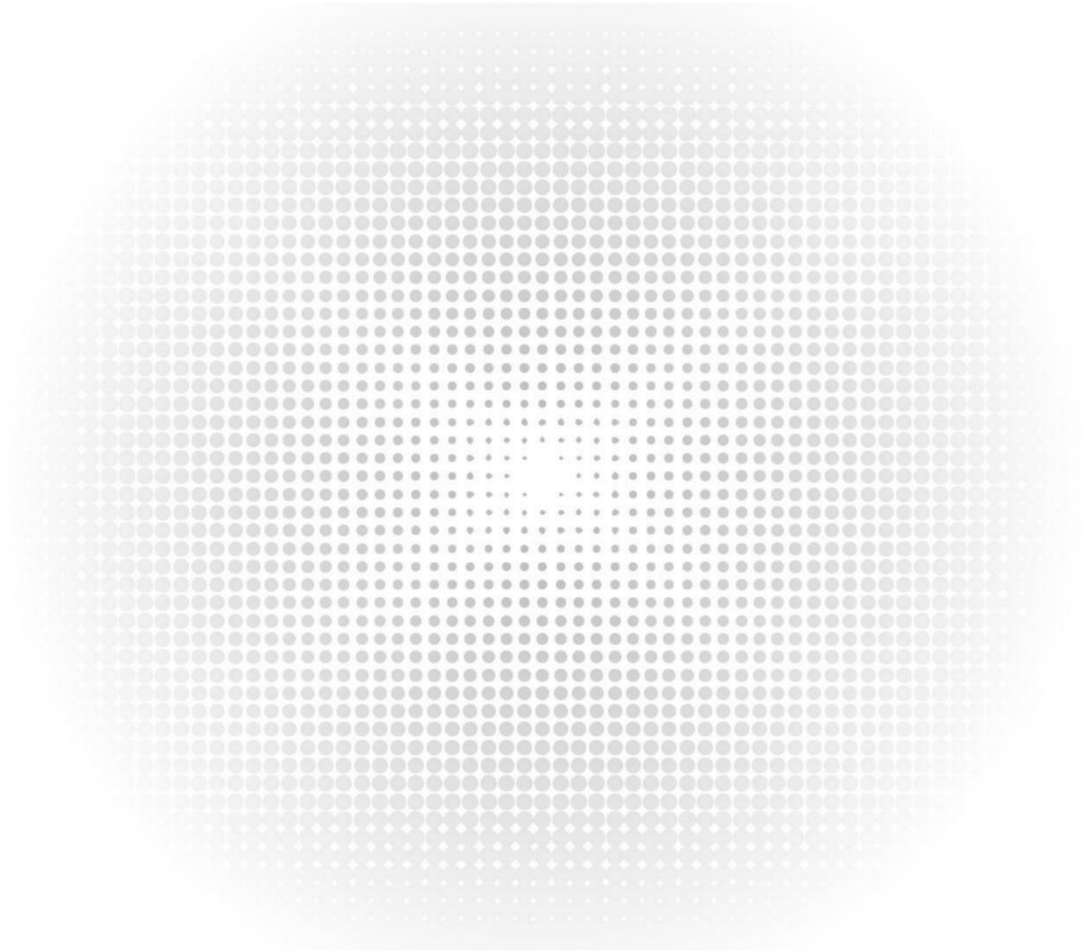
S3400 Series Switches Web-based Configuration Guide

Models: S3400-48T6SP、S3400-24T4SP、S3400-24T4FP



Content

Chapter 1 HTTP Switch Configuration

1.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and SNMP but also through Web browser. The switches support the HTTP configuration, the abnormal packet timeout configuration, and so on.

1.1.1 Choosing the Prompt Language

Up to now, switches support two languages, that is, English and Chinese, and the two languages can be switched over through the following command.

Command	Purpose
[no] ip http language {english}	Sets the prompt language of Web configuration to **English**.

1.1.2 Setting the HTTP Port

Generally, the HTTPportisport80bydefault, 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 192.168.1.3 and **1234** respectively, the HTTP access address should be changed to **http://192.168.1.3:1234**.You'd better not use other common protocols' ports so that access collision should not happen. 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{*port Number*}	Sets the HTTP 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 the switch and PC, when the HTTP service is closed, HTTP exchange stops.

Command	Purpose
ip http server	Enables the HTTP service.

1.1.4 Setting the HTTP Access Mode

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	Command
ip http http-accessenable	Sets the HTTP access mode.

1.1.5 Configuring HTTP application access-list

Command	Command
ip http access-list {name}	Configures HTTP application access-list.

1.1.6 Setting the automatic disconnection time after timeout on the Web page

The switch supports a timeout range of 180 seconds to 1800 seconds, with a default of 300 seconds.

Command	Command
ip http session timeout {seconds}	Configures to disconnect the web connection if there has been no activity for a certain number of seconds.

1.1.7 Setting whether to display footer.asp on the Web page

By default, the switch page does not display this content. Clicking on 'About' on the page can make it display at the bottom of the page.

Command	Command
ip http web use-footer	Configures to display the footer.asp page on the Web page.

1.1.8 Setting the Maximum Number of VLAN Entries on Web Page

A switch supports at most 4094 VLANs and in most cases Web only displays parts of VLANs, that is, those VLANs users want to see. You can use the following command to set the maximum number of VLANs. The default maximum number of VLANs is 100.

Command	Command

ip http web max-vlan {*max-vlan*}	Sets the maximum number of VLAN entries displayed in a web page.

1.1.9 Setting the Maximum Number of MAC address Entries on Web Page

A switch supports at most 500 MACs. The default maximum number of MACs is 100.

Command	Command
ip http web max-macaddr-table {*max-macadr-table*}	Sets the maximum number of MAC entries displayed in a web page.

1.1.10 Setting the Maximum Number of Multicast Entries Displayed on a Web Page

A switch supports at most 100 multicast entries. You can run the following command to set the maximum number of multicast entries, and then show these multicast entries. The default maximum number of multicast entries is 15.

Command	Command
ip http webigmp-groups {*igmp-groups*}	Sets the maximum number of multicast entries displayed on a web page.

1.1.11 Configuring the maximum number of log entries displayed on the Web page

The switch supports up to 2000 log entries. Users can set the maximum log entries using the following command. Only the log entry information from 1 to the set maximum will be displayed on the web. The default number of multicast entries is 2000.

Command	Command
ip http web max-syslogs {syslogs}	The maximum number of multicast entries displayed on the 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 Setting the HTTP Access Mode

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

Command	Command
ip http ssl-accessenable	Sets the HTTPS access mode.

1.2.2 Setting the HTTPS port

As the HTTP port, HTTPS has its default service port, port 443, and you can also run the following command to change its service port. It is recommended to use those ports following port 1024 so as to avoid collision with other protocols' ports.

Parameter	Remarks
ip http secure-port{*port Number*}	Sets the HTTPS port.

1.2.3 Configuring the key for the HTTPS authentication certificate

When creating an SSL authentication certificate, this key is needed for certificate generation. By default, the key value is "kerry".

Parameter	Remarks
ip http private-password {password}	Configures the key for the HTTPS service authentication certificate.

Chapter 2 Accessing the Switch

2.1 Accessing the Switch through HTTP

When accessing the switch through Web, please make sure that the applied browser complies with the following requirements:
HTML of version 4.0
HTTP of version1.1
Java Script TM of version 1.5
What's more, please ensure that the main program file, running on a switch, supports Web access and your computer has already connected the network in which the switch is located.

2.1.1 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 192.168.1.2 and 255.255.255.0, respectively.

2. Open the Web browser and enter **192.168.1.1** in the address bar. It is noted that **192.168.1.1** is the default management address of the switch.

3. If the Internet Explorer browser is used, you can see the dialog box in Figure 1. Both the original username and the password are "admin", which is capital sensitive.

Figure 1: ID checkup of WEB login

4. After successful authentication, the systematic information about the switch will appear on the IE browser.

2.1.2 Upgrading to the Web-Supported Version

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

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.

2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Switch_config#"

3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.

4. Enter the **ip http server** commanding lobal 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 store the current configuration to the configuration file.

2.2 Accessing a Switch through Secure Links

The data between the WEB browser and the switch will not be encrypted if you access a switch through a common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to access the switch.
To do this, you should follow the following steps:
1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.

2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Switch_config#"

3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.

4. Enter the **ip http server** commanding lobal 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.

6. Run **ip httpssl-accessenable** to enable these cure link access of the switch.

7. Run **no ip http http-accessenable** to forbid to access the switch through insecure links.

8. Enter **write** to store the current configuration to the configuration file.

9. Open the WEB browser on the PC that the switch connects, enter 192.168.1.1 on the address bar (**192.168.1.1** 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.

2.3 Introduction of Web Interface

The homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

2.3.1 Top Control Bar

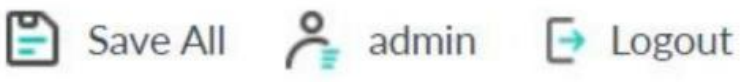


Figure 2: Top control bar

Save All	Write the current settings to the configuration file of the device. It is equivalent to the execution of the **write** command. The configuration that is made through Web will not be promptly written to the configuration file after validation. If you click "Save All", the unsaved configuration will be lost after rebooting.
admin	Current login user
Logout	Exit from the current login state. After you click "logout", you have to enter the username and the password again if you want to continue the Web function.

After you configure the device, the result of the previous step will appear on the left side of the top control bar. If error occurs, please check your configuration and retry it later.

2.3.2 Navigation Bar

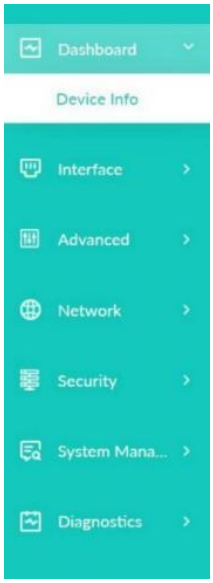


Figure 3 Navigation bar

The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at "Runtime Info" If a certain item need be configured, please click the group name and then the sub-item. For example, to browse information about the current device, you have to click "Device Info"

Note:

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

2.3.3 Configuration Information Area

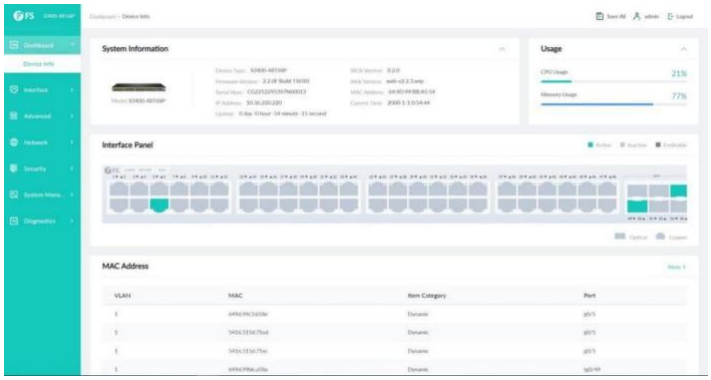


Figure 4 Configuration Area

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.

2.3.4 Configuration Area

The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to the device. The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click “Save All” on the top control bar.
Reset	Means discarding the modification of the sheet. The content of the sheet will be reset.
Clear	
Add	Creates a list item. For example, you can create a VLAN item or a new user.
Delete	Deletes an item in the list.
Batch Delete	Delete multiple items from the list

Chapter 3 Dashboard

3.1 Device Info

If you click **Dashboard > Device Info** in the navigation bar, the **System Information** page appears, as shown in the figure.

Chapter 4 Interface

4.1 Port Config

4.1.1 Port Config

If you click **Interface > Port Config > Port Config** in the navigation bar, the **Port Config** page appears, as shown in figure 1.

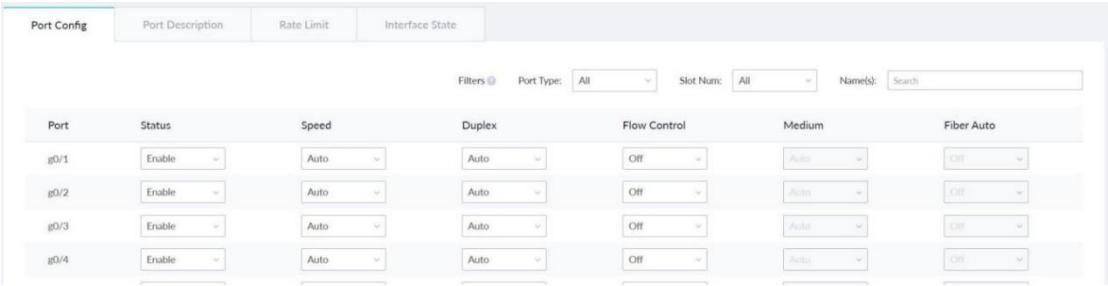


Figure 1 Configuring the port attributes

On this page you can modify the on/off status, rate, duplex mode, flow control status and medium type of a port.

Note:

After the speed or duplex mode of a port is modified, the link state of the port may be switched over and the network communication may be impaired.

4.1.2 Port Description

If you click **Interface > Port Config > Port description** in the navigation bar, the **Port description** page appears, as shown in the figure.

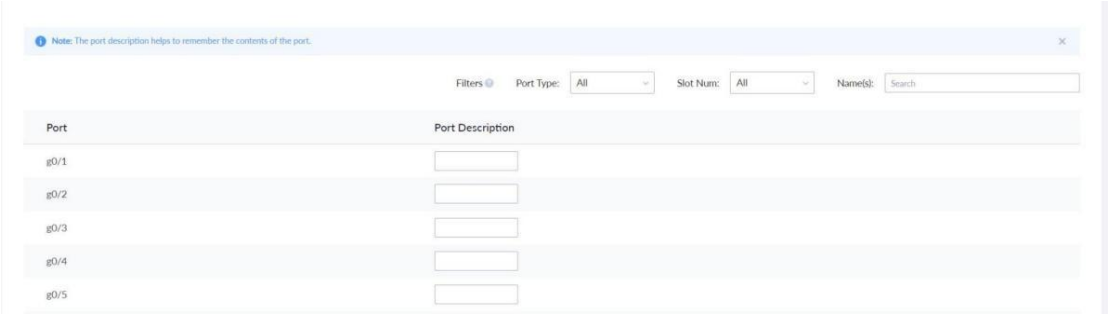


Figure 2: Port description configuration

You can modify the port description on this page and enter up to 120 characters (Chinese character is not supported). The description of the VLAN port cannot be set at present.

4.1.3 Rate Limit

If you click **Interface > Port Config > Rate Limit** in the navigation bar, the **Rate Limit** page appears, as shown in figure 3.

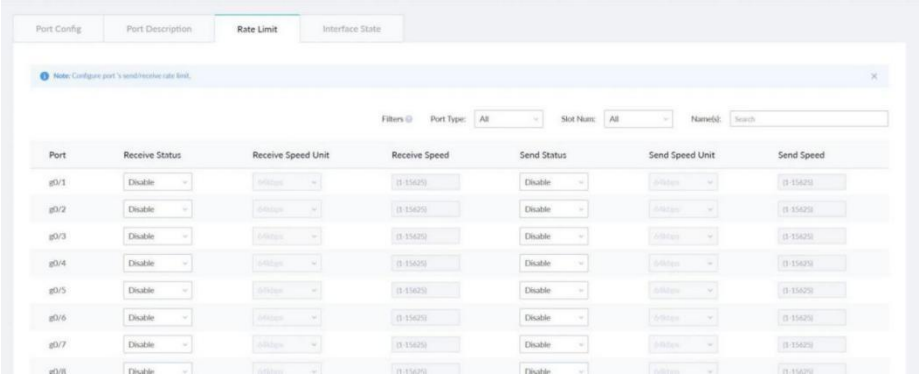


Figure 3 Port's rate limit

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited. The receiving and sending rates can be configured either by percentage or by specific units of the switch.

4.1.4 Interface State

If you click **Interface > Port Config > Interface State** in the navigation bar, the **Interface State** page appears, as shown in the figure 4.

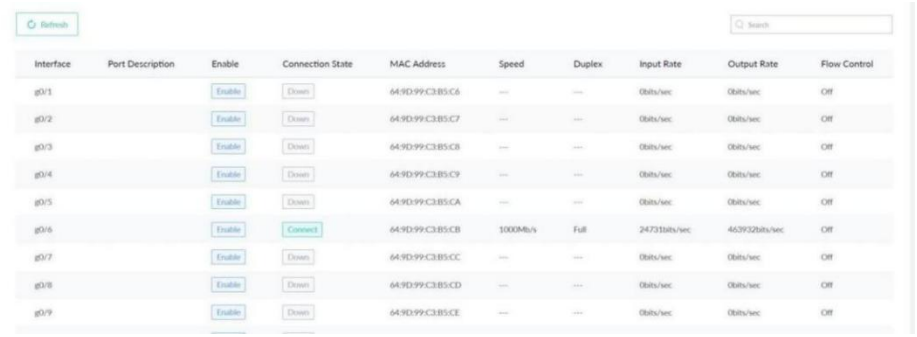


Figure 4 Interface State

4.2 Storm Control

In the navigation bar, click **Interface > Storm Control**. The system then enters the page, on which the broadcast/multicast/unknown unicast storm control can be set.

4.2.1 Broadcast Storm Control

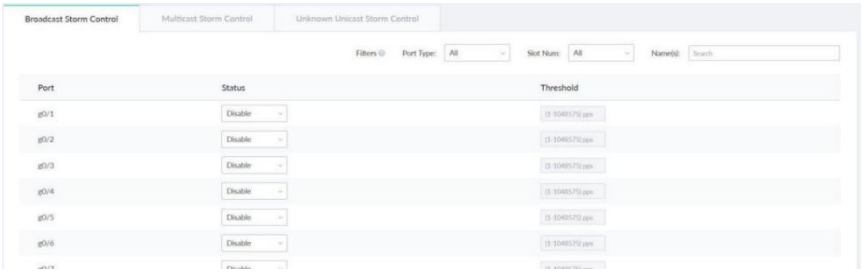


Figure 5 Broadcast storm control

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

4.2.2 Multicast Storm Control

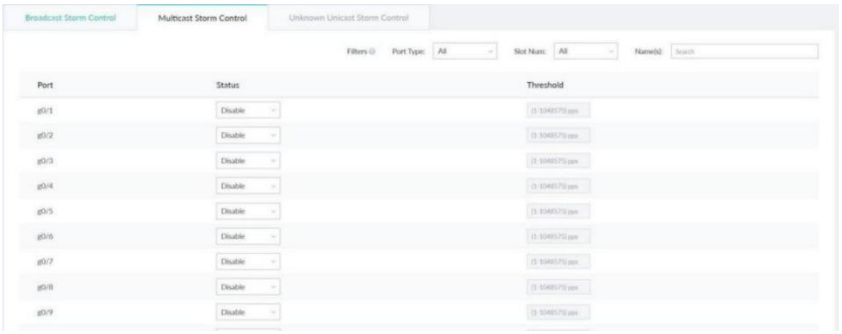


Figure 6 Setting the broadcast storm control

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

4.2.3 Unknown Unicast Storm Control

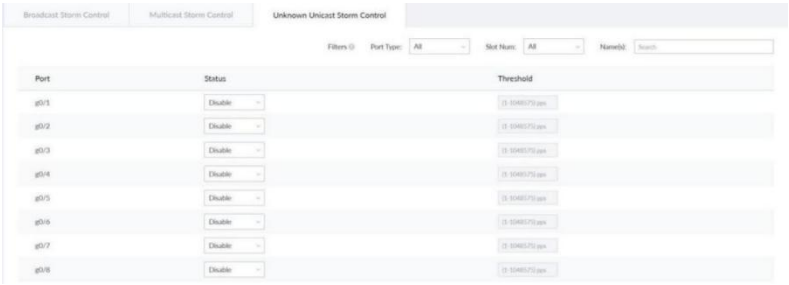
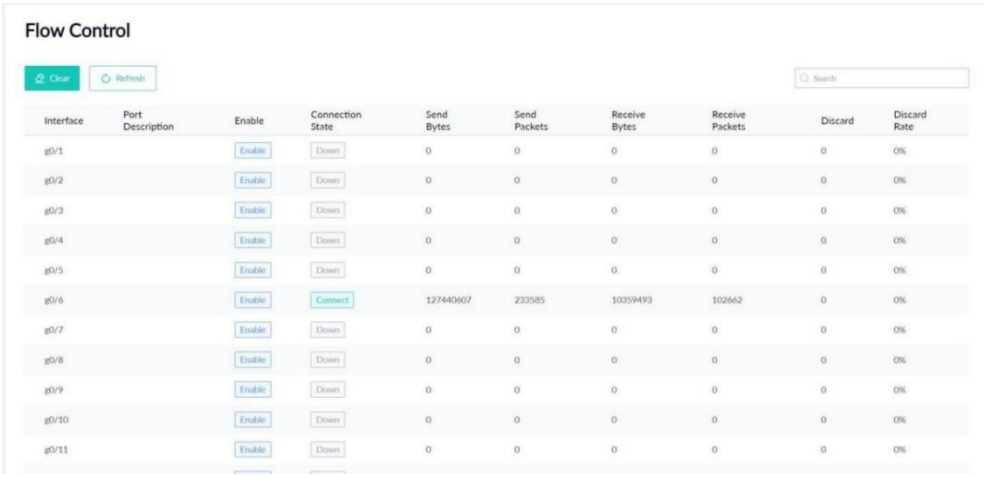


Figure 7 Unknown unicast storm control

In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.3 Flow Control

If you click **Interface > Flow Control** in the navigation bar, the **Interface Flow** page appears, as shown in the figure.



4.4 SPAN

If you click **Interface > SPAN** in the navigation bar, the **Port Mirror Config** page appears, as shown in figure 4-5.

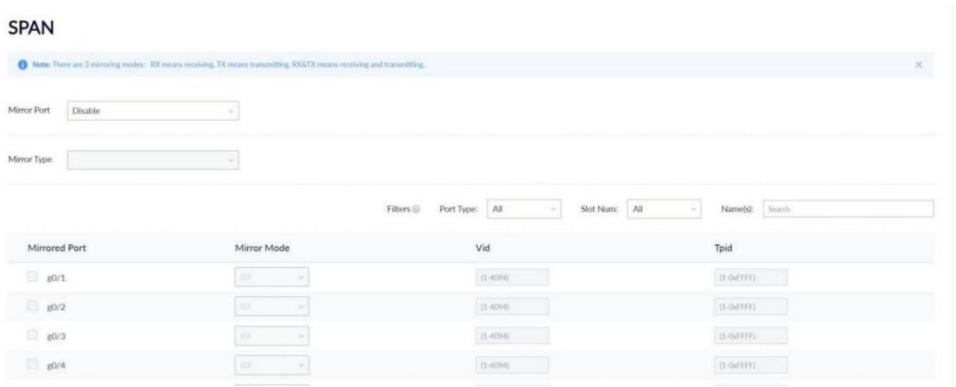


Figure 4-5 Port mirror configuration

Click the drop down list on the right side of "Mirror Port" and select a port to be the destination port of mirror.

Click the drop down list on the right side of "Mirror Type" and select the type of mirror.

Click a checkbox and select a source port of mirror, that is, a mirrored port.

RX	The received packets will be mirrored to the destination port.
TX	The transmitted packets will be mirrored to a destination port.

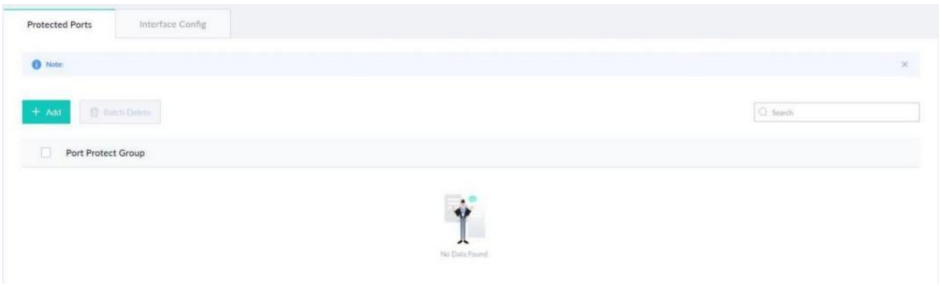
RX & TX	The received and transmitted packets will be mirrored simultaneously.

4.5 Protected Ports

Click "Interface > Protected Ports > Protected Port " in the navigation bar, and enter the configuration page of Protected Port and Interface Config.

4.5.1 Protected Ports

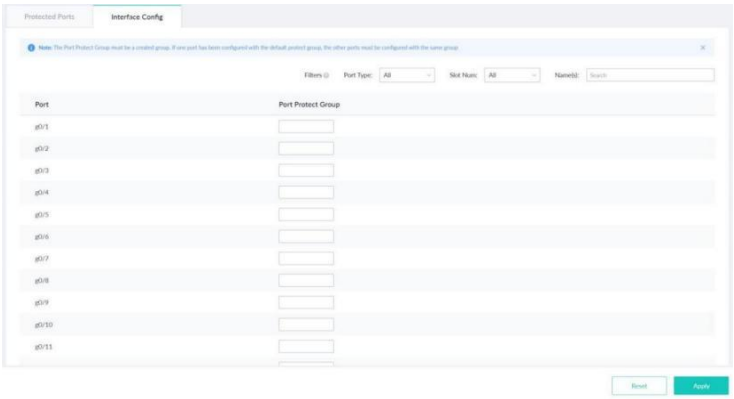
Click "Interface > Protected Ports > Protected Port" in the navigation bar, and enter the configuration page of"Port Protect Group List"



Click "ADD" to create a new port protect group, as shown in the above figure.
Tick one port protect group and delete it. The port protect group is 0 by default, which cannot be deleted.

4.5.2 Interface Config

Click "Interface > Protected Ports > Interface Config" in the navigation bar, and enter the configuration page of "Interface Config"



The port protect group must be a created group. If one port has configured the default protect group, other ports can only be configured with the default protect group.

4.6 Keepalive Detection

If you click **Interface > Keepalive Detection** in the navigation bar, the **Keepalive Detection** page appears, as shown in figure 4-6.

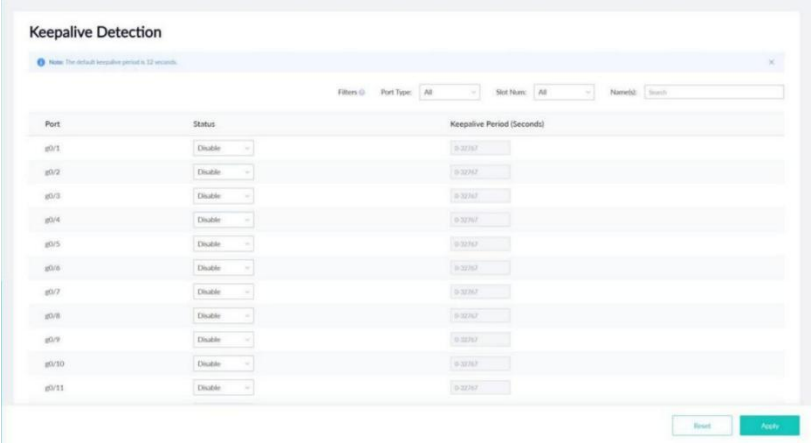


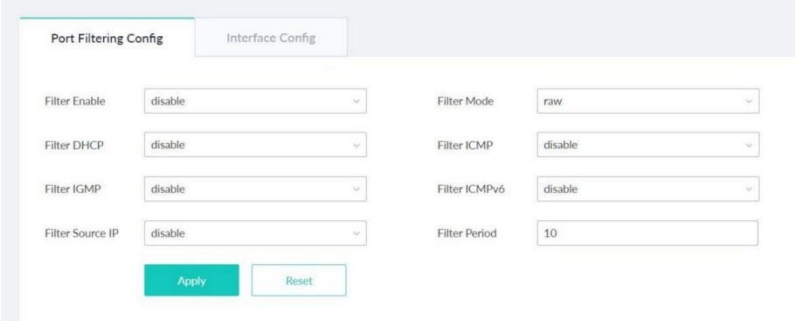
Figure 4-6: Port loopback detection

You can set the loopback detection cycle on the **Keep alive Detection** page.

4.7 Port Filtering

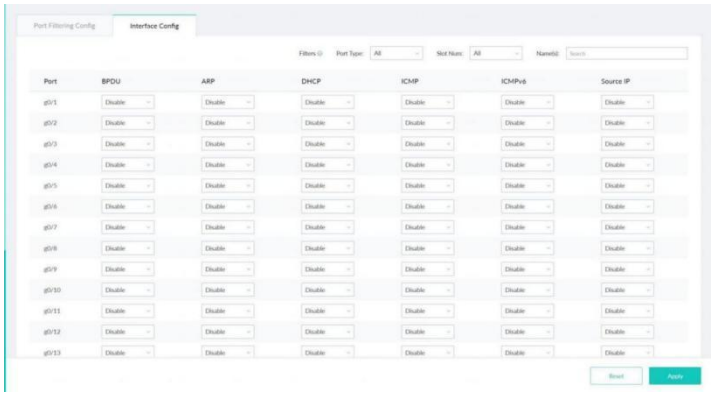
4.7.1 Port Filtering Config

If you click **Interface > Port Filtering > Port Filtering Config** in the navigation bar, the **Port Filtering Config** page appears, as shown in figure.



4.7.2 Interface Config

If you click **Interface > Port Filtering > Interface Config** in the navigation bar, the **Interface Config** page appears, as shown in figure.

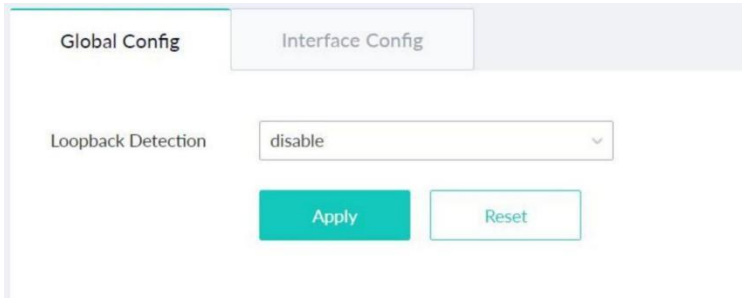


You can then configure filtering conditions for each port.

4.8 Loopback Detection

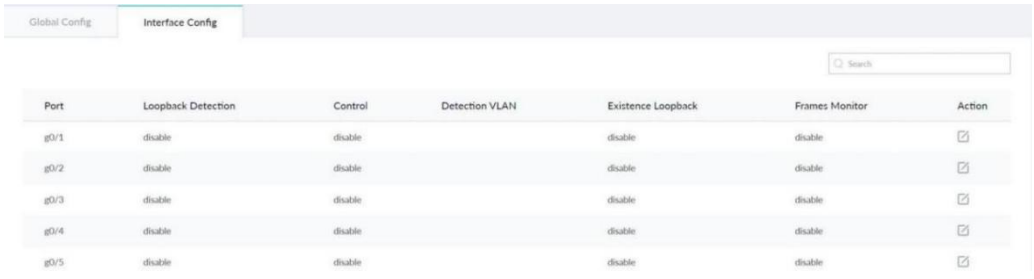
4.8.1 Global Config

If you click **Interface > Loopback Detection > Global Config** in the navigation bar, the **Loopback Detection Global Configuration** page appears, as shown in figure

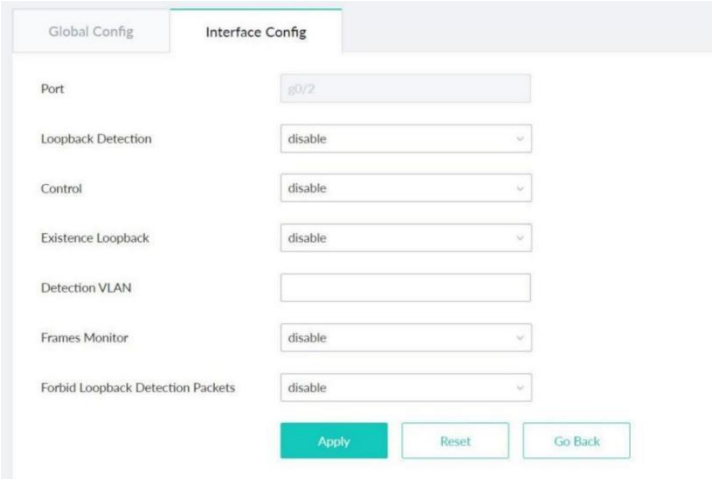


4.8.2 Interface Config

If you click **Interface > Loopback Detection > Interface Config** in the navigation bar, the **Interface Config** page appears, as shown in figure.



Click " " to configure loop detection for each physical port.



4.9 GVRP

4.9.1 Global Config

If you click **Interface > GVRP > Global Config** in the navigation bar, the **Global Config** page appears, as shown in the following Figure.

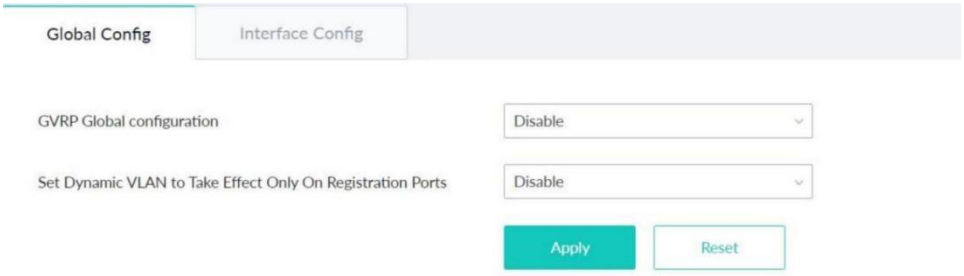


Figure 8 GVRP Global Configuration

You can enable or disable the global GVRP protocol and set whether the dynamic vlan is only effective on the registration interface.

4.9.2 Interface Config

If you click **Interface > GVRP > Interface Config** in the navigation bar, the **Interface Config** page appears, as shown in the following Figure.

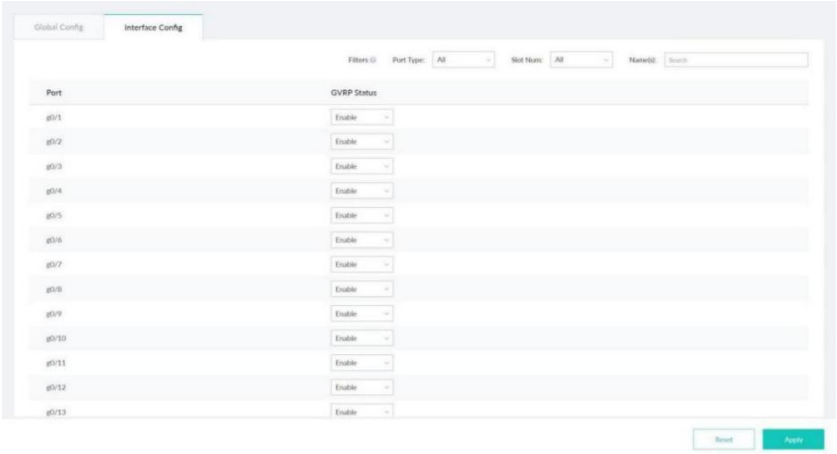


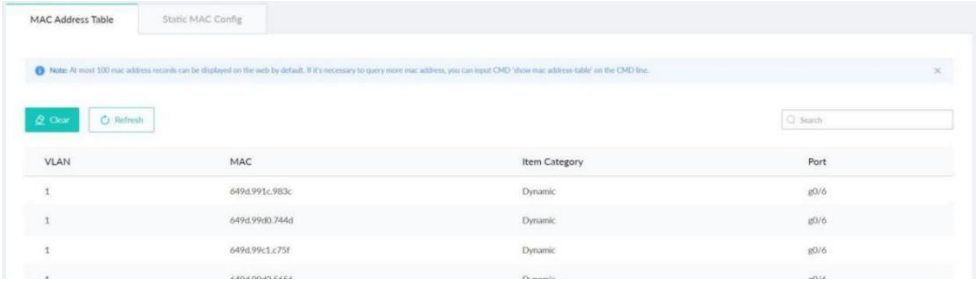
Figure 9 Interface Config

To enable or disable GVRP protocol on the GVRP interface configuration.

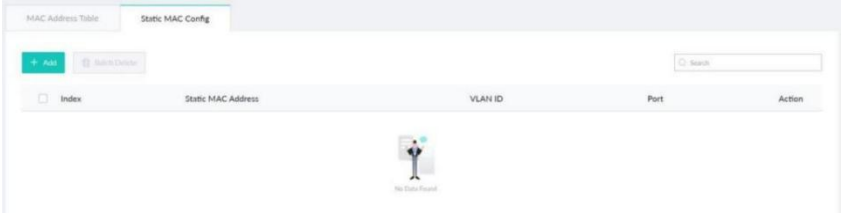
4.10 MAC

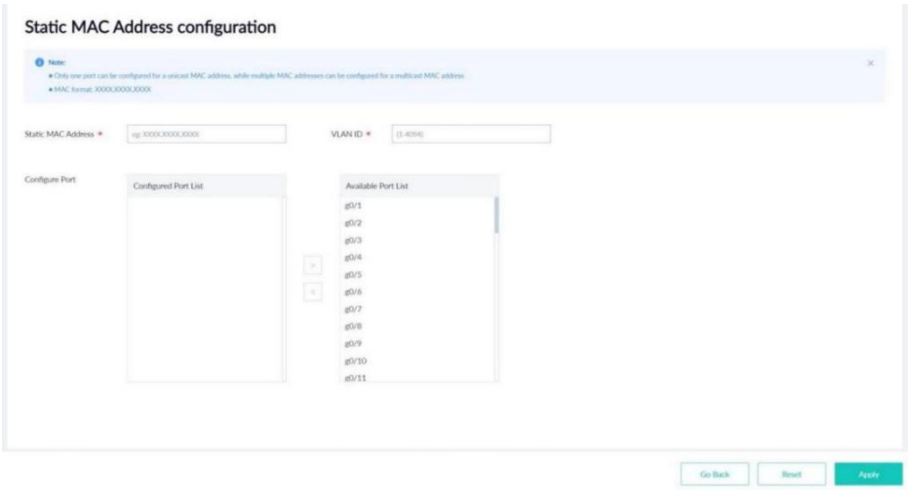
4.10.1 MAC Address Table

If you click **Interface > MAC > MAC Address Table** in the navigation bar, the **Mac Address Table** page appears, as shown in the figure.



4.10.2 Static MAC Config





4.11 STP

4.11.1 Global Config

If you click **Interface > STP > Global Config** in the navigation bar, the **Global Config** page appears, as shown in figure 10.

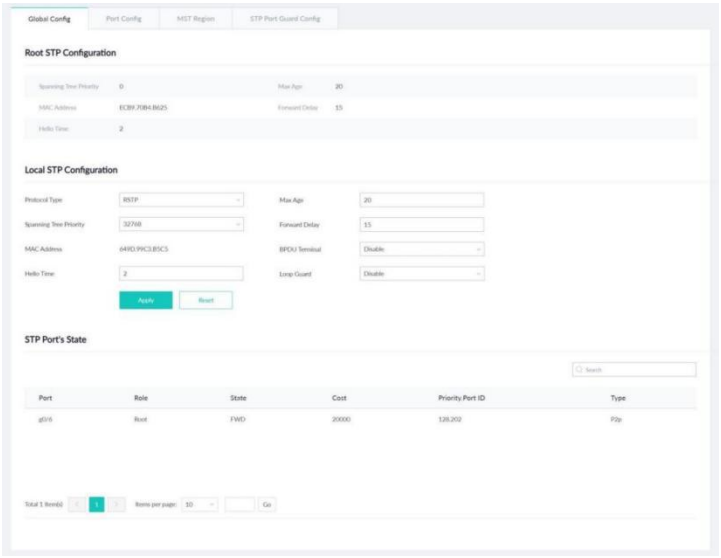


Figure 10 Configuring the global attributes of STP

The root STP configuration information and the STP port's status are only-read.

On the local STP configuration page, you can modify the running STP mode by clicking the Protocol type dropdown box. The STP modes include STP, RSTP and disabled STP.

The priority and the time need be configured for different modes.

Note:

The change of the STP mode may lead to the interruption of the network.

4.11.2 Port Config

If you click the "**Interface > STP > Port Config**" option, the "Port Config" page appears.

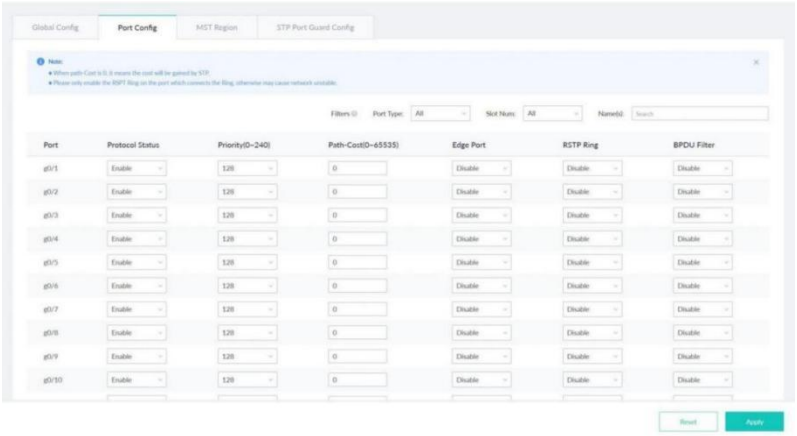
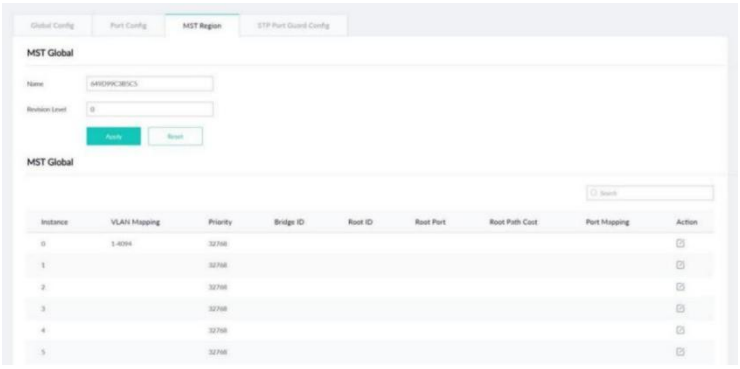


Figure 11 Configuring the attributes of RSTP

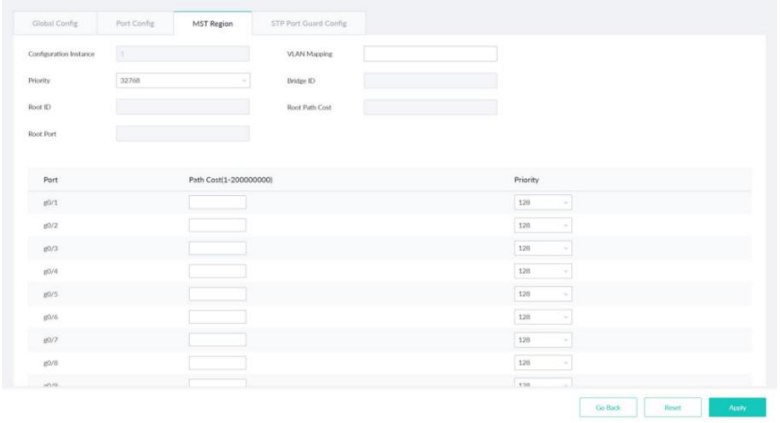
The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to "Disable" and the STP mode is also changed, the port will not run the protocol in the new mode. The default value of the path cost of the port is 0, meaning the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

4.11.3 MST Region

Click "**Interface > STP > MST Region**" in the navigation bar, and enter the configuration page of"MST Region"

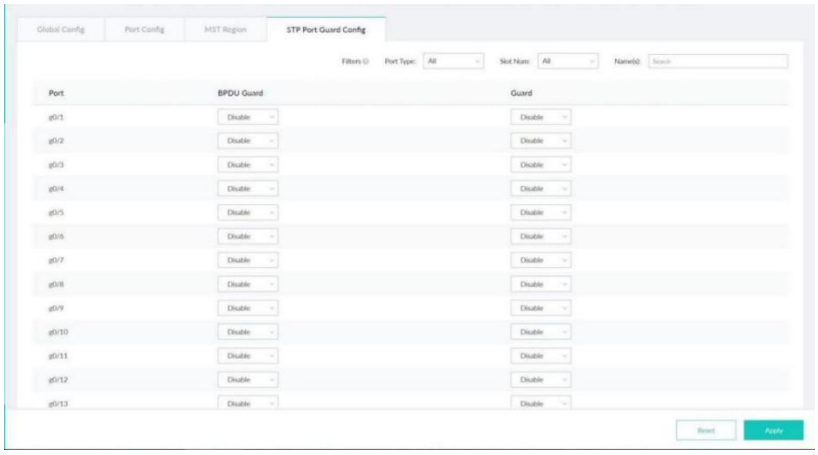


In MST (Multiple Spanning Tree) global configuration, you can change its name and revision level. By clicking "", you can change the configuration content within different instance numbers.



4.11.4 STP Port Guard Config

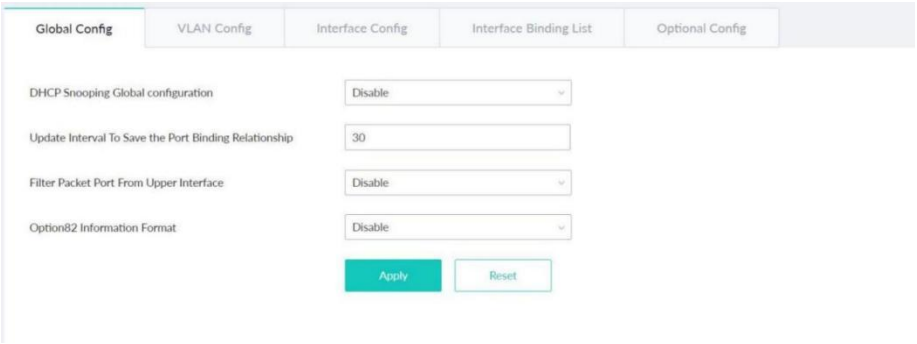
Click "**Interface > STP > STP Port Guard Config**" in the navigation bar, and enter the configuration page of "**STP Port Guard Config**"



4.12 DHCP Snooping

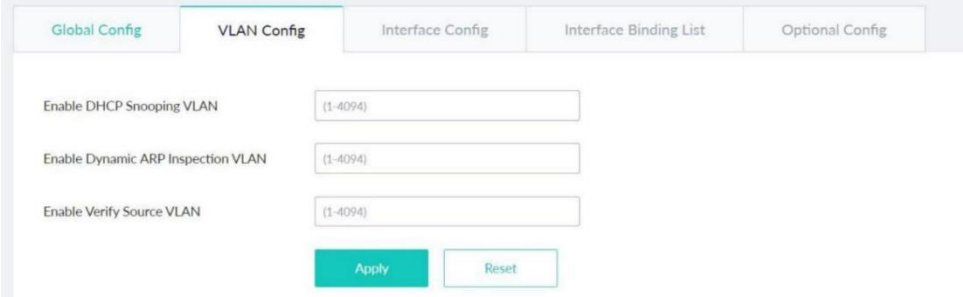
4.12.1 Global Config

If you click **Interface > DHCP Snooping > Global Config** on the navigation bar, the **Global Config** page appears.



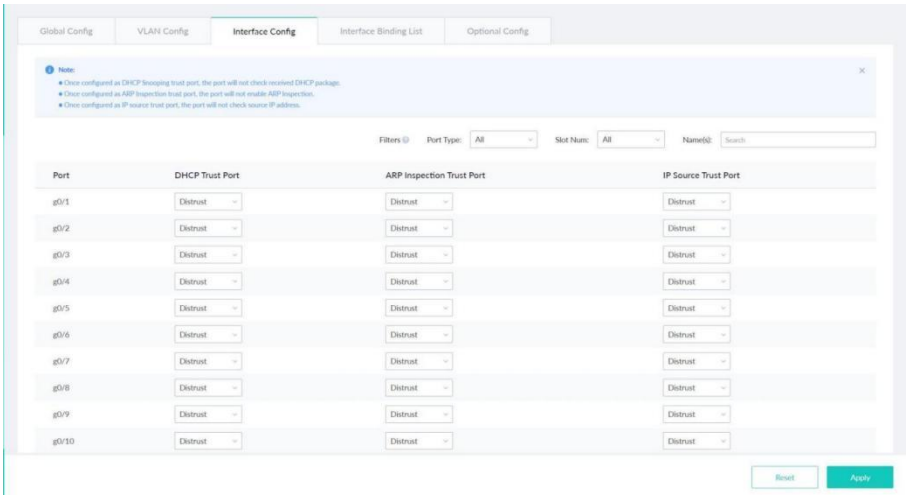
4.12.2 VLAN Config

If you click **Interface > DHCP Snooping > VLAN Config** on the navigation bar, the **VLAN configuration** page appears.



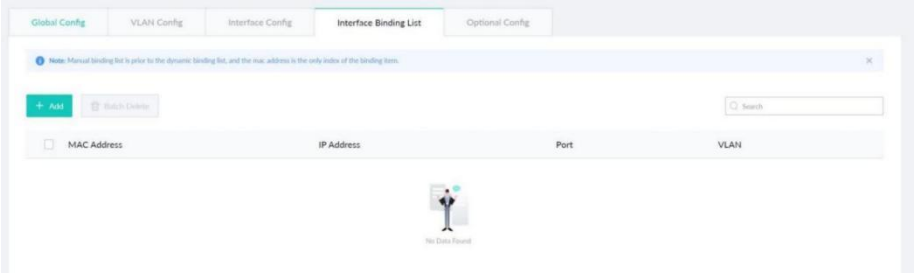
4.12.3 Interface Config

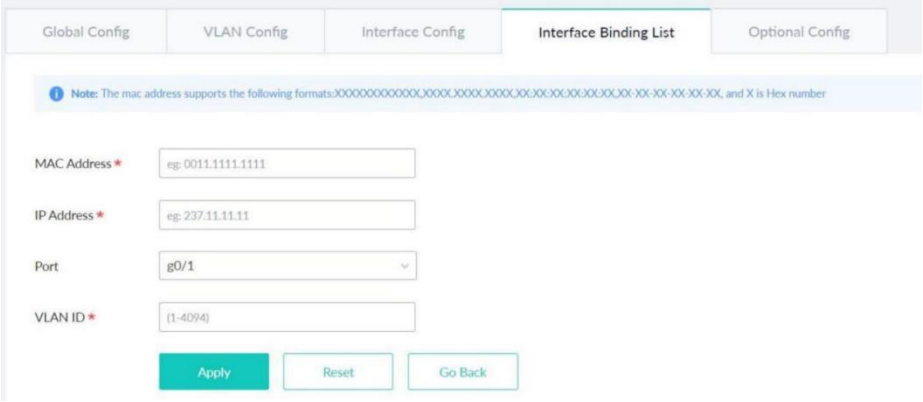
If you click **Interface > DHCP Snooping > Interface Config** on the navigation bar, the **Interface Config** page appears.



4.12.4 Interface Binding List

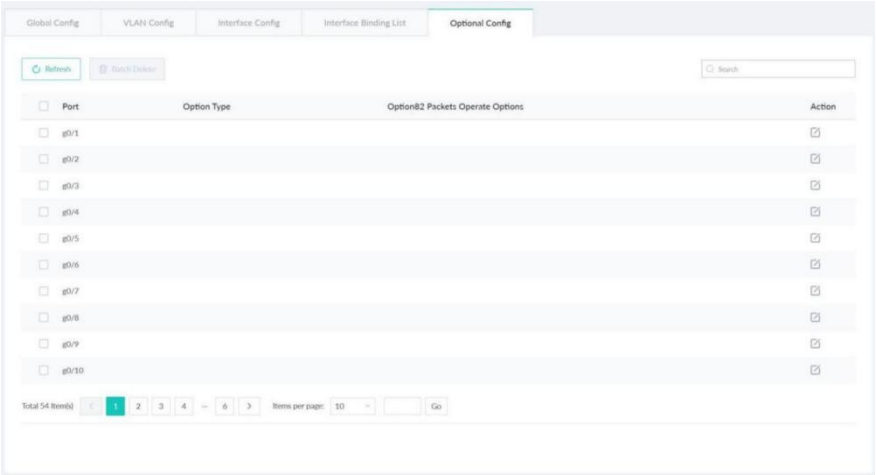
If you click **Interface > DHCP Snooping > Interface Binding List** on the navigation bar, the **Interface Binding List** page appears.



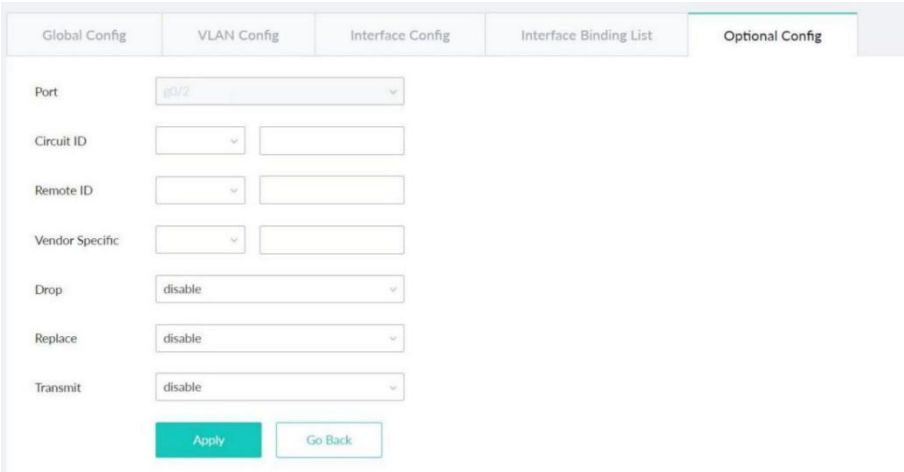


4.12.5 Optional Config

If you click **Interface > DHCP Snooping > Optional Config** on the navigation bar, the **Optional Config** page appears.



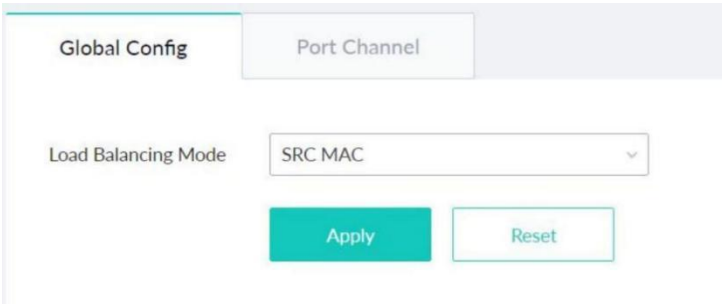
By clicking "", you can make corresponding configurations for each port.



4.13 Port Channel

4.13.1 Global Config

If you click **Interface > Port Channel > Global Config**, the **Global Config** page appears.



For Link Aggregation Load Balancing, some models support the configuration of load-balancing mode based on aggregation groups, while others do not.

4.13.2 Port Channel

If you click **Interface > Port Channel > Port Channel**, the **Port Channel** page appears.

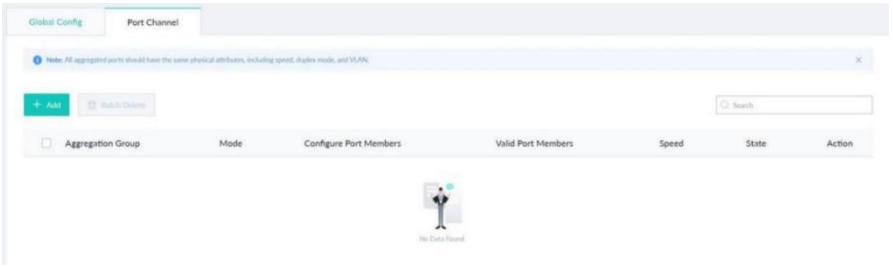


Figure 25 Port Aggregation Information

Click "Add" to create an aggregation group. It can configure 128 aggregation groups and each group is with 8 physical ports into aggregation. Click Batch Delete to delete the selected aggregation group. Click "**Reset**" to modify the setting.

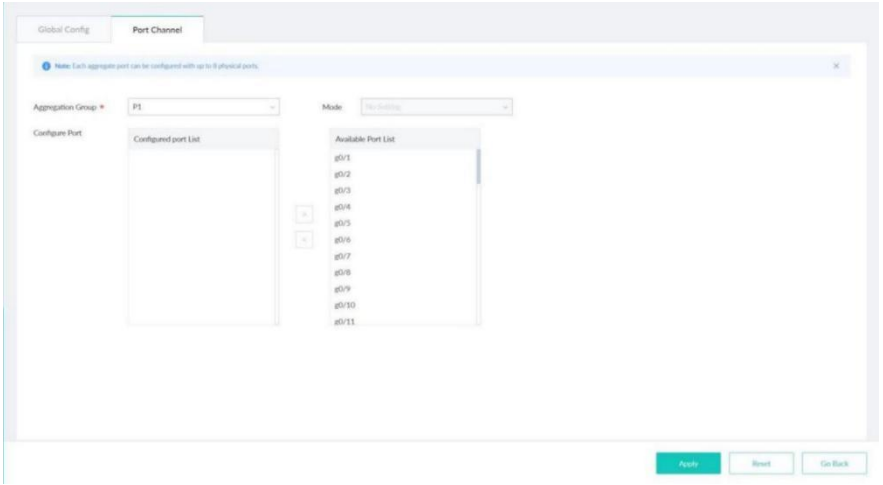


Figure 26 Port Aggregation Configuration

If you create an aggregation group, it is optional; if you modify the aggregation group, it is not optional.

When the aggregation port has a member port, the user can select the aggregation mode: static, LACP Active and LACP Passive.

You can click ">" and "<" to delete and add an aggregation member port.

4.14 DDM

If you click **Interface > DDM** in the navigation bar, the **DDM** page appears, as shown in figure 5-21.

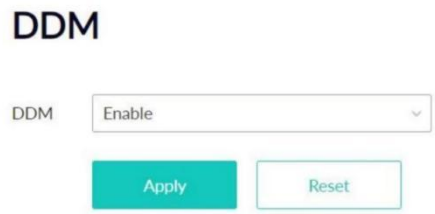


Figure 5-21: DDM

4.15 Ring Protection

4.15.1 Ether-ring

If you click **Interface > Ring protection > ether-ring**, the **ether-ring** page appears.

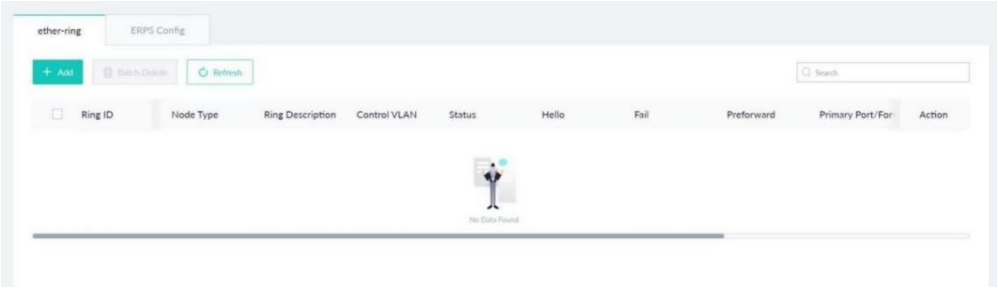
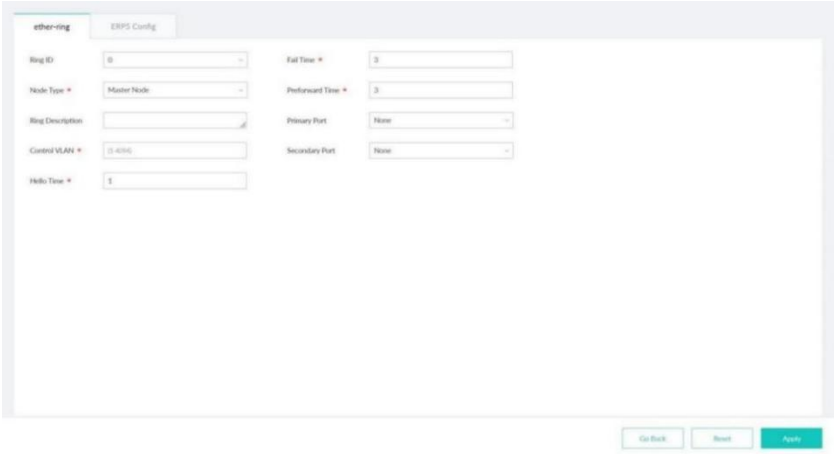


Figure 19 EAPS Ring List

In the list shows the currently configured Ethernet-ring, including the status of the ring, the forwarding status of the port and the status of the link.

Click"Add" to create a new EAPS ring.



Click the “Apply” option to configure the “Time” parameter of the ring.

Note:

1. The system can support 32 EAPS rings.

2. After a ring is configured, its port, node type and control Vlan cannot be modified. If the port of the ring, the node type or the control Vlan need be adjusted, please delete the ring and then establish a new one.

4.15.2 ERPS Config

If you click “Add” on the ERPS list, the “ERPS Configure ” page appears.

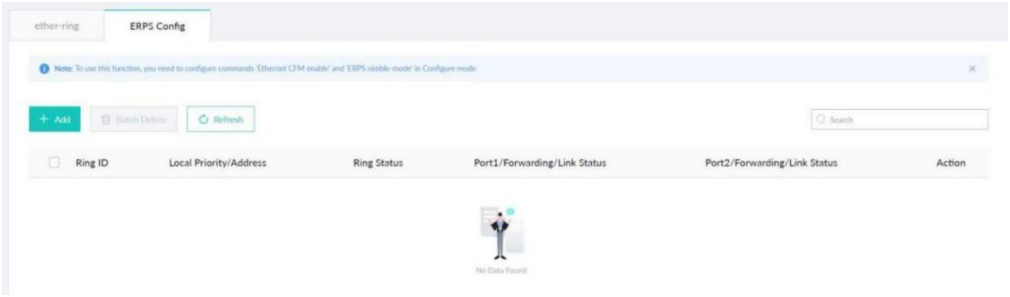
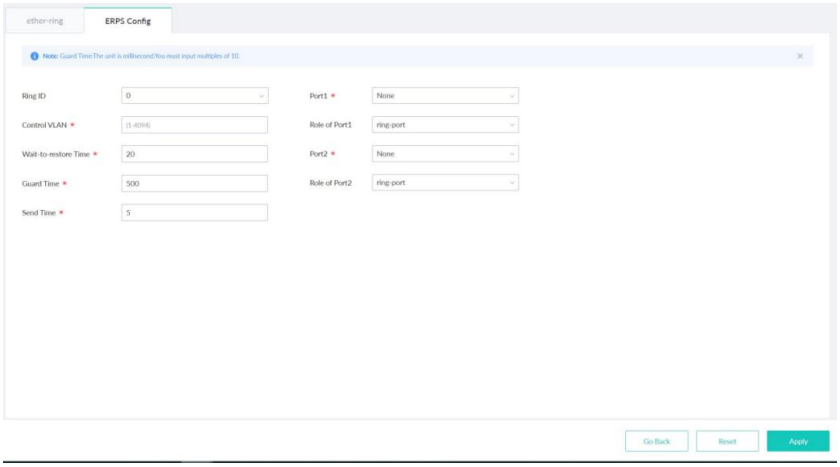


Figure 20 EAPS ring configuration

By clicking the 'Add' button in ERPS configuration, or the “Edit” option on the right side of the ERPS configuration ring entry, you can access the ERPS configuration page.



Note:

If you want to modify a ring on this page, the node type, the control VLAN, the primary port, and the secondary port cannot be modified.

In the dropdown box on the right of"Ring ID", select an ID as a ring ID. The ring IDs of all devices on the same ring must be the same.

Enter a value between 1 and 4094 in the text box on the right of "Control VLAN" as the control VLAN ID. When a ring is established, the control VLAN will be automatically established, too. Please note that if the designated control VLAN is 1 and the VLAN of the control device is also 1, the control device cannot access the control VLAN. Additionally, please do not enter a control VLAN ID that is the same as that of another ring.

In the text boxes of"Primary Port" and "Secondary Port", select a port as the ring port, respectively.

Click "Apply" to finish ERPS configuration, click "Reset" to resume the initial values of the configuration, or click "Return" to go back to the ERPS list page.

4.16 Multiple Ring Protection

Click "Interface " > "Multiple Ring Protection" in the navigation bar, and enter the multiple ring protection configuration page.

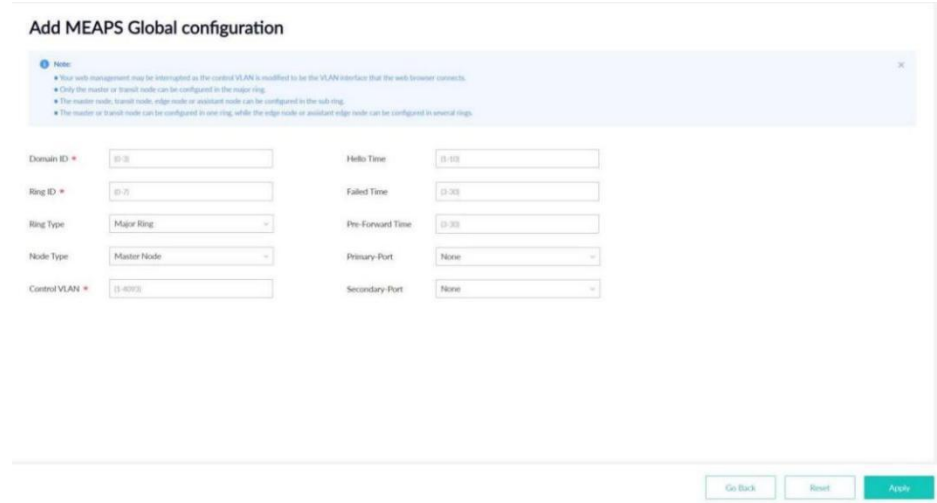
Figure 21 Multiple Ring List

The list displays the currently configured Multiple Ring, including the domain ID, the ring ID, the ring type, the node type, control VLAN, Hello Time, Fail Time, Pre Forward Time and the primary and secondary port on the ring.

Click "Add" to create MEAPS ring network.

Click" " right of the entry to configure the time parameter, and the primary and secondary port of the ring network.

Note that: 1. MEAPS domain numbers the system supported is 4 (0-3). 2. The ring numbers supported in the domain is 8 (0-7). 3. Once one MEAPS has configured, its ID, ring ID, ring type, node type and control Vlan cannot be configured. If these parameters need to be configured, please delete the net ring and re-create it.
Click "Add", and enter EAPS ring network configuration page.



Note that:

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

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

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

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

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

4.17 BackupLink

4.17.1 Global Config

If you click **Interface > BackupLink > Global Config** on the navigation bar, the **Global Config** page appears.

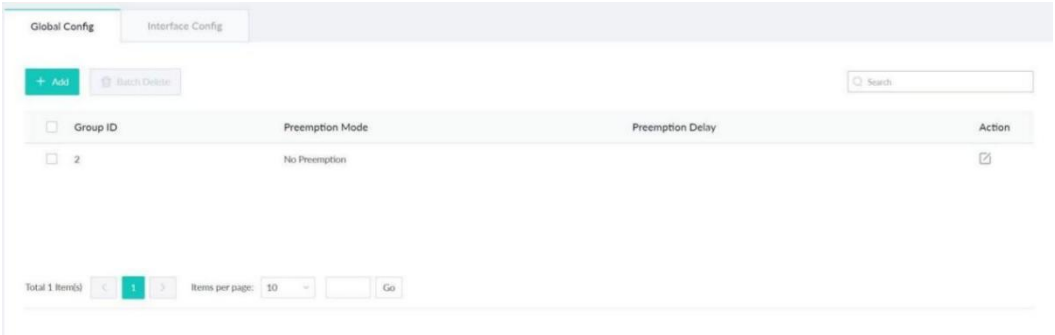


Figure 24 Backup Link Protocol Global Configuration

On the page, the current configured backup link groups are shown, including Preemption Mode and Preemption Delay. Click"Add" to create a new link backup group.

Click " " on the right to configure Preemption Mode and Preemption Delay.

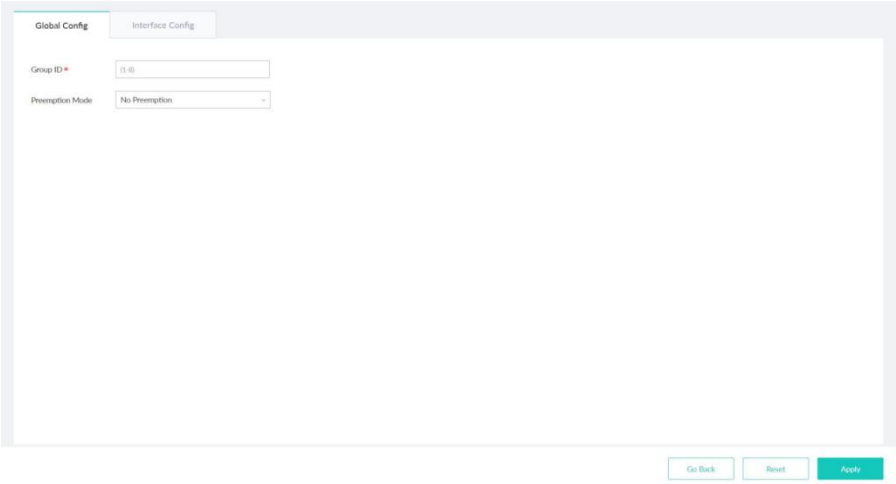


Figure 25 Backup Link Protocol Global Configuration

Note:

1. The system supports 8 link backup groups.
2. The Preemption mode determines the policy the primary port and the backup port forward packets.

4.17.2 Interface Config

If you click **Interface > BackupLink > Interface Config** on the navigation bar, the **Global Config** page appears.

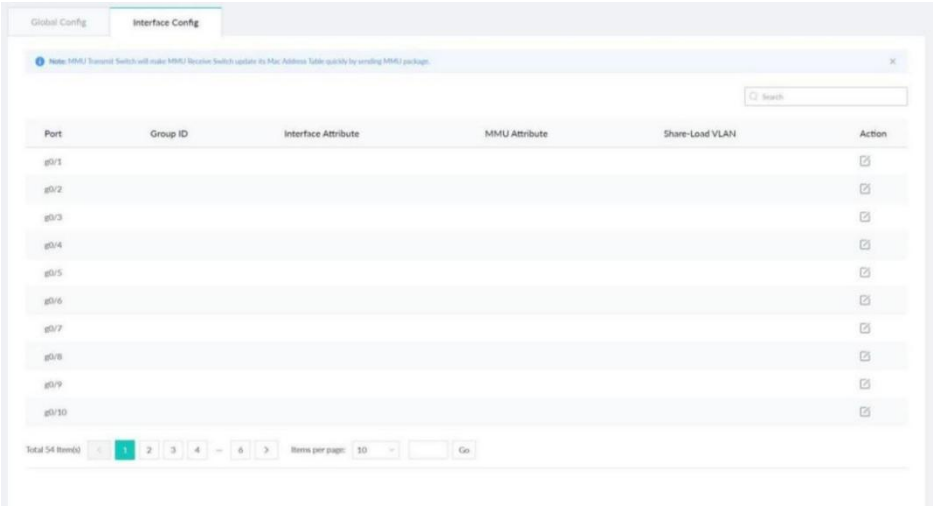


Figure 26 Backup Link Protocol Interface Configuration

This page shows the backup link group's member ports, Interface Attribute, MMU Attribute, Shareload Vlan, etc.

Click"☑ "on the right to configure the Backup Link Protocol.

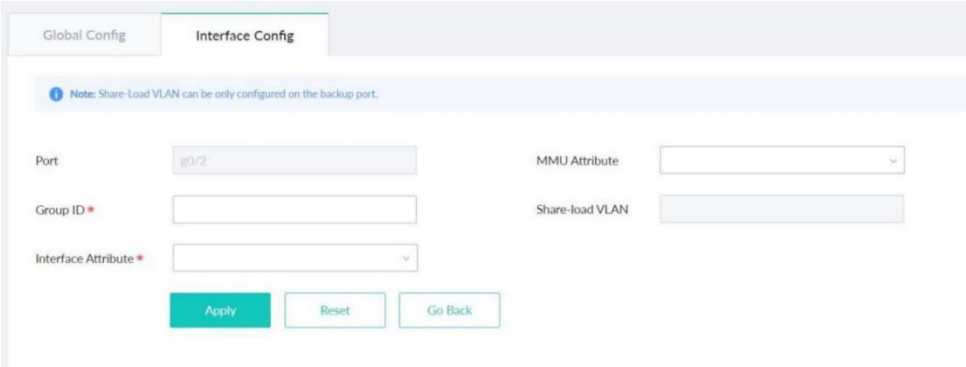


Figure 27 Backup Link Protocol Interface Configuration

The backup link group which has configured the primary port cannot take other ports as its primary port. Likewise, the backup link group which has configured the backup port cannot take other ports as its backup port.

4.18 MTU

If you click **Interface > MTU** on the navigation bar, the **MTU** page appears.

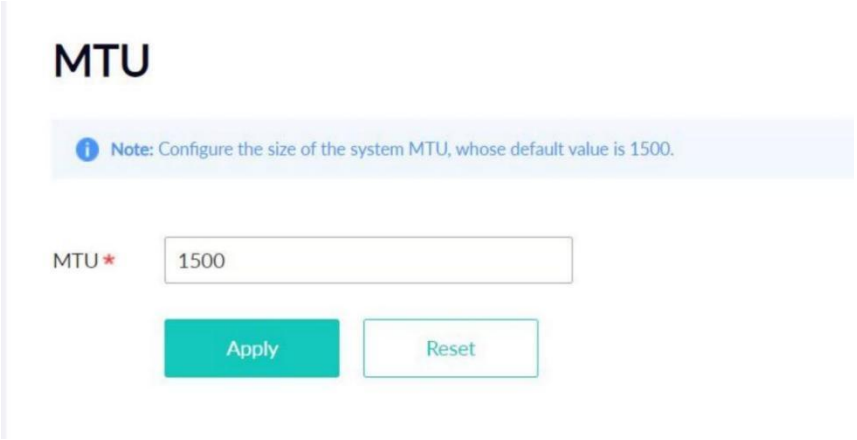


Figure 28 MTU

You can set the size of the maximum transmission unit (MTU).

4.19 PDP

4.19.1 Global Config

If you click **Interface > PDP > Global Config** in the navigation bar, the **Basic Config of PDP Protocol** page appears.

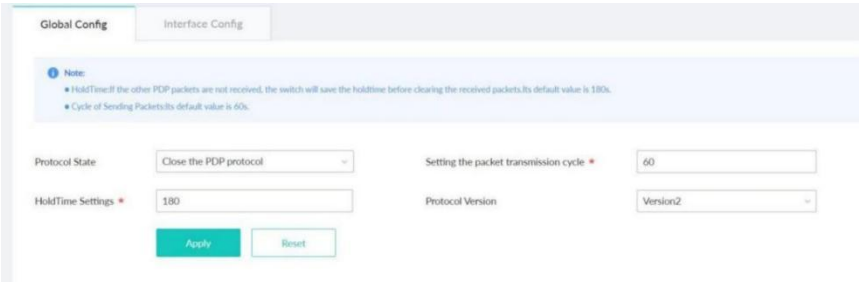


Figure 29 Basic Config of PDP Protocol

You can choose to enable PDP or disable it. When you choose to disable PDP, you cannot configure PDP.

The "**Hold Time**" parameter means the time to be saved before the router discards the received information if other PDP packets are not received.

4.19.2 Interface Config

If you click **Interface > PDP > Interface Config** in the navigation bar, the **Protocol Port Config** page appears.

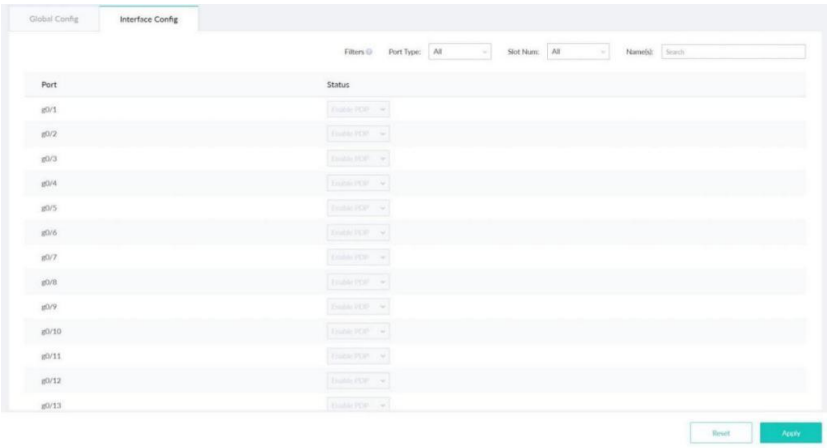
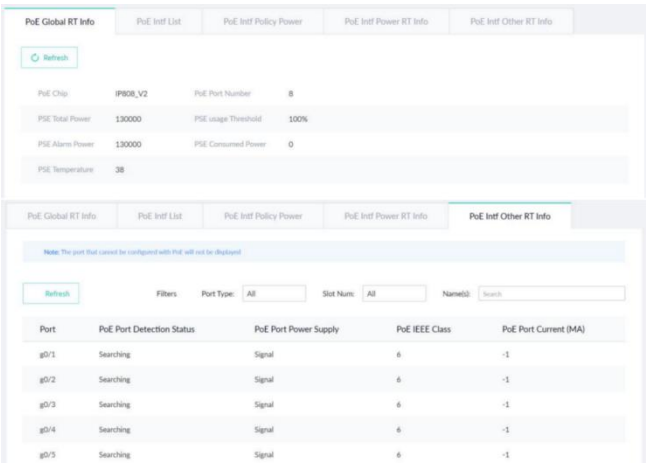
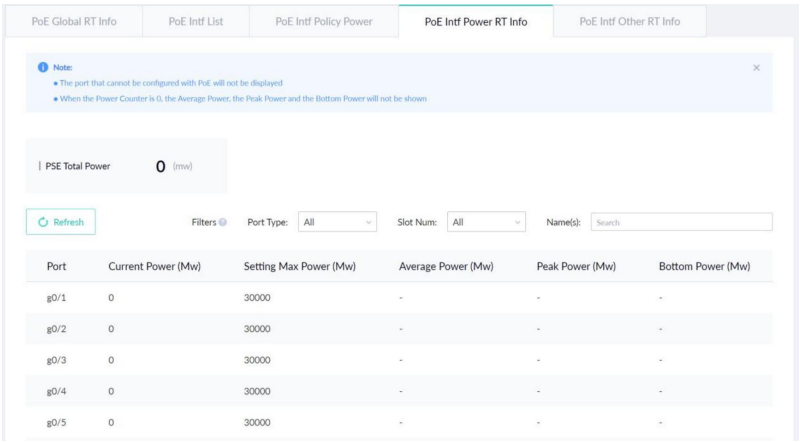


Figure 30 PDP Interface Attribute Configuration

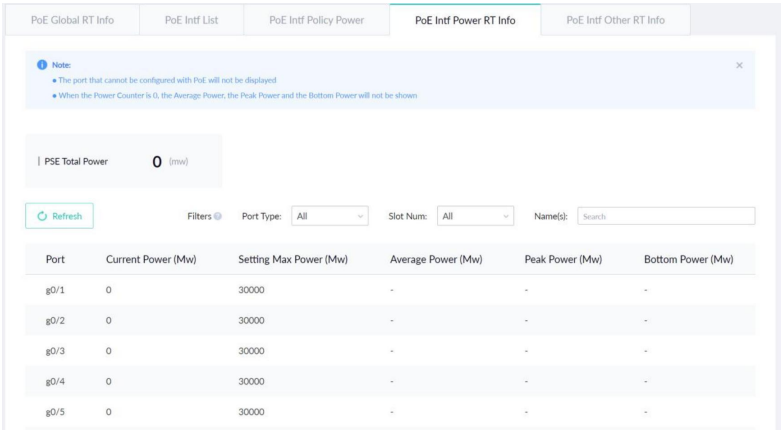
After the PDP port is configured, you can enable or disable PDP on this port.

4.20 PoE Global TR Info

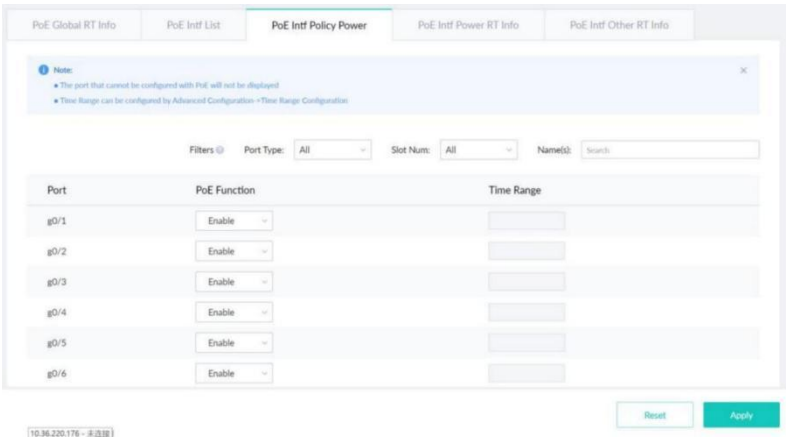




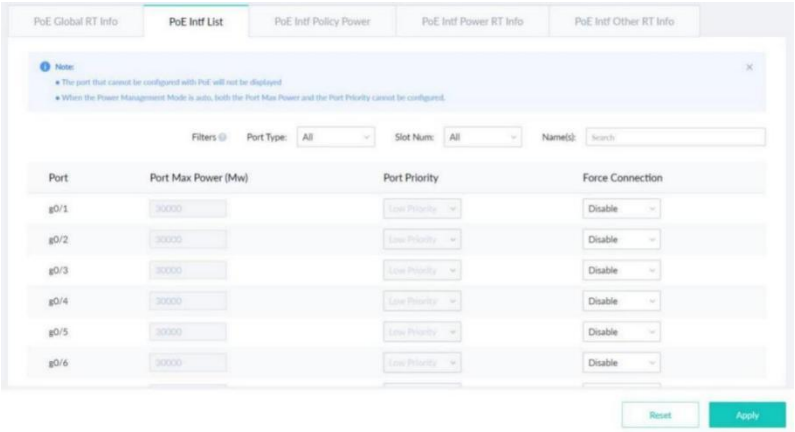
4.21 PoE Intf Power TR Info



4.22 PoE Intf Policy Power



4.23 PoE Intf List



Chapter 5 Advanced

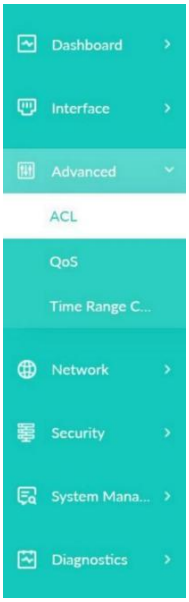


Figure 1 Advanced configuration

5.1 ACL

5.1.1 IP Access List Config

If you click **Advanced > ACL > IP Access List Config**, the IP ACL configuration page appears.

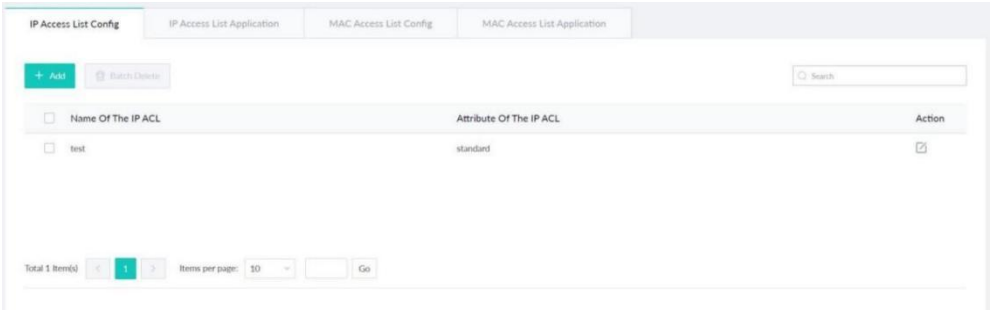


Figure 2: IP Access List Config

Click"Add" to add a name of the IP access control list. Click "Delete" to delete an IP access control list.

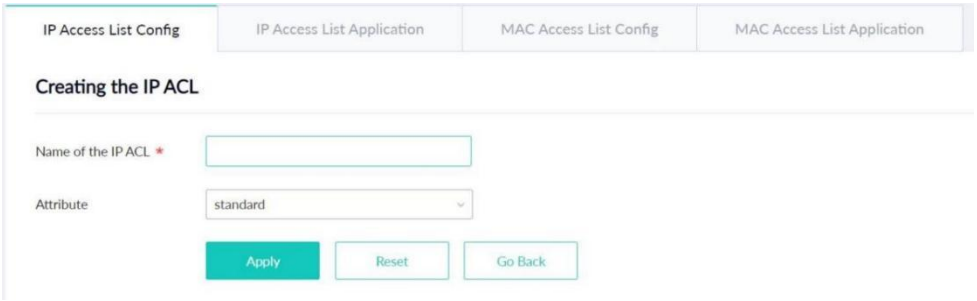


Figure 3: Creating a name of the IP access control list

5.1.2 IP Access List Application

If you click **Advanced > IP access control list > IP Access List Application**, the IP Access List Application page appears.

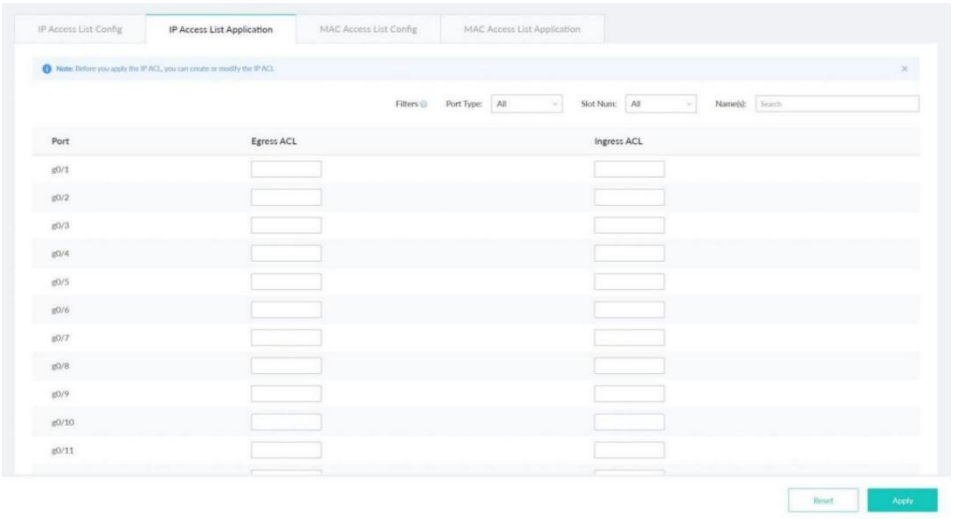


Figure 4: Applying the IP access control list

5.2 QoS

5.2.1 Global Config

If you click **Advanced > QoS > GlobalConfig**, the **Port's QoS parameter configuration** page appears.

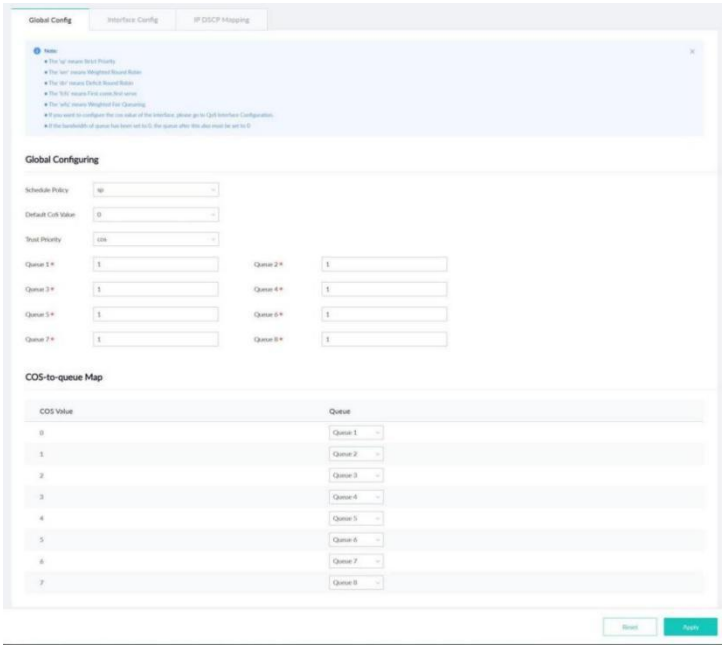


Figure 5 Configuring global QoS attributes

In WRR schedule mode, you can set the weights of the QoS queues. There are 4 queues, among which queue 1 has the lowest priority and queue 4 has the highest priority.

5.2.2 Interface Config

If you click **Advanced > QoS > Interface Config,** the **Port Priority Config** page appears.

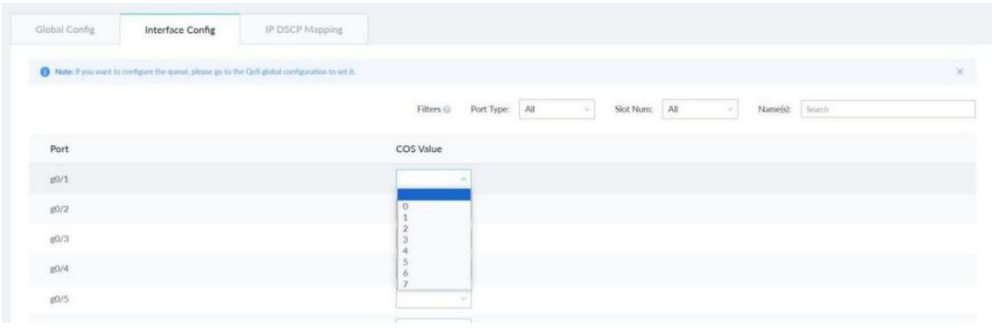


Figure 6 Configuring the QoS Port

You can set the CoS value by clicking the dropdown box on the right of each port and selecting a value. The default CoS value of a port is 0, meaning the lowest priority. If the CoS value is 7, it means that the priority is the highest.

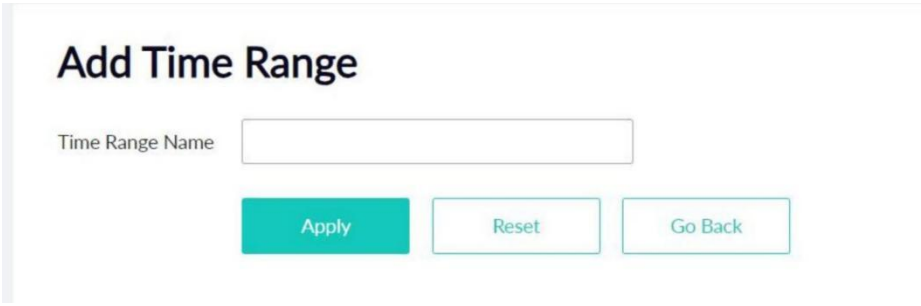
5.2.3 IP DSCP Mapping

If you click **Advanced Config > Qos Configuration** , the **IP DSCP Mapping** page appears.

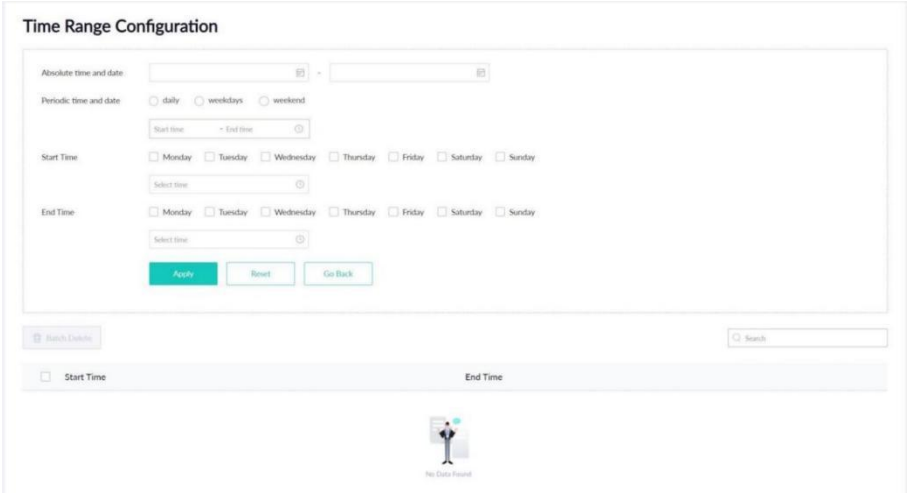
5.3 Time Range List Info

If you click **Advanced > Time Range List Info**, the **Time Range List Info** page appears.

Click 'Add' to create a new TimeRange.



Click " " to enter Time Range configuration.



Chapter 6 Network

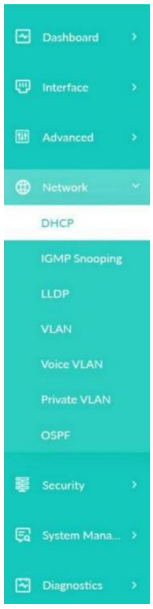
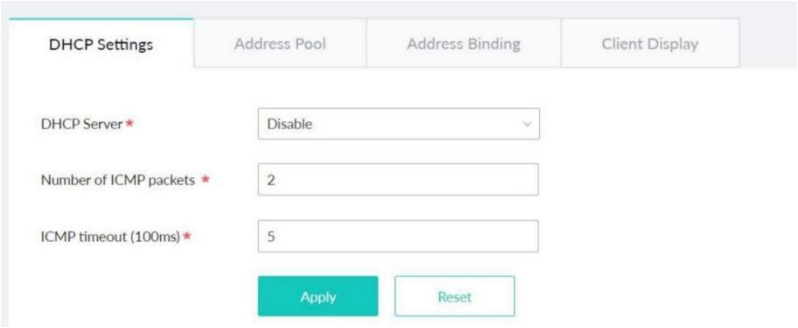


Figure 1: Physical port configuration list

6.1 DHCP

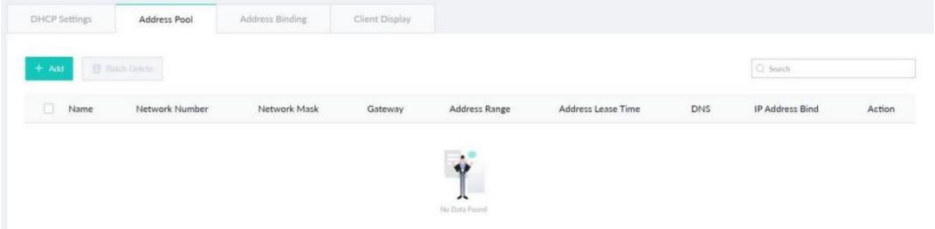
6.1.1 DHCP Settings

If you click **Network > DHCP > DHCP Settings**, the **DHCP Settings** page appears.

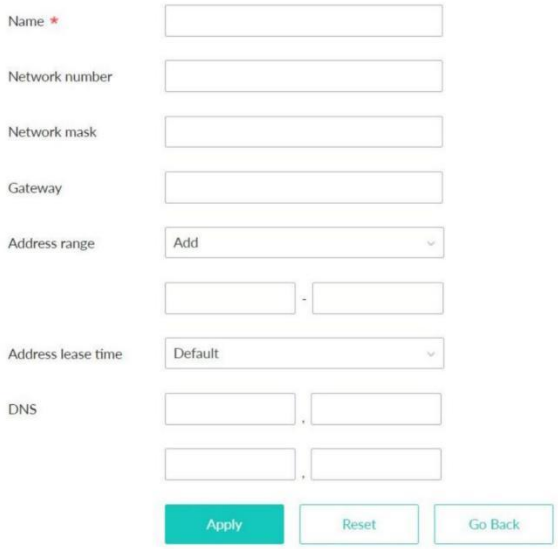


6.1.2 Address Pools

If you click **Network > DHCP > Address Pools**, the **DHCP Address Pools** page appears.



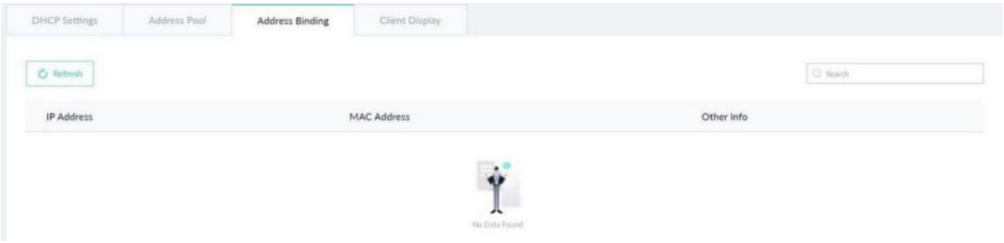
By clicking “Add' or ” ”, you can perform related configurations and modifications.



By clicking " " , you can set the binding information for the IP address.

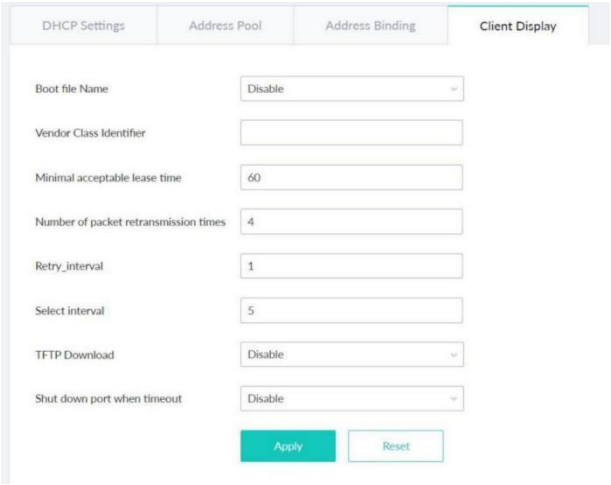
6.1.3 Address Bindings

If you click **Network > DHCP > Address Bindings**, the **DHCP Address Bindings** page appears.



6.1.4 Client Display

If you click **Network > DHCP > Client Display**, the **DHCP Client Configuration** page appears.



6.2 IGMP Snooping

6.2.1 IGMP Snooping

If you click **Network > IGMP Snooping > IGMP Snooping**, the IGMP Snooping configuration page appears.

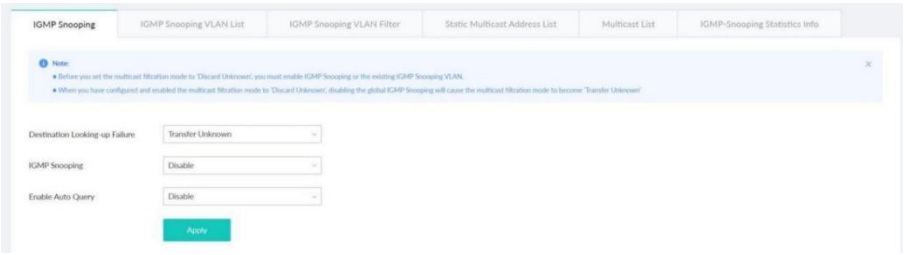


Figure 2 IGMP Snooping configuration

On this page you can set whether to make a switch to forward unknown multicasts, whether to enable IGMP Snooping, and whether to configure the switch as the querier of IGMP.

6.2.2 IGMP Snooping VLAN List

If you click **Network > IGMP Snooping > IGMP Snooping vlan list**, the **IGMP Snooping VLAN list** page appears.

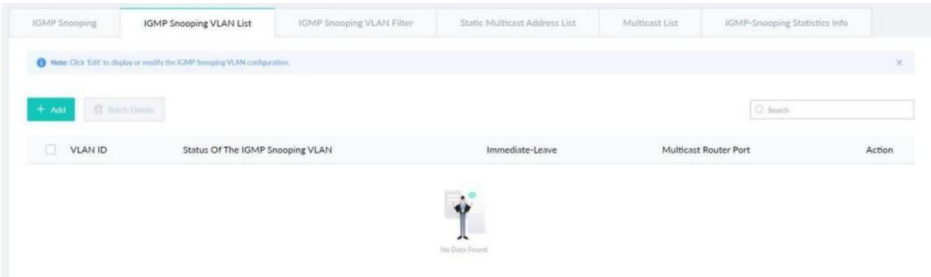


Figure 3: IGMP Snooping VLAN list

When IGMP Snooping has been enabled, if you click “Add”, IGMP Snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP Snooping VLAN. If you click Batch Delete, a selected IGMP Snooping VLAN can be deleted; if you click **Edit**, you can modify the member port, running status and immediate-leave of IGMP Snooping VLAN.

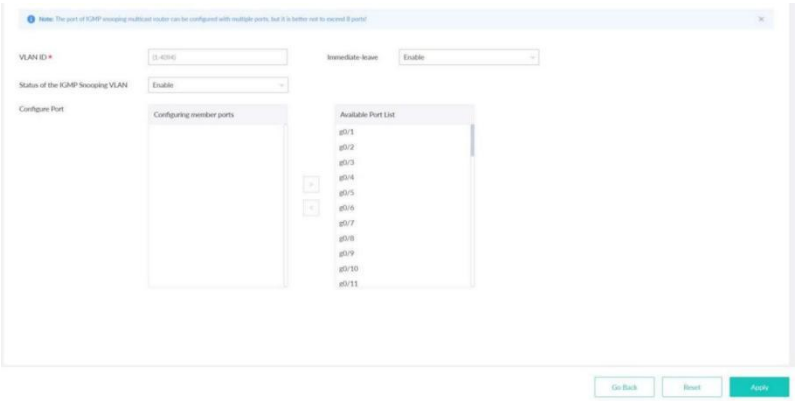


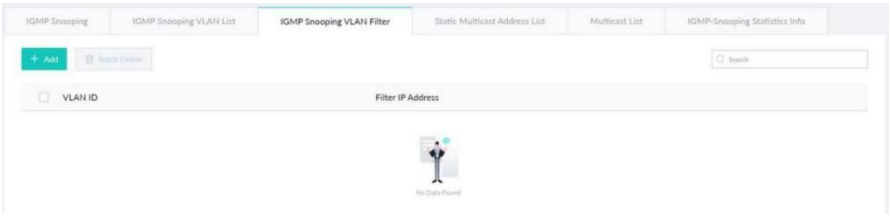
Figure 4: Static routing port of IGMP VLAN

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

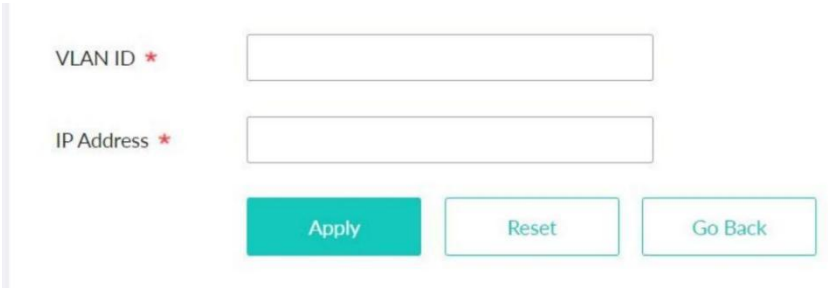
You can click ">" and "<" to delete and add a routing port.

6.2.3 IGMP Snooping VLAN Filter

If you click **Network > IGMP Snooping > IGMP Snooping VLAN Filter**, the **IGMP Snooping VLAN Filter List** page appears.



Click 'Add' to add a new IGMP Snooping filter configuration, which allows you to set a specific VLAN to filter out packets sent from a particular IP.



Ensure that the VLAN ID already exists, otherwise the configuration will not take effect.

6.2.4 Static Multicast Address List

If you click **Network > IGMP Snooping > Static Multicast Address List**, the **Setting the static multicast address** page appears.

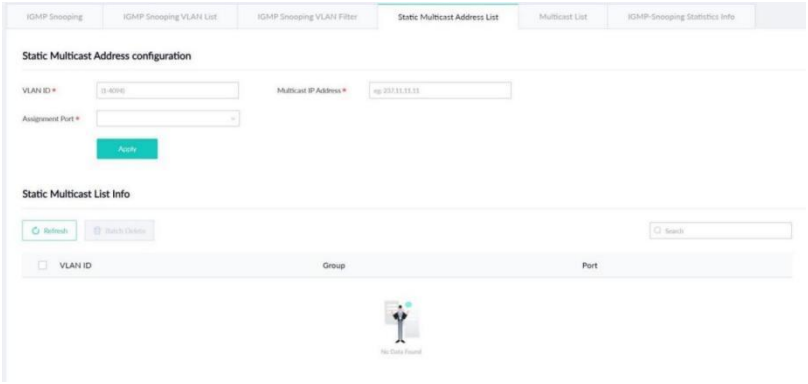


Figure 5 Multicast List

On this page, the currently existing static multicast groups and port groups in each static multicast group are shown. Click"Refresh" to refresh the contents in the list.

6.2.5 Multicast List

Click the **Network > IGMP Snooping > Multicast List Info** option at the top of the page, and the **Multicast List Info** page appears.

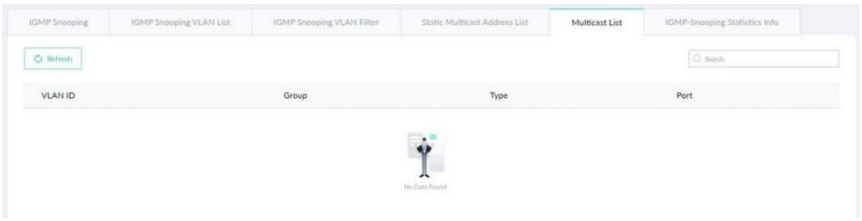


Figure 6 Multicast List

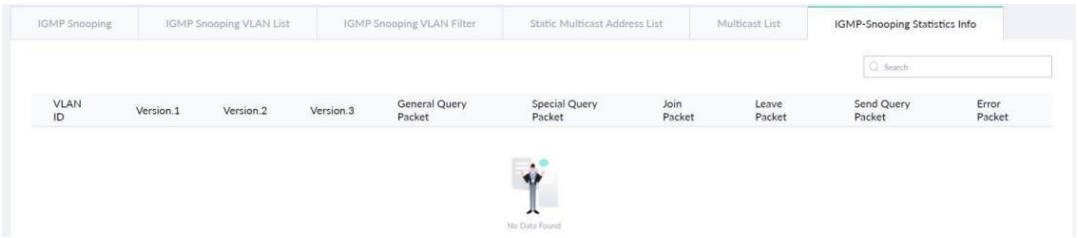
On this page the multicast groups, which are existent in the current network and are in the statistics of IGMP Snooping, as well as port sets which members in each group belong to are displayed.

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

Note:

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

6.2.6 IGMP-Snooping Statistics Info



6.3 LLDP

6.3.1 Global Config

If you click **Network > LLDP > Global Config** in the navigation bar, the **Basic Config of LLDP Protocol** page appears, as shown in the following Figure.

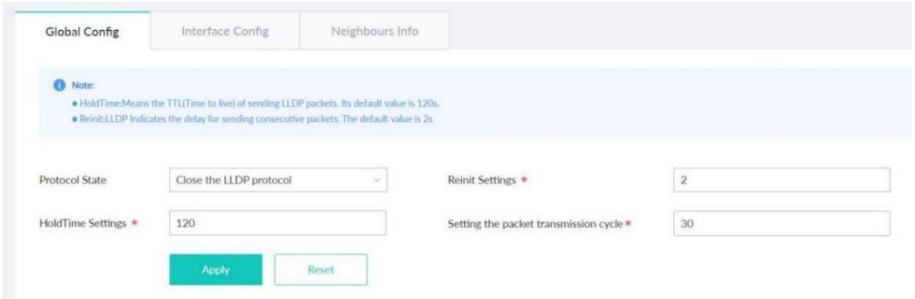


Figure 7 Configuring the Global Attributes of LLDP

You can choose to enable LLDP or disable it. When you choose to disable LLDP, you cannot configure LLDP.

The “Hold Time” parameter means the ttl value of the packet that is transmitted by LLDP. Its default value is 120s. The “Reinit” parameter means the delay of successive packet transmission of LLDP. Its default value is 2s.

6.3.2 Interface Config

If you click **Network > LLDP > Interface Config** in the navigation bar, the **LLDP Port Config** page appears.

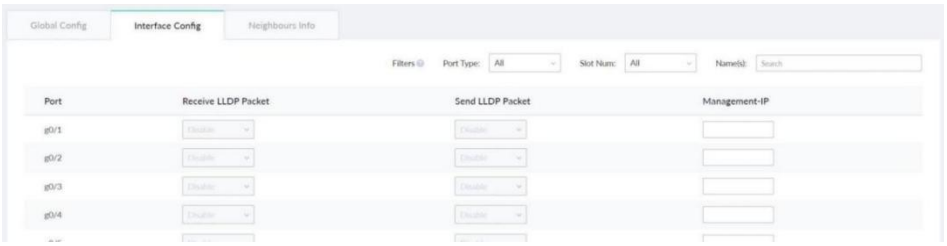
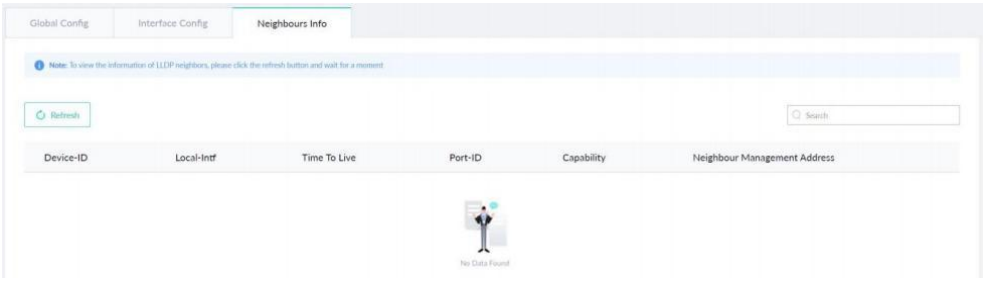


Figure 8 Configuring the LLDP port

After the LLDP port is configured, you can enable or disable LLDP on this port.

6.3.3 Neighbour Info

If you click **Network > LLDP > Neighbour Info** in the navigation bar, the **LLDP Neighbour Info** page appears, as shown in the figure.



6.4 VLAN

6.4.1 VLAN

If you click **Network > VLAN > VLAN** in the navigation bar, the **VLAN Config** page appears, as shown in the figure.

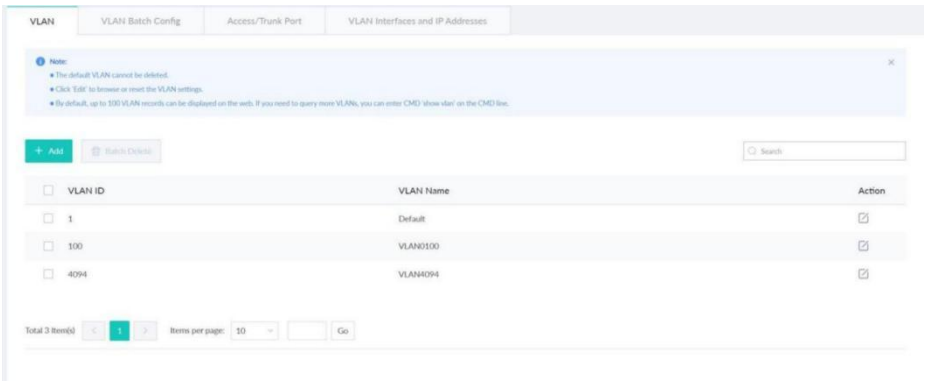


Figure 9 VLAN configuration

The VLAN list will display VLAN items that exist in the current device according to the ascending order. In case of lots of items, you can look for the to-be-configured VLAN through the buttons like " Prev", "Next" and "Search"

You can click "Add" to create a new VLAN.

You can also click "Edit" at the end of a VLAN item to modify the VLAN name and the port's attributes in the VLAN.

If you select the checkbox before a VLAN and then click "Delete", the selected VLAN will be deleted.

Note:

By default, a VLAN list can display up to 100 VLAN items. If you want to configure more VLANs through Web, please log on to the switch through the Console port or Telnet, enter the global configuration mode and then run the "**ip httpweb max-vlan**" command to modify the maximum number of VLANs that will be displayed.

If you click "Add" or "Edit" in the VLAN list, the VLAN configuration page appears, on which new VLANs can be created or the attributes of an existent VLAN can be modified.

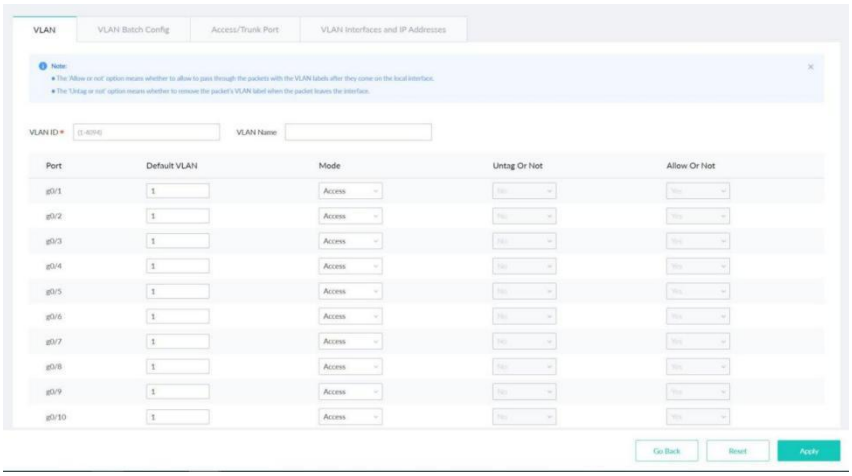


Figure 10 Revising VLAN configuration

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

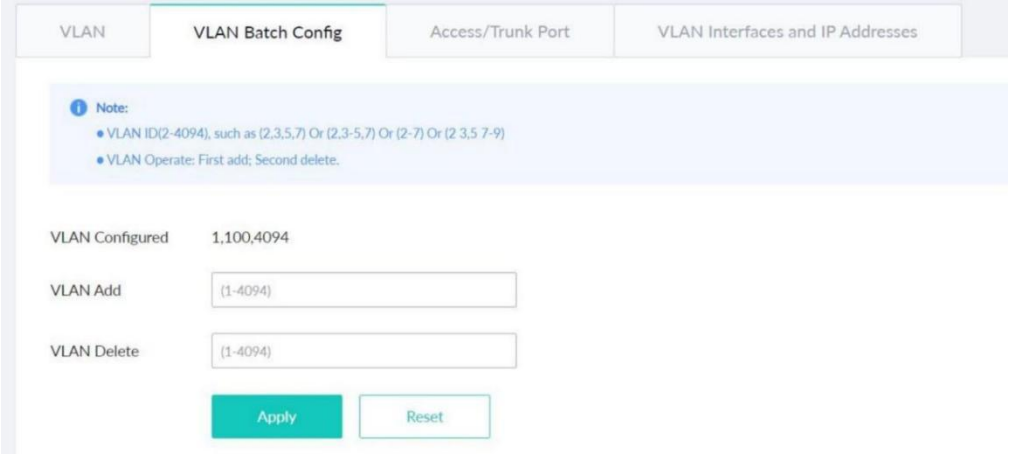
Through the port list, you can set for each port the default VLAN , the VLAN mode (Trunk or Access), whether to allow the entrance of current VLAN packets and whether to execute the untagging of the current VLAN when the port works as the egress port.

Note:

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

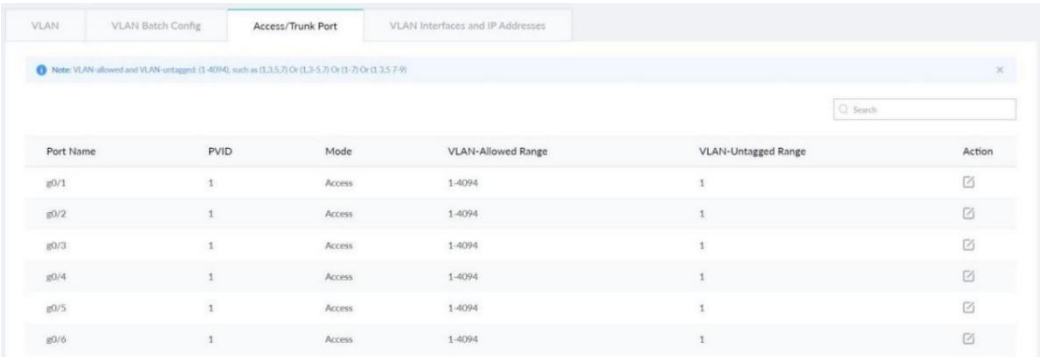
6.4.2 VLAN Batch Config

If you click **Network > VLAN > VLAN Batch Config** in the navigation bar, the **VLAN Batch Config** page appears, as shown in the figure.

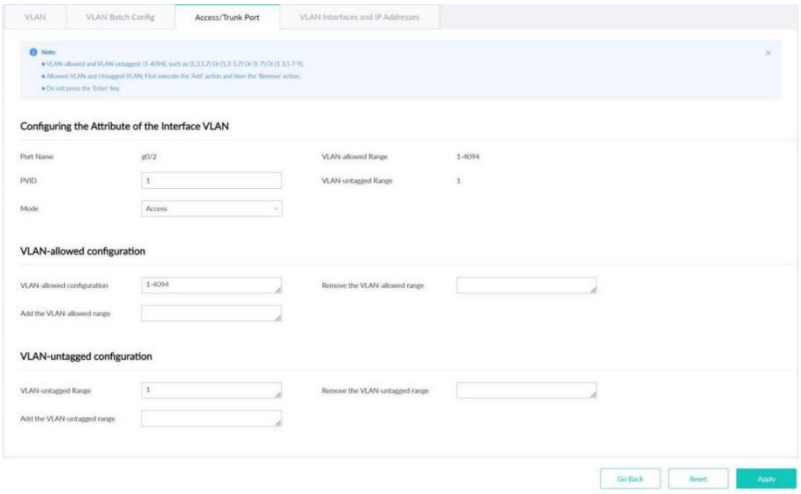


6.4.3 Access/Trunk Port

If you click **Interface > VLAN Config > Access/Trunk Port** in the navigation bar, the **Access/Trunk Port** page appears, as shown in the figure.



Click " " to configure the VLAN settings for this port.



6.4.4 VLAN Interfaces and IP Addresses

If you click **Network > VLAN interface and IP address Config**, the **VLAN Interfaces and IP Addresses** page appears.

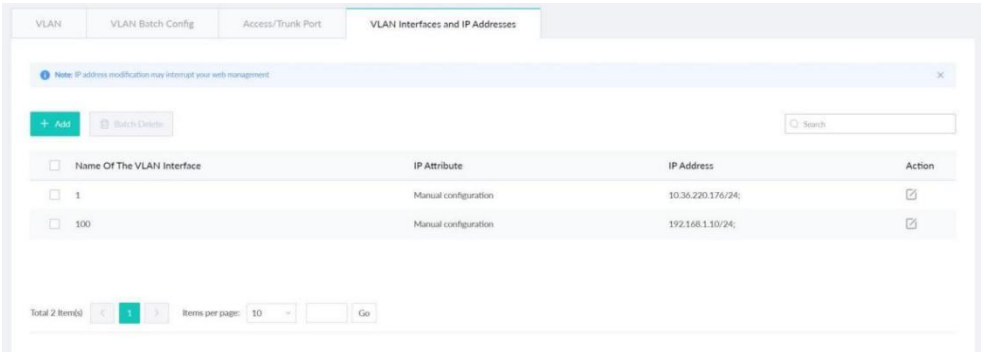


Figure 11: Configuring the VLAN interface

Click "Add" to add a new VLAN interface. Click "Delete" to delete a VLAN interface. Click "Edit" to modify the settings of a corresponding VLAN interface.

When you click "Add", the name of the corresponding VLAN interface can be modified; but if you click "Edit", the name of the corresponding VLAN interface cannot be modified.

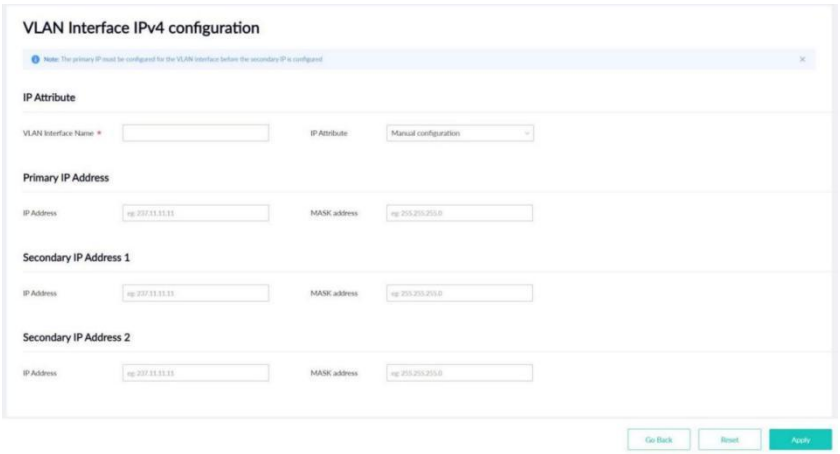


Figure 12: VLAN interface configuration

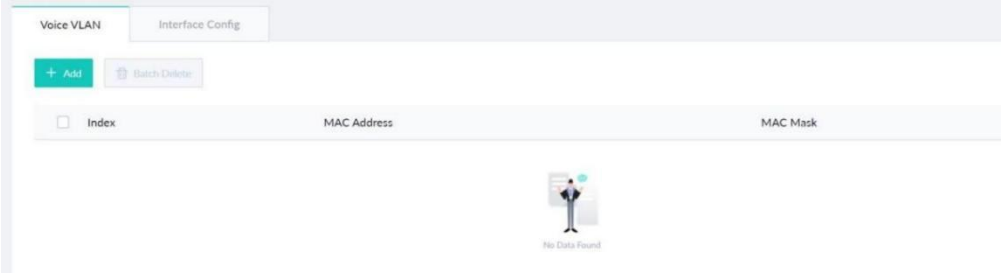
Note:

Before the accessory IP of a VLAN interface is set, you have to set the main IP.

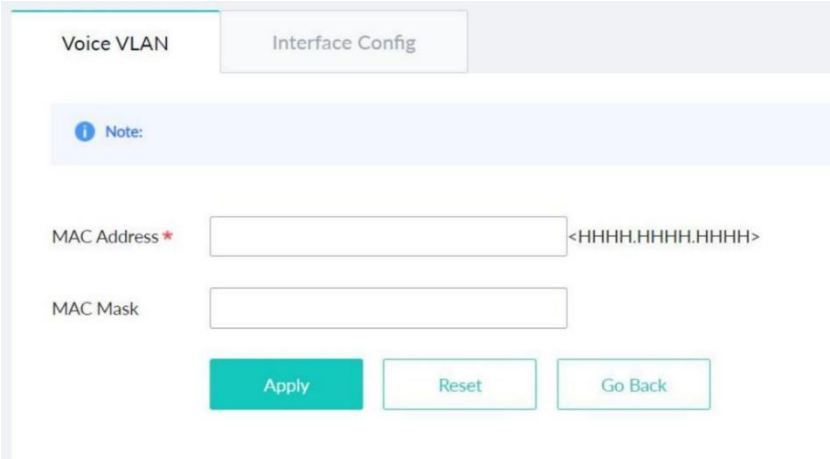
6.5 Voice VLAN

6.5.1 Voice VLAN

If you click **Network > Voice VLAN > Voice VLAN** in the navigation bar, the **Voice VLAN** page appears, as shown in figure.

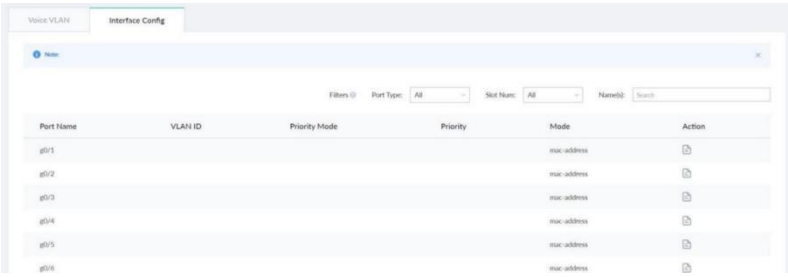


Click 'Add' to create a set of Voice VLAN MAC address and MAC mask entries.

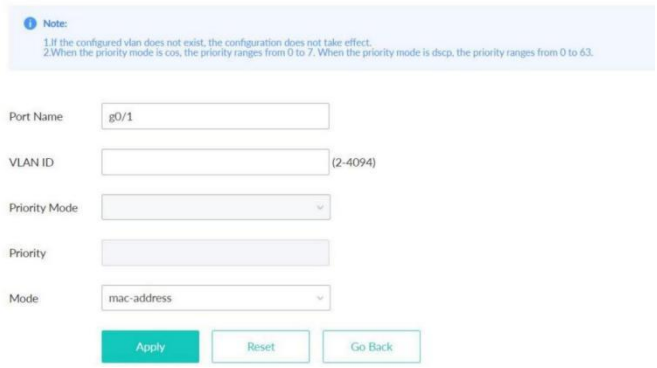


6.5.2 Interface Config

If you click **Network > Voice VLAN > Interface Config** in the navigation bar, the **Interface Config** page appears, as shown in figure.



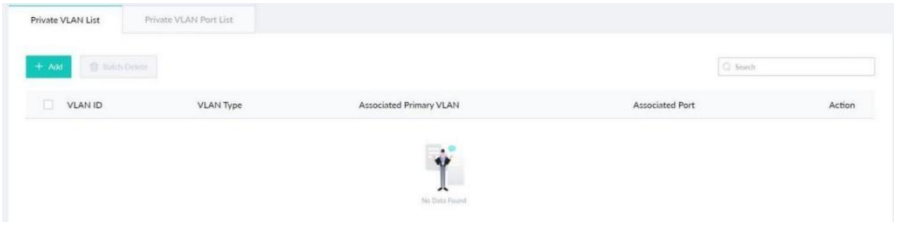
Click " " to enter the detailed configuration page for this port, as shown below:



6.6 Private VLAN

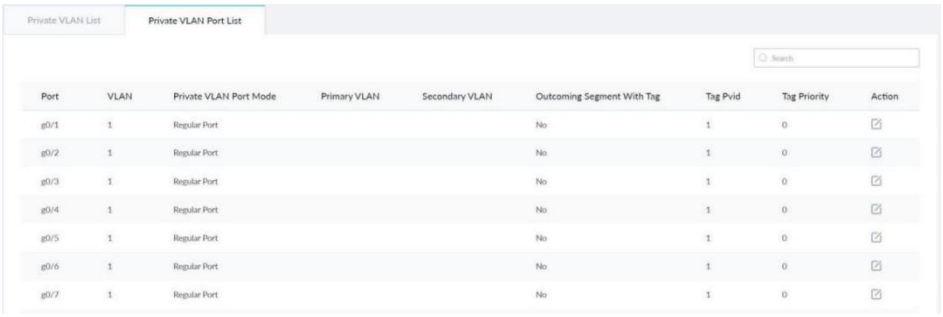
6.6.1 Private VLAN List

If you click **Network > Private VLAN > Private VLAN List** on the navigation bar, the **Private VLAN List** page appears.



6.6.2 Private VLAN Port List

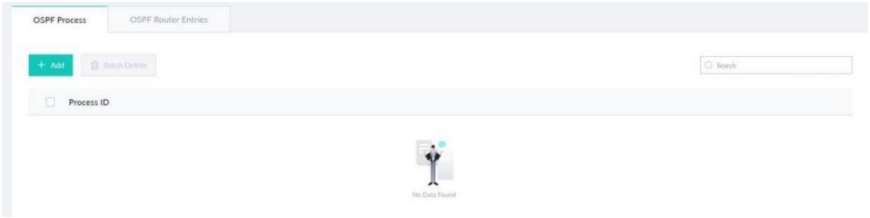
If you click **Network > Private VLAN > Private VLAN Port List** on the navigation bar, the **Private VLAN Port List** page appears.



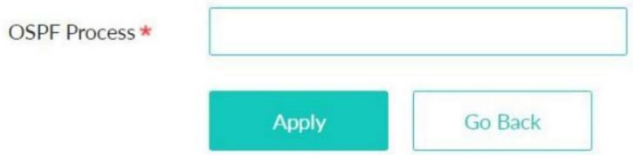
6.7 OSPF

6.7.1 OSPF Process

If you click **Network > OSPF > OSPF Process**, the **OSPF Process** page appears.

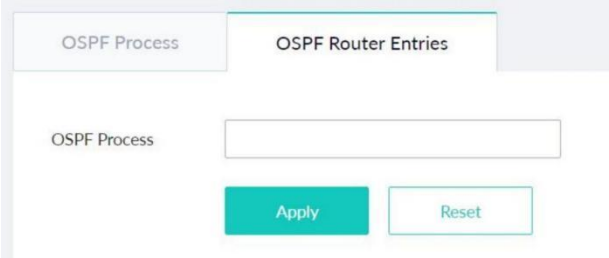


Click the 'Add' to establish a new OSPF process.



6.7.2 OSPF Router Entries

If you click **Network > OSPF > OSPF Router Entries**, the **OSPF Route Entries**page appears.



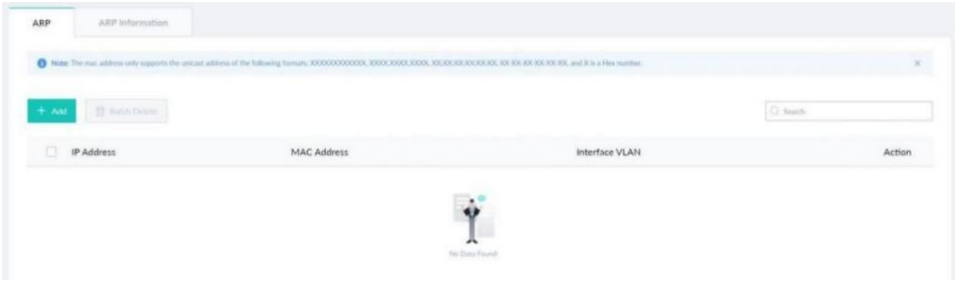
Chapter 7 Security

Figure 1: Security configuration list

7.1 ARP

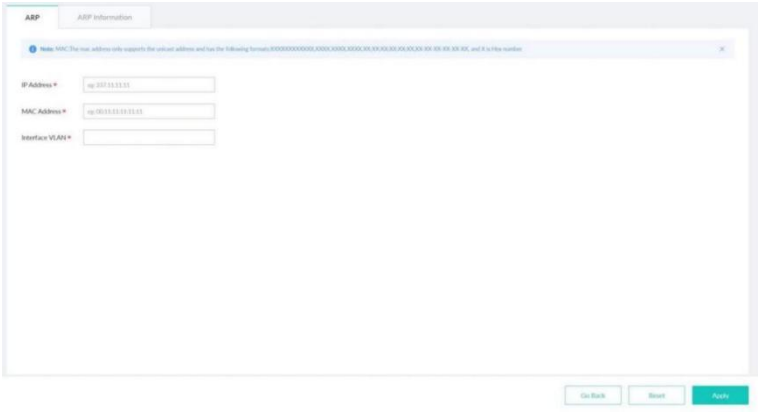
7.1.1 Basic ARP

Click "Security> ARP > ARP" in the navigation bar, and enter the configuration page of "Basic ARP"



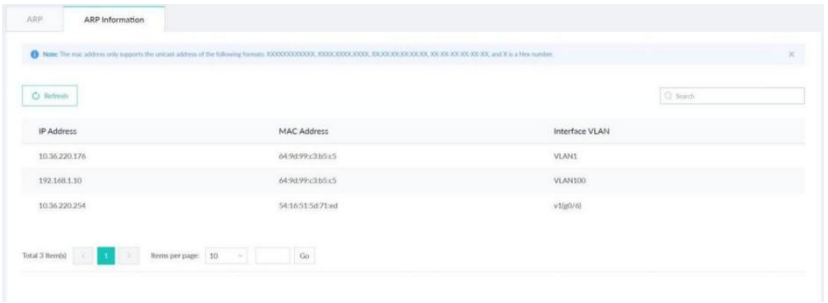
Click "Add" to add ARP table entries. When configuring ARP table entries, you need to specify the VLAN interface. Click "Edit" to change the ARP table entries of the current item.

Click "Delete" to remove the selected ARP entries.



7.1.2 ARP Information

Click "Security > ARP > ARP configuration" in the navigation bar, and enter the configuration page of "ARP configuration"



7.2 Port Security

7.2.1 IP-MAC Binding

If you click **Security > Port Security > IP-MAC Binding** in the navigation bar, the **Configure the IP-Binding Info** page appears, as shown in Figure 4-7.

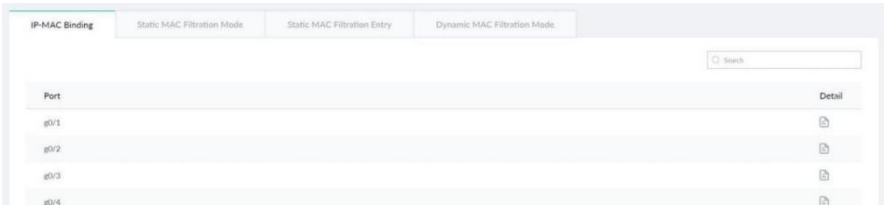


Figure 2 IP binding configuration

Click " " and then you can conduct the binding of the source IP address for each physical port. In this way, the IP address that is allowed to visit the port will be limited.

Figure 3 Setting the binding of the source IP address

7.2.2 Static MAC Filtration Mode

If you click **Security > Port Security > Static MAC Filtration Mode** in the navigation bar, the **Configure the Static MAC Filtration Mode** page appears, as shown in figure 4-11.

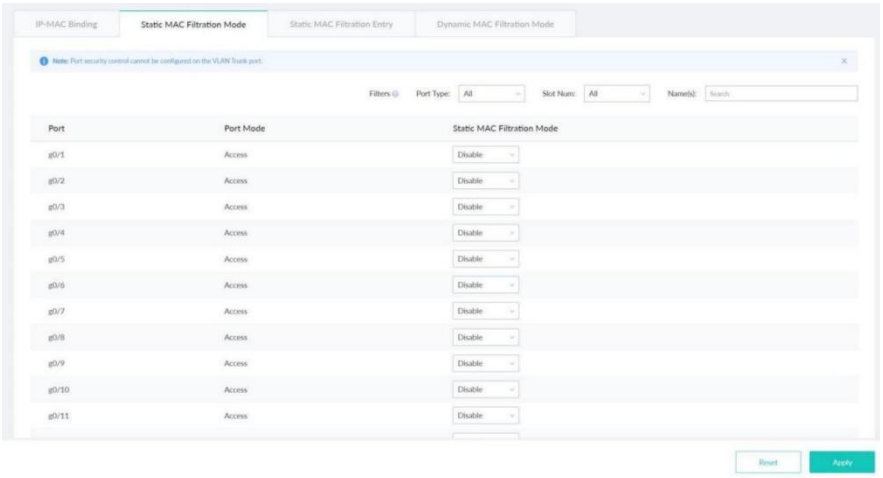


Figure 4: Setting the static MAC filtration mode

On this page you can set the static MAC filtration mode. By default, the static MAC filter is disabled. Also, the static MAC filter mode cannot be set on ports in trunk mode.

7.2.3 Static MAC Filtration Entries

If you click **Security > Port Security > Static MAC filtration entries** in the navigation bar, the **Setting the static MAC filtration entries** page appears.

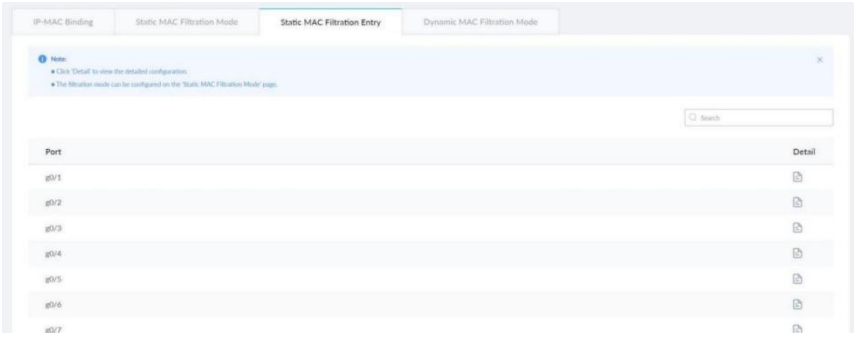


Figure 5: Static MAC filtration entry list

If you click " ", you can conduct the binding of the source MAC address for each physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.

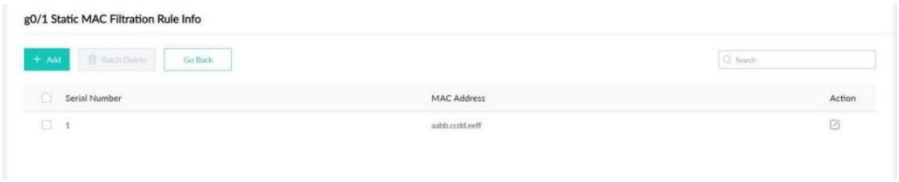


Figure 6: Setting static MAC filtration entries

7.2.4 Dynamic MAC Filtration Mode

If you click **Security > Port Security > Dynamic MAC Filtration Mode** in the navigation bar, the **Configure the dynamic MAC filtration mode** page appears, as shown in figure 4-14.

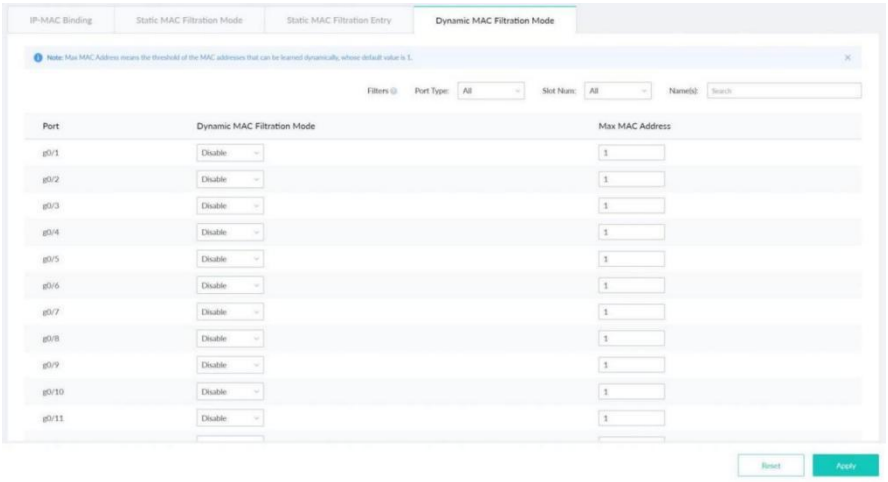


Figure 7 Dynamic MAC Filtration Mode

You can set the dynamic MAC filtration mode and the allowable maximum number of addresses on this page. By default, the dynamic MAC filtration mode is disabled and the maximum number of addresses is 1.

7.3 SNMP

7.3.1 Community Management

If you click **Security > SNMP > Community Management** in the navigation bar, the **Community Management** page appears, as shown in figure

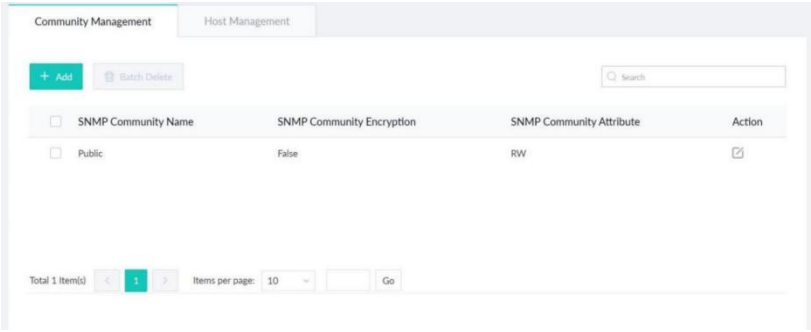


Figure 8 SNMP community management

On the SNMP community management page, you can know the related configuration information about SNMP community.

You can create, modify or cancel the SNMP community information, and if you click "Add" or " ", you can switch to the configuration page of SNMP community.

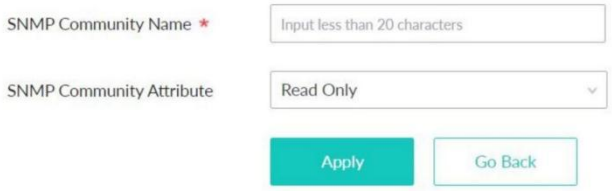


Figure 9 SNMP community management settings

On the SNMP community management page you can enter the SNMP community name, select the attributes of SNMP community, which include Read only and Read-Write.

7.3.2 Host Management

If you click **Security > SNMP > Host Management** in the navigation bar, the **Host Management** page appears, as shown in figure

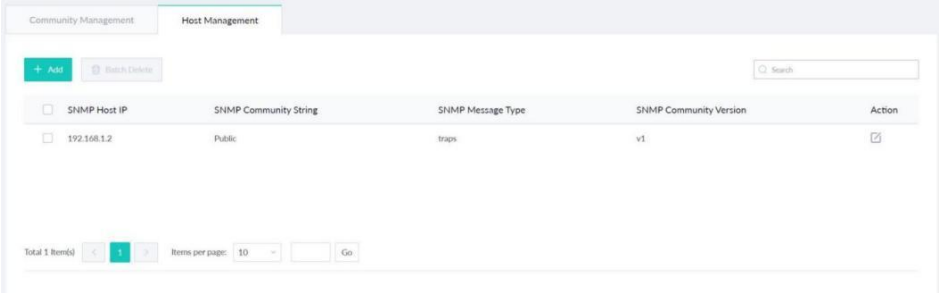


Figure 10 SNMP host management

On the SNMP community host page, you can know the related configuration information about SNMP host.

You can create, modify or cancel the SNMP host information, and if you click "Add" or " ", you can switch to the configuration page of SNMP host.

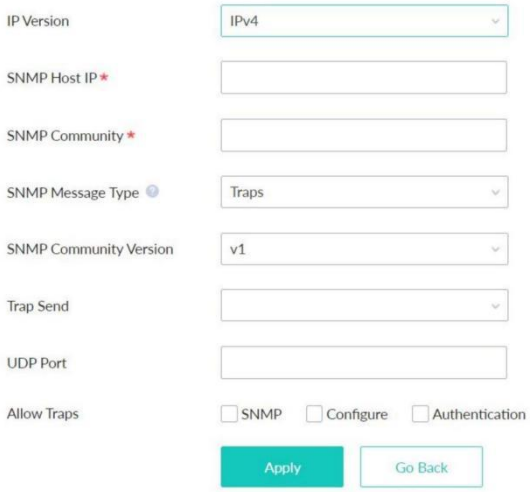
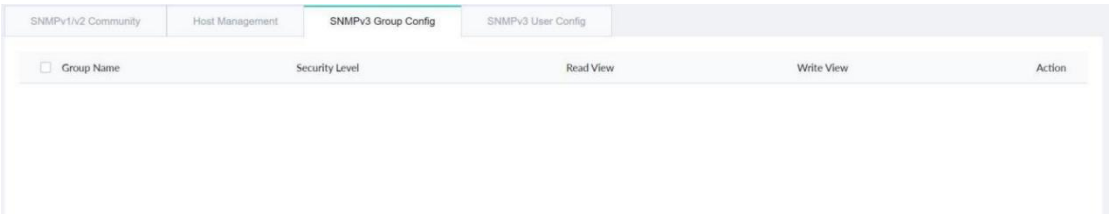


Figure 11 SNMP host management settings

On the SNMP host configuration page, you can enter the SNMP Host IP, SNMP Community, SNMP Message Type, and SNMP Community Version. SNMP Message Type includes Traps and Informs. For version 1, SNMP Message Type does not support Informs.

7.3.3 SNMPv3 Group Config

If you click **Security > SNMP > SNMPv3 Config** in the navigation bar, the **SNMPv3 Group Config** page appears, as shown in the figure.



Users can create, modify, or batch delete SNMP v3 group configuration information. By clicking 'Add' or 'Edit', you can switch to the SNMP v3 group configuration page.

7.3.4 SNMPv3 User Config

If you click **Security > SNMP > SNMPv3 Config > SNMPv3 User Configuration** in the navigation bar, the **SNMPv3 User Configuration** page appears, as shown in the figure.

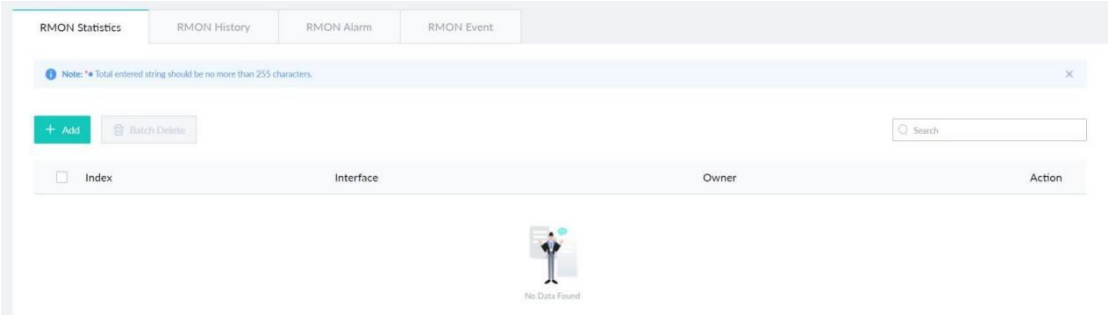
Through the SNMP v3 user configuration page, users can understand the related configuration information of SNMP v3 users.

Users can create, modify, or batch delete SNMP v3 user configuration information. By clicking 'Add' or 'Edit', you can switch to the SNMP v3 user configuration page.

7.4 RMON

7.4.1 RMON Statistic

If you click **Security > RMON> RMON Statistic** in the navigation bar, the **RMON Statistic** page appears, as shown in figure



If you click **Network Management Config > RMON > RMON Statistics > Add**, the **RMON Statistics** page appears.

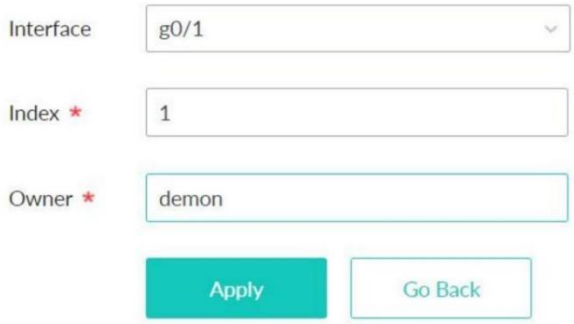


Figure 12 Configuring the RMON statistic information

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

At present, the monitor statistic information can be obtained through the command line "show rmon statistics", but the Web does not support this function.

7.4.2 RMON History

If you click **Security > RMON> RMON History** the **RMON History** page appears.

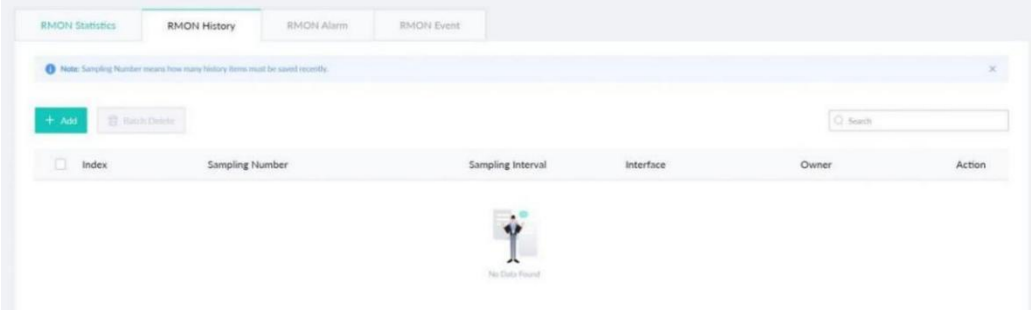
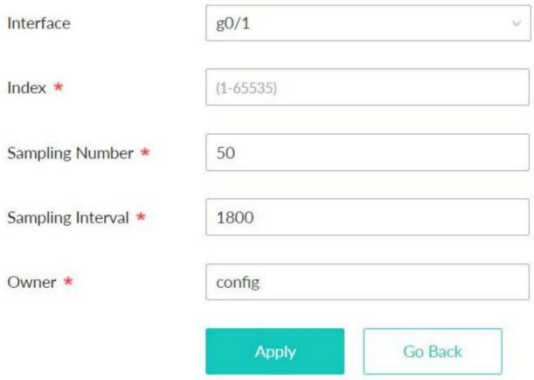


Figure 13 Configuring the RMON history information

Click"Add",



You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

The sampling number means the items that need be reserved, whose default value is 50.

The sampling interval means the time between two data collection, whose default value is 1800s.

At present, the monitor statistic information can be obtained through the command line "show rmon history", but the Web does not support this function.

7.4.3 RMON Alarm

If you click **Security > RMON> RMON Alarm**, the **RMON Alarm** page appears.

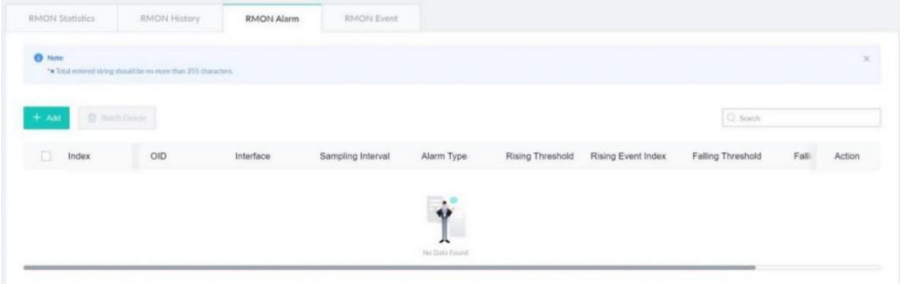
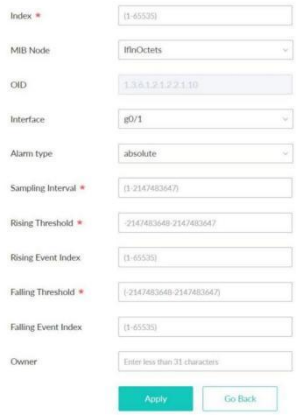


Figure 14 Configuring the RMON alarm information



The index is used to identify a specific alarm information; if the index is same to the previously applied index, it will replace the previous one.

The MIB node corresponds to OID.

If the alarm type is **absolute**, the value of the MIB object will be directly minitored; if the alarm type is **delta**, the change of the value of the MIB object in two sampling will be monitored.

When the monitored MIB object reaches or exceeds the rising threshold, the event corresponding to the index of the rising event will be triggered.

When the monitored MIB object reaches or exceeds the falling threshold, the event corresponding to the index of the falling event will be triggered.

7.4.4 RMON Event

If you click **Security > RMON> RMON Event**, the **RMON event** page appears.

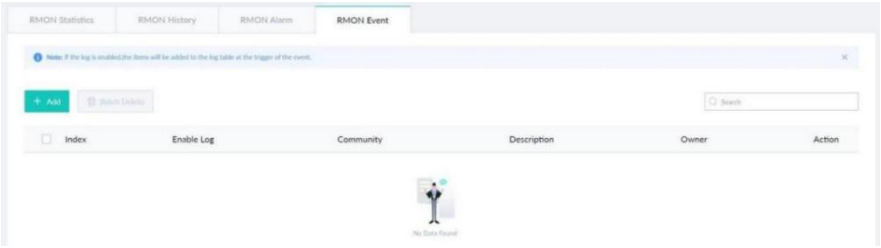


Figure 15 RMON event configuration

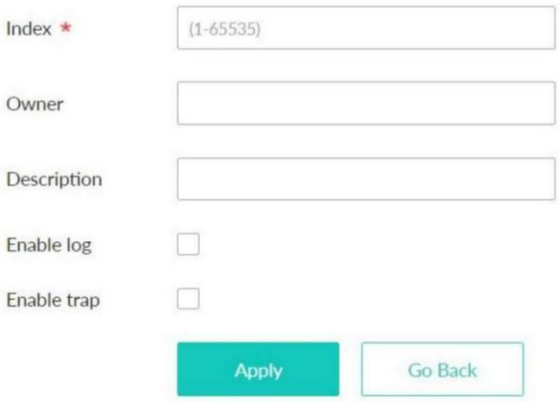
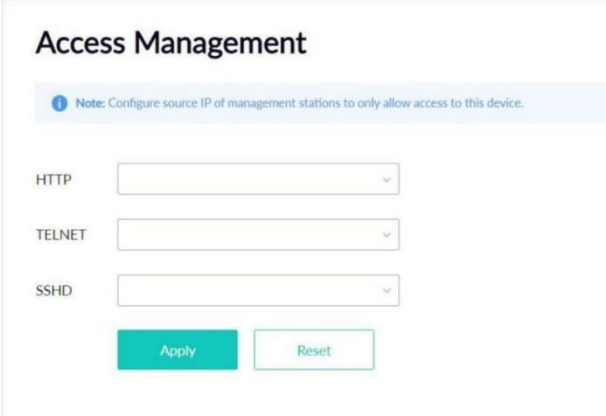


Figure 16 RMON event configuration

The index corresponds to the rising event index and the falling event index that have already been configured on the **RMON alarm config** page.
The owner is used to describe the descriptive information of an event.
"Enable log" means to add an item of information in the log table when the event is triggered.
“Enable trap” means a trap will be generated if the event is triggered.

7.5 Access Management

If you click **Security > Access Management** in the navigation bar, the **Access Management** page appears, as shown in the figure.



HTTP, TELNET, and SSHD all need to be created in advance from the command line before they can be directly selected here.

7.6 Static Routing

If you click **Security > Static Routing**, the **Configuring the static routing table** page appears.

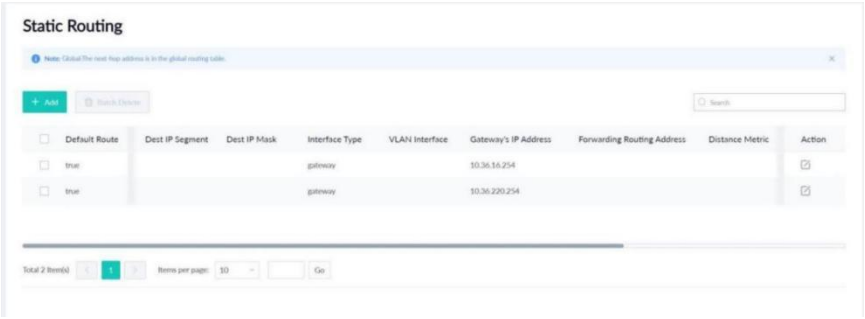


Figure 17: configure Static Routing
Click “Add” to add a new static routing table.

Click " " to modify the settings of a corresponding static routing table. Click “Batch Delete” to delete a static routing table.

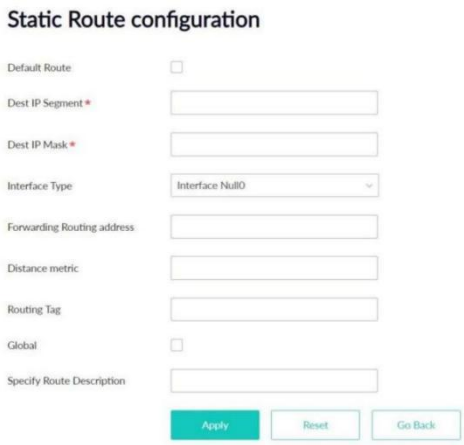
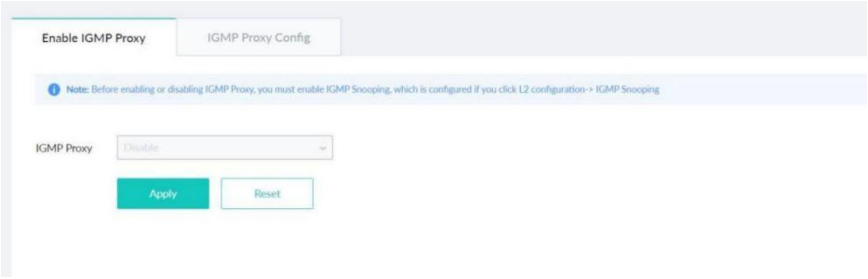


Figure 18: Static Routing configuration

7.7 IGMP Proxy

7.7.1 Enable IGMP Proxy

If you click **Security > IGMP Proxy > Enable IGMP Proxy**, the **Enable IGMP Proxy** page appears.



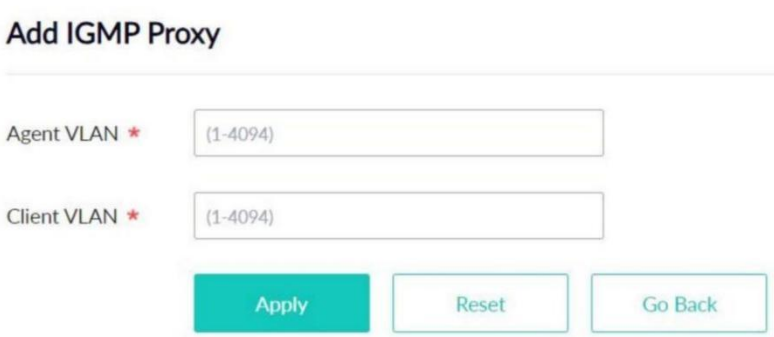
You need to enable "IGMP Snooping" before you can create a new IGMP proxy on this page.

7.7.2 IGMP Proxy Config

If you click **Security > IGMP Proxy > IGMP Proxy Config**, the **IGMP Proxy Config** page appears.

You can only create a new IGMP proxy after enabling the IGMP proxy feature.

Clicking "Add" allows you to create a VLAN for IGMP proxy.



Chapter 8 System Management

Figure 1: System Management configuration list

8.1 Reboot

8.1.1 Reboot

If you click **System Management > Reboot > Reboot** , the **Reboot** page appears.

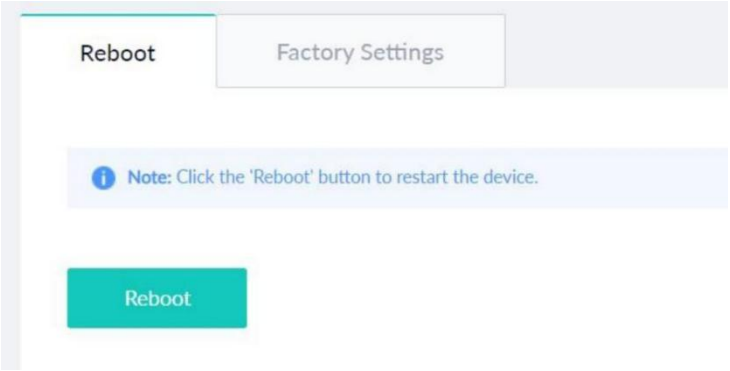
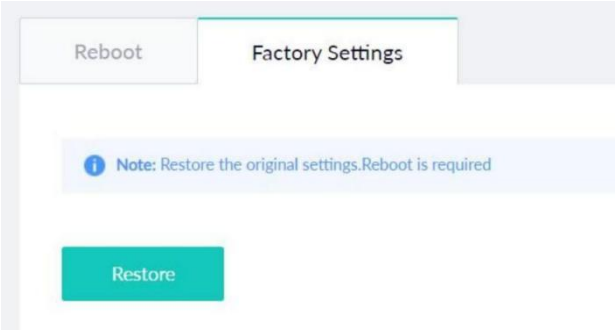


Figure 2 Rebooting the device

If the device need be rebooted, please first make sure that the modified configuration of the device has already been saved, and then click the "Reboot" button.

8.1.2 Factory Settings

If you click **System Management > Reboot > Factory Settings**, the **Factory Settings** page appears.



8.2 Users

8.2.1 User List

If you click **System Management > Users > User Management,** the **User Management** page appears.

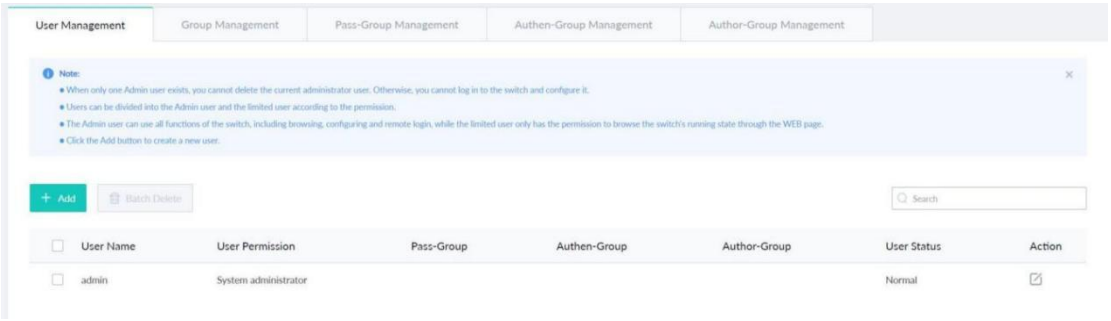


Figure 3 User list

You can click "Add" to create a new user.

To modify the permission or the login password, click "Edit" on the right of the user list.

Note:

1. Please make sure that at least one system administrator exists in the system, so that you can manage the devices through Web.
2. The limited user can only browse the status of the device.

If you click "Add" on the **User Management** page, the **Creating User** page appears.

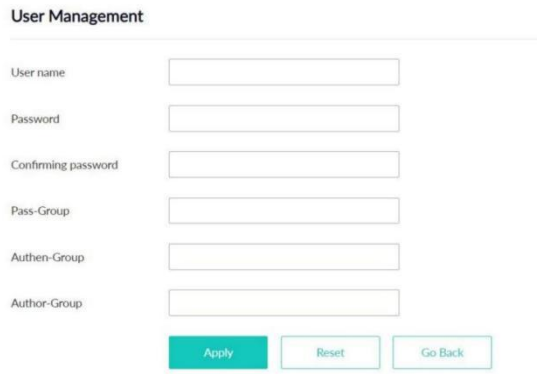


Figure 4 Creating new users

In the “User name” text box, enter a name, which contains letters, numbers and symbols except “?”, “\”, “&”, “#” and the “Space” symbol. \ “ & # and characters other than spaces.

In the “Password” textbox enter a login password, and in the “Confirming password” textbox enter this login password again.

8.2.2 Group Management

If you click “Add” on the **User Management.** page, the **User Group Management** page appears.

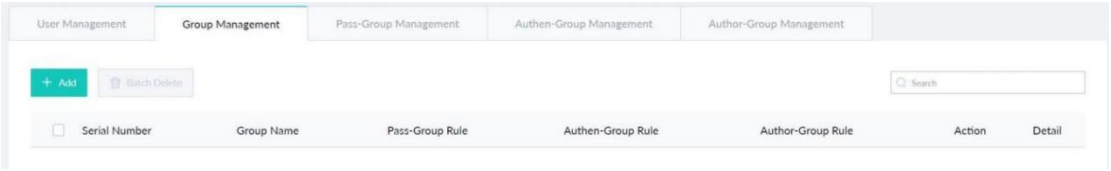


Figure 5 User group list

Click“Add” to create a new user group.

Click Batch Delete to delete the user group.

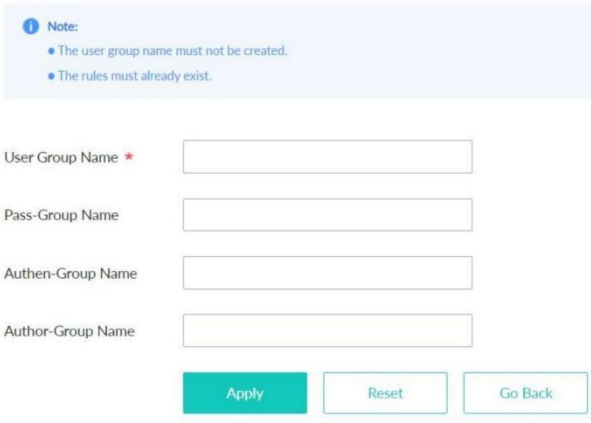


Figure 6 User group configuration

The User Group Name must be different with the existing group names. The user group cannot be created until the Pass- Group name, Authen-Group Name and Author-Group Name are specified. Configuring the Pass-Group name, Authen- Group Name and Author-Group Name in another 3 pages.

8.2.3 Pass-Group Management

Click **Pass-Group Management,** and the **Pass-Group Management.** The page appears.

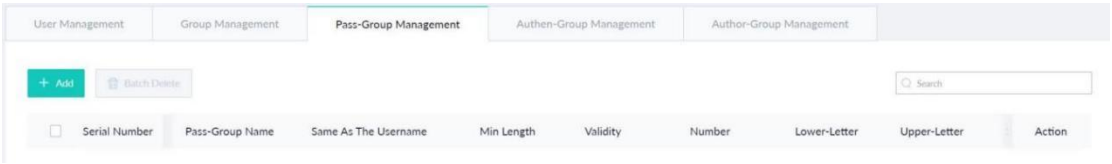
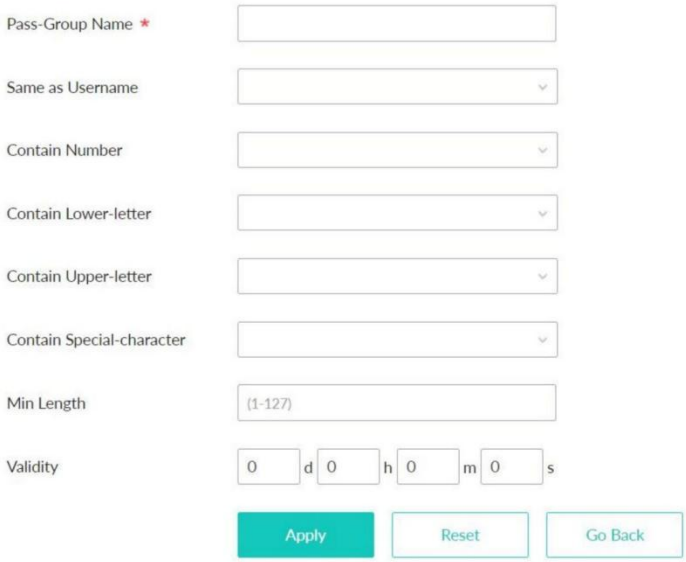


Figure 7 Password Group Management

Click"Add" to create a new password rule.

Click Batch Delete to delete the password rule.



In the Pass-Group Configuration, the password can be set whether to be same as Username, Contain Number, Contain Lower-letter, Contain Upper-letter, Contain Special-character, Min Length and validity.

The rule can be applied to the user management. The password is valid only when it conforms to the rule.

8.2.4 Authen-Group Management

Click **Authen-Group Management.** on the navigation bar, and **Authen-Group Management** appears.

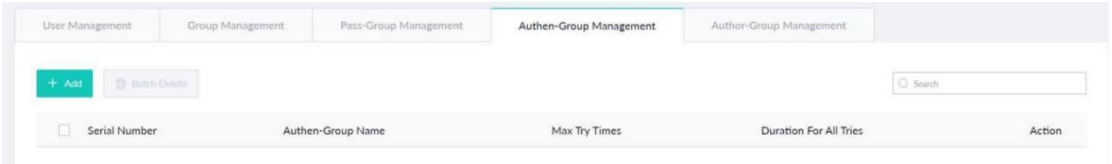
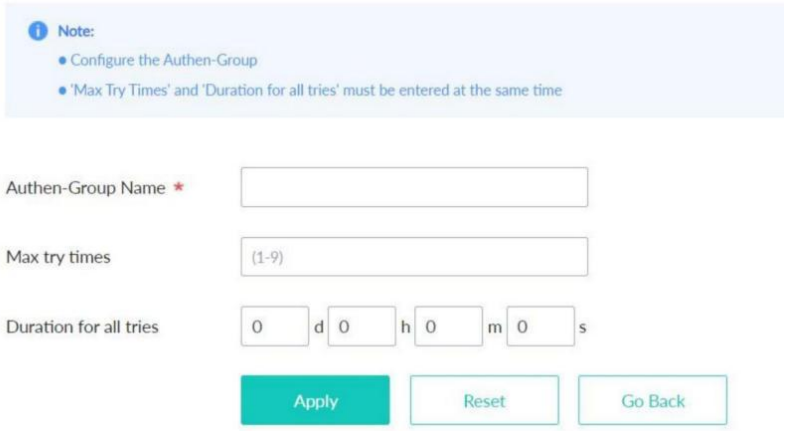


Figure 8 Pass Group Configuration

Click"Add" to create a new authorization rule.

Click Batch Delete to delete the authorization rule.



The **Max try times** and **Duration of all tries** can be configured or not. But they must be adjusted simultaneously.

8.2.5 Author-Group Management

If you click **Author-Group Management**. and the **Author-Group Mgr.** page appears.

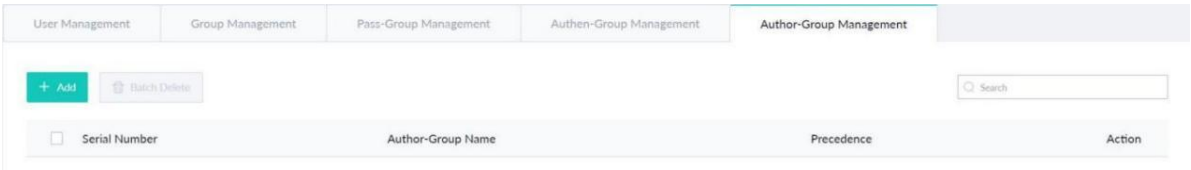


Figure 9 Author Group Management

Click"Add" to create a new authorization rule.

Click Batch Delete to delete the new authorization rule.

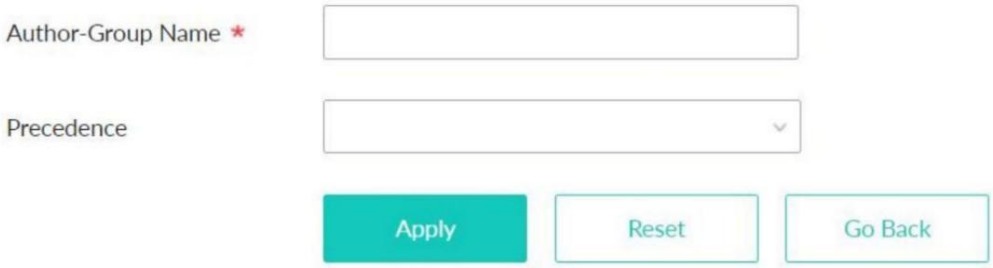
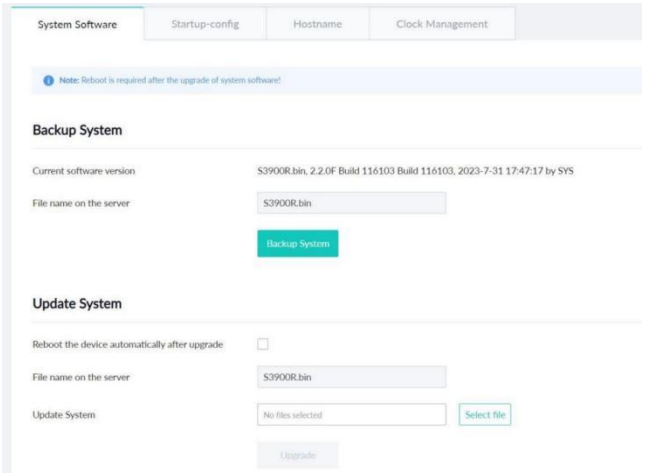


Figure 10 Author Group Configuration

The authorization rule determines the user's access: Administrator or Limited user. The **Administrator** has full access to the configuration and the **Limited user** only has access to check the configuration.

8.3 System Management

8.3.1 System Software



On this page the currently running software version is displayed. If you want to back up, please click "Backup System"; then on the browser, the file download dialog box appears; click "Save" to store the file to the disk of the PC, mobile storage device or other network location.

Backup Note:

The default name of the document is "Switch.bin" It is suggested to modify it as a name which is detectable and searchable when its backup is created.

Update Note:

1. Please make sure that your upgrade matches the device type, because the matchable will not lead to the normal startup of the device.

2. The upgrade of probably takes one to two minutes; when the "Upgrade" button is clicked, the files will be uploaded to the device.

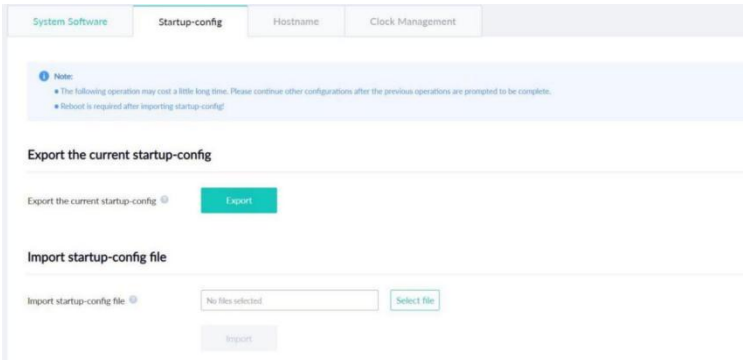
3. If errors occur during upgrade, please do not restart the device or cut off the power of the device, or the device cannot be started. Please try the upgrade again.

4. After the upgrade please save the configuration and then restart the device to run the new.

The upgraded is always used to solve the already known problems or to perfect a specific function. If you device run normally, do not upgrade your software frequently.

If need be upgraded, please first enter the complete path of the new files in the textbox on the right of "Upgrading", or click the "Browsing" button and select the new files on your computer, and then click "Updating."

8.3.2 Startup-config



The current configuration file can be exported, saved in the disk of PC or in the mobile storage device as the backup file. To export the configuration file, please click the “Export” button

The default name of the configuration file is “startup-config”, but you are suggested to set it to an easily memorable name.

You can import the configuration files from PC to the device and replace the configuration file that is currently being used. For example, by importing the backup configuration files, you can resume the device to its configuration of a previous moment.

Import Note:

1. Please make sure that the imported configuration file has the legal format for the configuration file with illegal format cannot lead to the normal startup of the device.

2. If error occurs during the process of importation, please try it later again, or click the “Save All” button to make the device re-establish the configuration file with the current configuration, avoiding the incomplete file and the abnormality of the device.

3. After the configuration file is imported, if you want to use the imported configuration file immediately, do not click

“Save All”, but reboot the device directly.

8.3.3 Hostname

If you click **System Management > System Management > Hostname** in the navigation bar, the **Hostname Configuration** page appears, as shown in the figure.

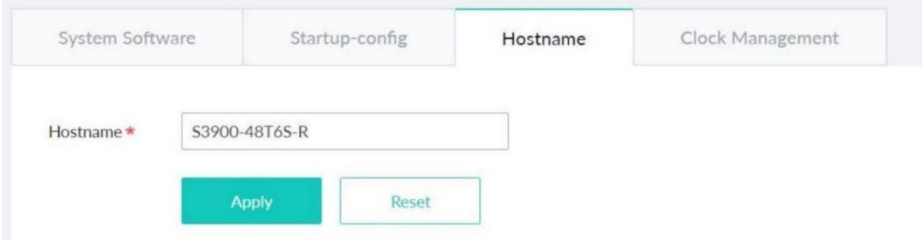


Figure 11 Hostname configuration

The hostname will be displayed in the login dialog box.

The default name of the device is “Switch” You can enter the new hostname (Chinese characters are not supported) in the text box shown in figure 3 and then click “Apply”

8.3.4 Clock Management

If you click **System Management > System Management > Clock Management,** the **Clock Management** page appears.

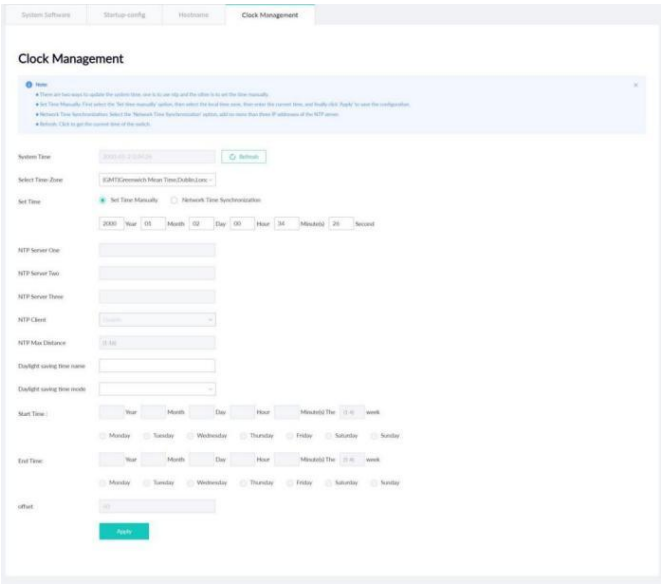


Figure 12 Clock management

To refresh the clock of the displayed device, click “Refresh”

In the “Select Time-Zone” dropdown box select the time zone where the device is located. When you select “Set Time Manually”, you can set the time of the device manually. When you select “Network Time Synchronization”, you can designate 3 SNTP servers for the device. The synchronization function of the NTP client can also be enabled. When configuring daylight saving time, there are two options: absolute and periodical. 'Absolute' specifies the exact year, month, day, hour, and minute when daylight saving time starts and ends. 'Periodical' specifies the start and end time of daylight saving time in the format of "the xth week of x month, hh:mm", and this is repeated annually.

8.4 Log

8.4.1 Log

If you click **System Manage > Log Manage**, the **Log Management** page appears.

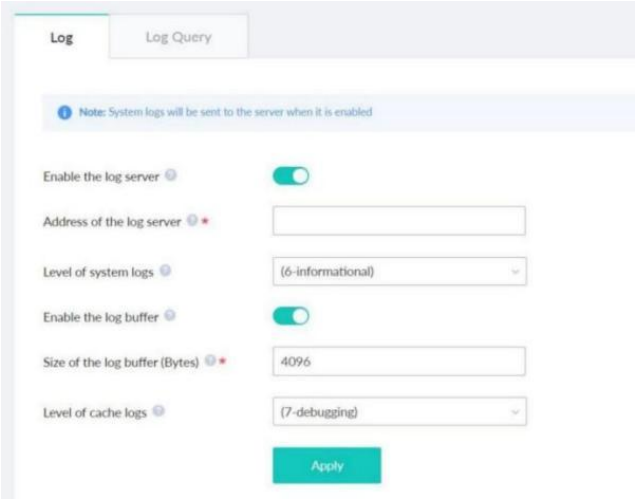


Figure 13 Log management

If “Enabling the log server” is 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 “Address of the system log server” textbox and select the log's grade in the “Grade of the system log information” dropdown box.

If “Enabling the log buffer” is 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 which is saved in the memory will be lost after rebooting. Please enter the size of the buffer area in the “Size of the system log buffer” textbox and select the grade of the cached log in the “Grade of the cache log information” dropdown box.

8.4.2 Log Query

If you click **Device Status > Log Query** in the navigation bar, the **Log Query** page appears, as shown in the figure.

Chapter 9 Diagnostics

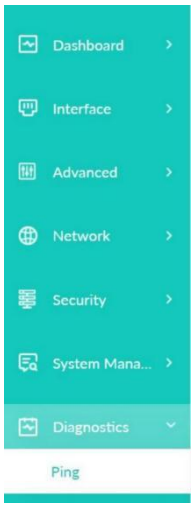


Figure 1: Diagnostics tool list

9.1 Ping

9.1.1 Ping

If you click **Diagnostics > Ping**, the **Ping** page appears.

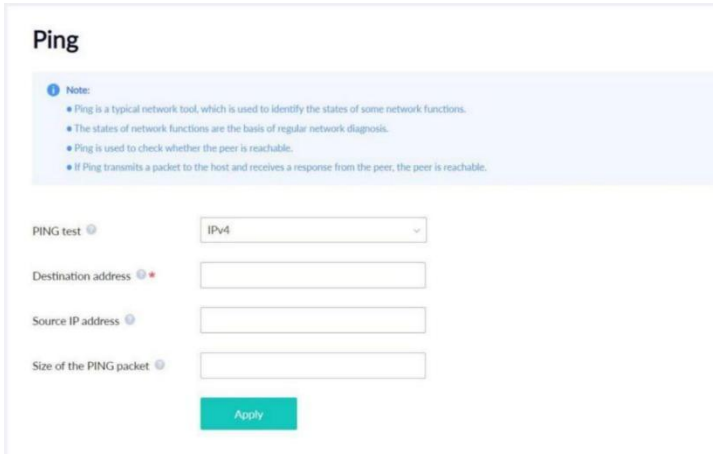


Figure 2 Ping

Ping is used to test whether the switch connects other devices.

If a Ping test need be conducted, please enter an IP address in the “Destination address” textbox, such as the IP address of your PC, and then click the “PING” button. If the switch connects your entered address, the device can promptly return a test result to you; if not, the device will take a little more time to return the test result.

“Source IP address” is used to set the source IP address which is carried in the Ping packet.

“Size of the PING packet” is used to set the length of the Ping packet which is transmitted by the device.