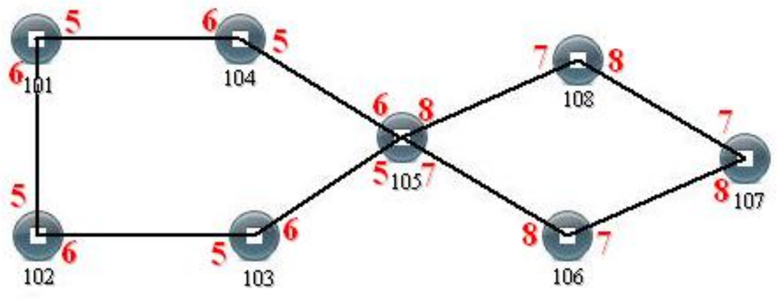
Single Ring Configuration

Enable Single, enable ring group 1 (other ring group is OK), Set the device port 4 and port 5 to ring port, choose one of the devices as master device and the rest of them as slave devices, then set other switches to the same ring network parameters, reboot these devices, and adopt network cable to connect port 4 and port 5 of the switch, then search it via network management software, the ring topology structure picture as below:



Double Ring Configuration

Double ring as shown below, in the figure, double ring is the tangency between two rings, and the point of tangency is NO. 105 switch.



Configuration Method:

Step 1 Adopt single ring configuration method to configure port 5 and port 6 of NO. 101, 102, 103, 104, 105 switches as the ring port, and the ring group is 1; set 105 as master device and others as slave devices;

Step 2 Adopt single ring configuration method to configure port 7 and port 8 of NO. 105, 106, 107 and 108 switches as the ring ports and the ring group 2; set 105 as master device and others as slave devices;

Step 3 Adopt network cable to connect the ring group 1;

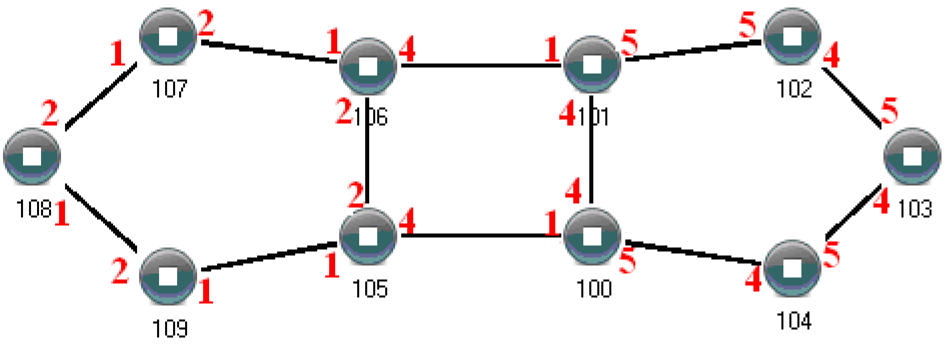
Step 4 Adopt network cable 2 to connect the ring group 2;

Step 5 Search the topology structure picture via network management software;

Since NO. 105 devices belong to two ring groups, the network IDs of the two ring groups cannot be the same.

Coupling Ring Configuration

Coupling ring basic framework as the picture below



Operation method:

Step 1 Enable ring group 1 and ring group 2; (Hello_time is disable, but setting time can't cause too fast sending of Hello packet, otherwise, it will seriously influence CPU processing speed);

Step 2 Set the ring port of NO. 105, 106 device ring group to port 1 and port 2, network identification to 1, ring type to Single; Set the coupling port of ring group 2 to port 4, console port to 2, ring identification to 3, ring type to Coupling.

Step 3 Set the ring port of NO. 100, 101 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single; Set the coupling port of ring group 2 to port 1, console port to port 4, ring identification to 3, ring type to Coupling.

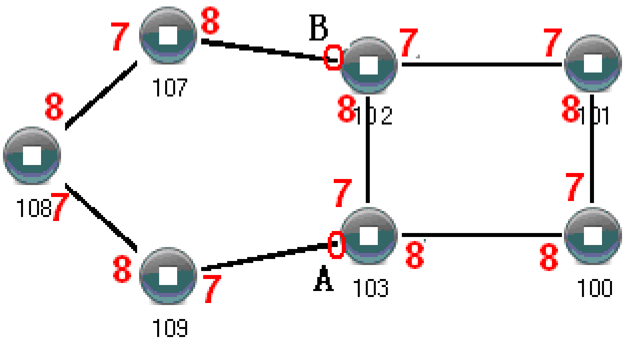
Step 4 Set the ring port of NO. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of NO. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

Step 5 Connect the port 4 and port 5 of five devices NO. 100-104 to the single ring in turn, adopt network cable to connect the port 1 and port 2 of four devices NO. 105-109 to the single ring in turn, Then adopt Ethernet cable to connect port 4 of NO. 106 device to port 1 of NO. 101 device, port 4 of NO. 105 device to port 1 of NO. 100 device, coupling ring combination is completed.

Console ports are two ports connected to NO. 105 device and NO. 106 device in the above picture. The two ports connected to NO. 100 device and NO. 101 device are also called console ports.

Chain Configuration

Chain basic framework as the picture below:



Operation method:

Step 1 Enable the ring group 1; (Hello_time can be disable, but setting time can't cause too fast sending of Hello packet, otherwise it will seriously influence CPU dealing speed);

Step 2 Set the ring port of NO. 100, 101, 102 and 103 device ring group 1 to port 7 and port 8, network identification to 1, ring type to Single. Set the ring port of NO. 107, 108 and 109 devices ring group 1 to port 7 and port 8, network identification to 2, ring type to Chain.

Step 3 Adopt network cable to connect the port 7 and port 8 of three devices NO. 107-109, adopt network cable to connect the port 7 and port 8 of four devices NO. 100-103 to the single ring in turn, Then adopt network cable to connect port 7 of NO. 107 device and port 7 of NO. 109 device to normal ports of NO. 102 and 103 device, chain combination is complete.

Note

- Port that has been set to port aggregation can't be set to rapid ring port, and one port can't belong to multiple rings;
- Network identification in the same single ring must be consistent, otherwise it cannot form a normal ring or normal communicate;
- Network identification in different ring must be different;
- When forming double ring and other complex ring, user should notice whether the network identification in the same single ring is consistent, and network identification in different single ring is different.

4.8 GMRP Configuration

GMRP multicast registration protocol is an application of the universal attribute registration protocol, it mainly provides a limited multicast diffusion function similar to IGMP probing technology. GMRP allows bridge and end station to dynamically register group membership information to MAC bridges connected to the same LAN segment, and this information can be propagated to all bridge systems in a bridging LAN supporting extended filtering server. GMRP software runs on the host and switch.

When a host wants to join an IP multicast group, it needs to send an IGMP join information, The information evolves as a GMRP join information, once receiving GRMP join information, switch will add the port receiving the information to proper multicast group, Switch sends GMRP join information to other hosts in VLAN, among which one host as the multicast source, When the multicast source sends multicast information, switch will send the multicast information via the port that joins in the multicast group before. In addition, switch will periodically send GMRP query, if the host stays in the multicast group, it will response to GMRP query, In this case, the switch does nothing, and if the host does not want to stay in the multicast group, it can either send a leave message or not respond to periodic GMRP query. Once the host receives the leave message or does not receive a response message during the timer setting period, it deletes the host from multicast group.

Enable the function is OK while adopting this function, If the switch receives the host IGMP join information, then switch will build a multicast group according to IGMP join information, and add the port that receives IGMP join information to the multicast group, At this time, if the data destination address is the multicast address, then the data can only be forwarded from the multicast group member.

4.8.1GMRP Global Set

Function Description

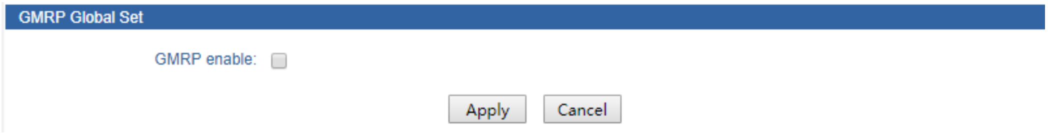
On the "GMRP Global Set" page, user can enable/disable the GMRP.

Operation Path

Open in order: "Main Menu > Layer 2 Config > GMRP Config > GMRP Global Config".

Interface Description

GMRP global configuration interface as follows:


GMRP Global Set

GMRP enable: □

The main element configuration description of GMRP global configuration interface.

Interface Element	Description
Enable GMRP	Enable GMRP multicast registration protocol.

4.8.2 GMRP Port Config

Function Description

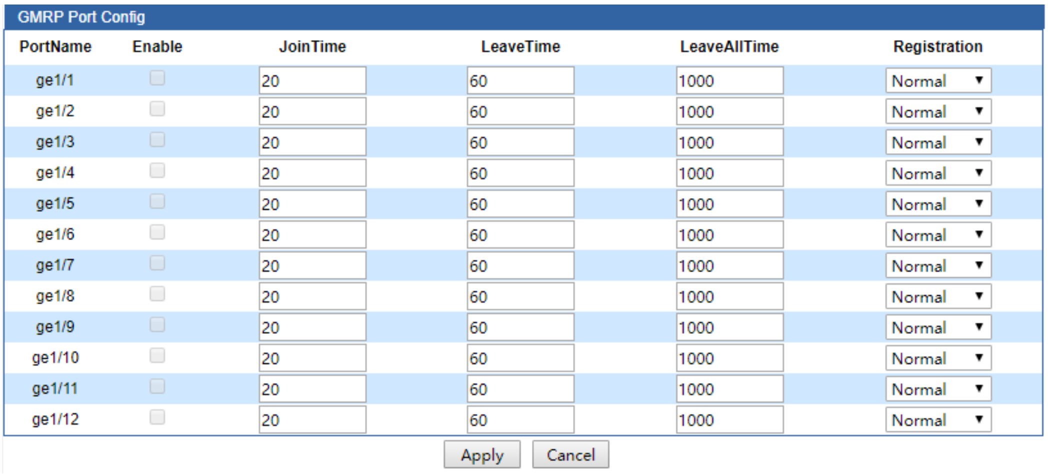
On the "GMRP Port Config" page, user can configure relative parameters of GMRP port.

Operation Path

Open in order: "Main Menu > Layer 2 Config > GMRP Config > GMRP Port Config".

Interface Description

GMRP port config interface as follows:



GMRP Port Config

PortName	Enable	JoinTime	LeaveTime	LeaveAllTime	Registration
ge1/1	□	20	60	1000	Normal ▼
ge1/2	□	20	60	1000	Normal ▼
ge1/3	□	20	60	1000	Normal ▼
ge1/4	□	20	60	1000	Normal ▼
ge1/5	□	20	60	1000	Normal ▼
ge1/6	□	20	60	1000	Normal ▼
ge1/7	□	20	60	1000	Normal ▼
ge1/8	□	20	60	1000	Normal ▼
ge1/9	□	20	60	1000	Normal ▼
ge1/10	□	20	60	1000	Normal ▼
ge1/11	□	20	60	1000	Normal ▼
ge1/12	□	20	60	1000	Normal ▼

The main element configuration description of GMRP port config interface.

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Enable	Port enables checkbox.
Join Time	Join timer time, it will send Join message outward after timeout.
Leave Time	Leave timer time, when the entity that receives the leave message does not receive the Join message after timeout; the attribute information should be canceled.
LeaveAll Time	The default value of Leave All Time timer is 1000 centiseconds, which is 10 seconds, Each GMRP application entity periodically sends a Leave All Time Message after the Leave All Time timer timeout, all VLAN information in the entity should be canceled.

Interface Element	Description
Registration	Registration state, options as follows: ● Normal; ● Fixed; ● Forbidden.

4.8.3 GMRP Group

Function Description

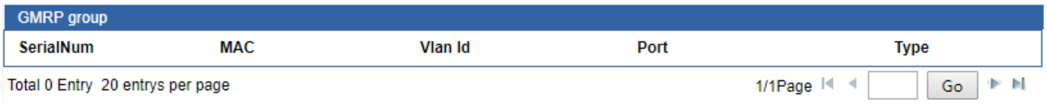
On the "GMRP Group" page, user can check GMRP group information.

Operation Path

Open in order: "Main Menu > Layer 2 Config > GMRP Config > GMRP Group".

Interface Description

Check GMRP group interface as below:



GMRP group

SerialNum	MAC	Vlan Id	Port	Type

Total 0 Entry 20 entrys per page

The main element configuration description of GMRP group interface.

Interface Element	Description
SerialNum	GMRP group serial number.
MAC	Multicast source MAC address.
Vlan ID	Vlan ID number.
Port	The corresponding port name of the device Ethernet port.
Type	Multicast address type.

5 Network Security

5.1 Access Control

Function Description

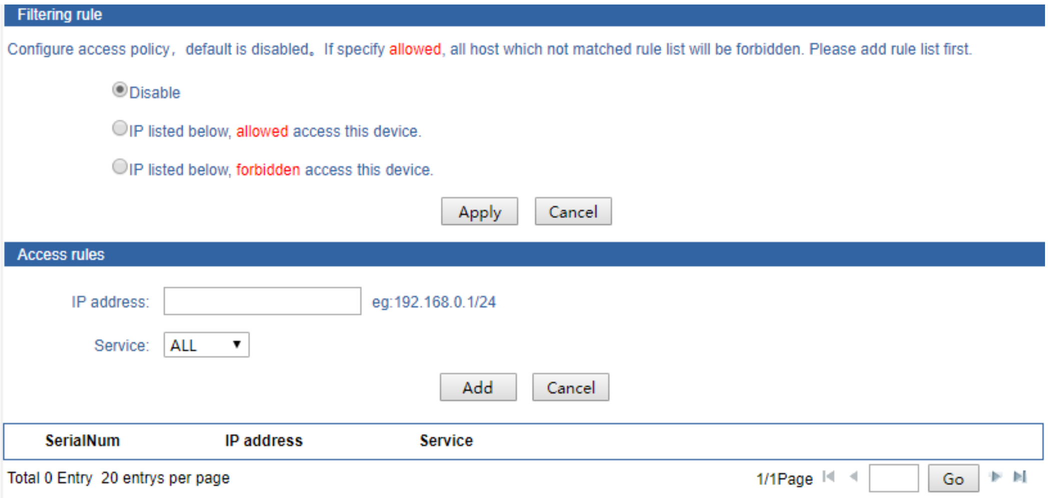
On the "Access Control" page, user can configure access rules and filtering rule.

Operation Path

Open in order: "Main Menu > Network security > Access Control".

Interface Description

Access control interface as follows:



Filtering rule

Configure access policy, default is disabled。If specify allowed, all host which not matched rule list will be forbidden. Please add rule list first.

● Disable

○ IP listed below, allowed access this device.

○ IP listed below, forbidden access this device.

Access rules

IP address: eg:192.168.0.1/24

Service: ALL

SerialNum	IP address	Service

Total 0 Entry 20 entrys per page 1/1Page

The main element configuration description of access control interface.

Interface Element	Description
Filtering rule	Set filtering rule, default to disable, that is disable access

Interface Element	Description
	filtering function. Options as follows: ● Disable; ● Hosts that meet the following rules are allowed to access the equipment corresponding service; ● Hosts that meet following rules are forbidden to access the equipment corresponding service.
Access rules	**Access rules setting column.**
IP address	Enable/disable device to access the switch IP address.
Service	Methods of enabling/disabling device to access the switch. Options as follows: ● ALL: Support HTTP and TELNET access; ● HTTP: Support WEB interface access; ● TELNET: Support Telnet client command line access;

⚠ Notice

- Please first add the rules, and then set the access rules, otherwise it may cause the current web can't be accessed.

5.2 ACL Configuration

Access Control List (ACL) is the aggregation of single or multiple rules, which is used to identify the message flow. Rule refers to the judgment statement describing the message matching condition. These conditions may be the source address, destination address, port number of message. Network devices identify specific messages according to these rules and process the messages according to pre-defined strategies.

5.2.1 ACL GROUP Configuration

Function Description

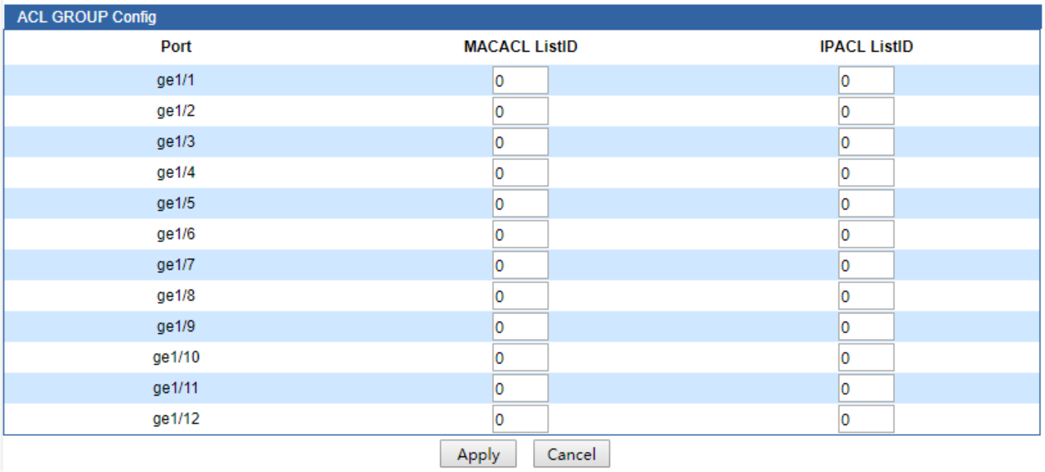
On the "ACL GROUP Configuration" page, user can set MAC access list ID and IP access list ID for the port.

Operation Path

Open in order: "Main Menu > Network security > ACL Config > ACL GROUP Config".

Interface Description

ACL GROUP Configuration interface as follows:



ACL GROUP Config

Port	MACACL ListID	IPACL ListID
ge1/1	0	0
ge1/2	0	0
ge1/3	0	0
ge1/4	0	0
ge1/5	0	0
ge1/6	0	0
ge1/7	0	0
ge1/8	0	0
ge1/9	0	0
ge1/10	0	0
ge1/11	0	0
ge1/12	0	0

The main element configuration description of ACL GROUP Configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
MAC ACL List ID	Rule ID of MAC address device accessing the device. MAC discards or forwards the message according to the MAC access rule.
IP ACL List ID	Configuration rule ID of IP address accessing the device. IP MAC discards or forwards the message according to IP access rule.

5.2.2 Time Range Configuration

When ACL rule is valid only for a certain period of time, user can set time-based ACL filtering. Therefore, first user can configure one or more time periods, and then reference the time periods in the rule, the rule will be valid only for the specified time period.

Users can adopt the same name to configure multiple time segments with different contents. After gain the union of each cycle time period and each absolute time period, the intersection of each union will become the final valid time range.

Function Description

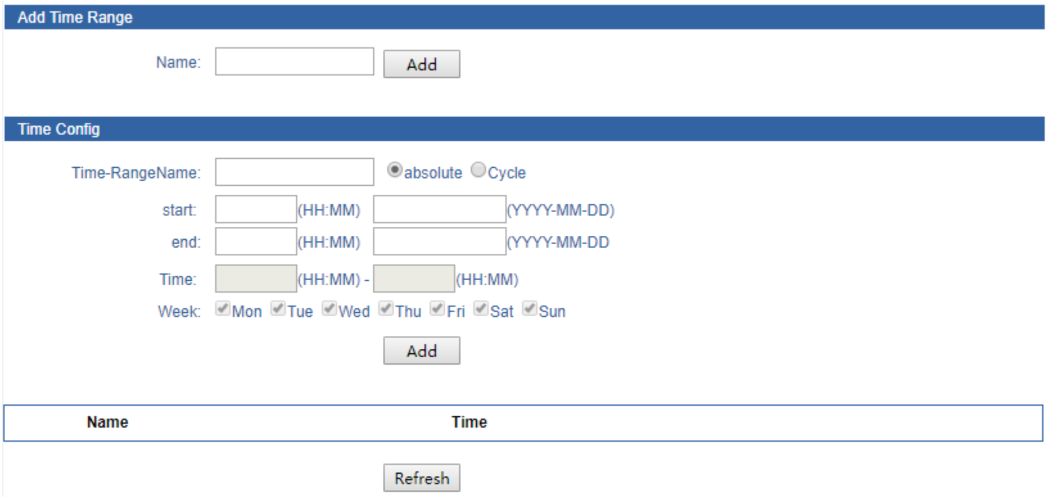
On the "Time Range Config" page, user can add or delete the absolute time and cycle time.

Operation Path

Open in order: "Main Menu > Network security > ACL Config > Time Range Config".

Interface Description

Time Range configuration interface as follows:



Add Time Range

Name: [ ] Add

Time Config

Time-RangeName: [ ] ● absolute ○ Cycle

start: [ ] (HH:MM) [ ] (YYYY-MM-DD)

end: [ ] (HH:MM) [ ] (YYYY-MM-DD

Time: [ ] (HH:MM) - [ ] (HH:MM)

Week: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Add

Name	Time

Refresh

The main element configuration description of Time Range configuration interface.

Interface Element	Description
Add Time Range	**Add Time Range setting column**
Name	Time period range name entering.
Time Config	**Configuration time setting column**
Time-Range Name	Time-Range name filling, select relative time method： ● Absolute It represents the rule is valid in appointed time range (such as 8 o'clock 1st January 2017 to 18 o'clock 3rd January 2017). ● Cycle time: It represents the rule is valid in the cycle of a week (such as 8 o'clock to 12 o'clock per Monday).
start	Starting time of absolute time, format: HH: MM (Hour:

Interface Element	Description
	minute); YYYY-MM-DD (Year-month-day).
end	End time of absolute time, format: HH: MM (Hour: minute); YYYY-MM-DD (Year-month-day).
Time	Time range of cycle time, format: HH: MM (Hour: minute).
Week	Cycle date of cycle time; take one week as a cycle.

5.2.3MAC ACL Configuration

MAC ACL is used to identify the destination MAC address in the message. Identify the specific message according to the rules in MAC ACL and process the messages according to the preset strategies.

Function Description

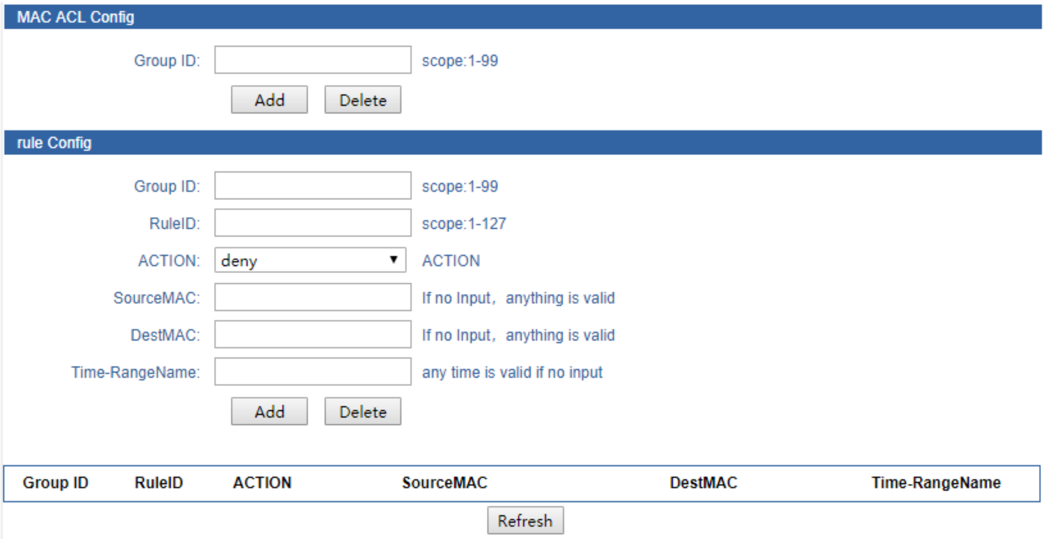
On the "MAC ACL Config" page, user can add or delete MAC access list.

Operation Path

Open in order: "Main Menu > Network security > ACL Config > MAC ACL Config".

Interface Description

MAC ACL Configuration interface as follows:



MAC ACL Config

Group ID: scope:1-99

rule Config

Group ID: scope:1-99

RuleID: scope:1-127

ACTION: deny ▾ ACTION

SourceMAC: If no Input，anything is valid

DestMAC: If no Input，anything is valid

Time-RangeName: any time is valid if no input

Group ID	RuleID	ACTION	SourceMAC	DestMAC	Time-RangeName

The main element configuration description of MAC ACL configuration interface.

Interface Element	Description
MAC ACL Config	**Bar of MAC access list.** Note: Add MAC address access rules list group ID.
Group ID	Group ID serial number, support 1-99.
rule Config	**Rule configuration bar.** Note: MAC address access rule configuration column.
Group ID	Corresponding MAC address access list group ID.
Rule ID	Different rule ID number under group ID, value range is 1-127.
ACTION	MAC address access rule operation: ● Deny: Access denied; ● Permit: Access allowed.
Source MAC	Access the source MAC address of data information Notes: If no input, anything is valid.
Dest MAC	Access the destination MAC address of data information Notes: If no input, anything is valid.
Time-Range Name	Time range name. Notes: Any time is valid if no input.

5.2.4IP ACL Config

IP ACL is used to identify the destination MAC address in the message flow for access control. The specific message is identified according to the rules in MAC ACL and is processed according to a preset strategy.

Function Description

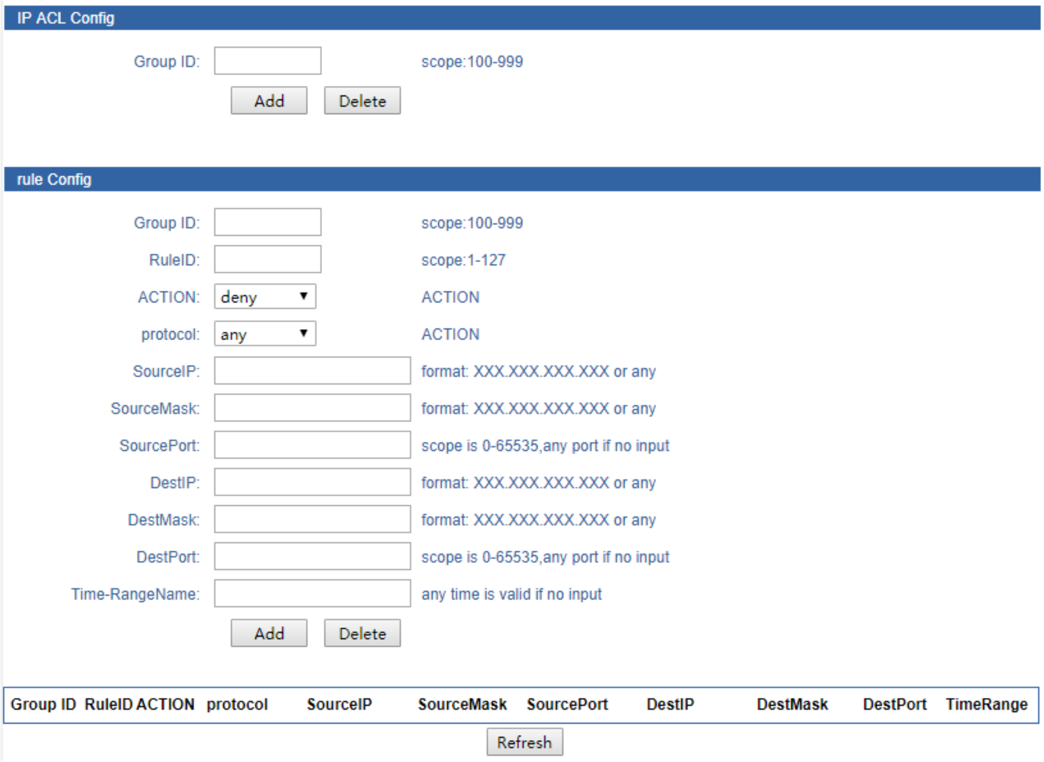
On the "IP ACL Config" page, user can add or delete MAC access list.

Operation Path

Open in order: "Main Menu > Network security > ACL Config > IP ACL Config".

Interface Description

IP ACL configuration serial setting interface as follows:



IP ACL Config

Group ID: scope:100-999

rule Config

Group ID: scope:100-999

RuleID: scope:1-127

ACTION: deny ACTION

protocol: any ACTION

SourceIP: format: XXX.XXX.XXX.XXX or any

SourceMask: format: XXX.XXX.XXX.XXX or any

SourcePort: scope is 0-65535,any port if no input

DestIP: format: XXX.XXX.XXX.XXX or any

DestMask: format: XXX.XXX.XXX.XXX or any

DestPort: scope is 0-65535,any port if no input

Time-RangeName: any time is valid if no input

Group ID	RuleID	ACTION	protocol	SourceIP	SourceMask	SourcePort	DestIP	DestMask	DestPort	TimeRange

The main element configuration description of IP ACL Configuration interface.

Interface Element	Description
IP ACL Config	**Add IP address access rules list group ID.**
Group ID	Group ID serial number, support 1-99.
rule Config	**IP address access rules configuration.**
Group ID	Corresponding IP address access list group ID.
Rule ID	Different rule ID number under group ID, value range is 1-127.
ACTION	IP address access rule operation: ● Deny: Access denied; ● Permit: Access allowed.
Protocol	Protocol data packet access rule operation: ● Any: any protocol data; ● Icmp: Control message protocol data; ● Igmp: Internet group management protocol data; ● TCP: Transmission control protocol data; ● UDP: User data message protocol.

Interface Element	Description
Source IP	Access the source IP address of data information. Notes: If no input, anything is valid.
Source Mask	Access the source mask address of data information. Notes: If no input, anything is valid.
Source Port	Access the source port information of data information. Notes: If no input, anything is valid.
Dest IP	Access the destination IP address of data information. Notes: If no input, anything is valid.
Dest Mask	Access the destination mask address of data information. Notes: If no input, anything is valid.
Dest port	Access the destination port information of the data. Notes: If no input, anything is valid.
Time-Range Name	Time range name. Notes: Any time is valid if no input.

5.3 802.1X Configuration

IEEE 802.1X protocol is a port-based network access control protocol, That is, accessed user equipment is authenticated on the port of LAN access device, so that user equipment controls the access to network resources.

IEEE 802.1x authentication system structure adopts "controllable port" and "uncontrollable port" logic function, which can achieve the separation of business and authentication. After user passes authentication, the business flow and authentication flow achieve separation, there exists no special requirements for subsequent data packet process, business can be flexible, and the business has great advantages in carrying out broadband multicast and other aspects; all businesses are not subject to the authentication method.

802.1X structure is mainly composed of three parts:

- Supplicant: User or client who wants to gain authentication;
- Authentication server: A typical example is RADIUS server;
- Authenticator: Interterminal equipment, such as wireless access point, switch and so on.

5.3.1 Global Configuration

Function Description

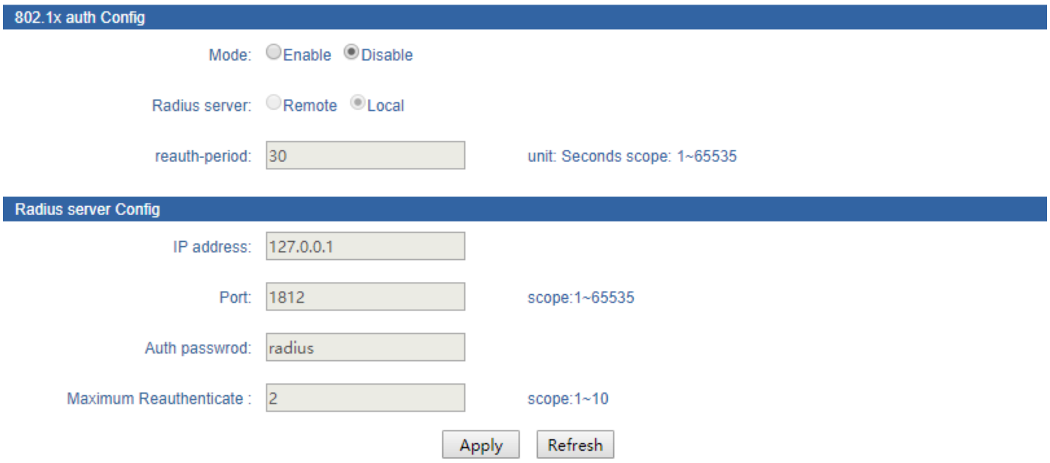
On the "Global Config" page, user can configure 802.1X authentication function and Radius server parameters.

Operation Path

Open in order: "Main Menu > Network security > 802.1X Config > Global Config".

Interface Description

Global configuration interface as follows:



802.1x auth Config

Mode: ○Enable ●Disable

Radius server: ○Remote ●Local

reauth-period: 30 unit: Seconds scope: 1~65535

Radius server Config

IP address: 127.0.0.1

Port: 1812 scope:1~65535

Auth passwrod: radius

Maximum Reauthenticate : 2 scope:1~10

The main element configuration description of global configuration interface.

Interface Element	Description
802.1X auth Config	**802.1X authentication configuration column**
Mode	802.1X authentication state setting: ● Enable; ● Disable.
Radius server	Local internal Radius server and external Radius server configuration: ● Local: Built-in Radius server in the equipment, if user

Interface Element	Description
	selects an internal Radius server, applicants will only be able to use the user name and password of internal Radius database. ● Remote: If using the external Radius server, user needs to fill in the authentication server IP address and port number.
reauth-period	Interval time range for updating the authentication information is 1-65535, unit is second. 802.1X re-authentication cycle time, which is used to enhance the authentication security.
Radius server Config	**Radius server configuration column** Notes: Radius remote access authentication server, which is used for authentication, the IP address / domain name is accessible to device, default port is 1812.
IP address	Radius server IP address.
Port	Radius server port, default to 1812, value range is 1-65535.
Auth password	The shared password string for the device to access authentication server.
Maximum Reauthenticate	Allowed authentication retry time, value range is 1-10.

Global Configuration Steps:

Step 1 Select "enable" or "disable" 802.1X authentication;

Step 2 Select Radius server "Remote" or "Local", fill in the authentication updating interval;

Step 3 Fill in the IP address, port, auth password and maximum reauthenticate;

Step 4 Click the "Apply" button;

Step 5 End.

5.3.2 Port Configuration

Function Description

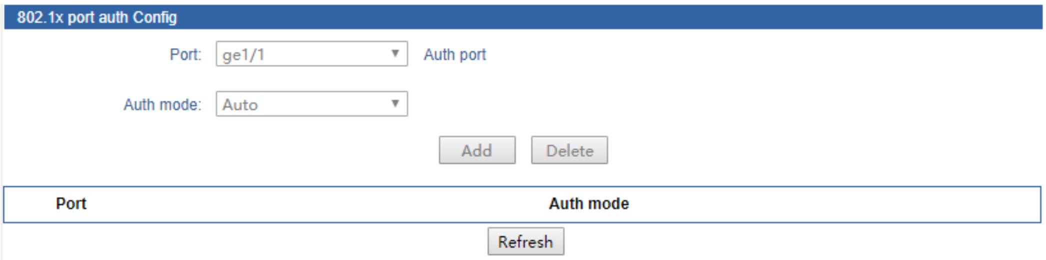
On the "Port Config" page, user can enable 802.1X port authentication.

Operation Path

Open in order: "Main Menu > Network security > 802.1X Config > Port Config".

Interface Description

Port configuration interface as follows:



The main element configuration description of port configuration interface.

Interface Element	Description
Port	Pull down the port list and select the port name corresponding to the device Ethernet port as authentication port.
Auth mode	802.1X port authentication mode: • Auto: In normal authentication state, the interface will be in pass state of force authentication when the host passes authentication; and the interface will be in no pass state when the authentication is unsuccessful; • Force authentication pass: Forces the interface to the status of passing authentication; • No pass of force authentication: Forces the interface to the status of not passing authentication.

Note

- Adopt MD5-Challenge between applicant and authentication system, don't support other methods;
- If the network connection properties do not include "Authentication" option, please choose "Attachment" -> "Administrative Tool" -> "Component Service" -> "Service", and set "Wired AutoConfig" to "Automatic".

6 Advanced Configuration

6.1 QOS Configuration

Quality of Service (QoS) is the service quality. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on. In network, user can improve the service quality by ensuring the transmission bandwidth, reducing transfer delay, data packet loss rate, delay jitter and other measures.

Network resources are always limited, as long as there exists the case of snatching network resources, there will be service quality requirements. Quality of service is relative to the network business, while ensuring the service quality of a certain type of business; it may damage the service quality of other businesses. For example, in the case of total network bandwidth is fixed, if a type of business occupies more bandwidth, other businesses will be able to use less bandwidth, which may influence the usage of other businesses. Therefore, network managers need to make rational planning and distribution of network resources according to the characteristics of various businesses, so that network resources can be efficiently utilized.

6.1.1Global Configuration

QoS function provides 8 internal queues, each queue supports 4 different levels traffic, High-priority data packets stay on the switch for a short period of time, and some latency-sensitive traffic supports lower latency. According to 802.1p priority level tag, IP TOS, the device can classify packets to a certain level.

Function Description

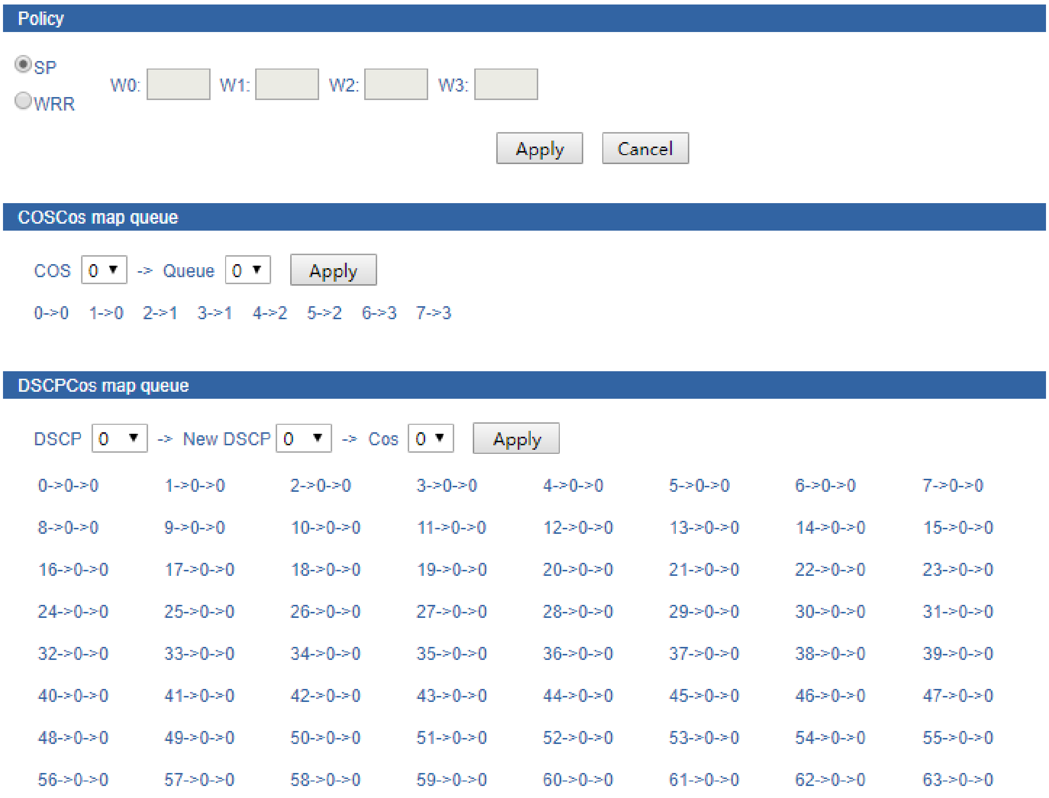
On the "Global Config" page, user can configure QOS scheduling policies, COS queue mapping, and DSCP queue mapping.

Operation Path

Open in order: "Main Menu > Advanced Config > QOS Config > Global Config".

Interface Description

Global configuration interface as follows:



Policy

● SP W0: W1: W2: W3:

○ WRR

Apply Cancel

COSCos map queue

COS 0 -> Queue 0 Apply

0->0 1->0 2->1 3->1 4->2 5->2 6->3 7->3

DSCPCos map queue

DSCP 0 -> New DSCP 0 -> Cos 0 Apply

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

The main element configuration description of global configuration interface.

Interface Element	Description
Policy	**SP strict priority and WRR weighted round robin scheduling algorithm two scheduling strategies.**
SP	SP functional status, check to enable this strategy. Notes: SP strict priority. SP schedule sends the higher-priority queues strictly according to the priority level from high to low. Queue 7 has the highest priority level and queue 0 has the lowest priority level.

Interface Element	Description
WWR	Gain the resource special gravity equivalent, value range is 0-100. Notes: Weighted Round Robin (WRR) is a weighted round robin (WRR) scheduling algorithm. WRR can configure the scheduled packets number in each queue, and conduct schedule between queues in turn.
Cos map queue	**IEEE802.1p priority level and queue mapping relation.**
COS	Grade of service, value range is 0-7. Notes: The service level value is larger, the level is lower, for example, "7" represents the highest priority level and "0" represents the lowest priority level.
Queue	QoS internal priority level queue, value range is 0-7.
DSCP mapping	**Mapping relation between DSCP priority level and COS queue.**
DSCP	DSCP priority level value is 0 - 63, 63 is the highest priority level, 0 is the lowest priority level.
New DSCP	In the drop-down list, New DSCP priority level 0 - 63 is optional.
Cos	In the drop-down list, COS priority level 0 - 7 is optional.

6.1.2 Port Configuration

Function Description

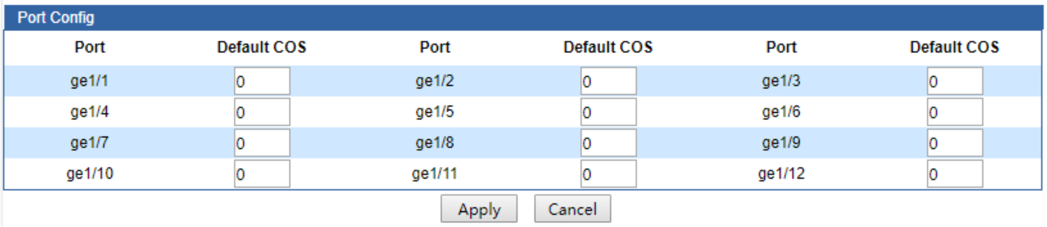
On the "Port Config" page, user can configure the port default COS.

Operation Path

Open in order: "Main Menu > Advanced Config > QOS Config > Port Config".

Interface Description

Port configuration interface as follows:



Port Config

Port	Default COS	Port	Default COS	Port	Default COS
ge1/1	0	ge1/2	0	ge1/3	0
ge1/4	0	ge1/5	0	ge1/6	0
ge1/7	0	ge1/8	0	ge1/9	0
ge1/10	0	ge1/11	0	ge1/12	0

The main element configuration description of port configuration interface.

Interface Element	Description
Port	Ethernet port number of the switch.
Default COS	Port default COS priority level. Notes: Value range is 0-7.

6.2 PoE Configuration

PoE (Power over Ethernet) means supplying power through Ethernet. It's a wired Ethernet power supply technology that enables electric power to transmit to terminal device through data line or free line.

PoE power supply system includes:

- PSE (Power-sourcing Equipment): PoE device that supplies powered device with power through Ethernet.
- PD (Powered Device): powered device like wireless AP (Access Point), POS machine, camera and so on.
- PoE power supply: PoE power supply powers the whole PoE system. The quantity of PD that connects to PSE is limited by the power of PoE power supply.

Note

This series of products have two types, PoE and non-PoE. Please take actual product as standard. Only PoE product supports PoE configuration and provides PoE output power supply function; non-PoE product doesn't support this configuration.

6.2.1 Global Configuration

Function Description

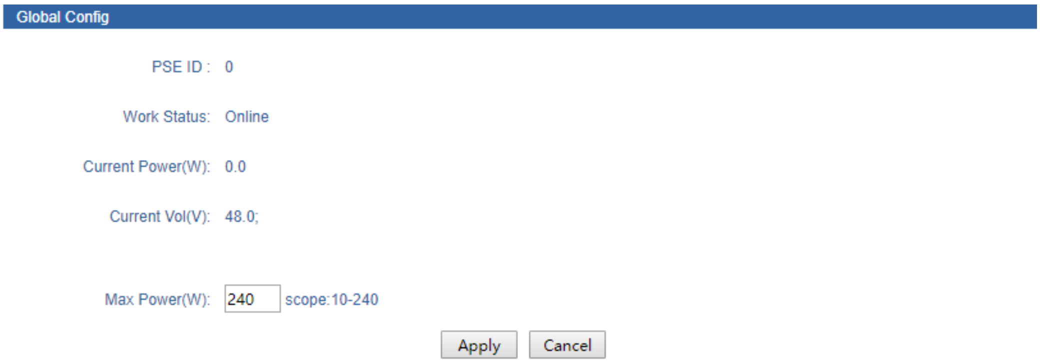
On the "Global Config" page, user can configure the maximum PoE output power of the device.

Operation Path

Open in order: "Main Menu > Advanced Config > PoE Config > Global Config".

Interface Description

Global configuration interface as follows:



Global Config

PSE ID : 0

Work Status: Online

Current Power(W): 0.0

Current Vol(V): 48.0;

Max Power(W): 240 scope:10-240

The main element configuration description of global configuration interface:

Interface Element	Description
PSE ID	The PSE ID display of current device.
Work status	The work status display of PSE power supply module of current device. Its status are shown as follow: • Online: PSE power supply module operates normally; • Off-line: PSE power supply module operates abnormally and disconnects.
Current power (W)	The PoE output power value display of current device, the unit is W.
Current Vol (V)	The PoE output voltage value display of current device, the unit is V.
Max Power (W)	The maximum PoE output power value configuration of current device. The value range is 10-240, and the unit is W.

6.2.2 PoE Port Configuration

Function Description

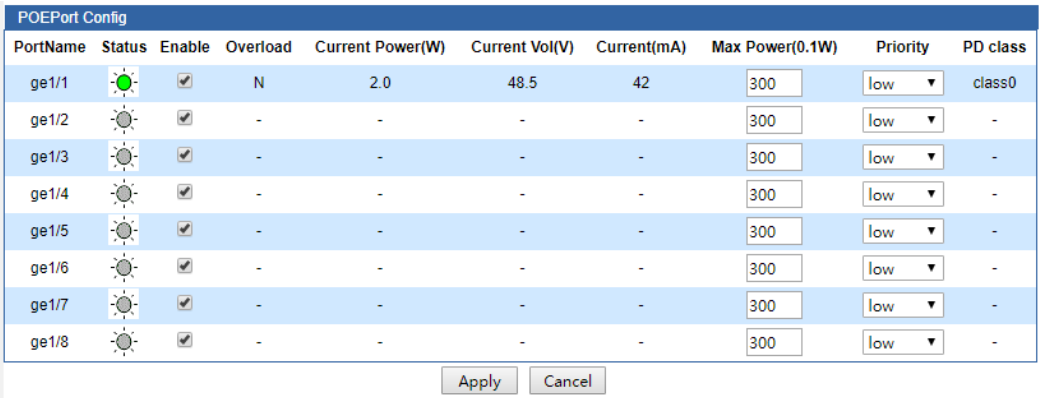
On the "PoE Port Config" page, user can configure the enablement, maximum output power and power supply priority of each PoE port of the device.

Operation Path

Open in order: "Main Menu > Advanced Config > PoE Config > PoE Port Config".

Interface Description

PoE Port configuration interface as follows:



POEPort Config

PortName	Status	Enable	Overload	Current Power(W)	Current Vol(V)	Current(mA)	Max Power(0.1W)	Priority	PD class
ge1/1	🟢	☑	N	2.0	48.5	42	300	low ▼	class0
ge1/2	⚪	☑	-	-	-	-	300	low ▼	-
ge1/3	⚪	☑	-	-	-	-	300	low ▼	-
ge1/4	⚪	☑	-	-	-	-	300	low ▼	-
ge1/5	⚪	☑	-	-	-	-	300	low ▼	-
ge1/6	⚪	☑	-	-	-	-	300	low ▼	-
ge1/7	⚪	☑	-	-	-	-	300	low ▼	-
ge1/8	⚪	☑	-	-	-	-	300	low ▼	-

The main element configuration description of PoE port configuration interface:

Interface Element	Description
Port Name	The corresponding name of this device’s PoE Ethernet port.
Status	The PoE power supply status of current port. The status displays as follow: • 🟢: PD device is powered by PoE port; • ⚪: PD device is not powered by PoE port or disconnected.
Enable	Checkbox of port enablement. Check the box to enable PoE port; otherwise the PoE port would be disabled.
Overload	The overload status of current PoE port. The status displays as follow: • Y: the output power of current PoE port is larger than the maximum power.

Interface Element	Description
	● N: the output power of current PoE port is equal to or smaller than the maximum power.
Current power (W)	The output power value of current PoE port. Unit: W.
Current Vol (V)	The output voltage value of current PoE port. Unit: V.
Current (mA)	The current value of current PoE port. Unit: mA.
Max power (0.1W)	The maximum output power value of current PoE. The value range is 0-300. Unit: 0.1W.
Priority	The priority configuration of PoE port power supply. Port power distribution priority with the constraint of gross power. Its pull-down list options are shown as below: ● High: high priority; ● Medium: medium priority ● Low: low priority. Note: When the switch supplies power at nearly full capacity, it would first supply power to the PD device that connects to the port with High priority; then the PD device that connects to port with Medium priority.
PD class	Power class of PD device. It shows as below: ● Class0: default class, when it’s unable to classify PD. ● Class1: extremely low power ● Class2: low power ● Class3: medium power ● Class4: high power, this class is supported by IEEE 802.3at standard.

6.3 LLDP Configuration

LLDP is a layer 2 topology discovery protocol, its basic principle is: Devices in network send the status information message to adjacent device, and each port in the device stores its own information, if there is change in the status of local device, it can also send updated information to the adjacent device directly connected to it. Adjacent devices will store the information in standard SNMP MIB bank. The network management system could inquiry the connection status of current layer 2 from SNMP MIB bank. It should be noted that LLDP is only a remote device status information discovery protocol, which cannot complete the network device configuration, port control and other functions.

6.3.1 Global Configuration

Function Description

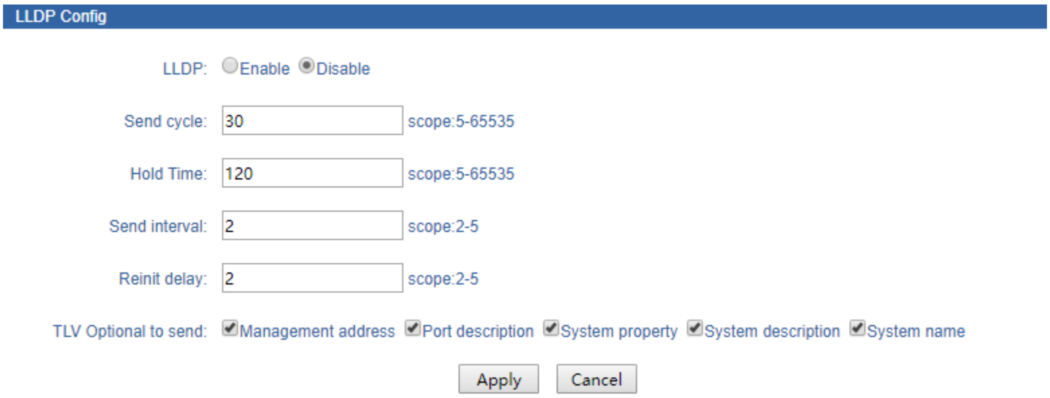
On the "Global Config" page, user can configure LLDP relative parameters.

Operation Path

Open in order: "Main Menu > Advanced Config > LLDP Config > Global Config".

Interface Description

Global configuration interface as follows:



LLDP Config

LLDP: ○Enable ●Disable

Send cycle: 30 scope:5-65535

Hold Time: 120 scope:5-65535

Send interval: 2 scope:2-5

Reinit delay: 2 scope:2-5

TLV Optional to send: ☑Management address ☑Port description ☑System property ☑System description ☑System name

The main element configuration description of global configuration interface.

Interface Element	Description
LLDP	LLDP function status, options as follows: • Enable; • Disable.
Send cycle	LLDP send cycle range is 5-65535. Notes: When no device status changes, the device periodically sends LLDP packets to its adjacent nodes. The interval is called the period for sending LLDP packets.
Hold Time	LLDP hold time range is 5-65535.

Interface Element	Description
	Notes: Hold time can control the aging time of device information in the adjacent device.
Send interval	LLDP send interval range is 2-5, that is the delay time of LLDP continuous message sending.
Reinit delay	Reinit delay time range is 2-5. Notes: When LLDP work mode of the port changes, port will conduct initialization operation to the protocol state machine, Re-enable the delay time via configuration to avoid continuous initialization of port due to the frequent changes in working mode.
TLV Optional to send	TLV sends information, options below are optional: ● Management address; ● Port description; ● System property; ● System description; ● System name. Notes: TLV is a unit that makes up LLDPDU. Each TLV represents a piece of information. LLDPDU is the data unit encapsulated in the data part of LLDP packet.

6.3.2 Port Configuration

Function Description

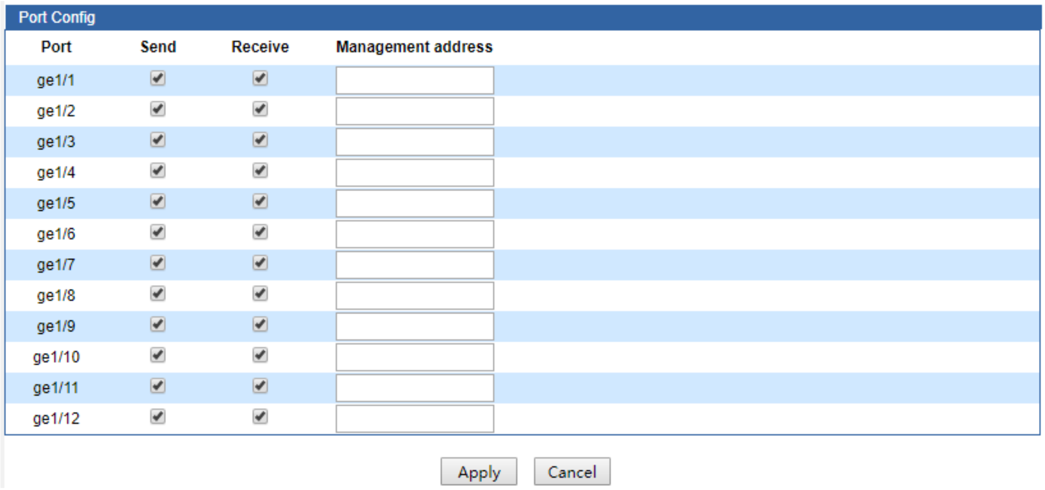
On the "Port Config" page, user can configure the sending and receiving mode and management address of the port.

Operation Path

Open in order: "Main Menu > Advanced Config > LLDP Config > Port Config".

Interface Description

Port configuration interface as follows:



Port Config

Port	Send	Receive	Management address
ge1/1	☑	☑	
ge1/2	☑	☑	
ge1/3	☑	☑	
ge1/4	☑	☑	
ge1/5	☑	☑	
ge1/6	☑	☑	
ge1/7	☑	☑	
ge1/8	☑	☑	
ge1/9	☑	☑	
ge1/10	☑	☑	
ge1/11	☑	☑	
ge1/12	☑	☑	

The main element configuration description of port configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Send	The device won't receive LLDP information from adjacent device but will send LLDP information.
Receive	The device won't send LLDP information, but will receive and analyze LLDP information from adjacent device.
Management address	Corresponding LLDP management IP address of the port. Notes: LLDP management address is the address to be marked and managed by network management system. Management address can definitely mark a device, which is beneficial to the drawing of network topology and network management. Management address is encapsulated in Management Address TLV field of LLDP message and sent to adjacent nodes.

6.3.3 LLDP Neighbors

Function Description

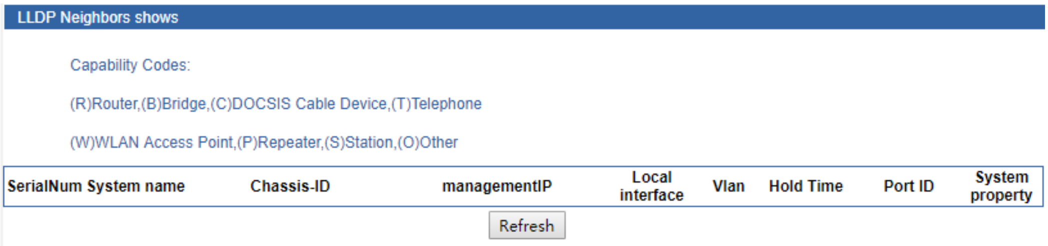
On the "LLDP Neighbors" page, user can look over the relative information of neighbors.

Operation Path

Open in order: "Main Menu > Advanced Config > LLDP Config > LLDP Neighbors".

Interface Description

LLDP neighbors interface as below:



LLDP Neighbors shows

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point,(P)Repeater,(S)Station,(O)Other

SerialNum	System name	Chassis-ID	managementIP	Local interface	Vlan	Hold Time	Port ID	System property

The main element configuration description of LLDP neighbors interface.

Interface Element	Description
SerialNum	LLDP neighbors information display serial number.
System name	System name of neighbor devices.
Chassis-ID	Bridge MAC address of neighbor device or port.
management IP	Management IP address of neighbor device or port.
Local interface	Local port number of local switch connected to adjacent devices.
Vlan	Local switch port VLAN PVID number.
Hold Time	LLDP hold time of neighbor device.
Port ID	Neighbor device port ID number.
System property	System property, abbreviated code as below: ● R: Router; ● B: Bridge; ● C: DOCSIS Cable Device; ● T: Telephone; ● W: WLAN Access Point; ● P: Repeater; ● S: Station; ● O: Other.

6.4 SNMP Configuration

SNMP Introduction

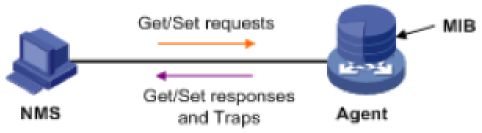
Now, the broadest network management protocol in network is SNMP (Simple Network Management Protocol). SNMP is the industrial standard that is widely accepted and comes into use, it's used for guaranteeing the management information transmission between two points in network, and is convenient for network manager search information, modify information, locate faults, complete fault diagnosis, conduct capacity plan and generate a report. SNMP adopts polling mechanism and only provides the most basic function library, especially suit for using in minitype, rapid and low price environment. SNMP implementation is based on connectionless transmission layer protocol UDP, therefore, it can achieve barrier - free connection to many other products.

SNMP Working Mechanism

SNMP is divided into NMS and Agent:

- Network Management Station (NMS) is the work station that runs client procedure, at present, common network management platforms include Quid View, Sun Net Manager and IBM Net View. Agent is the server software that runs in network device.
- NMS can send Get Request, Get Next Request and Set Request messages to Agent, after receiving these request messages from NMS, Agent will conduct Read or Write operation, generate Response message and return messages to NMS according to the message type. When the device appears abnormal situation or the state changes (such as device resets), Agent will forwardly send Trap message to NMS and report occurred event to NMS.

Any managed resource is represented as an object, called a managed object. MIB (Management Information Base, management information base) is the collection of managed objects. NMS manages the device via MIB. MIB has defined the hierarchical relationship between the nodes and a set of properties of objects, such as objects' name, access privilege and data type, etc. Each Agent has its own MIB. Managed device has its own MIB files; compiling these MIB files in NMS can generate MIB of the device. NMS conducts read/write operation according to access privilege, and achieves Agent management. Relationship of NMS, Agent and MIB as the picture below.



MIB is organized according to a tree structure, consisting of a number of nodes; each node represents a managed object that can be uniquely identified by a string of path-specific numbers starting from the root, this string of OID (Object Identifier) ".

SNMP supports three basic operations:

- **Get operation:** Manager adopts the operation to inquire a variable value of Agent;
- **Set operation:** Manager adopts the operation to set a variable value of Agent;
- **Trap operation:** Agent adopts the operation to send abnormal alarm information to manager.

SNMP Protocol Version

At present, SNMP Agent in the device supports SNMP v1 version, SNMP v2c and SNMP v3 version. SNMP v1, SNMP v2c adopt community name authentication, SNMP message of community name without device authentication will be discarded. SNMP community name is used for defining the relationship of SNMP, NMS and SNMP Agent. Community name plays a role similar to password, and can limit SNMP Agent in SNMP NMS access device. User can choose and appoint one or more characters relative to community name:

- Define MIB view that community name can access.
- Configure MIB object access privilege of community name as read-write privilege or read-only privilege. Community name with read-only privilege can only inquire the device information; community name with read-write privilege can configure the device.
- Set the basic access control list appointed by community name.

6.4.1System Information

Function Description

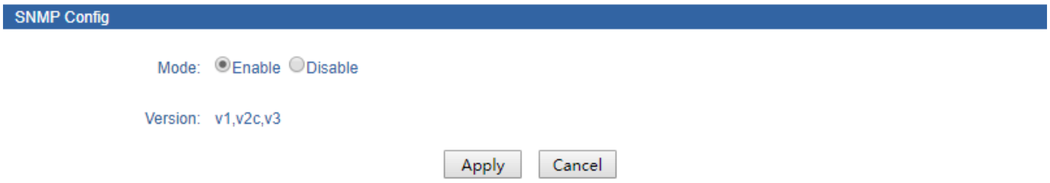
On the "System Information" page, user can choose enable or disable SNMP function.

Operation Path

Open in order: "Main Menu > Advanced Config > SNMP Config > System Information".

Interface Description

System Info interface as follows:


SNMP Config

Mode: ● Enable ○ Disable

Version: v1,v2c,v3

The main element configuration description of system information interface.

Interface Element	Description
Mode	SNMP function state: • Enable; • Disable.
Version	Compatible with v1, v2c, v3 versions.

6.4.2 View

Function Description

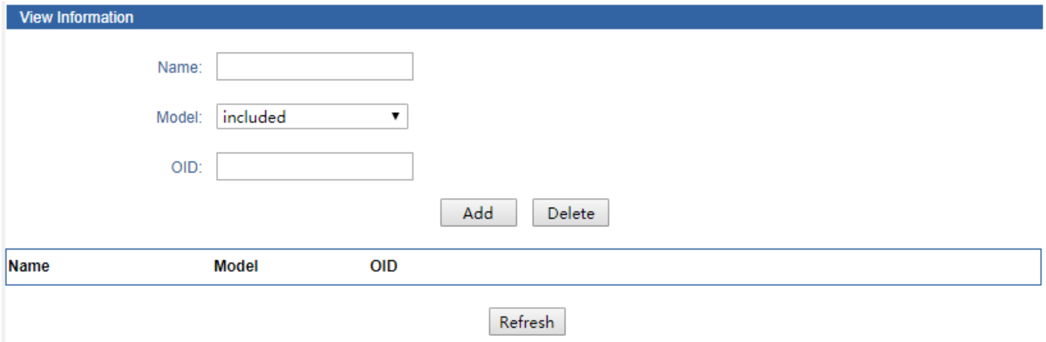
On the "View" page, user can add/delete view.

Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > View".

Interface Description

View interface as below:


View Information

Name:

Model: included

OID:

Name	Model	OID

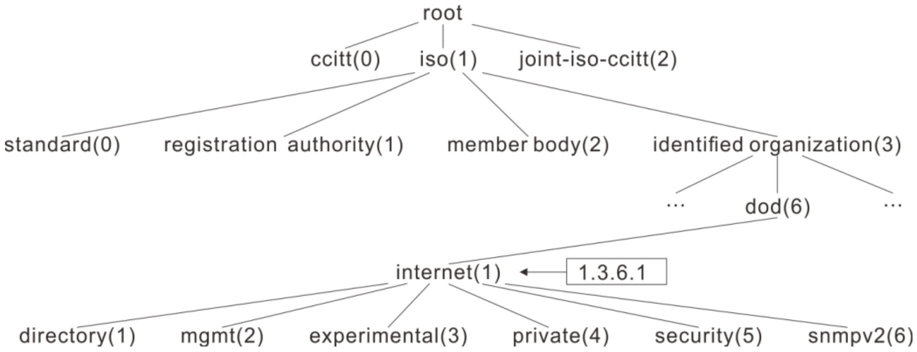
The main element configuration description of view interface:

Interface Element	Description

Name	SNMP view name definition, support 32 characters input. Note: Name can't be empty or contain "&" or ";" or " or ' or "\" or "/"
Model	Node OID dealing method, options as below: ● Included: It contains all objects under the node subtree; ● Excluded: Eliminate all objects beyond the node subtree.
OID	Node location information of MIB tree where the device resides. Notes: OID object identifier, a component node of MIB, uniquely identified by a string of numbers that represent the path.

Note

- In the SNMP view configuration, if user configures the "Node OID" to ".1.3.6.1", that is the INTERNET layer under MIB library, as shown in the following figure:



- When "Model" is "included", it contains all objects under MIB library 1.3.6.1 subtree;
- When "Model" is "excluded", it represents eliminating all objects beyond MIB library 1.3.6.1 subtree.
- It is recommended that non-professionals fill in ".1" in "OID". That is, OID is 1, indicating all objects under MIB library 1 subtree.

6.4.3 Community

Function Description

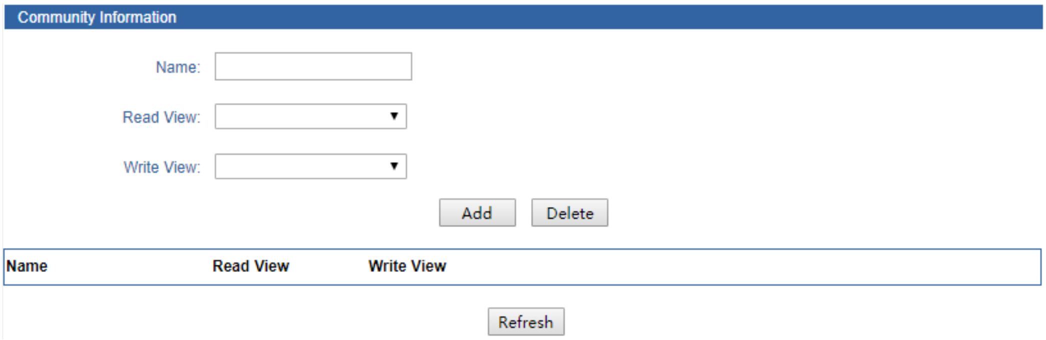
On the "Community" page, user can add/delete community. Define MIB view that community name can access, set MIB object access privilege of community name as read-write privilege or read-only privilege.

Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > Community".

Interface Description

Community interface as below:



The main element configuration description of community interface.

Interface Element	Description
Name	Community name definition. Note: The name needs to be same to view name.
Read View	Read only privilege view name selection.
Write View	Read-write privilege view name selection.

6.4.4V3 User

SNMPv3 adopts User-Based Security Model (USM) authentication mechanism. Network manager can configure authentication and encryption function. Authentication is used to verify the validity of the packet sender and prevent unauthorized users from accessing it. Encryption encrypts the transmission packet between NMS and Agent to prevent eavesdropping. It adopts authentication and encryption function to provide higher security for the communication between NMS and Agent.

Function Description

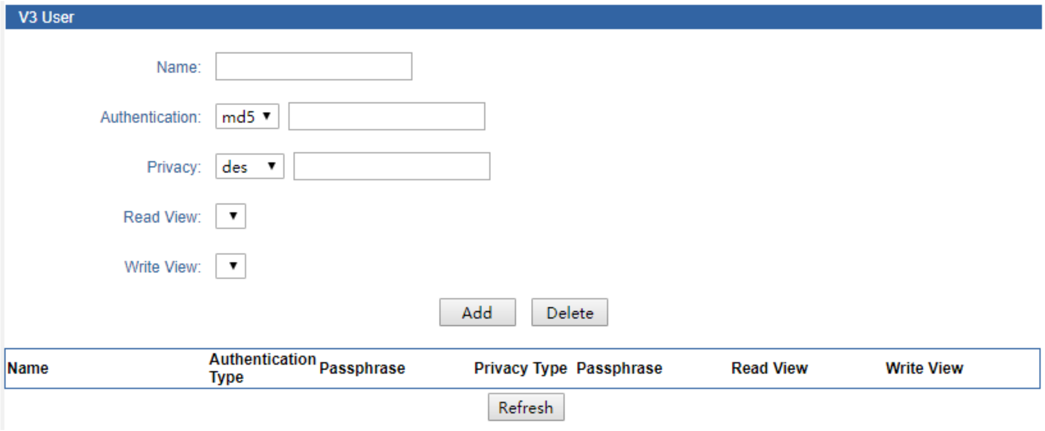
On the "V3 User" page, user can configure SNMP V3 user information.

Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > V3 User".

Interface Description

V3 user interface as follows:



The main element configuration description of V3 user interface:

Interface Element	Description
Name	SNMP v3 version user name definition, combination of letters and numbers.
Authentication	Authentication information filling, two authentication methods optional: • Md5:Information abstract algorithm 5; • Sha: Secure hash algorithm.
Privacy	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard; • None: No encryption.
Read View	Read only privilege view name selection.
Write View	Read-write privilege view name selection.

6.4.5 Trap

Base on TCP/IP protocol, SNMP usually adopts UDP port 161 (SNMP) and 162 (SNMP-traps), SNMP protocol agent exists in the network device and adopts information specific to the device (MIBs) as the device interface; these network devices can be monitored or controlled via Agent. When a trap event occurs, the message is transmitted by SNMP Trap. At this point, an available trap receiver can receive the trap message.

Function Description

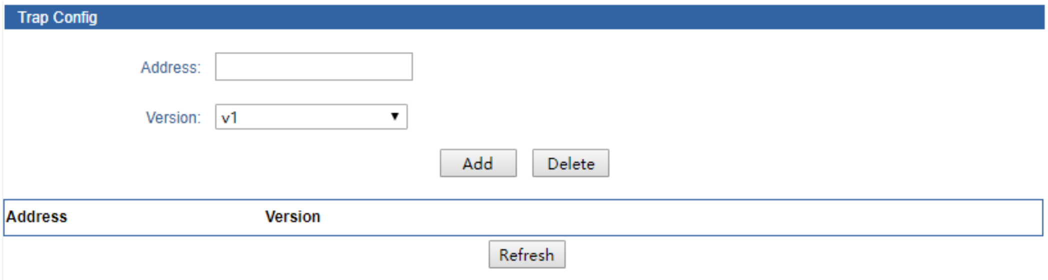
On the "Trap" page, user can configure the Trap information.

Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > Trap".

Interface Description

Trap interface as below:



The main element configuration description of Trap interface:

Interface Element	Description
Address	IP address of SNMP management device, such as PC.
Version	SNMP management device version, options as below: • v1; • v2c;

6.5 RMON Configuration

RMON (Remote Network Monitoring) mainly achieves statistics and alarm functions, which are used for remote monitoring and management of management device to managed devices. Statistical function refers to that managed device can periodically or continuously keep track of all the traffic information on the network segment connected to the port , For example, the total number of packets received on a network segment in a period of time, or the total number of received super long packets. Alarm function refers to the managed device can monitor the value of specified MIB variables, When the alarm threshold is reached (for example, the port rate reaches specified value or the broadcast packet reaches specified rate), the system will automatically log and send Trap messages to the management device.

6.5.1 Event

Function Description

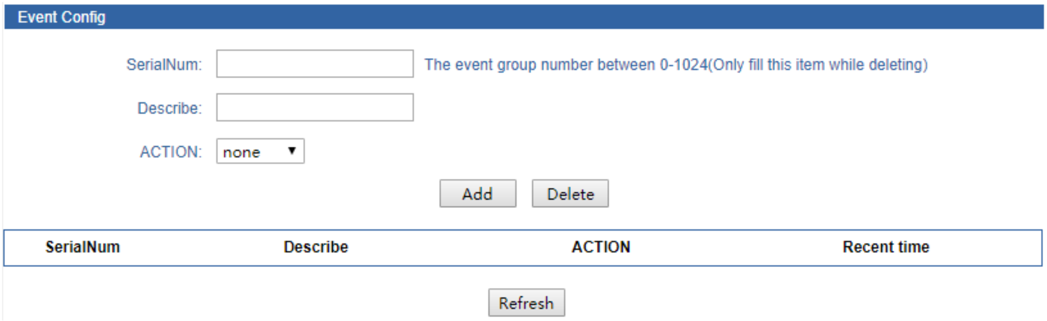
On the "Event" page, user can add, delete or check the configuration information of event.

Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > Event".

Interface Description

Check event interface as below:



Event Config

SerialNum: The event group number between 0-1024(Only fill this item while deleting)

Describe:

ACTION: none

SerialNum	Describe	ACTION	Recent time

The main element configuration description of event interface.

Interface Element	Description
SerialNum	Triggered event serial number when monitoring MIB object exceeds threshold value. Notes: This serial number corresponds to the rising event index and falling event index set in RMON alarm configuration information.
Description	Some description information for describing the event.
ACTION	Event dealing method, options as below: ● None: No dealing; ● log: Record the event in the log table when the event is triggered; ● trap: Send Trap information to management station for informing the occurring of event when the event is triggered;

Interface Element	Description
	- Log, trap: Record the event in the log table and produce a trap information when the event is triggered.

6.5.2 Statistical

Function Description

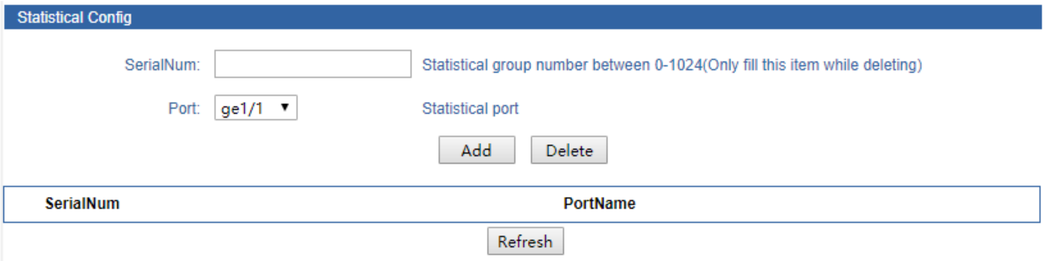
On the "Statistical" page, user can add, delete or check the configuration information of statistical.

Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > Statistical".

Interface Description

Statistical interface as below:



The main element configuration description of statistical interface.

Interface Element	Description
SerialNum	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Port	Set a port number (physical interface) as the receiving end of monitoring data information.

6.5.3 History

Function Description

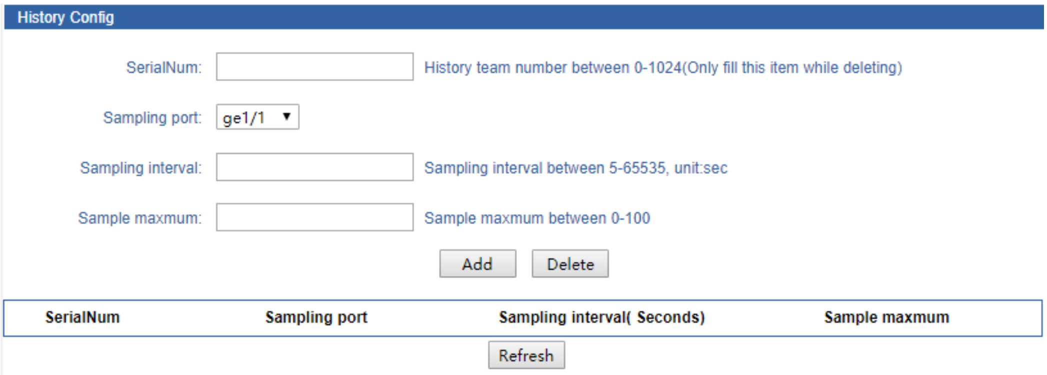
On the "History" page, user can add, delete or check the configuration information of history.

Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > History".

Interface Description

History interface as below:



History Config

SerialNum: History team number between 0-1024(Only fill this item while deleting)

Sampling port: ge1/1

Sampling interval: Sampling interval between 5-65535, unit:sec

Sample maxmum: Sample maxmum between 0-100

SerialNum	Sampling port	Sampling interval(Seconds)	Sample maxmum

The main element configuration description of history interface.

Interface Element	Description
SerialNum	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Sampling port	Set a physical interface as the receiving end of monitoring information.
Sampling interval	The interval time of gaining statistics data each two times.
Sample maxnum	Table entries needed to be reserved.

6.5.4 Alarm

Function Description

On the "Alarm" page, user can add, delete the alarm or check the alarm configuration information.

Alarm type adopts absolute to directly monitor MIB object value; Alarm type adopts delta to monitor changes in MIB object values between two samples;

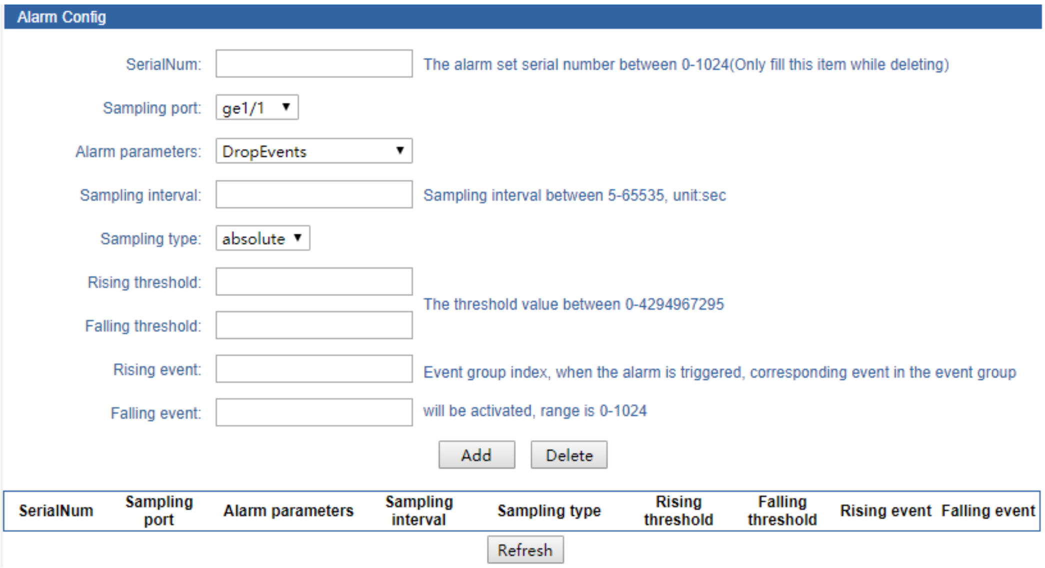
- When monitoring MIB object reaches or surpasses the rising threshold value, it will trigger corresponding event of rising event index;
- When monitoring MIB object reaches or surpasses declining threshold value, it will trigger corresponding event of declining event index;

Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > Alarm".

Interface Description

Alarm interface as below:



Alarm Config

SerialNum: [ ] The alarm set serial number between 0-1024(Only fill this item while deleting)

Sampling port: ge1/1

Alarm parameters: DropEvents

Sampling interval: [ ] Sampling interval between 5-65535, unit:sec

Sampling type: absolute

Rising threshold: [ ]

Falling threshold: [ ]

The threshold value between 0-4294967295

Rising event: [ ]

Falling event: [ ]

Event group index, when the alarm is triggered, corresponding event in the event group will be activated, range is 0-1024

SerialNum	Sampling port	Alarm parameters	Sampling interval	Sampling type	Rising threshold	Falling threshold	Rising event	Falling event

The main element configuration description of alarm interface.

Interface Element	Description
SerialNum	Serial number is used to identify a special alarm configuration information, when the serial number is same to the application serial number set before, previous

Interface Element	Description
	configuration will be replaced.
Sampling port	Set a physical interface as the receiving end of monitoring information.
Alarm parameters	Alarm parameters, options as follows: ● DropEvents: Falling edge event; ● Octets: Byte. ● Pkts: Data packet. ● BroadcastPkts: Broadcast packet; ● MulticastPkts: Multicast packet; ● CRCAlignErrors: CRC alignment errors; ● UndersizePkts: Ultra short packet number, less than 64 bytes; ● OversizePkts: Ultra-long packet number, more than 1518 bytes; ● Fragments: Fragment frame data; ● Jabbers: Invalid huge frame data, more than 1518 bytes; ● Collisions: Conflicts occur; ● Pkts64Octets: 64 bytes data packet; ● Pkts65to127Octets: 65-127 bytes data packet; ● Pkts128to255Octets: 128-255 bytes data packet; ● Pkts256to511Octets: 256-511 bytes data packet; ● Pkts512to1023Octets: 512-1023 bytes data packet; ● Pkts1024to1518Octets: 1024-1518 bytes data packet.
Sampling interval	Sampling time interval value, value range is 5-65535, unit: second.
Sampling type	Two sampling methods, options as follows: ● Absolute: When alarm variable value reaches alarm threshold value, an alarm is triggered; If the second sampling is same to last sampling alarm type, alarm isn't triggered again; ● Delte: When alarm variable value reaches alarm threshold value during each sampling, an alarm is triggered.
Rising threshold	Alarm variable value, upper limit alarm, threshold value is 0-4294967295. Notes:

Interface Element	Description
	In the rising process of alarm variable value, when the variable value surpasses rising threshold, an alarm occurs at least one time.
Falling threshold	Alarm variable value, lower limit alarm, threshold value is 0-4294967295. Notes: In the falling process of alarm variable value, when the variable value reaches falling threshold, an alarm occurs at least one time.
Rising event	Event index, when alarm variable value reaches or surpasses the rising event threshold value, it will activate corresponding event in event group, value range is 0-1024.
Falling event	Event index, when alarm variable value reaches or is less than the falling threshold value, it will activate corresponding event in event group, value range is 0-1024.

6.6 DHCP Server Configuration

Dynamic Host Configuration Protocol (DHCP) is usually applied in large LAN network environment, its main functions include intensively manage, distribute IP address, make the host in network environment actively gain IP address, Gateway address, DNS server address and other information, and improve the address utilization rate.

6.6.1DHCP Server Configuration

Function Description

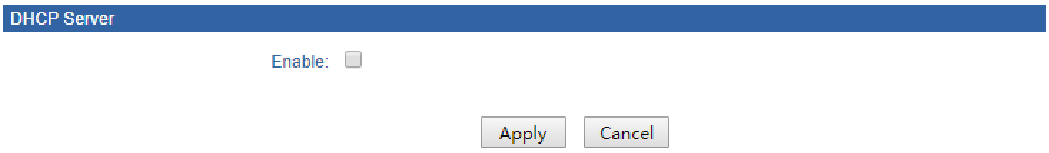
On the "DHCP Server Config" page, user can enable/disable DHCP Server.

Operation Path

Open in order: "Main Menu > Advanced Config > QOS Server Config > DHCP Server Config".

Interface Description

DHCP Server configuration interface as follows:


DHCP Server

Enable: □

Apply Cancel

The main element configuration description of DHCP Server configuration interface.

Interface Element	Description
DHCP Server	After enable DHCP Server function, set the device as a DHCP server by setting static allocation address table, the device can distribute IP address to devices connected to it.

6.6.2 DHCP Pool Configuration

After user defines DHCP range and exclusion range, surplus addresses constitute an address pool; addresses in the address pool can be dynamically distributed to hosts in network. Address pool is valid only for the method of automated IP acquisition; manual IP configuration can ignore this option only if conforming to the rules.

DHCP server chooses and distributes IP address and other relative parameters for client-side from address pool.

DHCP server adopts tree structure: Tree root is the address pool of natural network segment. Branch is the subnet address pool of the network segment. Leaf node is the manually binding client address. Same level address pool order is decided by the configuration order. This kind of tree structure has realized the inheritance of configuration, that is, subnet configuration inherits the configuration of natural network segment, and client configuration inherits the subnet configuration. Therefore, as for some common parameters (such as DNS server address), user only needs to configure in the natural network segment or subnet. Specific inheritance situation as follows:

1. When the parent-child relationship is established, sub address pool will inherit the existing configuration of parent address pool.
2. After the parent-child relationship is established, parent address pool is configured, sub-address pool will inherit or not, two situations as follows:

- If the child address pool doesn't include the configuration, it will inherit the configuration of parent address pool;
- If the child address pool has included the configuration, it won't inherit the configuration of parent address pool.

Function Description

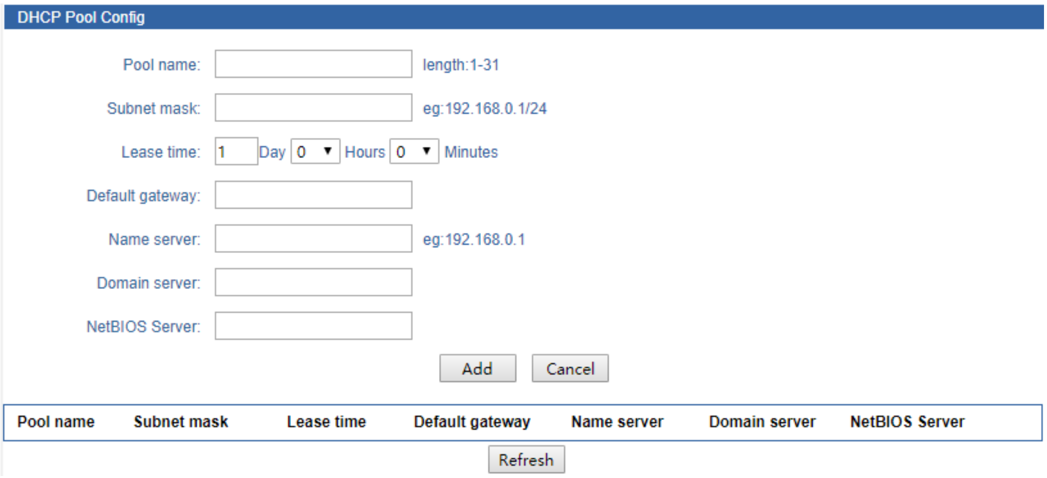
On the "DHCP Pool Config" page, user can add, delete the address pool and look over the configuration information of address pool.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > DHCP Pool Config".

Interface Description

DHCP address pool configuration interface as follows:


DHCP Pool Config

Pool name: length:1-31
Subnet mask: eg:192.168.0.1/24
Lease time: 1 Day 0 Hours 0 Minutes
Default gateway:
Name server: eg:192.168.0.1
Domain server:
NetBIOS Server:

Pool name	Subnet mask	Lease time	Default gateway	Name server	Domain server	NetBIOS Server

The main element configuration description of DHCP pool configuration interface.

Interface Element	Description
Pool name	Address pool name, length range is 1-31.
Subnet mask	Address pool distributes the IP address network segment of client-side, for example: 192.168.0.1/24.
Lease time	IP address utilization valid time of client-side, range is 0-999 days.
Default gateway	Default gateway address of client-side.
DNS server	DNS server IP address of client-side.
Domain server	DNS server domain address of client-side.

Interface Element	Description
NetBIOS Server	NetBIOS server IP address of client-side.

6.6.3 Client List

Function Description

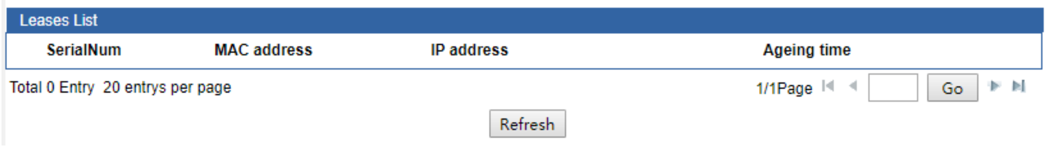
On the "Client List" page, user can look over the information of DHCP client-side.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > Client List".

Interface Description

Client list interface as follows:


Leases List

SerialNum	MAC address	IP address	Ageing time

Total 0 Entry 20 entrys per page

The main element configuration description of client list interface.

Interface Element	Description
SerialNum	Serial number name of DHCP client-side.
MAC address	MAC address of DHCP client-side device.
IP address	IP address of DHCP client-side device.
Expire	Aging time of the client-side address.

6.6.4 Static Client Configuration

Function Description

On the "Static Client Config" page, user can add, delete the static client-side and look over the configuration information of static client-side.

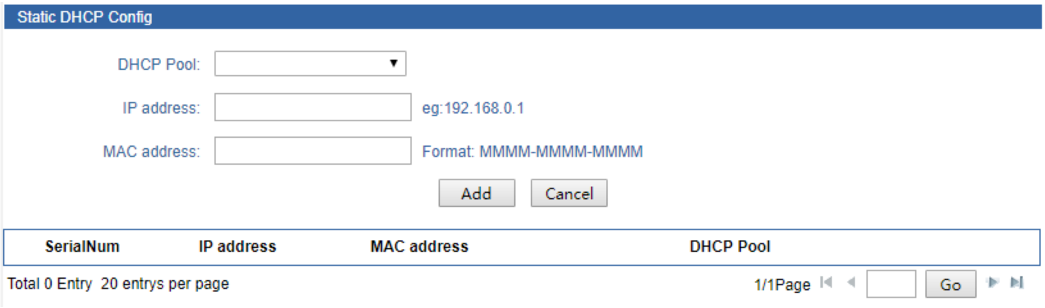
The client MAC address is bound to the address assigned by DHCP server, therefore, each address obtained by the client from server is a binding IP address.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > Static Client Config".

Interface Description

Static Client Configuration interface as follows:



Static DHCP Config

DHCP Pool:

IP address: eg:192.168.0.1

MAC address: Format: MMMM-MMMM-MMMM

SerialNum	IP address	MAC address	DHCP Pool

Total 0 Entry 20 entrys per page

The main element configuration description of static client configuration interface.

Interface Element	Description
DHCP Pool	Corresponding list name of DHCP address pool.
IP address	IP address that DHCP address pool distributes, client-side needs to gain the static IP address.
MAC address	MAC address of DHCP client.

6.6.5 Port Address Binding Configuration

Function Description

On the "Port binding config" page, user can bind IP address relation port distributes.

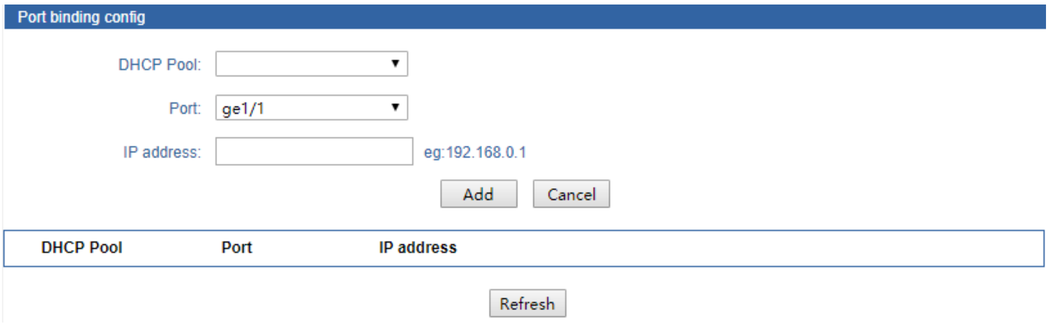
Device A enable DHCP Server function and set 2 static distribution address tables: 192.168.1.19 corresponding port is 1; 192.168.1.20 corresponding port is 2. After device B enable IP address automated acquisition function, if device A is connected to device B via port 1, device B can automatically gain IP address 192.168.1.19; If device A is connected to device B via port 2, device B can automatically gain IP address 192.168.1.20.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > Port binding config".

Interface Description

Port binding configuration interface as follows:



Port binding config

DHCP Pool:

Port: ge1/1

IP address: eg:192.168.0.1

DHCP Pool	Port	IP address

The main element configuration description of port binding configuration interface.

Interface Element	Description
DHCP Pool	Corresponding list name of DHCP address pool.
Port	The corresponding port name of the device Ethernet port.
IP Address	IP address that DHCP address pool distributes, the IP address that client-side gains in the port .

6.7 DHCP-snooping

DHCP Snooping is layer 2 snooping function of DHCP service, after enable DHCP Snooping function, device can extract and record IP address and MAC address information from received DHCP-ACK and DHCP-REQUEST messages.

For security reasons, security department needs to record the IP address used by user to access the Internet, and confirm the correspondence between IP address applied by user and MAC address of the host used by user. User can snoop DHCP-REQUEST messages and DHCP-ACK messages via DHCP Snooping function, and record IP address information user gains.

6.7.1 Global Configuration

Function Description

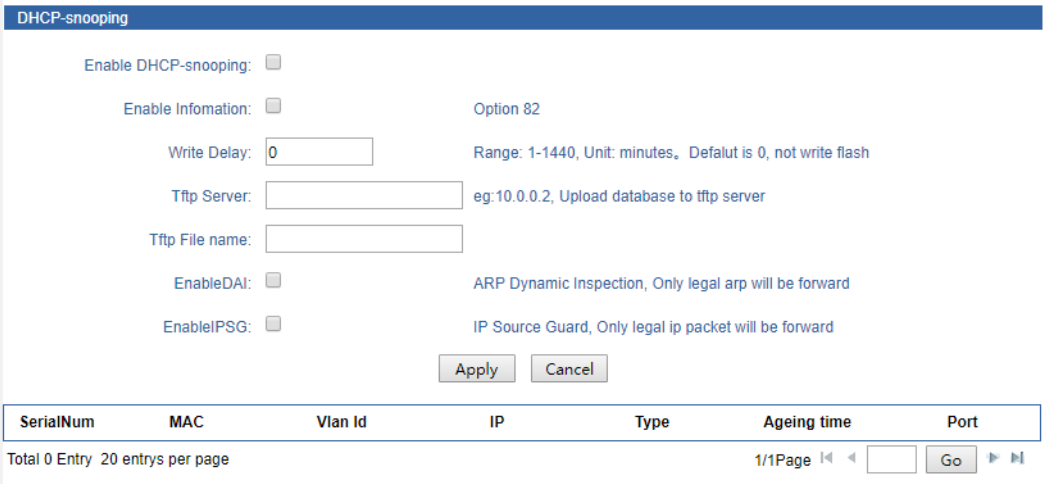
On the "Global Config" page, user can configure DHCP-Snooping parameters information.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Global Config".

Interface Description

Global configuration interface as follows:



DHCP-snooping

Enable DHCP-snooping: ☐

Enable Infomation: ☐ Option 82

Write Delay: 0 Range: 1-1440, Unit: minutes。 Defalut is 0, not write flash

Tftp Server: eg:10.0.0.2, Upload database to tftp server

Tftp File name:

EnableDAI: ☐ ARP Dynamic Inspection, Only legal arp will be forward

EnableIPSG: ☐ IP Source Guard, Only legal ip packet will be forward

SerialNum	MAC	Vlan Id	IP	Type	Ageing time	Port

Total 0 Entry 20 entrys per page 1/1Page

The main element configuration description of global configuration interface.

Interface Element	Description
Enable DHCP-Snooping	Enable DHCP-Snooping function checkbox.
Enable Information	Enable information function checkbox, after checking, enable Option 82 relay agent function which has recorded the location information of DHCP client.
Write Delay	Write delay range is 1-1440; unit is minute, default to 0, which represents not writing.
Tftp Server	Upload database to IP address of TFTP server, for example 10.0.0.2.
Tftp filename	Folder name of database uploading to TFTP server.

Interface Element	Description
Enable DAI	Enable DAI optional box, after checking, forward ARP sent by legitimate host according to DHCP Snooping table items.
Enable IPSG	Enable IPSG optional box, after checking, forward IP message sent by legitimate host via dynamically gaining DHCP Snooping table items.

6.7.2 Static Binding

Function Description

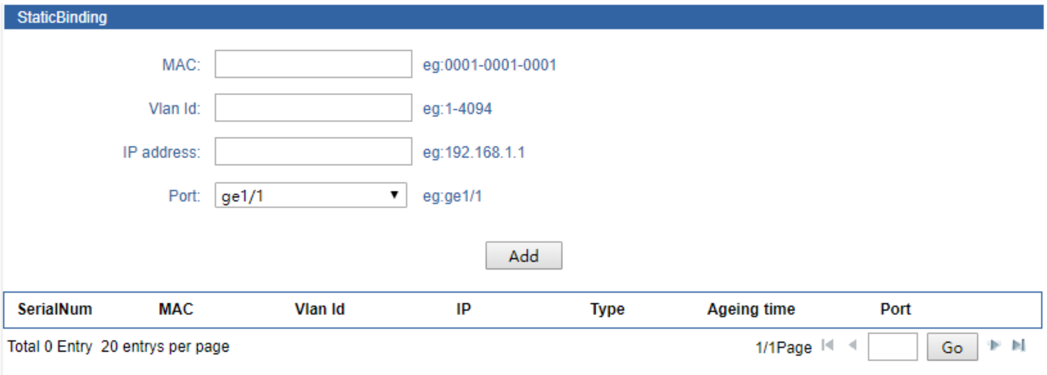
On the "Static Binding" page, user can bind static MAC and port.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Static Binding".

Interface Description

Static binding interface as follows:



StaticBinding

MAC: eg:0001-0001-0001

Vlan Id: eg:1-4094

IP address: eg:192.168.1.1

Port: ge1/1 eg:ge1/1

SerialNum	MAC	Vlan Id	IP	Type	Ageing time	Port

Total 0 Entry 20 entrys per page 1/1Page

The main element configuration description of static binding interface.

Interface Element	Description
MAC	Binding MAC address, for example: 0001-0001-0001.
Vlan ID	Binding VLAN ID information, for example: 1-4096.
IP address	Binding IP address, for example: 192.168.1.1.
Port	The corresponding port name of the device Ethernet port.

6.7.3 Port Configuration

Function Description

On the "Port Config" page, user can configure DHCP Snooping port information. DHCP Snooping trust function can provide users with further security, and ensure that DHCP Snooping trust function can control the source of DHCP server response messages, preventing existing spurious or forbidden DHCP server distributing IP address and other configuration information for other hosts.

DHCP Snooping trust function divides ports into trust port and distrustful port:

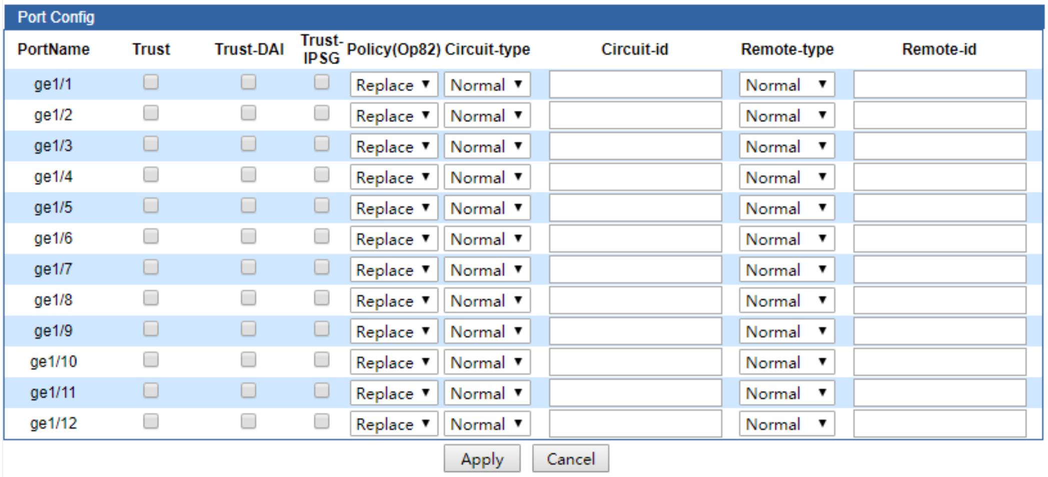
- Trust port is the port that is directly or indirectly connected to legitimate DHCP server. Trust port normally forwards received DHCP messages to ensure that DHCP client can gain correct IP address.
- Distrustful port is the port that isn't connected to legitimate DHCP server. DHCP-ACK, DHCP-NAK and DHCP-OFFER messages received from distrustful port in response to DHCP server are discarded, preventing DHCP client obtaining the wrong IP address.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Port Config".

Interface Description

Port configuration interface as follows:



PortName	Trust	Trust-DAI	Trust-IPSG	Policy(Op82)	Circuit-type	Circuit-id	Remote-type	Remote-id
ge1/1	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/2	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/3	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/4	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/5	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/6	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/7	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/8	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/9	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/10	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/11	□	□	□	Replace ▼	Normal ▼		Normal ▼	
ge1/12	□	□	□	Replace ▼	Normal ▼		Normal ▼	

The main element configuration description of port configuration interface.

Interface Element	Description

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Trust	Trust checkbox, trust port.
Trust-DAI	Trust-DAI checkbox, trust port ARP dynamic snooping.
Trust-IPSG	Trust-IPSG checkbox, trust port IP source address examination.
Policy (Op82)	Option 82 dealing strategy, options as follows: ● Replace: Keep Option 82 in messages unchanged and forward. ● Keep: Adopt different modes to fill Option 82, replace prime Option 82 in message and forward, filling modes will be described as below. ● Drop: Discard messages.
Circuit-type	Circuit ID sub-option filling type, options as follows: ● Normal: Normal mode; ● String: Detailed mode.
Circuit-id	Circuit ID sub-option filling content, support ASCII and HEX mode.
Remote-type	Remote ID sub-option filling type, options as follows: Normal: Normal mode; Sysname: Directly adopt device system name to fill Option 82; String: Detailed mode.
Remote-id	Remote ID sub-option filling content, support ASCII and HEX mode.

6.8 DNS Configuration

DNS, full name is Domain Name System, which is Domain Name Server. DNS helps user find path in the Internet. Each computer possesses the only address in Internet, which is called "IP address" (that is Internet Protocol Address). Because IP address (a string of numbers) isn't easy to remember, DNS allows users to adopt a string of common letters (that is "domain name") to replace.

DNS refers to: Domain Name Server. Domain name is corresponding to the IP address one by one in Internet, although the domain name is easy to remember, but two machines can only mutually recognize IP address, the converting work between them is called domain name analysis, domain analysis is completed by special domain name analysis server, DNS is the server conducting domain analysis.

Function Description

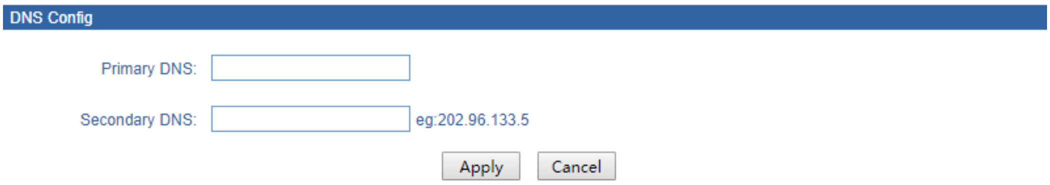
On the "DNS Config" page, user can configure primary DNS and secondary DNS.

Operation Path

Open in order: "Main Menu > Advanced Config > DNS Config".

Interface Description

DNS configuration interface as follows:



The main element configuration description of DNS configuration interface:

Interface Element	Description
Primary DNS	DNS server IP address, for example: 202.96.133.4.
Secondary DNS	DNS server secondary IP address, for example: 202.96.133.5.

6.9 NTP Configuration

The full name of NTP protocol is Network Time Protocol. Its destination is to transmit uniform and standard time in international Internet. Specific implementation scheme is appointing several clock source websites in the network to provide user with timing service, and these websites should be able to mutually compare to improve the accuracy. It can provide millisecond time correction, and adopt the encrypted way to prevent malicious protocol attacks.

Function Description

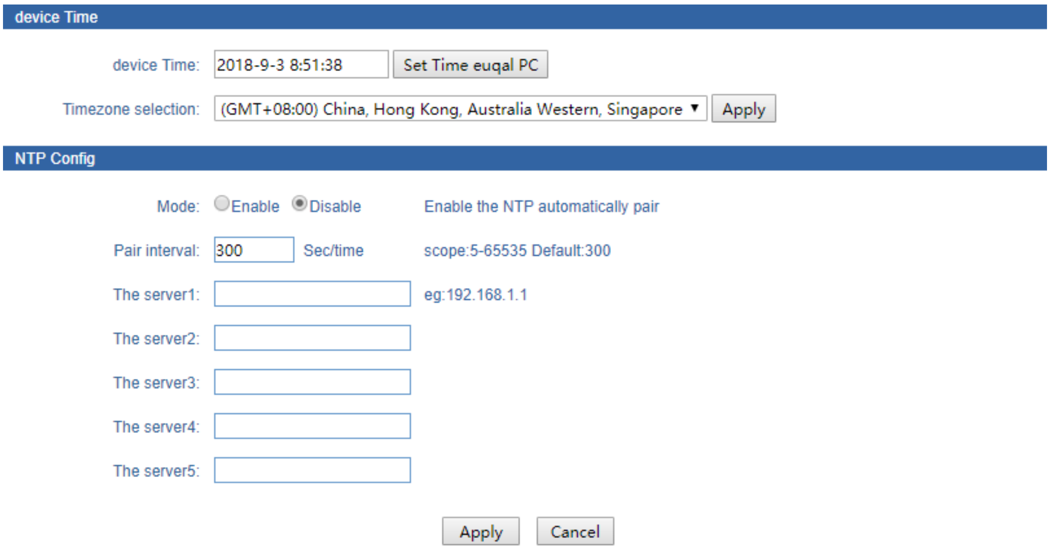
On the "NTP Config" page, user can configure the device time and NTP server information.

Operation Path

Open in order: "Main Menu > Advanced Config > NTP Config".

Interface Description

NTP configuration interface as follows:



device Time

device Time: 2018-9-3 8:51:38 [Set Time euqal PC]

Timezone selection: (GMT+08:00) China, Hong Kong, Australia Western, Singapore ▾ [Apply]

NTP Config

Mode: ○Enable ●Disable Enable the NTP automatically pair

Pair interval: 300 Sec/time scope:5-65535 Default:300

The server1: eg:192.168.1.1

The server2:

The server3:

The server4:

The server5:

[Apply] [Cancel]

The main element configuration description of NTP configuration interface.

Interface Element	Description
Device time	**The configuration bar of device time.**
device Time	The device own time, which can be synchronized to current computer time.
Timezone selection	Time standard of global different regions.
NTP Config	**Configuration bar of NTP server.**
Mode	NTP automatic pair function status, options as follows: ● Enable; ● Disable.
Pair interval	Pair time interval, value range is 5-65535, default value is 300.
The server1	IP address of pair server1, for example: 192.168.1.1.

Interface Element	Description
The server2	IP address of pair server2, for example: 192.168.1.1.
The server3	IP address of pair server3, for example: 192.168.1.1.
The server4	IP address of pair server4, for example: 192.168.1.1.
The server5	IP address of pair server5, for example: 192.168.1.1.

7 System Management

7.1 Management File

7.1.1 View Launch Configuration

Function Description

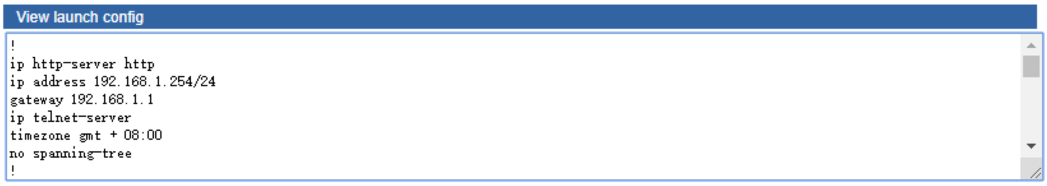
On the "View launch config" page, user can view current configuration information.

Operation Path

Open in order: "Main Menu > System management > Management File > View launch config".

Interface Description

View launch configuration interface as follows:



```
!
ip http-server http
ip address 192.168.1.254/24
gateway 192.168.1.1
ip telnet-server
timezone gmt + 08:00
no spanning-tree
!
```

7.1.2 Management File

Function Description

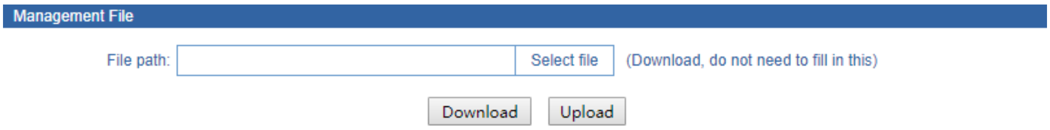
On the "Management File" page, user can download and upload configuration file.

Operation Path

Open in order: "Main Menu > System management > Management File > Management File".

Interface Description

Management file interface as follows:



The main element configuration description of management file interface.

Interface Element	Description
File path	Locally uploading configuration file path, click "Select File" to select required configuration file.
Download	Download the configuration file of current device, format: .conf.
Upload	Upload configuration file.

Note

- After finishing update, the device will automatically open a new page to "System State", and uploading configuration file will be valid after the device is reset.
- When uploading configuration files, the page would not be opened if the static IP and computer IP are not in the same network segment
- When uploading configuration files, the IP part would not be updated if using dynamic IP in configuration files while there is no DHCP server in network segment.
- Please don’t click or configure other WEB pages of the switch, nor reboot the switch during configuration file uploading or software upgrading. Otherwise it would lead to configuration file upload or software update failure, or even system breakdown.

7.2 Save

Function Description

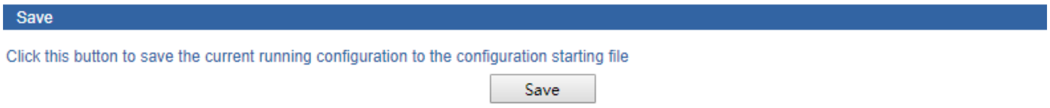
On the "Save" page, user can save the configuration file of current device.

Operation Path

Open in order: "Main Menu > System management > Save".

Interface Description

Save configuration interface as follows:



Click this button to save the current running configuration to the configuration starting file

The main element configuration description of save configuration interface.

Interface Element	Description
Save	Save current configuration file.

7.3 Reboot

Function Description

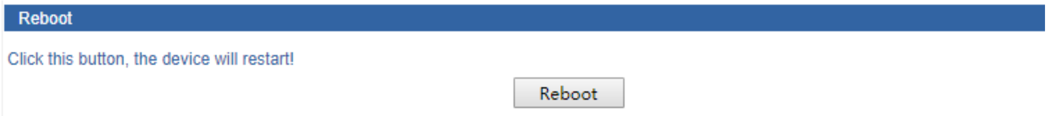
On the "Reboot" page, user can reset the device.

Operation Path

Open in order: "Main Menu > System management > Reboot".

Interface Description

Reboot interface as follows:



Click this button, the device will restart!

The main element configuration description of reboot interface.

Interface Element	Description
Reboot	Click the button to reset the device.

7.4 Restore Default Setting

Function Description

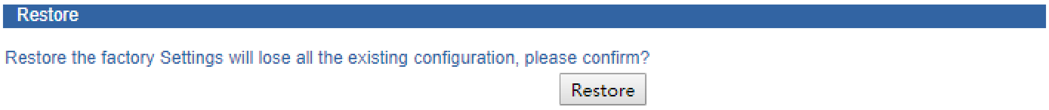
On the "Restore" page, user can restore the device to default setting.

Operation Path

Open in order: "Main Menu > System management > Restore".

Interface Description

Restore interface as follows:



Restore

Restore the factory Settings will lose all the existing configuration, please confirm?

The main element configuration description of restore interface.

Interface Element	Description
Restore	Click the button, the device will lose all existing configuration and restore to default setting.

Note

Clicking “Restore” will restore all configuration back to factory settings. IP address would be a static IP address “192.168.1.254”, user name and password would be “admin” by default.

7.5 Online Upgrade

Function Description

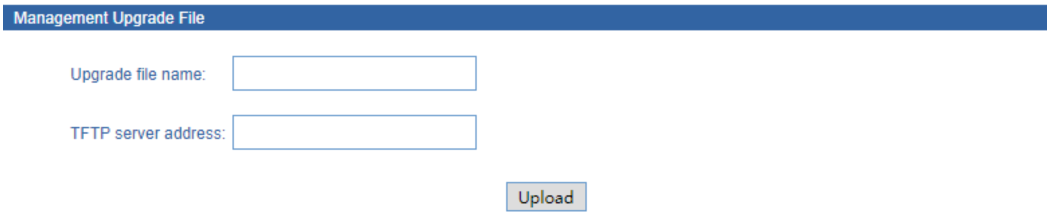
On the "Online Upgrade" page, user can update and upgrade the device procedure via TFTP server.

Operation Path

Open in order: "Main Menu > System management > Online Upgrade".

Interface Description

Online upgrade interface as follows:



Management Upgrade File

Upgrade file name:

TFTP server address:

The main element configuration description of online upgrade interface.

Interface Element	Description
Upgrade file name	Name with file format of upgrade file stored in TFTP server.
TFTP server address	TFTP server IP addresses that upgrade file stores.

Step 1 Online upgrade: put upgrade file into TFTP server;

Note:

If there is no TFTP server, user could create a server on PC by using TFTP tool.

Step 2 On the textbox of “upgrade file name”, enter the name of upgrade file and add file format “bin”.

Step 3 Enter the IP address of TFTP server in the textbox of “TFTP server address”;

Step 4 Click "Upload" button;

Step 5 End.

Note

- Please don’t click or configure other WEB pages of the switch, nor reboot the switch and turn off power supply during software upgrading. Otherwise it would lead to software update failure, or even system breakdown.
- Please ensure stable wired connection during upgrading.
- Device will reboot after finishing online upgrading.

7.6 HTTP Upgrade

Function Description

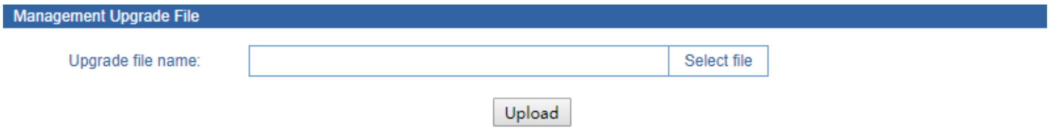
On the "HTTP Upgrade" page, user can update and upgrade the device procedure via local browser.

Operation Path

Open in order: "Main Menu > System management > HTTP Upgrade".

Interface Description

HTTP upgrade interface as follows:



The main element configuration description of HTTP upgrade interface:

Interface Element	Description
Upgrade file name	By clicking “select file” button, user could choose update file stored in local host. Then click “upload” button to start upgrading firmware.

⚠ Warning

- Please don’t click or configure other WEB pages of the switch, nor reboot the switch during configuration file uploading or software upgrading. Otherwise it would lead to configuration file upload or software update failure, or even system breakdown.

The Second Part: Frequently Asked Questions

8 FAQ

8.1 Sign in Problems

1. **Why the webpage display abnormally when browsing the configuration via WEB?**

   Before access the WEB, please eliminate IE cache buffer and cookies. Otherwise, the webpage will display abnormally.

2. **How about forget the login password?**

   For forgetting the login password, the password can be initialized by restoring factory setting, specific method is adopt BlueEyes_Ⅱ software to search and use restore factory setting function to initialize the password. Both of the initial user name and password are "admin".

3. **Is configuring via WEB browser same to configuring via BlueEyes_Ⅱ software?**

   Both configurations are the same, without conflict.

8.2 Configuration Problem

1. **Why the bandwidth can't be increased after configure Trunking (port aggregation) function?**

   Check whether the port attributes set to Trunking are consistent, such as rate, duplex mode, VLAN and other attributes.

2. **How to deal with the problem that part of switch ports are impassable?**

   When some ports on the switch are impassable, it may be network cable, network adapter and switch port faults. User can locate the faults via following tests:

   - Connected computer and switch ports keep invariant, change other network cable;
   - Connected network cable and switch port keep invariant, change other computers;
   - Connected network cable and computer keep invariant, change other switch port;
   - If the switch port faults are confirmed, please contact supplier for maintenance.

3. **How about the order of port self-adaption state detection?**

   The port self-adaption state detection is conducted according to following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half-duplex, 10Mbps full duplex, 10Mbps half-duplex, detect in order from high to low, connect automatically in supported highest speed.

8.3 Indicator Problem

1. **Power indicator isn't bright, what's the reason?**

   Possible reasons include:

   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Power supply or indicators faults; troubleshooting, change the power supply or device test.

- Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Link/Act indicator isn't bright, what's the reason?**

Possible reasons include:

- The network cable portion of Ethernet copper port is disconnected or bad contact; troubleshooting, connect the network cable again.
- Ethernet terminal device or network card works abnormally; troubleshooting, eliminate the terminal device fault.
- Not connected to the power socket; troubleshooting, connected to the power socket.
- Interface rate doesn't match the pattern; troubleshooting, examine whether the device transmission speed matches the duplex mode.

3. **The switch halts after communicate for a period time, and returns to normal after reboot, what's the reason?**

Reasons may include:

- Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
- Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
- Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
- High and low temperature influence; troubleshooting, check the device temperature usage range.

Make network communication more reliable

3onedata Co., Ltd.

Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen

Technology support: tech-support@3onedata.com

Service hotline: +86-400-880-4496

Official Website: http://www.3onedata.com