# WEB Configuration Manual

# Table of Contents

1. WEB 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 - 3 -
1.2.2 HTTPS Service Port Configuration - 3 -
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 - 7 -
2.4.3 Configuration Display Area - 7 -
2.4.4 Bottom Control Bar - 8 -
3 Basic Configuration - 9 -
3.1 System - 9 -
3.2 Global Configuration Mode (Management Interface) - 9 -
3.3 Port Configuration - 10 -
3.4 Software - 11 -
3.5 Load/Save - 11 -
3.6 Restart - 11 -
3.7 Factory Settings - 12 -
4 Security - 13 -
4.1 User Management - 13 -
4.1.1 User Management - 13 -
4.1.2 Group Management - 14 -
4.1.3 Password Rule Management - 15 -
4.1.4 Author Rule Management - 16 -
4.1.5 Authentication Rule Management - 17 -
4.2 Management Access - 18 -
4.2.1 Server - 18 -
4.2.2 SNMP Community Management (SNMPv1/v2 community) - 19 -
4.2.3 SNMPv3 Configuration - 21 -

4.2.4 CLI ( Command Line Interface ) - 23 -
4.3 Port Security - 24 -
4.3.1 IP MAC Binding - 24 -
4.3.2 Static MAC Filter Mode - 25 -
4.3.3 Static MAC Filter - 26 -
4.3.4 Dynamic MAC Mode - 27 -
4.4 Switchport Protect - 27 -
4.5 Keepalive - 29 -
4.6 802.1X Port Authentication - 30 -
4.6.1 Global - 30 -
4.6.2 Authentication List - 30 -
4.6.3 Port Configuration - 31 -
4.6.4 Statistics - 31 -
4.7 RADIUS - 32 -
4.7.1 Global - 32 -
4.7.2 Service - 32 -
5 Time - 34 -
5.1 Basic Setting - 34 -
5.2 NTP - 34 -
6 Network Security - 36 -
6.1 DOS Configuration - 36 -
6.1.1 DOS Global Configuration - 36 -
6.2 DHCP Snooping Configuration - 37 -
6.2.1 DHCP Snooping Global Configuration - 37 -
6.2.2 DHCP Snooping VLAN Configuration - 38 -
6.2.3 DHCP Snooping Interface Configuration - 38 -
6.2.4 DHCP Snooping Bindings - 39 -
6.3 Access Control List - 40 -
6.3.1 IPv4 Rules - 40 -
6.3.2 MAC Rules - 41 -
6.3.3 Assignment - 42 -
6.4 Filter Function - 42 -
7 Switching - 44 -
7.1 Storm Control - 44 -
7.1.1 Broadcast Storm Control - 44 -
7.1.2 Multicast Storm Control - 45 -
7.1.3 Unicast Storm Control - 45 -
7.2 Port Rate Limits - 45 -
7.3 MAC Address Table - 46 -
7.4 IGMP Snooping - 47 -
7.4.1 IGMP Snooping Configuration - 47 -
7.4.2 IGMP-Snooping VLAN - 48 -
7.4.3 Static Multicast Mac Address Configuration - 49 -
7.4.4 Multicast list - 50 -
7.5 VLAN - 50 -

7.5.1 VLAN configuration ..... - 50 -
7.5.2 VLAN Batch Configuration ..... - 51 -
7.5.3 Port VLAN Configuration ..... - 52 -
8 Routing ..... - 54 -
8.1 VLAN Interface and IP Address Configuration ..... - 54 -
8.2 VRRP Configuration ..... - 55 -
8.3 IP Express Forwarding ..... - 56 -
8.4 Static ARP ..... - 56 -
8.5 Static Route ..... - 57 -
8.6 RIP Configuration ..... - 58 -
8.6.1 RIP Configuration ..... - 58 -
8.6.2 RIP Router Entries ..... - 59 -
8.7 OSPF Configuration ..... - 60 -
8.7.1 OSPF process ..... - 60 -
8.7.2 OSPF Router Entries ..... - 61 -
9 POE Mgr ..... - 63 -
10 QoS/Priority ..... - 66 -
10.1 Global ..... - 66 -
10.2 Port Configuration ..... - 66 -
10.3 802.1D/p Mapping ..... - 67 -
10.4 IP DSCP Mapping ..... - 67 -
10.5 Queue Management ..... - 68 -
11 Redundancy ..... - 69 -
11.1 Link Aggregation Configuration ..... - 69 -
11.1.1 Port Aggregation Configuration ..... - 69 -
11.1.2 Port Channel Global Loading Balance ..... - 70 -
11.2 Backup Link ..... - 71 -
11.2.1 Backup Link Global Configuration ..... - 71 -
11.2.2 Link Backup Protocol Port Configuration ..... - 72 -
11.3 Spanning Tree ..... - 72 -
11.3.1 Global ..... - 72 -
11.3.2 MSTP ..... - 73 -
11.3.3 Spanning Tree Ports ..... - 74 -
11.4 EAPS (ether-ring) ..... - 75 -
11.5 MEAPS ..... - 77 -
11.6 ERPS ..... - 78 -
12 Diagnostics ..... - 80 -
12.1 System ..... - 80 -
12.1.1 System Information ..... - 80 -
12.2 Report ..... - 81 -
12.2.1 Log Management ..... - 81 -
12.2.2 Log Query ..... - 82 -
12.3 Ports ..... - 83 -
12.3.1 Statistics Table ..... - 83 -

12.3.2 Error Packet Statistics ..... - 83 -
12.3.3 SFP ..... - 84 -
12.3.4 Port Mirroring ..... - 84 -
12.4 LLDP Configuration ..... - 85 -
12.4.1 LLDP Basic Configuration ..... - 85 -
12.4.2 LLDP Interface ..... - 85 -
12.4.3 Topology Discovery ..... - 86 -
13 Advanced ..... - 87 -
12.1 DHCP Server ..... - 87 -
13.1.1 DHCP Server Global Configuration ..... - 87 -
13.1.2 DHCP Server Pool Configuration ..... - 87 -
14 Help ..... - 89 -
14.1 About ..... - 89 -

# 1. WEB 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 TNM4000 series 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 { *portNumber* } | Configuring HTTP service port |

### 1.1.3 Enabling the HTTP service

Switches support to control the HTTP access. Only when the HTTP service is enabled can HTTP

exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops. Configure global mode by the following command:

| Command | Purpose |
|---|---|
| ip http server | Enabling HTTP service |

### 1.1.4 HTTP access mode Configuration

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

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

### 1.1.5 Setting the Max-VLAN 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 { *max-vlan* } | Setting the Max-VLAN numbers to display in Web page |

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

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

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

## 1.2 HTTPS Configuration

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

### 1.2.1 HTTPS Access Configuration

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

| Command | Description |
|---|---|
| ip http ssl-access enable | Enable the HTTPS access 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 |
|---|---|
| ip http secure-port {*portNumber*} | Setting the HTTPS port number |

# 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:

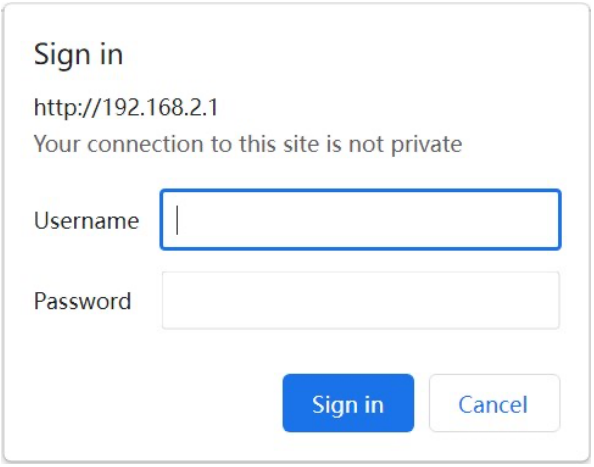
- HTML of version 4.0
- HTTP of version 1.1
- JavaScript™ of version 1.5

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.



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.

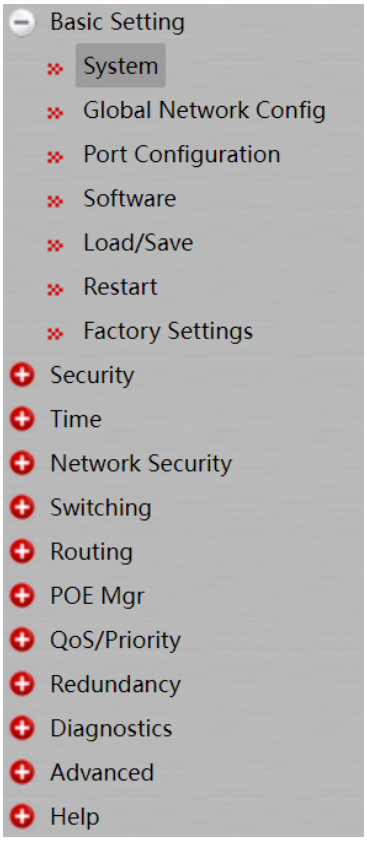
## 2.4 Introduction of Web Interface

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 **write** command.<br><br>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. |

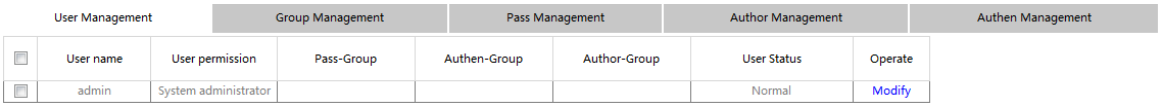
## 2.4.2 Navigation Bar




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



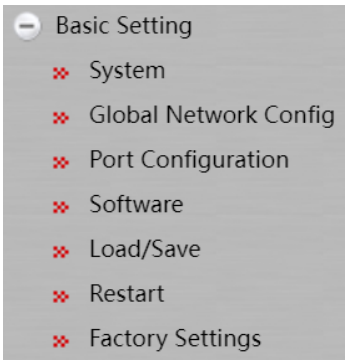

The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

### 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 | Apply the modified configuration to the device.<br>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. |
| 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. |

# 3 Basic Configuration




## 3.1 System

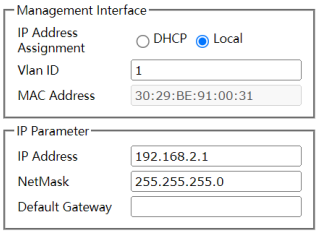
If you click **Basic Setting -> System** in the navigation bar, the page appears as shown as below:


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:

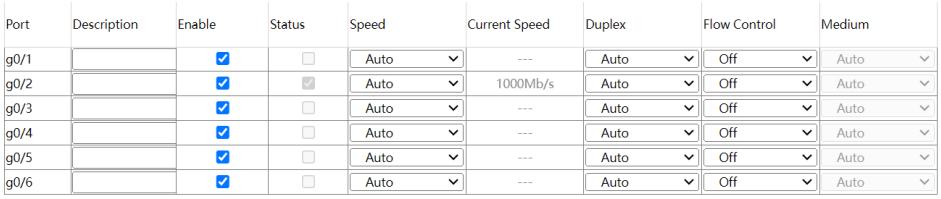




- Setting the IP address of Interface VLAN 1 , in order to access the switch
- This page is used to set the IP address of Interface Vlan 1 in the management interface of the device. In initial conditions, the MAC address of the device, the IP address, mask and gateway of the interface will appear on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



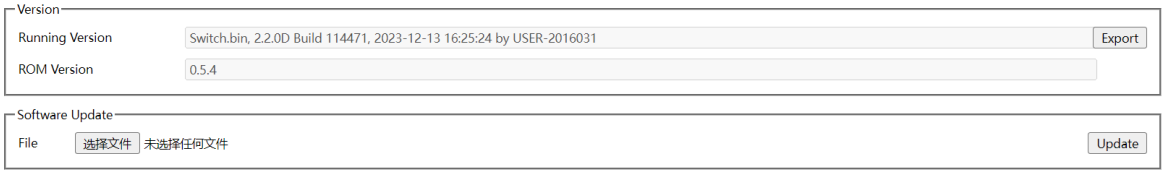
| Port | Description | Enable | Status | Speed | Current Speed | Duplex | Flow Control | Medium |
|---|---|---|---|---|---|---|---|---|
| g0/1 | | ☑ | ☐ | Auto | --- | Auto | Off | Auto |
| g0/2 | | ☑ | ☑ | Auto | 1000Mb/s | Auto | Off | Auto |
| g0/3 | | ☑ | ☐ | Auto | --- | Auto | Off | Auto |
| g0/4 | | ☑ | ☐ | Auto | --- | Auto | Off | Auto |
| g0/5 | | ☑ | ☐ | Auto | --- | Auto | Off | Auto |
| g0/6 | | ☑ | ☐ | Auto | --- | Auto | Off | Auto |


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

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

## 3.4 Software

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




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.

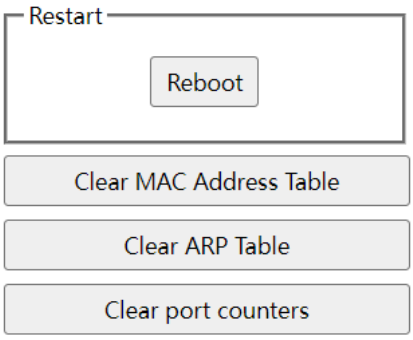
## 3.5 Load/Save

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


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.

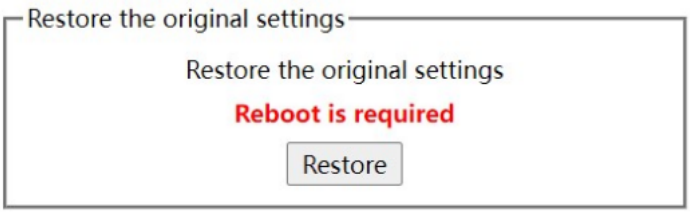
## 3.6 Restart

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



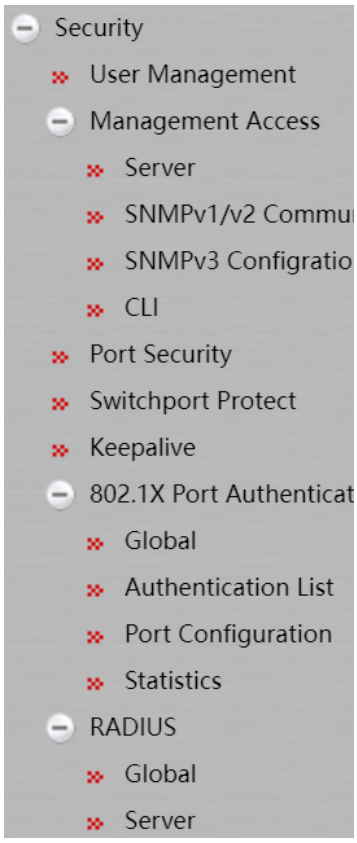
You can choose “Reboot” to reboot the switch, or choose “Clear MAC Address Table” , “Clear ARP Table”, “Clear port counters”.

## 3.7 Factory Settings




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

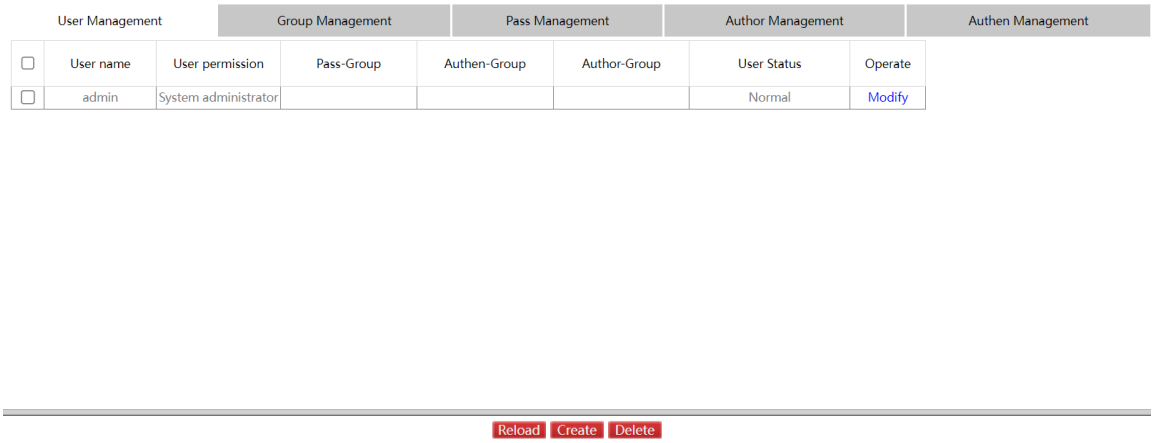
# 4 Security




## 4.1 User Management

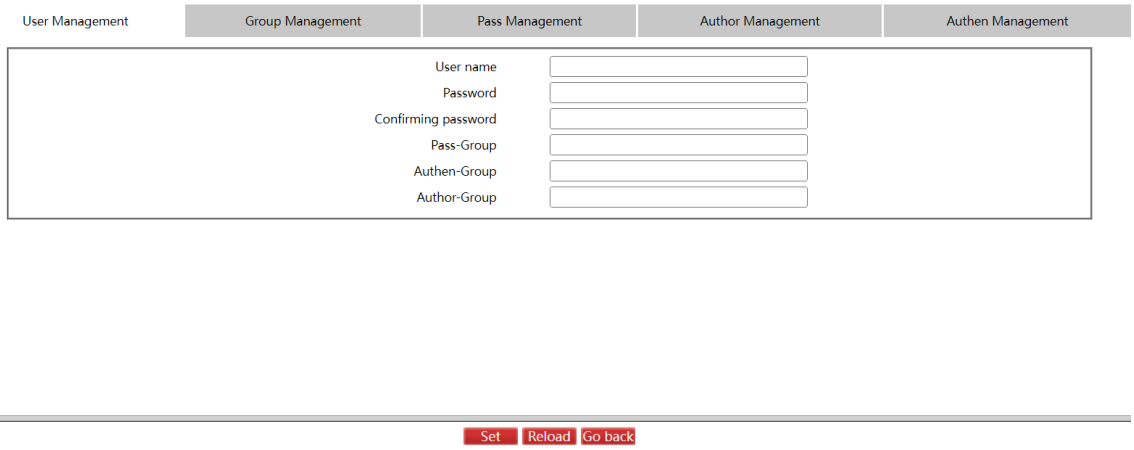
### 4.1.1 User Management

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



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

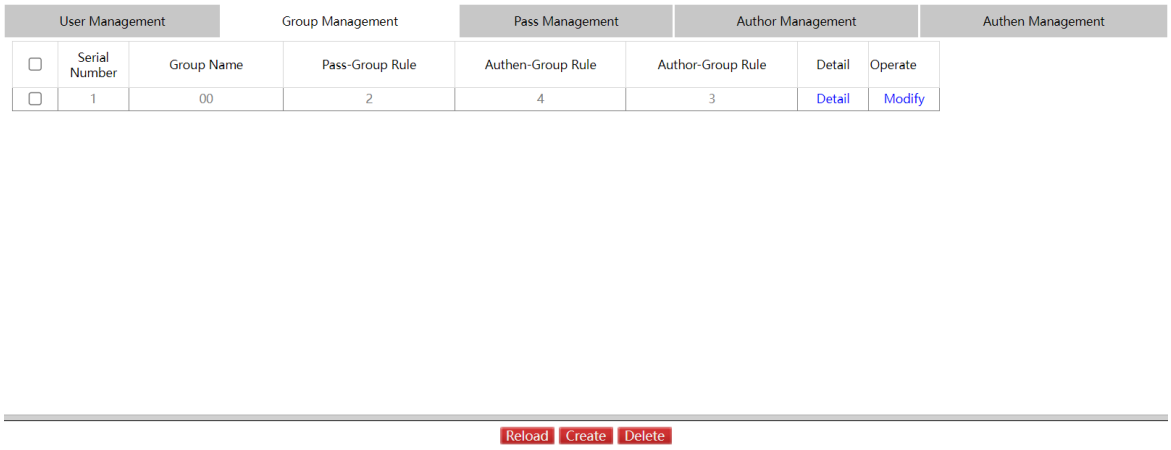
Click **Create** at the bottom bar to enter the following page:




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.

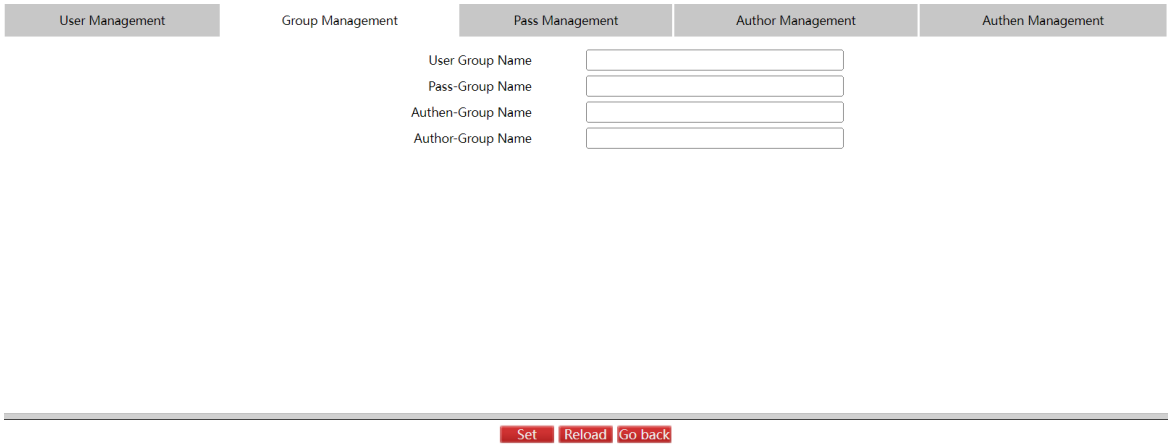
### 4.1.2 Group Management

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




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:

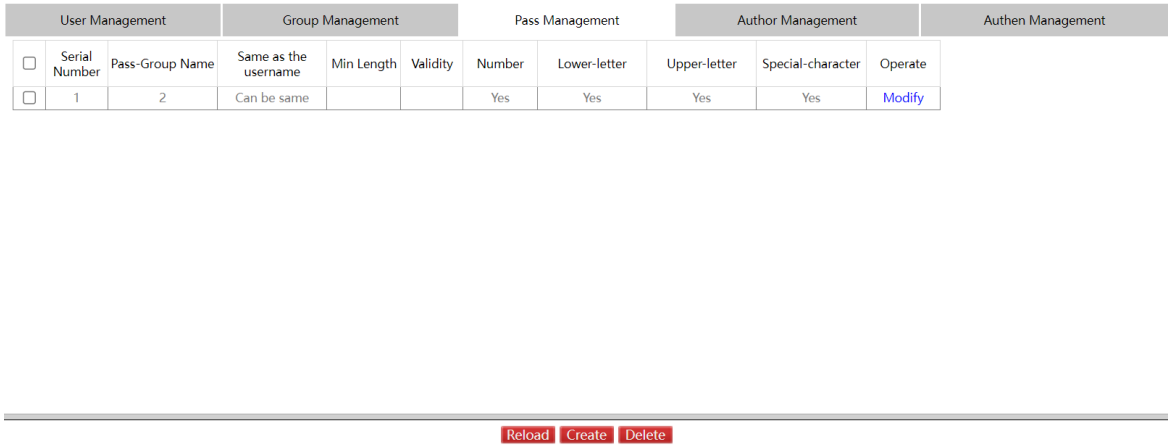
Click **Create** at the bottom bar of group management page to enter the following page:




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

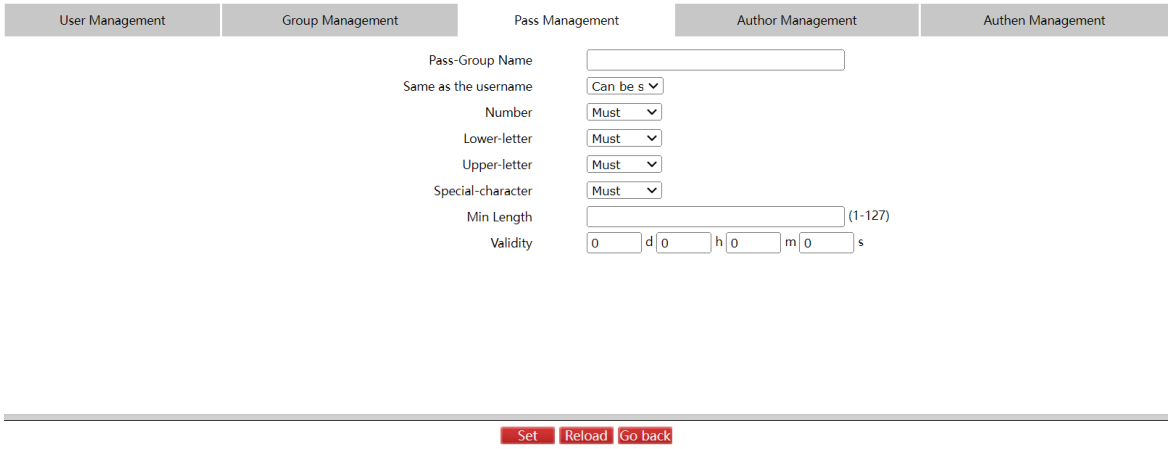
### 4.1.3 Password Rule Management

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




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

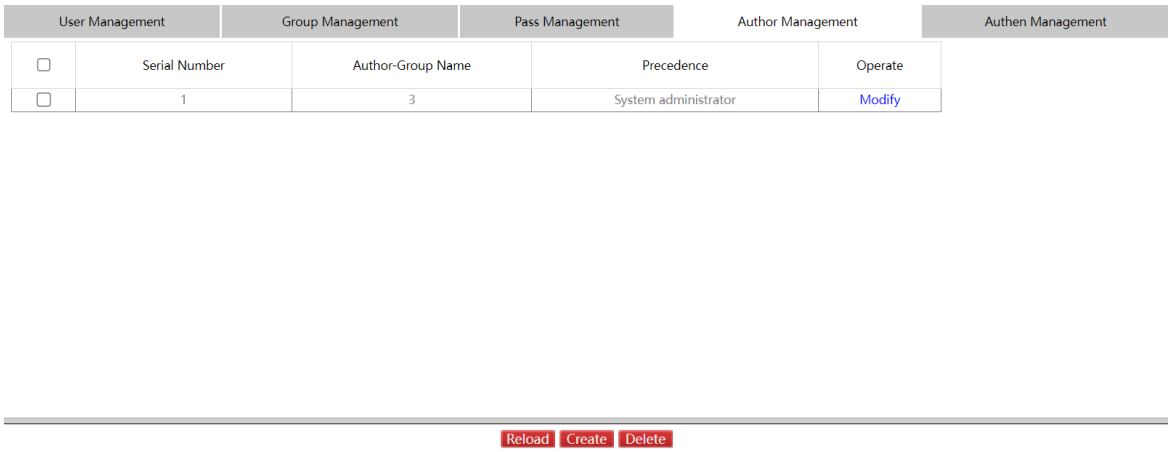
Click **Create** at the bottom bar to enter the following configuration page:




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

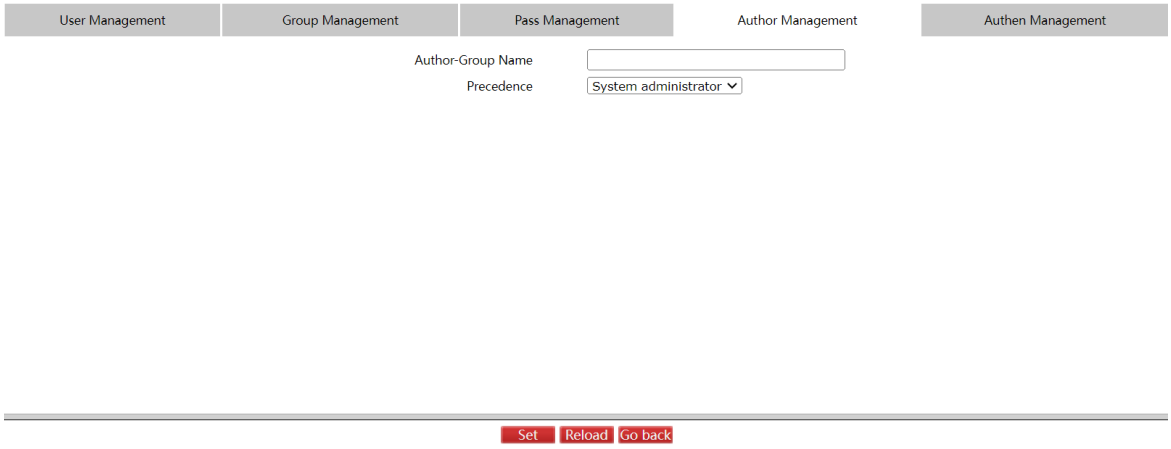
### 4.1.4 Author Rule Management

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




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

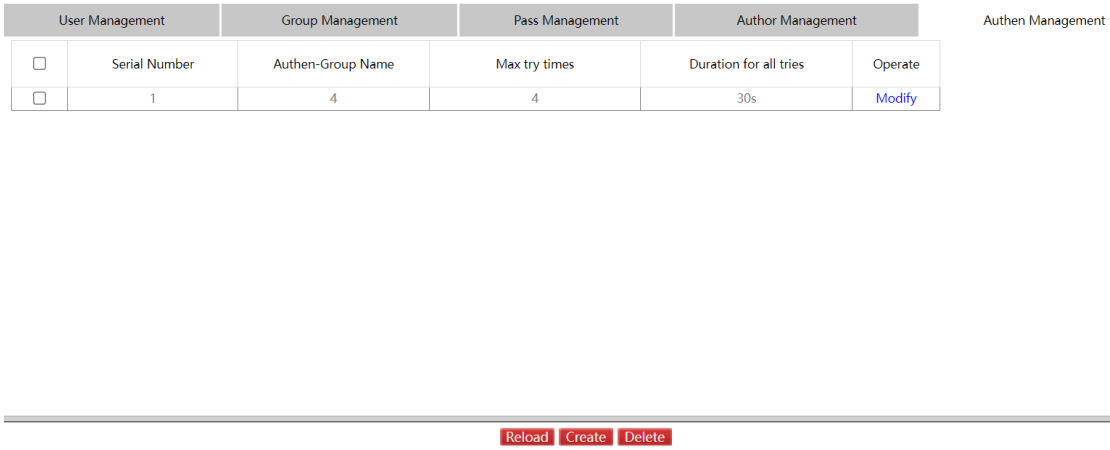
Click **Create** at the bottom bar to enter the following page:




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

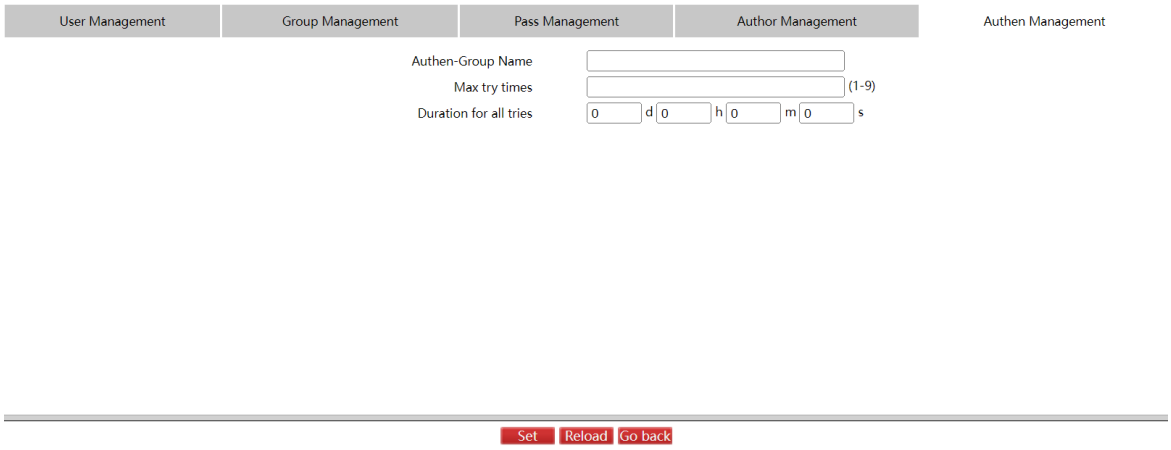
### 4.1.5 Authentication Rule Management

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




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:

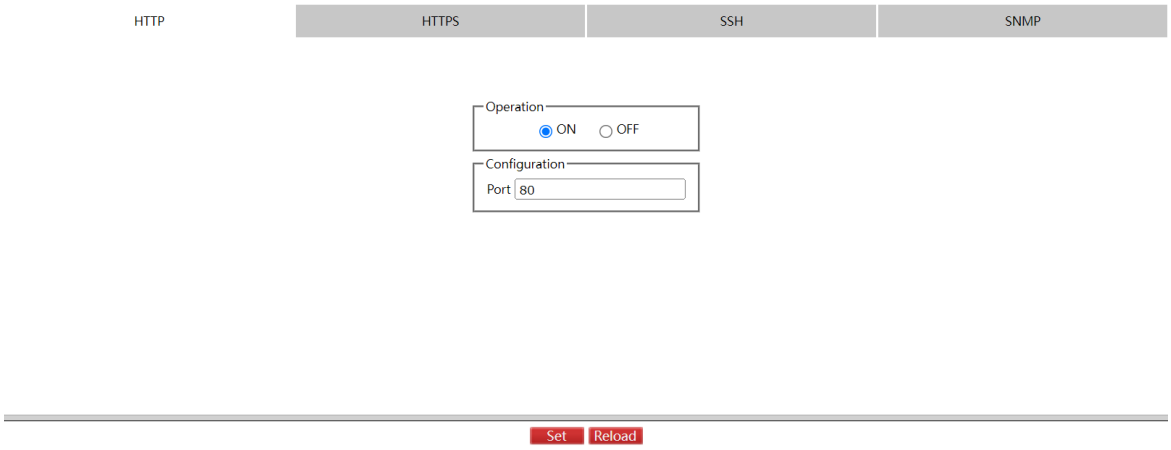



Fill in configuration at every configuration column and click **Setup** at the bottom bar to create new authentication rules。

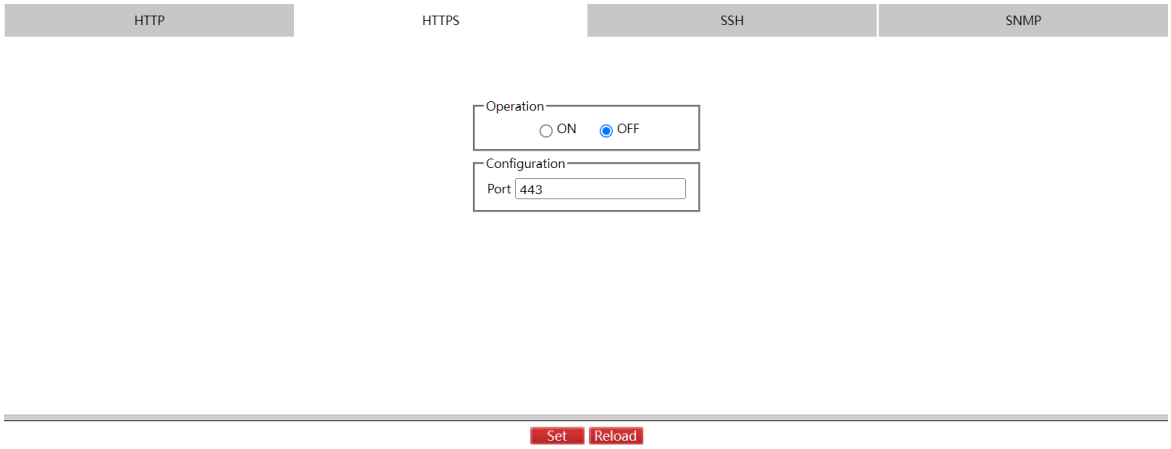
# 4.2 Management Access

## 4.2.1 Server

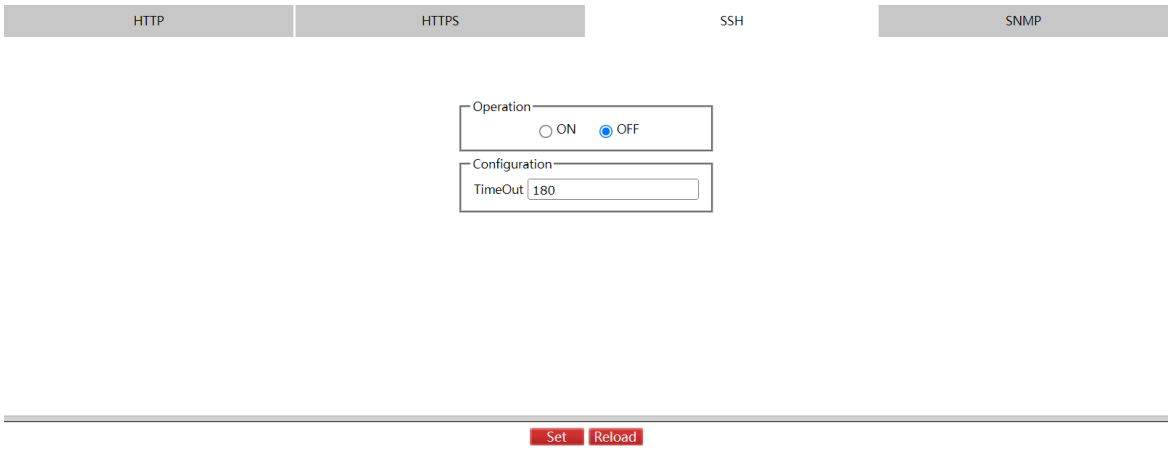
HTTP, HTTPS, SSH and SNMP could be configured at this page. Click **Security -> Management Access -> Server** at navigation bar in order to enter service configuration page. Click **HTTP** at this page to enter HTTP configuration.



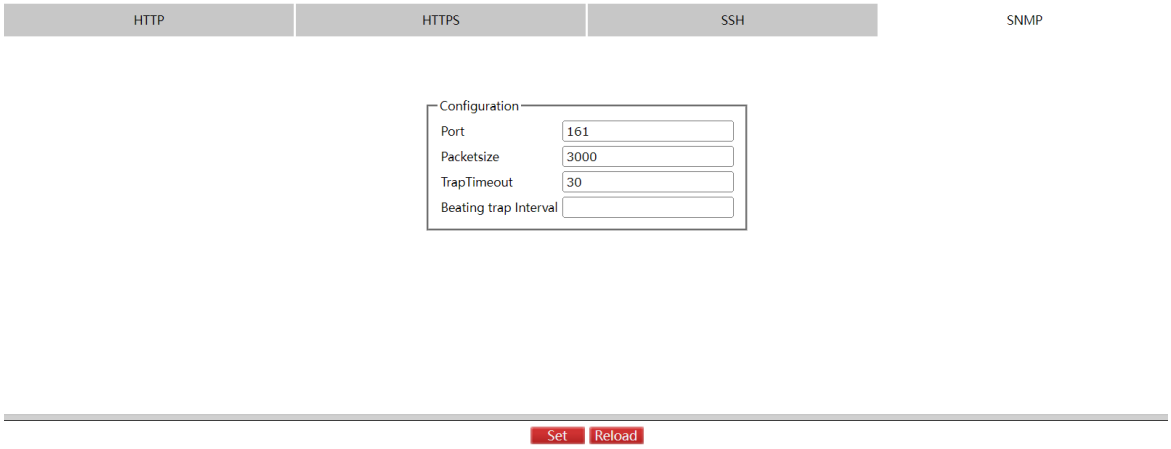

Click **HTTPS** to configure HTTPS related:




Click **SSH** to configure SSH related:




Click **SNMP** to configure SNMP related:




## 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

| | SNMP Community Name | SNMP Community Encryption | SNMP Community Attribute | Operate |
|---|---|---|---|---|
| ☐ | 1 | False | RO | Modify |
| ☐ | 2 | False | RW | Modify |

Reload Create Delete

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

Set Go back

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

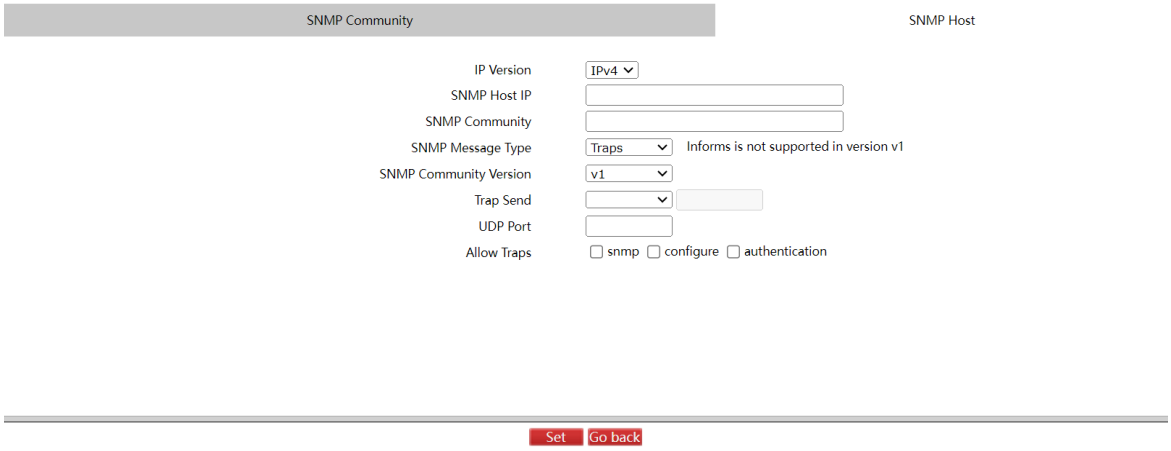
Click **SNMP Host** to switch to the SNMP Host configuration page:

SNMP Community | SNMP Host

| | SNMP Host IP | SNMP Community String | SNMP Message Type | SNMP Community Version | Operate |
|---|---|---|---|---|---|
| ☐ | 192.168.3.4 | 1 | Traps | v1 | Modify |

Reload Create Delete

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




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

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

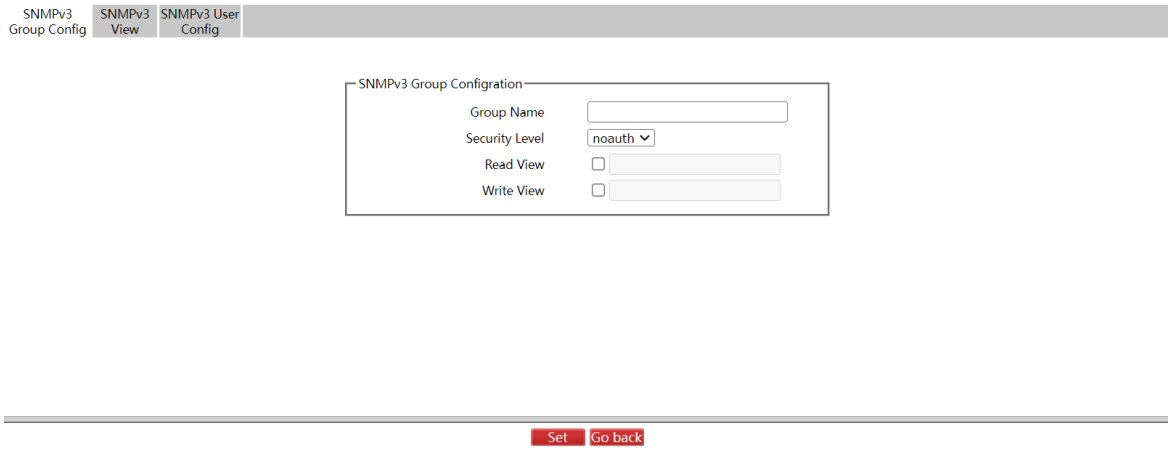
## 4.2.3 SNMPv3 Configuration

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

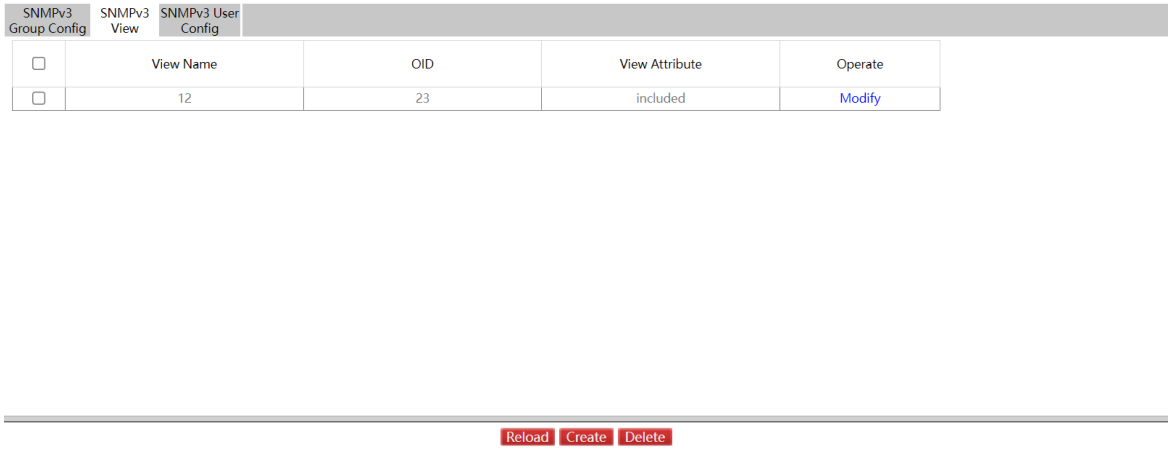

Click the **Modify** to change the features of SNMPv3 Group Configuration.

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

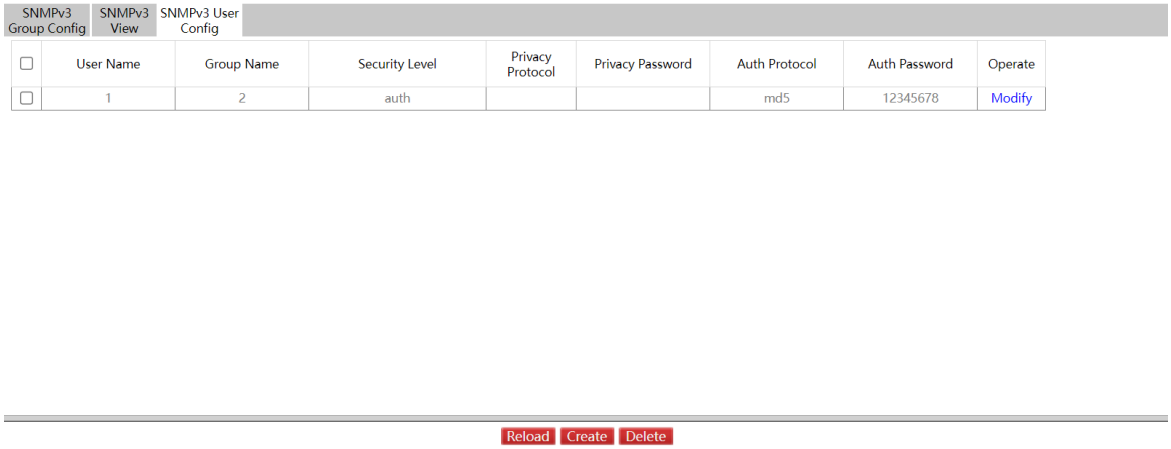
Click **Create** to create a new configuration for SNMPv3 Group:




Click **SNMPv3 View** to enter the following view page:



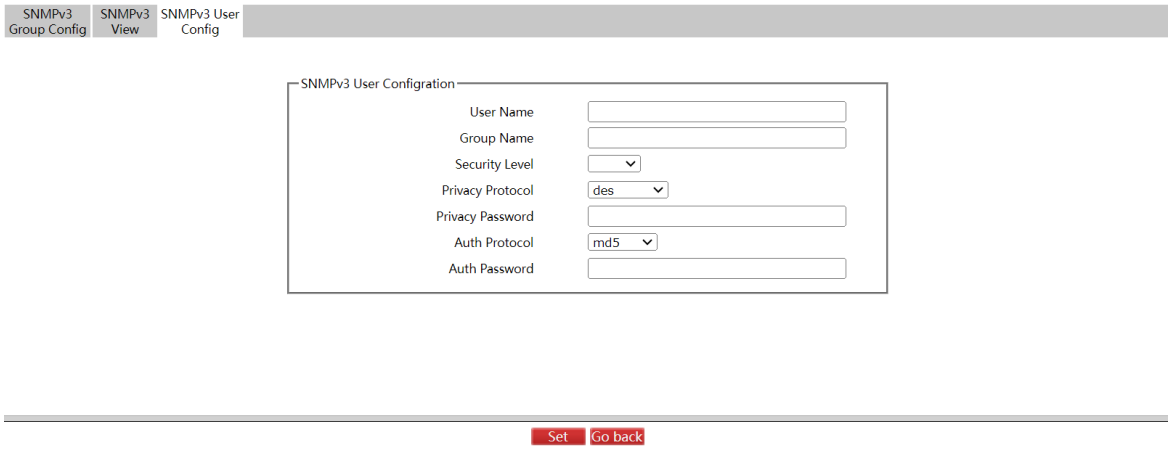

Click **SNMPv3 User Config** to enter the following configuration page:




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.

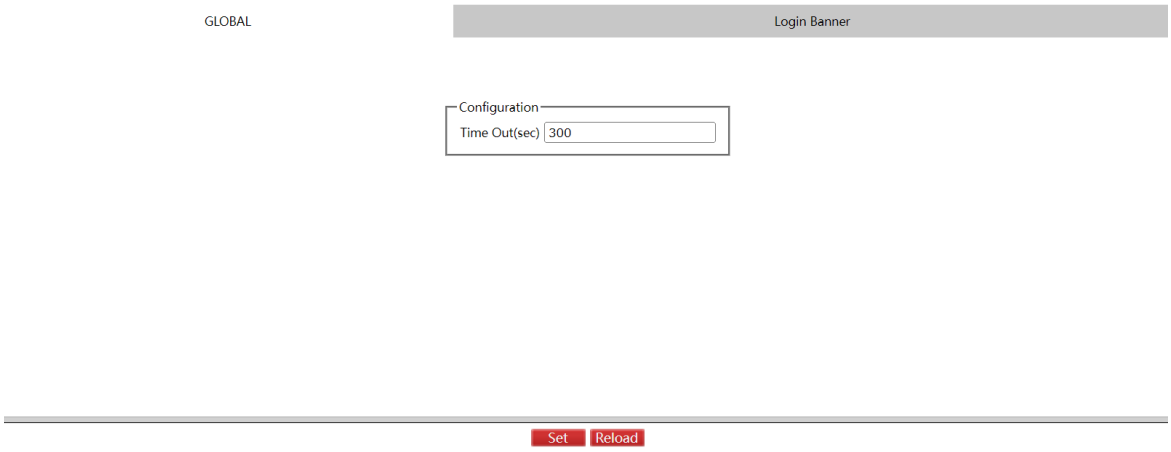
Click **Create** to create new configuration of SNMPv3:




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

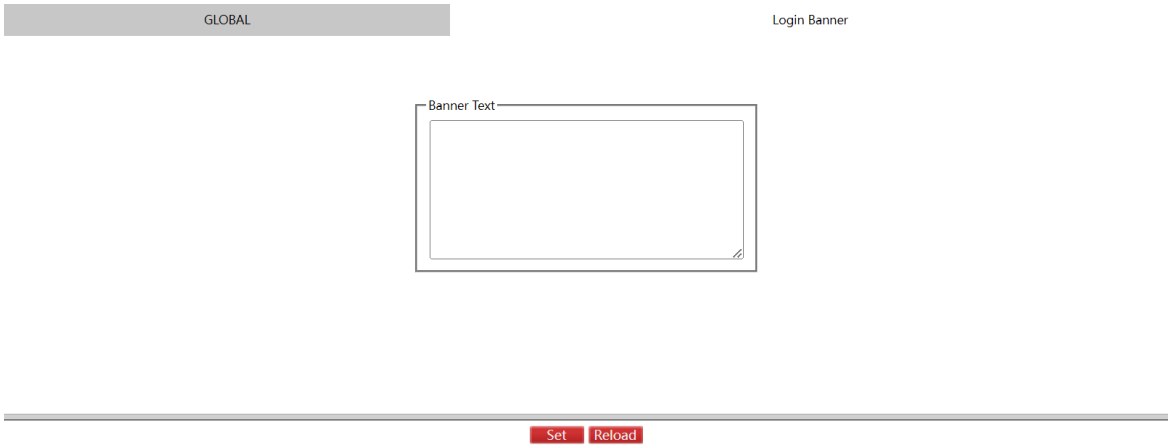
## 4.2.4 CLI ( Command Line Interface )

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




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

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

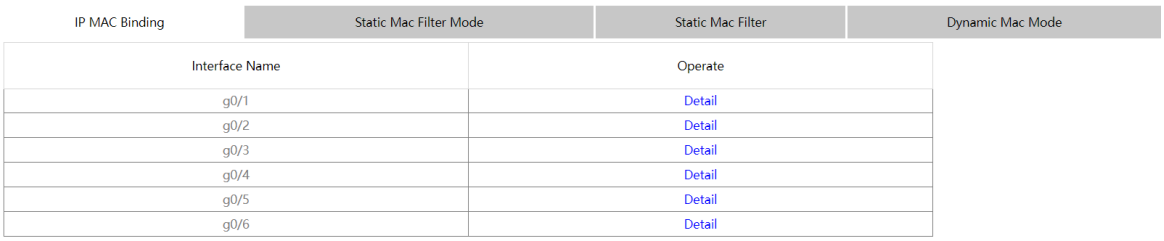



Terminal's Login Banner could be configured at this page.

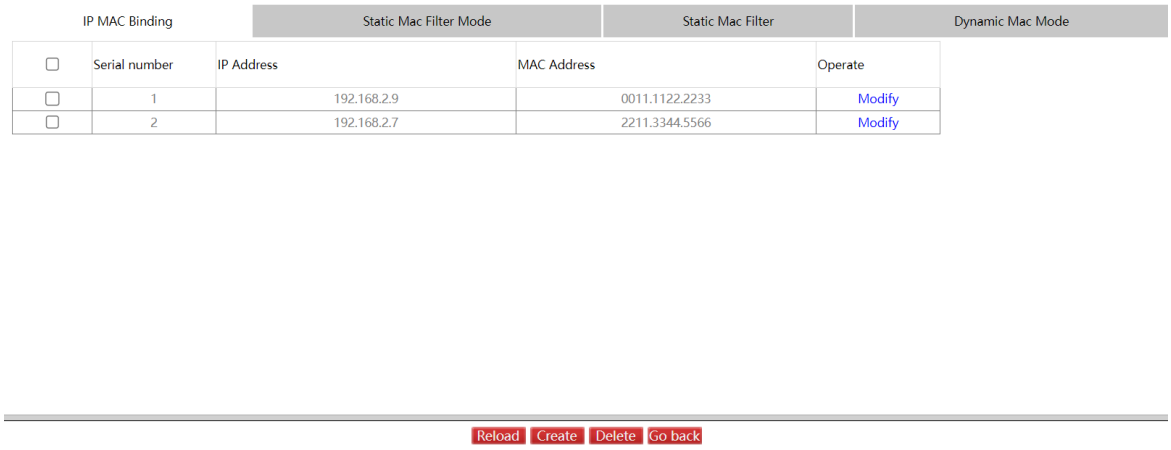
# 4.3 Port Security

## 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:



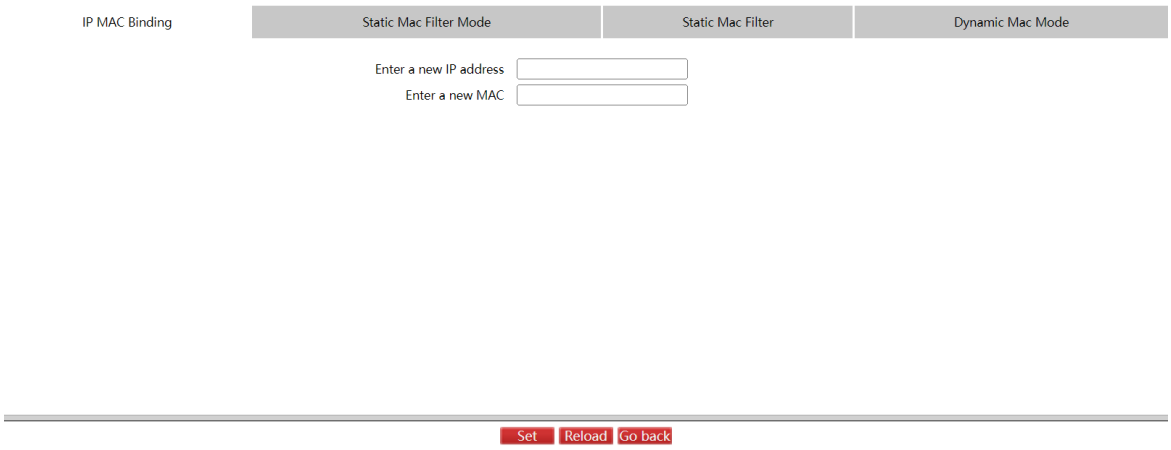

Click **Detail** to check the IP MAC binding information of that port.




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.




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 |
|---|---|---|
| g0/1 | Access | Disable |
| g0/2 | Access | Disable |
| g0/3 | Access | Disable |
| g0/4 | Access | Disable |
| g0/5 | Access | Disable |
| g0/6 | 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 |
|---|---|
| g0/1 | Detail |
| g0/2 | Detail |
| g0/3 | Detail |
| g0/4 | Detail |
| g0/5 | Detail |
| g0/6 | Detail |

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

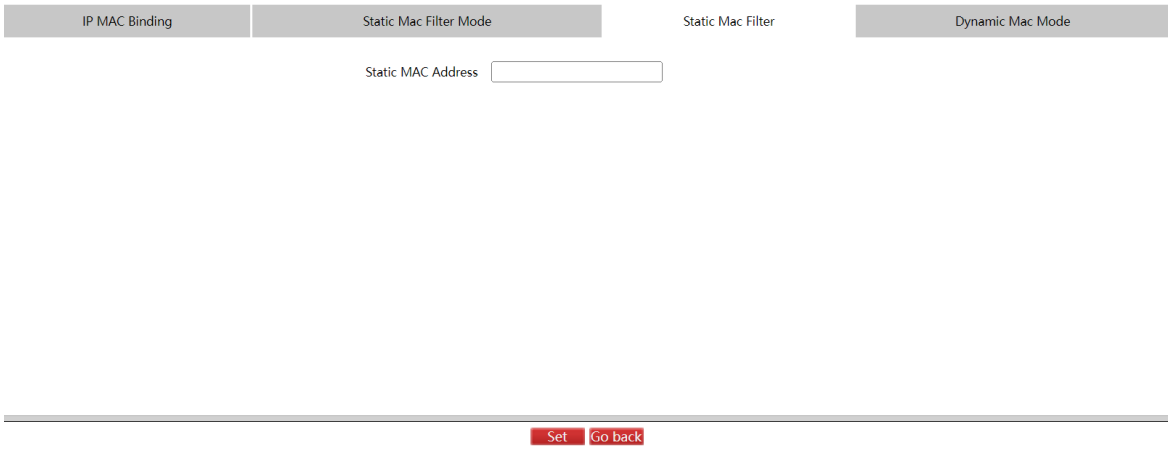
IP MAC Binding | Static Mac Filter Mode | Static Mac Filter | Dynamic Mac Mode

| | Serial number | MAC Address | Operate |
|---|---|---|---|
| ☐ | 1 | 2211.3344.5566 | Modify |

Create Delete Go back

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

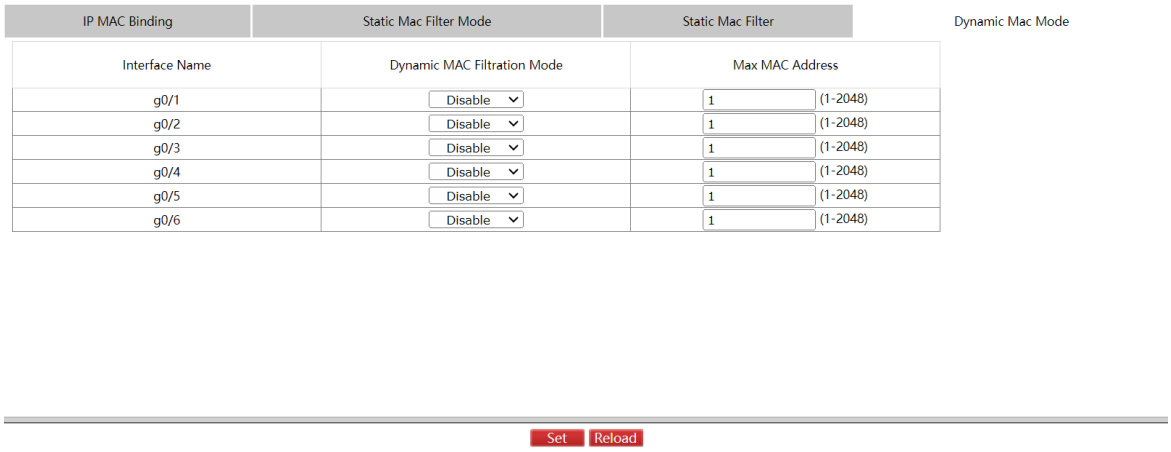
Click **Create** to create new static MAC filtration items.




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:




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

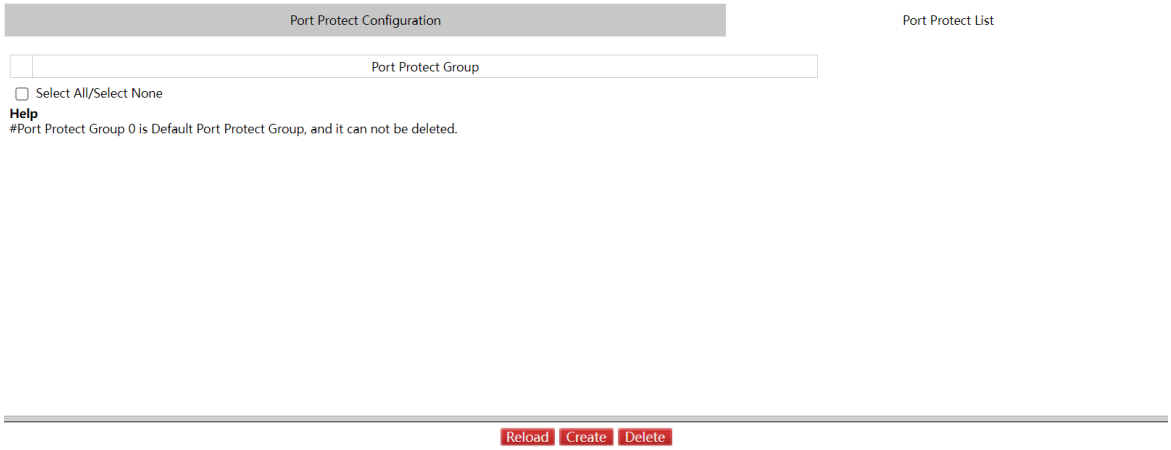
## 4.4 Switchport Protect

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


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.

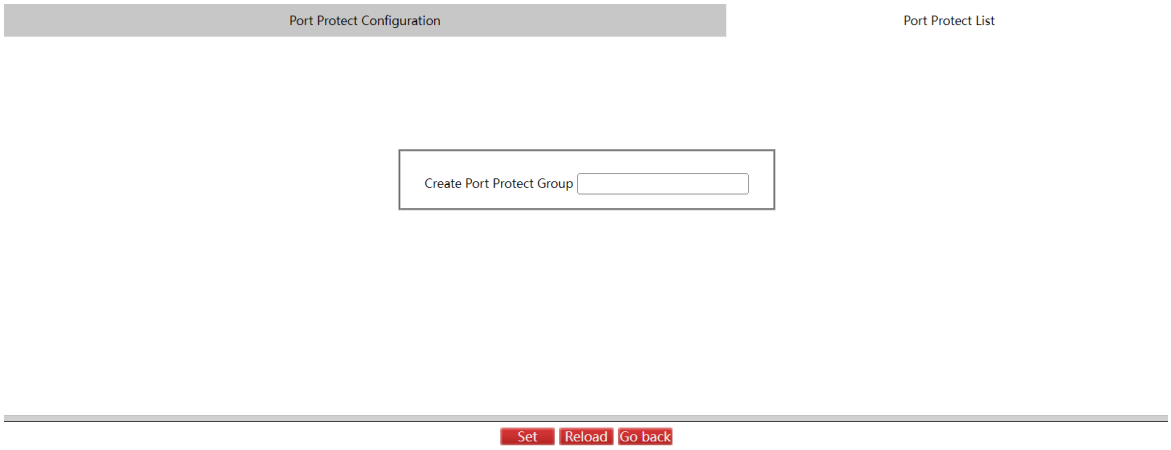
Click “Port Protect List”, enter the Port Protect Group Creating page:




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:



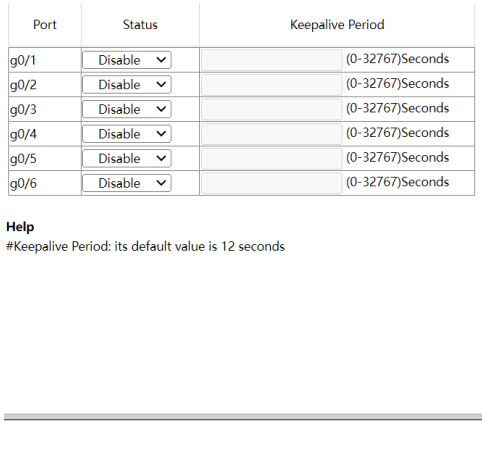

Click **Set** at the bottom control bar, to finish the setting.

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 |
|---|---|---|
| g0/1 | Disable | (0-32767)Seconds |
| g0/2 | Disable | (0-32767)Seconds |
| g0/3 | Disable | (0-32767)Seconds |
| g0/4 | Disable | (0-32767)Seconds |
| g0/5 | Disable | (0-32767)Seconds |
| g0/6 | Disable | (0-32767)Seconds |

**Help**
#Keepalive Period: its default value is 12 seconds

Set Reload

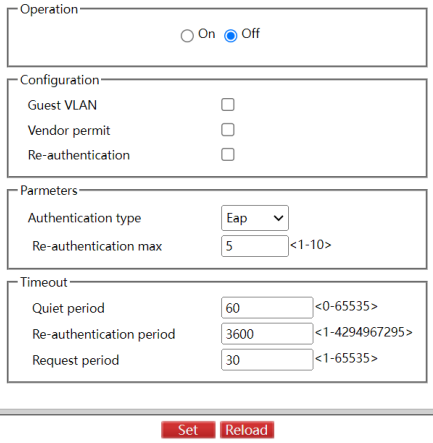
Click **Set** at the bottom control bar after configuration, to finish the port status setting.

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

# 4.6 802.1X Port Authentication

## 4.6.1 Global

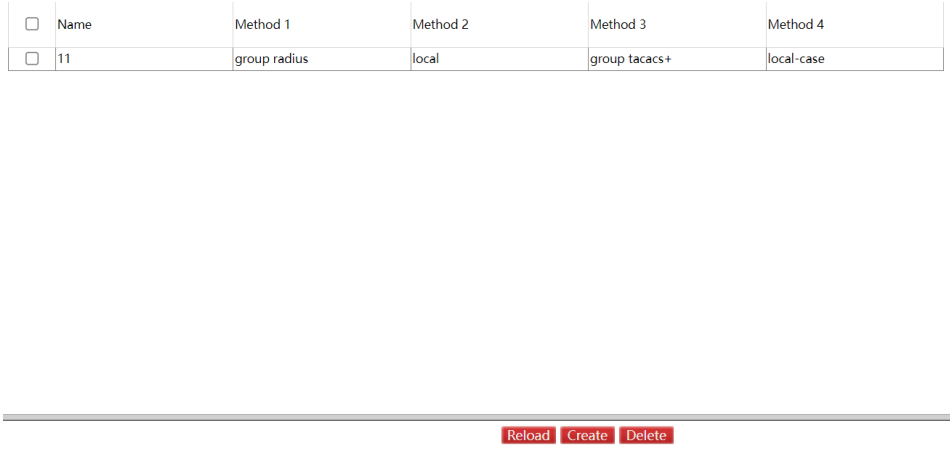
Click **Security -> 802.1X Port Authentication -> Global** at navigation bar in order to enter configuration page as following:




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

## 4.6.2 Authentication List

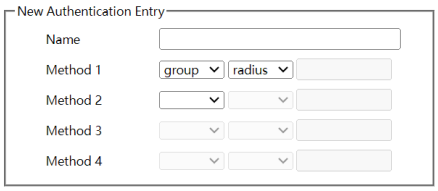
Click **Security -> 802.1X Port Authentication -> Authentication List** at navigation bar in order to enter configuration page as following:




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:




Set Reload Go back

## 4.6.3 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 |
|---|---|---|---|---|---|---|---|
| g0/1 | Force authorized | ☐ | Eap | Single hosts | ☐ | <1-4094> | |
| g0/2 | Force authorized | ☐ | Eap | Single hosts | ☐ | <1-4094> | |
| g0/3 | Force authorized | ☐ | Eap | Single hosts | ☐ | <1-4094> | |
| g0/4 | Force authorized | ☐ | Eap | Single hosts | ☐ | <1-4094> | |
| g0/5 | Force authorized | ☐ | Eap | Single hosts | ☐ | <1-4094> | |
| g0/6 | Force authorized | ☐ | Eap | Single hosts | ☐ | <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 | EAPOL Start | EAPOL Logoff | EAPOL Invalid | Received EAPOL Total | EAP Response Id | EAP Response Other | EAP Length Error | Transmitted EAPOL Total | EAP Request Id | EAP Other |
|---|---|---|---|---|---|---|---|---|---|---|
| g0/1 | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| g0/2 | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| g0/3 | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| g0/4 | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| g0/5 | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| g0/6 | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

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 | | |

Set Reload

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:

| | Address | Authentication port | Accounting port |
|---|---|---|---|
| ☐ | 192.168.0.4 | 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.

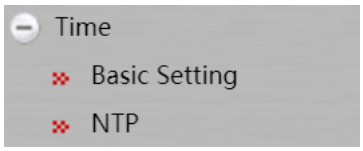
Click **Delete** at the bottom control bar, to delete the selected authentication port and accounting port information of RADIUS Server.

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

Server Ip Address:

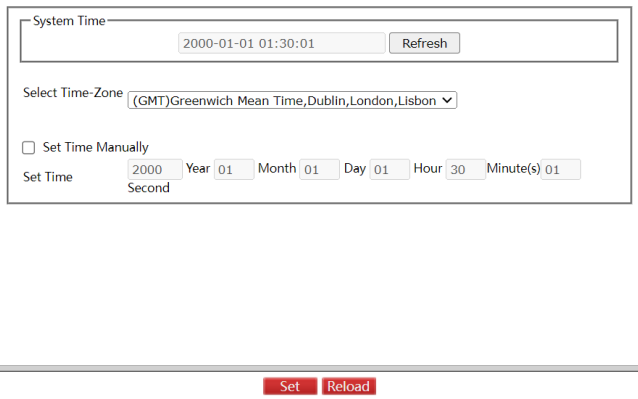
Set Go back

# 5 Time




## 5.1 Basic Setting

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

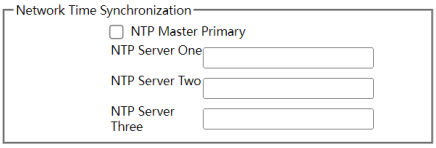



Click **Reload** to refresh the current displayed system time.

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

## 5.2 NTP

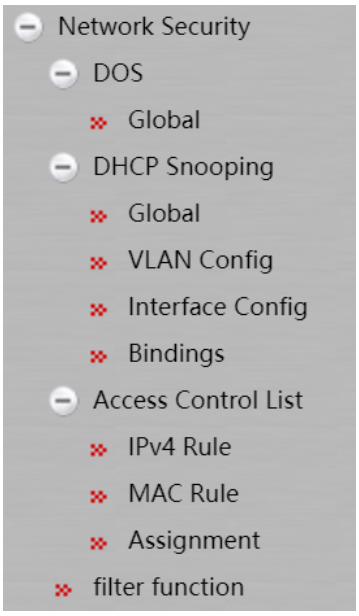
Click **Time -> NTP** at navigation bar in order to enter configuration page as following:





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

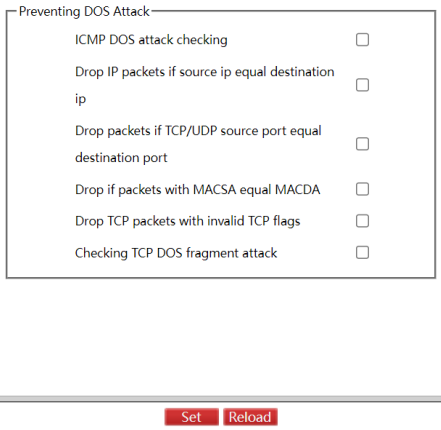
# 6 Network Security




## 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:

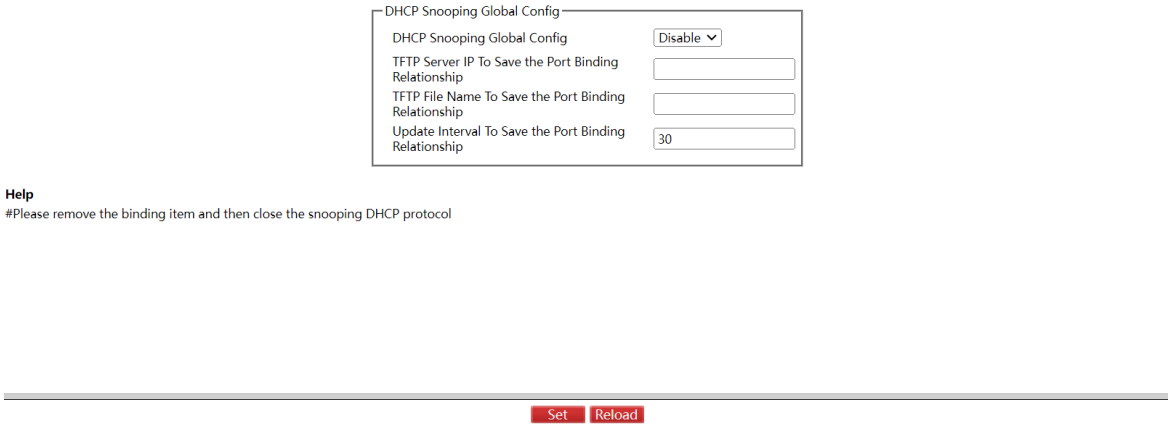



You could set or cancel the related Preventing DOS Attack according to needs. Click **Set** to save configuration.

# 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:




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.

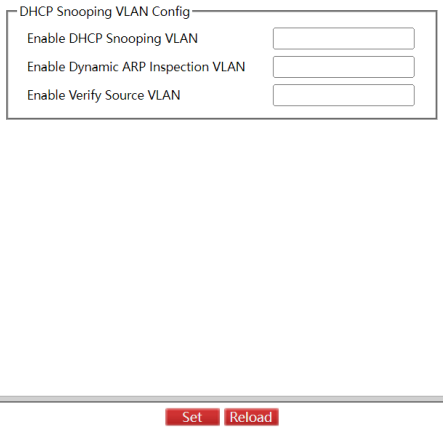
After switch's configuration is saved, restart the switch. All previous configured interface binding relationship would be dropped. At the meantime, the interface has no binding relationship, and switch would denying the forwarding of all IP messages after IP source address monitoring function is enabled. 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 | Distrust | Distrust | Distrust |
| g0/2 | Distrust | Distrust | Distrust |
| g0/3 | Distrust | Distrust | Distrust |
| g0/4 | Distrust | Distrust | Distrust |
| g0/5 | Distrust | Distrust | Distrust |
| g0/6 | Distrust | Distrust | Distrust |

Set Reload

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

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

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

### 6.2.4 DHCP Snooping Bindings

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

| | MAC Address | IP Address | Interface Name | VLAN |
|---|---|---|---|---|
| ☐ | 22:11:22:33:55:44 | 192.168.0.9 | GigaEthernet0/1 | 1 |

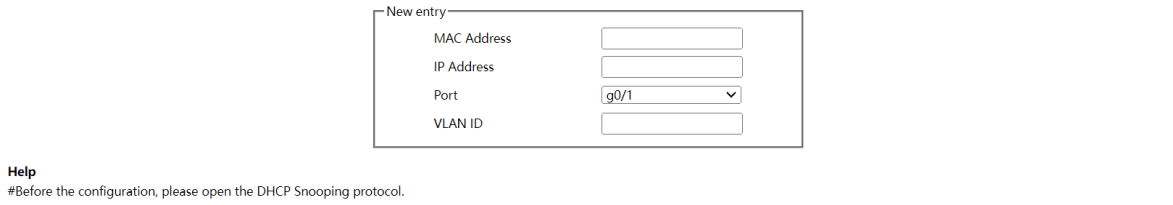
Reload Create Delete

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.

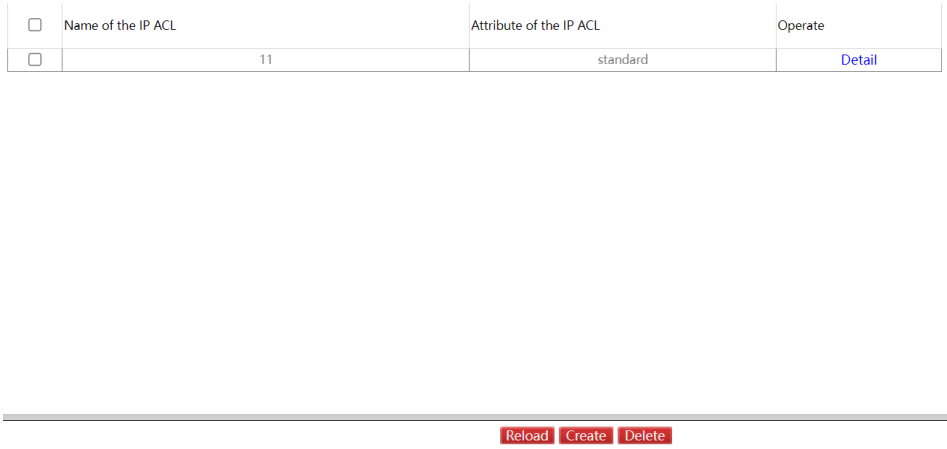



Note：
Binding entries can be created only if enabling DHCP Snooping protocol.

# 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:




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.

| | Authority | Src IP | Src IP Mask | Record the log | Operate |
|---|---|---|---|---|---|
| | permit | any | | | Modify |

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: tom

Attribute: 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:

| | Name of the MAC Access Control List | Operate |
|---|---|---|
| | 33 | Detail |

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

Set Go back

### 6.3.3 Assignment

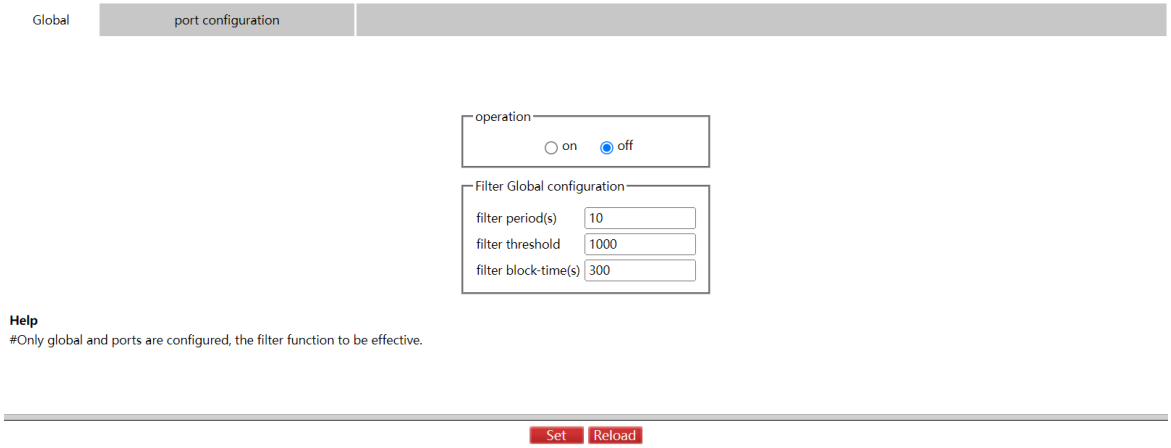
Click **Network Security -> Access Control List -> Assignment** at navigation bar in order to enter distribution page of access control list as following:

| Port | Ingress IP ACL | Ingress MAC ACL |
|---|---|---|
| g0/1 | | |
| g0/2 | | |
| g0/3 | | |
| g0/4 | | |
| g0/5 | | |
| g0/6 | | |

Set Reload

## 6.4 Filter Function

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




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:


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

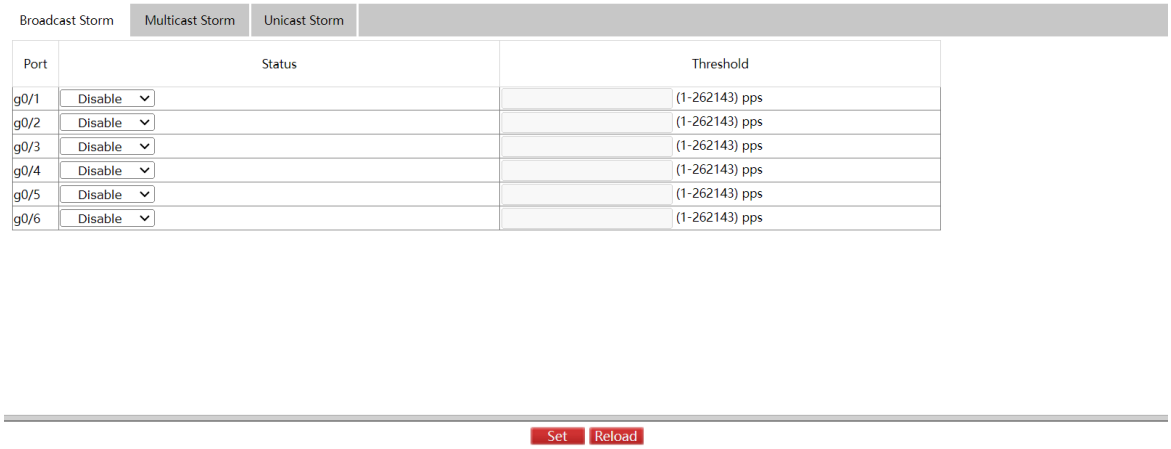
Click **Reload** at the bottom control bar, refresh the port configuration of filter function.

# 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




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 | (1-262143) pps |
| g0/2 | Disable | (1-262143) pps |
| g0/3 | Disable | (1-262143) pps |
| g0/4 | Disable | (1-262143) pps |
| g0/5 | Disable | (1-262143) pps |
| g0/6 | Disable | (1-262143) pps |

Set Reload

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 | (1-262143) pps |
| g0/2 | Disable | (1-262143) pps |
| g0/3 | Disable | (1-262143) pps |
| g0/4 | Disable | (1-262143) pps |
| g0/5 | Disable | (1-262143) pps |
| g0/6 | Disable | (1-262143) pps |

Set Reload

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 | (1-15625) | Disable | 64kbps | (1-15625) |
| g0/2 | Disable | 64kbps | (1-15625) | Disable | 64kbps | (1-15625) |
| g0/3 | Disable | 64kbps | (1-15625) | Disable | 64kbps | (1-15625) |
| g0/4 | Disable | 64kbps | (1-15625) | Disable | 64kbps | (1-15625) |
| g0/5 | Disable | 64kbps | (1-15625) | Disable | 64kbps | (1-15625) |
| g0/6 | Disable | 64kbps | (1-15625) | Disable | 64kbps | (1-15625) |

Set Reload

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

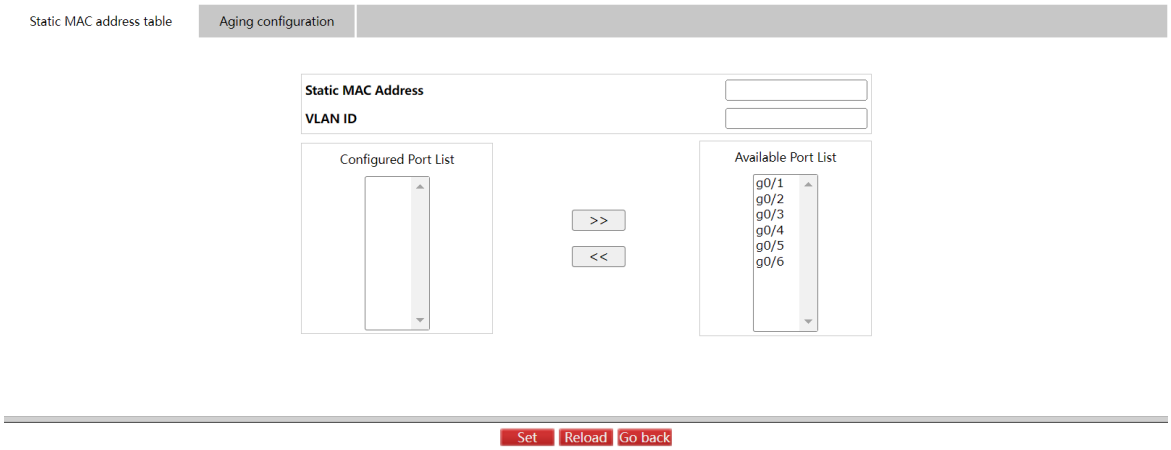
Click **Switching -> MAC Address Table** at navigation bar in order to enter static MAC address table as following:

Static MAC address table | Aging configuration

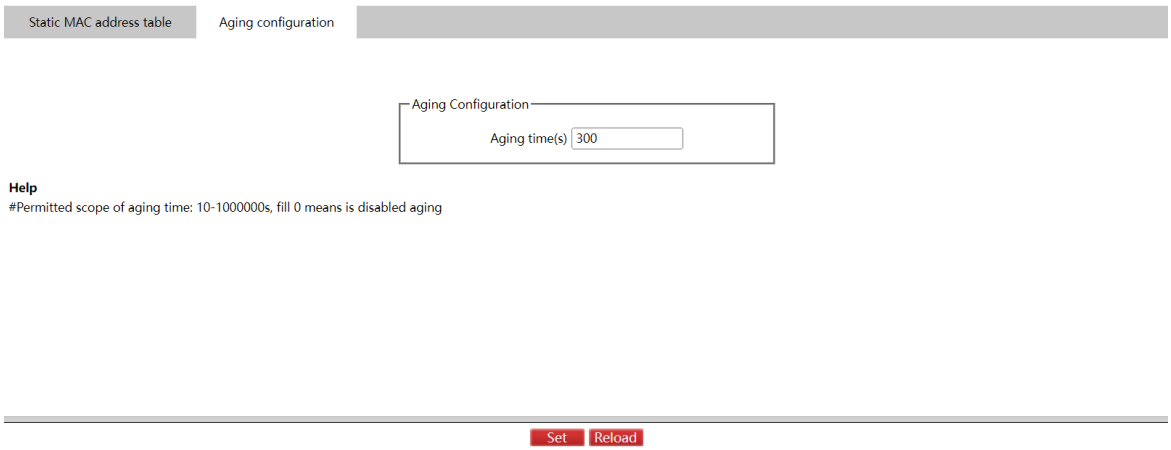
| | Index | Static MAC Address | VLAN ID | Port | Operate |
|---|---|---|---|---|---|
| ☐ | 1 | 2233.1122.4455 | 1 | G0/1 | Modify |

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.



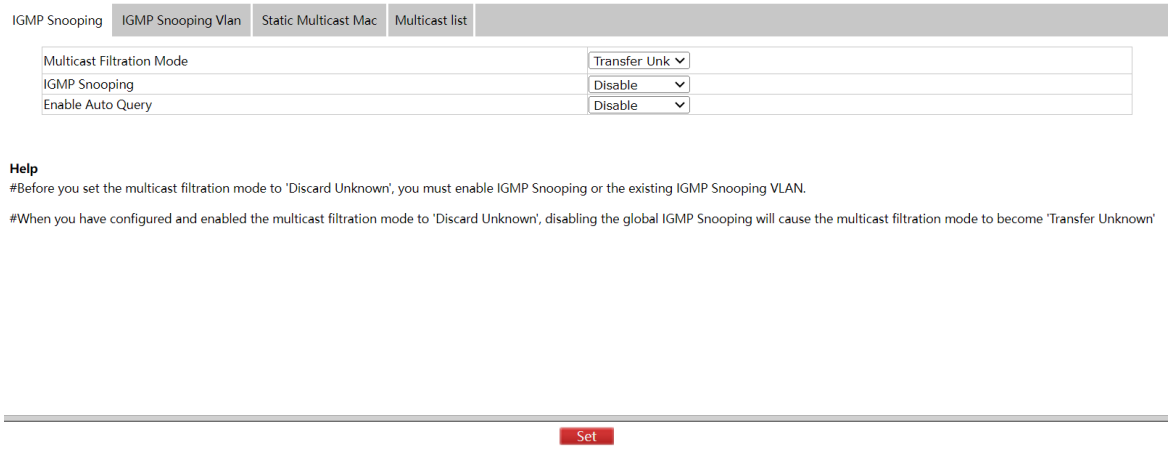

Click “Aging Configuration” on the right of “Static MAC Address Table”, enter the aging configuration page:




# 7.4 IGMP Snooping

## 7.4.1 IGMP Snooping Configuration

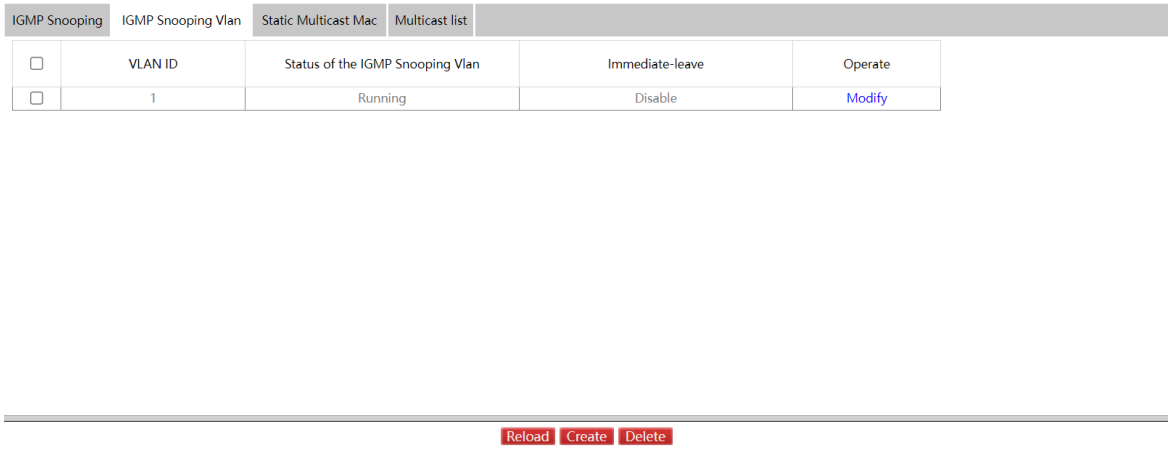
Click Switching -> IGMP Snooping, at navigation bar in order, and select “IGMP Snooping” tab page to enter IGMP Snooping configuration page as following:



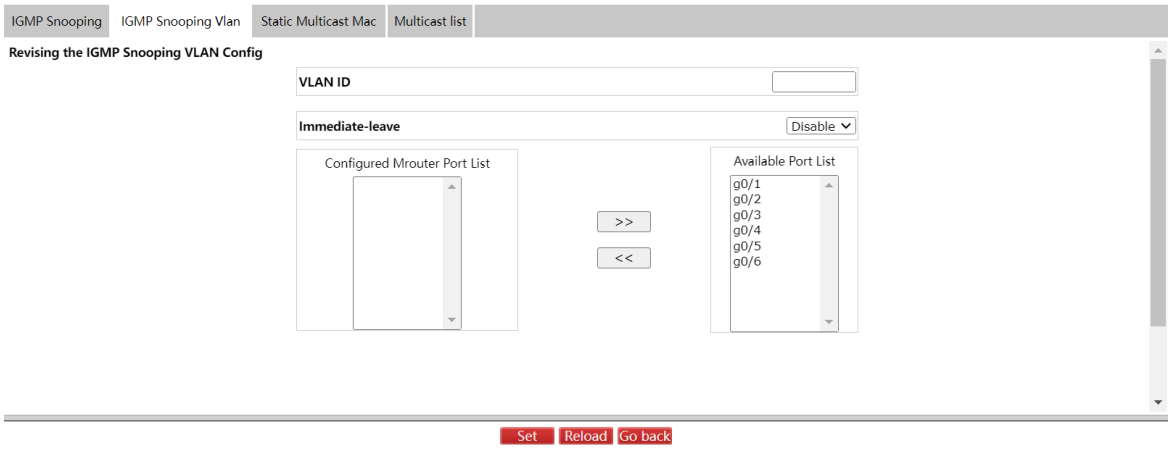

Whether switch forwarding unknown multicast, whether enabling IGMP-Snooping and whether taken as IGMP's Querier can be configured at this page.

## 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:




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 6 physical ports can be set on each IGMP snooping VLAN. Click **Delete**, a selected IGMP-Snooping VLAN can be deleted.

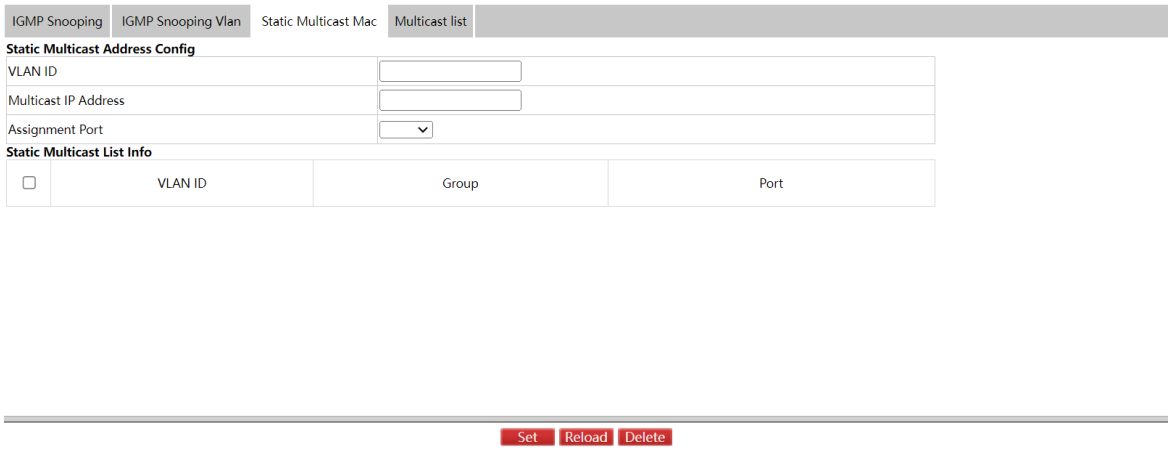



When an IGMP-Snooping VLAN is created, its VLAN ID can be set; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

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:




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 | Port |
|---|---|---|---|
| 6 | 235.2.3.1 | USER | g0/4 |

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

Click **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

| | VLAN ID | VLAN Name | Operate |
|---|---|---|---|
| ☐ | 1 | Default | Modify |

current 1 page/total1 page firstpage beforepage nextpage lastpage goto Di page

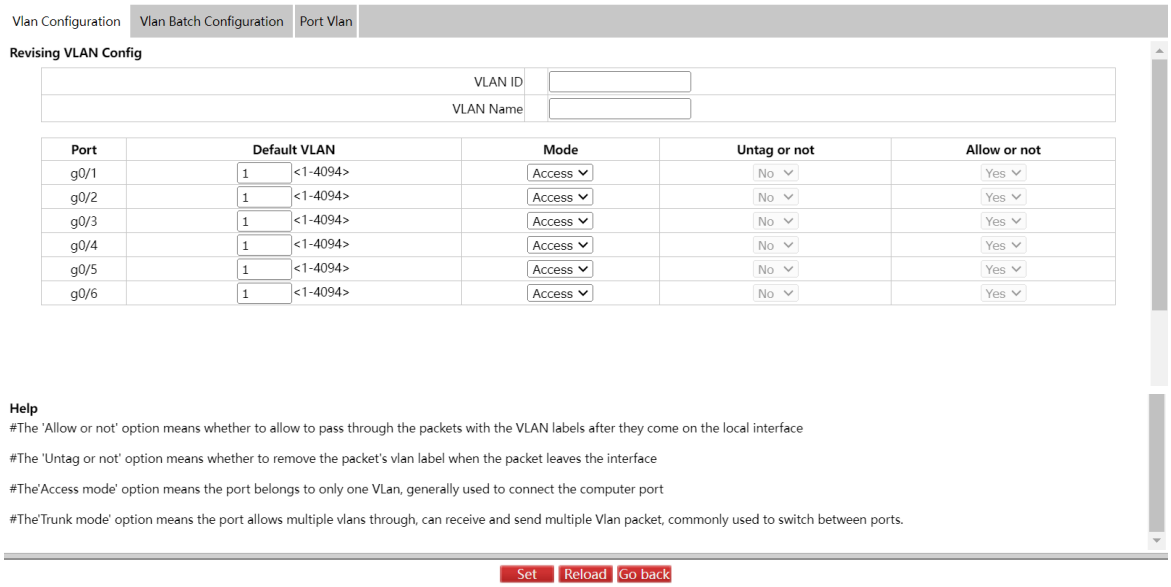
Create Delete

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.



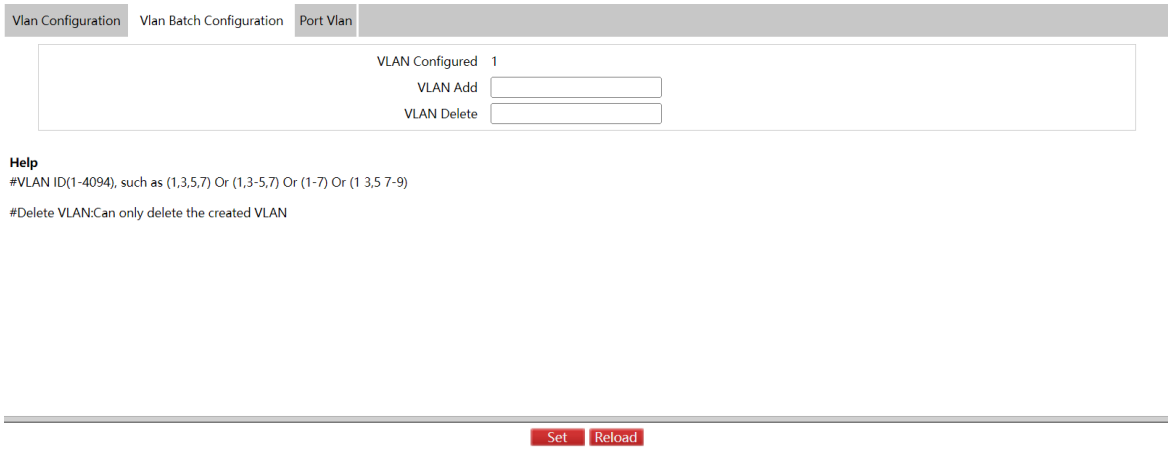

If you want to create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be null.

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

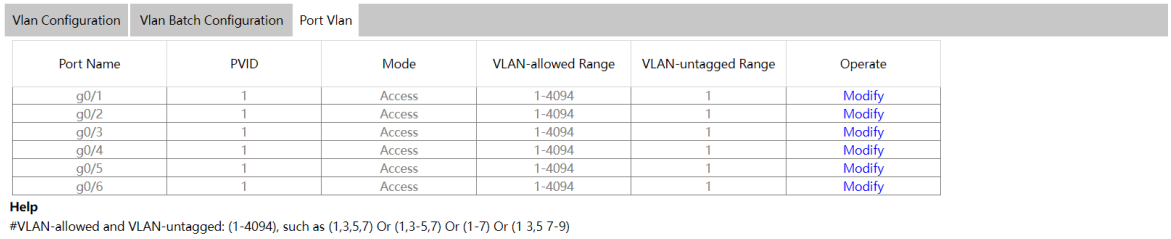
Click **Switching -> VLAN,** at navigation bar in order, and select “VLAN Batch Configuration” tab page to enter VLAN configuration page as following:



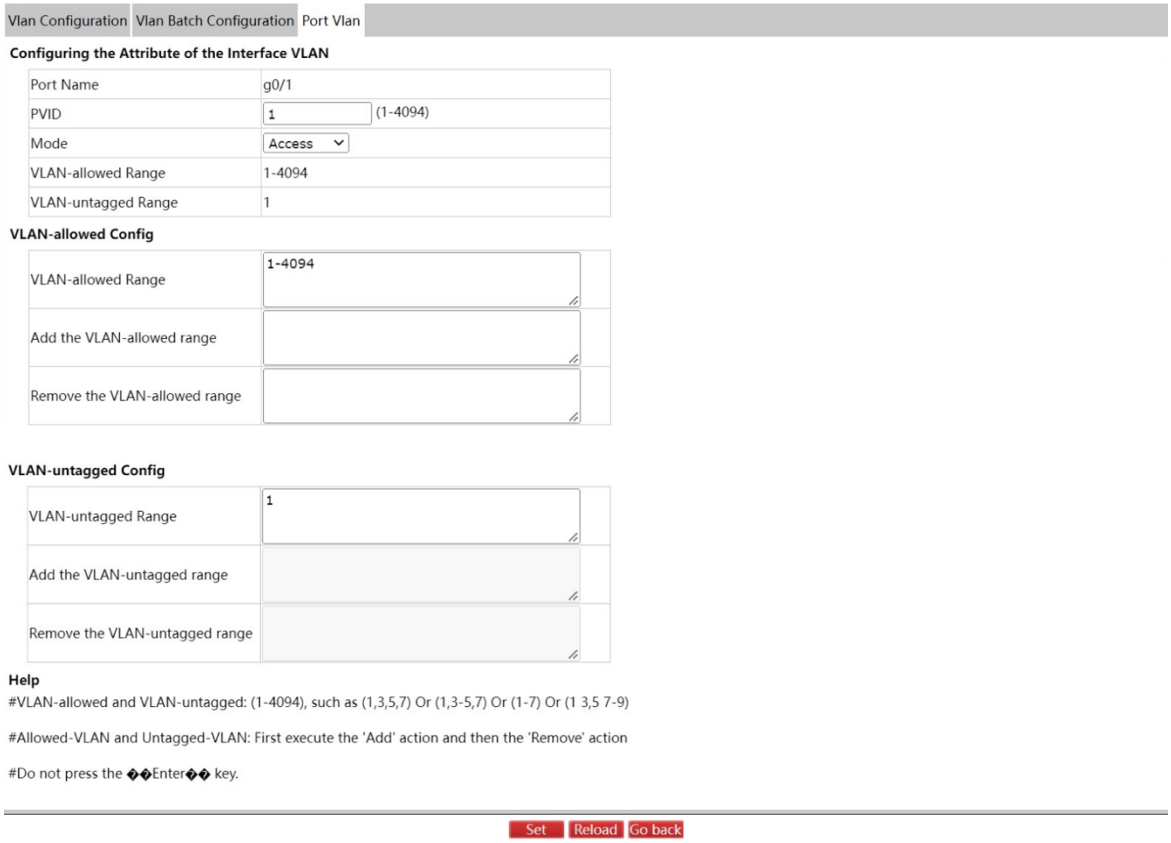

Note:
Before VLAN to be deleted, it should be added first.

## 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:

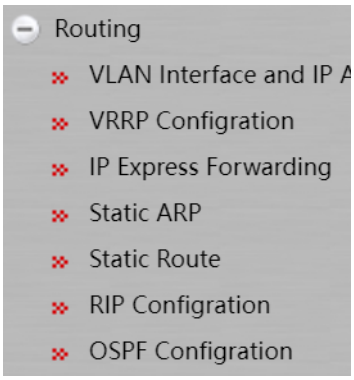



This page shows all ports’ PVIDs, modes, allowed VLAN range and VLAN range without tag. Click **Modify** to change port’s VLAN feature configuration, VLAN-allowed configuration and VLAN-untagged configuration.




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

# 8 Routing




## 8.1 VLAN Interface and IP Address Configuration

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

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

current 1 page/total 1 page firstpage beforepage nextpage lastpage goto Di page

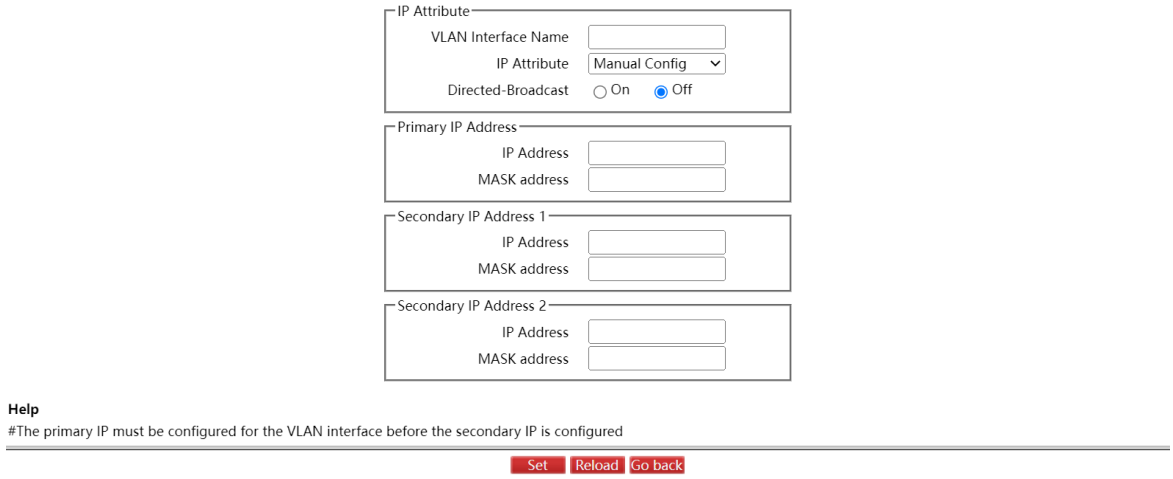
Reload Create Delete

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.

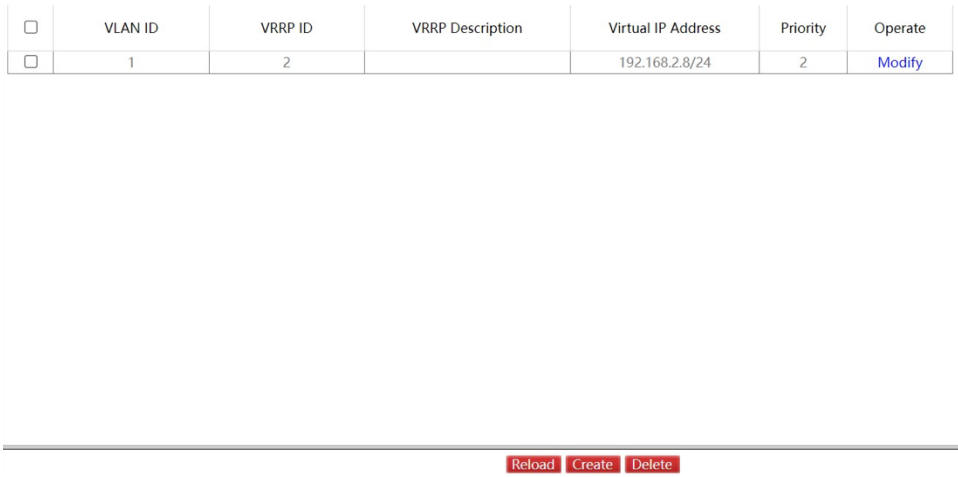
You can change the VLAN name when you click the “Create” bottom. It’s cannot change VLAN name when click “Modify” just can do the VLAN related items modification.




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:



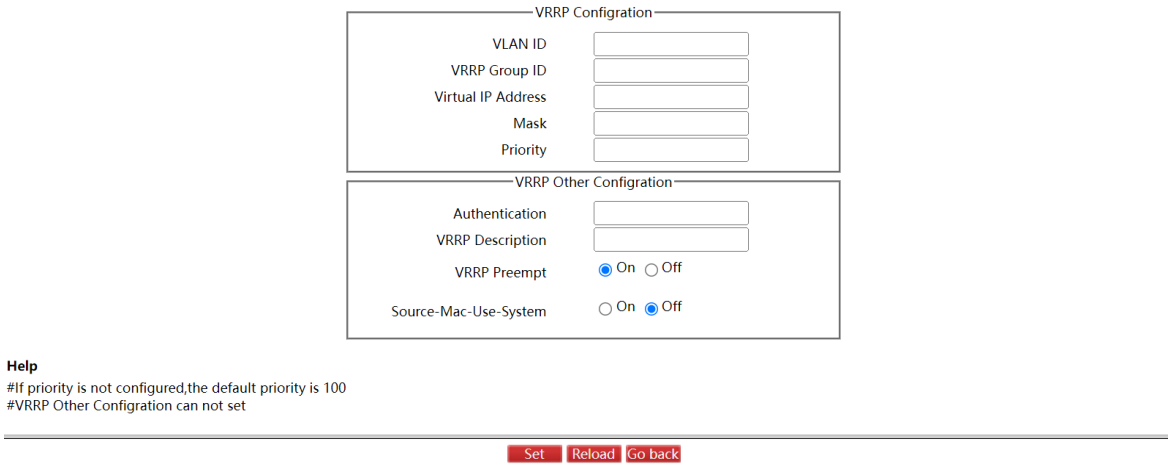
| | VLAN ID | VRRP ID | VRRP Description | Virtual IP Address | Priority | Operate |
|---|---|---|---|---|---|---|
| ☐ | 1 | 2 | | 192.168.2.8/24 | 2 | Modify |

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:

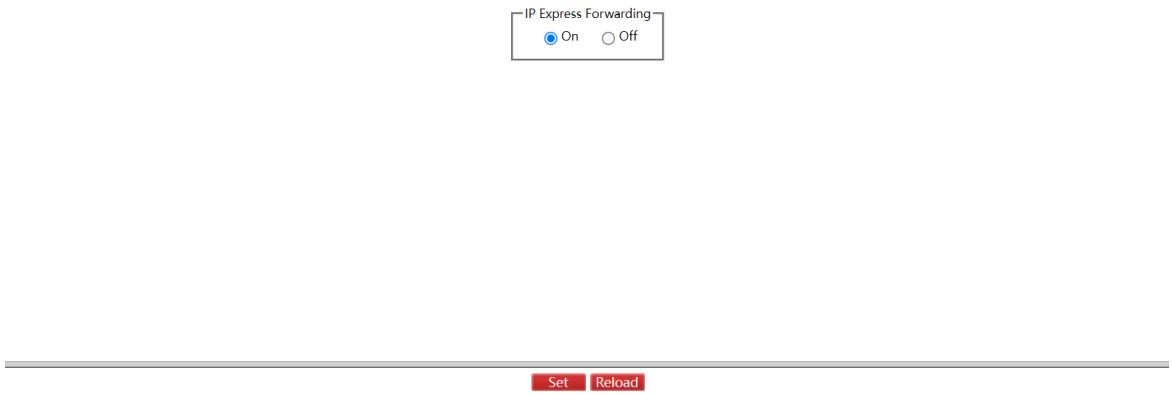



Click **Set** at the bottom control bar, finish the configuration of VRRP and other information.

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:




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

| | IP Address | MAC Address | Interface VLAN | Operate |
|---|---|---|---|---|
| ☐ | 192.168.0.2 | 22:00:11:33:22:33 | 2 | Modify |
| ☐ | 192.168.0.9 | 22:11:22:33:55:44 | 1 | Modify |

Reload Create Delete

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

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

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

ARP Config

IP Address

MAC Address

Interface VLAN

**Help**

#MAC:The mac address only supports the unicast address and has the following formats:XXXXXXXXXXXX,XXXX.XXXX.XXXX,XX:XX:XX:XX:XX:XX,XX-XX-XX-XX-XX-XX, and X is Hex number

Set Reload Go back

# 8.5 Static Route

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

| | Default Route | Dest IP Segment | Dest IP Mask | Interface Type | VLAN Interface | Gateway's IP Address | Forwarding Routing Address | Distance metric | Routing Tag | Specify the route description | Operate |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | false | 192.168.3.0 | 255.255.255.0 | Null0 | | | | | | | Modify |

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 | |
| Specify Route Description | |

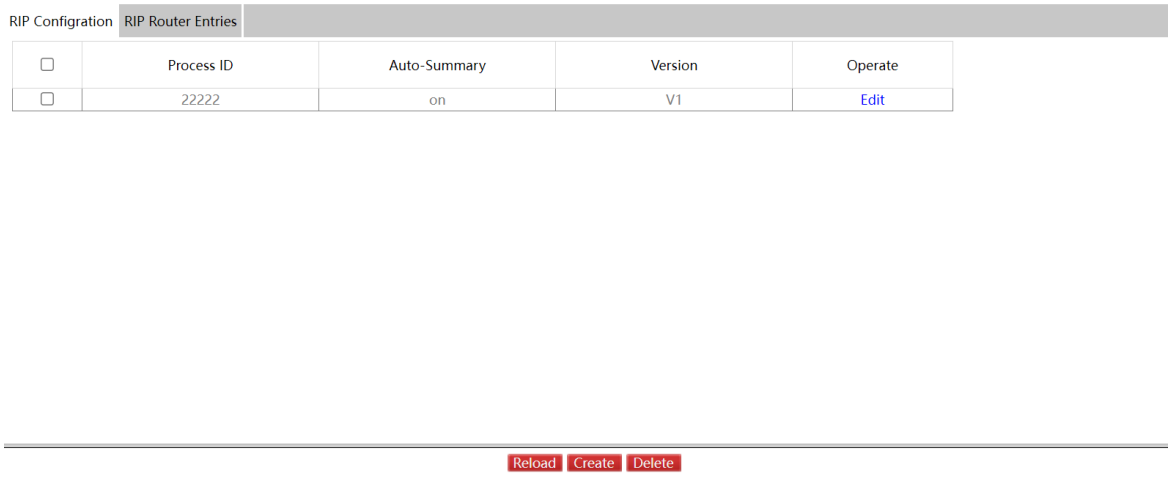
Set Reload Go back

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

# 8.6 RIP Configuration

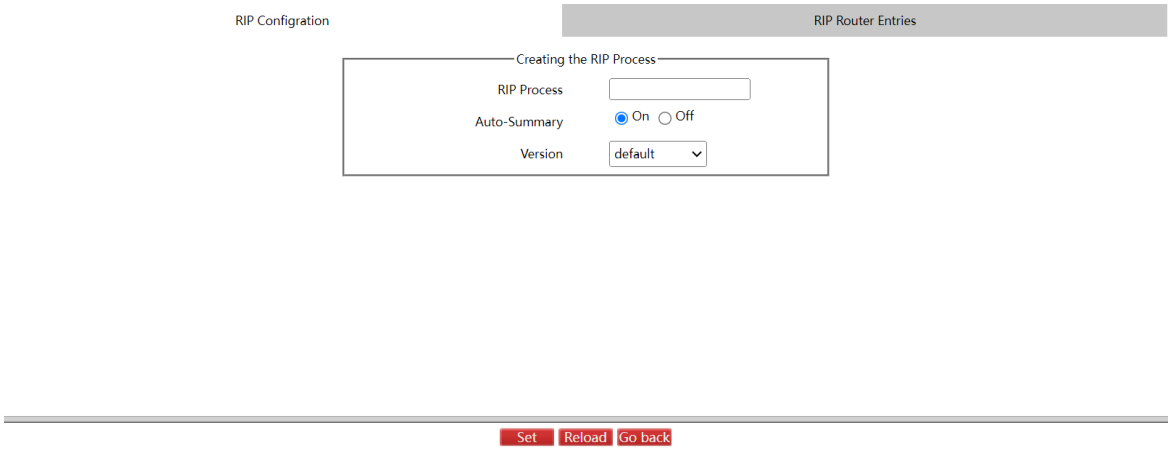
## 8.6.1 RIP Configuration

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



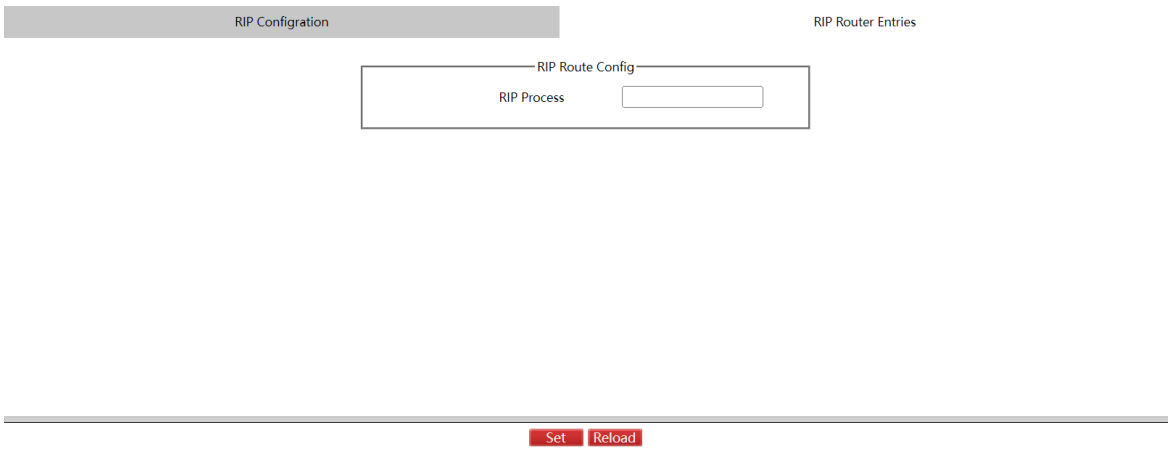

You should have created a RIP process firstly, before do the RIP entry configuration. When **Edit** the RIP process can create the new RIP process or delete it also.

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

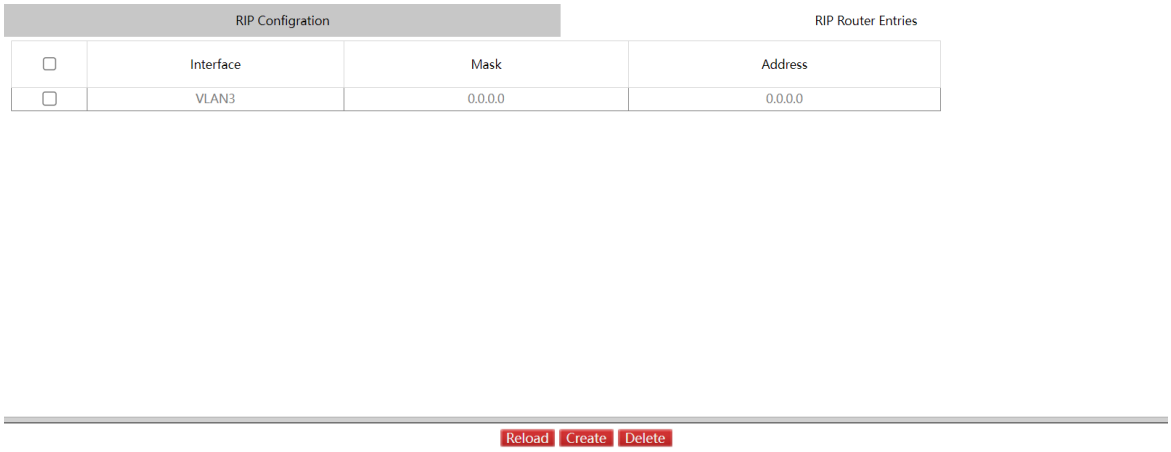



## 8.6.2 RIP Router Entries

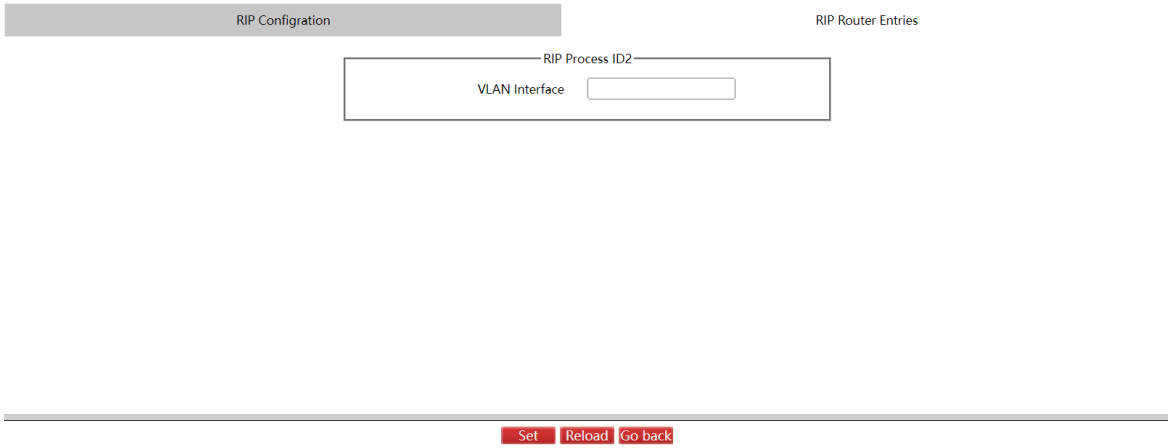
Click **Routing -> RIP Configuration** at navigation bar in order, and then click **RIP Router Entries** to enter RIP Router Entries configuration page as following：



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



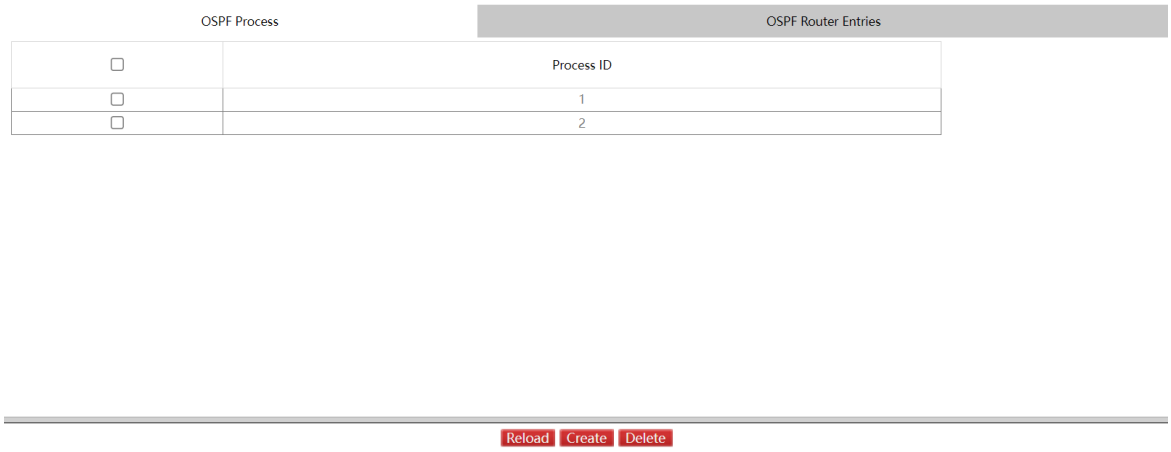

Click **Create** to create a new RIP Router Entries of selected RIP process.




# 8.7 OSPF Configuration

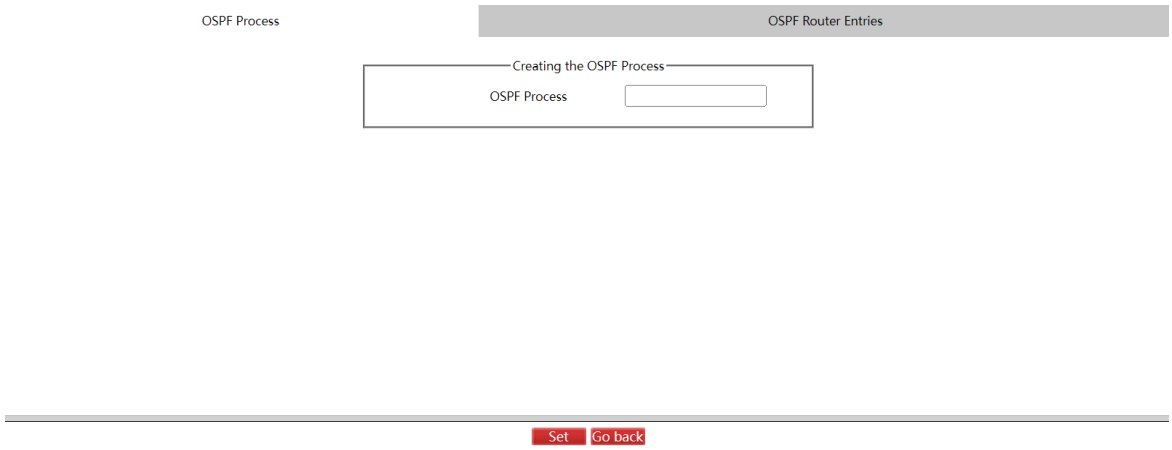
## 8.7.1 OSPF process

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



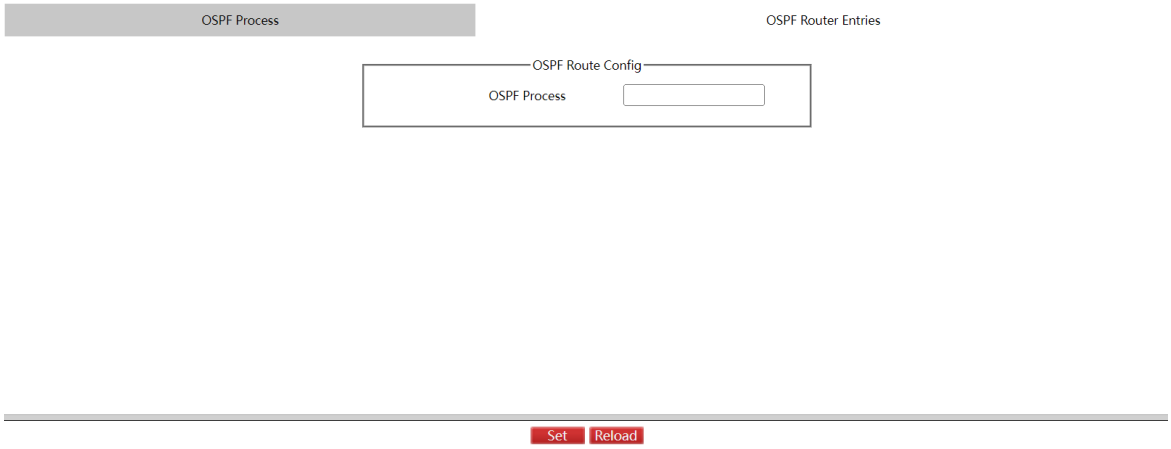

You should have created a OSPF process firstly, before to do the OSPF Router Entries configuration otherwise cannot do any editing.

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

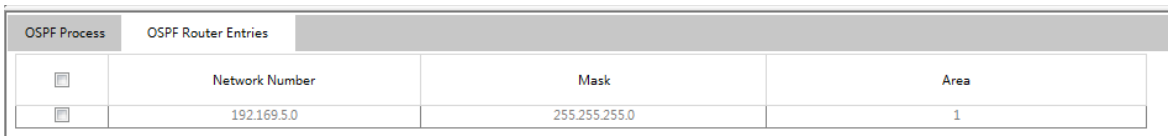



## 8.7.2 OSPF Router Entries

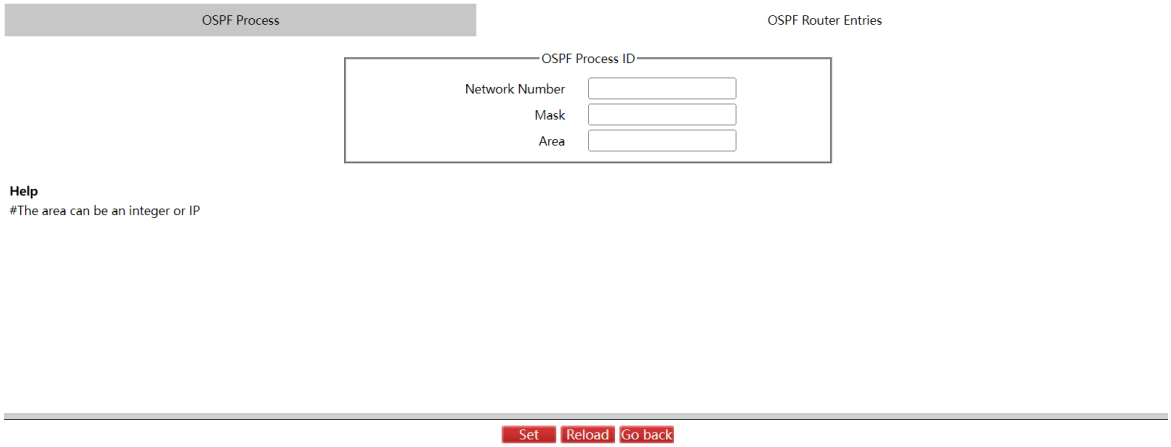
Click **Routing -> OSPF Configuration** at navigation bar in order, and then click **OSPF Router Entries** to enter OSPF Router Entries configuration page as following:




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




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

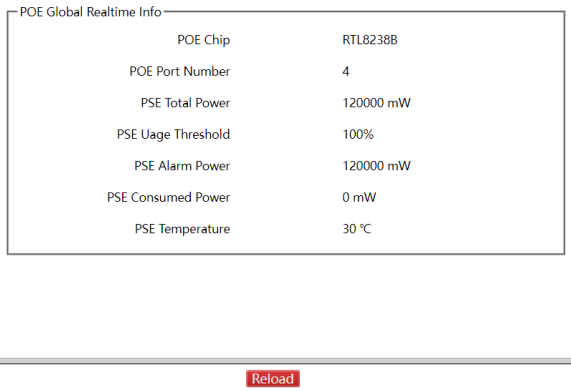



The format that the **Area** column can accept is an integer or IP address。

# 9 POE Mgr


## 9.1 POE Global RT information

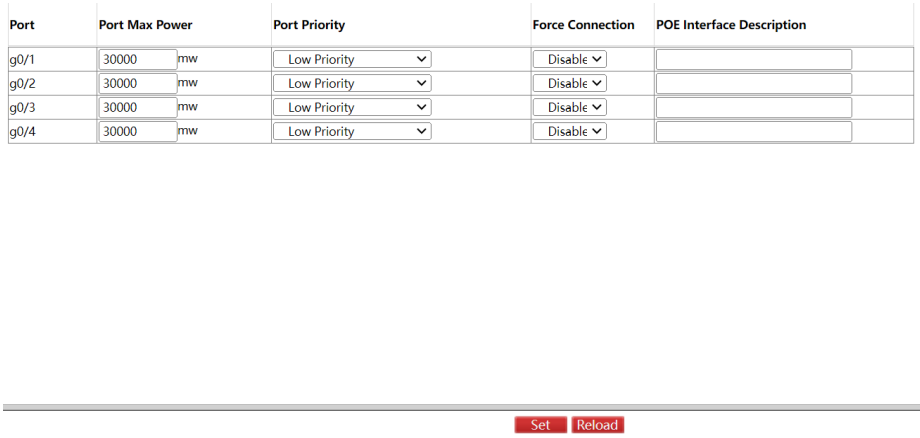
Click **POE Mgr -> POE Global RT Info** at navigation bar in order, and then enter the POE Global Realtime Information page as following:




This page shows the POE Chip, POE port number, PSE Toal Power, PSE Usage Threshold, PSE Alarm Power, PSE Consumed Power and PSE Temperature.

## 9.2 POE Interface List

Click **POE Mgr -> POE Intf List** at navigation bar in order, and then enter the POE Interface List page as following:



You can set the Port Max Power, Port Priority (Critical Priority, High Priority, Low Priority), Force Connection (Enable, Disable) and POE Interface Description.

Click the **Set** at the bottom control bar, to save the changing configurations.

Click the **Reload** to refresh the information of the POE port.

## 9.3 POE Interface Policy Power

Click **POE Mgr -> POE Intf Policy Power** at navigation bar in order, and then enter the POE Port Policy Power page as following:

| Port | POE Function | Time Range |
|---|---|---|
| g0/1 | Enable | |
| g0/2 | Disable | |
| g0/3 | Enable | |
| g0/4 | Enable | |

Set Reload

On this page, you can set the POE function (Enable, Disable) of each POE port. When the POE function disabled, the Time Range can be set. After all the POE ports configured, then click the **Set** at the bottom control bar to finish the settings.

Click Reload to refresh the Information of this page.

## 9.4 POE Interface Power Realtime Information

Click **POE Mgr -> POE Intf Power RT Info** at navigation bar in order, and then enter the POE Port Power Realtime Information page as following:

| Port | Current Power | Setting Max Power | Average Power | Peak Power | Bottom Power |
|---|---|---|---|---|---|
| g0/1 | 0mw | 30000mw | - | - | - |
| g0/2 | 0mw | 30000mw | - | - | - |
| g0/3 | 0mw | 30000mw | - | - | - |
| g0/4 | 0mw | 30000mw | - | - | - |

PSE Total Power 0

Reload

On this page, you can check the POE port's power information, such as Current Power, Setting Max Power, Average Power, Peak Power, Bottom Power.

Click **Reload** to refresh the information on this page.

## 9.5 POE Interface Other Realtime Information

Click **POE Mgr -> POE Intf Other RT Info** at navigation bar in order, and then enter the POE Port Other Realtime Information page as following:

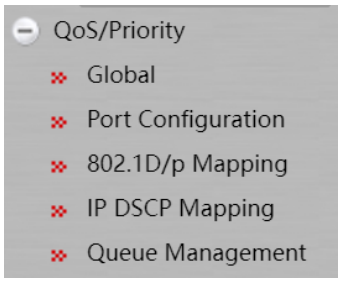
| Port | POE Port Detection Status | POE Port Power Supply | POE IEEE Class | POE Port Current |
|---|---|---|---|---|
| g0/1 | Searching | Signal | 0 | 0mA |
| g0/2 | Searching | Signal | 0 | 0mA |
| g0/3 | Searching | Signal | 0 | 0mA |
| g0/4 | Searching | Signal | 0 | 0mA |

Reload

On this page, you can check other realtime information of each POE port, such as POE Port Detection Status, POE Port Power Supply, POE IEEE Class, POE Port Current.

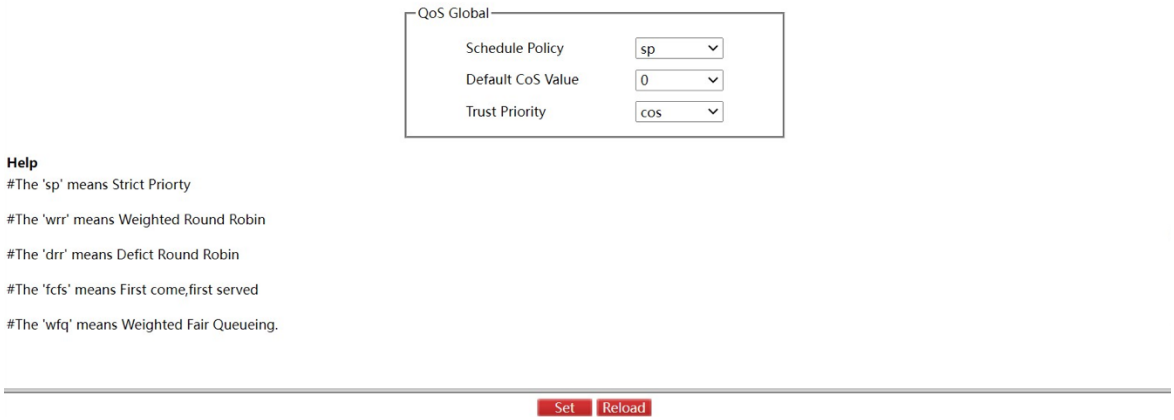
Click Reload at the bottom control bar to refresh the information of this page.

# 10 QoS/Priority




## 10.1 Global

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




You can do the settings of Schedule Policy, Default CoS Value and Trust Priority in the QoS Global page.

## 10.2 Port Configuration

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

| Port | CoS value |
|---|---|
| g0/1 | |
| g0/2 | |
| g0/3 | |
| g0/4 | |
| g0/5 | |
| g0/6 | |

Set Reload

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

## 10.3 802.1D/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 2 |
| 2 | Queue 3 |
| 3 | Queue 4 |
| 4 | Queue 5 |
| 5 | Queue 6 |
| 6 | Queue 7 |
| 7 | Queue 8 |

Set Reload

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

## 10.4 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 |
|---|---|---|
| 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 |

Set Reload Clear

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.

Click **Reload** to refresh the information of each DSCP.

Click **Set** to save the changes of the DSCP.

Note:

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

## 10.5 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 | (1-127) |
| 2 | 1 | (1-127) |
| 3 | 1 | (0-127) |
| 4 | 1 | (0-127) |
| 5 | 1 | (0-127) |
| 6 | 1 | (0-127) |
| 7 | 1 | (0-127) |
| 8 | 1 | (0-127) |

**Help**

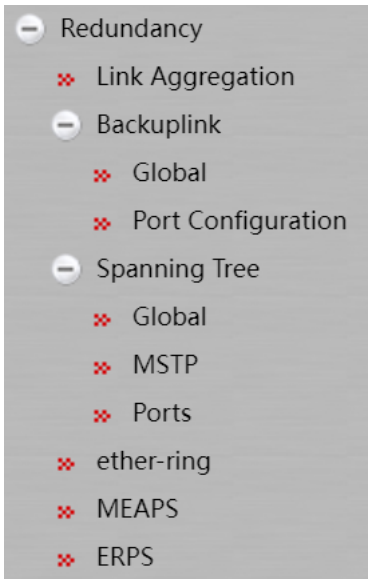
#if the bandwidth of queue has been set to 0, the queue after this also must be set to 0

Set Reload

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.

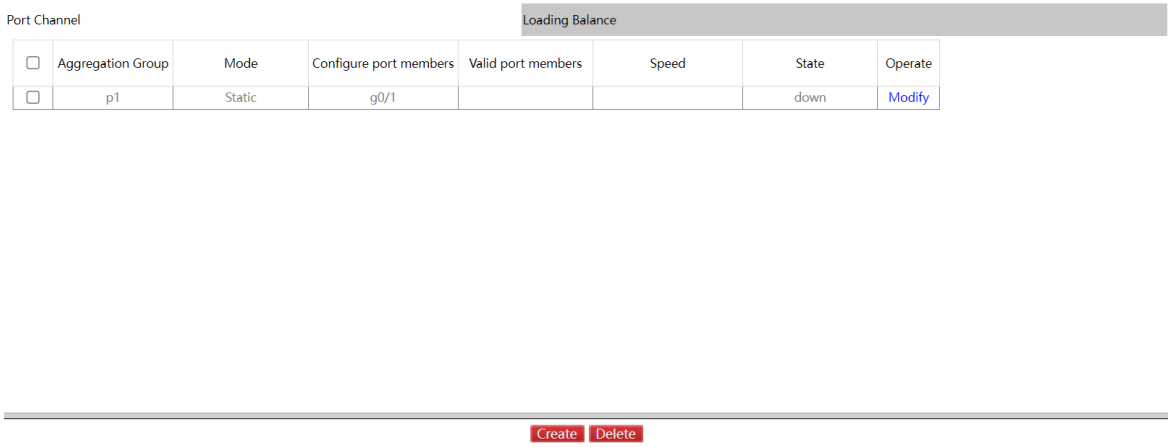
# 11 Redundancy




## 11.1 Link Aggregation Configuration

### 11.1.1 Port Aggregation Configuration

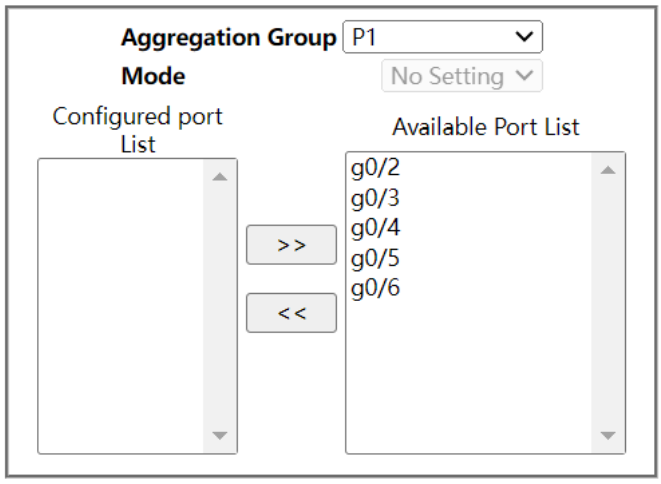
Click **Redundancy -> Link Aggregation** at navigation bar in order, and then enter the link aggregation configuration port channel page as following:




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.



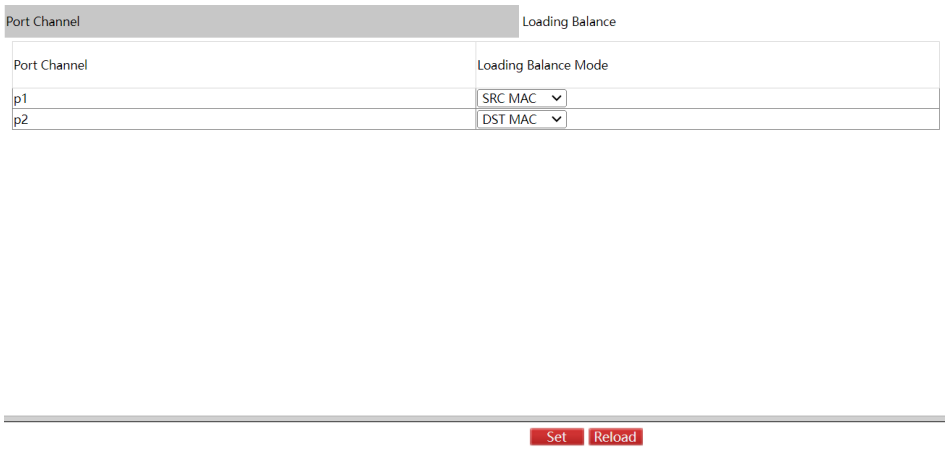

An aggregation group is selectable when it is created but is not selectable when it is modified.

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 "**>>**".

### 11.1.2 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.

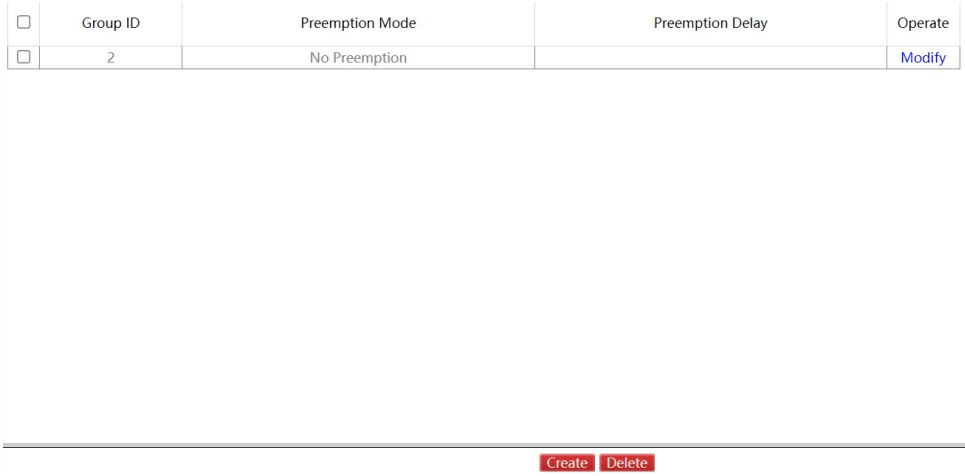



You can set different aggregation modes for different aggregation groups.

# 11.2 Backup Link

## 11.2.1 Backup Link Global Configuration

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




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.


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.

### 11.2.2 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 |
|---|---|---|---|---|---|
| g0/1 | | | | | Modify |
| g0/2 | | | | | Modify |
| g0/3 | | | | | Modify |
| g0/4 | | | | | Modify |
| g0/5 | | | | | Modify |
| g0/6 | | | | | Modify |

Set Reload

The page lists the member port has joined the backup link group, port attribute of the member port, MMU attribute, Share load 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 | |
| Interface Attribute | |
| MMU Attribute | |
| Shareload VLAN | |

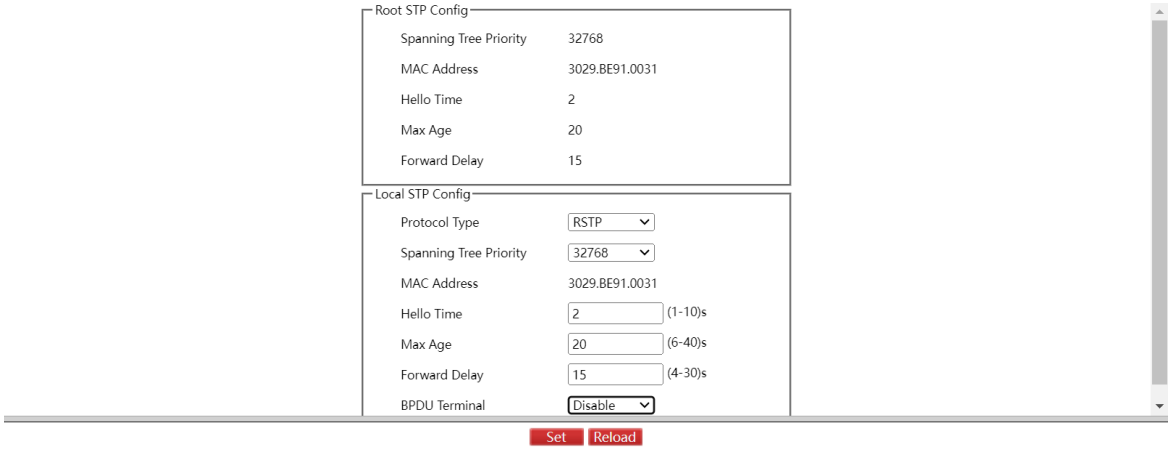
Set Reload Go back

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.

## 11.3 Spanning Tree

### 11.3.1 Global

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

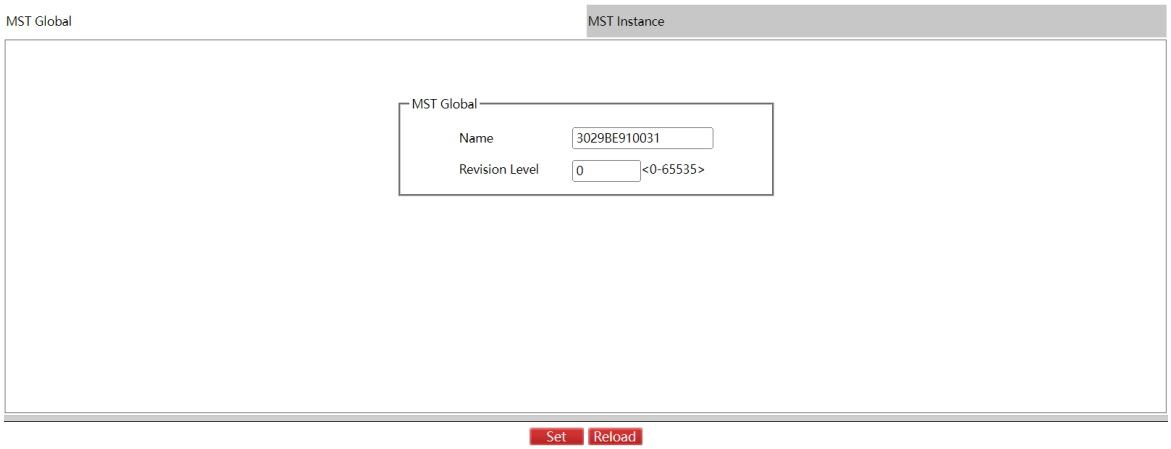



The page can configure the local STP protocol, such as protocol type, spanning tree priorities etc. Click **Set** to save configuration.

## 11.3.2 MSTP

### 11.3.2.1 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:




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

Click **Set** to save configuration.

### 11.3.2.2 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 | | | | | | Modify |
| 1 | | 32768 | | | | | | Modify |
| 2 | | 32768 | | | | | | Modify |
| 3 | | 32768 | | | | | | Modify |
| 4 | | 32768 | | | | | | Modify |
| 5 | | 32768 | | | | | | Modify |
| 6 | | 32768 | | | | | | Modify |
| 7 | | 32768 | | | | | | Modify |
| 8 | | 32768 | | | | | | Modify |
| 9 | | 32768 | | | | | | Modify |
| 10 | | 32768 | | | | | | Modify |
| 11 | | 32768 | | | | | | Modify |
| 12 | | 32768 | | | | | | Modify |
| 13 | | 32768 | | | | | | Modify |
| 14 | | 32768 | | | | | | Modify |
| 15 | | 32768 | | | | | | Modify |

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.

MST Global | MST Instance

Configuration Instance 3

VLAN Mapping

Priority 32768

Bridge ID

Root ID

Root Path Cost

Root Port

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

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.

## 11.3.3 Spanning Tree Ports

### 11.3.3.1 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 |
|---|---|---|---|---|---|---|---|---|
| g0/1 | Enable | 128 | 0 | Disable | Disable | none | Disable | Disable |
| g0/2 | Enable | 128 | 0 | Disable | Disable | none | Disable | Disable |
| g0/3 | Enable | 128 | 0 | Disable | Disable | none | Disable | Disable |
| g0/4 | Enable | 128 | 0 | Disable | Disable | none | Disable | Disable |
| g0/5 | Enable | 128 | 0 | Disable | Disable | none | Disable | Disable |
| g0/6 | Enable | 128 | 0 | Disable | Disable | none | Disable | Disable |

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.

### 11.3.3.2 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 |
|---|---|---|---|---|---|
| g0/2 | Desg | FWD | 20000 | 128.2 | Edge |

Reload

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

## 11.4 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:

| ☐ | Ring ID | Node Type | Ring Description | Control VLAN | Status | Hello | Fail | Preforward | Primary Port/Forwarding/Link Status | Secondary Port/Forwarding/Link Status | Operate |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 0 | Master-node | | 2 | RingFail | 1 | 3 | 3 | None/Blocking/Linkdown | None/Blocking/Linkdown | Modify |

Reload Create Delete

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:

ether-ring Configuration

| | | |
|---|---|---|
| Ring ID | 0 | |
| Node Type | Master Node | |
| Ring Description | | |
| Control VLAN | | |
| Hello Time | 1 | (1-10)s |
| Fail Time | 3 | (3-30)s |
| Preforward Time | 3 | (3-30)s |
| Primary Port | None | |
| Secondary Port | 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.

## 11.5 MEAPS

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

| ☐ | Domain ID | Ring ID | Ring Type | Node Type | Control Vlan | Hello Time | Failed Time | Pre Forward Time | Port | Type | Port | Type | Operate |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 2 | 2 | Major Ring | Master Node | 3 | 3 | 9 | 9 | None | Primary-Port | None | Secondary-Port | Modify |

Reload Create Delete

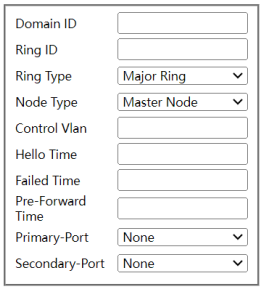
The list displays the currently configured MEAPS ring, including the Domain ID, Ring ID, Ring Type, Node Type, Control VLAN, Hello Time, Failed Time, Pre Forward Time and the Primary/Secondary Port on the ring.

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 new 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.





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.

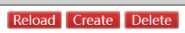
In the text boxes of “Primary Port” and “Secondary Port”, select a port as the ring port respectively or select “None”.

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

## 11.6 ERPS

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

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 3 | 2 | 1 | Protection | False | 20 | 500 | 5 | g0/1/Blocking/Linkdown | g0/4/Blocking/Linkdown | Modify |



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.

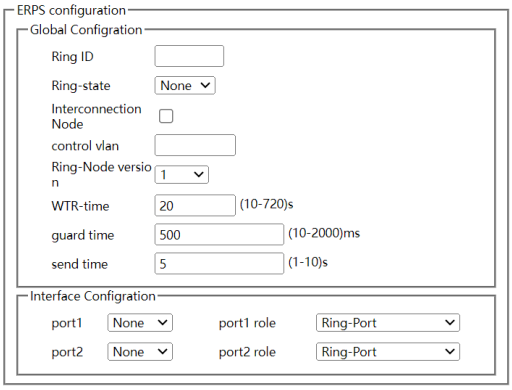
Note:

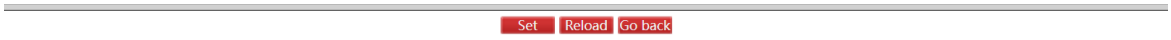
1. This system only supports ERPS single ring configuration.

2. Max 8 ERPS ring node.

3. Once one ERPS has been configured, its 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:




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

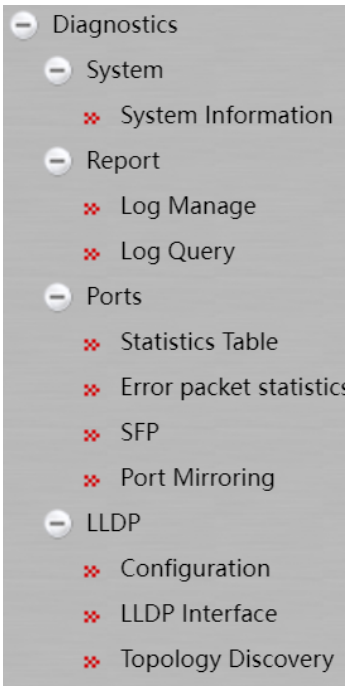
After the port 1 and port 2 configured, the corresponding port role should be configured.

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 ring ID, ring type, node type and control Vlan cannot be configured

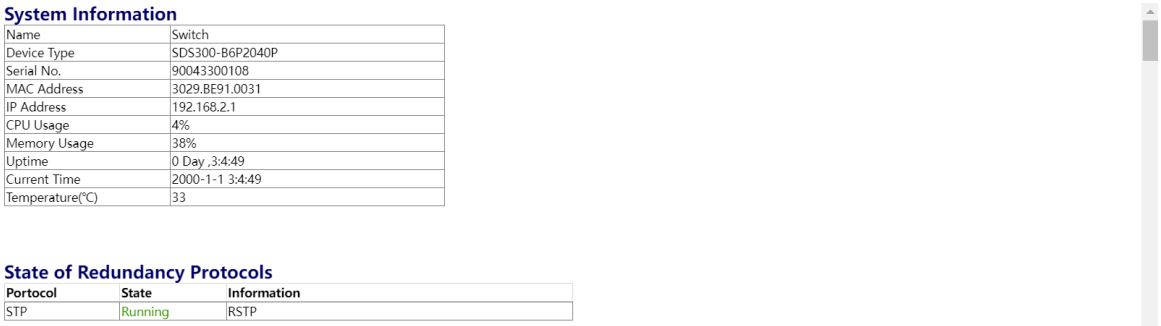
# 12 Diagnostics




## 12.1 System

### 12.1.1 System Information

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



**System Information**

| | |
|---|---|
| Name | Switch |
| Device Type | SDS300-B6P2040P |
| Serial No. | 90043300108 |
| MAC Address | 3029.BE91.0031 |
| IP Address | 192.168.2.1 |
| CPU Usage | 4% |
| Memory Usage | 38% |
| Uptime | 0 Day ,3:4:49 |
| Current Time | 2000-1-1 3:4:49 |
| Temperature(℃) | 33 |

**State of Redundancy Protocols**

| Portocol | State | Information |
|---|---|---|
| STP | Running | RSTP |

**Port Configuration**

| Port | Enable | State | Speed | Duplex | Flow Control |
|---|---|---|---|---|---|
| g0/1 | enabled | down | auto | auto | Off |
| g0/2 | enabled | up | auto | auto | Off |
| g0/3 | enabled | down | auto | auto | Off |
| g0/4 | enabled | down | auto | auto | Off |
| g0/5 | enabled | down | auto | auto | Off |
| g0/6 | enabled | down | auto | auto | Off |

**Port Statistics**

| Port | Send Bytes | Send Packets | Receive Bytes | Receive Packets | Discard | Discard Rate |
|---|---|---|---|---|---|---|
| g0/1 | 0 | 0 | 0 | 0 | 0 | 0% |
| g0/2 | 5678702 | 10484 | 1018616 | 7024 | 0 | 0% |
| g0/3 | 0 | 0 | 0 | 0 | 0 | 0% |
| g0/4 | 0 | 0 | 0 | 0 | 0 | 0% |
| g0/5 | 0 | 0 | 0 | 0 | 0 | 0% |
| g0/6 | 0 | 0 | 0 | 0 | 0 | 0% |

**Used Management Ports**

| Portocol : | SNMP | HTTP | HTTPS |
|---|---|---|---|
| Port: | 161 | 80 | 443 |

Display More Diagnostic Information

The page lists the system information, state of redundancy protocol, port configuration, port statistics, user management port. Click **Display More Diagnostic Information** can check more information such as CPU utilization, task information and etc.

**Tasks:**

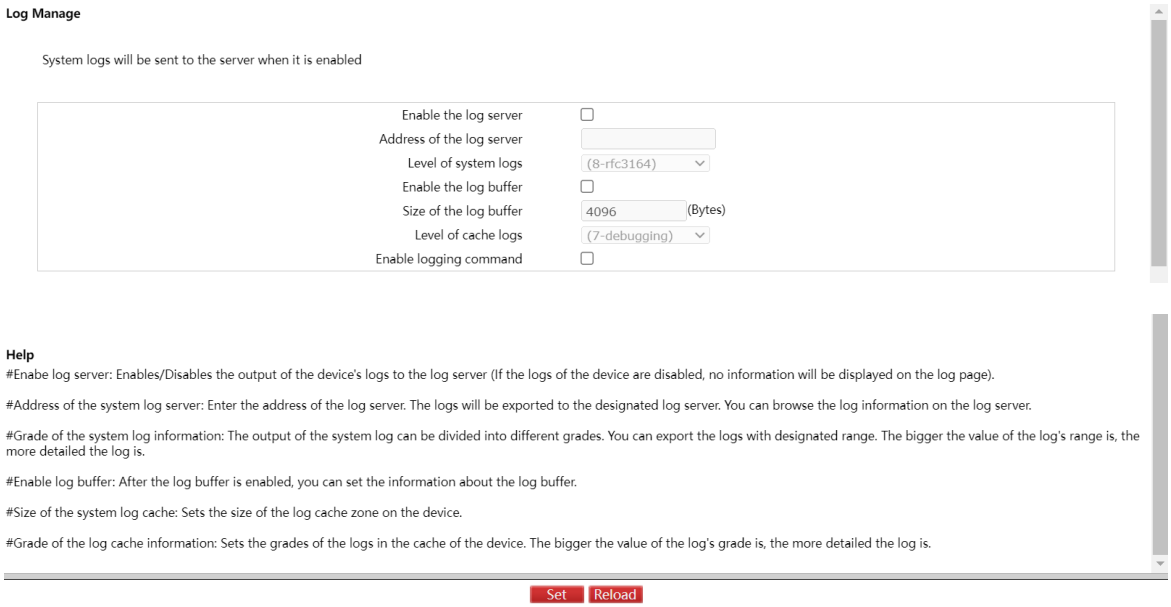
```
CPU utilization for one second: 4; one minute: 4; five minutes: 4
    P - Pending D - Delay       R - Ready       S - Suspend     E - Estimated
NAME   ENTRY  TID      PRI   PC      Stk Ptr  SP lmt   ERR.NO ST   CPU   invoked
-------------------------------------------------------------------------------
tExc 80969ad8 815b8750 000 80990368 815bec00 815bcd18 000000 P   0.00E        0
tJob 8096ab9c 815e5280 000 80990368 815e5118 815e3340 000000 P   0.00E        3
tLog 8096b338 815e93d8 000 8098dde8 815e9278 815e8050 000000 P   0.00E        0
IDLE 803c441c 84b204d0 255 803c4424 84b20310 84b1e4d0 000000 R  96.99  1105335
RCVR 803c4f08 84b42660 060 8098dde8 84b42388 84b32660 000000 P   0.01        1
ATDT 803c5438 84b546d0 180 8098dde8 84b543d0 84b4c6d0 000000 P   0.00       93
DM   801aac14 87edbcc0 128 8098dde8 87edb9f0 87ed3cc0 000000 P   0.00        4
SLOG 803e3844 87ef0340 128 8098dde8 87eeff28 87eec340 000000 P   0.00       57
STRL 803e48d0 87ef6600 128 8098dde8 87ef6310 87ef2600 000000 P   0.00       26
_USM 8091192c 84b88f60 128 8098dde8 84b88c60 84b78f60 000000 P   0.00        1
CPRI 809a8ed4 84b99210 128 8098dde8 84b98f28 84b89210 000000 P   0.00        1
_NTM 803bada8 84ba14c0 055 809967c0 84ba1268 84b994c0 000000  D  0.16  1108760
waMo 8073147c 84bb0280 200 80990368 84bb0180 84bac280 3d0004 R   0.00E    22167
```

Set Reload

# 12.2 Report

## 12.2.1 Log Management

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

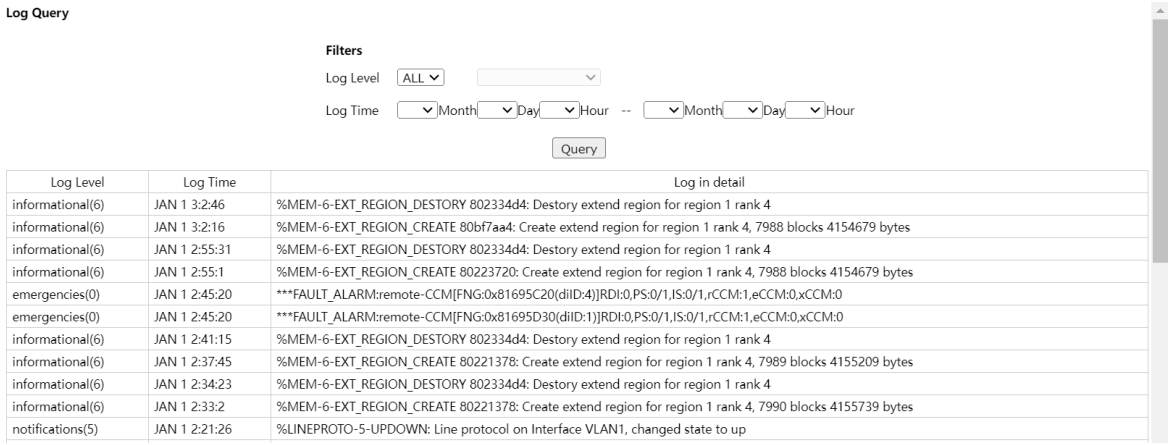



When **Enabling the log server** was selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the Web Configuration "**Address of the system log server**" textbox and select the log's grade in the "Grade of the system log information" dropdown box (grade 9 – rfc5424 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 log buffer" textbox and select the grade of the cached log in the "Grade of the cache log information" dropdown box.

## 12.2.2 Log Query

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




| Log Level | Log Time | Log in detail |
|---|---|---|
| informational(6) | JAN 1 3:2:46 | %MEM-6-EXT_REGION_DESTORY 802334d4: Destory extend region for region 1 rank 4 |
| informational(6) | JAN 1 3:2:16 | %MEM-6-EXT_REGION_CREATE 80bf7aa4: Create extend region for region 1 rank 4, 7988 blocks 4154679 bytes |
| informational(6) | JAN 1 2:55:31 | %MEM-6-EXT_REGION_DESTORY 802334d4: Destory extend region for region 1 rank 4 |
| informational(6) | JAN 1 2:55:1 | %MEM-6-EXT_REGION_CREATE 80223720: Create extend region for region 1 rank 4, 7988 blocks 4154679 bytes |
| emergencies(0) | JAN 1 2:45:20 | ***FAULT_ALARM:remote-CCM[FNG:0x81695C20(diiID:4)]RDI:0,PS:0/1,IS:0/1,rCCM:1,eCCM:0,xCCM:0 |
| emergencies(0) | JAN 1 2:45:20 | ***FAULT_ALARM:remote-CCM[FNG:0x81695D30(diiID:1)]RDI:0,PS:0/1,IS:0/1,rCCM:1,eCCM:0,xCCM:0 |
| informational(6) | JAN 1 2:41:15 | %MEM-6-EXT_REGION_DESTORY 802334d4: Destory extend region for region 1 rank 4 |
| informational(6) | JAN 1 2:37:45 | %MEM-6-EXT_REGION_CREATE 80221378: Create extend region for region 1 rank 4, 7989 blocks 4155209 bytes |
| informational(6) | JAN 1 2:34:23 | %MEM-6-EXT_REGION_DESTORY 802334d4: Destory extend region for region 1 rank 4 |
| informational(6) | JAN 1 2:33:2 | %MEM-6-EXT_REGION_CREATE 80221378: Create extend region for region 1 rank 4, 7990 blocks 4155739 bytes |
| notifications(5) | JAN 1 2:21:26 | %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN1, changed state to up |

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.

# 12.3 Ports

## 12.3.1 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 | 11298 | 1587481 | 9765 | 1394 | 139 | 18655 | 10668543 | 13084 | 5571 | 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% |
| g0/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% |
| g0/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% |

Reload Clear

The page lists the port information, including the Receive Packets, Receive Bytes, Received Unicast Packets, Received Multicast Packets, Received Broadcast Packets …etc.

## 12.3.2 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 |
|---|---|---|---|---|---|---|---|---|---|
| g0/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| g0/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| g0/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| g0/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| g0/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| g0/6 | 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.

## 12.3.3 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 (℃) | Supply Voltage (V) | Bias (mA) |
|---|---|---|---|---|---|

Reload

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

## 12.3.4 Port Mirroring

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

Mirror Port

Disable

| Mirrored Port | Enabled | Mirror Mode |
|---|---|---|
| g0/1 | ☐ | RX |
| g0/2 | ☐ | RX |
| g0/3 | ☐ | RX |
| g0/4 | ☐ | RX |
| g0/5 | ☐ | RX |
| g0/6 | ☐ | RX |

Set Reload

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 。

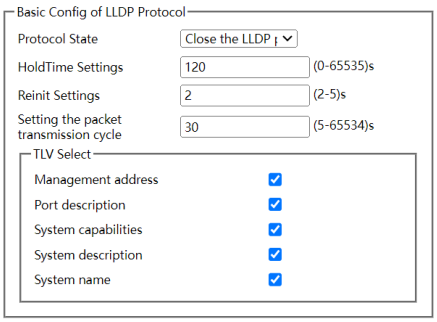
TX The transmitted packets will be mirrored to a destination port。

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

# 12.4 LLDP Configuration

## 12.4.1 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.

## 12.4.2 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 | ☑ | ☑ | ☑ |
| g0/2 | Disable | Disable | ☑ | ☑ | ☑ |
| g0/3 | Disable | Disable | ☑ | ☑ | ☑ |
| g0/4 | Disable | Disable | ☑ | ☑ | ☑ |
| g0/5 | Disable | Disable | ☑ | ☑ | ☑ |
| g0/6 | Disable | Disable | ☑ | ☑ | ☑ |

Set Reload

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.

## 12.4.3 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 |
|---|---|---|---|---|---|---|---|

LLDP | LLDP-MED

| PORT | Hardware Revision | Software Revision | Serial Number | Manufacturer Name | Model Name | Asset ID |
|---|---|---|---|---|---|---|

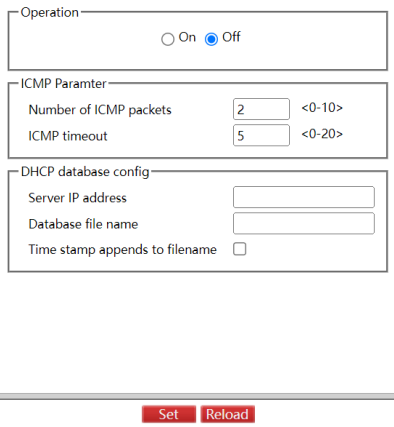
The page lists the devices that have been found by this device.

# 13 Advanced


## 12.1 DHCP Server

### 13.1.1 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:




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.

### 13.1.2 DHCP Server Pool Configuration

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

| | Name | Network number | Network mask | Address range | Address lease time | Operate |
|---|---|---|---|---|---|---|
| ☐ | 1 | 192.168.3.0 | 255.255.255.0 | | Infinite | Modify |

Reload Create Delete

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

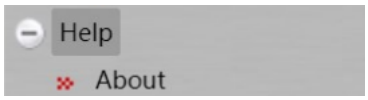
Address range Add

-

Address lease time Default

Set Reload Go back

# 14 Help




## 14.1 About

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

**Version 2.2.0D Build 114471**

(Build 114471)

Copyright (c) 2022

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 ---