AVCOMM Technologies Inc.

7024GX12 User Manual

Table of Contents

Chapter 1　Basic Configuration

1.1　HTTP protocol configuration

Switches support not only being configured by CLI and SNMP protocol; it also supports being configured by web. HTTP service port configuration and time configuration of abnormal message overtime and etc are also supported.

1.1.1　Language Selection

In currently, there are supporting two languages in the Industrial Switch：　you may choice English or Chinese。User can setting the language in the global configuration mode　through the command line as shown as below：

Enter the command as shown as below in global configuration mode and then system language changed.

Command	Description
[no] ip http language { english}	Setting the Web language to English。The Web interface will turn into the English version.

1.1.2　HTTP service port configuration

Generally, the HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support users to change the service port and after the service port is changed you have to use the IP address and the changed port to access switches. For example, if you set the IP address and the service port to **192.168.2.1** and **1234** respectively, the HTTP access address should be changed to **http:// 192.168.2.1:1234**. You'd better not use other common protocols' ports so that access collision should not happen. For example, **ftp-20，telnet-23，dns-53，snmp-161**. Because the ports used by a lot of protocols are hard to remember, you'd better use port IDs following port 1024.

Command	Purpose
ip http port { *portNumber* }	Configuring HTTP service port

1.1.3　Enabling the HTTP service

Switches support to control the HTTP access. Only when the HTTP service is enabled can HTTP exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops. Configure global mode by the following command:

Command	Purpose
ip http server	Enabling HTTP service

1.1.4 HTTP access mode Configuration

You can access a switch through two access modes: HTTP access and HTTPS access, and you can use the following command to set the access mode to **HTTP**.

Command	Purpose
ip http http-access enable	Configuring HTTP access mode

1.1.5 Setting the Max-VLAN numbers to display in Web page

Setting a value between 1 and 4094 in the global configuration mode (4094 which is the max value，default max-vlan value is 100)

Command	Description
ip http web max-vlan { *max-vlan* }	Setting the Max-VLAN numbers to display in Web page

1.1.6 Setting the IGMP-Groups number to display in Web page

Setting a value between 1 and 100 in the global configuration mode。(100 which is the max value，default value is 15)

Command	Description
ip http web igmp-groups { *igmp-groups* }	Setting the IGMP-Groups number to display in Web page

1.2 HTTPS Configuration

In order to improve the security of communications, switches support not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

1.2.1 HTTPS Access Configuration

You can run the following command to set the access mode to **HTTPS** at global configuration mode.

Command	Description

ip http ssl-access enable	Enable the HTTPS access mod

1.2.2 HTTPS Service Port Configuration

As same as the HTTP service port， there is also the 443 port in HTTPS. User can change the port number through command line in global configuration mode. Suggesting the port number is bigger than 1024.

Command	Description
ip http secure-port {*portNumber*}	Setting the HTTPS port number

Chapter 2 Accessing Switch

2.1 Accessing the Switch Through Web

When accessing the switch through Web, please make sure that the applied browser complies with the following requirements:

- HTML of version 4.0
- HTTP of version 1.1
- JavaScript™ of version 1.5

What's more, please ensure that the main program file, running on a switch, supports Web access and your computer has already connected the network in which the switch is located.

2.2 Initially Accessing the Switch

When the switch is initially used, you can use the Web access without any extra settings:

1. Modify the IP address of the network adapter and subnet mask of your computer to **192.168.2.2** and **255.255.255.0** respectively.
2. Open the Web browser and enter **192.168.2.1** in the address bar. It is noted that **192.168.2.1** is the default management address of the switch.
3. If the IE browser is used, please enter the username and the password in the ID authentication dialog box. Both the original username and the password are “admin”, which is capital sensitive.
4. After successful authentication, the systematic information about the switch will appear on the IE browser.

2.2.1 Upgrading to the Web-Supported Version

If your switch is upgraded to the Web-supported version during its operation and the switch has already stored its configuration files, the Web visit cannot be directly applied on the switch. Perform the following steps one by one to enable the Web visit on the switch:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to “Switch_config#”.
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
4. Enter the **ip http server** command in global configuration mode and start the Web service.
5. Run **username** to set the username and password of the switch. For how to use this command, refer to the “Security Configuration” section in the user manual.

After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.

6. Enter **write** to save the current configuration to the configuration file.

2.3 Accessing Switch Through Secure Links

The data between the WEB browser and the switch will not be encrypted if you access switch through common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to access the switch.

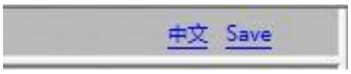
To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to “Switch_config#”.
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
4. Enter the **ip http server** command at global configuration mode and start the Web service.
5. Run **username** to set the username and password of the switch. For how to use this command, please refer to the “Security Configuration” section in the user manual.
6. Run **ip http ssl-access enable** to enable the secure link access of the switch.
7. Run **no ip http http-access enable** to forbid to access the switch through insecure links.
8. Enter **write** to store the current configuration to the configuration file.
9. Open the WEB browser on the PC that the switch connects, enter **https://192.168.2.1** on the address bar (**192.168.2.1** stands for the management IP address of the switch) and then press the **Enter** key. Then the switch can be accessed through the secure links.

2.4 Introduction of Web Interface

The Web homepage appears after login, the whole homepage consists of the **top control bar**, the **navigation bar**, the **configuration display area** and the **bottom control bar**.

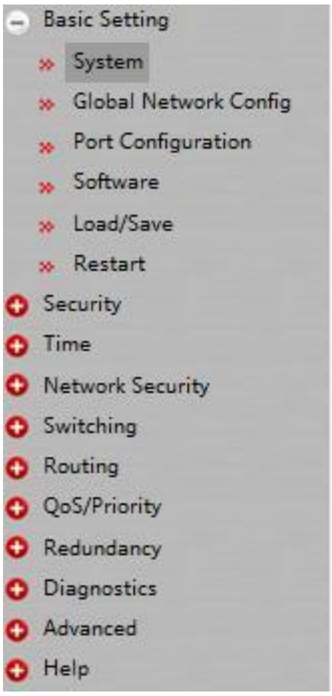
2.4.1 Top Control Bar



Save	Write the current settings to the configuration file of the device. It is

	equivalent to the execution of the **write** command. The configuration that is made through Web will not be promptly written to the configuration file after validation. If you click “Save”, the unsaved configuration will be lost after rebooting.
English	The interface will turn into the English version.
Chinese	The interface will turn into the Chinese version.

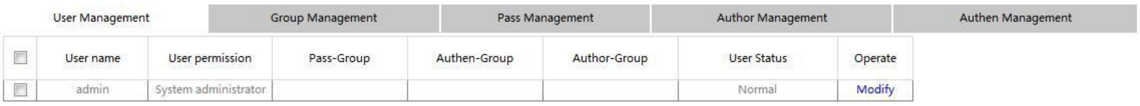
2.4.2 Navigation Bar



The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at “system”. If a certain item need be configured, please click the group name and then the sub-item. For example, to browse the flux of the current port, you have to click “Interface State" and then “Interface Flow”.

Note:
The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web with limited user’s permissions, only “Interface State” will appear.

2.4.3 Configuration Display Area



□	User name	User permission	Pass-Group	Authen-Group	Author-Group	User Status	Operate
□	admin	System administrator				Normal	Modify

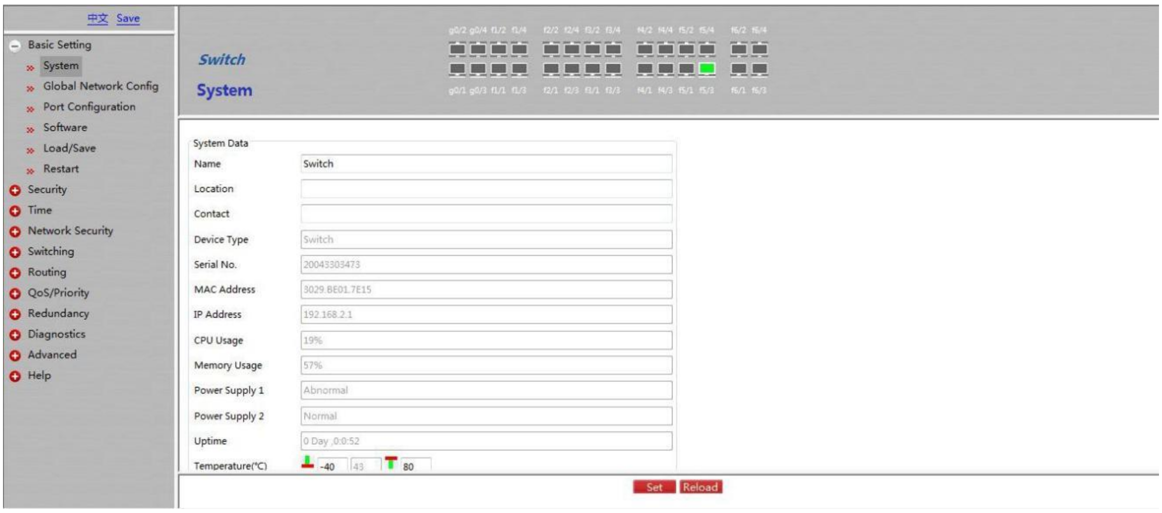
The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

2.4.4 Bottom Control Bar

The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to the device. The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click “Save All” on the top control bar.
Reset	Mean discarding the modification of the sheet. The content of the sheet will be reset.
New	Create a list item. For example, you can create a VLAN item or a new user.
Delete	Delete an item in the list.
Back	Go back to the previous-level configuration page.

Chapter 3 Basic Configuration

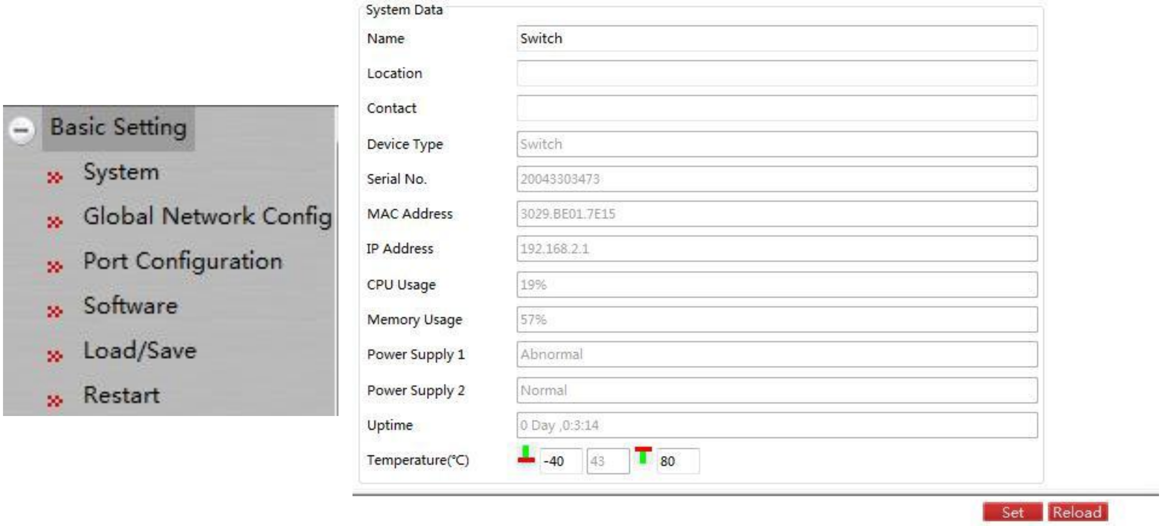


System Data

Name	Switch
Location	
Contact	
Device Type	Switch
Serial No.	20043303473
MAC Address	3029.BE01.7E15
IP Address	192.168.2.1
CPU Usage	19%
Memory Usage	57%
Power Supply 1	Abnormal
Power Supply 2	Normal
Uptime	0 Day ,0:0:52
Temperature(℃)	-40 43 80

3.1 System Information

If you click **Basic Config -> System Data** in the navigation bar, the page appears as shown as below：



System Data

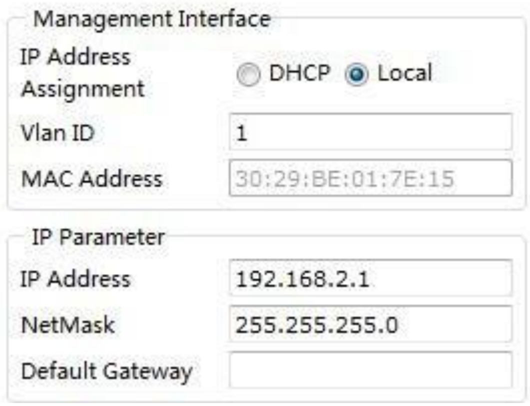
Name	Switch
Location	
Contact	
Device Type	Switch
Serial No.	20043303473
MAC Address	3029.BE01.7E15
IP Address	192.168.2.1
CPU Usage	19%
Memory Usage	57%
Power Supply 1	Abnormal
Power Supply 2	Normal
Uptime	0 Day ,0:3:14
Temperature(℃)	-40 43 80

The system message will be displayed in the dialog box.

The default name of the device is “Switch”. You can enter the new hostname in the text box and then click “Set”.

3.2 Global configuration mode (Management Interface)

If you click **Basic Config -> Management Interface** in the navigation bar, the page appears as shown as below：



Management Interface

IP Address Assignment ○ DHCP ● Local

Vlan ID: 1

MAC Address: 30:29:BE:01:7E:15

IP Parameter

IP Address: 192.168.2.1

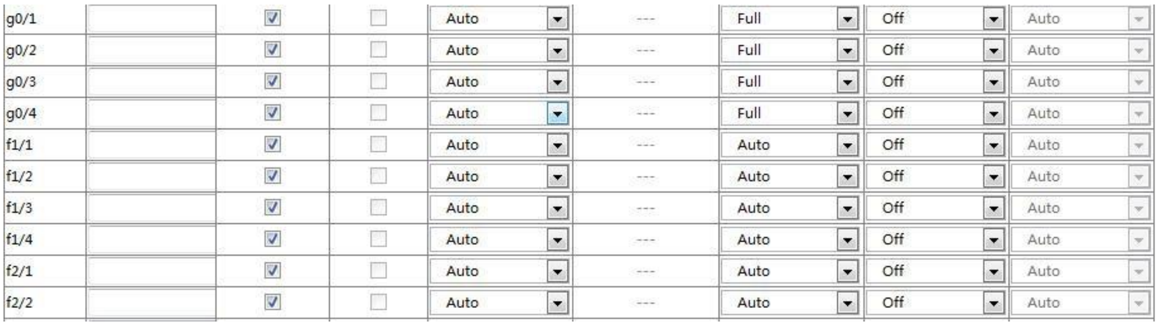
NetMask: 255.255.255.0

Default Gateway:

- Setting the IP address of Interface VLAN 1 , in order to access the switch
- This page is used to set the IP address of Interface Vlan 1 in the management interface of the device. In initial conditions, the MAC address of the device, the IP address, mask and gateway of the interface will appear on this page.

3.3 Port Configuration

If you click **Basic Config -> Port Config** in the navigation bar, the **Port Configuration** page appears, as shown as below figure



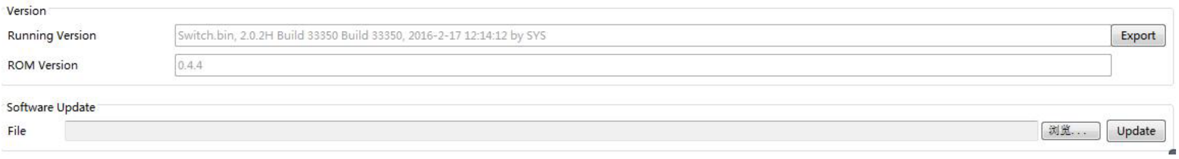
g0/1		☑	□	Auto	---	Full	Off	Auto
g0/2		☑	□	Auto	---	Full	Off	Auto
g0/3		☑	□	Auto	---	Full	Off	Auto
g0/4		☑	□	Auto	---	Full	Off	Auto
f1/1		☑	□	Auto	---	Auto	Off	Auto
f1/2		☑	□	Auto	---	Auto	Off	Auto
f1/3		☑	□	Auto	---	Auto	Off	Auto
f1/4		☑	□	Auto	---	Auto	Off	Auto
f2/1		☑	□	Auto	---	Auto	Off	Auto
f2/2		☑	□	Auto	---	Auto	Off	Auto

You can change the status, speed, duplex mode and flow control of a port on this page.

Note:
Port link switching might happen if modifying port’s speed or duplex mode. Network communication might be affected.

3.4 Software

If you click **Basic Config -> Software** in the navigation bar, the **Software management** page appears, as shown as below figure



Version

Running Version: Switch.bin, 2.0.2H Build 33350 Build 33350, 2016-2-17 12:14:12 by SYS

ROM Version: 0.4.4

Software Update

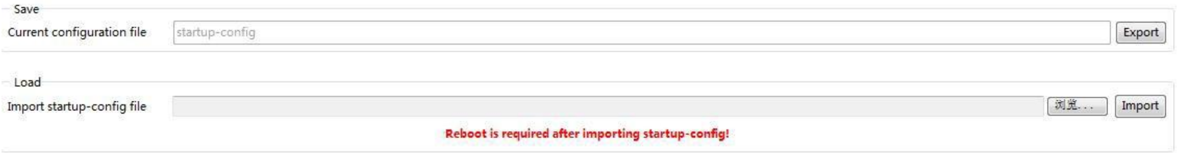
File

Current running version and rom version could be checked at this page. Click **Export** to export current running version to computer. Choose the to-be-updated software version and click **Update** to change system's software version on **Software Update** Column.

Note: The updated system's software would be valid only if the device is restarted.

3.5 Save/Load

If you click **Basic Config -> Save/Load** in the navigation bar, the page appears as shown as below figure：



Save

Current configuration file: startup-config

Load

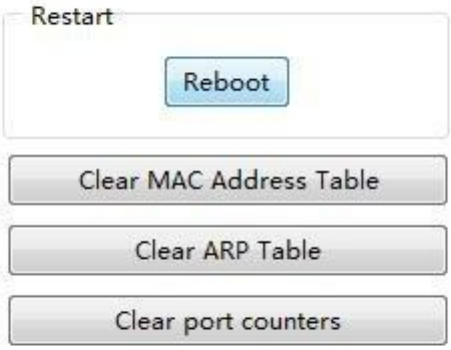
Import startup-config file

Reboot is required after importing startup-config!

Click the "Export" then the current configuration of system will be exported to computer， if you click the " Import" then related configuration document will be imported to switch.

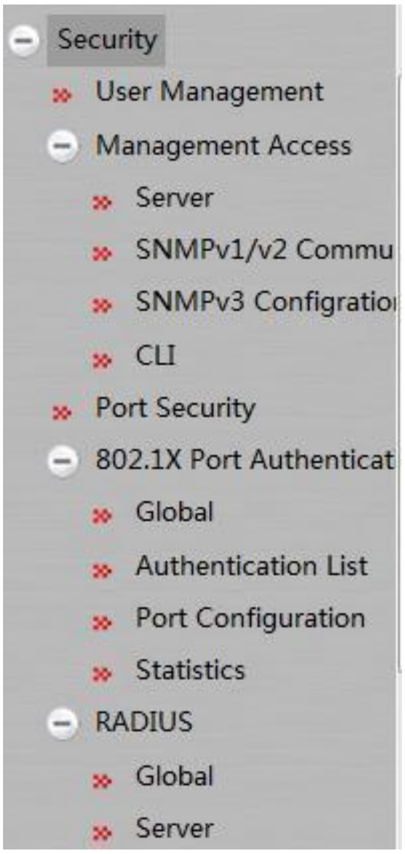
3.6 Restart

If you click **Basic Config -> Restart** in the navigation bar, the page appears as shown as below figure：



You can choice "Reboot" to reboot the switch， or choice "Clear MAC Address Table" 、"Clear ARP Table"、"Clear port counters" 。

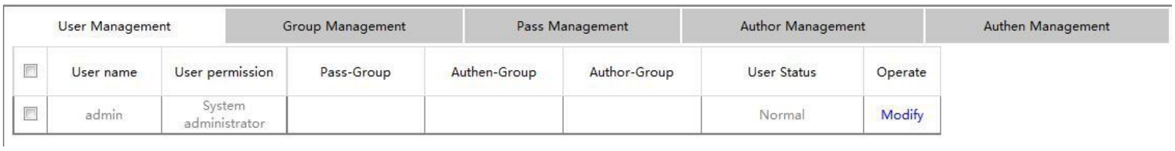
Chapter 4 Security



4.1 User Management

4.1.1 User Management

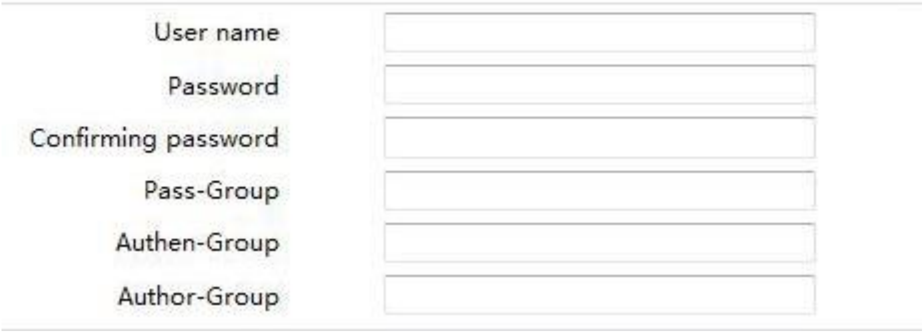
If you click **Security -> User Management** in the navigation bar, the page appears as shown as below figure：



□	User name	User permission	Pass-Group	Authen-Group	Author-Group	User Status	Operate
□	admin	System administrator				Normal	Modify

Click **Modify** to change user’s configuration at this page, and then click **Delete** at the bottom bar after selecting user to delete user.

Click **New** at the bottom bar to enter the following page:

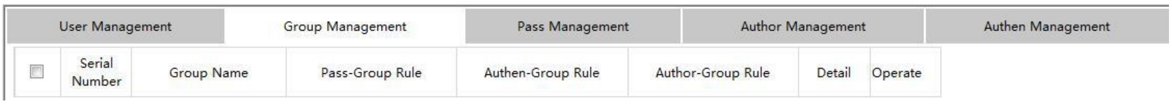


User name	
Password	
Confirming password	
Pass-Group	
Authen-Group	
Author-Group	

Fill in configuration at every configuration column and click **Setup** at the bottom bar to create new user.

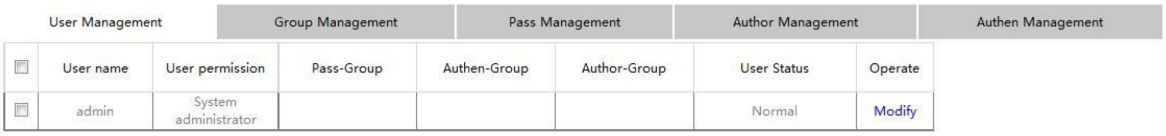
4.1.2 Group Management

Click **Security -> User Management** in order and then click **Group Management** to open configuration page as following:



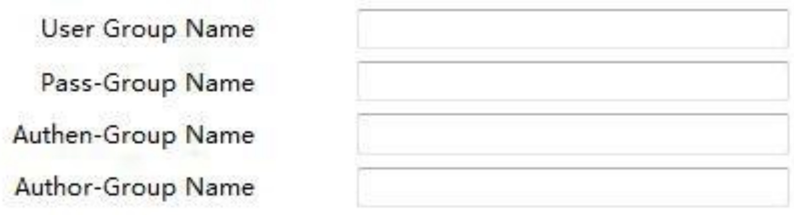
□	Serial Number	Group Name	Pass-Group Rule	Authen-Group Rule	Author-Group Rule	Detail	Operate

Click **Modify** to change user group's configuration at this page. Select user and click **Delete** at the bottom bar to delete user group. Click **Details** to check and configure members of group as following:



□	User name	User permission	Pass-Group	Authen-Group	Author-Group	User Status	Operate
□	admin	System administrator				Normal	Modify

Click **New** at the bottom bar of group management page to enter the following page:

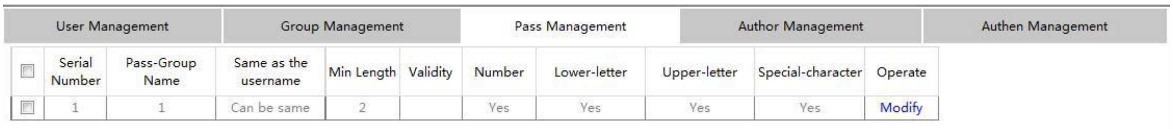


User Group Name	
Pass-Group Name	
Authen-Group Name	
Author-Group Name	

Fill in configuration at every configuration column and click **Setup** at the bottom bar to create new user group.

4.1.3 Password Rule Management

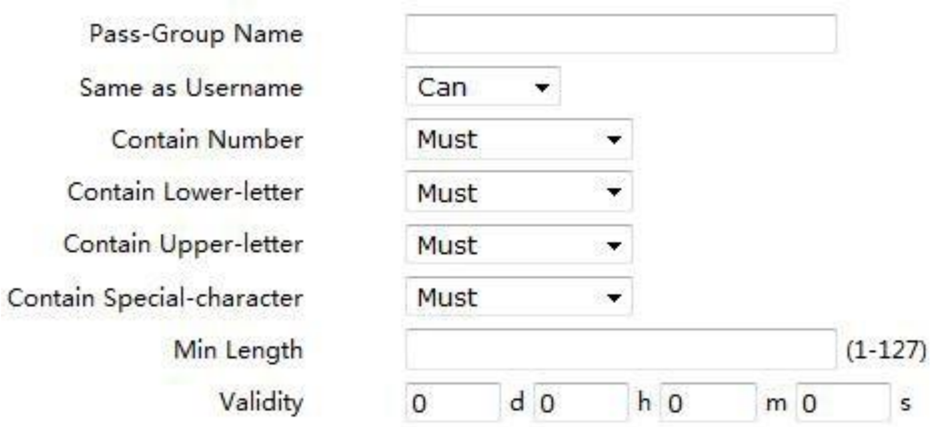
Click **Security -> User Management** in order and then click **Pass Management** to open configuration page as following:



□	Serial Number	Pass-Group Name	Same as the username	Min Length	Validity	Number	Lower-letter	Upper-letter	Special-character	Operate
□	1	1	Can be same	2		Yes	Yes	Yes	Yes	Modify

Click **Modify** to change password regulation at this page. Click **Delete** at the bottom bar to delete password regulation.

Click **New** at the bottom bar to enter the following page:

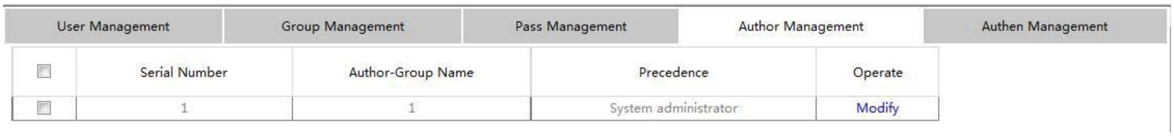


Pass-Group Name	
Same as Username	Can
Contain Number	Must
Contain Lower-letter	Must
Contain Upper-letter	Must
Contain Special-character	Must
Min Length	(1-127)
Validity	0 d 0 h 0 m 0 s

Fill in configuration at every configuration column and click **Setup** at the bottom bar to create new password regulation.

4.1.4 Author Rule Management

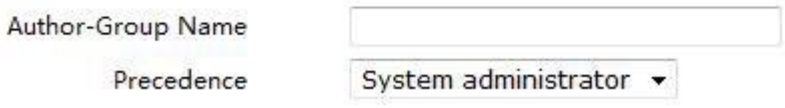
Click **Security -> User Management** in order and then click **Author Management** to open configuration page as following:



□	Serial Number	Author-Group Name	Precedence	Operate
□	1	1	System administrator	Modify

Click **Modify** to change author rules at this page. Click **Delete** at the bottom bar to delete author rules.

Click **New** at the bottom bar to enter the following page:

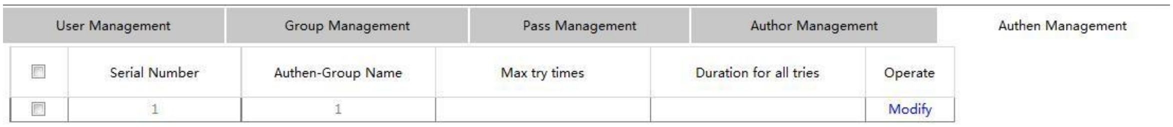


Author-Group Name	
Precedence	System administrator

Fill in configuration at every configuration column and click **Setup** at the bottom bar to create new author rules.

4.1.5 Authentication Rule Management

Click **Security -> User Management** in order and then click **Authen Management** to open configuration page as following:

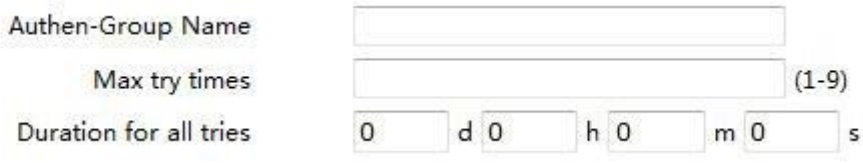


User Management | Group Management | Pass Management | Author Management | Authen Management

☐	Serial Number	Authen-Group Name	Max try times	Duration for all tries	Operate
☐	1	1			Modify

Click **Modify** to change authentication rules at this page. Click **Delete** at the bottom bar to delete authentication rules.

Click **New** at the bottom bar to enter the following page:



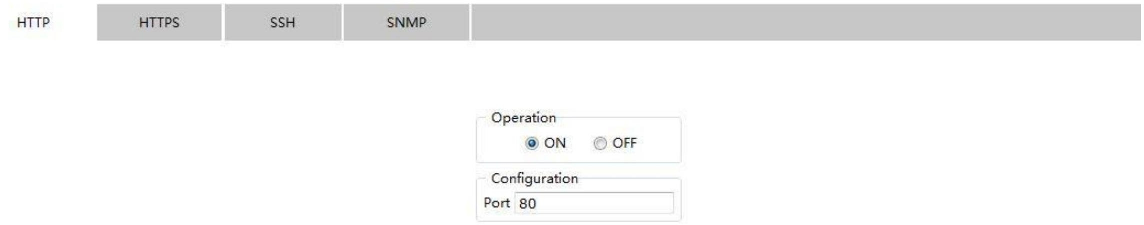
Authen-Group Name		
Max try times		(1-9)
Duration for all tries	0 d 0 h 0 m 0 s	

Fill in configuration at every configuration column and click **Setup** at the bottom bar to create new authentication rules。

4.2 Access Management

4.2.1 Service

HTTP, HTTPS, SSH and SNMP could be configured at this page. Click **Security -> Access Management -> Service** at navigation bar in order to enter service configuration page. Click **HTTP** at this page to enter HTTP configuration.

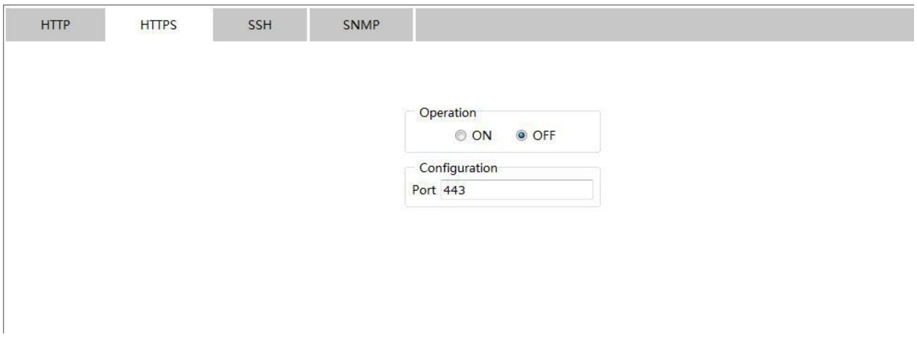


HTTP | HTTPS | SSH | SNMP

Operation
● ON ○ OFF

Configuration
Port 80

Click **HTTPS** to configure HTTPS related:

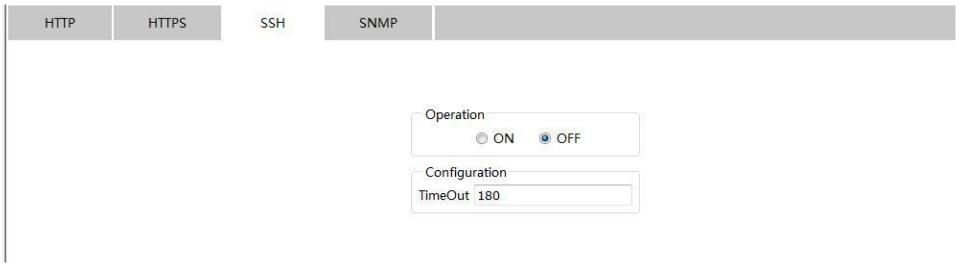


HTTP | HTTPS | SSH | SNMP

Operation
○ ON ● OFF

Configuration
Port 443

Click **SSH** to configure SSH related:



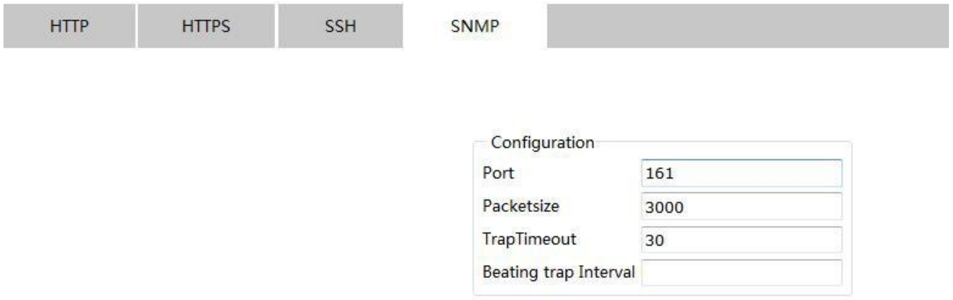
Operation

○ ON ● OFF

Configuration

TimeOut 180

Click **SNMP** to configure SNMP related:

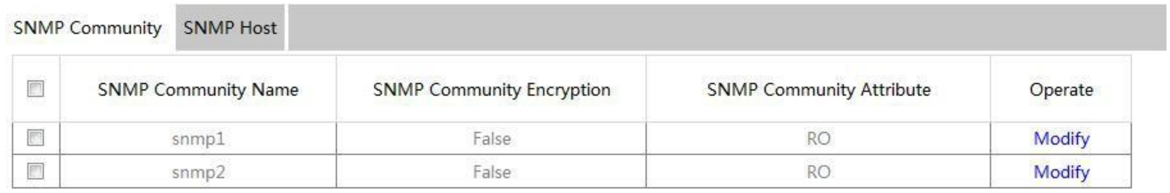


Configuration

Port	161
Packetsize	3000
TrapTimeout	30
Beating trap Interval	

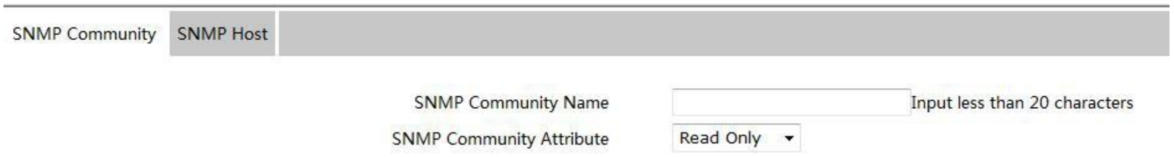
4.2.2 SNMP Community Management (SNMPv1/v2 community)

Click **Security -> Access Management -> SNMPv1/v2 Community** at navigation bar in order to enter configuration page as following:



□	SNMP Community Name	SNMP Community Encryption	SNMP Community Attribute	Operate
□	snmp1	False	RO	Modify
□	snmp2	False	RO	Modify

Click **New** to create new SNMP Community:



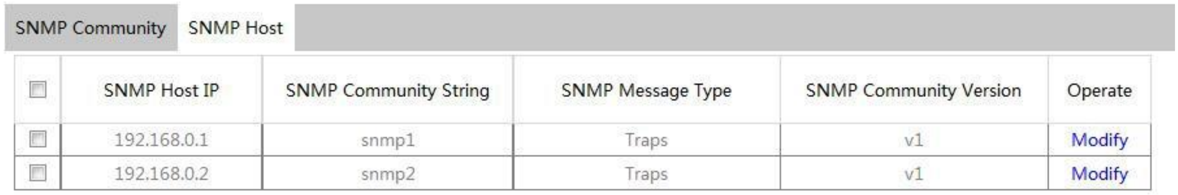
SNMP Community Name [ ] Input less than 20 characters

SNMP Community Attribute Read Only

Click **Modify** to change the feature of SNMP Community;

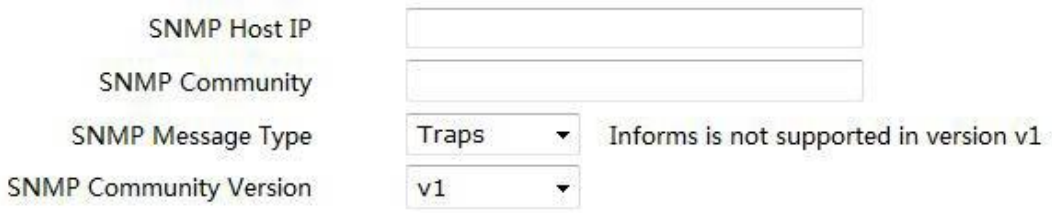
Click **Delete** to delete the selected SNMP Community;

Click **SNMP Host** to switch to the SNMP Host configuration page:



□	SNMP Host IP	SNMP Community String	SNMP Message Type	SNMP Community Version	Operate
□	192.168.0.1	snmp1	Traps	v1	Modify
□	192.168.0.2	snmp2	Traps	v1	Modify

Click **New** to create new SNMP Host:



SNMP Host IP

SNMP Community

SNMP Message Type: Traps — Informs is not supported in version v1

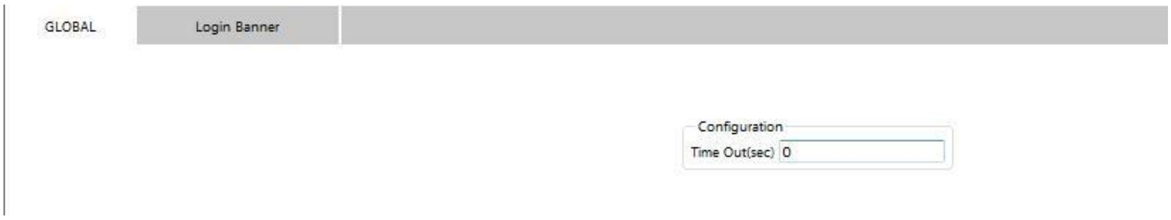
SNMP Community Version: v1

Click **Modify** to modify feature of SNMP Host;

Click **Delete** to delete the selected SNMP Host.

4.2.3 CLI (Command Line Interface)

Click **Security -> Access Management -> CLI** at navigation bar in order to enter configuration page as following:

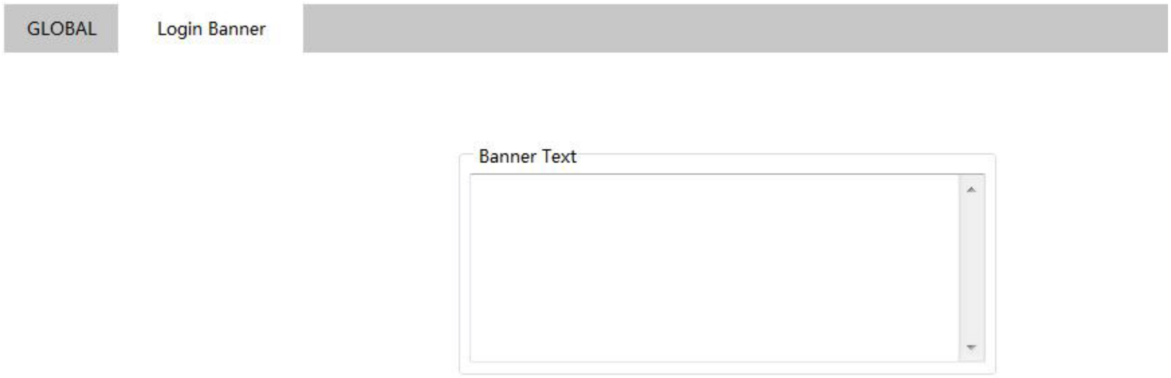


Configuration

Time Out(sec): 0

Terminal's overtime time could be configured at this page, and if configured as 0, it means there would be never overtime.

Click **Login Banner** to enter the following page:

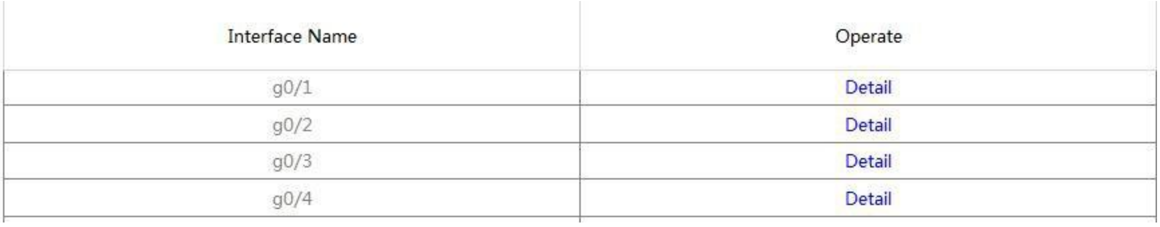


Terminal's Login Banner could be configured at this page.

4.3 Interface Security

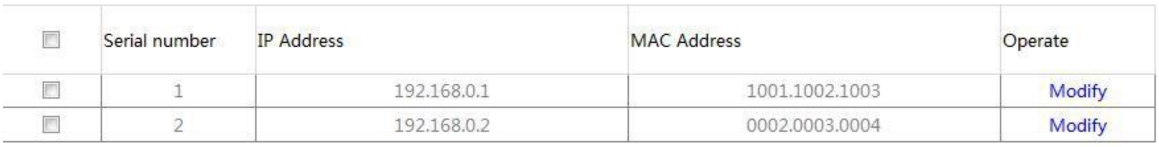
4.3.1 IP MAC Interface Binding Configuration

Click **Security -> Interface Security** at navigation bar in order, and then click **IP MAC Interface Binding Configuration** to enter configuration page as following:



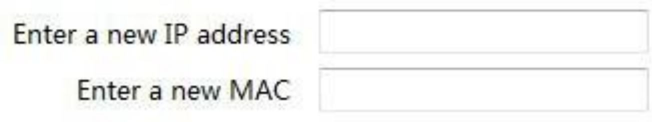
Interface Name	Operate
g0/1	Detail
g0/2	Detail
g0/3	Detail
g0/4	Detail

Click Detail to check this interface's IP MAC binding information.



□	Serial number	IP Address	MAC Address	Operate
□	1	192.168.0.1	1001.1002.1003	Modify
□	2	192.168.0.2	0002.0003.0004	Modify

Click **New** to create new IP MAC binding item.



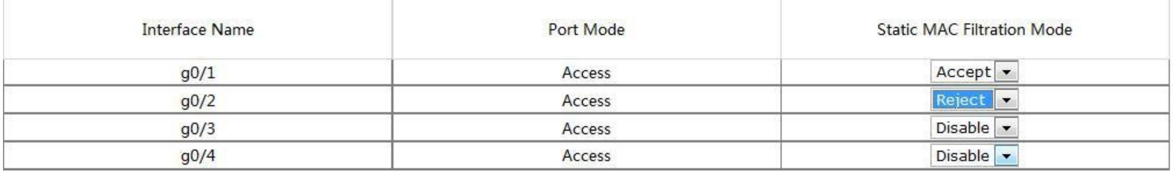
Enter a new IP address	
Enter a new MAC	

Click **Modify** to modify IP MAC binding item;

Click **Delete** to delete the selected IP MAC binding item.

4.3.2 Static MAC Filtration Mode Configuration

Click **Security -> Interface Security** at navigation bar in order, and then click **Static MAC Filtration Mode Configuration** to enter configuration page as following:

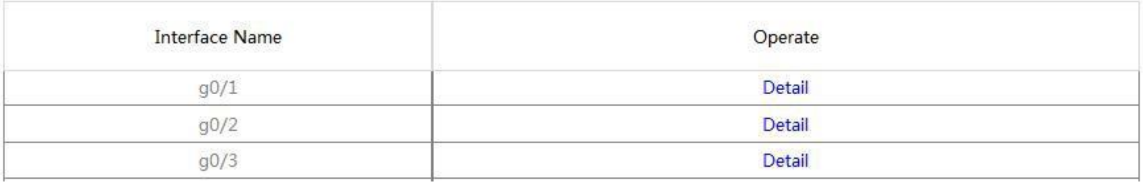


Interface Name	Port Mode	Static MAC Filtration Mode
g0/1	Access	Accept ▾
g0/2	Access	Reject ▾
g0/3	Access	Disable ▾
g0/4	Access	Disable ▾

Interface's Static MAC Filtration Mode could be configured at this page.

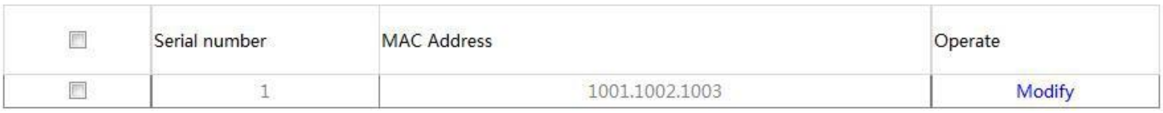
4.3.3 Static MAC Filtration Configuration

Click **Security -> Interface Security** at navigation bar in order, and then click **Static MAC Filtration Configuration** to enter configuration page as following:



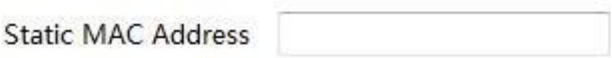
Interface Name	Operate
g0/1	Detail
g0/2	Detail
g0/3	Detail

Click **Detail** to check the interface's static MAC filtration items.



□	Serial number	MAC Address	Operate
□	1	1001.1002.1003	Modify

Click **New** to create new static MAC filtration items.



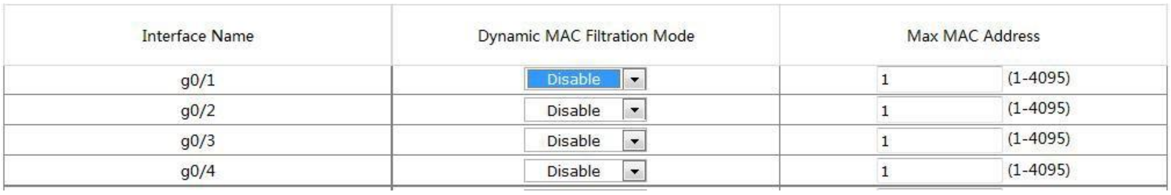
Static MAC Address

Click **Modify** to modify static MAC filtration items;

Click **Delete** to delete the selected static MAC filtration items.

4.3.4 Dynamic MAC Filtration Mode Configuration

Click **Security -> Interface Security** at navigation bar in order, and then click **Dynamic MAC Filtration Mode Configuration** to enter configuration page as following:



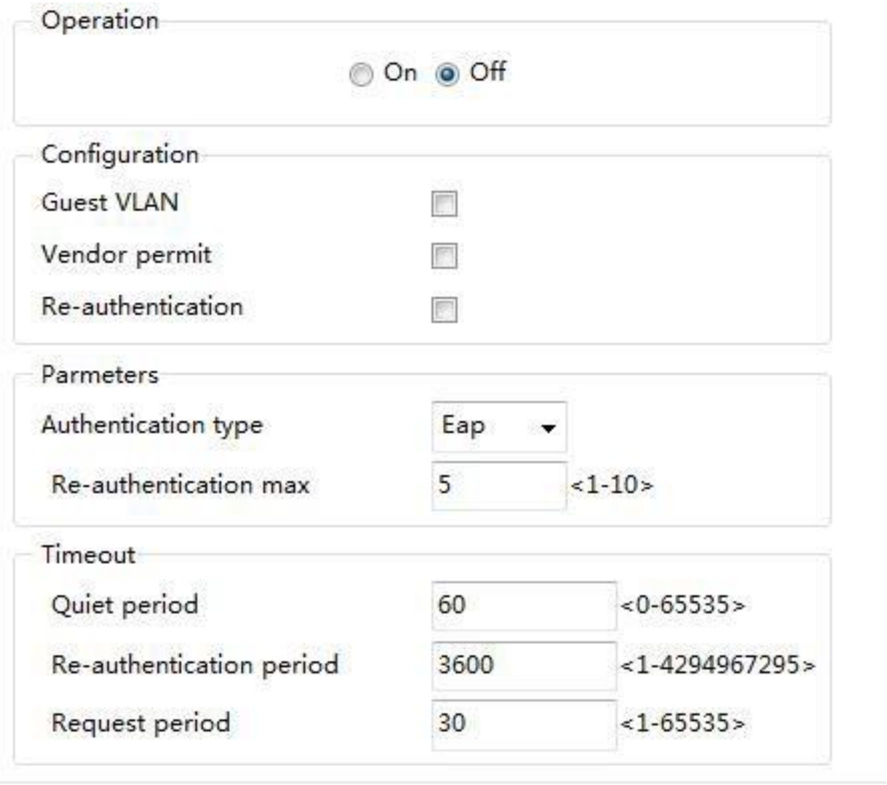
Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
g0/1	Disable ▾	1 (1-4095)
g0/2	Disable ▾	1 (1-4095)
g0/3	Disable ▾	1 (1-4095)
g0/4	Disable ▾	1 (1-4095)

Interface's Dynamic MAC Filtration Mode could be configured at this page.

4.4 802.1X Interface Authentication

4.4.1 Global

Click **Security -> 802.1X Interface Authentication -> Global** at navigation bar in order to enter configuration page as following:



Operation

○ On ● Off

Configuration

Guest VLAN □

Vendor permit □

Re-authentication □

Parmeters

Authentication type: Eap

Re-authentication max: 5 <1-10>

Timeout

Quiet period: 60 <0-65535>

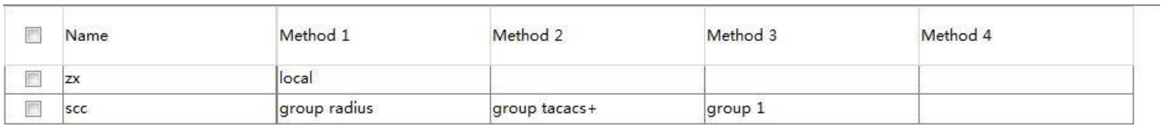
Re-authentication period: 3600 <1-4294967295>

Request period: 30 <1-65535>

Configure the enabling/disabling operations of 802.1X interface authentication at this page.

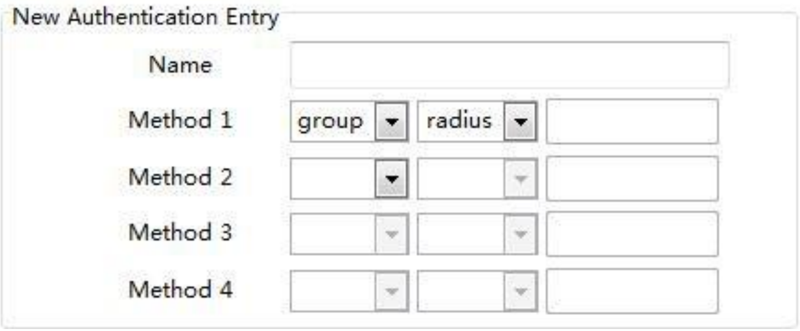
4.4.2 Authentication List

Click **Security -> 802.1X Interface Authentication -> Authentication List** at navigation bar in order to enter configuration page as following:



□	Name	Method 1	Method 2	Method 3	Method 4
□	zx	local			
□	scc	group radius	group tacacs+	group 1	

Click **New** to create new authentication entry:

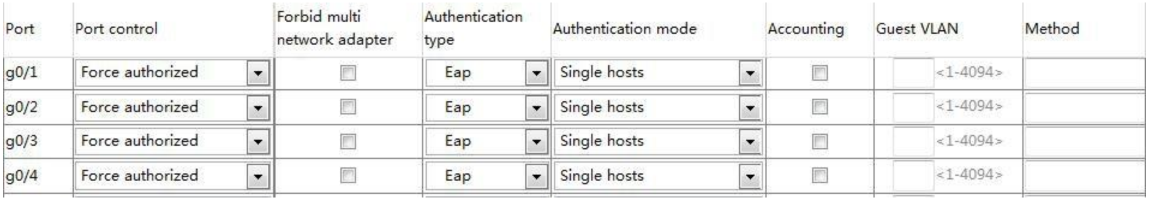


New Authentication Entry

Name			
Method 1	group	radius	
Method 2			
Method 3			
Method 4			

4.4.3 Interface Configuration

Click **Security -> 802.1X Interface Authentication -> Interface Configuration** at navigation bar in order to enter configuration page as following:



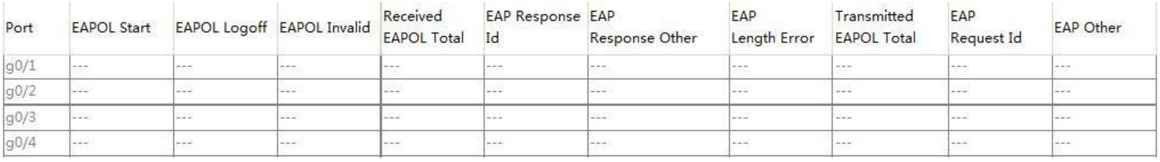
Port	Port control	Forbid multi network adapter	Authentication type	Authentication mode	Accounting	Guest VLAN	Method
g0/1	Force authorized	□	Eap	Single hosts	□	<1-4094>	
g0/2	Force authorized	□	Eap	Single hosts	□	<1-4094>	
g0/3	Force authorized	□	Eap	Single hosts	□	<1-4094>	
g0/4	Force authorized	□	Eap	Single hosts	□	<1-4094>	

You could configure interface’s enabling/disabling 802.1x interface authentication, authentication type, authentication mode, method and etc at this page.

Note:
Some configurations can only be configured when 802.1x interface authentication is enabled.

4.4.4 Statistics

Click **Security -> 802.1X Interface Authentication -> Statistics** at navigation bar in order to enter configuration page as following:



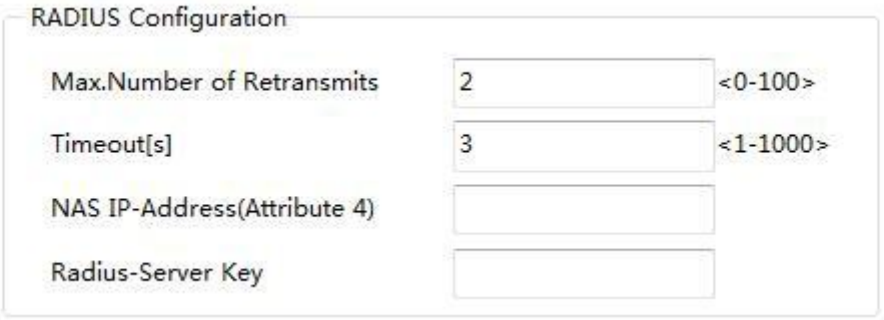
Port	EAPOL Start	EAPOL Logoff	EAPOL Invalid	Received EAPOL Total	EAP Response Id	EAP Response Other	EAP Length Error	Transmitted EAPOL Total	EAP Request Id	EAP Other
g0/1	---	---	---	---	---	---	---	---	---	---
g0/2	---	---	---	---	---	---	---	---	---	---
g0/3	---	---	---	---	---	---	---	---	---	---
g0/4	---	---	---	---	---	---	---	---	---	---

All interfaces’ statistic information of 802.1x messages could be checked at this page.

4.5 RADIUS

4.5.1 Global

Click **Security -> RADIUS -> Global** at navigation bar in order to enter configuration page as following:



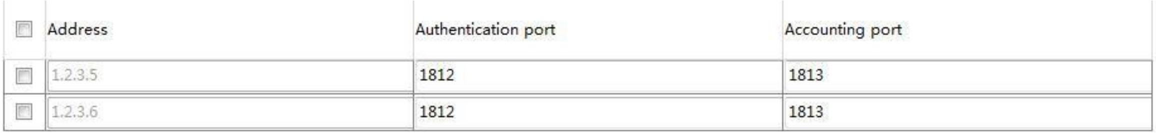
RADIUS Configuration

Max.Number of Retransmits	2	<0-100>
Timeout[s]	3	<1-1000>
NAS IP-Address(Attribute 4)		
Radius-Server Key		

Max. Number of retransmits of radius, overtime, NAS and Radius-Server Key could be configured at this page.

4.5.2 Service

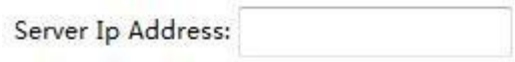
Click **Security -> RADIUS -> Service** at navigation bar in order to enter configuration page as following:



□	Address	Authentication port	Accounting port
□	1.2.3.5	1812	1813
□	1.2.3.6	1812	1813

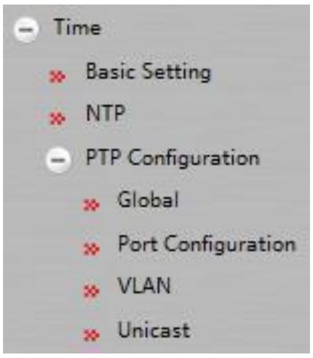
Radius server's authentication port and accounting port can be configured at this page;

Click **New** to create new radius server items:



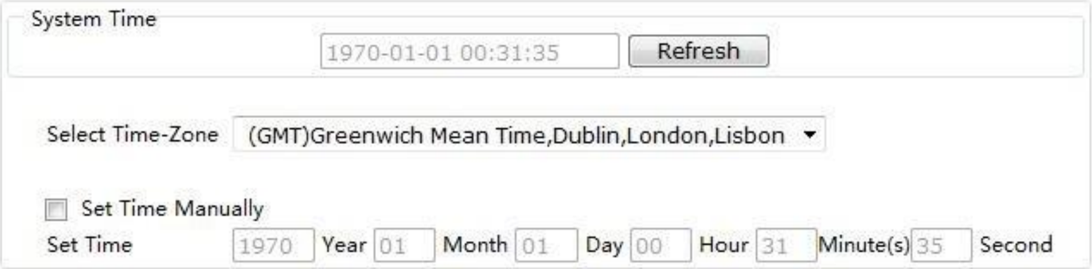
Server Ip Address:

Chapter 5 Time



5.1 Basic Configuration

Click **Time -> Basic Configuration** at navigation bar in order to enter configuration page as following:



System Time

1970-01-01 00:31:35 Refresh

Select Time-Zone: (GMT)Greenwich Mean Time,Dublin,London,Lisbon ▾

□ Set Time Manually

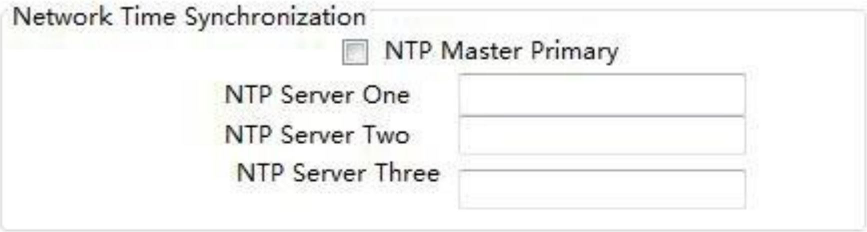
Set Time 1970 Year 01 Month 01 Day 00 Hour 31 Minute(s) 35 Second

Click **Refresh** to refresh the current displayed system time.

System's time-zone could be configured at this page. Select **Set Time Manually** to set system time manually.

5.2 NTP

Click **Time -> NTP** at navigation bar in order to enter configuration page as following:



Network Time Synchronization

□ NTP Master Primary

NTP Server One

NTP Server Two

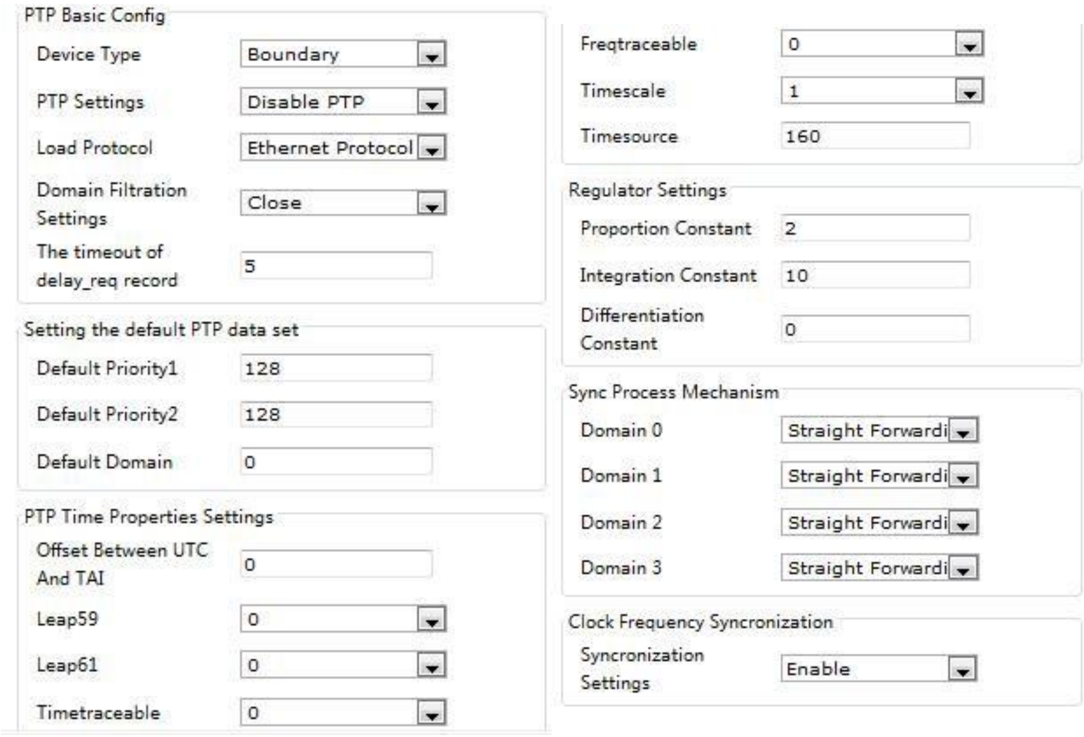
NTP Server Three

NTP server's IP address of NTP (Network Time Synchronization) could be configured at this page.

5.3 PTP Configuration

5.3.1 Global

Click **Time -> PTP -> Global** at navigation bar in order to enter configuration page as following:



PTP Basic Config

Device Type: Boundary

PTP Settings: Disable PTP

Load Protocol: Ethernet Protocol

Domain Filtration Settings: Close

The timeout of delay_req record: 5

Setting the default PTP data set

Default Priority1: 128

Default Priority2: 128

Default Domain: 0

PTP Time Properties Settings

Offset Between UTC And TAI: 0

Leap59: 0

Leap61: 0

Timetraceable: 0

Freqtraceable: 0

Timescale: 1

Timesource: 160

Regulator Settings

Proportion Constant: 2

Integration Constant: 10

Differentiation Constant: 0

Sync Process Mechanism

Domain 0: Straight Forwardi

Domain 1: Straight Forwardi

Domain 2: Straight Forwardi

Domain 3: Straight Forwardi

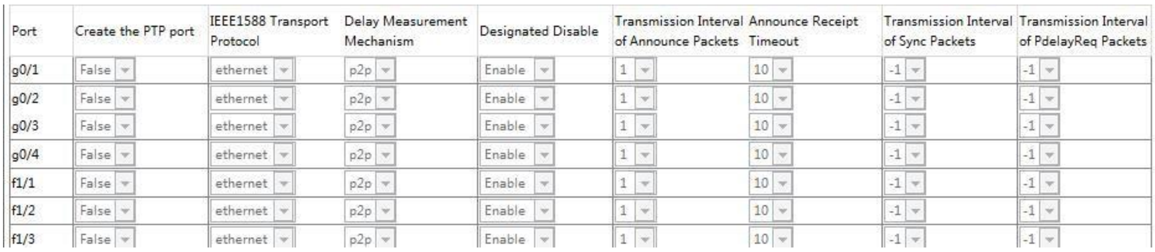
Clock Frequency Syncronization

Syncronization Settings: Enable

Enabling/disabling PTP and timeout parameter can be configured at this page.

5.3.2 Port Configuration

Click **Time -> PTP -> Port Configuration** at navigation bar in order to enter configuration page as following:



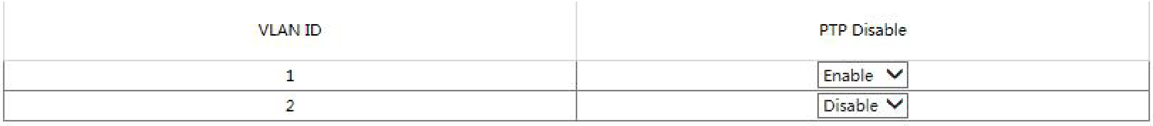
Port	Create the PTP port	IEEE1588 Transport Protocol	Delay Measurement Mechanism	Designated Disable	Transmission Interval of Announce Packets	Announce Receipt Timeout	Transmission Interval of Sync Packets	Transmission Interval of PdelayReq Packets
g0/1	False	ethernet	p2p	Enable	1	10	-1	-1
g0/2	False	ethernet	p2p	Enable	1	10	-1	-1
g0/3	False	ethernet	p2p	Enable	1	10	-1	-1
g0/4	False	ethernet	p2p	Enable	1	10	-1	-1
f1/1	False	ethernet	p2p	Enable	1	10	-1	-1
f1/2	False	ethernet	p2p	Enable	1	10	-1	-1
f1/3	False	ethernet	p2p	Enable	1	10	-1	-1

PTP port’s creation, IEEE1588 Transport Protocol type, delay measurement mechanism, and etc, all of which are under port, could be configured at this page.

> Note：
> This page could only be configured after PTP protocol is enable。

5.3.3 VLAN

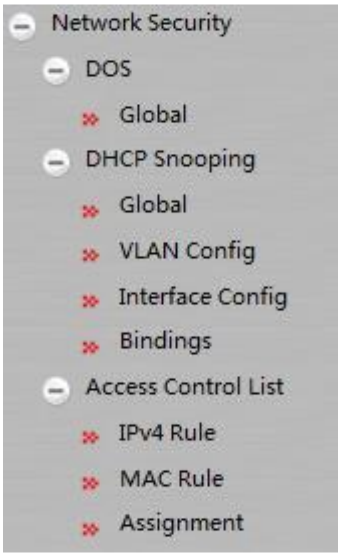
Click **Time -> PTP -> VLAN** at navigation bar in order to enter configuration page as following:



VLAN ID	PTP Disable
1	Enable
2	Disable

You can enable or disable Interface VLAN’s PTP function at this page.

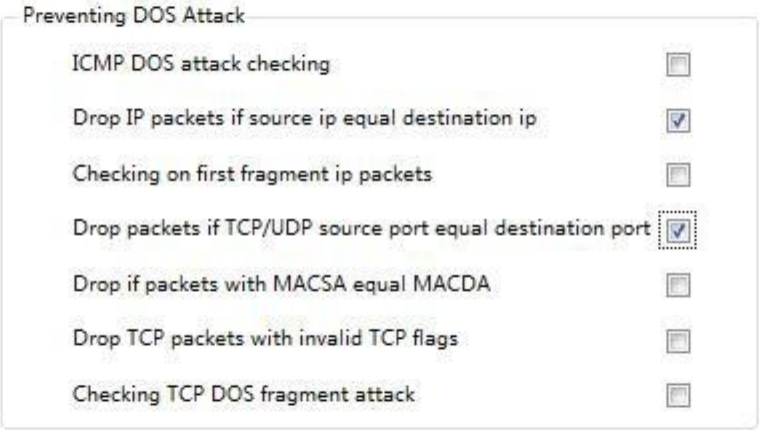
Chapter 6   Network Security



6.1 DOS Configuration

6.1.1 DOS Global Configuration

Click **Network Security -> DOS-> Global** at navigation bar in order to enter DOS global configuration page as following:



Preventing DOS Attack

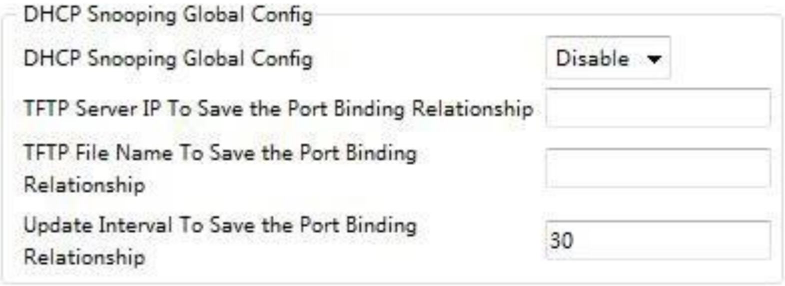
- ICMP DOS attack checking □
- Drop IP packets if source ip equal destination ip ☑
- Checking on first fragment ip packets □
- Drop packets if TCP/UDP source port equal destination port ☑
- Drop if packets with MACSA equal MACDA □
- Drop TCP packets with invalid TCP flags □
- Checking TCP DOS fragment attack □

You could set or cancel the related Preventing DOS Attack according to needs. Click **Setup** to save configuration.

6.2 DHCP Snooping Configuration

6.2.1 DHCP Snooping Global Configuration

Click **Network Security -> DHCP Snooping -> Global** at navigation bar in order to enter DHCP Snooping global configuration page as following:



DHCP Snooping Global Config

DHCP Snooping Global Config	Disable
TFTP Server IP To Save the Port Binding Relationship	
TFTP File Name To Save the Port Binding Relationship	
Update Interval To Save the Port Binding Relationship	30

Enable global DHCP Snooping protocol to detect all DHCP messages. Relative binding relationships forms. If client obtains addresses by the switch before the command is configured previously, switch cannot add relative binding relationships.

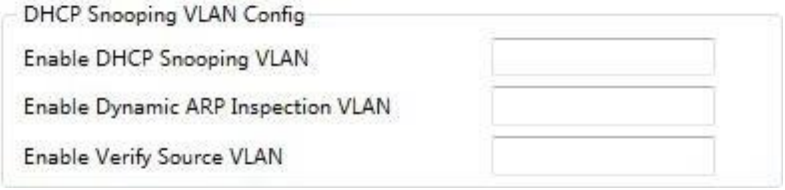
After switch's configuration is saved, restart the switch. All previous configured interface binding relationship would be dropped. At the meantime, the interface has no binding relationship, and switch would denying the forwarding of all IP messages after IP source address monitoring function is enabled. After the interface binding relationship's backup TFTP server is configured, binding relationship would be copied to server by TFTP protocol. After switch restarted, it would download binding list from TFTP server automatically to ensure network's normal operation.

When configuring backup interface binding relationships, save file name on TFTP server. Therefore, different switches can copy their interface binding relationship list to the same TFTP server.

The binding relationship list of interface's MAC address and IP address is dynamic. It is required to check whether the binding is updated. If there is (like binding items are added or deleted), backup should be done again. The default time interval is 30 minutes.

6.2.2 DHCP Snooping VLAN Configuration

Click **Network Security -> DHCP Snooping -> VLAN Configuration** at navigation bar in order to enter DHCP Snooping VLAN configuration page as following:



DHCP Snooping VLAN Config

Enable DHCP Snooping VLAN	
Enable Dynamic ARP Inspection VLAN	
Enable Verify Source VLAN	

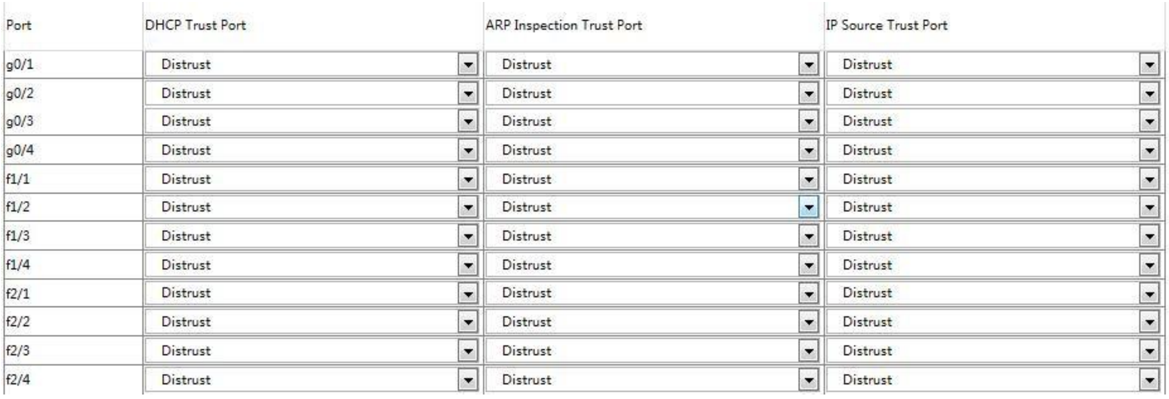
After the DHCP Snooping function is enabled on the VLAN, the DHCP messages received by all untrusted physical ports on the entire VLAN will be legally inspected. Any responded DHCP messages received by untrusted physical ports within a VLAN will be lost to prevent users from counterfeiting messages or prevent a mistaken DHCP server from assigning addresses. For the DHCP requests from untrusted ports, if the MAC address does not match the hardware address field in the messages, the requests will be considered as attacking messages counterfeited by users for the purpose of DHCP DOS (denial of service) and the switch will be abandoned too.

Monitor the ARP dynamics of all physical ports of a VLAN. If the source MAC and IP addresses of the ARP messages received by the ports do not match the MAC and IP address binding relations configured for the ports, the messages cannot be processed. The binding relations configured for the ports may be dynamic along with the DHCP or manually configured. If no MAC and IP address binding relations are configured for a physical port, the switch will refuse to forward all the ARP messages.

In a VLAN where IP source addresses are monitored, if the source MAC and IP addresses of the IP messages received by all the physical ports in the VLAN do not match the MAC and IP address binding relations configured for the ports, the messages cannot be processed. The binding relations configured for the ports may be dynamic along with the DHCP or manually configured. If no MAC and IP address binding relations are configured for a physical port, the switch will refuse to forward all the IP messages received by all the ports.

6.2.3 DHCP Snooping Port Configuration

Click **Network Security -> DHCP Snooping -> Port Configuration** at navigation bar in order to enter DHCP Snooping Port configuration page as following:



Port	DHCP Trust Port	ARP Inspection Trust Port	IP Source Trust Port
g0/1	Distrust	Distrust	Distrust
g0/2	Distrust	Distrust	Distrust
g0/3	Distrust	Distrust	Distrust
g0/4	Distrust	Distrust	Distrust
f1/1	Distrust	Distrust	Distrust
f1/2	Distrust	Distrust	Distrust
f1/3	Distrust	Distrust	Distrust
f1/4	Distrust	Distrust	Distrust
f2/1	Distrust	Distrust	Distrust
f2/2	Distrust	Distrust	Distrust
f2/3	Distrust	Distrust	Distrust
f2/4	Distrust	Distrust	Distrust

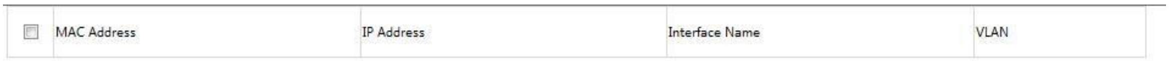
If a port is configured as the DHCP-trusted port, the DHCP messaged received by this port will not be inspected.

The ARP monitoring function will not be enabled for ARP-trusted ports. Ports are untrusted by default.

The source address inspection function is not enabled for ports trusted by IP source addresses.

6.2.3 DHCP Snooping Binding Configuration

Click **Network Security -> DHCP Snooping -> Binding** at navigation bar in order to enter DHCP Snooping Binding configuration page as following:

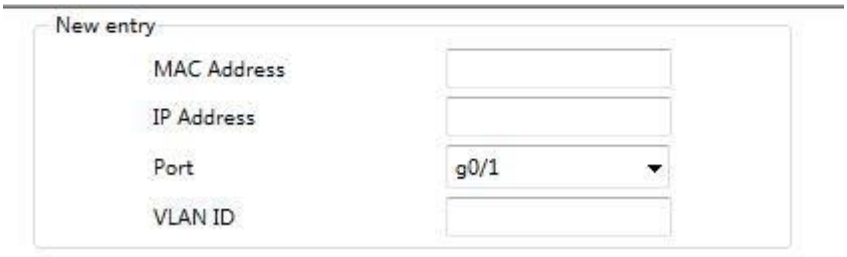


□	MAC Address	IP Address	Interface Name	VLAN

For hosts that do not use DHCP to obtain addresses, users can manually add entries for binding at the switch ports to enable the host to smoothly access the network. The no command can be used to delete the bound entries.

Entries bound manually proceed over those bound through dynamic configuration. If the MAC address of the configured entry is the same as the MAC address of the dynamically configured entry, the latter will be updated based on the former. The MAC address is the only one index for bound entries of a port.

Click "New" to create entries for binding manually configured DHCP Snooping ports.



New entry

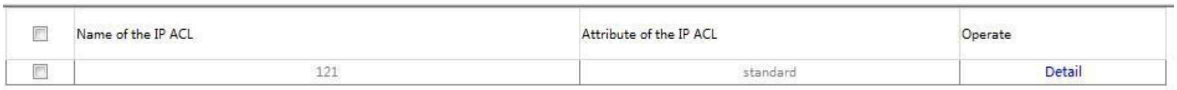
MAC Address	
IP Address	
Port	g0/1
VLAN ID	

Note：
Binding entries can be created only if enabling DHCP Snooping protocol.

6.3 Access Control List Configuration

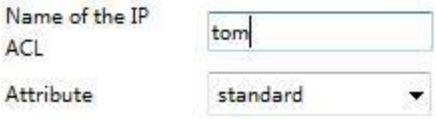
6.3.1 IPv4 Rules

Click **Network Security -> Access Control List -> IPv4 Rules** at navigation bar in order to enter IPv4 rules' page as following:



□	Name of the IP ACL	Attribute of the IP ACL	Operate
□	121	standard	Detail

Click **New** to create an IP access control list. Click **Delete** to delete the access control list.

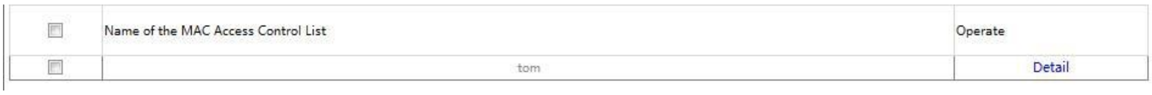


Name of the IP ACL	tom
Attribute	standard

Click **Modify** to enter relative IP access control list to do rules' setup.

6.3.2 MAC Rules

Click **Network Security -> Access Control List -> MAC Rules** at navigation bar in order to enter MAC rules' page as following:



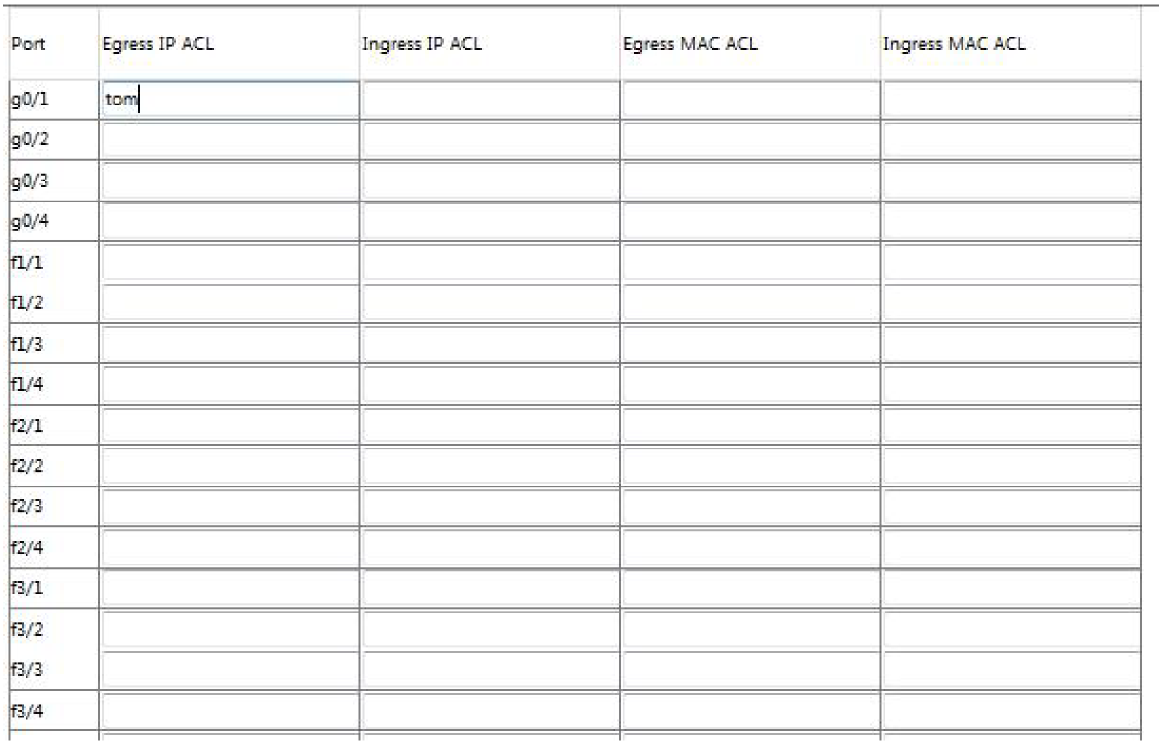
☐	Name of the MAC Access Control List	Operate
☐	tom	Detail

Click **New** to create a MAC access control list. Click **Delete** to delete the access control list.

Name of the MAC ACL	

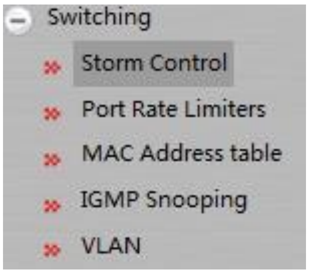
6.3.3 Distribution

Click **Network Security -> Access Control List -> Distribution** at navigation bar in order to enter distribution page of access control list as following:



Port	Egress IP ACL	Ingress IP ACL	Egress MAC ACL	Ingress MAC ACL
g0/1	tom			
g0/2				
g0/3				
g0/4				
f1/1				
f1/2				
f1/3				
f1/4				
f2/1				
f2/2				
f2/3				
f2/4				
f3/1				
f3/2				
f3/3				
f3/4				

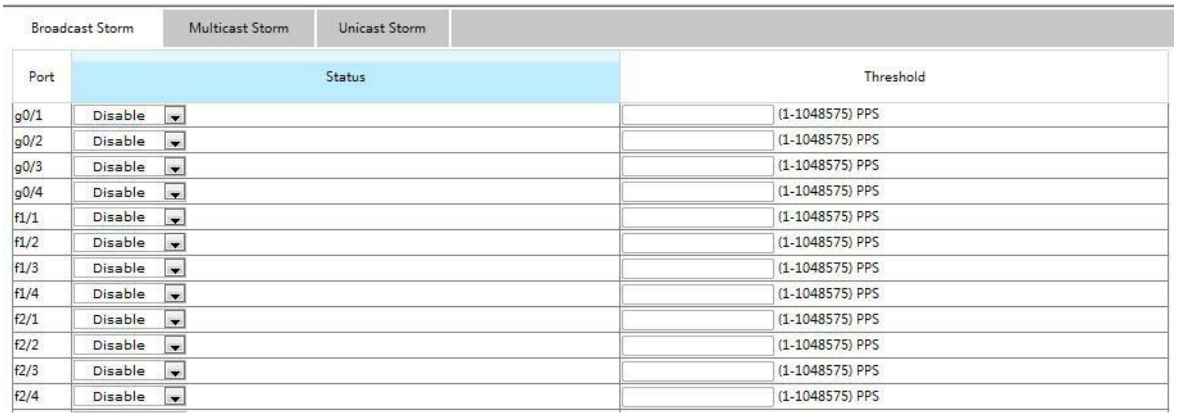
Chapter 7 Switching



7.1 Storm Control

Click **Physical Port Configuration -> Storm Control** at navigation bar in order to enter broadcast storm control, multicast storm control and unicast storm control as following:

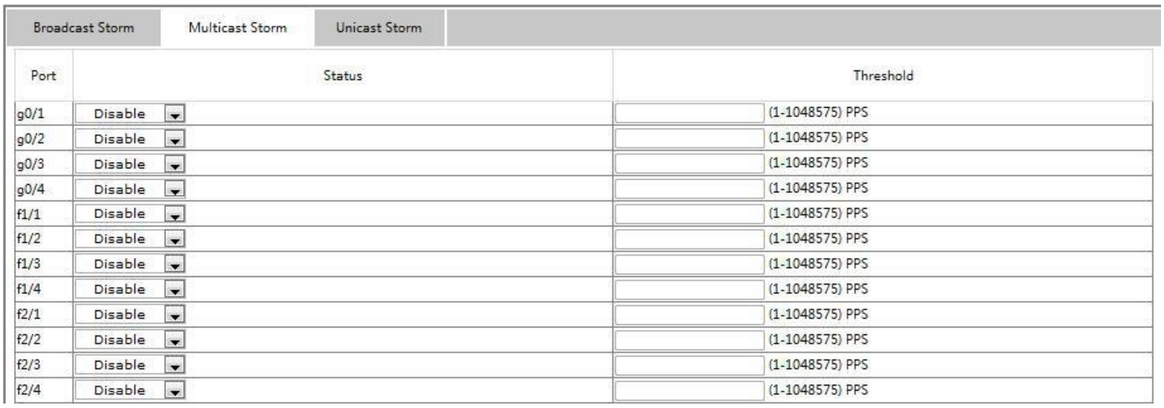
7.1.1 Broadcast Storm Control



Port	Status	Threshold
g0/1	Disable	(1-1048575) PPS
g0/2	Disable	(1-1048575) PPS
g0/3	Disable	(1-1048575) PPS
g0/4	Disable	(1-1048575) PPS
f1/1	Disable	(1-1048575) PPS
f1/2	Disable	(1-1048575) PPS
f1/3	Disable	(1-1048575) PPS
f1/4	Disable	(1-1048575) PPS
f2/1	Disable	(1-1048575) PPS
f2/2	Disable	(1-1048575) PPS
f2/3	Disable	(1-1048575) PPS
f2/4	Disable	(1-1048575) PPS

Through the dropdown boxes in the **Status** column, you can decide whether to enable broadcast storm control on a port. In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

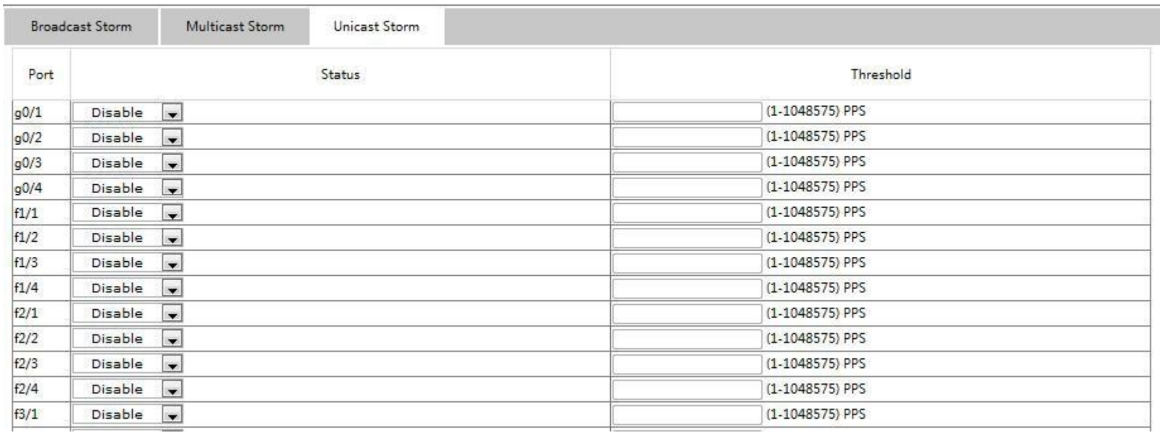
7.1.2 Multicast Storm Control



Port	Status	Threshold
g0/1	Disable	(1-1048575) PPS
g0/2	Disable	(1-1048575) PPS
g0/3	Disable	(1-1048575) PPS
g0/4	Disable	(1-1048575) PPS
f1/1	Disable	(1-1048575) PPS
f1/2	Disable	(1-1048575) PPS
f1/3	Disable	(1-1048575) PPS
f1/4	Disable	(1-1048575) PPS
f2/1	Disable	(1-1048575) PPS
f2/2	Disable	(1-1048575) PPS
f2/3	Disable	(1-1048575) PPS
f2/4	Disable	(1-1048575) PPS

Through the dropdown boxes in the **Status** column, you can decide whether to enable multicast storm control on a port. In the **Threshold** column you can enter the threshold of the multicast packets. The legal threshold range for each port is given behind the threshold.

7.1.3 Unknown Unicast Storm Control



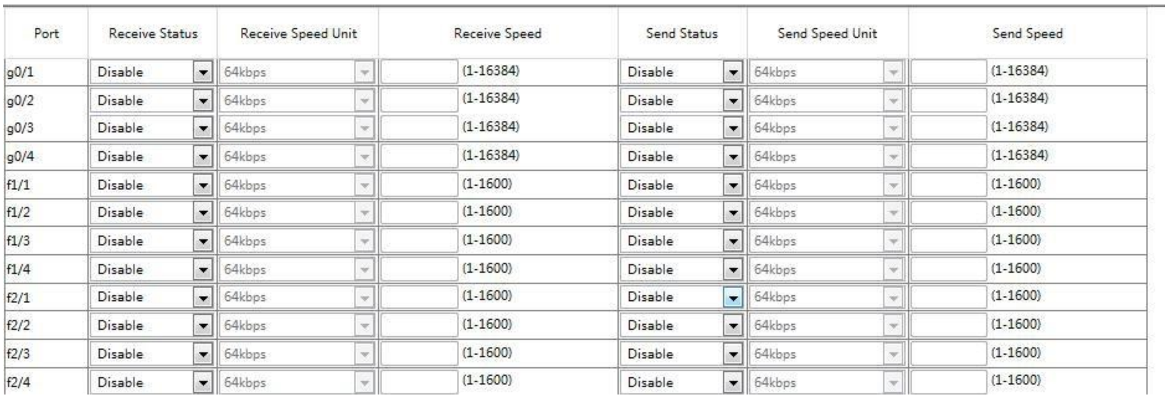
Broadcast Storm | Multicast Storm | Unicast Storm

Port	Status	Threshold
g0/1	Disable	(1-1048575) PPS
g0/2	Disable	(1-1048575) PPS
g0/3	Disable	(1-1048575) PPS
g0/4	Disable	(1-1048575) PPS
f1/1	Disable	(1-1048575) PPS
f1/2	Disable	(1-1048575) PPS
f1/3	Disable	(1-1048575) PPS
f1/4	Disable	(1-1048575) PPS
f2/1	Disable	(1-1048575) PPS
f2/2	Disable	(1-1048575) PPS
f2/3	Disable	(1-1048575) PPS
f2/4	Disable	(1-1048575) PPS
f3/1	Disable	(1-1048575) PPS

Through the dropdown boxes in the **Status** column, you can decide whether to enable unicast storm control on a port. In the **Threshold** column you can enter the threshold of the unicast packets. The legal threshold range for each port is given behind the threshold.

7.2 Port’s Speed-limit

Click **Exchange -> Port’s Speed-limit** at navigation bar in order to enter port’s speed-limit as following:

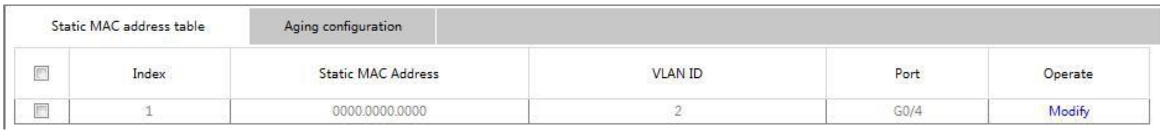


Port	Receive Status	Receive Speed Unit	Receive Speed	Send Status	Send Speed Unit	Send Speed
g0/1	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/2	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/3	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/4	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
f1/1	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)
f1/2	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)
f1/3	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)
f1/4	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)
f2/1	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)
f2/2	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)
f2/3	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)
f2/4	Disable	64kbps	(1-1600)	Disable	64kbps	(1-1600)

Do speed-limit on ports receive speed and send speed of port at this page. By default all ports' speed is not limited. Receive speed and send speed can be configured according to ratio or switch's defined unit.

7.3 MAC Address Filtration

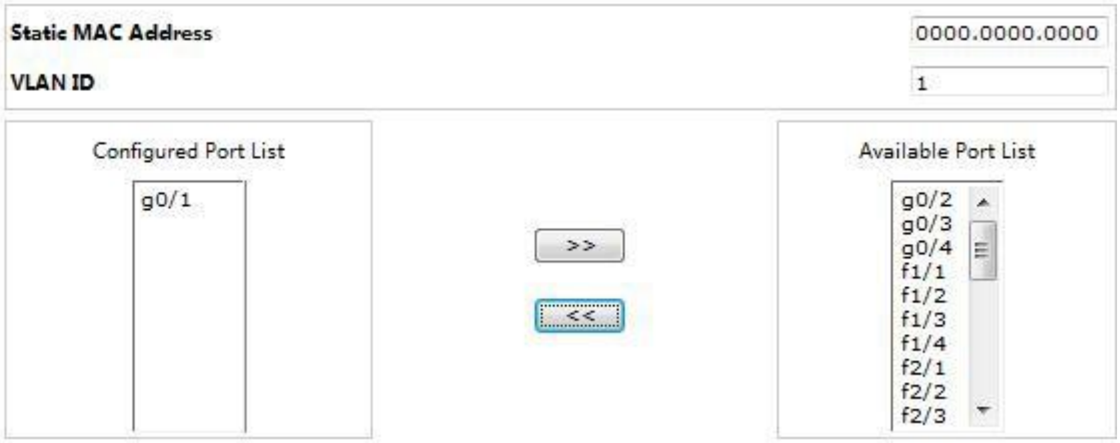
Click **Exchange -> MAC Address Filtration** at navigation bar in order to enter static MAC address table as following:



Static MAC address table | Aging configuration

☐	Index	Static MAC Address	VLAN ID	Port	Operate
☐	1	0000.0000.0000	2	G0/4	Modify

Static MAC address, VLAN ID and index are shown on the page. Click **New** or **Modify** to enter static MAC address configuration page and do modifications on configured static MAC address table。



Static MAC Address: 0000.0000.0000

VLAN ID: 1

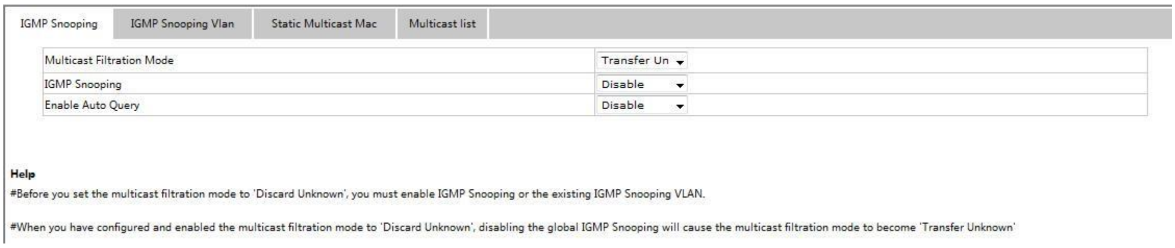
Configured Port List: g0/1

Available Port List: g0/2, g0/3, g0/4, f1/1, f1/2, f1/3, f1/4, f2/1, f2/2, f2/3

7.4 IGMP Snooping Configuration

7.4.1 IGMP Snooping Configuration

Click **Exchange -> IGMP Snooping,** at navigation bar in order, and select IGMP Snooping tab page to enter IGMP Snooping configuration page as following:



IGMP Snooping | IGMP Snooping Vlan | Static Multicast Mac | Multicast list

Multicast Filtration Mode	Transfer Un
IGMP Snooping	Disable
Enable Auto Query	Disable

Help

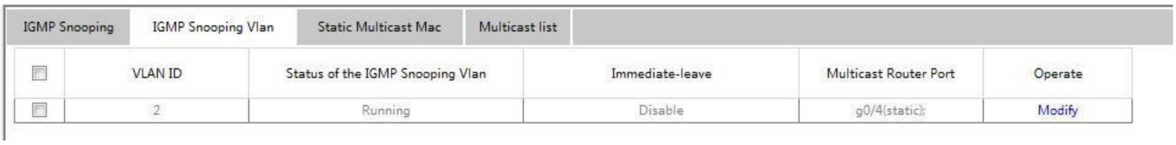
#Before you set the multicast filtration mode to 'Discard Unknown', you must enable IGMP Snooping or the existing IGMP Snooping VLAN.

#When you have configured and enabled the multicast filtration mode to 'Discard Unknown', disabling the global IGMP Snooping will cause the multicast filtration mode to become 'Transfer Unknown'

Whether switch forwarding unknown multicast, whether enabling IGMP-Snooping and whether taken as IGMP's Querier can be configured at this page.

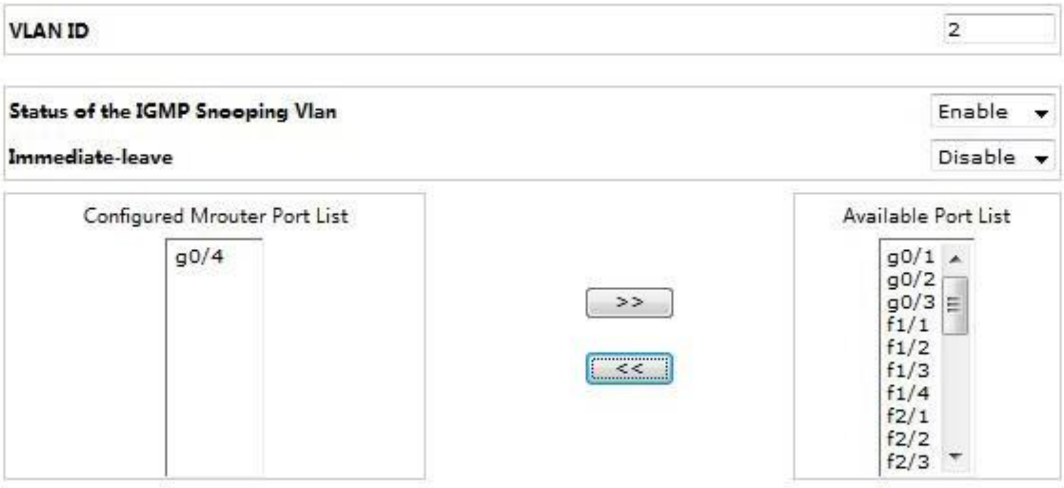
7.4.2 IGMP-Snooping VLAN List

Click **Exchange -> IGMP Snooping,** at navigation bar in order, and select IGMP Snooping VLAN tab page to enter IGMP Snooping VLAN configuration page as following:



□	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router Port	Operate
□	2	Running	Disable	g0/4(static);	Modify

If you click **New**, IGMP-snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP snooping VLAN. If you click **Delete**, a selected IGMP-Snooping VLAN can be deleted; if you click **Modify**, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.



VLAN ID 2

Status of the IGMP Snooping Vlan Enable

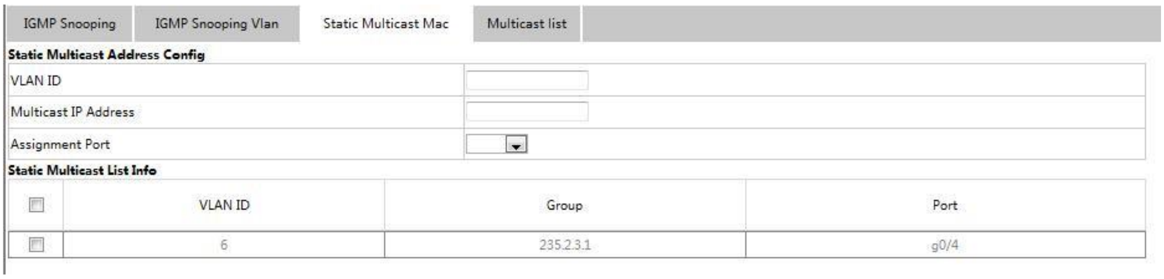
Immediate-leave Disable

When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click “**>>**” and “**<<**” to delete and add a routing port.

7.4.3 Static Multicast Mac Address Configuration

Click **Exchange -> IGMP Snooping,** at navigation bar in order, and select static multicast address tab page to enter static multicast address page as following:



Static Multicast Address Config

VLAN ID

Multicast IP Address

Assignment Port

Static Multicast List Info

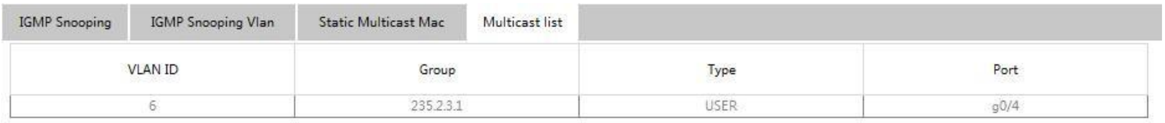
□	VLAN ID	Group	Port
□	6	235.2.3.1	g0/4

On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

Click **Refresh** to refresh the contents in the list.

7.4.4 Multicast list

Click **Exchange -> IGMP Snooping,** at navigation bar in order, and select multicast member list tab page to enter multicast member list configuration page as following:



VLAN ID	Group	Type	Port
6	235.2.3.1	USER	g0/4

The multicast groups in current network and ports' set where every group member exists counted by IGMP-Snooping, are shown on this page.

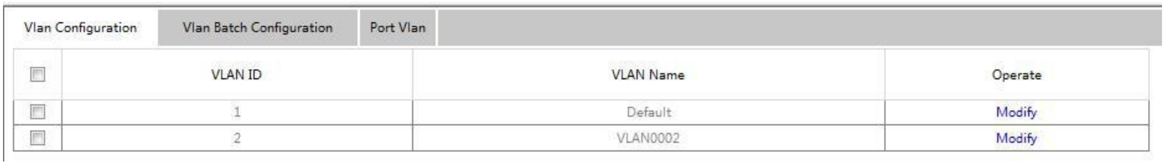
Click **Refresh** to refresh the contents in the list.

Note:
By default, a multicast list can display up to 15 VLAN items. You can modify the number of multicast items by running **ip http web igmp-groups** after you log on to the device through the Console port or Telnet.

7.5 VLAN

7.5.1 VLAN configuration

Click **Exchange -> VLAN,** at navigation bar in order, and select VLAN configuration tab page to enter VLAN configuration page as following:



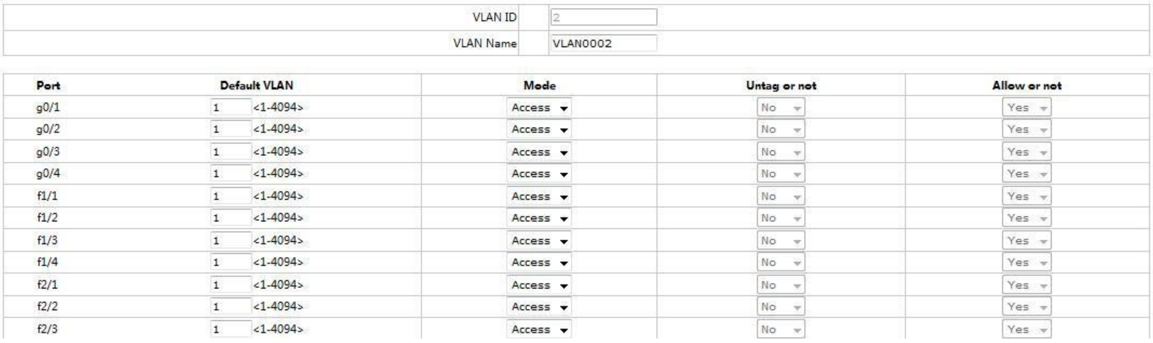
□	VLAN ID	VLAN Name	Operate
□	1	Default	Modify
□	2	VLAN0002	Modify

Click **Modify** after VLAN entry to change VLAN name and this VLAN's port feature.

Select the check box before item and click **Delete** to delete the selected VLAN.

Note:
By default, the maximum quantity of shown items of VLAN list is 100. If you want to configure more VLAN through Web, please login switch by Console port or Telnet to enter global configuration mode and use command **ip http web max-vlan** to modify maximum shown VLAN quantity.

Click **New** or **Modify** to enter VLAN configuration page.



VLAN ID: 2
VLAN Name: VLAN0002

Port	Default VLAN	Mode	Untag or not	Allow or not
g0/1	1 <1-4094>	Access	No	Yes
g0/2	1 <1-4094>	Access	No	Yes
g0/3	1 <1-4094>	Access	No	Yes
g0/4	1 <1-4094>	Access	No	Yes
f1/1	1 <1-4094>	Access	No	Yes
f1/2	1 <1-4094>	Access	No	Yes
f1/3	1 <1-4094>	Access	No	Yes
f1/4	1 <1-4094>	Access	No	Yes
f2/1	1 <1-4094>	Access	No	Yes
f2/2	1 <1-4094>	Access	No	Yes
f2/3	1 <1-4094>	Access	No	Yes

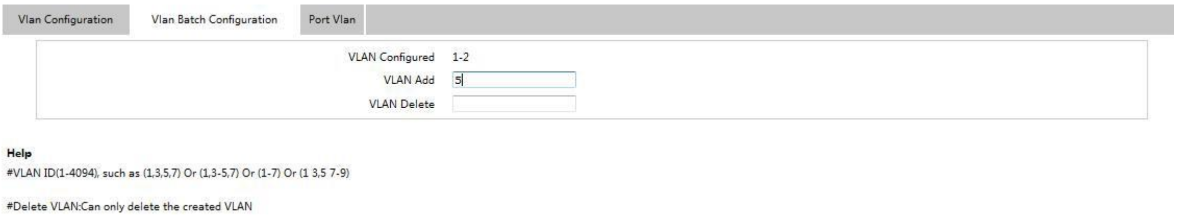
If you want to create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be null.

Through the port list, you can set for each port the default VLAN, the VLAN mode (Trunk or Access), whether to allow the entrance of current VLAN packets and whether to execute the untagging of the current VLAN when the port works as the egress port.

Note:
When a port in Trunk mode serves as an egress port, it will untag the default VLAN by default.

7.5.2 VLAN batch configuration

Click **Exchange -> VLAN,** at navigation bar in order, and select VLAN batch configuration tab page to enter VLAN configuration page as following:



VLAN Configured 1-2
VLAN Add 5
VLAN Delete

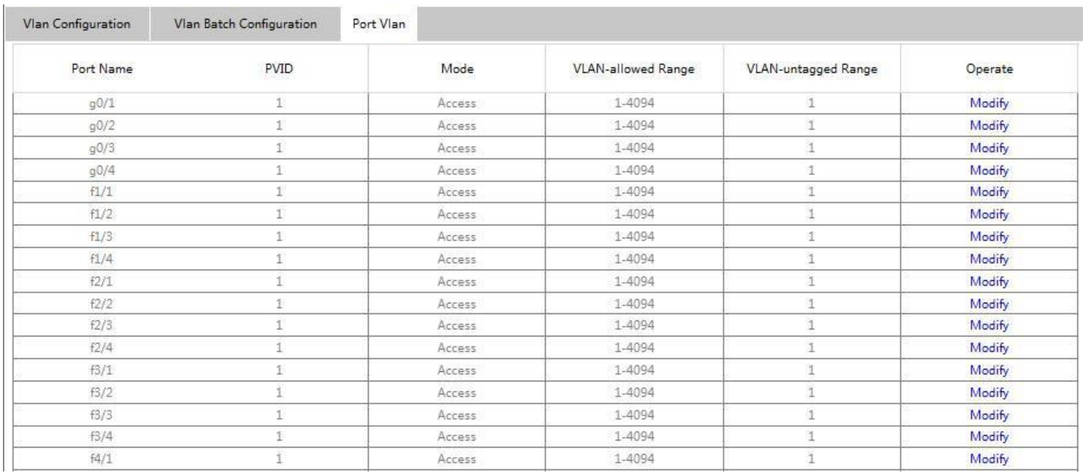
Help
#VLAN ID(1-4094), such as (1,3,5,7) Or (1,3-5,7) Or (1-7) Or (1 3,5 7-9)

#Delete VLAN:Can only delete the created VLAN

Note:
Before VLAN to be deleted, it should be added first.

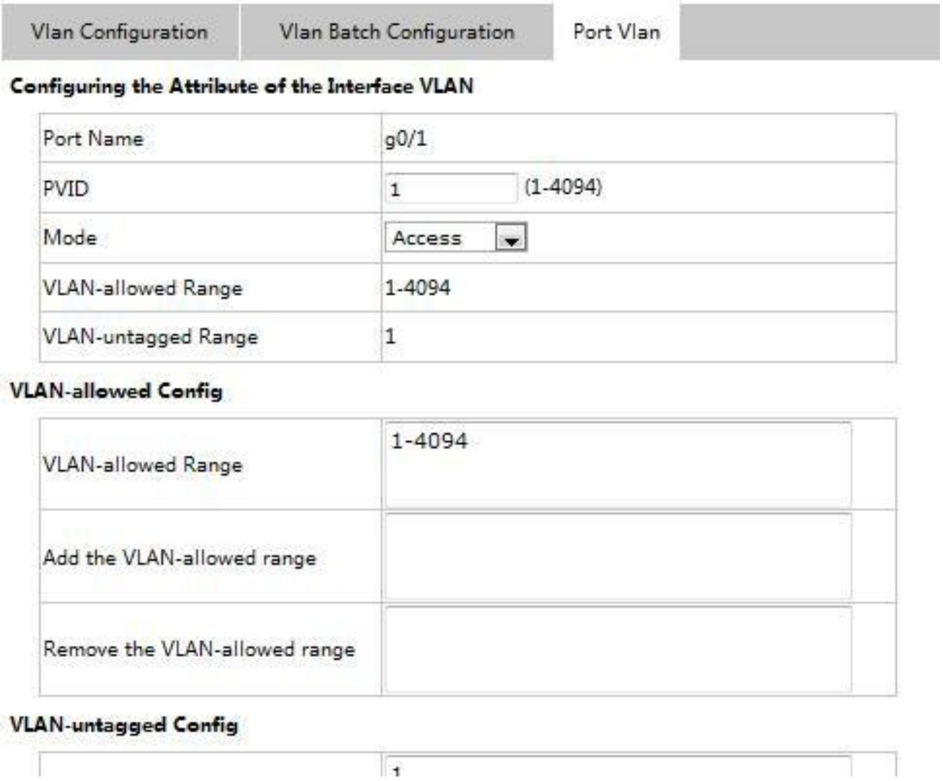
7.5.3 Port VLAN Configuration

Click **Exchange -> VLAN,** at navigation bar in order, and select VLAN tab page to enter port VLAN configuration page as following:



Port Name	PVID	Mode	VLAN-allowed Range	VLAN-untagged Range	Operate
g0/1	1	Access	1-4094	1	Modify
g0/2	1	Access	1-4094	1	Modify
g0/3	1	Access	1-4094	1	Modify
g0/4	1	Access	1-4094	1	Modify
f1/1	1	Access	1-4094	1	Modify
f1/2	1	Access	1-4094	1	Modify
f1/3	1	Access	1-4094	1	Modify
f1/4	1	Access	1-4094	1	Modify
f2/1	1	Access	1-4094	1	Modify
f2/2	1	Access	1-4094	1	Modify
f2/3	1	Access	1-4094	1	Modify
f2/4	1	Access	1-4094	1	Modify
f3/1	1	Access	1-4094	1	Modify
f3/2	1	Access	1-4094	1	Modify
f3/3	1	Access	1-4094	1	Modify
f3/4	1	Access	1-4094	1	Modify
f4/1	1	Access	1-4094	1	Modify

This page shows all ports’ PVIDs, modes, allowed VLAN range and VLAN range without tag. Click **Modify** to change port’s VLAN feature configuration, VLAN-allowed configuration and VLAN-untagged configuration.



Configuring the Attribute of the Interface VLAN

Port Name	g0/1
PVID	1 (1-4094)
Mode	Access
VLAN-allowed Range	1-4094
VLAN-untagged Range	1

VLAN-allowed Config

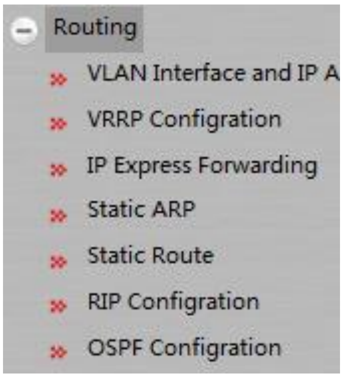
VLAN-allowed Range	1-4094
Add the VLAN-allowed range	
Remove the VLAN-allowed range	

VLAN-untagged Config

	1

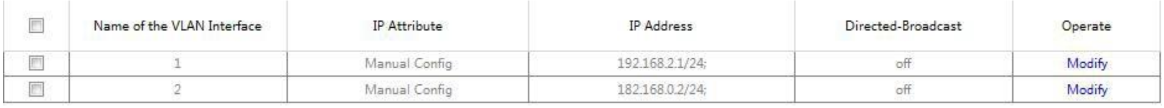
Note:
VLAN-allowed and VLAN-untagged：Please add first before do delete operation.
Please do not key enter.

Chapter 8　Routing



8.1　VLAN Interface and IP Address Configuration

Click **Routing -> VLAN Interface and IP Address** at navigation bar in order，and then enter configuration page as following：



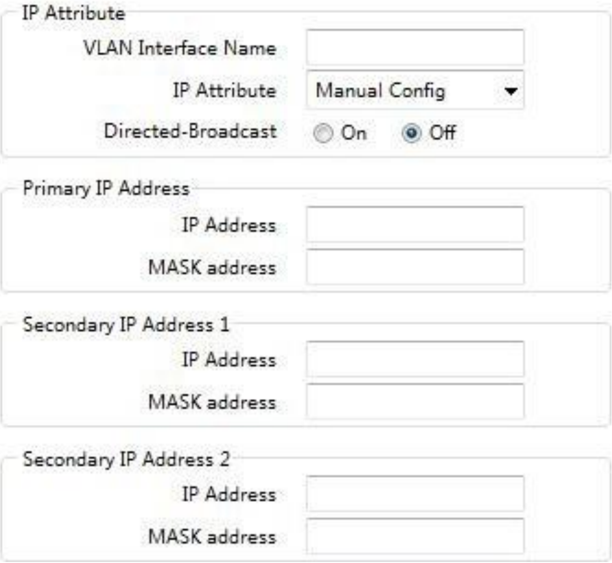
□	Name of the VLAN Interface	IP Attribute	IP Address	Directed-Broadcast	Operate
□	1	Manual Config	192.168.2.1/24;	off	Modify
□	2	Manual Config	182.168.0.2/24;	off	Modify

Click **New** to create a new VLAN interface items.

Click **Modify** to enter relative VLAN interface items to do the modification.

Click **Delete** to delete the selected VLAN interface items.

You can change the VLAN name when you click the “New” bottom, it’s cannot change VLAN name when click “Modify” just can do the VLAN related items modification.



IP Attribute

VLAN Interface Name

IP Attribute: Manual Config

Directed-Broadcast: ○ On ● Off

Primary IP Address

IP Address

MASK address

Secondary IP Address 1

IP Address

MASK address

Secondary IP Address 2

IP Address

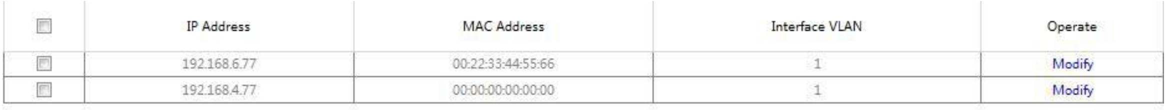
MASK address

Note：

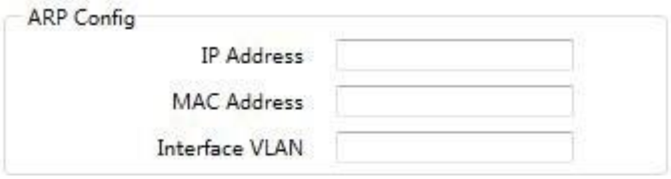
Before you want setting the VLAN secondary IP address， must need setting the Primary IP Address finished。

8.2 Static ARP Configuration

Click **Routing -> Static ARP** at navigation bar in order，and then enter configuration page as following：



□	IP Address	MAC Address	Interface VLAN	Operate
□	192.168.6.77	00:22:33:44:55:66	1	Modify
□	192.168.4.77	00:00:00:00:00:00	1	Modify



ARP Config

IP Address

MAC Address

Interface VLAN

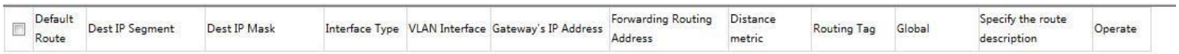
Click **New** to create a new Static ARP.

Click **Modify** to modify the current Static ARP。

Click **Delete** to delete the selected Static ARP items。

8.3 Static Route Configuration

Click **Routing -> Static Route** at navigation bar in order, and then enter configuration page as following：



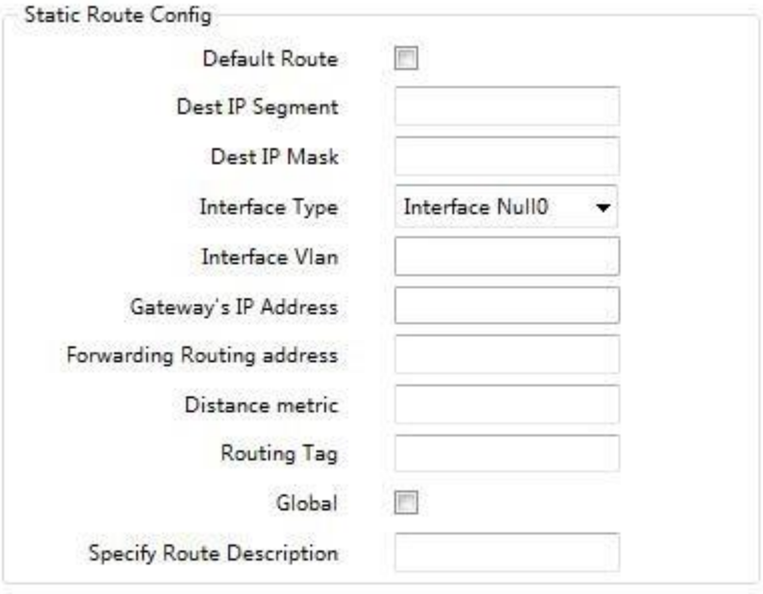
□	Default Route	Dest IP Segment	Dest IP Mask	Interface Type	VLAN Interface	Gateway's IP Address	Forwarding Routing Address	Distance metric	Routing Tag	Global	Specify the route description	Operate

Click **New** to create a new Static ARP.

Click **Modify** to modify the current Static ARP。

Click **Delete** to delete the selected Static ARP items。

Note:
Only the L3 switches have the static route configuration page.



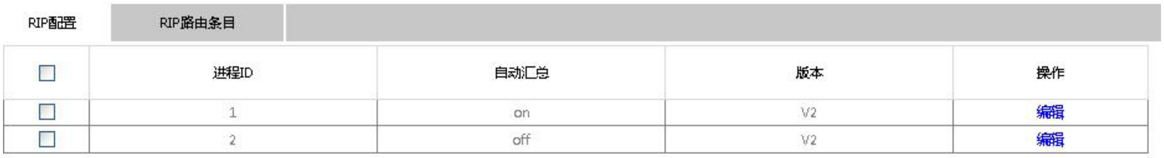
Static Route Config

Default Route	□
Dest IP Segment	
Dest IP Mask	
Interface Type	Interface Null0 ▾
Interface Vlan	
Gateway's IP Address	
Forwarding Routing address	
Distance metric	
Routing Tag	
Global	□
Specify Route Description	

8.4 RIP

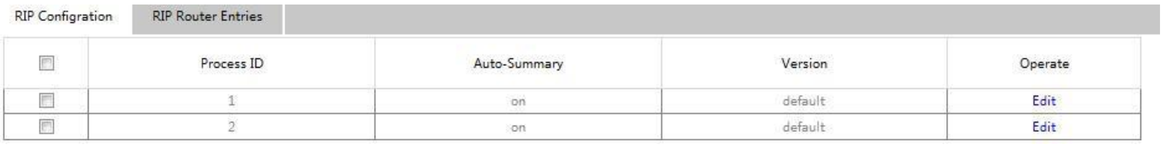
8.4.1 RIP process configuration

Click **Routing -> RIP Configuration** at navigation bar in order, and then enter configuration page as following：



RIP配置 | RIP路由条目

□	进程ID	自动汇总	版本	操作
□	1	on	V2	编辑
□	2	off	V2	编辑

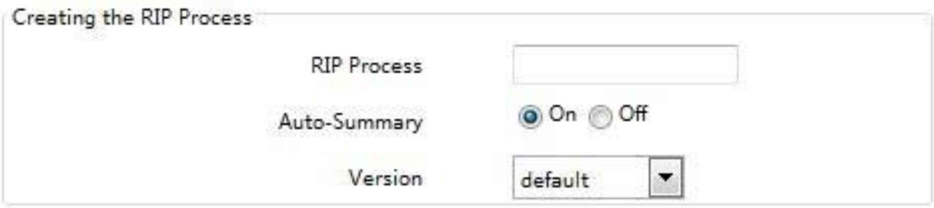


RIP Configration | RIP Router Entries

□	Process ID	Auto-Summary	Version	Operate
□	1	on	default	Edit
□	2	on	default	Edit

You should have created a RIP process firstly，before do the RIP entry configuration。When **Edit** the RIP process can create the new RIP process or delete it also.

Click **New** to create a new RIP process.

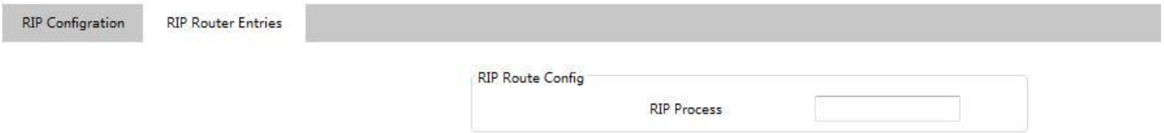


Creating the RIP Process

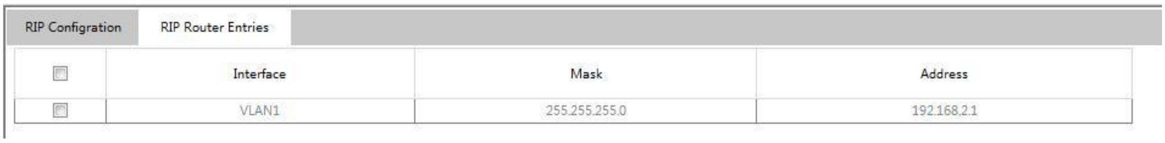
RIP Process	
Auto-Summary	● On ○ Off
Version	default ▾

8.4.2 RIP Entries Configuration

Click **Routing -> RIP Configuration** at navigation bar in order, and then click **RIP Router Entries** to enter RIP Router Entries configuration page as following：

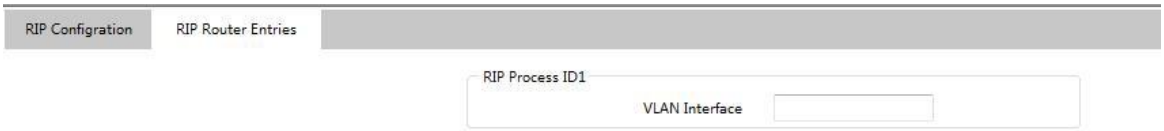


Enter the created RIP process ID，Click Apply to entry the selected RIP Router Entries page



☐	Interface	Mask	Address
☐	VLAN1	255.255.255.0	192.168.2.1

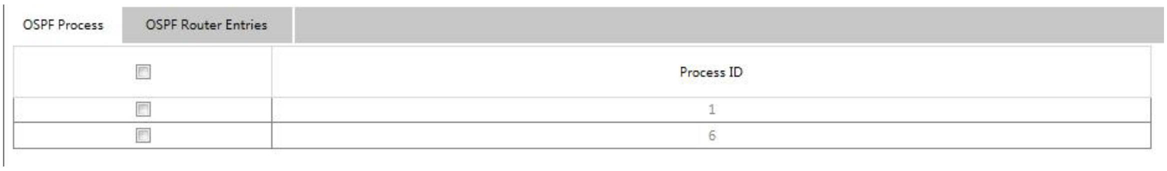
Click **New** to create a new RIP Router Entries of selected RIP process 。



8.5 OSPF Route Configuration

8.5.1 OSPF process configuration

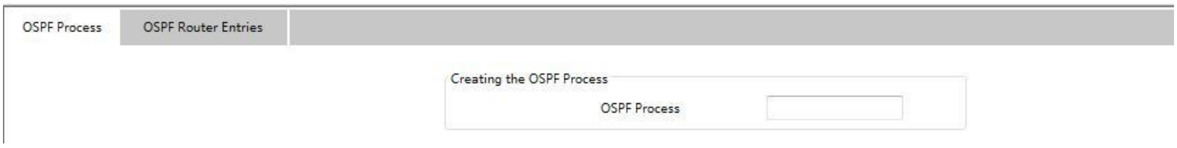
Click **Routing -> OSPF Configuration** at navigation bar in order, and then click **OSPF Process** to enter configuration page as following：



☐	Process ID
☐	1
☐	6

You should have created a OSPF process firstly ， before to do the OSPF Router Entries configuration otherwise cannot do any editing。When click **Edit** enter the RIP process page，you can create the new RIP process or delete it also。

Click **New** to entry the RIP process creating page。

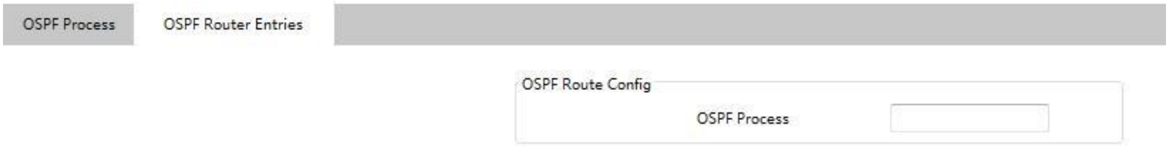


Creating the OSPF Process

OSPF Process

8.5.2 OSPF Router Entries Configuration

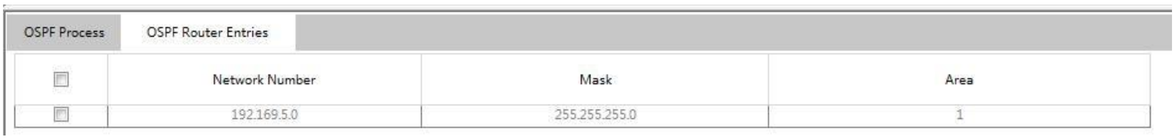
Click **Routing -> OSPF Configuration** at navigation bar in order, and then click **OSPF Router Entries** to enter OSPF Router Entries configuration page as following：



OSPF Route Config

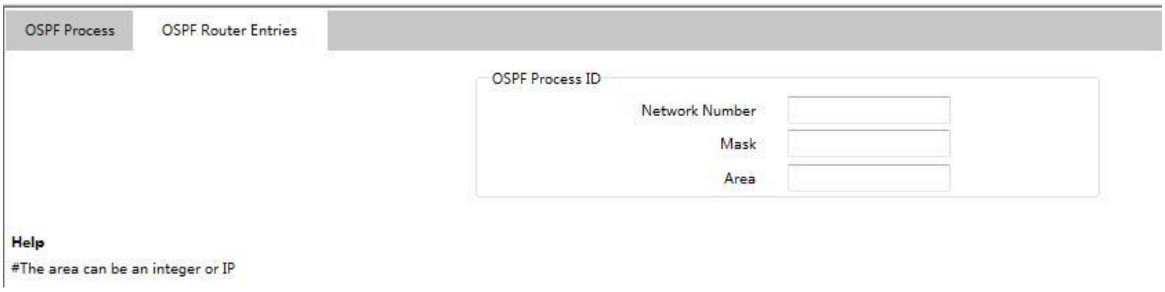
OSPF Process

Enter the OSPF process ID which was created already， click **Apply** to enter the selected OSPF Router Entries configuration page。



□	Network Number	Mask	Area
□	192.169.5.0	255.255.255.0	1

Click **New** to create the OSPF Router Entries of OSPF process selected。



OSPF Process ID

Network Number

Mask

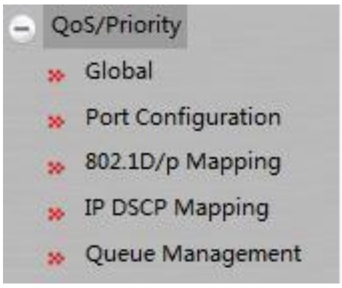
Area

Help

#The area can be an integer or IP

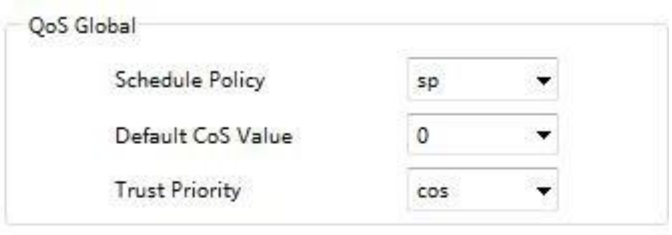
The **Area** column can accept the format is an integer or IP address。

Chapter 9 QoS/Priority



9.1 QoS Global Configuration

Click **QoS/Priority -> Global** at navigation bar in order, and then enter the configuration page as following：



QoS Global

Schedule Policy: sp

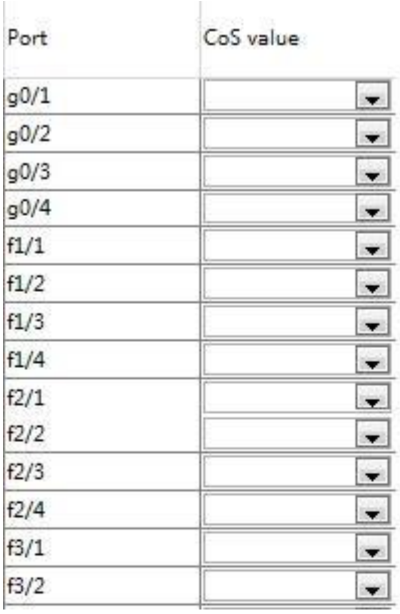
Default CoS Value: 0

Trust Priority: cos

You can do the setting of Schedule Policy、Default CoS Value and Trust Priority in the QoS Global page。

9.2 Port Configuration

Click **QoS/Priority -> Port Configuration** at navigation bar in order, and then enter the configuration page as following：

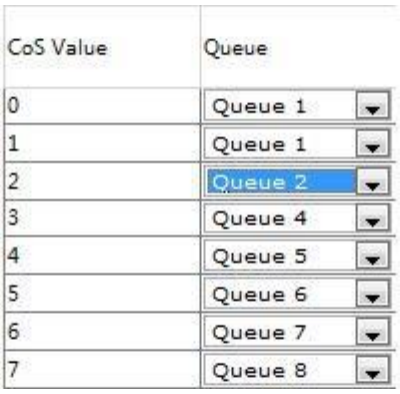


Port	CoS value
g0/1	
g0/2	
g0/3	
g0/4	
f1/1	
f1/2	
f1/3	
f1/4	
f2/1	
f2/2	
f2/3	
f2/4	
f3/1	
f3/2	

You can setting the Port CoS value by port， and then click **Setup** to save the changes。

9.3 802.1D/p mapping Configuration

Click **QoS/Priority -> 802.1D/p mapping** at navigation bar in order, and then enter the configuration page as following：

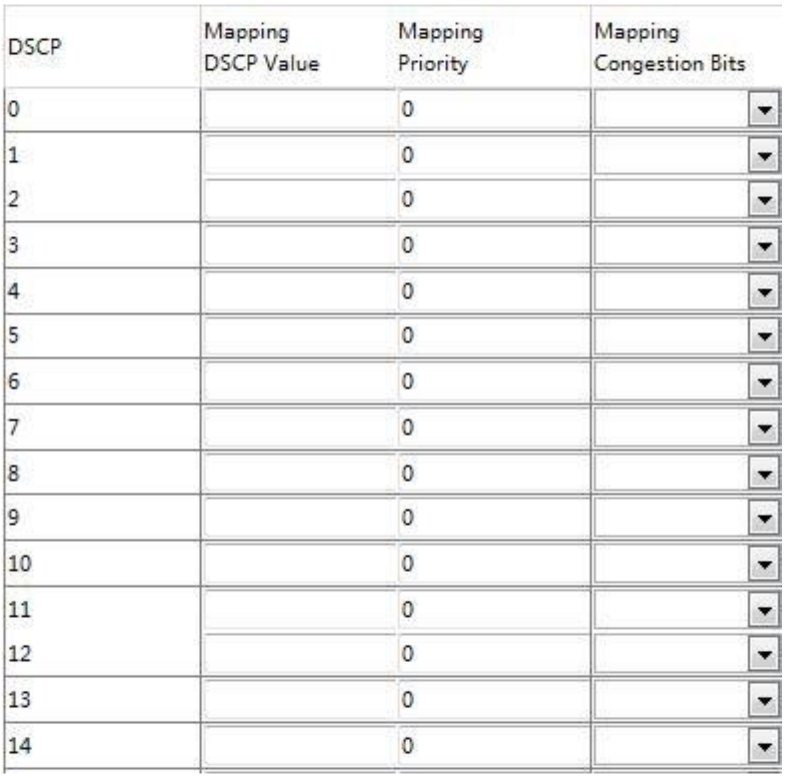


CoS Value	Queue
0	Queue 1
1	Queue 1
2	Queue 2
3	Queue 4
4	Queue 5
5	Queue 6
6	Queue 7
7	Queue 8

Click **Setup** to save all 802.1D/p mapping configurations.

9.4 IP DSCP Mapping Configuration

Click **QoS/Priority -> IP DSCP Mapping** at navigation bar in order, and then enter the configuration page as following：



DSCP	Mapping DSCP Value	Mapping Priority	Mapping Congestion Bits
0		0	
1		0	
2		0	
3		0	
4		0	
5		0	
6		0	
7		0	
8		0	
9		0	
10		0	
11		0	
12		0	
13		0	
14		0	

There are listed the 64 values of DSCP in the IP DSCP mapping page， you can setting the mapping value per each DSCP。

Click Zero and then clean all of the DSCP mapping configuration。

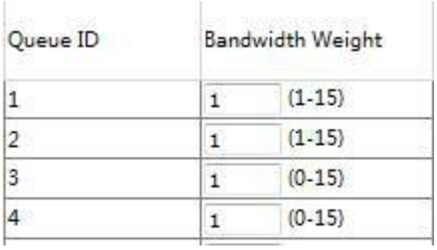
Note：

The number of table parameter may different between different device model.

9.5 Config the Queue Management

Click **QoS/Priority -> Queue Management** at navigation bar in order, and then enter the configuration page as following：

Click **Setup** can save all configuration。

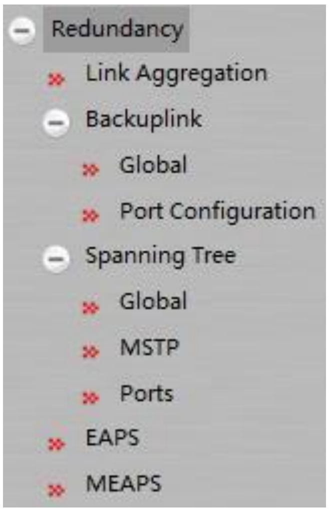


Queue ID	Bandwidth Weight
1	1 (1-15)
2	1 (1-15)
3	1 (0-15)
4	1 (0-15)

Note：

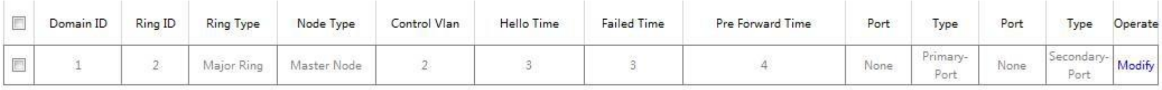
If one Queue ID setting the bandwidth weight to Zero value， then the weight value must only can setting Zero that behind this Queue ID。

Chapter 10 Redundancy



10.1 MEAPS Multi-ring Network Protection Protocol Configuration

Click **Redundancy -> MEAPS** at navigation bar in order, and then enter the MEAPS list configuration page as following：



□	Domain ID	Ring ID	Ring Type	Node Type	Control Vlan	Hello Time	Failed Time	Pre Forward Time	Port	Type	Port	Type	Operate
□	1	2	Major Ring	Master Node	2	3	3	4	None	Primary-Port	None	Secondary-Port	Modify

The list displays the currently configured MEAPS ring, including the Domain ID、Ring ID、Ring Type、Control VLAN、Hello Time、Failed Time、Pre Forward Time and the Primary/Secondary Port on the ring.

Click **New** to create MEAPS ring network。

Click **Modify** right of the entry to configure the time parameter and the Primary and Secondary port of the MEAPS ring network。

Note：

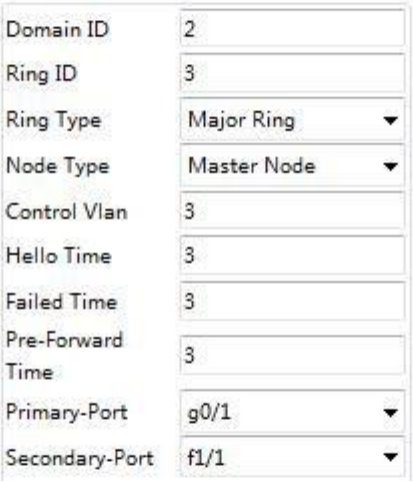
1、Supporting max four MEAPS domains（0-3）。

2、Supporting max eight Rings in one domain(0-7)。

3、Once one MEAPS has configured, its Domain ID, Ring ID, Ring Type, Node Type and Control VLAN cannot be changed. If these parameters need to be configured, please delete this ring and re-create it.

10.1.1 MEAPS Ring Network Configuration

Click **New** or **Modify** on the right of the entry in MEAPS network ring list, and enter MEAPS configuration page.



Domain ID	2
Ring ID	3
Ring Type	Major Ring
Node Type	Master Node
Control Vlan	3
Hello Time	3
Failed Time	3
Pre-Forward Time	3
Primary-Port	g0/1
Secondary-Port	f1/1

Figure: MEAPS Configuration

The primary ring can only configure the master node and the transit node。

The secondary ring can configure the primary node, the transit node, the edge node。

The primary node and the transit node can only exit in one ring, and the edge node and the assistant edge node can exist in many rings simultaneously.。

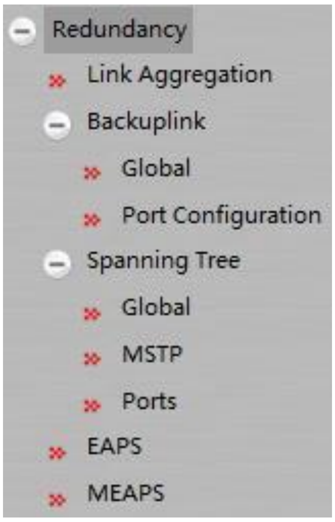
In the text boxes of "Primary Port" and "Secondary Port", select a port as the ring port respectively or select "None"。

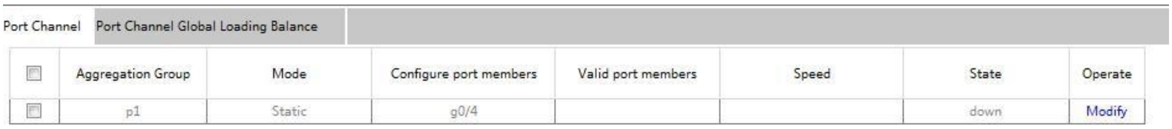
Note：
Once one MEAPS has configured, its ID, ring ID, ring type, node type and control Vlan cannot be configured。

10.2 Link Aggregation Configuration

10.2.1 Port Aggregation Configuration

Click **Redundancy -> Link Aggregation** at navigation bar in order, and then enter the link aggregation configuration page as following：





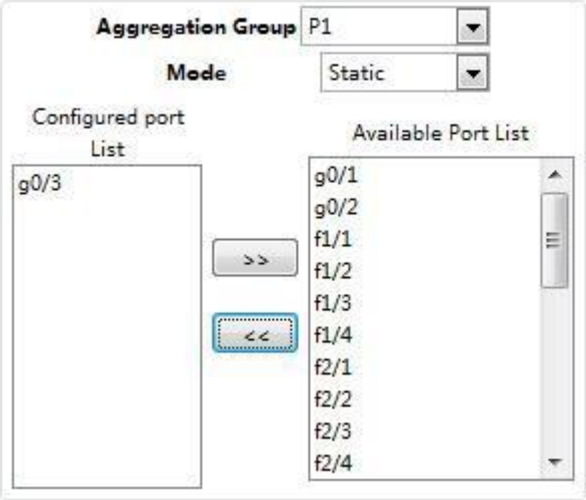
□	Aggregation Group	Mode	Configure port members	Valid port members	Speed	State	Operate
□	p1	Static	g0/4			down	Modify

Figure: Port Aggregation Configuration

Click **New** to create a new aggregation group. As much as 32 aggregation groups can be configured through Web. Each group can configure at most 8 physical port aggregations.

Click **Delete** to delete the selected aggregation group.

Click **Modify** to modify the member port and aggregation mode of the aggregation port.



Aggregation Group: P1

Mode: Static

Configured port List: g0/3

Available Port List: g0/1, g0/2, f1/1, f1/2, f1/3, f1/4, f2/1, f2/2, f2/3, f2/4

Figure: Aggregation Group Member Port Configuration

An aggregation group is selectable when it is created but is not selectable when it is modified.

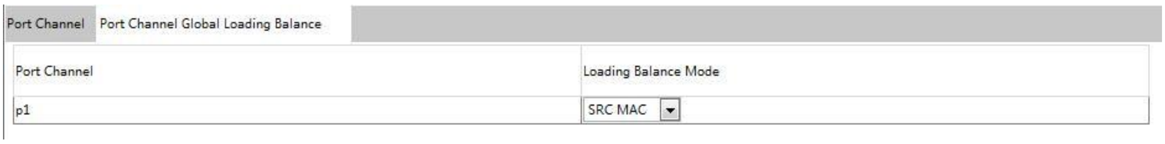
When a member port exists on the aggregation port, you can choose the aggregation mode to be Static, LACP Active or LACP Passive.

You can add or delete the aggregation group member port by buttons **>>** or **<<**

10.2.2 Link Aggregation Load Balancing Configuration

Some models support link aggregation load balancing configuration and others not, but they can be configured in the global configuration mode.

This Layer 3 model can support the aggregation group based load balancing configuration:

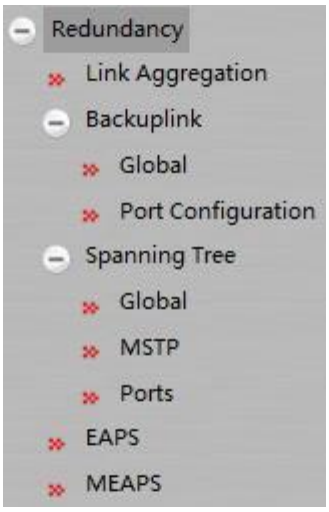


Port Channel	Loading Balance Mode
p1	SRC MAC

Figure: The Aggregation Group Based Load Balancing Configuration

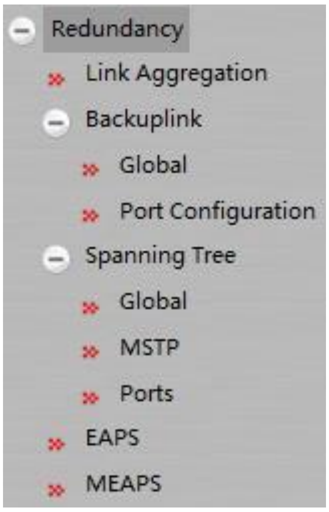
You can use different aggregation groups to set different aggregation modes。

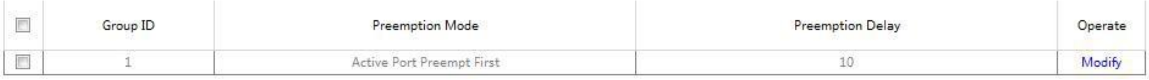
10.3 Link Backup Protocol Configuration



10.3.1 Link Backup Protocol Global Configuration

Click **Redundancy -> Backuplink -> Global** at navigation bar in order, and then enter the link backup protocol global configuration page as following：

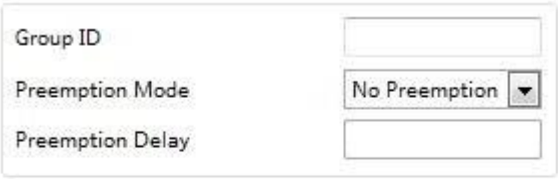




□	Group ID	Preemption Mode	Preemption Delay	Operate
□	1	Active Port Preempt First	10	Modify

The page lists current configured link backup group, including the preemption mode and the preemption delay mode. Click **New** to create a new link backup group。

Click **Modify** on the right of the entry and configure the preemption mode and the preemption delay mode of the link backup group。



Group ID	
Preemption Mode	No Preemption ▼
Preemption Delay	

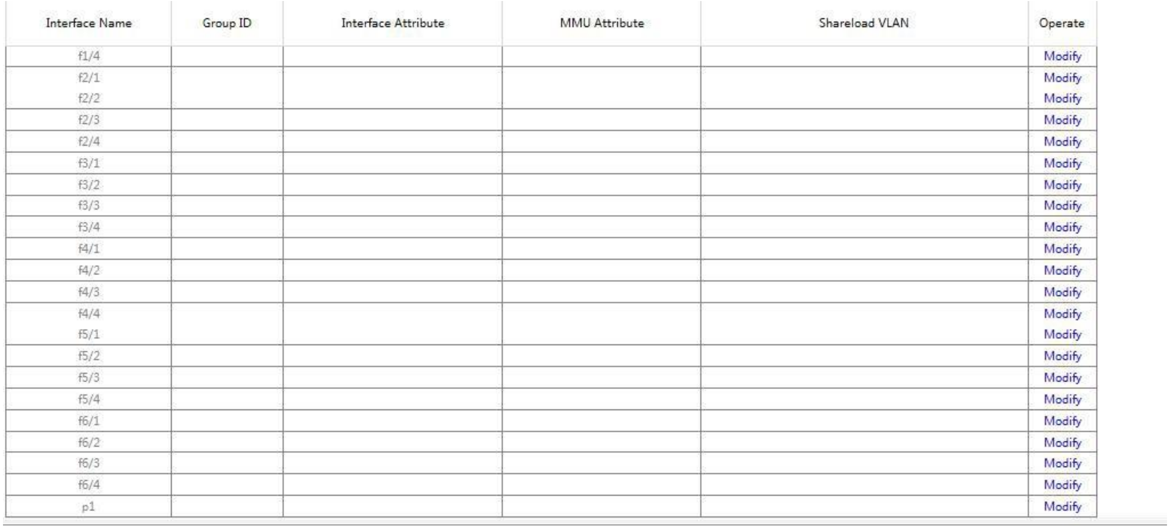
Figure: Link Backup Protocol Group Attribute Configuration

Note：

1. There are supported 8 group numbers of link backup group in this system。
2. The preemption mode of the link backup group decides the policy of the primary port and the backup port selecting forwarding packets.

10.3.2 Link Backup Protocol Port Configuration

Click **Redundancy -> Backuplink -> Port Configuration** at navigation bar in order, and then enter the link backup protocol port configuration page as following：

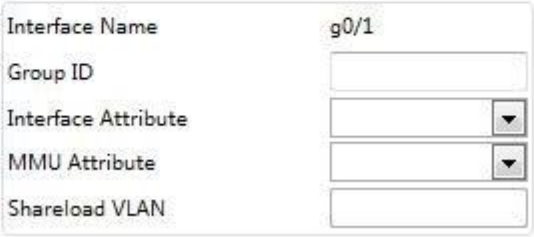


Interface Name	Group ID	Interface Attribute	MMU Attribute	Shareload VLAN	Operate
f1/4					Modify
f2/1					Modify
f2/2					Modify
f2/3					Modify
f2/4					Modify
f3/1					Modify
f3/2					Modify
f3/3					Modify
f3/4					Modify
f4/1					Modify
f4/2					Modify
f4/3					Modify
f4/4					Modify
f5/1					Modify
f5/2					Modify
f5/3					Modify
f5/4					Modify
f6/1					Modify
f6/2					Modify
f6/3					Modify
f6/4					Modify
p1					Modify

Figure: Link Backup Port List

The page lists the member port has joined the backup link group, port attribute of the member port, MMU attribute, load balance vlan. MMU sender can transmit the message to MMU receiver to make the receiver quick update the mac address table.

Click **Modify** on the right of the entry and configure the link backup protocol of the port.

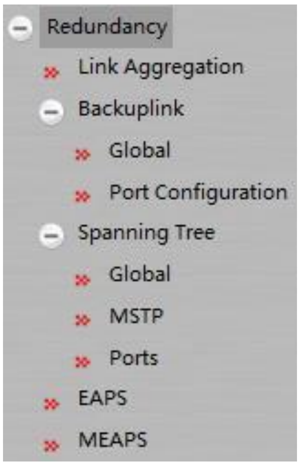


Interface Name	g0/1
Group ID	
Interface Attribute	
MMU Attribute	
Shareload VLAN	

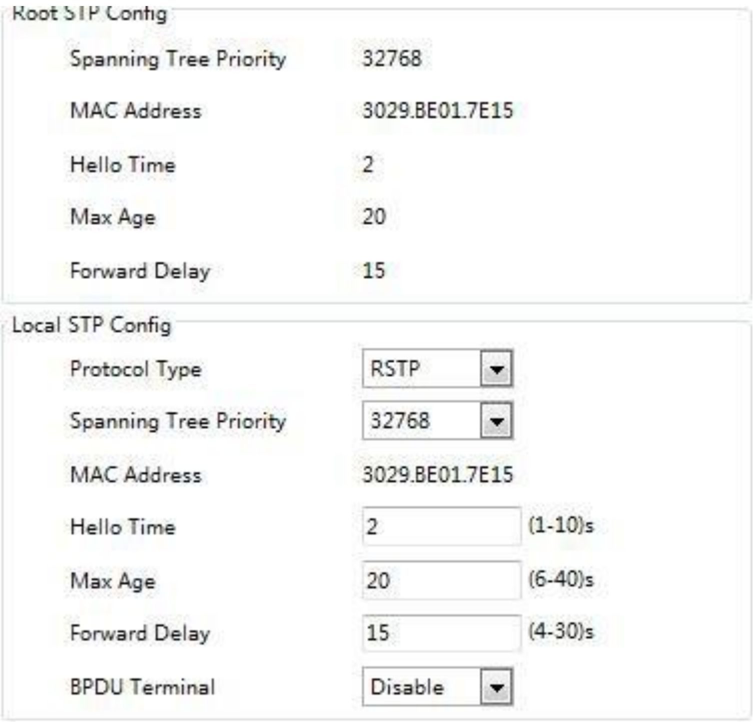
Figure: Link Backup Port Configuration

The link backup group which has been configured the primary port cannot be configured with other port as the primary one. In the same way, the link backup group which has been configured with the backup port cannot be configured with other port as the backup one.

10.4 Spanning-Tree Global Configuration



Click **Redundancy -> Spanning Tree -> Global** at navigation bar in order, and then enter the spanning tree configuration page as following：



Root STP Config

Spanning Tree Priority	32768
MAC Address	3029.BE01.7E15
Hello Time	2
Max Age	20
Forward Delay	15

Local STP Config

Protocol Type	RSTP	
Spanning Tree Priority	32768	
MAC Address	3029.BE01.7E15	
Hello Time	2	(1-10)s
Max Age	20	(6-40)s
Forward Delay	15	(4-30)s
BPDU Terminal	Disable	

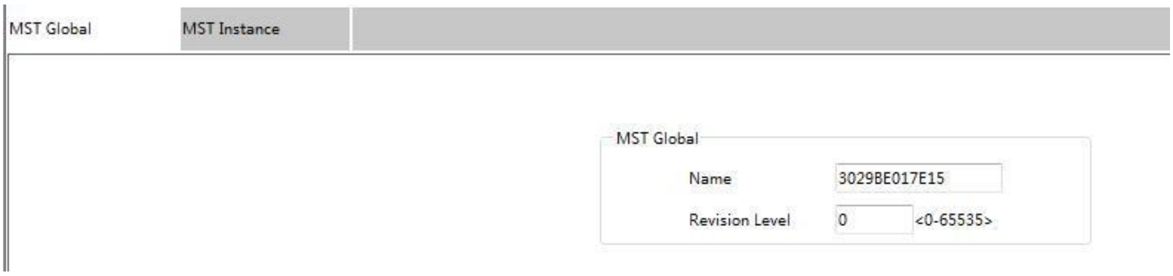
Figure: Spanning Tree Global Configuration

The page can configure the local STP protocol， such as protocol type 、spanning tree priority…etc。Click Setup to save configuration。

10.5 MSTP Configuration

10.5.1 MST Global Configuration

Click **Redundancy -> Spanning Tree -> MSTP** at navigation bar in order, and then click the **MST Global** enter the configuration page as following：



MST Global

Name	3029BE017E15	
Revision Level	0	<0-65535>

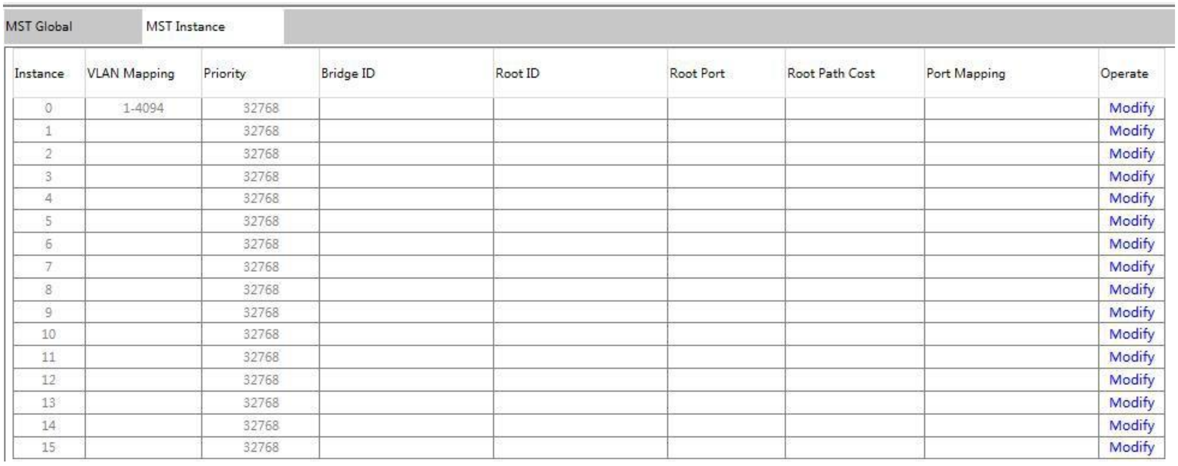
Figure: Spanning Tree MST Configuration

You can configure the MST Global Revision Level in this page.

Click Setup to save configuration。

10.5.2 MST Instance Configuration

Click **Redundancy -> Spanning Tree -> MSTP** at navigation bar in order, and then click the **MST Instance** enter the configuration page as following：

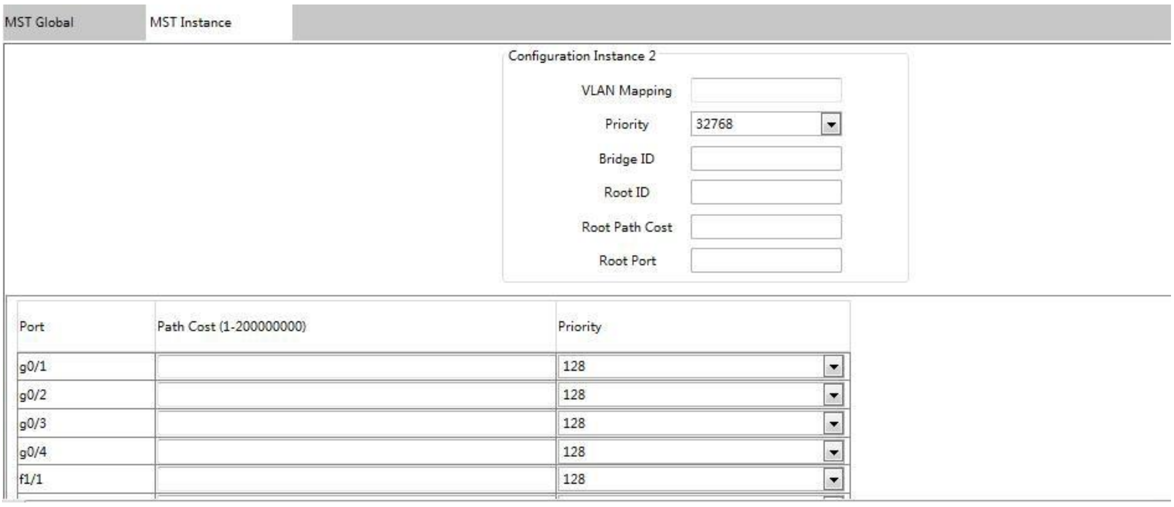


Instance	VLAN Mapping	Priority	Bridge ID	Root ID	Root Port	Root Path Cost	Port Mapping	Operate
0	1-4094	32768						Modify
1		32768						Modify
2		32768						Modify
3		32768						Modify
4		32768						Modify
5		32768						Modify
6		32768						Modify
7		32768						Modify
8		32768						Modify
9		32768						Modify
10		32768						Modify
11		32768						Modify
12		32768						Modify
13		32768						Modify
14		32768						Modify
15		32768						Modify

Figure: Spanning Tree MST Instance Configuration

The page lists the instance related parameter，such as VLAN mapping、Priority、Bridge ID、Root ID、Root Port、Root Path Cost、Port Mapping.

Click **Modify** on the right of the entry and configure the MST instance。



Configuration Instance 2

VLAN Mapping:

Priority: 32768

Bridge ID:

Root ID:

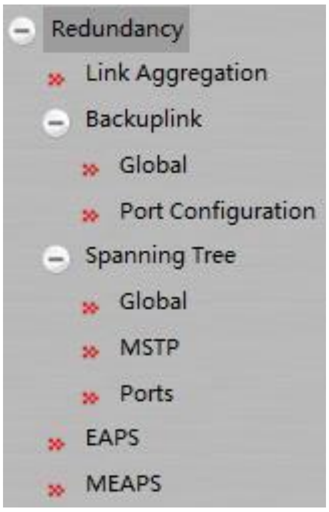
Root Path Cost:

Root Port:

Port	Path Cost (1-200000000)	Priority
g0/1		128
g0/2		128
g0/3		128
g0/4		128
f1/1		128

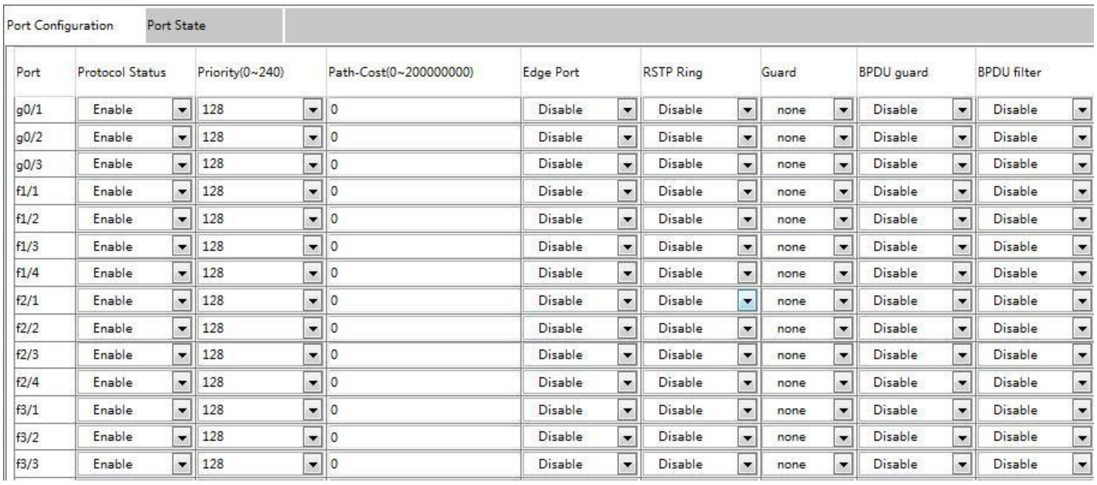
Click **Setup** to save configuration。

10.6 Spanning-Tree Port Configuration



10.6.1 Port Configuration

Click **Redundancy -> Spanning Tree -> Ports** at navigation bar in order, and then click the **Port Configuration** enter the configuration page as following：

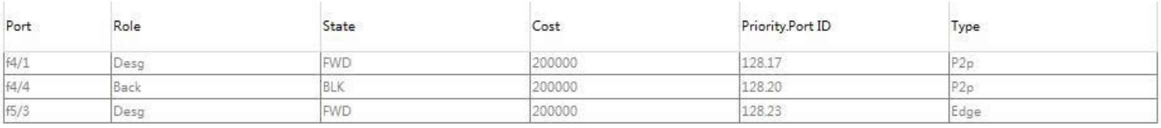


Port	Protocol Status	Priority(0~240)	Path-Cost(0~200000000)	Edge Port	RSTP Ring	Guard	BPDU guard	BPDU filter
g0/1	Enable	128	0	Disable	Disable	none	Disable	Disable
g0/2	Enable	128	0	Disable	Disable	none	Disable	Disable
g0/3	Enable	128	0	Disable	Disable	none	Disable	Disable
f1/1	Enable	128	0	Disable	Disable	none	Disable	Disable
f1/2	Enable	128	0	Disable	Disable	none	Disable	Disable
f1/3	Enable	128	0	Disable	Disable	none	Disable	Disable
f1/4	Enable	128	0	Disable	Disable	none	Disable	Disable
f2/1	Enable	128	0	Disable	Disable	none	Disable	Disable
f2/2	Enable	128	0	Disable	Disable	none	Disable	Disable
f2/3	Enable	128	0	Disable	Disable	none	Disable	Disable
f2/4	Enable	128	0	Disable	Disable	none	Disable	Disable
f3/1	Enable	128	0	Disable	Disable	none	Disable	Disable
f3/2	Enable	128	0	Disable	Disable	none	Disable	Disable
f3/3	Enable	128	0	Disable	Disable	none	Disable	Disable

The page lists the usage status of spanning tree per port, you can configure the parameters。Click Setup then save the configuration.

10.6.2 Spanning Tree Ports Status

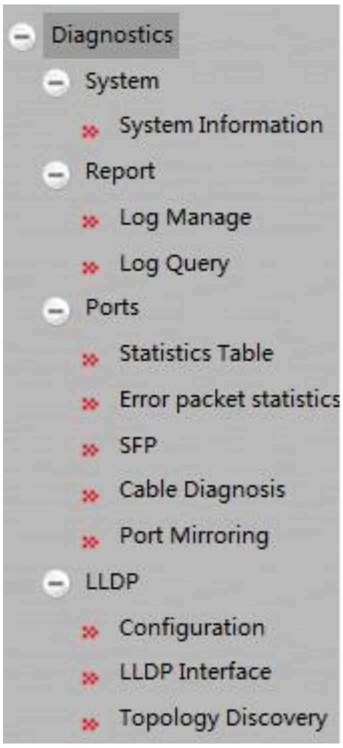
Click **Redundancy -> Spanning Tree -> Ports** at navigation bar in order, and then click the **Port State** enter the configuration page as following：



Port	Role	State	Cost	Priority.Port ID	Type
f4/1	Desg	FWD	200000	128.17	P2p
f4/4	Back	BLK	200000	128.20	P2p
f5/3	Desg	FWD	200000	128.23	Edge

The page lists the port information and usage status of spanning tree ， Click **Reload** can refresh the data.

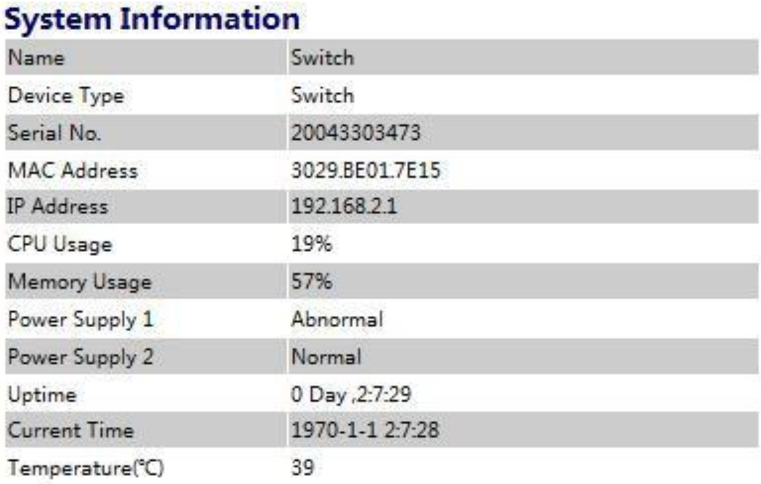
Chapter 11 Diagnostics



11.1 System

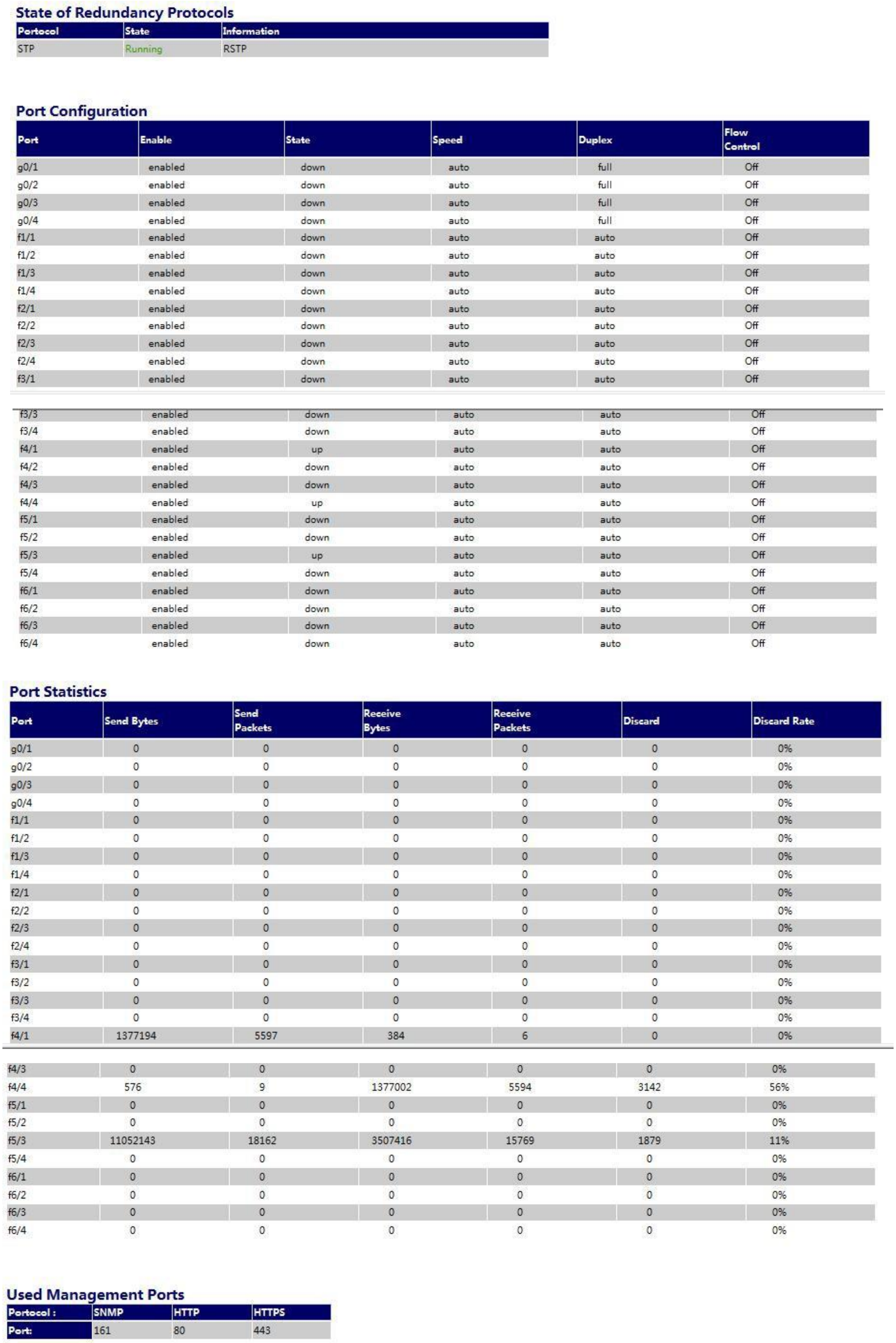
11.1.1 System Information

Click **Diagnostics -> System -> System Information** at navigation bar in order, and then enter the configuration page as following：



System Information

Name	Switch
Device Type	Switch
Serial No.	20043303473
MAC Address	3029.BE01.7E15
IP Address	192.168.2.1
CPU Usage	19%
Memory Usage	57%
Power Supply 1	Abnormal
Power Supply 2	Normal
Uptime	0 Day ,2:7:29
Current Time	1970-1-1 2:7:28
Temperature(℃)	39



State of Redundancy Protocols

Portocol	State	Information
STP	Running	RSTP

Port Configuration

Port	Enable	State	Speed	Duplex	Flow Control
g0/1	enabled	down	auto	full	Off
g0/2	enabled	down	auto	full	Off
g0/3	enabled	down	auto	full	Off
g0/4	enabled	down	auto	full	Off
f1/1	enabled	down	auto	auto	Off
f1/2	enabled	down	auto	auto	Off
f1/3	enabled	down	auto	auto	Off
f1/4	enabled	down	auto	auto	Off
f2/1	enabled	down	auto	auto	Off
f2/2	enabled	down	auto	auto	Off
f2/3	enabled	down	auto	auto	Off
f2/4	enabled	down	auto	auto	Off
f3/1	enabled	down	auto	auto	Off
f3/3	enabled	down	auto	auto	Off
f3/4	enabled	down	auto	auto	Off
f4/1	enabled	up	auto	auto	Off
f4/2	enabled	down	auto	auto	Off
f4/3	enabled	down	auto	auto	Off
f4/4	enabled	up	auto	auto	Off
f5/1	enabled	down	auto	auto	Off
f5/2	enabled	down	auto	auto	Off
f5/3	enabled	up	auto	auto	Off
f5/4	enabled	down	auto	auto	Off
f6/1	enabled	down	auto	auto	Off
f6/2	enabled	down	auto	auto	Off
f6/3	enabled	down	auto	auto	Off
f6/4	enabled	down	auto	auto	Off

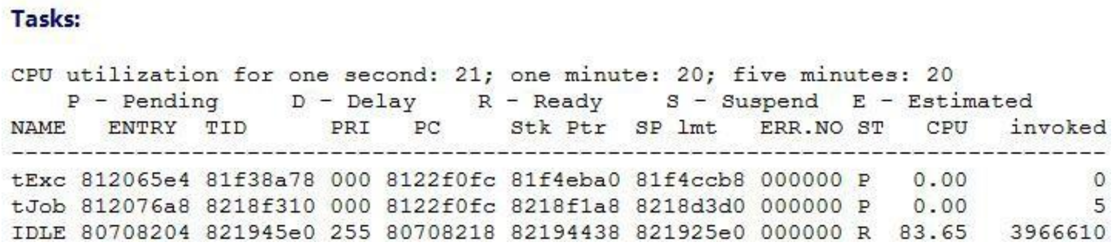
Port Statistics

Port	Send Bytes	Send Packets	Receive Bytes	Receive Packets	Discard	Discard Rate
g0/1	0	0	0	0	0	0%
g0/2	0	0	0	0	0	0%
g0/3	0	0	0	0	0	0%
g0/4	0	0	0	0	0	0%
f1/1	0	0	0	0	0	0%
f1/2	0	0	0	0	0	0%
f1/3	0	0	0	0	0	0%
f1/4	0	0	0	0	0	0%
f2/1	0	0	0	0	0	0%
f2/2	0	0	0	0	0	0%
f2/3	0	0	0	0	0	0%
f2/4	0	0	0	0	0	0%
f3/1	0	0	0	0	0	0%
f3/2	0	0	0	0	0	0%
f3/3	0	0	0	0	0	0%
f3/4	0	0	0	0	0	0%
f4/1	1377194	5597	384	6	0	0%
f4/3	0	0	0	0	0	0%
f4/4	576	9	1377002	5594	3142	56%
f5/1	0	0	0	0	0	0%
f5/2	0	0	0	0	0	0%
f5/3	11052143	18162	3507416	15769	1879	11%
f5/4	0	0	0	0	0	0%
f6/1	0	0	0	0	0	0%
f6/2	0	0	0	0	0	0%
f6/3	0	0	0	0	0	0%
f6/4	0	0	0	0	0	0%

Used Management Ports

Portocol :	SNMP	HTTP	HTTPS
Port:	161	80	443

The page lists the system information、state of redundancy protocol、port configuration、port statistics 、user management port ； Click **Display more** can check more information such as CPU utilization 、task information… etc。



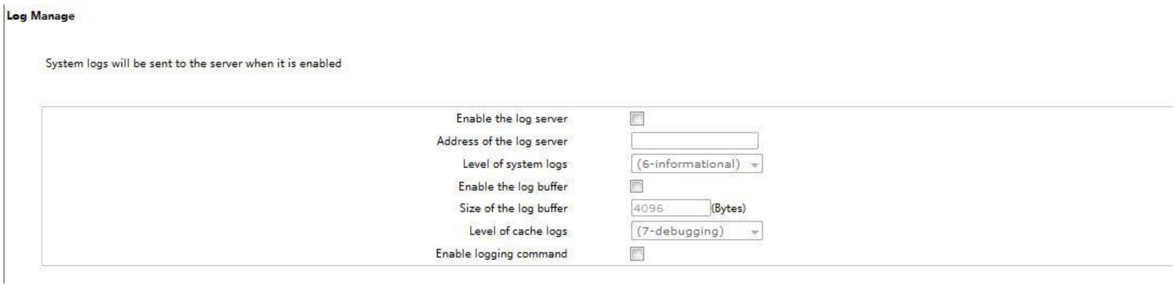
Tasks:

```
CPU utilization for one second: 21; one minute: 20; five minutes: 20
    P - Pending      D - Delay     R - Ready     S - Suspend   E - Estimated
NAME    ENTRY   TID      PRI   PC      Stk Ptr  SP lmt   ERR.NO ST   CPU   invoked
--------------------------------------------------------------------------------
tExc 812065e4 81f38a78 000 8122f0fc 81f4eba0 81f4ccb8 000000 P   0.00        0
tJob 812076a8 8218f310 000 8122f0fc 8218f1a8 8218d3d0 000000 P   0.00        5
IDLE 80708204 821945e0 255 80708218 82194438 821925e0 000000 R  83.65  3966610
```

11.2 Report

11.2.1 Log Management

Click **Diagnostics -> Report -> Log Manage** at navigation bar in order, and then enter the configuration page as following：



Log Manage

System logs will be sent to the server when it is enabled

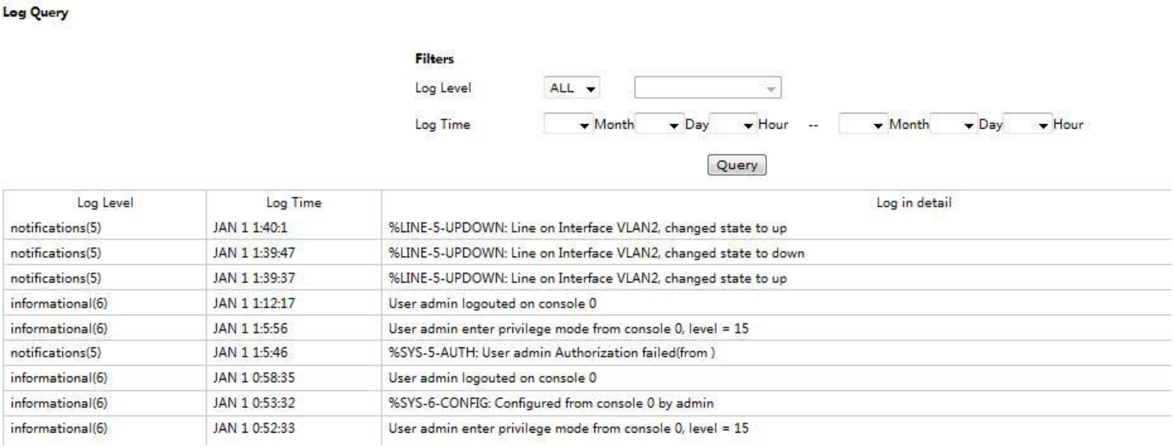
Enable the log server	□
Address of the log server	
Level of system logs	(6-informational)
Enable the log buffer	□
Size of the log buffer	4096 (Bytes)
Level of cache logs	(7-debugging)
Enable logging command	□

When **Enabling the log server** was selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the Web Configuration “**<u>Address of the system log server</u>**” textbox and select the log's grade in the “Grade of the system log information” dropdown box (grade 7 – debugging is the lowest grade of log)。

When **enabling the log buffer** was selected, the device will record the log information to the memory. By logging on to the device through the Console port or Telnet, you can run the command “**<u>show log</u>**” to browse the logs which are saved on the device. The log information saved in the memory will lost when restarting the device. Please enter the size of the buffer area in the “Size of the system log buffer” textbox and select the grade of the cached log in the “Grade of the cache log information” dropdown box。

11.2.2 Log Query

Click **Diagnostics -> Report -> Log Query** at navigation bar in order, and then enter the configuration page as following：



Log Query

Filters

Log Level ALL ▾ ▾

Log Time ▾ Month ▾ Day ▾ Hour -- ▾ Month ▾ Day ▾ Hour

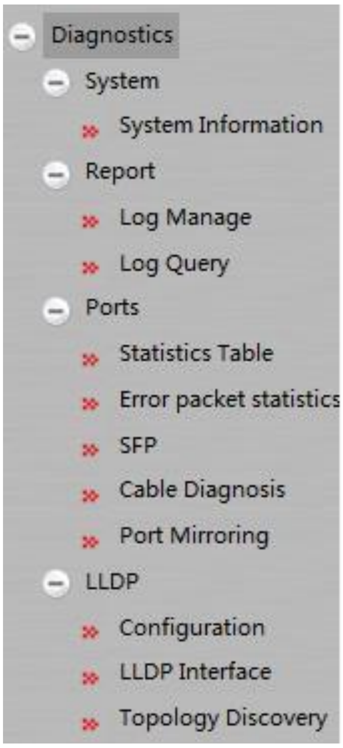
Query

Log Level	Log Time	Log in detail
notifications(5)	JAN 1 1:40:1	%LINE-5-UPDOWN: Line on Interface VLAN2, changed state to up
notifications(5)	JAN 1 1:39:47	%LINE-5-UPDOWN: Line on Interface VLAN2, changed state to down
notifications(5)	JAN 1 1:39:37	%LINE-5-UPDOWN: Line on Interface VLAN2, changed state to up
informational(6)	JAN 1 1:12:17	User admin logouted on console 0
informational(6)	JAN 1 1:5:56	User admin enter privilege mode from console 0, level = 15
notifications(5)	JAN 1 1:5:46	%SYS-5-AUTH: User admin Authorization failed(from)
informational(6)	JAN 1 0:58:35	User admin logouted on console 0
informational(6)	JAN 1 0:53:32	%SYS-6-CONFIG: Configured from console 0 by admin
informational(6)	JAN 1 0:52:33	User admin enter privilege mode from console 0, level = 15

Note：

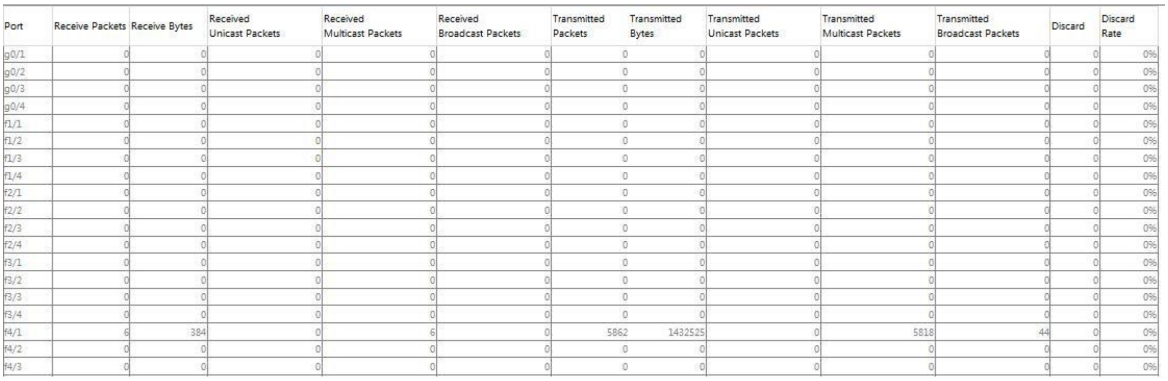
If you need more information, you can Query it by setting the log level and log time. Do not set the log time means that the query log of all time；Only set the starting time of log queries are expressed by the time for starting time log of all；only set the end time means queries are expressed by the time as the end time of all log。

11.3 Port



11.3.1 Ports Statistics Table

Click **Diagnostics -> Port -> Statistics Table** at navigation bar in order, and then enter the configuration page as following：

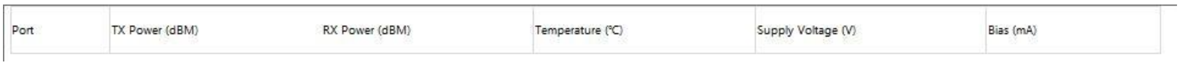


Port	Receive Packets	Receive Bytes	Received Unicast Packets	Received Multicast Packets	Received Broadcast Packets	Transmitted Packets	Transmitted Bytes	Transmitted Unicast Packets	Transmitted Multicast Packets	Transmitted Broadcast Packets	Discard	Discard Rate
g0/1	0	0	0	0	0	0	0	0	0	0	0	0%
g0/2	0	0	0	0	0	0	0	0	0	0	0	0%
g0/3	0	0	0	0	0	0	0	0	0	0	0	0%
g0/4	0	0	0	0	0	0	0	0	0	0	0	0%
f1/1	0	0	0	0	0	0	0	0	0	0	0	0%
f1/2	0	0	0	0	0	0	0	0	0	0	0	0%
f1/3	0	0	0	0	0	0	0	0	0	0	0	0%
f1/4	0	0	0	0	0	0	0	0	0	0	0	0%
f2/1	0	0	0	0	0	0	0	0	0	0	0	0%
f2/2	0	0	0	0	0	0	0	0	0	0	0	0%
f2/3	0	0	0	0	0	0	0	0	0	0	0	0%
f2/4	0	0	0	0	0	0	0	0	0	0	0	0%
f3/1	0	0	0	0	0	0	0	0	0	0	0	0%
f3/2	0	0	0	0	0	0	0	0	0	0	0	0%
f3/3	0	0	0	0	0	0	0	0	0	0	0	0%
f3/4	0	0	0	0	0	0	0	0	0	0	0	0%
f4/1	6	384	0	6	0	5862	1432525	0	5818	44	0	0%
f4/2	0	0	0	0	0	0	0	0	0	0	0	0%
f4/3	0	0	0	0	0	0	0	0	0	0	0	0%

The page lists the port information，there are included the Receive Packets、Receive Bytes、Received Unicast Packets、Received Multicast Packets、Received Broadcast Packets …etc。

11.3.2 SFP Information

Click **Diagnostics -> Port -> SFP** at navigation bar in order, and then enter the configuration page as following：

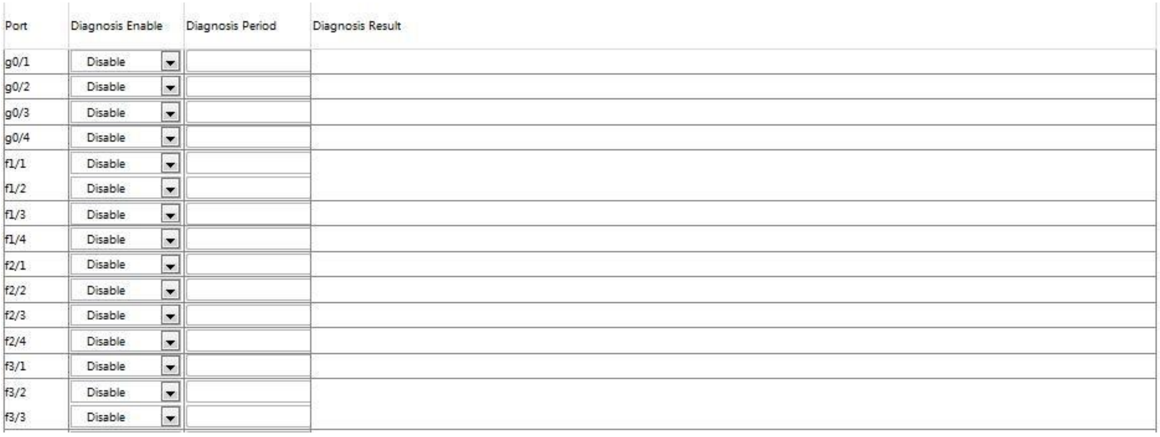


Port	TX Power (dBM)	RX Power (dBM)	Temperature (℃)	Supply Voltage (V)	Bias (mA)

Note：SFP port information can be read when the DDM has been enabled.

11.3.3 Cable Diagnosis

Click **Diagnostics -> Port -> Cable Diagnosis** at navigation bar in order, and then enter the configuration page as following：



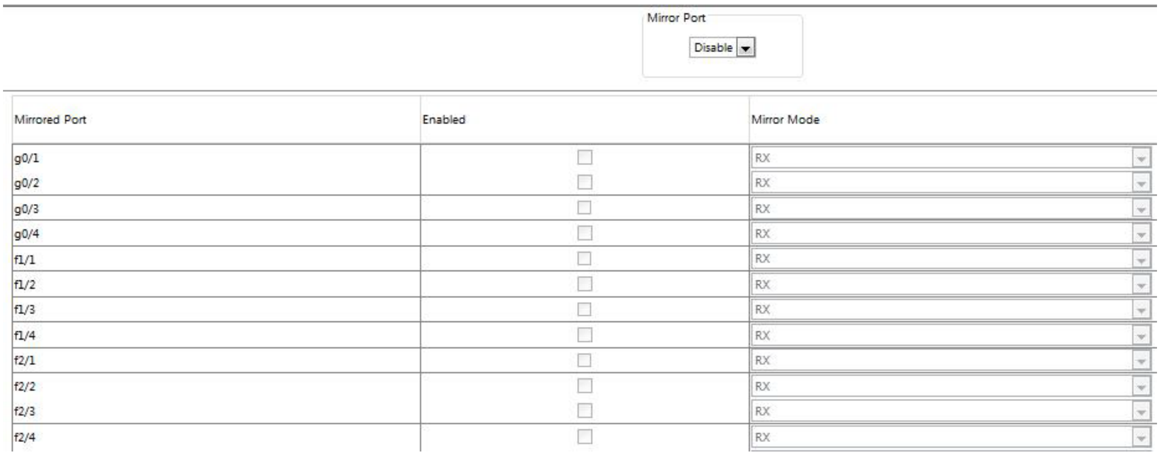
Port	Diagnosis Enable	Diagnosis Period	Diagnosis Result
g0/1	Disable		
g0/2	Disable		
g0/3	Disable		
g0/4	Disable		
f1/1	Disable		
f1/2	Disable		
f1/3	Disable		
f1/4	Disable		
f2/1	Disable		
f2/2	Disable		
f2/3	Disable		
f2/4	Disable		
f3/1	Disable		
f3/2	Disable		
f3/3	Disable		

You can configure each port of cable diagnosis is enable or disable, and also can configure the diagnosis period。

Click **Setup** to view the results of the diagnosis。

11.3.4 Port Mirroring

Click **Diagnostics -> Port -> Port Mirroring** at navigation bar in order, and then enter the configuration page as following：



Mirror Port

Disable

Mirrored Port	Enabled	Mirror Mode
g0/1	☐	RX
g0/2	☐	RX
g0/3	☐	RX
g0/4	☐	RX
f1/1	☐	RX
f1/2	☐	RX
f1/3	☐	RX
f1/4	☐	RX
f2/1	☐	RX
f2/2	☐	RX
f2/3	☐	RX
f2/4	☐	RX

Click the dropdown box right of the **Mirror Port** and select a port to be the destination port of mirror。

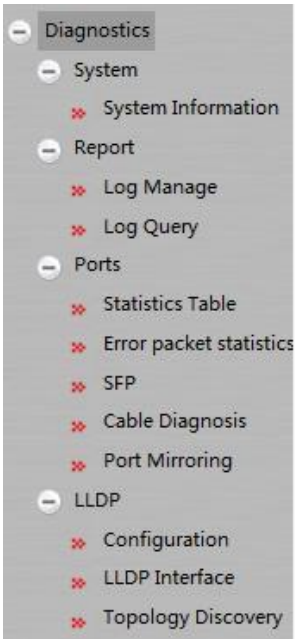
Click the checkbox and select the mirroring source port:

RX The received packets will be mirrored to the destination port 。

TX The transmitted packets will be mirrored to a destination port。

RX & TX The received and transmitted packets will be mirrored simultaneously。

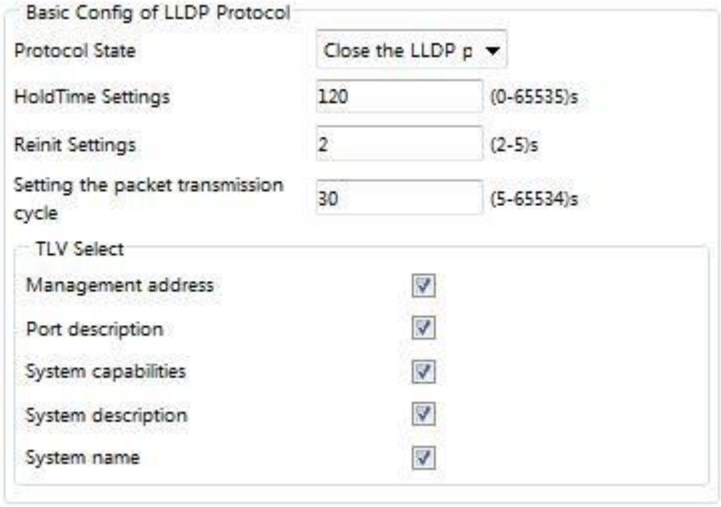
11.4 LLDP Configuration



- Diagnostics
  - System
    - System Information
  - Report
    - Log Manage
    - Log Query
  - Ports
    - Statistics Table
    - Error packet statistics
    - SFP
    - Cable Diagnosis
    - Port Mirroring
  - LLDP
    - Configuration
    - LLDP Interface
    - Topology Discovery

11.4.1 LLDP Basic Configuration

Click **Diagnostics -> LLDP -> Configuration** at navigation bar in order, and then enter the LLDP configuration page as following：



Basic Config of LLDP Protocol

Protocol State	Close the LLDP p ▾	
HoldTime Settings	120	(0-65535)s
Reinit Settings	2	(2-5)s
Setting the packet transmission cycle	30	(5-65534)s

TLV Select

Management address	☑
Port description	☑
System capabilities	☑
System description	☑
System name	☑

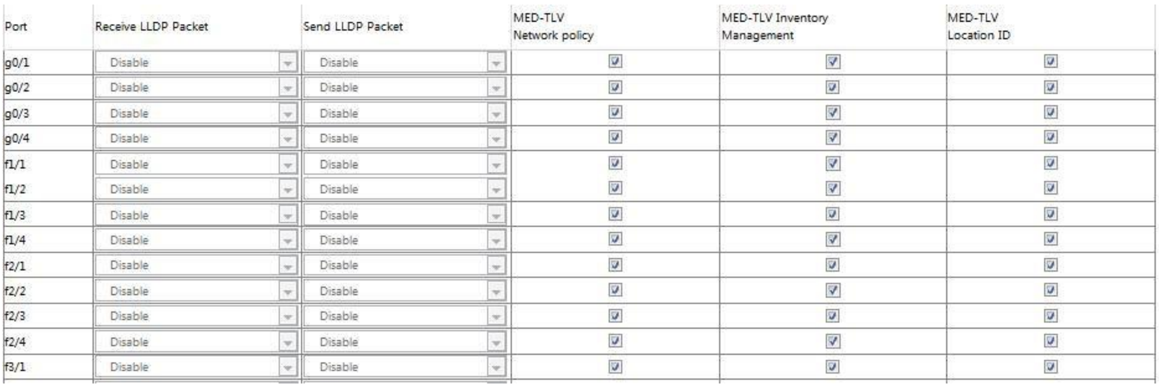
You can enable or disable the LLDP protocol. You cannot configure the LLDP protocol of the port when LLDP is disabled 。

HoldTime refers to the ttl value for transmitting the LLDP message. The default value is 120s。

Reinit refers to the transmission delay of LLDP. The default value is 2s。

11.4.2 LLDP Port Configuration

Click **Diagnostics -> LLDP -> LLDP Interface** at navigation bar in order, and then enter the LLDP port configuration page as following：

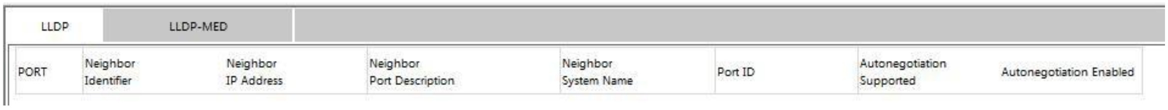


Port	Receive LLDP Packet	Send LLDP Packet	MED-TLV Network policy	MED-TLV Inventory Management	MED-TLV Location ID
g0/1	Disable	Disable	☑	☑	☑
g0/2	Disable	Disable	☑	☑	☑
g0/3	Disable	Disable	☑	☑	☑
g0/4	Disable	Disable	☑	☑	☑
f1/1	Disable	Disable	☑	☑	☑
f1/2	Disable	Disable	☑	☑	☑
f1/3	Disable	Disable	☑	☑	☑
f1/4	Disable	Disable	☑	☑	☑
f2/1	Disable	Disable	☑	☑	☑
f2/2	Disable	Disable	☑	☑	☑
f2/3	Disable	Disable	☑	☑	☑
f2/4	Disable	Disable	☑	☑	☑
f3/1	Disable	Disable	☑	☑	☑

LLDP port configuration can enable or disable the port transmitting LLDP packets，the default value was disable both of receive and send LLDP packet。The default of MED-TLV is enabled.

11.4.3 Topology Discovery

Click **Diagnostics -> LLDP -> Topology Discovery** at navigation bar in order, and then enter the LLDP topology discovery and configuration page as following：

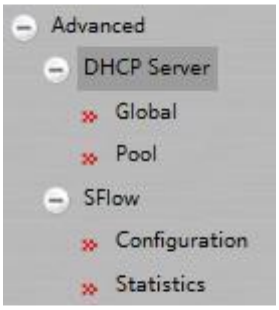


LLDP | LLDP-MED

PORT	Neighbor Identifier	Neighbor IP Address	Neighbor Port Description	Neighbor System Name	Port ID	Autonegotiation Supported	Autonegotiation Enabled

The page lists the devices that have been found。

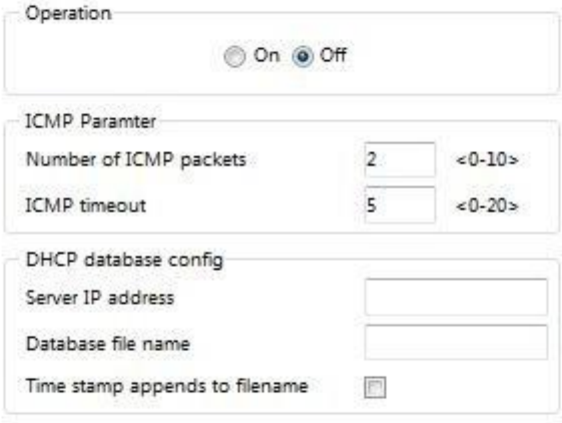
Chapter 12 Advanced



12.1 DHCP Server

12.1.1 DHCP Server Global Configuration

Click **Advanced -> DHCP Server -> Global** at navigation bar in order, and then enter the DHCP server global configuration page as following：



Operation

○ On ● Off

ICMP Paramter

Number of ICMP packets	2	<0-10>
ICMP timeout	5	<0-20>

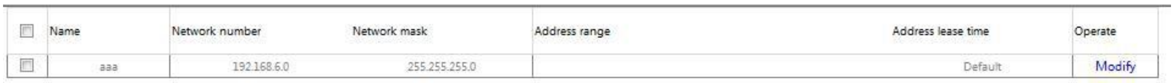
DHCP database config

Server IP address	
Database file name	
Time stamp appends to filename	□

You can enable or disable the DHCP server feature in this page。The default value is 2 for Number of ICMP packets，ICMP timeout default value is 5 seconds；BTW you also can configure the DHCP database parameters such as server IP address 、 database file name 、 time stamp appends to filename.

12.1.2 DHCP Server Pool Configuration

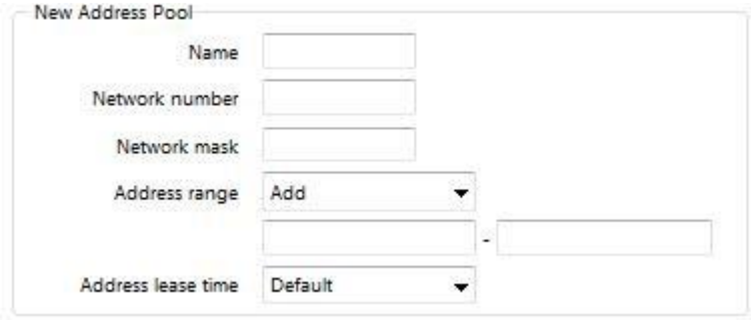
Click **Advanced -> DHCP Server -> Pool** at navigation bar in order, and then enter the DHCP server pool configuration page as following：



□	Name	Network number	Network mask	Address range	Address lease time	Operate
□	aaa	192.168.6.0	255.255.255.0		Default	Modify

The page lists the DHCP server pool information that have been configured。

Click New to create a new DHCP server pool，page as following：



New Address Pool

Name

Network number

Network mask

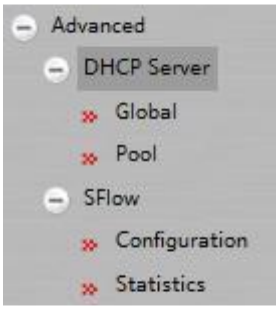
Address range Add ▾

-

Address lease time Default ▾

Click **Modify** on the right of the entry and configure the parameter of DHCP server pool。

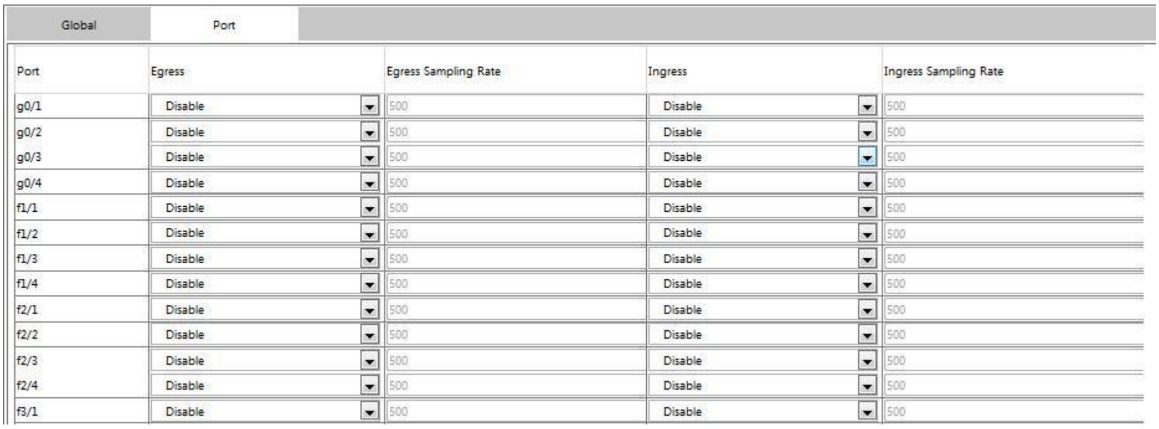
12.2 SFlow



- Advanced
  - DHCP Server
    - Global
    - Pool
  - SFlow
    - Configuration
    - Statistics

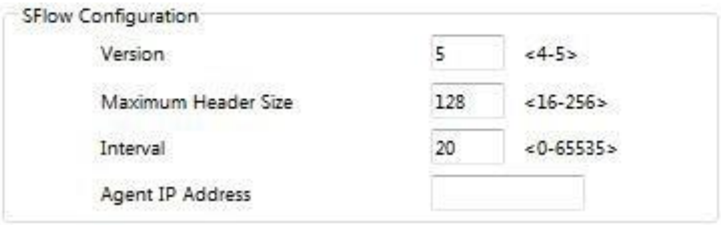
12.2.1 SFlow Global Configuration

Click **Advanced -> SFlow -> Configuration** at navigation bar in order, and then click the Global tab page enter the SFlow global configuration page as following：



Global | Port

Port	Egress	Egress Sampling Rate	Ingress	Ingress Sampling Rate
g0/1	Disable	500	Disable	500
g0/2	Disable	500	Disable	500
g0/3	Disable	500	Disable	500
g0/4	Disable	500	Disable	500
f1/1	Disable	500	Disable	500
f1/2	Disable	500	Disable	500
f1/3	Disable	500	Disable	500
f1/4	Disable	500	Disable	500
f2/1	Disable	500	Disable	500
f2/2	Disable	500	Disable	500
f2/3	Disable	500	Disable	500
f2/4	Disable	500	Disable	500
f3/1	Disable	500	Disable	500



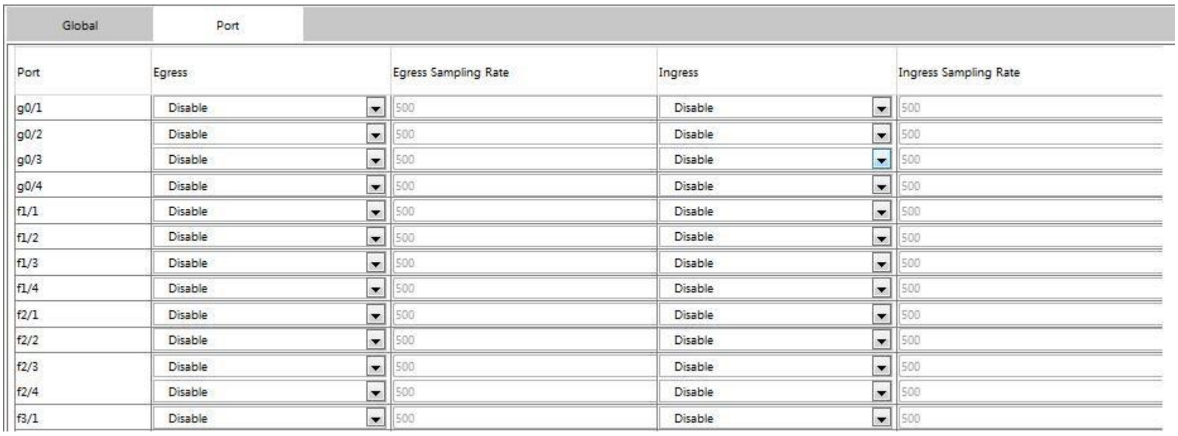
SFlow Configuration

Version	5	<4-5>
Maximum Header Size	128	<16-256>
Interval	20	<0-65535>
Agent IP Address		

You can configure the Agent IP address on this page， the default value of SFlow **Version** is 5 ；default value of **Maximum Header Size** is 20 (maximum number is 128)。

12.2.2 SFlow Port Configuration

Click **Advanced -> SFlow -> Configuration** at navigation bar in order, and then click the Port tab page enter the SFlow port configuration page as following：



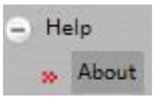
Port	Egress	Egress Sampling Rate	Ingress	Ingress Sampling Rate
g0/1	Disable	500	Disable	500
g0/2	Disable	500	Disable	500
g0/3	Disable	500	Disable	500
g0/4	Disable	500	Disable	500
f1/1	Disable	500	Disable	500
f1/2	Disable	500	Disable	500
f1/3	Disable	500	Disable	500
f1/4	Disable	500	Disable	500
f2/1	Disable	500	Disable	500
f2/2	Disable	500	Disable	500
f2/3	Disable	500	Disable	500
f2/4	Disable	500	Disable	500
f3/1	Disable	500	Disable	500

The page lists the port of SFlow enable/disable status， the default value of Egress/Ingress Sampling Rate is 500; you can configure the rate upon your requirement when it is setting to be enabled。

Chapter 13 Help

13.1 About

Click **Help -> About** at navigation bar in order，and then enter the About page as following：



The information will shown in this page which are included IOS version messages 、company website 、contact telephone… etc.

--- End of File ---