

# **Web Configuration Manual**

# Table of Contents

Web Configuration Manual .....	1
Chapter 1 Basic Configuration .....	- 1 -
1.1 HTTP protocol configuration .....	- 1 -
1.1.1 Language Selection .....	- 1 -
1.1.2 HTTP service port configuration .....	- 1 -
1.1.3 Enabling the HTTP service .....	- 1 -
1.1.4 HTTP access mode Configuration .....	- 2 -
1.1.5 Setting the Max-VLAN number to display in Web page .....	- 2 -
1.1.6 Setting the IGMP-Groups number to display in Web page .....	- 2 -
1.2 HTTPS Configuration .....	- 2 -
1.2.1 HTTPS Access Configuration .....	- 2 -
1.2.2 HTTPS Service Port Configuration .....	- 3 -
Chapter 2 Accessing Switch .....	- 4 -
2.1 Accessing the Switch Through Web .....	- 4 -
2.2 Initially Accessing the Switch .....	- 4 -
2.2.1 Upgrading to the Web-Supported Version .....	- 5 -
2.3 Accessing Switch Through Secure Links .....	- 5 -
2.4 Introduction of Web Interface .....	- 6 -
2.4.1 Top Control Bar .....	- 6 -
2.4.2 Navigation Bar .....	- 6 -
2.4.3 Configuration Display Area .....	- 7 -
2.4.4 Bottom Control Bar .....	- 7 -
Chapter 3 Basic Configuration .....	- 8 -
3.1 System .....	- 8 -
3.2 Global Configuration Mode (Management Interface) .....	- 8 -
3.3 Port Configuration .....	- 9 -
3.4 Auto-Shutdown .....	- 9 -
3.5 Software .....	- 10 -
3.6 Load/Save .....	- 10 -
3.7 Restart .....	- 11 -
3.8 Factory Settings .....	- 11 -
Chapter 4 Security .....	- 12 -
4.1 User Management .....	- 12 -
4.1.1 User Management .....	- 12 -
4.1.2 Group Management .....	- 13 -

---

4.1.3	Password Rule Management .....	- 13 -
4.1.4	Author Rule Management .....	- 14 -
4.1.5	Authentication Rule Management .....	- 15 -
4.2	Management Access .....	- 15 -
4.2.1	Server .....	- 15 -
4.2.2	SNMP Community Management (SNMPv1/v2 community) .....	- 16 -
4.2.3	SNMPv3 Configuration .....	- 17 -
4.2.4	CLI ( Command Line Interface ) .....	- 18 -
4.3	Port Security .....	- 18 -
4.3.1	IP MAC Binding .....	- 19 -
4.3.2	Static MAC Filter Mode .....	- 19 -
4.3.3	Static MAC Filter .....	- 20 -
4.3.4	Dynamic MAC Mode .....	- 21 -
4.4	Switchport Protect .....	- 21 -
4.5	Keepalive .....	- 22 -
4.6	802.1X Port Authentication .....	- 23 -
4.6.1	Global .....	- 23 -
4.6.2	Authentication List .....	- 24 -
4.6.3	Port Configuration .....	- 24 -
4.6.4	Statistics .....	- 25 -
4.7	RADIUS .....	- 25 -
4.7.1	Global .....	- 25 -
4.7.2	Service .....	- 25 -
Chapter 5	Time .....	- 27 -
5.1	Basic Setting .....	- 27 -
5.2	NTP .....	- 27 -
5.3	PTP Configuration .....	- 28 -
5.3.1	Global .....	- 28 -
5.3.2	Port Configuration .....	- 28 -
5.3.3	Unicast .....	- 29 -
Chapter 6	Network Security .....	- 30 -
6.1	DOS Configuration .....	- 30 -
6.1.1	DOS Global Configuration .....	- 30 -
6.2	DHCP Snooping Configuration .....	- 30 -
6.2.1	DHCP Snooping Global Configuration .....	- 30 -
6.2.2	DHCP Snooping VLAN Configuration .....	- 31 -
6.2.3	DHCP Snooping Interface Configuration .....	- 32 -
6.2.4	DHCP Snooping Bindings .....	- 32 -

---

6.3	Access Control List .....	- 33 -
6.3.1	IPv4 Rules .....	- 33 -
6.3.2	MAC Rules .....	- 34 -
6.3.3	Assignment .....	- 35 -
6.4	Filter Function .....	- 35 -
Chapter 7	Switching .....	- 37 -
7.1	Storm Control .....	- 37 -
7.1.1	Broadcast Storm Control .....	- 37 -
7.1.2	Multicast Storm Control .....	- 37 -
7.1.3	Unicast Storm Control .....	- 38 -
7.2	Port Rate Limits .....	- 38 -
7.3	MAC Address Table .....	- 39 -
7.4	IGMP Snooping .....	- 40 -
7.4.1	IGMP Snooping Configuration .....	- 40 -
7.4.2	IGMP-Snooping VLAN .....	- 41 -
7.4.3	Static Multicast Mac Address Configuration .....	- 41 -
7.4.4	Multicast list .....	- 42 -
7.5	VLAN .....	- 42 -
7.5.1	VLAN configuration .....	- 42 -
7.5.2	VLAN Batch Configuration .....	- 43 -
7.5.3	Port VLAN Configuration .....	- 44 -
7.6	GMRP .....	- 45 -
7.6.1	VLAN List .....	- 45 -
7.6.2	Port Configuration .....	- 46 -
7.6.3	Multicast List .....	- 46 -
Chapter 8	Routing .....	- 48 -
8.1	VLAN Interface and IP Address Configuration .....	- 48 -
8.2	VRRP Configuration .....	- 49 -
8.3	IP Express Forwarding .....	- 49 -
8.4	Static ARP .....	- 50 -
8.5	Static Route .....	- 50 -
8.6	RIP Configuration .....	- 51 -
8.6.1	RIP Configuration .....	- 51 -
8.6.2	RIP Router Entries .....	- 52 -
8.7	OSPF Configuration .....	- 52 -
8.7.1	OSPF process .....	- 52 -
8.7.2	OSPF Router Entries .....	- 53 -
Chapter 9	QoS/Priority .....	- 54 -

---

9.1	Global .....	- 54 -
9.2	Port Configuration .....	- 54 -
9.3	802.1D/p Mapping .....	- 55 -
9.4	IP DSCP Mapping .....	- 55 -
9.5	Queue Management .....	- 56 -
Chapter 10	Redundancy .....	- 57 -
10.1	Link Aggregation Configuration .....	- 57 -
10.1.1	Port Aggregation Configuration .....	- 57 -
10.1.2	Port Channel Global Loading Balance .....	- 58 -
10.2	Backup Link .....	- 58 -
10.2.1	Backup Link Global Configuration .....	- 58 -
10.2.2	Link Backup Protocol Port Configuration .....	- 59 -
10.3	Spanning Tree .....	- 60 -
10.3.1	Global .....	- 60 -
10.3.2	MSTP .....	- 61 -
10.3.3	Spanning Tree Ports .....	- 62 -
10.4	EAPS (ether-ring) .....	- 63 -
10.5	MEAPS .....	- 65 -
10.6	ERPS .....	- 66 -
10.7	CFM Function .....	- 67 -
10.7.1	Global .....	- 67 -
10.7.2	Interface Configuration .....	- 68 -
Chapter 11	Diagnostics .....	- 70 -
11.1	System .....	- 70 -
11.1.1	System Information .....	- 70 -
11.2	Report .....	- 71 -
11.2.1	Log Management .....	- 71 -
11.2.2	Log Query .....	- 72 -
11.3	Ports .....	- 72 -
11.3.1	Statistics Table .....	- 72 -
11.3.2	Error Packet Statistics .....	- 73 -
11.3.3	SFP .....	- 73 -
11.3.4	Cable Diagnosis .....	- 74 -
11.3.5	Port Mirroring .....	- 74 -
11.4	LLDP Configuration .....	- 74 -
11.4.1	LLDP Basic Configuration .....	- 75 -
11.4.2	LLDP Interface .....	- 75 -
11.4.3	Topology Discovery .....	- 75 -

Chapter 12	Advanced .....	- 77 -
12.1	DHCP Server .....	- 77 -
12.1.1	DHCP Server Global Configuration .....	- 77 -
12.1.2	DHCP Server Pool Configuration .....	- 77 -
12.2	SFlow .....	- 78 -
12.2.1	SFlow Global Configuration .....	- 78 -
12.2.2	SFlow Statistics .....	- 79 -
Chapter 13	Help .....	- 80 -
13.1	About .....	- 80 -

## Chapter 1 Basic Configuration

### 1.1 HTTP protocol configuration

Switches support not only can be 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

Currently, there are two languages in the Industrial Switch: you may choose English or Chinese. User can set the language in the global configuration mode through the command line 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 would 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 { <i>portNumber</i> }	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 number 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 { <i>max-vlan</i> }	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 is the max value, default value is 15).

Command	Description
ip http web igmp-groups { <i>igmp-groups</i> }	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 mode



### 1.2.2 HTTPS Service Port Configuration

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

Command	Description
<code>ip http secure-port {portNumber}</code>	Setting the HTTPS port number

## Chapter 2 Accessing Switch

### 2.1 Accessing the Switch Through Web

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

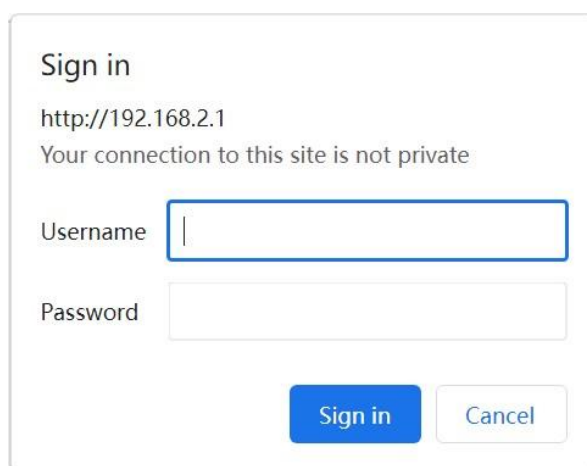
- HTML of version 4.0
- HTTP of version 1.1
- JavaScript™ of version 1.5

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



The image shows a 'Sign in' dialog box with the following elements:

- Title: Sign in
- Address: http://192.168.2.1
- Warning: Your connection to this site is not private
- Username field: A text input box with a blue border and a vertical cursor.
- Password field: A text input box.
- Buttons: A blue 'Sign in' button and a light blue 'Cancel' button.

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, then 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 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 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 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 <b>write</b> 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 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 “Diagnostics” and then “Ports”, “Statistics Table”.

---

**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 “System” will appear.

---

### 2.4.3 Configuration Display Area

User Management		Group Management		Pass Management		Author Management		Authen Management	
<input type="checkbox"/>	User name	User permission	Pass-Group	Authen-Group	Author-Group	User Status	Operate		
<input type="checkbox"/>	admin	System administrator				Normal	<a href="#">Modify</a>		

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.

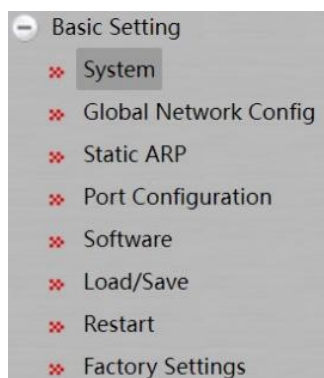
### 2.4.4 Bottom Control Bar



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

Set	<p>Apply the modified configuration to the device.</p> <p>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” on the top control bar.</p>
Reload	Refresh the content shown in the current configuration area.
Create	Create a list item. For example, you can create a VLAN item or a new user.
Delete	Delete an item in the list.
Go Back	Go back to the previous-level configuration page.
Clear	Clear the content of current configuration, such as statistics of port.

## Chapter 3 Basic Configuration



### 3.1 System

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

System Data	
Name	<input type="text" value="Switch"/>
Location	<input type="text"/>
Contact	<input type="text"/>
Device Type	<input type="text"/>
Serial No.	<input type="text" value="90009301762"/>
MAC Address	<input type="text" value="3029.BE30.3A65"/>
IP Address	<input type="text" value="192.168.2.1"/>
CPU Usage	<input type="text" value="18%"/>
Memory Usage	<input type="text" value="28%"/>
Power Supply 1	<input type="text" value="Normal"/>
Power Supply 2	<input type="text" value="Abnormal"/>
Uptime	<input type="text" value="0 Day ,0:46:31"/>
Temperature(°C)	<div><div><div></div><div></div><div></div></div><div><input type="text" value="-15"/> <input type="text" value="35"/> <input type="text" value="115"/></div><div><div></div><div></div><div></div></div></div>

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" in the bottom control bar.

### 3.2 Global Configuration Mode (Management Interface)

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

Port	Description	Enable	Status	Speed	Current Speed	Duplex	Flow Control	Medium
g1/1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g1/2		<input type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g1/3		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g1/4		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g1/5		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g1/6		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g1/7		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g1/8		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g2/1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g2/2		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g2/3		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g2/4		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g2/5		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto
g2/6		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto	100Mb/s	Auto	Off	Auto
g2/7		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto	---	Auto	Off	Auto

Set
Reload

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 Auto-Shutdown

Click **Basic Setting -> auto-shutdown** in the navigation bar, the auto-shutdown page appears, as shown as below:

Global	
Delay	0 <0-600>
PORT	
Port Configuration Enable Auto Shutdown function	
GigaEthernet1/1	<input type="checkbox"/>
GigaEthernet1/2	<input type="checkbox"/>
GigaEthernet1/3	<input type="checkbox"/>
GigaEthernet1/4	<input type="checkbox"/>
GigaEthernet1/5	<input type="checkbox"/>
GigaEthernet1/6	<input type="checkbox"/>
GigaEthernet1/7	<input type="checkbox"/>
GigaEthernet1/8	<input type="checkbox"/>
GigaEthernet2/1	<input type="checkbox"/>
GigaEthernet2/2	<input type="checkbox"/>
GigaEthernet2/3	<input type="checkbox"/>
GigaEthernet2/4	<input type="checkbox"/>
GigaEthernet2/5	<input type="checkbox"/>
GigaEthernet2/6	<input type="checkbox"/>
<div style="text-align: right;"> <input type="button" value="Set"/> <input type="button" value="Reload"/> </div>	

This page set the auto-shutdown port and delay time of shutdown. Click the **Set** in the bottom control bar to complete the configuration, and click the **Save** on the top. The corresponding port will be shutdown in delayed time after the switch turned on.

### 3.5 Software

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

Version	
Running Version	Switch.bin, 2.0.2I Build 88942, 2021-9-29 16:16:27 by USER-2016031 <input type="button" value="Export"/>
ROM Version	0.5.0
Software Update	
File	<input type="button" value="选择文件"/> 未选择任何文件 <input type="button" value="Update"/>

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 will be valid only if the device is restarted.

---

### 3.6 Load/Save

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

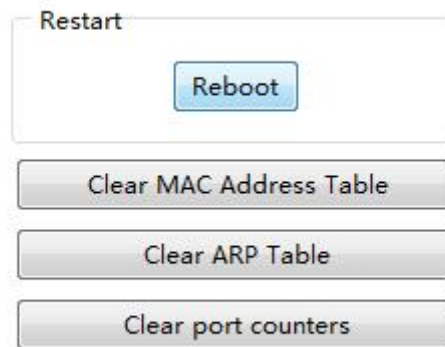
Save	
Current configuration file	startup-config <input type="button" value="Export"/>
Load	
Import startup-config file	<input type="button" value="选择文件"/> 未选择任何文件 <input type="button" value="Import"/>
Reboot is required after importing startup-config!	

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



### 3.7 Restart

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



You can choose “Reboot” to reboot the switch, or choose “Clear MAC Address Table”, “Clear ARP Table”, “Clear port counters”.

### 3.8 Factory Settings



On this page you can reset the equipment to factory setting, click the “Restore” button to reset to factory setting.

# 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 Management			Group Management		Pass Management		Author Management		Authen Management	
<input type="checkbox"/>	User name	User permission	Pass-Group	Authen-Group	Author-Group	User Status	Operate			
<input type="checkbox"/>	admin	System administrator				Normal	<a href="#">Modify</a>			

Click **Modify** to change user's configuration at this page, and click **Delete** at the bottom bar to delete the selected user.

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

User name	<input type="text"/>
Password	<input type="text"/>
Confirming password	<input type="text"/>
Pass-Group	<input type="text"/>
Authen-Group	<input type="text"/>
Author-Group	<input type="text"/>

Fill in configuration at every configuration column and click **Set** at the bottom bar to create new user. Click **Reload** to refresh the user information. And click **Go Back** to go back to previous level page.

### 4.1.2 Group Management

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

User Management		Group Management		Pass Management	Author Management		Authen Management
<input type="checkbox"/>	Serial Number	Group Name	Pass-Group Rule	Authen-Group Rule	Author-Group Rule	Detail	Operate
<input type="checkbox"/>	1	group	1	3	2	<a href="#">Detail</a>	<a href="#">Modify</a>

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

User Management		Group Management		Pass Management	Author Management		Authen Management
<input type="checkbox"/>	Serial Number	User Name	Pass-Group Name	Authen-Group Name	Author-Group Name	User Status	Operate

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

User Group Name	<input type="text"/>
Pass-Group Name	<input type="text"/>
Authen-Group Name	<input type="text"/>
Author-Group Name	<input type="text"/>

Fill in configuration at every configuration column and click **Set** at the bottom bar to create a 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:

User Management		Group Management			Pass Management		Author Management			Authen Management
<input type="checkbox"/>	Serial Number	Pass-Group Name	Same as the username	Min Length	Validity	Number	Lower-letter	Upper-letter	Special-character	Operate
<input type="checkbox"/>	1	1	Can be same	2		Yes	Yes	Yes	Yes	<a href="#">Modify</a>

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

Click **Create** at the bottom bar to enter the following configuration page:

Pass-Group Name	<input type="text"/>
Same as Username	<input type="text" value="Can"/>
Contain Number	<input type="text" value="Must"/>
Contain Lower-letter	<input type="text" value="Must"/>
Contain Upper-letter	<input type="text" value="Must"/>
Contain Special-character	<input type="text" value="Must"/>
Min Length	<input type="text"/> (1-127)
Validity	<input type="text" value="0"/> d <input type="text" value="0"/> h <input type="text" value="0"/> m <input type="text" value="0"/> s

Fill in configuration at every configuration column and click **Set** 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:

User Management		Group Management		Pass Management	Author Management	Authen Management
<input type="checkbox"/>	Serial Number	Author-Group Name		Precedence		Operate
<input type="checkbox"/>	1	1		System administrator		<a href="#">Modify</a>

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

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

Author-Group Name	<input type="text"/>
Precedence	<input type="text" value="System administrator"/>

Fill in configuration at every configuration column and click **Set** 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
<input type="checkbox"/>	Serial Number	Authen-Group Name	Max try times	Duration for all tries
<input type="checkbox"/>	1	1		
				<a href="#">Modify</a>

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

Click **Create** 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 Management Access

### 4.2.1 Server

HTTP, HTTPS, SSH and SNMP could be configured at this page. Click **Security -> Management Access -> Server** 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:

Click **SNMP** to configure SNMP related:

HTTP

HTTPS

SSH

SNMP

Configuration

Port

Packetsize

TrapTimeout

Beating trap Interval

HTTP

HTTPS

SSH

SNMP

Operation

☐ ON
 ☒ OFF

Configuration

TimeOut

#### 4.2.2 SNMP Community Management (SNMPv1/v2 community)

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

SNMP Community				
SNMP Host				
<input type="checkbox"/>	SNMP Community Name	SNMP Community Encryption	SNMP Community Attribute	Operate
<input type="checkbox"/>	snmp1	False	RO	<a href="#">Modify</a>
<input type="checkbox"/>	snmp2	False	RO	<a href="#">Modify</a>

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

Click **Create** to create a new SNMP Community:

SNMP Community

SNMP Host

SNMP Community Name

Input less than 20 characters

SNMP Community Attribute

Read Only

▼

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

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

SNMP Community					
SNMP Host					
<input type="checkbox"/>	SNMP Host IP	SNMP Community String	SNMP Message Type	SNMP Community Version	Operate
<input type="checkbox"/>	192.168.0.1	snmp1	Traps	v1	<a href="#">Modify</a>
<input type="checkbox"/>	192.168.0.2	snmp2	Traps	v1	<a href="#">Modify</a>

Click **Create** to create a new SNMP Host:

SNMP Host IP	<input type="text"/>
SNMP Community	<input type="text"/>
SNMP Message Type	Traps ▼ <span>Informs is not supported in version v1</span>
SNMP Community Version	v1 ▼

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

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

### 4.2.3 SNMPv3 Configuration

Click **Security -> Management Access -> SNMPv3 Configuration** at navigation bar in order to enter configuration page as following:

SNMPv3 Group Config	SNMPv3 User Config			
<input type="checkbox"/>	Group Name	Security Level	Operate	
<input type="checkbox"/>	group	noauth	<a href="#">Modify</a>	

Click the **Modify** to change the features of SNMPv3 Group Configuration.

Click the **Reload** at the bottom control bar to refresh the configuration information of SNMPv3 Group.

Click **Create** to create a new configuration for SNMPv3 Group:

SNMPv3 Group Configuration

Group Name	<input type="text"/>
Security Level	noauth ▼

Click **SNMPv3 User Config** to enter the following configuration page:

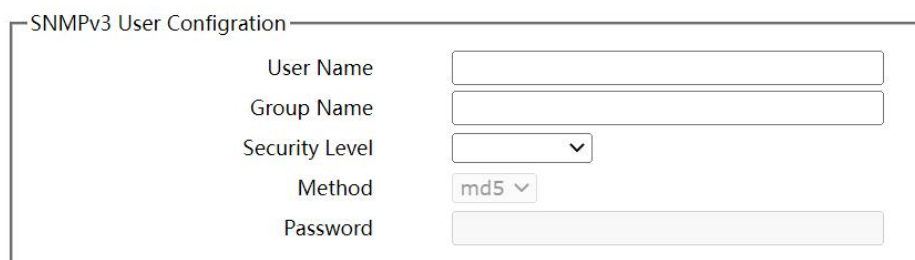
SNMPv3 Group Config	SNMPv3 User Config					
<input type="checkbox"/>	User Name	Group Name	Security Level	Method	Password	Operate
<input type="checkbox"/>	aaa	1	auth	md5	12345678	<a href="#">Modify</a>

[Reload](#) [Create](#) [Delete](#)

Click **Modify** to change the features of SNMPv3 User Configuration.

Click **Reload** at the bottom control bar to refresh the information of SNMPv3 User Configuration.

Click **Create** to create new configuration of SNMPv3:



SNMPv3 User Configuration

User Name	<input type="text"/>
Group Name	<input type="text"/>
Security Level	<input type="text" value="↓"/>
Method	<input type="text" value="md5"/>
Password	<input type="password"/>

Click **Delete** at bottom control bar to delete the selected configuration information of SNMPv3 Group.

#### 4.2.4 CLI ( Command Line Interface )

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



GLOBAL Login Banner

Configuration  
Time Out(sec)

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:



GLOBAL Login Banner

Banner Text

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

### 4.3 Port Security



### 4.3.1 IP MAC Binding

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

IP MAC Binding	Static Mac Filter Mode	Static Mac Filter	Dynamic Mac Mode
Interface Name	Operate		
g1/1	<a href="#">Detail</a>		
g1/2	<a href="#">Detail</a>		
g1/3	<a href="#">Detail</a>		
g1/4	<a href="#">Detail</a>		
g1/5	<a href="#">Detail</a>		
g1/6	<a href="#">Detail</a>		
g1/7	<a href="#">Detail</a>		
g1/8	<a href="#">Detail</a>		
g2/1	<a href="#">Detail</a>		
g2/2	<a href="#">Detail</a>		
g2/3	<a href="#">Detail</a>		
g2/4	<a href="#">Detail</a>		
g2/5	<a href="#">Detail</a>		
g2/6	<a href="#">Detail</a>		
g2/7	<a href="#">Detail</a>		
g2/8	<a href="#">Detail</a>		

Click **Detail** to check the IP MAC binding information of that port.

<input type="checkbox"/>	Serial number	IP Address	MAC Address	Operate
<input type="checkbox"/>	1	192.168.0.1	1001.1002.1003	<a href="#">Modify</a>
<input type="checkbox"/>	2	192.168.0.2	0002.0003.0004	<a href="#">Modify</a>

Click **Modify** to change the selected binding items of the IP MAC.

Click **Reload** to refresh the configuration of the IP MAC binding.

Click **Create** to create a new IP MAC binding item.

Enter a new IP address

Enter a new MAC

Click **Delete** at the bottom control bar to delete the selected IP MAC binding item.

### 4.3.2 Static MAC Filter Mode

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

IP MAC Binding	Static Mac Filter Mode	Static Mac Filter	Dynamic Mac Mode
Interface Name	Port Mode	Static MAC Filtration Mode	
g1/1	Access	Disable ▾	
g1/2	Access	Disable ▾	
g1/3	Access	Disable ▾	
g1/4	Access	Disable ▾	
g1/5	Access	Disable ▾	
g1/6	Access	Disable ▾	
g1/7	Access	Disable ▾	
g1/8	Access	Disable ▾	
g2/1	Access	Disable ▾	
g2/2	Access	Disable ▾	
g2/3	Access	Disable ▾	
g2/4	Access	Disable ▾	
g2/5	Access	Disable ▾	
g2/6	Access	Disable ▾	
g2/7	Access	Disable ▾	
g2/8	Access	Disable ▾	

Set
Reload

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

### 4.3.3 Static MAC Filter

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

IP MAC Binding	Static Mac Filter Mode	Static Mac Filter	Dynamic Mac Mode
Interface Name	Operate		
g1/1	<a href="#">Detail</a>		
g1/2	<a href="#">Detail</a>		
g1/3	<a href="#">Detail</a>		
g1/4	<a href="#">Detail</a>		
g1/5	<a href="#">Detail</a>		
g1/6	<a href="#">Detail</a>		
g1/7	<a href="#">Detail</a>		
g1/8	<a href="#">Detail</a>		
g2/1	<a href="#">Detail</a>		
g2/2	<a href="#">Detail</a>		
g2/3	<a href="#">Detail</a>		
g2/4	<a href="#">Detail</a>		
g2/5	<a href="#">Detail</a>		
g2/6	<a href="#">Detail</a>		
g2/7	<a href="#">Detail</a>		
g2/8	<a href="#">Detail</a>		

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

	Serial number	MAC Address	Operate
	1	1001.1002.1003	<a href="#">Modify</a>

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

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

Static MAC Address

Click **Delete** at bottom control bar to delete the selected static MAC filtration items.

### 4.3.4 Dynamic MAC Mode

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

IP MAC Binding	Static Mac Filter Mode	Static Mac Filter	Dynamic Mac Mode
Interface Name	Dynamic MAC Filtration Mode	Max MAC Address	
g1/1	Disable ▾	1 (1-4095)	
g1/2	Disable ▾	1 (1-4095)	
g1/3	Disable ▾	1 (1-4095)	
g1/4	Disable ▾	1 (1-4095)	
g1/5	Disable ▾	1 (1-4095)	
g1/6	Disable ▾	1 (1-4095)	
g1/7	Disable ▾	1 (1-4095)	
g1/8	Disable ▾	1 (1-4095)	
g2/1	Disable ▾	1 (1-4095)	
g2/2	Disable ▾	1 (1-4095)	
g2/3	Disable ▾	1 (1-4095)	
g2/4	Disable ▾	1 (1-4095)	
g2/5	Disable ▾	1 (1-4095)	
q2/6	Disable ▾	1 (1-4095)	

Set Go back

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

## 4.4 Switchport Protect

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

Port Protect Configuration		Port Protect List
Port	Port Protect Group	
g1/1		
g1/2		
g1/3		
g1/4		
g1/5		
g1/6		
g1/7		
g1/8		
g2/1		
g2/2		
g2/3		
g2/4		
g2/5		
q2/6		

Set Reload

Set the Port Protect Group at this page, click **Set** at the bottom control bar to finish the setting.

Click **Reload** to refresh the port protection group information.

Click "Port Protect List", enter the Port Protect Group Creating page:

Port Protect Configuration		Port Protect List
<input type="checkbox"/>	Port Protect Group 1	
<input type="checkbox"/> Select All/Select None		
No.1 Page/Total 1 Page   First   Prev   Next   Last   Go No. <input type="text"/> Page   Search: <input type="text"/>		Current 1 Item/Total 1 Item

**Help**

#Port Protect Group 0 is Default Port Protect Group, and it can not be deleted.

[Reload](#) [Create](#) [Delete](#)

Click **Reload** at the bottom control bar, refresh the Port Protect Group information.

Click **Delete** at the bottom control bar, delete the selected port protect group.

Click **Create** at the bottom control bar, enter the Port Protect Group Creating page:

Port Protect Configuration		Port Protect List
<div style="border: 1px solid black; padding: 10px; margin: 20px auto; width: 300px;">           Create Port Protect Group <input style="width: 100%;" type="text"/> </div>		

[Set](#) [Reload](#) [Go back](#)

Click **Set** at the bottom control bar, to finish the setting.

Click **Reload** at the bottom control bar, refresh the Port Protect Group Creating page.

Click **Go Back** at the bottom control bar, go back to the “Port Protect List” page.

## 4.5 Keepalive

Click **Security -> Keepalive** at navigation bar in order to enter port status configuration page as following:

Port	Status	Keepalive Period
g1/1	Enable ▾	(0-32767)S
g1/2	Enable ▾	(0-32767)S
g1/3	Enable ▾	(0-32767)S
g1/4	Enable ▾	(0-32767)S
g1/5	Enable ▾	(0-32767)S
g1/6	Enable ▾	(0-32767)S
g1/7	Enable ▾	(0-32767)S
g1/8	Enable ▾	(0-32767)S
g2/1	Enable ▾	(0-32767)S
g2/2	Enable ▾	(0-32767)S
g2/3	Enable ▾	(0-32767)S
g2/4	Enable ▾	(0-32767)S
g2/5	Enable ▾	(0-32767)S
g2/6	Enable ▾	(0-32767)S
g2/7	Enable ▾	(0-32767)S

Set Reload

Click **Set** at the bottom control bar after configuration, to finish the port status setting.

Click **Reload** at the bottom control bar, refresh the port setting information.

## 4.6 802.1X Port Authentication

### 4.6.1 Global

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

Operation

☐ On
☒ Off

Configuration

Guest VLAN

☐

Vendor permit

☐

Re-authentication

☐

Parameters

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 port authentication at this page.

## 4.6.2 Authentication List

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

<input type="checkbox"/>	Name	Method 1	Method 2	Method 3	Method 4
<input type="checkbox"/>	zx	local			
<input type="checkbox"/>	scc	group radius	group tacacs+	group 1	

Click **Reload** at the bottom control bar, to refresh the authentication list.

Click **Delete** at the bottom control bar, to delete the selected port authentication list.

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

**New Authentication Entry**

Name

Method 1

group ▼ radius ▼

Method 2

▼ ▼

Method 3

▼ ▼

Method 4

▼ ▼

## 4.4.3 Port Configuration

Click **Security -> 802.1X Port Authentication -> Port 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
g1/1	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g1/2	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g1/3	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g1/4	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g1/5	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g1/6	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g1/7	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g1/8	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g2/1	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g2/2	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g2/3	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g2/4	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g2/5	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g2/6	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	
g2/7	Force authorized ▼	<input type="checkbox"/>	Eap ▼	Single hosts ▼	<input type="checkbox"/>	<1-4094>	

Set Reload

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

### Note:

Some configurations can only be configured when 802.1x port authentication is enabled.

## 4.6.4 Statistics

Click **Security -> 802.1X Port Authentication -> Statistics** 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
g1/1	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g1/2	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Multiple hosts ▾	<input type="checkbox"/>	<1-4094>	
g1/3	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Multiple Authenticate ▾	<input type="checkbox"/>	<1-4094>	
g1/4	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g1/5	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g1/6	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g1/7	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g1/8	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g2/1	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g2/2	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g2/3	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g2/4	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g2/5	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g2/6	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	
g2/7	Force authorized ▾	<input type="checkbox"/>	Eap ▾	Single hosts ▾	<input type="checkbox"/>	<1-4094>	

Set
Reload

All ports' statistic information of 802.1x messages could be checked at this page.

## 4.7 RADIUS

### 4.7.1 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.

### 4.7.2 Service

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

<input type="checkbox"/>	Address	Authentication port	Accounting port
<input type="checkbox"/>	192.168.2.7	1812	1813

---

[Set](#) [Reload](#) [Create](#) [Delete](#)

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

Click **Set** at the bottom control bar, to finish the setting.

Click **Reload** at the bottom control bar, refresh the authentication port and accounting port information.

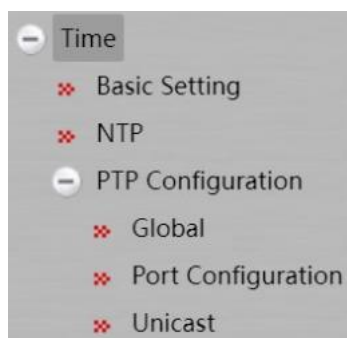
Click **Delete** at the bottom control bar, to delete the selected authentication port and accounting port information of RADIUS Server.

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

Server Ip Address:



## Chapter 5 Time



### 5.1 Basic Setting

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

 A screenshot of the 'System Time' configuration page. At the top, there is a text box displaying the current system time '1970-01-01 00:31:35' and a 'Refresh' button. Below this, there is a 'Select Time-Zone' dropdown menu currently set to '(GMT)Greenwich Mean Time,Dublin,London,Lisbon'. Further down, there is a checkbox labeled 'Set Time Manually'. Below the checkbox, there are input fields for 'Set Time' with values: Year '1970', Month '01', Day '00', Hour '31', Minute(s) '35', and Second.

Click **Reload** 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:

 A screenshot of the 'Network Time Synchronization' configuration page. It features a checkbox labeled 'NTP Master Primary'. Below this, there are three input fields for NTP servers, labeled 'NTP Server One', 'NTP Server Two', and '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:

The screenshot displays the PTP Global Configuration interface, organized into several sections:

- PTP Basic Config:**
  - Device Type: Boundary (dropdown)
  - PTP Settings: Disable PTP (dropdown)
  - Load Protocol: Ethernet Protocol (dropdown)
  - Domain Filtration Settings: Close (dropdown)
  - The timeout of delay\_req record: 5 (text input)
- Setting the default PTP data set:**
  - Default Priority1: 128 (text input)
  - Default Priority2: 128 (text input)
  - Default Domain: 0 (text input)
- PTP Time Properties Settings:**
  - Offset Between UTC And TAI: 0 (text input)
  - Leap59: 0 (dropdown)
  - Leap61: 0 (dropdown)
  - Timetraceable: 0 (dropdown)
- Regulator Settings:**
  - Freqtraceable: 0 (dropdown)
  - Timescale: 1 (dropdown)
  - Timesource: 160 (text input)
  - Proportion Constant: 2 (text input)
  - Integration Constant: 10 (text input)
  - Differentiation Constant: 0 (text input)
- Sync Process Mechanism:**
  - Domain 0: Straight Forward (dropdown)
  - Domain 1: Straight Forward (dropdown)
  - Domain 2: Straight Forward (dropdown)
  - Domain 3: Straight Forward (dropdown)
- Clock Frequency Synchronization:**
  - Synchronization Settings: Enable (dropdown)

Enabling/disabling PTP and PTP basic setting, default PTP data set, PTP Time Properties Settings, Regulator Settings, Sync Process Mechanism and Clock Frequency Synchronization can be configured at this page. Click **Set** at the bottom control bar at settings, to finish the setting.

Click **Reload** at the bottom control bar, refresh the PTP Global Configuration.

### 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 ▾
g0/5	False ▾	ethernet ▾	p2p ▾	Enable ▾	1 ▾	10 ▾	-1 ▾	-1 ▾
g0/6	False ▾	ethernet ▾	p2p ▾	Enable ▾	1 ▾	10 ▾	-1 ▾	-1 ▾
g0/7	False ▾	ethernet ▾	p2p ▾	Enable ▾	1 ▾	10 ▾	-1 ▾	-1 ▾
g0/8	False ▾	ethernet ▾	p2p ▾	Enable ▾	1 ▾	10 ▾	-1 ▾	-1 ▾

Set Reload

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. Click **Reload** at the bottom control bar, refresh the configuration of each port.

**Note:**

This page could only be configured after PTP protocol is enable.

### 5.3.3 Unicast

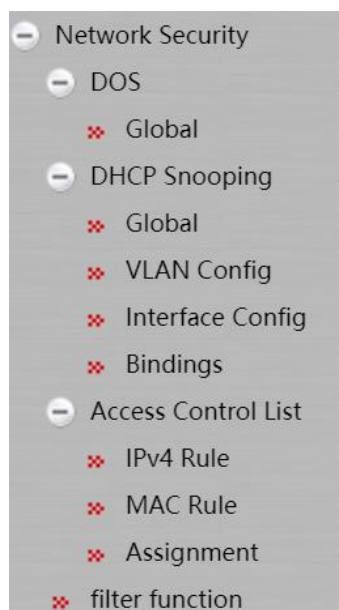
Click **Time -> PTP -> Unicast** at navigation bar in order to enter configuration page as following:

<input type="checkbox"/>	Port	Unicast State	IP Address	Operate
--------------------------	------	---------------	------------	---------

Delete

Unicast status and IP address of each port could be checked and the unicast state of each port could be changed 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:

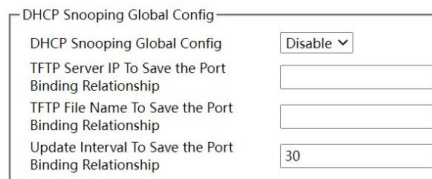
Preventing DOS Attack	
ICMP DOS attack checking	<input type="checkbox"/>
Drop IP packets if source ip equal destination ip	<input type="checkbox"/>
Checking on first fragment ip packets	<input type="checkbox"/>
Drop packets if TCP/UDP source port equal destination port	<input type="checkbox"/>
Drop if packets with MACSA equal MACDA	<input type="checkbox"/>
Drop TCP packets with invalid TCP flags	<input type="checkbox"/>
Checking TCP DOS fragment attack	<input type="checkbox"/>

You could set or cancel the related Preventing DOS Attack according to needs. Click **Set** 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:

**Help**

#Please remove the binding item and then close the snooping DHCP protocol

Set Reload

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 Config** at navigation bar in order to enter DHCP Snooping VLAN configuration page as following:



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 Interface Configuration

Click **Network Security -> DHCP Snooping -> Interface Config** 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	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
g0/2	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
g0/3	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
g0/4	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f1/1	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f1/2	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f1/3	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f1/4	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f2/1	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f2/2	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f2/3	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>
f2/4	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>

If a port is configured as the DHCP-trusted port, the DHCP messages 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.

### 6.2.4 DHCP Snooping Bindings

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

<input type="checkbox"/>	MAC Address	IP Address	Interface Name	VLAN
<input type="checkbox"/>	00:00:00:00:00:00	192.168.2.6	GigaEthernet1/1	2

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 to the network. The “no” command can be used to delete the binding entries.

Entries bound manually proceed over those bindings 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 binding entries of a port.

Click "Create" 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

### 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:

<input type="checkbox"/>	Name of the IP ACL	Attribute of the IP ACL	Operate
<input type="checkbox"/>	22	standard	<a href="#">Detail</a>

Reload Create Delete

Click **Delete** at the bottom control bar, delete the selected access control list.

Click **Detail** on the right of the table to enter the IP Access Control List page.

<input type="checkbox"/>	Authority	Src IP	Src IP Mask	Record the log	Operate
<input type="checkbox"/>	permit	any			<a href="#">Modify</a>

---

[Reload](#) [Create](#) [Delete](#) [Go back](#)

Click **Modify** on this page, to configure the rules of corresponding IP Access Control list.

Click **Go Back** on the IP Access Control List page to go back to IPv4 Rules' Page.

Click **Create** to create an IP access control list.

Name of the IP ACL	<input type="text" value="tom"/>
Attribute	<input type="text" value="standard"/>

Click **Delete** to delete the access control list.

### 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:

<input type="checkbox"/>	Name of the MAC Access Control List	Operate
<input type="checkbox"/>	33	<a href="#">Detail</a>

---

[Reload](#) [Create](#) [Delete](#)

Click **Create** at the bottom control bar to create a MAC access control list. Click **Delete** to delete the selected access control list.

Name of the MAC ACL	<input type="text"/>
---------------------	----------------------



### 6.3.3 Assignment

Click **Network Security -> Access Control List -> Assignment** 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				

## 6.4 Filter Function

Click **Network Security -> Filter Function** at navigation bar in order to enter the filter function global page as following:

Global
port configuration
statistics

operation

☐ on
☒ off

Filter Global configuration

filter period(s) 10
arp filter threshold 1000
bpdu filter threshold 1000
erps filter threshold 1000
dhcp filter threshold 1000
filter block-time(s) 300

Help
#Only global and ports are configured, the filter function to be effective.

Set
Reload

Click **Set** at the bottom control bar to finish the global configuration of filter function.

Click **Reload** at the bottom control bar to refresh the global configuration of filter function.

Click "Port Configuration" on the right of "Global", enter the port configuration page as follows:

Global	port configuration				statistics
interface	arp	bpd	erps	DHCP	
g0/1	Disable	Disable	Disable	Disable	
g0/2	Disable	Disable	Disable	Disable	
g0/3	Disable	Disable	Disable	Disable	
g0/4	Disable	Disable	Disable	Disable	
g0/5	Disable	Disable	Disable	Disable	
g0/6	Disable	Disable	Disable	Disable	
g0/7	Disable	Disable	Disable	Disable	
g0/8	Disable	Disable	Disable	Disable	

Set Reload

Click **Set** at the bottom control bar, to finish the configuration of port.

Click **Reload** at the bottom control bar, refresh the port configuration of filter function.

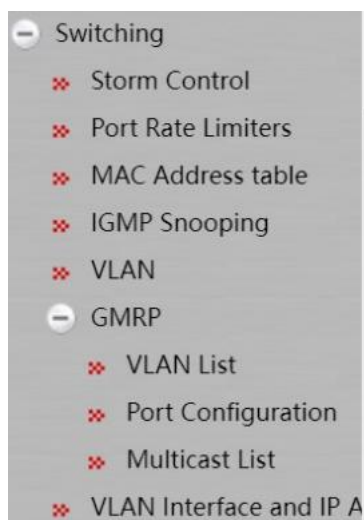
Click “Statistics” on the right of “Port Configuration” enter the statistics page of filters blocked and filters counting as following:

Global	port configuration		statistics			
Filters blocked						
Cause	Address	Seconds(s)	Discard	Rate	Polling	Interface
Filters counting						
Cause	Address	Seconds(s)	Count	Interface		

Reload

Click **Reload** at the bottom control bar, refresh the filters blocked and filters accounting information.

## Chapter 7 Switching



### 7.1 Storm Control

Click **Switching** -> **Storm Control** at navigation bar in order to enter broadcast storm control, multicast storm control and unicast storm control configuration pages.

#### 7.1.1 Broadcast 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	

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 value of the broadcast packets. The legal threshold range for each port is given behind the threshold.

#### 7.1.2 Multicast 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

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 value of the multicast packets. The legal threshold range for each port is given behind the threshold.

### 7.1.3 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 value of the unicast packets. The legal threshold range for each port is given behind the threshold.

## 7.2 Port Rate Limits

Click **Switching -> Port Rate Limits** at navigation bar in order to enter port rate limit page 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)

Set rate-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 Table

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

Static MAC address table		Aging configuration			
<input type="checkbox"/>	Index	Static MAC Address	VLAN ID	Port	Operate
<input type="checkbox"/>	1	2222.2222.2222	2	G0/1	<a href="#">Modify</a>

[Reload](#) [Create](#) [Delete](#)

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

<b>Static MAC Address</b>		0000.0000.0000
<b>VLAN ID</b>		1
<b>Configured Port List</b> <div>g0/1</div>	<div>&gt;&gt;</div> <div>&lt;&lt;</div>	<b>Available Port List</b> <div> g0/2  g0/3  g0/4  f1/1  f1/2  f1/3  f1/4  f2/1  f2/2  f2/3 </div>

Click “Aging Configuration” on the right of “Static MAC Address Table”, enter the aging configuration page:

Static MAC address table	Aging configuration
--------------------------	---------------------

Aging Configuration

Aging time(s)

**Help**  
 #Permitted scope of aging time: 10-1000000s, fill 0 means is disabled aging

## 7.4 IGMP Snooping

### 7.4.1 IGMP Snooping Configuration

Click Switching -> 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

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

IGMP Snooping	IGMP Snooping Vlan	Static Multicast Mac	Multicast list	
<input type="checkbox"/>	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router Port
<input type="checkbox"/>	2	Running	Disable	g0/1(static); <a href="#">Modify</a>

[Reload](#) [Create](#) [Delete](#)

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

VLAN ID

2

Status of the IGMP Snooping Vlan

Enable

Immediate-leave

Disable

Configured Mrouter Port List

g0/4

>>

<<

Available Port List

g0/1  
g0/2  
g0/3  
f1/1  
f1/2  
f1/3  
f1/4  
f2/1  
f2/2  
f2/3

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 **Switching -> IGMP Snooping**, at navigation bar in order, and select “Static Multicast Address” tab page to enter static multicast address page as following:

IGMP Snooping	IGMP Snooping Vlan	Static Multicast Mac	Multicast list
<b>Static Multicast Address Config</b>			
VLAN ID	<input type="text"/>		
Multicast IP Address	<input type="text"/>		
Assignment Port	<input type="text"/>		
<b>Static Multicast List Info</b>			
<input type="checkbox"/>	VLAN ID	Group	Port

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

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

#### 7.4.4 Multicast list

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

IGMP Snooping	IGMP Snooping Vlan	Static Multicast Mac	Multicast list
	VLAN ID	Group	Type
	6	235.2.3.1	USER
			Port
			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 **Reload** 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 **Switching -> VLAN**, at navigation bar in order, and select "VLAN configuration" tab page to enter VLAN configuration page as following:



Vlan Configuration	Vlan Batch Configuration	Port Vlan	
<input type="checkbox"/>	VLAN ID	VLAN Name	Operate
<input type="checkbox"/>	1	Default	<a href="#">Modify</a>
<input type="checkbox"/>	2	VLAN0002	<a href="#">Modify</a>

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

Select the check box before item and click **Delete** at the bottom control bar 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 **Create** 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 **Switching -> VLAN**, at navigation bar in order, and select "VLAN Batch Configuration" tab page to enter VLAN configuration page as following:

Vlan Configuration	Vlan Batch Configuration	Port Vlan
<div>VLAN Configured 1-12</div> <div>VLAN Add <input type="text"/></div> <div>VLAN Delete <input type="text"/></div>		
<p><b>Help</b></p> <p>#VLAN ID(1-4094), such as (1,3,5,7) Or (1,3-5,7) Or (1-7) Or (1 3,5 7-9)</p> <p>#Delete VLAN:Can only delete the created VLAN</p>		
<div>Set Reload</div>		

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

### 7.5.3 Port VLAN Configuration

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

Vlan Configuration	Vlan Batch Configuration	Port Vlan			
Port Name	PVID	Mode	VLAN-allowed Range	VLAN-untagged Range	Operate
g0/1	1	Access	1-4094	1	<a href="#">Modify</a>
g0/2	1	Access	1-4094	1	<a href="#">Modify</a>
g0/3	1	Access	1-4094	1	<a href="#">Modify</a>
g0/4	1	Access	1-4094	1	<a href="#">Modify</a>
f1/1	1	Access	1-4094	1	<a href="#">Modify</a>
f1/2	1	Access	1-4094	1	<a href="#">Modify</a>
f1/3	1	Access	1-4094	1	<a href="#">Modify</a>
f1/4	1	Access	1-4094	1	<a href="#">Modify</a>
f2/1	1	Access	1-4094	1	<a href="#">Modify</a>
f2/2	1	Access	1-4094	1	<a href="#">Modify</a>
f2/3	1	Access	1-4094	1	<a href="#">Modify</a>
f2/4	1	Access	1-4094	1	<a href="#">Modify</a>
f3/1	1	Access	1-4094	1	<a href="#">Modify</a>
f3/2	1	Access	1-4094	1	<a href="#">Modify</a>
f3/3	1	Access	1-4094	1	<a href="#">Modify</a>
f3/4	1	Access	1-4094	1	<a href="#">Modify</a>
f4/1	1	Access	1-4094	1	<a href="#">Modify</a>

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.

Vlan Configuration

Vlan Batch Configuration

Port Vlan

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

VLAN-untagged Range	1	
Add the VLAN-untagged range		
Remove the VLAN-untagged range		

Help

#VLAN-allowed and VLAN-untagged: (1-4094), such as (1,3,5,7) Or (1,3-5,7) Or (1-7) Or (1 3,5 7-9)

#Allowed-VLAN and Untagged-VLAN: First execute the 'Add' action and then the 'Remove' action

#Do not press the **Enter** key.

SetReloadGo back

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

7.6 GMRP

7.6.1 VLAN List

Click **Switching -> GMRP -> VLAN List** at navigation bar in order, to enter port VLAN configuration page as following:

<input type="checkbox"/>	Serial number	GMRP VLAN ID
<input type="checkbox"/>	1	1

ReloadCreateDelete

This page shows the ID list information of GMRP VLAN. Click **Reload** at the bottom control bar to refresh the list.

Click **Create** at the bottom control bar, create GMRP VLAN configuration.

New GMRP VLAN

Configuration method

Specify VLAN

GMRP VLAN

#When the configuration mode is **Default VLAN**, It is to enable GMRP on vlan <1-16>. If vlan number is bigger than 16, only the firstly configured 16 vlans are effective

#GMRP VLAN (1-4094), such as vlan (1,3,5,7), vlan (1,3-5,7), vlan (1-7), or (1 3,5 7-9)

SetGo back

7.6.2 Port Configuration

Click **Switching -> GMRP -> Port Configuration** at navigation bar in order, to enter Port Configuration page as following:

Port Name	GMRP Status	GMRP Status	GMRP Frames Received	GMRP Frames Transmitted	GMRP Frames Discarded	GMRP Last Pdu Origin
g0/1	Enable	Enabled	0	0	0	0000.0000.0000
g0/2	Enable	Enabled	0	0	0	0000.0000.0000
g0/3	Enable	Enabled	0	0	0	0000.0000.0000
g0/4	Enable	Enabled	0	0	0	0000.0000.0000
g0/5	Enable	Enabled	0	0	0	0000.0000.0000
g0/6	Enable	Enabled	0	0	0	0000.0000.0000
g0/7	Enable	Enabled	0	0	0	0000.0000.0000
g0/8	Enable	Enabled	0	0	0	0000.0000.0000

**Help**  
#Before enabling GMRP on port, please config GMRP VLAN first.

SetReload

Click **Set** at the bottom control bar, finish the configuration.

7.6.3 Multicast List

Click **Switching -> GMRP -> Multicast List** at navigation bar in order, to enter Multicast List page as following:

---

Index	VLAN ID	Multicast MAC Address	Port
-------	---------	-----------------------	------

---

Reload

This page shows the VLAN ID, multicast MAC address and member port information of GMRP multicast list. Click **Reload** at the bottom control bar, refresh the multicast list information.

## 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:

<input type="checkbox"/>	Name of the VLAN Interface	IP Attribute	IP Address	Directed-Broadcast	Operate
<input type="checkbox"/>	1	Manual Config	192.168.2.1/24;	off	<a href="#">Modify</a>
<input type="checkbox"/>	2	Manual Config	182.168.0.2/24;	off	<a href="#">Modify</a>

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

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

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

You can change the VLAN name when you click the “Create” 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

Directed-Broadcast

Manual Config

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

#### Help

#The primary IP must be configured for the VLAN interface before the secondary IP is configured

[Set](#) [Reload](#) [Go back](#)

#### Note:

Before setting the VLAN secondary IP address, you need to set the Primary IP Address first.

## 8.2 VRRP Configuration

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

<input type="checkbox"/>	VLAN ID	VRRP ID	VRRP Description	Virtual IP Address	Priority	Operate
<input type="checkbox"/>	1	2		192.168.2.8/24	2	<a href="#">Modify</a>

[Reload](#) [Create](#) [Delete](#)

Click **Reload** at the bottom control bar, refresh VRRP list information.

Click **Delete** at the bottom control bar, delete the selected VRRP configuration information.

Click **Create** at the bottom control bar, to enter new VRRP configuration page:

VRRP Configuration

VLAN ID

VRRP Group ID

Virtual IP Address

Mask

Priority

VRRP Other Configuration

Authentication

VRRP Description

VRRP Preempt ☒ On ☐ Off

Source-Mac-Use-System ☐ On ☒ Off

### Help

#If priority is not configured,the default priority is 100  
#VRRP Other Configuration can not set

[Set](#) [Reload](#) [Go back](#)

Click **Set** at the bottom control bar, finish the configuration of VRRP and other information.

Click **Go Back** at the bottom control bar, back to the VRRP List Page.

## 8.3 IP Express Forwarding

Click **Routing -> IP Express Forwarding** at navigation bar in order, and then enter IP Express Forwarding switch page as following:

IP Express Forwarding

☒ On
 ☐ Off

Click **Set** at the bottom control bar, to finish the setting of IP Express Forwarding.

Click **Reload** at the bottom control bar, refresh the information of IP Express Forwarding information.

## 8.4 Static ARP

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

<input type="checkbox"/>	IP Address	MAC Address	Interface VLAN	Operate
<input type="checkbox"/>	192.168.6.77	00:22:33:44:55:66	1	<a href="#">Modify</a>
<input type="checkbox"/>	192.168.4.77	00:00:00:00:00:00	1	<a href="#">Modify</a>

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

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

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

ARP Config

IP Address

MAC Address

Interface VLAN

## 8.5 Static Route

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

<input type="checkbox"/>	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
<input type="checkbox"/>	true			Null0			192.168.2.7	5	3	false	4	<a href="#">Modify</a>

[Reload](#) [Create](#) [Delete](#)

Click **Modify** to modify the current Static Route.

Click **Reload** to refresh the static route information.

Click **Delete** to delete the selected Static Route items.

Click **Create** to create a new Static Route.



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

Note:  
Only the Layer3 switches have the static route configuration page.

## 8.6 RIP Configuration

### 8.6.1 RIP Configuration

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

RIP Configuration	RIP Router Entries			
<input type="checkbox"/>	Process ID	Auto-Summary	Version	Operate
<input type="checkbox"/>	22222	on	V1	<a href="#">Edit</a>

[Reload](#) [Create](#) [Delete](#)

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 **Create** to create a new RIP process.

Creating the RIP Process

RIP Process	<input type="text"/>
Auto-Summary	<input checked="" type="radio"/> On <input type="radio"/> Off
Version	default ▼

## 8.6.2 RIP Router Entries

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

RIP Configuration   RIP Router Entries

RIP Route Config

RIP Process

Enter the created RIP process ID, Click **Set** to enter the selected RIP Router Entries page.

RIP Configuration		RIP Router Entries	
	Interface	Mask	Address
	VLAN1	255.255.255.0	192.168.2.1

Click **Create** to create a new RIP Router Entries of selected RIP process.

RIP Configuration   RIP Router Entries

RIP Process ID1

VLAN Interface

## 8.7 OSPF Configuration

### 8.7.1 OSPF process

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

OSPF Process	OSPF Router Entries	
		Process ID
<input type="checkbox"/>		1
<input type="checkbox"/>		6

You should have created a OSPF process firstly, before to do the OSPF Router Entries configuration otherwise cannot do any editing.

Click **Create** to entry the RIP process creating page.

The screenshot shows the 'OSPF Router Entries' tab in the configuration interface. A dialog box titled 'Creating the OSPF Process' is open, containing a label 'OSPF Process' and an empty text input field.

## 8.7.2 OSPF Router Entries

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

The screenshot shows the 'OSPF Router Entries' tab. A dialog box titled 'OSPF Route Config' is open, containing a label 'OSPF Process' and an empty text input field.

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

	OSPF Process	OSPF Router Entries			
			Network Number	Mask	Area
<input type="checkbox"/>			192.169.5.0	255.255.255.0	1

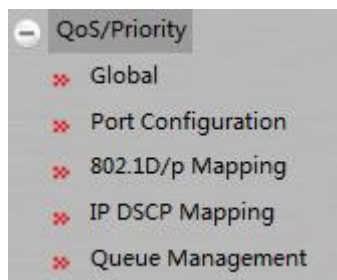
Click **Create** to create the OSPF Router Entries of OSPF process selected.

The screenshot shows the 'OSPF Router Entries' tab. A dialog box titled 'OSPF Process ID' is open, containing three input fields labeled 'Network Number', 'Mask', and 'Area'.

**Help**  
#The area can be an integer or IP

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

## Chapter 9 QoS/Priority



### 9.1 Global

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

QoS Global	
Schedule Policy	<input type="text" value="sp"/>
Default CoS Value	<input type="text" value="0"/>
Trust Priority	<input type="text" value="cos"/>

#### Help

#The 'sp' means Strict Priority

#The 'wrr' means Weighted Round Robin

#The 'drr' means Deficit Round Robin

#The 'fcfs' means First come, first served

#The 'wfq' means Weighted Fair Queueing.

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	<input type="text"/>
g0/2	<input type="text"/>
g0/3	<input type="text"/>
g0/4	<input type="text"/>
f1/1	<input type="text"/>
f1/2	<input type="text"/>
f1/3	<input type="text"/>
f1/4	<input type="text"/>
f2/1	<input type="text"/>
f2/2	<input type="text"/>
f2/3	<input type="text"/>
f2/4	<input type="text"/>
f3/1	<input type="text"/>
f3/2	<input type="text"/>

You can set the Port CoS value by port, and then click **Set** to save the changes.

### 9.3 802.1D/p Mapping

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 **Set** to save all 802.1D/p mapping configurations.

### 9.4 IP DSCP Mapping

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 set the mapping value per each DSCP.

Click **Clear** and then clean all of the DSCP mapping configuration.

Note:

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

## 9.5 Queue Management

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

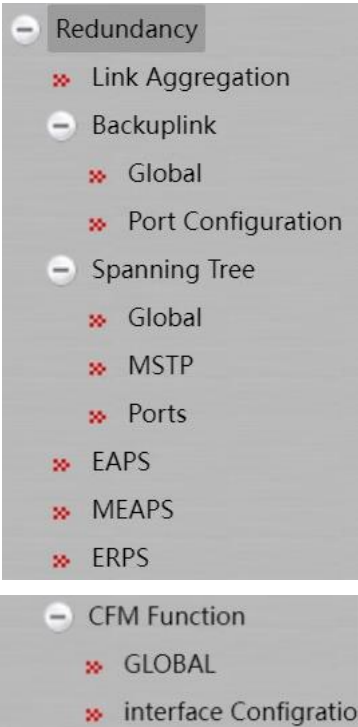
Click **Set** to save all configuration.

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 set the bandwidth weight to Zero value. then the weight value of the other queue ID must must be set to Zero.

# Chapter 10 Redundancy



## 10.1 Link Aggregation Configuration

### 10.1.1 Port Aggregation Configuration

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

Port Channel		Port Channel Global Loading Balance					
<input type="checkbox"/>	Aggregation Group	Mode	Configure port members	Valid port members	Speed	State	Operate
<input type="checkbox"/>	p1	Static	g1/1,g1/2			down	<a href="#">Modify</a>

Create Delete

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

Click **Create** 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.

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 “>>”.

## 10.1.2 Port Channel Global Loading Balance

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

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

Port Channel Global Loading Balance	
Port Channel	Loading Balance Mode
p1	SRC MAC

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

## 10.2 Backup Link

### 10.2.1 Backup Link Global Configuration

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



<input type="checkbox"/>	Group ID	Preemption Mode	Preemption Delay	Operate
<input type="checkbox"/>	2	No Preemption		<a href="#">Modify</a>

---

[Create](#) [Delete](#)

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

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

Group ID

Preemption Mode

No Preemption ▼

Preemption Delay

---

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.
- 

### 10.2.2 Link Backup Protocol Port Configuration

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

Interface Name	Group ID	Interface Attribute	MMU Attribute	Shareload VLAN	Operate
f1/4					<a href="#">Modify</a>
f2/1					<a href="#">Modify</a>
f2/2					<a href="#">Modify</a>
f2/3					<a href="#">Modify</a>
f2/4					<a href="#">Modify</a>
f3/1					<a href="#">Modify</a>
f3/2					<a href="#">Modify</a>
f3/3					<a href="#">Modify</a>
f3/4					<a href="#">Modify</a>
f4/1					<a href="#">Modify</a>
f4/2					<a href="#">Modify</a>
f4/3					<a href="#">Modify</a>
f4/4					<a href="#">Modify</a>
f5/1					<a href="#">Modify</a>
f5/2					<a href="#">Modify</a>
f5/3					<a href="#">Modify</a>
f5/4					<a href="#">Modify</a>
f6/1					<a href="#">Modify</a>
f6/2					<a href="#">Modify</a>
f6/3					<a href="#">Modify</a>
f6/4					<a href="#">Modify</a>
p1					<a href="#">Modify</a>

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 quickly 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	<input type="text"/>
Interface Attribute	<input type="text"/> ▼
MMU Attribute	<input type="text"/> ▼
Shareload VLAN	<input type="text"/>

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

## 10.3 Spanning Tree

### 10.3.1 Global

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

Root STP Config	
Spanning Tree Priority	32768
MAC Address	3029.BEB0.AE90
Hello Time	2
Max Age	20
Forward Delay	15

Local STP Config	
Protocol Type	RSTP ▼
Spanning Tree Priority	32768 ▼
MAC Address	3029.BEB0.AE90
Hello Time	2 (1-10)s
Max Age	20 (6-40)s
Forward Delay	15 (4-30)s
BPDU Terminal	Disable ▼

[Set](#) [Reload](#)

The page can configure the local STP protocol, such as protocol type, spanning tree priorities etc. Click **Set** to save configuration.

## 10.3.2 MSTP

### 10.3.2.1 MST Global

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

MST Global	MST Instance
------------	--------------

MST Global	
Name	3029BEB0AE90
Revision Level	0 <0-65535>

[Set](#) [Reload](#)

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

Click **Set** to save configuration.

### 10.3.2.2 MST Instance

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

MST Global		MST Instance						
Instance	VLAN Mapping	Priority	Bridge ID	Root ID	Root Port	Root Path Cost	Port Mapping	Operate
0	1-4094	32768						<a href="#">Modify</a>
1		32768						<a href="#">Modify</a>
2		32768						<a href="#">Modify</a>
3		32768						<a href="#">Modify</a>
4		32768						<a href="#">Modify</a>
5		32768						<a href="#">Modify</a>
6		32768						<a href="#">Modify</a>
7		32768						<a href="#">Modify</a>
8		32768						<a href="#">Modify</a>
9		32768						<a href="#">Modify</a>
10		32768						<a href="#">Modify</a>
11		32768						<a href="#">Modify</a>
12		32768						<a href="#">Modify</a>
13		32768						<a href="#">Modify</a>
14		32768						<a href="#">Modify</a>
15		32768						<a href="#">Modify</a>

[Reload](#)

This page shows the VLAN Mapping, priority and etc. of every instance.

Click **Reload** at the bottom control bar, refresh the MST Instance information.

Click **Modify** on the right of the table, configure the instance.

Configuration Instance 0

VLAN Mapping   
Priority   
Bridge ID   
Root ID   
Root Path Cost   
Root Port

Port	Path Cost (1-200000000)	Priority
g1/1	<input type="text"/>	<input type="text" value="0"/>
g1/2	<input type="text"/>	<input type="text" value="0"/>
g1/3	<input type="text"/>	<input type="text" value="0"/>
g1/4	<input type="text"/>	<input type="text" value="0"/>

[Set](#) [Reload](#) [Go back](#)

On this page, the path cost and priority can be configured. And click **Set** at the bottom control bar to save the configuration.

### 10.3.3 Spanning Tree Ports

#### 10.3.3.1 Port Configuration

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

Port Configuration		Port State							
Port	Protocol Status	Priority(0~240)	Path-Cost(0~200000000)	Edge Port	RSTP Ring	Guard	BPDU guard	BPDU filter	
g1/3	Enable	128	0	Disable	Disable	none	Disable	Disable	
g1/4	Enable	128	0	Disable	Disable	none	Disable	Disable	
g1/5	Enable	128	0	Disable	Disable	none	Disable	Disable	
g1/6	Enable	128	0	Disable	Disable	none	Disable	Disable	
g1/7	Enable	128	0	Disable	Disable	none	Disable	Disable	
g1/8	Enable	128	0	Disable	Disable	none	Disable	Disable	
g2/1	Enable	128	0	Disable	Disable	none	Disable	Disable	
g2/2	Enable	128	0	Disable	Disable	none	Disable	Disable	
g2/3	Enable	128	0	Disable	Disable	none	Disable	Disable	
g2/4	Enable	128	0	Disable	Disable	none	Disable	Disable	
g2/5	Enable	128	0	Disable	Disable	none	Disable	Disable	
g2/6	Enable	128	0	Disable	Disable	none	Disable	Disable	
g2/7	Enable	128	0	Disable	Disable	none	Disable	Disable	

Set

Reload

Set Reload

This page shows the protocol status, priority, path cost, edge port, RSTP ring, guard, BPDU guard and BPDU filter enabling status, which can be configured. After configuration, click **Set** at the bottom control bar to save the configuration.

### 10.3.3.2 Port Status

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

Port Configuration		Port State			
Port	Role	State	Cost	Priority.Port ID	Type
g2/6	Desg	FWD	200000	128.14	Edge

Reload

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

## 10.4 EAPS (ether-ring)

Click **Redundancy -> EAPS(ether-ring)** at navigation bar in order, and then enter the EAPS ring (Ether-ring) list configuration page as following:

<input type="checkbox"/>	Ring ID	Node Type	Ring Description	Control VLAN	Status	Hello	Fail	Preforward	Primary Port/Forwarding/Link Status	Secondary Port/Forwarding/Link Status	Operate
<input type="checkbox"/>	0	Master-node		2	RingFail	1	3	3	None/Blocking/Linkdown	None/Blocking/Linkdown	<a href="#">Modify</a>



This page shows the configuration of EAPS ring (ether-ring), including ring ID, node type, ring description, CONTROL VLAN, status, Hello Time, Fail Time, Pre Forward Time and primary and secondary port on the ring.

Click **Modify** on the right, change the time, primary and secondary port configuration on the EAPS (ether-ring).

Click **Create** at the bottom control bar, create new EAPS (ether-ring).

Note:

1. The EAPS ring (ether-ring) number the system supported is 32.
2. After the EAPS ring (ether-ring) configured, the ring ID, node type and CONTROL VLAN cannot be changed. If they needed to be changed, please delete the EAPS (ether-ring) and create new.

Click **Create** at the bottom control bar on the EAPS (ether-ring) page, or click **Modify** on the right, enter the EAPS ring (ether-ring) configuration page:

EAPS Config

Ring ID	<input type="text" value="0"/>
Node Type	<input type="text" value="Master Node"/>
Ring Description	<input type="text"/>
Control VLAN	<input type="text"/>
Hello Time	<input type="text" value="1"/> (1-10)s
Fail Time	<input type="text" value="3"/> (3-30)s
Preforward Time	<input type="text" value="3"/> (3-30)s
Primary Port	<input type="text" value="None"/>
Secondary Port	<input type="text" value="None"/>

[Set](#) [Reload](#) [Go back](#)

In the drop-down list on the right of primary and secondary port, port of the ring can be chosen, or "None" can be chosen.

Note:

If configure the existed EAPS ring (ether-ring), the ring ID, node type and CONTROL VLAN cannot be changed.

## 10.5 MEAPS

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

<input type="checkbox"/>	Domain ID	Ring ID	Ring Type	Node Type	Control Vlan	Hello Time	Failed Time	Pre Forward Time	Port	Type	Port	Type	Operate
<input type="checkbox"/>	1	2	Major Ring	Master Node	2	3	3	4	None	Primary-Port	None	Secondary-Port	<a href="#">Modify</a>

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

Click **Create** to create 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.

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

Domain ID	<input type="text" value="2"/>
Ring ID	<input type="text" value="3"/>
Ring Type	<input type="text" value="Major Ring"/>
Node Type	<input type="text" value="Master Node"/>
Control Vlan	<input type="text" value="3"/>
Hello Time	<input type="text" value="3"/>
Failed Time	<input type="text" value="3"/>
Pre-Forward Time	<input type="text" value="3"/>
Primary-Port	<input type="text" value="g0/1"/>
Secondary-Port	<input type="text" value="f1/1"/>

Master node and the transit node can only be configured in the the primary ring.

Primary node, transit node and edge node can be configured in the secondary ring.

The primary node and the transit node can only be exited in one ring, and the edge node and the assistant edge node can be existed 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.

## 10.6 ERPS

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

<input type="checkbox"/>	Ring ID	control vlan	Ring-Node version	Ring-state	Signal Fail	WTR-time	guard time	send time	port1/Forwarding/Link Status	port2/Forwarding/Link Status	Operate
<input type="checkbox"/>	0	2	1	Begin	False	20	500	5	None/Blocking/Linkdown	None/Blocking/Linkdown	<a href="#">Modify</a>

[Reload](#) [Create](#) [Delete](#)

This page shows the configured ERPS ring, including ring ID, control vlan, Ring-Node version, Ring-state, Signal Fail, WTR-time, guard time, send-time, primary and secondary port.

Click **Modify** on the right of the list, configure the time and primary and secondary port.

Click **Create** at the bottom control bar, create new ERPS ring.

Note:

1. This system only supports ERPS single ring configuration.
2. Max 8 ERPS ring node.
3. Once one ERPS has been configured, its ID, ring ID and control Vlan cannot be configured. If these parameters need to be configured, please delete this ring and re-create it.

Click **Create** at the bottom control bar or click **Modify** on the right of the item, enter the ERPS configuration page as following:



ERPS configuration

Ring ID	0	
control vlan		
Ring-Node version	1	
WTR-time	20	(10-720)s
guard time	500	(10-200)
send time	5	(1-10)s
port1	None	port1 role Ring-Pi
port2	None	port2 role Ring-Pi

Set Reload Go back

The ring ID of ERPS can be from 1 to 7.

After the port 1 and port 2 configured, the corresponding port role should be configured.

In the text boxes of “Port 1” and “Port 2”, select a port as the ring port respectively or select “None”.

Note:

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

## 10.7 CFM Function

### 10.7.1 Global

Click **Redundancy -> CFM Function -> GLOBAL** at navigation bar in order, and then enter the cfm enable configuration page as following:

cfm enable

cfm list

cfm enable configuration

cfm enable	disable
------------	---------

Set Reload

Click **Set** at the bottom control bar, finish the setting.

Click the “cfm list” on the top, enter the CFM list page:

cfm enable		cfm list				
<input type="checkbox"/>	md	level	ma	meps	vlan	cci

Reload Create Delete

Click **Create** at the bottom control bar, enter the CFM Global configuration page:

cfm enable	cfm list
------------	----------

cfm Global configuration

md \*

level \*

ma \*

meps \*

vlan \*

ci \* 10s

**Help**  
#MEP IDs(1-8191), such as (1,3,5,7) Or (1,3-5,7) Or (1-7).  
#At least two MEPs in an MA.

Set Reload Go back

After configuration, click **Set** at the bottom control bar to finish the setting.  
Click **Go Back** at the bottom control bar, back to the CFM List page.

10.7.2 Interface Configuration

Click **Redundancy -> CFM Function -> interface configuration** at navigation bar in order, and then enter the cfm port list page as following:

<input type="checkbox"/>	Port Name	cfm enable	md	ma	mepid	rmepid	direction
--------------------------	-----------	------------	----	----	-------	--------	-----------

**Help**  
#Configuration port CFM before, please configure the global cfm.

Set Reload Create Delete

Click **Set** at the bottom control bar, finish the cfm port list configuration.

Click **Reload** at the bottom control bar, refresh cfm port list information.

Click **Delete** at the bottom control bar, delete the selected cfm port configuration.

Click **Create** at the bottom control bar, enter the cfm port configuration page:

cfm Port configuration

Port Select	g0/1 ▾
Port Enable	disable ▾
md *	<input type="text"/>
ma *	<input type="text"/>
mepid *	<input type="text"/>
rmepid *	<input type="text"/>
direction *	down ▾

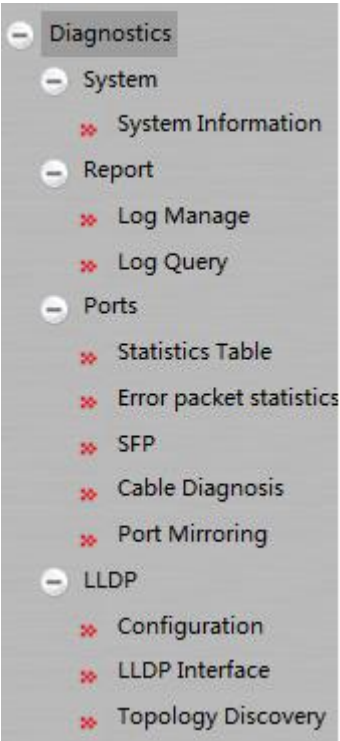
---

[Set](#) [Reload](#) [Go back](#)

Click **Set** to finish the cfm port configuration.

Click **Go Back**, back to the cfm port list page.

# 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	Switch1
Device Type	
Serial No.	20093340885
MAC Address	3029.BEB0.AE90
IP Address	192.168.2.3
CPU Usage	16%
Memory Usage	55%
Power Supply 1	Abnormal
Power Supply 2	Normal
Uptime	0 Day ,1:41:22
Current Time	1970-1-1 1:41:22
Temperature(°C)	33

#### State of Redundancy Protocols

Portocol	State	Information
STP	Running	RSTP



“**Address of the system log server**” textbox and select the log's grade in the “Grade of the system log information” dropdown box (grade 9 – 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 “**show log**” 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

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 Ports

### 11.3.1 Statistics Table

Click **Diagnostics -> Ports -> 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	0	6	0	5862	1432525	0	5818	44	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, including the Receive Packets, Receive Bytes, Received Unicast Packets, Received Multicast Packets, Received Broadcast Packets ...etc.

### 10.3.2 Error Packet Statistics

Click **Diagnostics -> Port -> Error Packet Statistics** at navigation bar in order, and then enter the error packet statistics page as following:

Port	Received Discard	Received Error Packets	FCS Packets	Jabber Packets	Received Oversize Packets	Received Undersize Packets	Transmitted Discard	Transmitted Error Packets	Transmitted Oversize Packets
g1/1	0	0	0	0	0	0	0	0	0
g1/2	0	0	0	0	0	0	0	0	0
g1/3	0	0	0	0	0	0	0	0	0
g1/4	0	0	0	0	0	0	0	0	0
g1/5	0	0	0	0	0	0	0	0	0
g1/6	111	0	0	0	0	0	0	0	0
g1/7	0	0	0	0	0	0	0	0	0
g1/8	0	0	0	0	0	0	0	0	0
g2/1	0	0	0	0	0	0	0	0	0
g2/2	0	0	0	0	0	0	0	0	0
g2/3	0	0	0	0	0	0	0	0	0
g2/4	0	0	0	0	0	0	0	0	0
g2/5	0	0	0	0	0	0	0	0	0
g2/6	118	0	0	0	0	0	45	0	0
g2/7	0	0	0	0	0	0	0	0	0
g2/8	0	0	0	0	0	0	0	0	0
g3/1	0	0	0	0	0	0	0	0	0
g3/2	0	0	0	0	0	0	0	0	0
g3/3	0	0	0	0	0	0	0	0	0

Reload Clear

This page shows the communication data, including received discard, received error packets, FCS packets, Jabber packets, received oversize packets, received undersize packets, transmitted discard, transmitted error packets, transmitted oversize packets etc.

Click **Clear** at the bottom control bar, to clean all the error packet statistics information.

### 11.3.3 SFP

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 (°C)	Supply Voltage (V)	Bias (mA)
------	----------------	----------------	------------------	--------------------	-----------

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

### 11.3.4 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 **Set** to view the results of the diagnosis。

### 11.3.5 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	<input type="checkbox"/>	RX
g0/2	<input type="checkbox"/>	RX
g0/3	<input type="checkbox"/>	RX
g0/4	<input type="checkbox"/>	RX
f1/1	<input type="checkbox"/>	RX
f1/2	<input type="checkbox"/>	RX
f1/3	<input type="checkbox"/>	RX
f1/4	<input type="checkbox"/>	RX
f2/1	<input type="checkbox"/>	RX
f2/2	<input type="checkbox"/>	RX
f2/3	<input type="checkbox"/>	RX
f2/4	<input type="checkbox"/>	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



### 11.4.1 LLDP Basic Configuration

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

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 Interface

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
g0/2	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
g0/3	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
g0/4	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f1/1	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f1/2	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f1/3	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f1/4	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f2/1	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f2/2	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f2/3	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f2/4	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f3/1	Disable	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

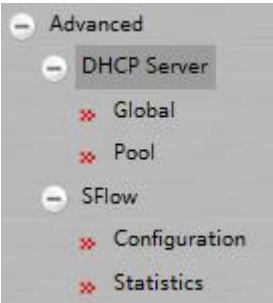
### 11.4.3 Topology Discovery

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 by this device.

# 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:

<input type="checkbox"/>	Name	Network number	Network mask	Address range	Address lease time	Operate
<input type="checkbox"/>	aaa	192.168.6.0	255.255.255.0		Default	<a href="#">Modify</a>

The page lists the DHCP server pool information that have been configured.  
Click **Modify** on the right of the entry and configure the parameter of DHCP server pool.  
Click **Create** 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

12.2 SFlow

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

SFlow Configuration

Version

5

<4-5>

Maximum Header Size

128

<16-256>

Interval

20

<0-65535>

Agent IP Address

Set

Reload

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).

Click Port tab to enter the SFlow port configuration page as following:

Global

Port

Port	Egress	Egress Sampling Rate	Ingress	Ingress Sampling Rate
g1/1	Disable	500	Disable	500
g1/2	Disable	500	Disable	500
g1/3	Disable	500	Disable	500
g1/4	Disable	500	Disable	500
g1/5	Disable	500	Disable	500
g1/6	Disable	500	Disable	500
g1/7	Disable	500	Disable	500
g1/8	Disable	500	Disable	500
g2/1	Disable	500	Disable	500
g2/2	Disable	500	Disable	500
g2/3	Disable	500	Disable	500
g2/4	Disable	500	Disable	500
g2/5	Disable	500	Disable	500

Set

Reload

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.

### 12.2.2 SFlow Statistics

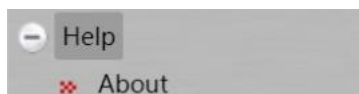
Click **Advanced -> SFlow -> Statistics** at navigation bar in order, and then click the Poller tab page enter the SFlow poller information page as following:

Poller		Sampler		
Source Port	Reference	Interval	ReTime	Status

Click **Advanced -> SFlow -> Statistics** at navigation bar in order, and then click the Sampler tab page enter the SFlow poller information page as following:

Poller	Sampler				
Source Port	Direction	Reference	ReRate	Poll	Samples

## Chapter 13 Help



### 13.1 About

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

#### **MRD**

Version 2.0.2I Build 88942

(Build 88942)

Homepage : <http://www.mrdcom.net/>

Telephone : 021-58330762

Copyright (c) 2003 by Shanghai MRDcom Co., Ltd.

All Rights Reserved.

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

--- End of File ---