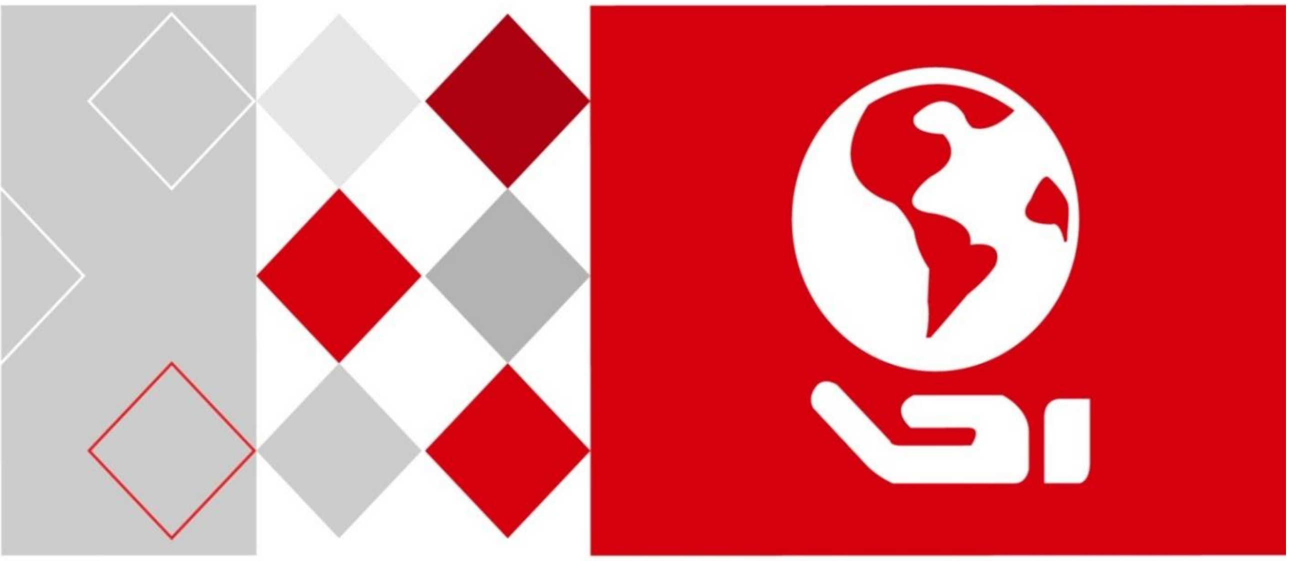


DS-3E2300P Series Ethernet Switch WEB Configuration

User Manual

UD03706B

User Manual

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to DS-3E2300P Series Ethernet Switch.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Table of Contents

Chapter 1 Configuration Preparation

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 HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support users to change the service port and after the service port is changed you have to use the IP address and the changed port to access switches. For example, if you set the IP address and the service port to 192.168.1.3 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 (such as ftp-20, telnet-23, dns-53, snmp-161) 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 { portNumber }	Setting 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 switch and PC and, when the HTTP service is closed, HTTP exchange stops.

Command	Purpose
ip http server	Enabling 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	Purpose
ip http http-access enable	Setting the HTTP Access Mode

1.1.5 Setting the Maximum Number of VLAN Entries Displayed on a 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	Purpose
ip http web max-vlan { *max-vlan* }	Sets the maximum number of VLAN entries displayed in a web page.

1.1.6 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 Web then shows these multicast entries. The default maximum number of multicast entries is 15.

Command	Purpose
ip http web igmp-groups { *igmp-groups* }	Sets the maximum number of multicast entries displayed in a 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	Purpose

ip http ssl-access enable	Setting 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 also can 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.

Parameters	Notes:
ip http secure-port {*portNumber*}	Sets the HTTPS port.

Chapter 2 Accessing the Switch through HTTP

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 version 1.1

JavaScriptTM 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.

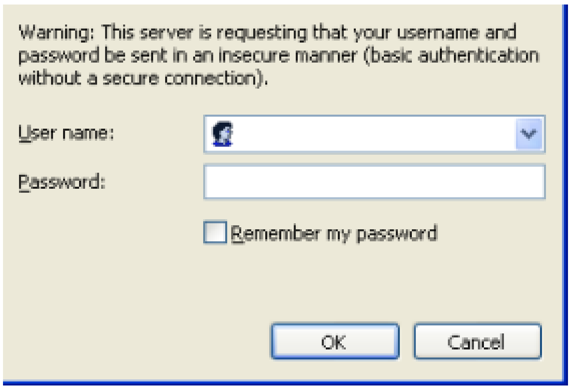
2.1.1 Initially Accessing the Switch

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

Step 1 Modify the IP address of the network adapter and subnet mask of your computer to 192.168.0.2 and 255.255.255.0 respectively.

Step 2 Open the Web browser and enter 192.168.0.1 in the address bar. It is noted that 192.168.0.1 is the default management address of the switch.

Step 3 If the Internet Explorer browser is used, you can see the dialog box as below. Both the original username and the password are “admin”, which is capital sensitive.



Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

Step 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:

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

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

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

Step 4 Enter the command**ip http server**", to enable Web service.

Step 5 Enter the**username**to set the user name and password of the switch For how to use this command, refer to the “Security Configuration” section in the user manual.

Step 6 After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.

Step 7 Enter the command**write**", to save 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 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:

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

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

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

Step 4 Enter the command **ip http server**", to enable Web service.

Step 5 Enter the **username** to set the user name and password of the switch For how to use this command, refer to the “Security Configuration” section in the user manual.

Step 6 Run **ip http ssl-access enable** to enable the secure link access of the switch.

Step 7 Run **no ip http http-access enable** to access the switch through insecure links.

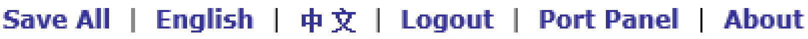
Step 8 Enter the command **write**", to save the current configuration to the configuration file.

Step 9 Open the WEB browser on the PC that the switch connects, enterhttps://192.168.0.1on the address bar (192.168.0.1 stands for the management IP address of the switch)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 whole Web homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

2.3.1 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.

English

The interface will turn into the English version.

Chinese

The interface will turn into the Chinese version.

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.

Interface panel

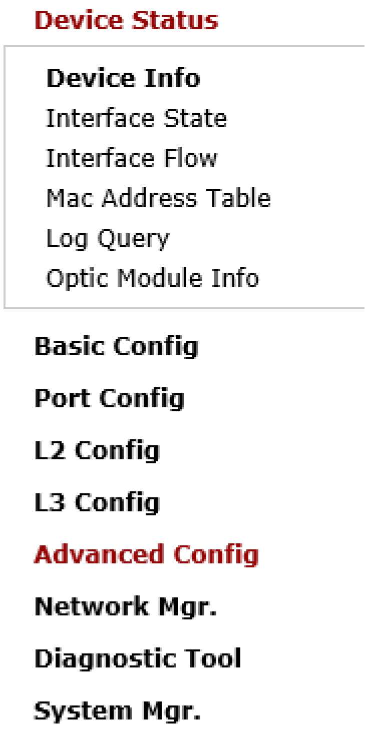
Displays the figure of interface panel

About

Displays the manufacturer information and sets auto-refresh.

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

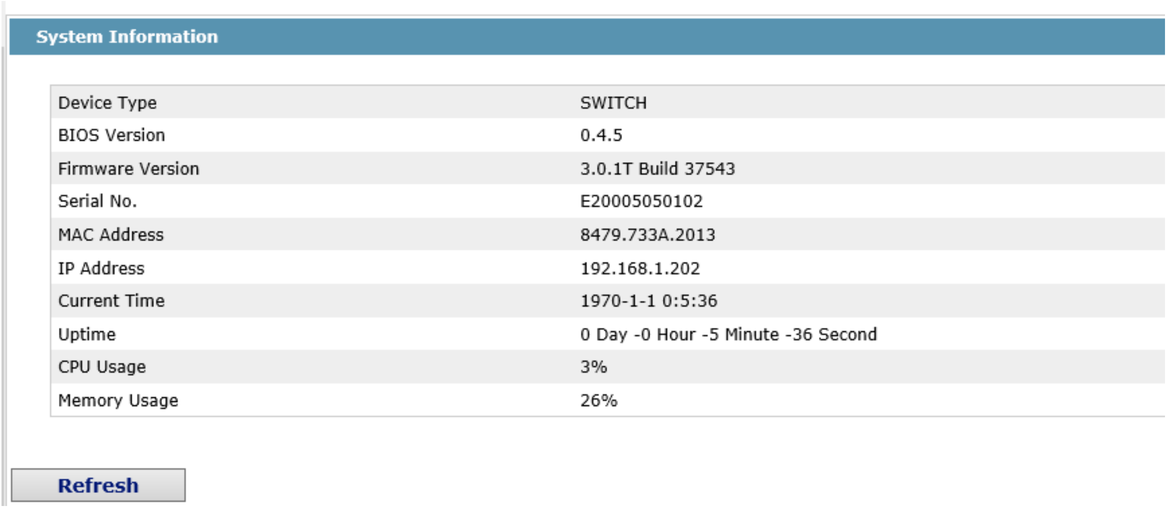


The contents shown in the navigation bar. The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at “Runtime Info”. If a certain item need be configured, please click the group name and then the subitem. For example, to browse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

NOTE

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

2.3.3 Configuration Area



System Information

Device Type	SWITCH
BIOS Version	0.4.5
Firmware Version	3.0.1T Build 37543
Serial No.	E20005050102
MAC Address	8479.733A.2013
IP Address	192.168.1.202
Current Time	1970-1-1 0:5:36
Uptime	0 Day -0 Hour -5 Minute -36 Second
CPU Usage	3%
Memory Usage	26%

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

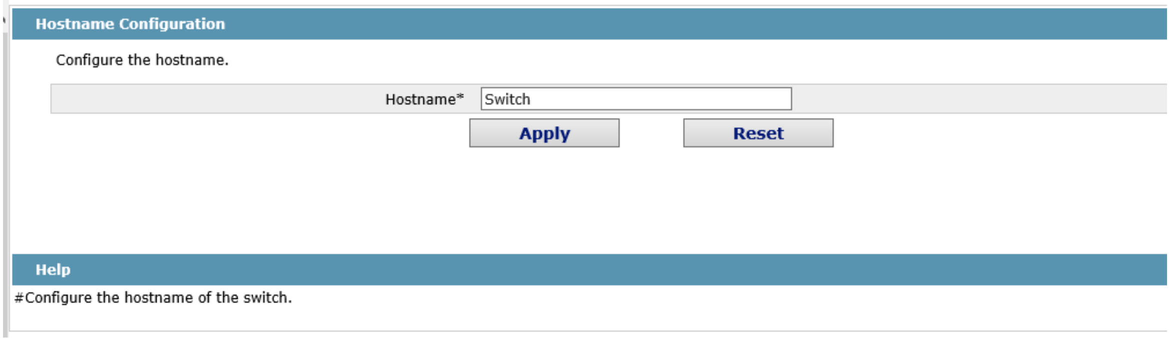
The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, and their functions are listed in the following table:

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 resetted.
New	Creates a list item. For example, you can create a VLAN item or a new user.
Delete	Deletes an item in the list.
Back	Go back to the previous-level configuration page.

Chapter 3 Basic Configuration

3.1 Hostname Configuration

Click **Basic Config -> Hostname** in the navigation bar, the Hostname Configuration page appears, as shown in the following figure.



Hostname Configuration

Configure the hostname.

Hostname* Switch

Help

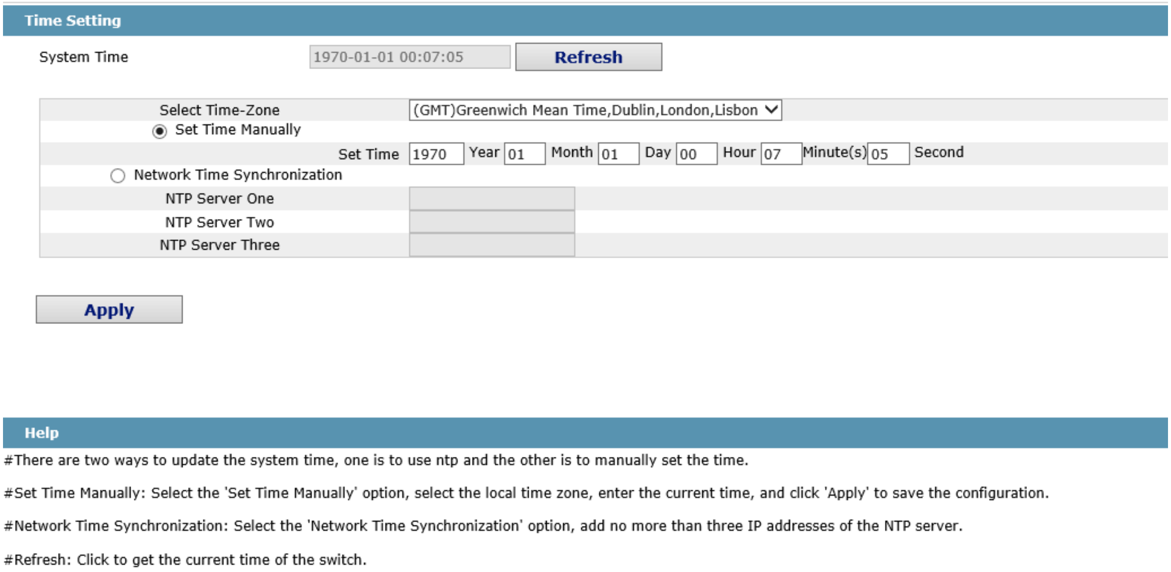
#Configure the hostname of the switch.

The hostname will be displayed in the login dialog box.

The default name of the device is "Switch". You can enter the new hostname in the text box shown in figure 3 and then click "Apply".

3.2 Time Management

Click **System Mgr. -> Time Setting**, the Time Setting page appears.



Time Setting

System Time 1970-01-01 00:07:05

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

● Set Time Manually

Set Time 1970 Year 01 Month 01 Day 00 Hour 07 Minute(s) 05 Second

○ Network Time Synchronization

NTP Server One

NTP Server Two

NTP Server Three

Help

#There are two ways to update the system time, one is to use ntp and the other is to manually set the time.

#Set Time Manually: Select the 'Set Time Manually' option, select the local time zone, enter the current time, and click 'Apply' to save the configuration.

#Network Time Synchronization: Select the 'Network Time Synchronization' option, add no more than three IP addresses of the NTP server.

#Refresh: Click to get the current time of the switch.

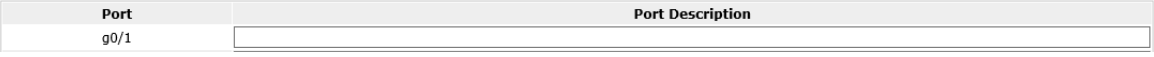
To refresh the clock of the displayed device, click "Refresh".

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 and set the interval of time synchronization.

Chapter 4 Configuration of the Physical Interface

4.1 Configuring Port Description

Click **Port Config -> Port Description** in the navigation bar, the Port description Configuration page appears, as shown in the following figure.

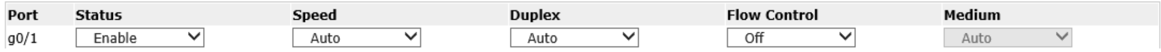


Port	Port Description
g0/1	

You can modify the port description on this page and enter up to 120 characters. The description of the VLAN port cannot be set at present.

4.2 Configuring the Attributes of the Port

Click Port Config**-> Port Config ->** Port attribute Config in the navigation bar, the Port Attribute Configuration page appears, as shown in the following figure.



Port	Status	Speed	Duplex	Flow Control	Medium
g0/1	Enable	Auto	Auto	Off	Auto

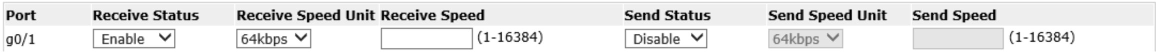
You can change the status, speed, duplex mode and flow control of a port on this page.

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.

4.3 Rate Limit

Click **Port Config -> Rate Limit** in the navigation bar, the Port rate limit page appears, as shown in figure 4.

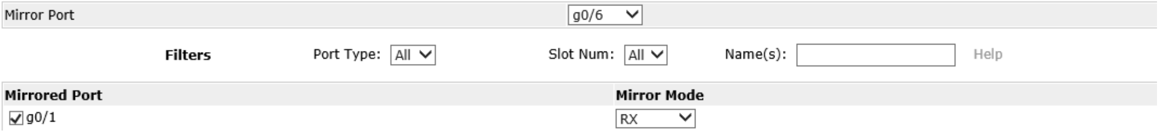


Port	Receive Status	Receive Speed Unit	Receive Speed	Send Status	Send Speed Unit	Send Speed
g0/1	Enable	64kbps	(1-16384)	Disable	64kbps	(1-16384)

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited. The reception speed and transmission speed are configured by a percentage or by the designated unit of the switch.

4.4 Port Mirror

Click **Port Config-> Port Mirror** in the navigation bar, the Port Mirror Config page appears, as shown in the following figure.



Mirror Port	g0/6

Filters Port Type: All Slot Num: All Name(s): Help

Mirrored Port	Mirror Mode
☑ g0/1	RX

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

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

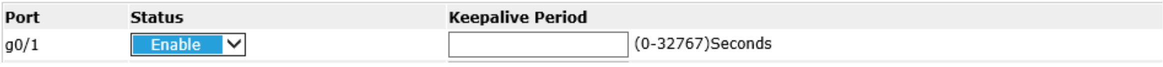
RX The received packets will be mirrored to the destination port.

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

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

4.5 Keepalive Detection

Click **Port Config-> Keepalive Detection** in the navigation bar, the Setting the port loopback detection page appears, as shown in the following figure.



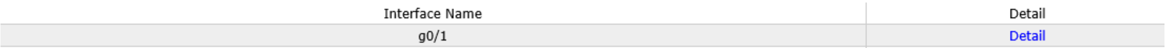
Port	Status	Keepalive Period
g0/1	Enable	(0-32767)Seconds

You can set the loopback detection cycle on the Loopback Detection page.

4.6 Port security

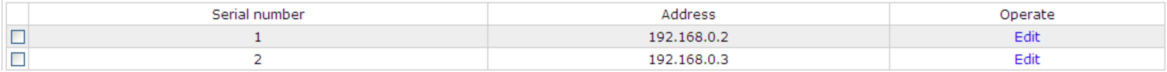
4.6.1 IP Binding Configuration

Click **Port Config-> Port Security -> IP Bind** in the navigation bar, the Configure the IP-Binding Info page appears, as shown in figure 7.



Interface Name	Detail
g0/1	Detail

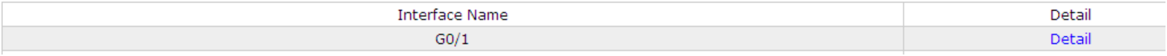
Click “Detail” and then you can conduct the binding of the source IP address for each physical port. In this way, the IP address that is allowed to visit the port will be limited.



	Serial number	Address	Operate
□	1	192.168.0.2	Edit
□	2	192.168.0.3	Edit

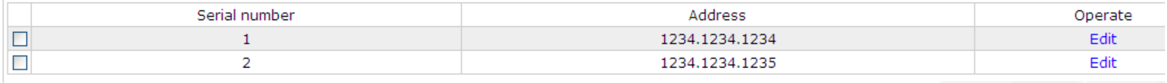
4.6.2 MAC Binding Configuration

Click **Port Config-> Port Security -> MAC Bind** in the navigation bar, the Configure the MAC-Binding Info page appears, as shown in the following figure.



Interface Name	Detail
G0/1	Detail

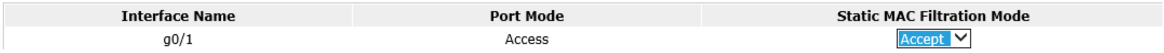
Click "Detail" and then you can conduct the binding of the source MAC address for each physical port. In this way, the MAC address that is allowed to visit the port will be limited.



	Serial number	Address	Operate
□	1	1234.1234.1234	Edit
□	2	1234.1234.1235	Edit

4.6.3 Setting the Static MAC Filtration Mode

Click **Port Config-> Port Security -> Static MAC Filtration Mode** in the navigation bar, the Configure the static MAC filtration mode page appears, as shown in the following figure.

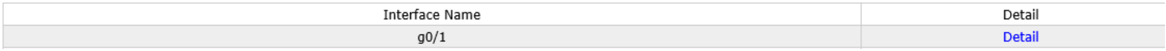


Interface Name	Port Mode	Static MAC Filtration Mode
g0/1	Access	Accept

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.

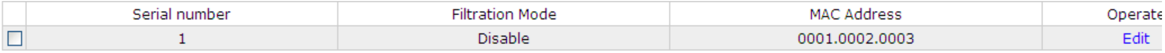
4.6.4 Static MAC Filtration Entries

Click **Port Config-> Port Security -> Static MAC Filtration Entries** in the navigation bar, the Setting the static MAC filtration entries page appears.



Interface Name	Detail
g0/1	Detail

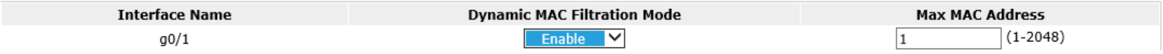
If you click "Detail", you can conduct the binding of the source MAC address for each physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.



	Serial number	Filtration Mode	MAC Address	Operate
□	1	Disable	0001.0002.0003	Edit

4.6.5 Setting the Dynamic MAC Filtration Mode

Click **Port Config-> Port Security -> Dynamic MAC Filtration Mode** in the navigation bar, the Configure the dynamic MAC filtration mode page appears, as shown in the following figure.



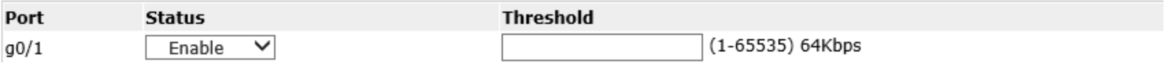
Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
g0/1	Enable	1 (1-2048)

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.

4.7 Storm Control

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

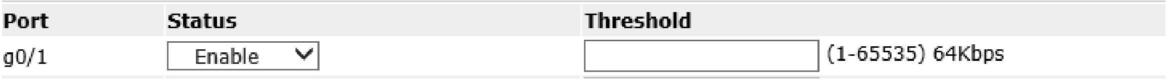
4.7.1 Broadcast storm control



Port	Status	Threshold
g0/1	Enable	(1-65535) 64Kbps

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

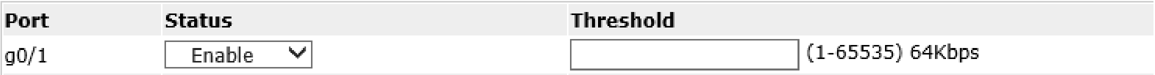
4.7.2 Multicast Storm Control



Port	Status	Threshold
g0/1	Enable	(1-65535) 64Kbps

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

4.7.3 Unknown Unicast Storm Control



Port	Status	Threshold
g0/1	Enable	(1-65535) 64Kbps

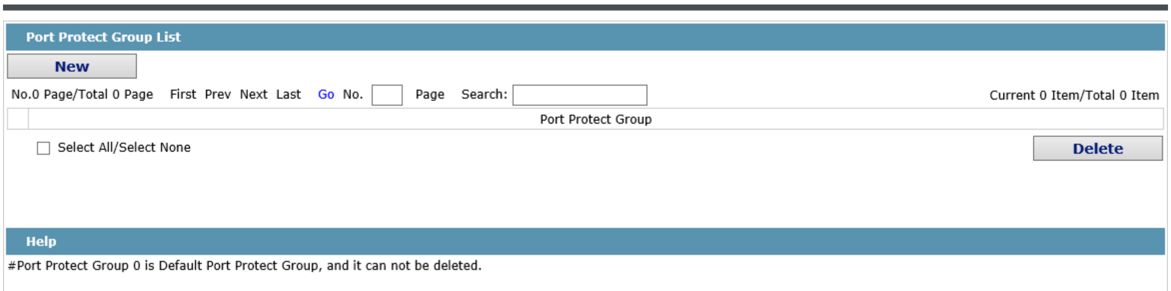
Through the “Status” dropdown box, you can decide whether to enable the unknown unicast storm limit on a port. In the Threshold column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.8 Port Protect Group Configuration

Click **Port Config-> Port Protect Group Config -> Port Protect Group List** in the navigation bar, the Port Protect Group List page appears.

4.8.1 Port Protect Group List

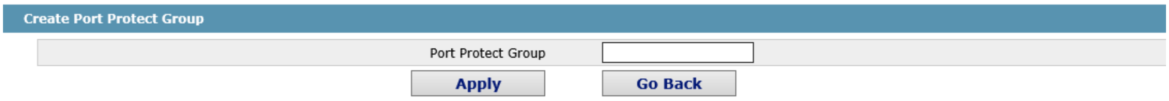
Click **Port Config-> Port Protect Group Config -> Port Protect Group List** in the navigation bar, the Port Protect Group List page appears.


Port Protect Group List
New
No.0 Page/Total 0 Page First Prev Next Last Go No. Page Search:
Current 0 Item/Total 0 Item
Port Protect Group
☐ Select All/Select None
Delete
Help

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

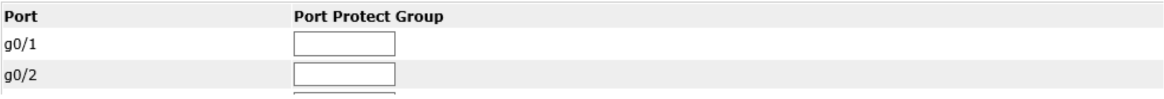
If you click New, a new port protect group will be created, as shown in the following figure.

If you tick a Port Protect Group, you can delete it. The port protect group 0 is by default, which cannot be deleted.



4.8.2 Port Protect Group Interface Configuration

Click **Port Config-> Port Protect Group Config -> Port Protect Group Interface Config** in the navigation bar, the Port Protect Group Config page appears.



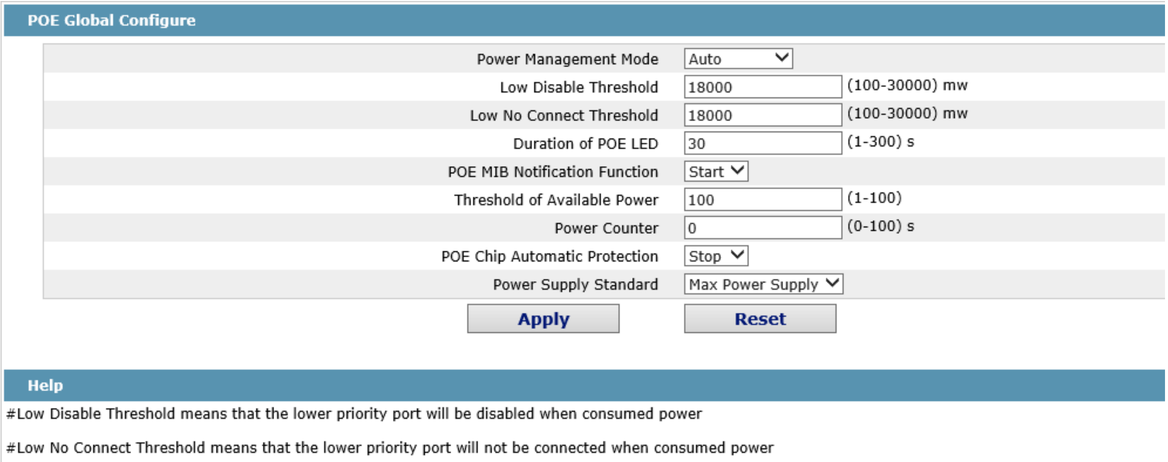
Port	Port Protect Group
g0/1	
g0/2	

The port protect group must be a created group. If one port has configured the default protect group, others ports can only configure the default groups.

4.9 POE Management

4.9.1 POE Global Configuration

If you click **Port Config -> POE Mgr** in the navigation bar, the POE management configuration page appears, as shown in the following figure.



POE Global Configure

Power Management Mode	Auto	
Low Disable Threshold	18000	(100-30000) mw
Low No Connect Threshold	18000	(100-30000) mw
Duration of POE LED	30	(1-300) s
POE MIB Notification Function	Start	
Threshold of Available Power	100	(1-100)
Power Counter	0	(0-100) s
POE Chip Automatic Protection	Stop	
Power Supply Standard	Max Power Supply	

Help

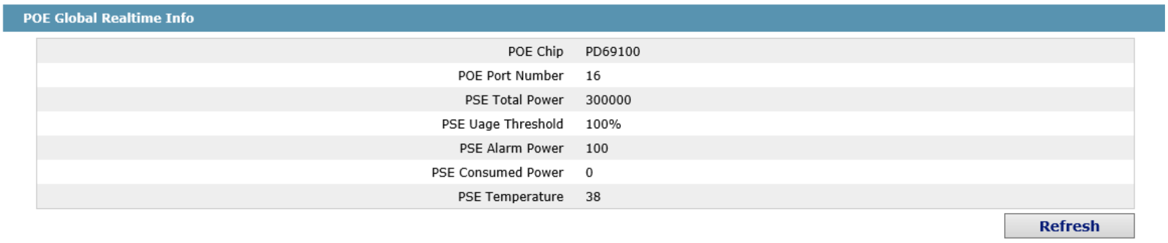
#Low Disable Threshold means that the lower priority port will be disabled when consumed power

#Low No Connect Threshold means that the lower priority port will not be connected when consumed power

On this page, you can configure the POE power supply management mode, lower priority upgrade preemption threshold, enable/disable POE MIB inform.

4.9.2 POE Global Realtime Info

Click **Port Config -> POE Mgr->POE Global Realtime Info** in the navigation bar, the POE management configuration page appears, as shown in the following figure.



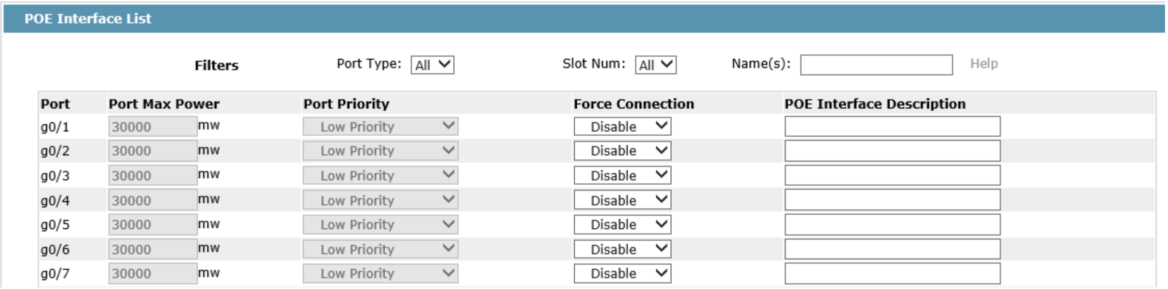
POE Global Realtime Info

POE Chip	PD69100
POE Port Number	16
PSE Total Power	300000
PSE Uage Threshold	100%
PSE Alarm Power	100
PSE Consumed Power	0
PSE Temperature	38

On this page, you can check POE port number, PSE power and PSE temperature.

4.9.3 POE Interface List

Click **Port Config -> POE Mgr->POE Interface List** in the navigation bar, the POE management configuration page appears, as shown in the following figure.



POE Interface List

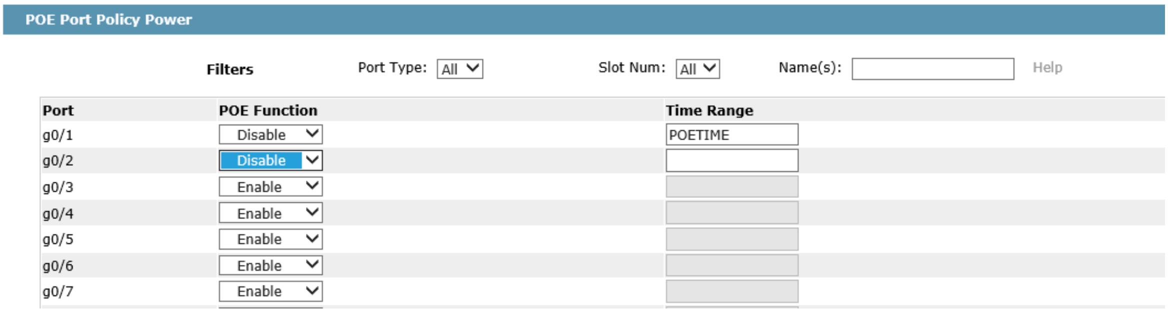
Filters Port Type: All Slot Num: All Name(s):

Port	Port Max Power	Port Priority	Force Connection	POE Interface Description
g0/1	30000 mw	Low Priority	Disable	
g0/2	30000 mw	Low Priority	Disable	
g0/3	30000 mw	Low Priority	Disable	
g0/4	30000 mw	Low Priority	Disable	
g0/5	30000 mw	Low Priority	Disable	
g0/6	30000 mw	Low Priority	Disable	
g0/7	30000 mw	Low Priority	Disable	

On this page, youc can configure the Port Priority, Port Max Power, Force Connection and POE Interface Description.

4.9.4 POE Port Policy Power

Click Port Config -> POE Mgr->POE Port Policy Power in the navigation bar, the POE Port Policy Power configuration page appears, as shown in the following figure.



POE Port Policy Power

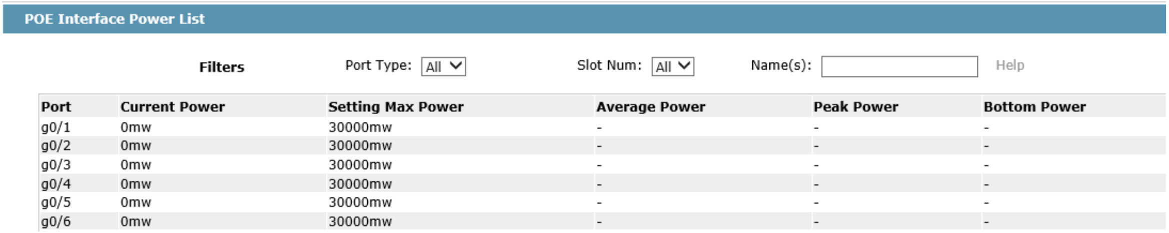
Filters Port Type: All Slot Num: All Name(s): Help

Port	POE Function	Time Range
g0/1	Disable	POETIME
g0/2	Disable	
g0/3	Enable	
g0/4	Enable	
g0/5	Enable	
g0/6	Enable	
g0/7	Enable	

On this page, you can enable/disable POE Function and Time Range.

4.9.5 POE Interface Power List

Click **Port Config -> POE Mgr-> POE Port Policy Power** in the navigation bar, the POE Port Policy Power configuration page appears, as shown in the following figure.



POE Interface Power List

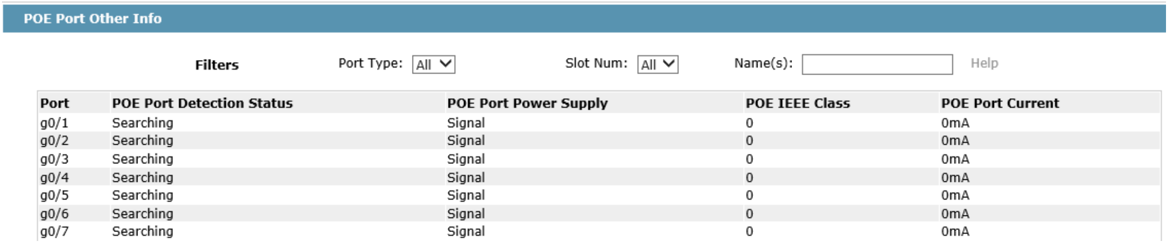
Filters Port Type: All Slot Num: All Name(s): Help

Port	Current Power	Setting Max Power	Average Power	Peak Power	Bottom Power
g0/1	0mw	30000mw	-	-	-
g0/2	0mw	30000mw	-	-	-
g0/3	0mw	30000mw	-	-	-
g0/4	0mw	30000mw	-	-	-
g0/5	0mw	30000mw	-	-	-
g0/6	0mw	30000mw	-	-	-

On this page, you can check Current Power, Setting Max Power, Average Power, Peak Power and Bottom Power.

4.9.6 POE Port Other Info

Click **Port Config -> POE Mgr-> POE Port Other Info** in the navigation bar, the PPOE Port Other Info configuration page appears, as shown in the following figure.



POE Port Other Info

Filters Port Type: All Slot Num: All Name(s): Help

Port	POE Port Detection Status	POE Port Power Supply	POE IEEE Class	POE Port Current
g0/1	Searching	Signal	0	0mA
g0/2	Searching	Signal	0	0mA
g0/3	Searching	Signal	0	0mA
g0/4	Searching	Signal	0	0mA
g0/5	Searching	Signal	0	0mA
g0/6	Searching	Signal	0	0mA
g0/7	Searching	Signal	0	0mA

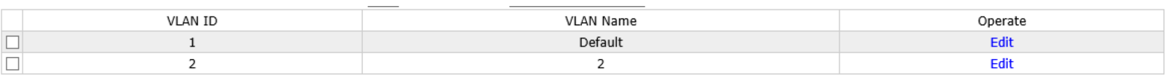
On this page, you can check POE Port Detection Status, POE Port Power Supply, POE IEEE Class, and POE Port Current.

Chapter 5 Layer-2 Configuration

5.1 VLAN Configuration

5.1.1 VLAN List

Click **Layer-2 Config -> VLAN Config** in the navigation bar, the VLAN Config page appears, as shown in the following figure.



	VLAN ID	VLAN Name	Operate
□	1	Default	Edit
□	2	2	Edit

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 “New” 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.

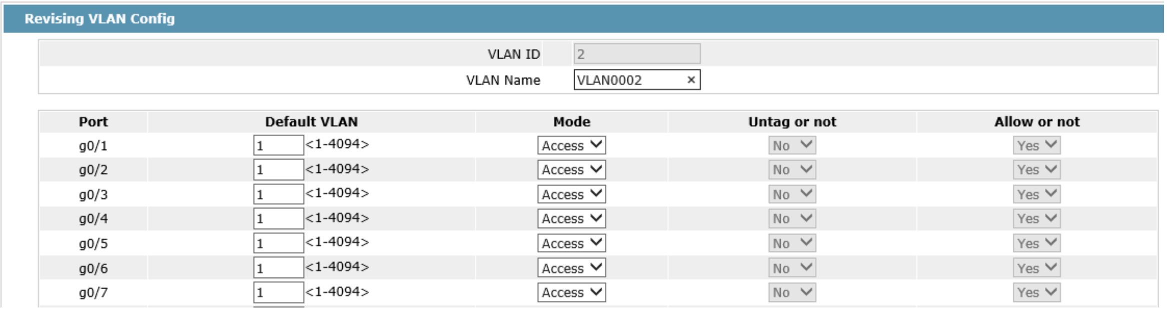
If you select the checkbox before a VLAN and then click “Delete”, the selected VLAN will be deleted.

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 http web max-vlan**” command to modify the maximum number of VLANs that will be displayed.

5.1.2 VLAN Configuration

If you click "New" 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.



Revising VLAN Config

VLAN ID: 2

VLAN Name: VLAN0002

Port	Default VLAN	Mode	Untag or not	Allow or not
g0/1	1 <1-4094>	Access	No	Yes
g0/2	1 <1-4094>	Access	No	Yes
g0/3	1 <1-4094>	Access	No	Yes
g0/4	1 <1-4094>	Access	No	Yes
g0/5	1 <1-4094>	Access	No	Yes
g0/6	1 <1-4094>	Access	No	Yes
g0/7	1 <1-4094>	Access	No	Yes

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

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

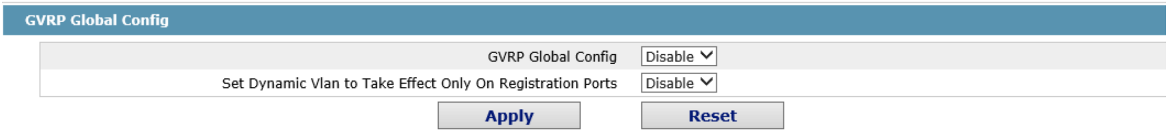
NOTE

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

5.2 GVRP Configuration

5.2.1 GVRP Global Attribute Configuration

Click **L2 Config -> GVRP Config -> GVRP Global Config** in the navigation bar, and enter GVRP global attribute configuration page.



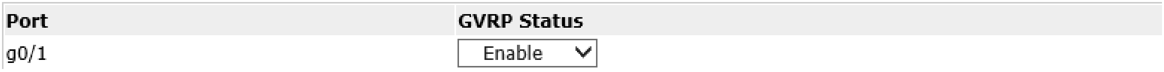
GVRP Global Config

GVRP Global Config	Disable
Set Dynamic Vlan to Take Effect Only On Registration Ports	Disable

You can enable or disable the global GVRP protocol, and set dynamic vlan to take effective or not only in the registered port.

5.2.2 GVRP Port Attribute Configuration

Click **L2 Config -> GVRP Config -> GVRP Interface Config** in the navigation bar and enter GVRP interface attribute configuration page.



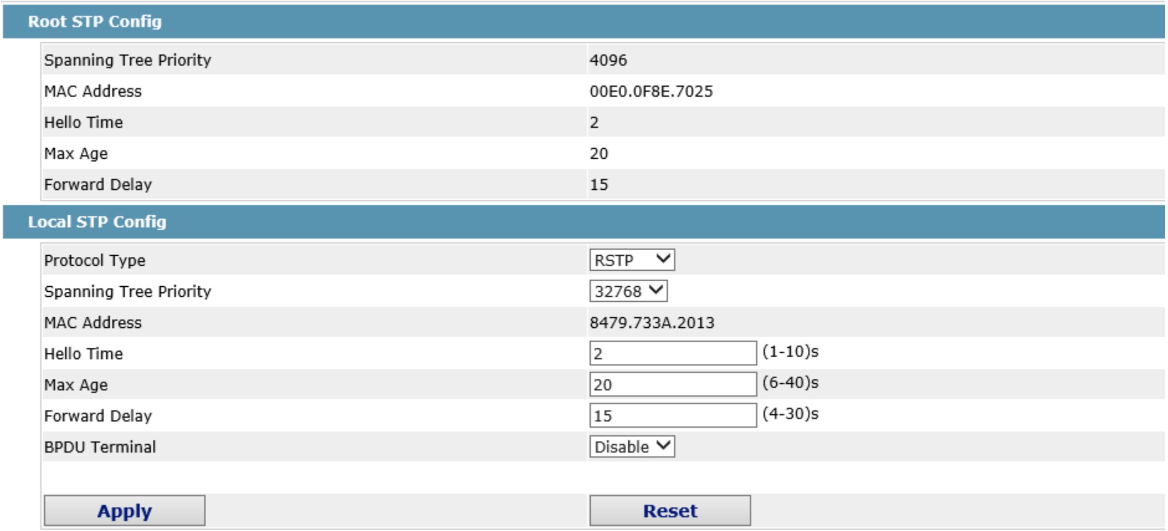
Port	GVRP Status
g0/1	Enable

GVRP interface configuration can enable or disable GVRP protocol of the port.

5.3 STP Configuration

5.3.1 STP Status Information

If you click **Advanced Config -> STP Config** in the navigation bar, the STP Config page appears, as shown in the following figure.



Root STP Config	
Spanning Tree Priority	4096
MAC Address	00E0.0F8E.7025
Hello Time	2
Max Age	20
Forward Delay	15

Local STP Config	
Protocol Type	RSTP
Spanning Tree Priority	32768
MAC Address	8479.733A.2013
Hello Time	2 (1-10)s
Max Age	20 (6-40)s
Forward Delay	15 (4-30)s
BPDU Terminal	Disable

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

Click the dropdown box on the right side of “Protocol” to change the currently running STP mode. The supported modes include STP, RSTP and Disabled STP.

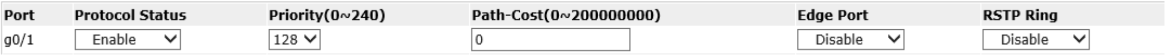
The priority and the time need be configured for different modes.

NOTE

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

5.3.2 Configuring the Attributes of the STP Port

If you click the "Configure RSTP Port" option, the “Configure RSTP Port” page appears.



Port	Protocol Status	Priority(0~240)	Path-Cost(0~200000000)	Edge Port	RSTP Ring
g0/1	Enable	128	0	Disable	Disable

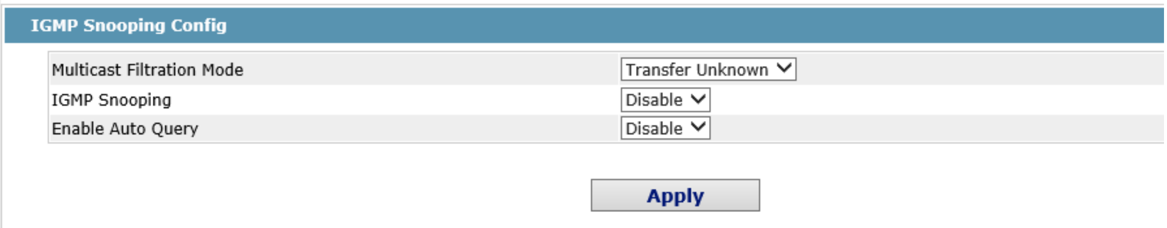
The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to “Disable” and the STP mode is also changed, the port will not run the protocol in the new mode.

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.

5.4 IGMP-Snooping Configuration

5.4.1 IGMP-Snooping Configuration

Click **L2 Config -> IGMP Snooping** in the navigation bar, and enter the IGMP-Snooping Configuration page.

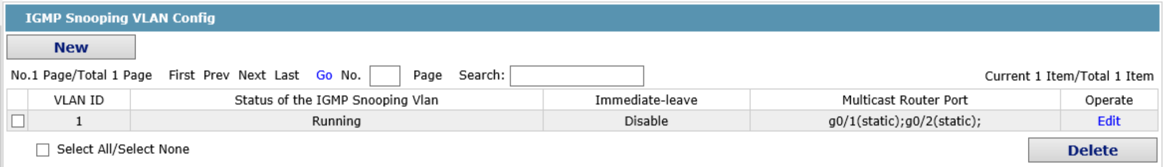

IGMP Snooping Config

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

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.

5.4.2 IGMP-Snooping VLAN List

In the navigation bar, click **L2 Config -> IGMP Snooping -> IGMP Snooping VLAN list** in the navigation bar, and enter IGMP-Snooping VLAN page.

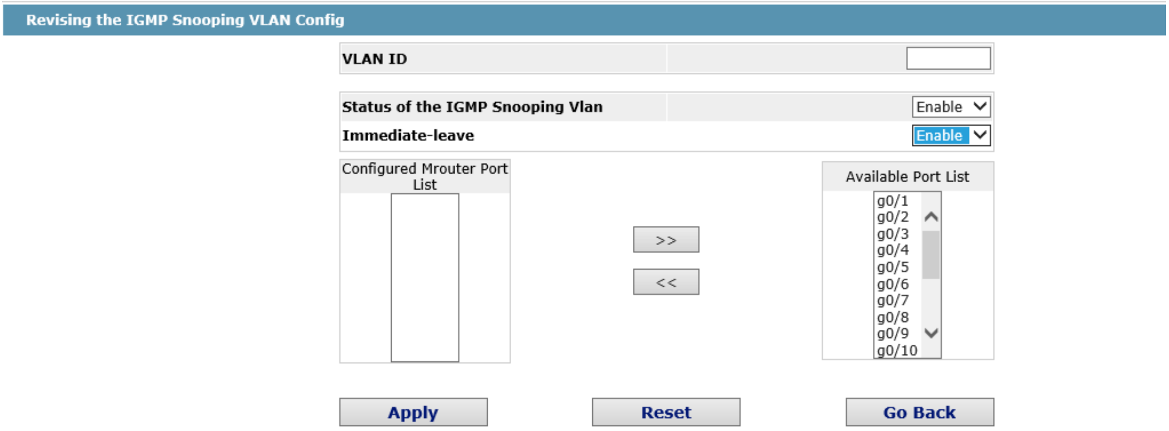

IGMP Snooping VLAN Config

New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item

	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router Port	Operate
□	1	Running	Disable	g0/1(static);g0/2(static);	Edit

□ Select All/Select None
Delete

If you click New, IGMP-snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP snooping VLAN. If you click Cancel, 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.


Revising the IGMP Snooping VLAN Config

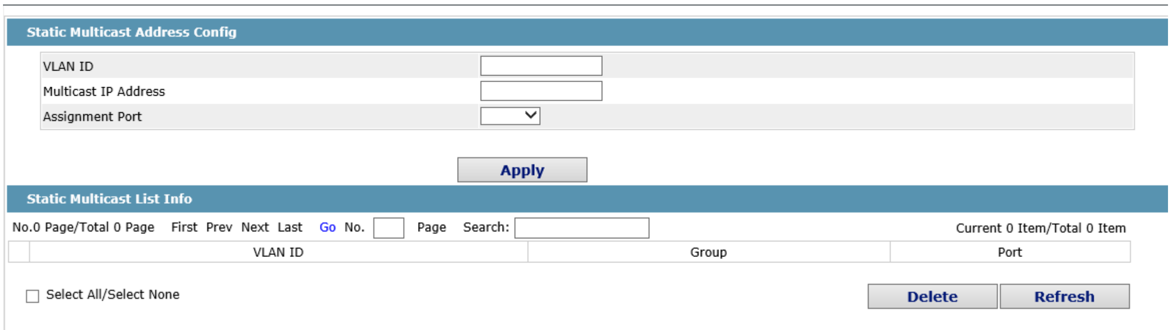
VLAN ID	
Status of the IGMP Snooping Vlan	Enable
Immediate-leave	Enable

When create new IGMP-Snooping Vlan, VLAN ID can be modified; when modify IGMP-Snooping Vlan, VLAN ID cannot be modified.

You can add or delete the routing port by buttons “>>” or “<<”.

5.4.3 Static Multicast Address

Click **L2 Config -> IGMP Snooping > Static Multicast Address List** in the navigation bar, and enter static multicast address configuration page.



Static Multicast Address Config

VLAN ID

Multicast IP Address

Assignment Port

Static Multicast List Info

No.0 Page/Total 0 Page First Prev Next Last Go No. Page Search: Current 0 Item/Total 0 Item

	VLAN ID	Group	Port

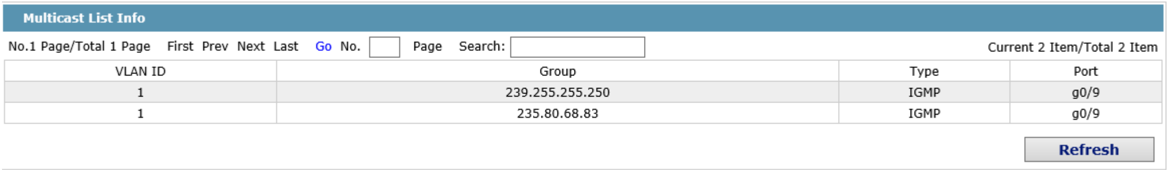
□ Select All/Select None

This page displays the static multicast group in current network according to IGMP-Snooping statistics and the port set each member belongs to.

Click “Refresh” to refresh the contents in the list.

5.4.4 Multicast List

Click the Multicast List Info option on the top of the page and the Multicast List Info page appears.



Multicast List Info

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 2 Item/Total 2 Item

VLAN ID	Group	Type	Port
1	239.255.255.250	IGMP	g0/9
1	235.80.68.83	IGMP	g0/9

On this page the multicat 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 dislayed.

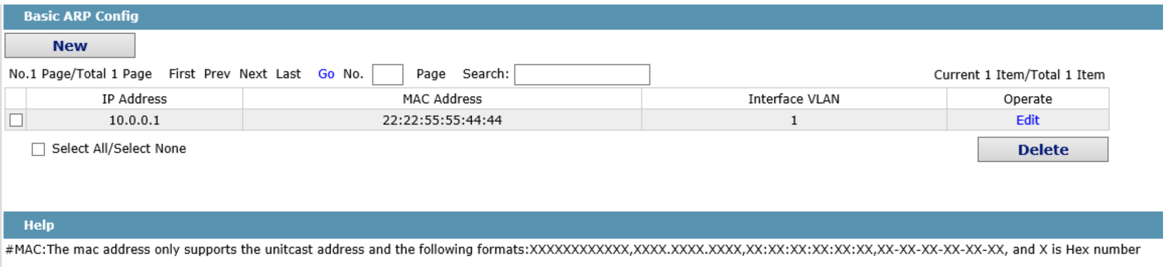
Click “Refresh” to refresh the contents in the list.

NOTE

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

5.5 Setting Static ARP

Step 1 Click **L2 Config -> Static ARP** in the navigation bar, and enter the basic ARP configuration page.


Basic ARP Config
New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item
Delete
Help

	IP Address	MAC Address	Interface VLAN	Operate
☐	10.0.0.1	22:22:55:55:44:44	1	Edit

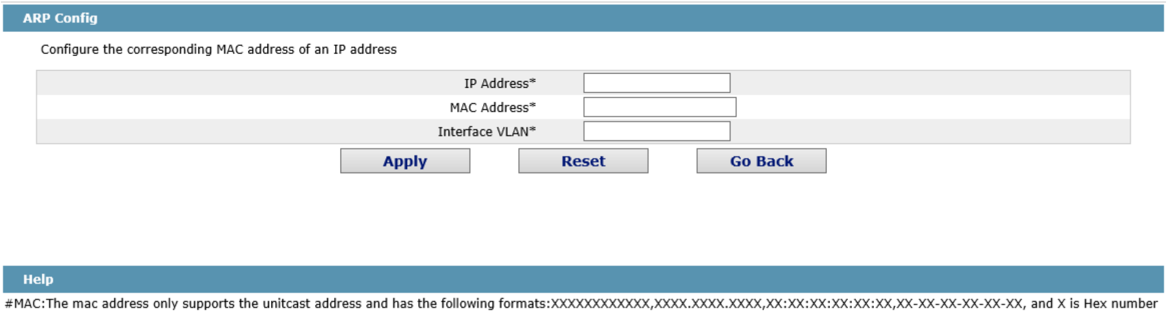
☐ Select All/Select None

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

Step 2 Click “New” to add ARP entry. The VLAN interface needs to be assigned when configuring the ARP entry.

Step 3 Click “Modify” to modify the current ARP entry.

Step 4 Click “Delete” to delete the selected ARP entry.



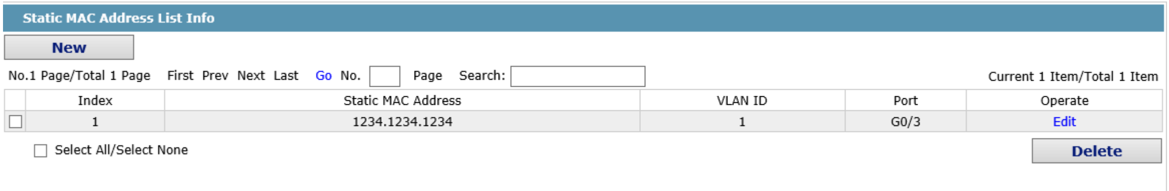
Configure the corresponding MAC address of an IP address

IP Address*	
MAC Address*	
Interface VLAN*	

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

5.6 Static MAC Configuration

Step 1 Click **L2 Config > Static MAC Config** in the navigation bar, and enter static MAC address configuration page.


Static MAC Address List Info
New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item
Delete

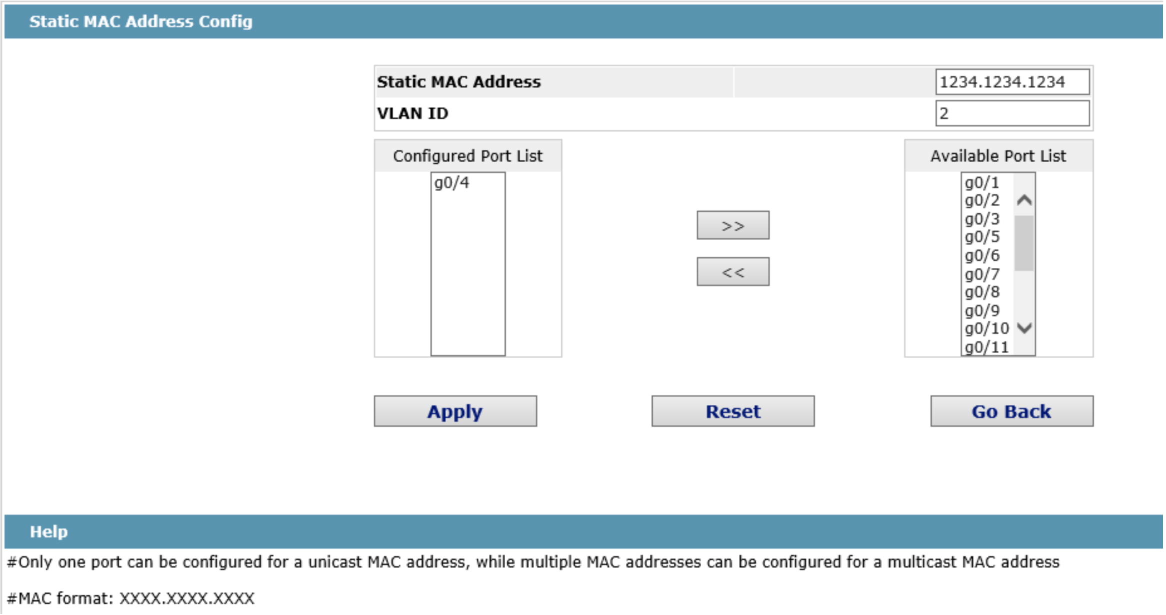
	Index	Static MAC Address	VLAN ID	Port	Operate
☐	1	1234.1234.1234	1	G0/3	Edit

☐ Select All/Select None

Step 2 Click “New” to configure static MAC address and VLAN for the assigned port. The unicast MAC address can only be configured with one port and the multicast MAC address can be configured with multiple ports.

Step 3 Click “Modify” to modify the configured static MAC address.

Step 4 Click “Delete” to delete the static MAC address entry.



Static MAC Address Config

Static MAC Address	1234.1234.1234
VLAN ID	2

Configured Port List: g0/4

Available Port List: g0/1, g0/2, g0/3, g0/5, g0/6, g0/7, g0/8, g0/9, g0/10, g0/11

Help

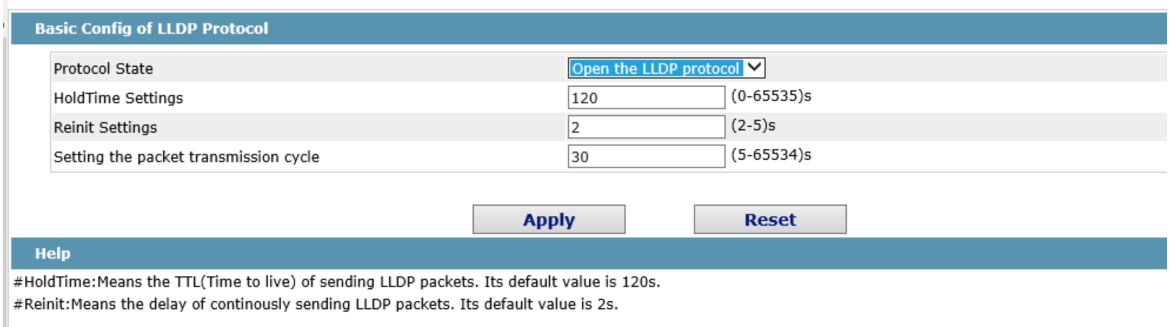
#Only one port can be configured for a unicast MAC address, while multiple MAC addresses can be configured for a multicast MAC address

#MAC format: XXXX.XXXX.XXXX

5.7 LLDP Configuration

5.7.1 Configuring the Global Attributes of LLDP

If you click **Layer-2 Config -> LLDP Config** in the navigation bar, the Global LLDP Config page appears, as shown in the following.



Basic Config of LLDP Protocol

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

Help

#HoldTime:Means the TTL(Time to live) of sending LLDP packets. Its default value is 120s.
#Reinit:Means the delay of continously sending LLDP packets. Its default value is 2s.

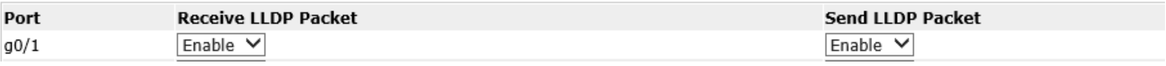
You can choose to enable LLDP or disable it. When you choose to disable LLDP, you cannot configure LLDP.

The “HoldTime” parameter refers to the ttl value of the packet that is transmitted by LLDP, whose default value is 120s.

The “Reinit” parameter refers to the delay of successive packet transmission of LLDP, whose default value is 2s.

5.7.2 Configuring the Attributes of the LLDP Port

If you click **Layer-2 Config -> LLDP Config-> LLDP Port Config** in the navigation bar, the Setting the attributes of the LLDP port page appears, as shown in the following figure.

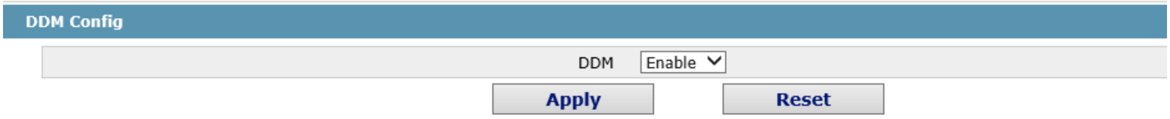


Port	Receive LLDP Packet	Send LLDP Packet
g0/1	Enable	Enable

LLDP interface configuration can enable or disable the port transmitting LLDP packets.

5.8 DDM Configuration

Click **L2 Config > DDM Config** in the navigation bar, and enter DDM configuration page.



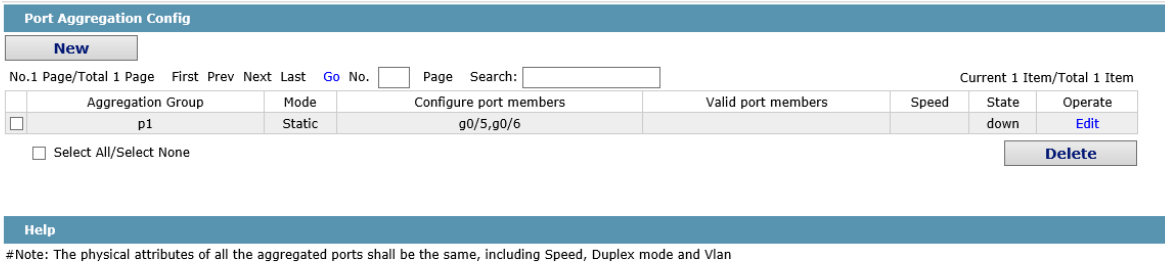
DDM Config

DDM: Enable

5.9 Link Aggregation Configuration

5.9.1 Port Aggregation Configuration

Click **Advanced Config -> Link Aggregation Config** in the navigation bar, the Link aggregation Config page appears, as shown in the following figure.



Port Aggregation Config

New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item

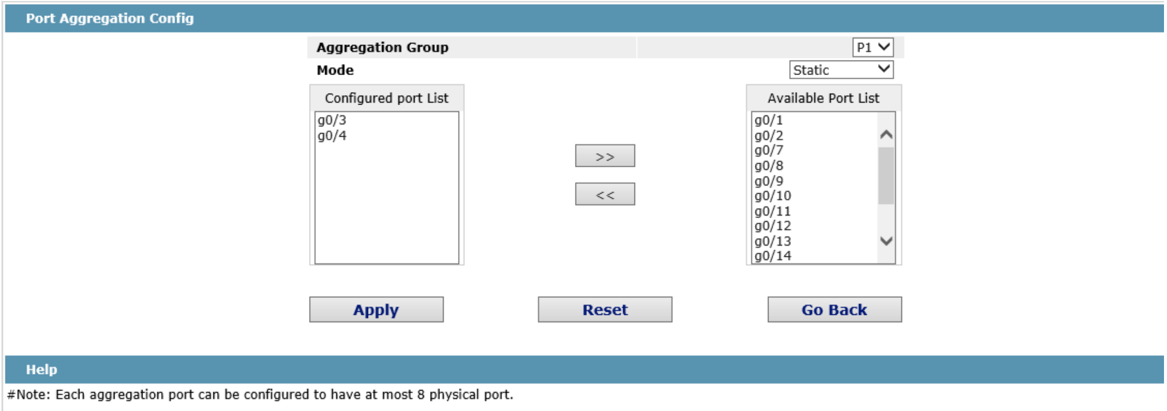
	Aggregation Group	Mode	Configure port members	Valid port members	Speed	State	Operate
□	p1	Static	g0/5,g0/6			down	Edit

□ Select All/Select None
Delete

Help

#Note: The physical attributes of all the aggregated ports shall be the same, including Speed, Duplex mode and Vlan

If you click New, an aggregation group can be created. Up to 32 aggregation groups can be configured through Web and up to 8 physical ports in each group can be aggregated. If you click Cancel, you can delete a selected aggregation group; if you click Modify, you can modify the member port and the aggregation mode.



Port Aggregation Config

Aggregation Group: P1

Mode: Static

Configured port List: g0/3, g0/4

Available Port List: g0/1, g0/2, g0/7, g0/8, g0/9, g0/10, g0/11, g0/12, g0/13, g0/14

Help

#Note: Each aggregation port can be configured to have at most 8 physical port.

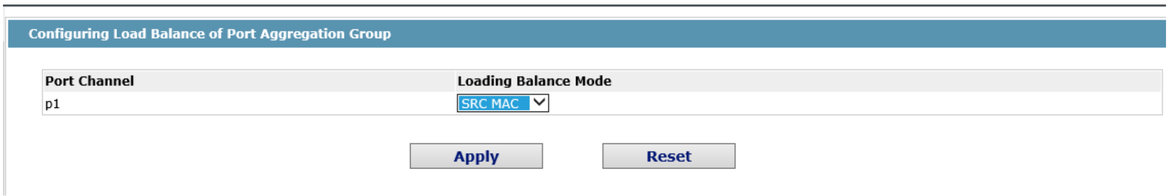
An aggregation group is selectable when it is created but is not selectable when it is modified.

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

You can click >> and << to delete and add a member port in the aggregation group.

5.9.2 Configuring Load Balance of Port Aggregation Group

Some models support aggregation group based load balance mode configuration and some not but can be configured in the global configuration mode.



Configuring Load Balance of Port Aggregation Group

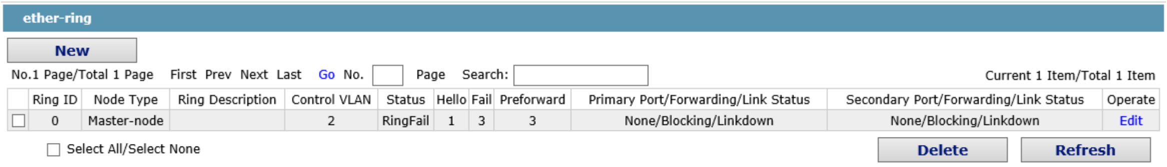
Port Channel	Loading Balance Mode
p1	SRC MAC

You can select link aggregation load balance mode and click "Apply" to apply it.

5.10 EAPS Ring Protection Configuration

5.10.1 EAPS Ring List

Step 1 Click Layer-2 Config -> Ring Protection ->EAPS Config, the EAPS Ring Config page appears.



ether-ring

New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item

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

□ Select All/Select None
Delete
Refresh

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

Step 2 Click “New” to create a new EAPS ring.

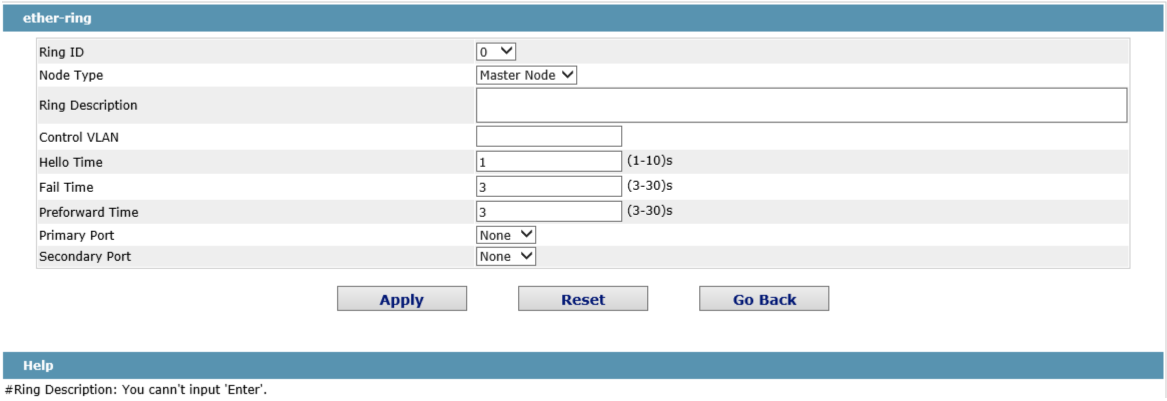
Step 3 Click the “Operate” option to configure the “Time” parameter of the ring.

NOTE

- 1. The system can support 8 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.

5.10.2 EAPS Ring Configuration

Click “New” on the EAPS ring list, or “Operate” on the right side of a ring item, the “Configure EAPS” page appears.



ether-ring

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

#Ring Description: You cann't input 'Enter'.

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.

The dropdown box on the right of “Node Type” is used to select the type of the node. Please note that only one master node can be configured on a ring.

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 same as that of another ring.

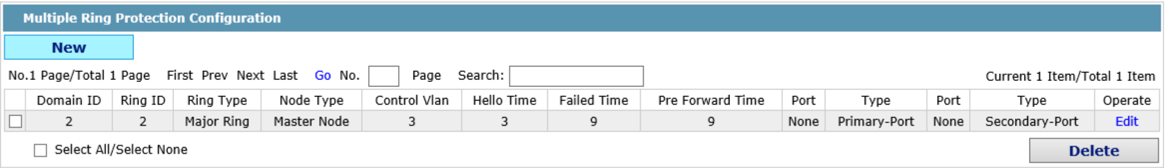
In the text boxes of “Primary Port” and “Secondary Port”, select a port as the ring port respectively. If "Node Type" is selected as “Transit-Node”, the two ports will be automatically set to transit ports.

Click “Apply” to finish EAPS ring configuration, click “Reset” to resume the initial values of the configuration, or click “Return” to go back to the EAPS list page.

5.11 MEAPS Configuration

5.11.1 MEAPS Ring Configuration

Step 1 Click **Layer-2 Config -> Multiple Ring Protection -> Multiple Ring Protection** on the navigation bar, the Multiple Ring Protection Configuration page appears.



Multiple Ring Protection Configuration

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

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

□ Select All/Select None

Delete

The list shows the current configured MEAPS ring, including Domain ID, Ring ID, Ring type, Node type, Control Vlan, Hello Time, Failed Time, Pre Forward Time, primary port and secondary port.

Step 2 Click “New” to create a MEAPS ring.

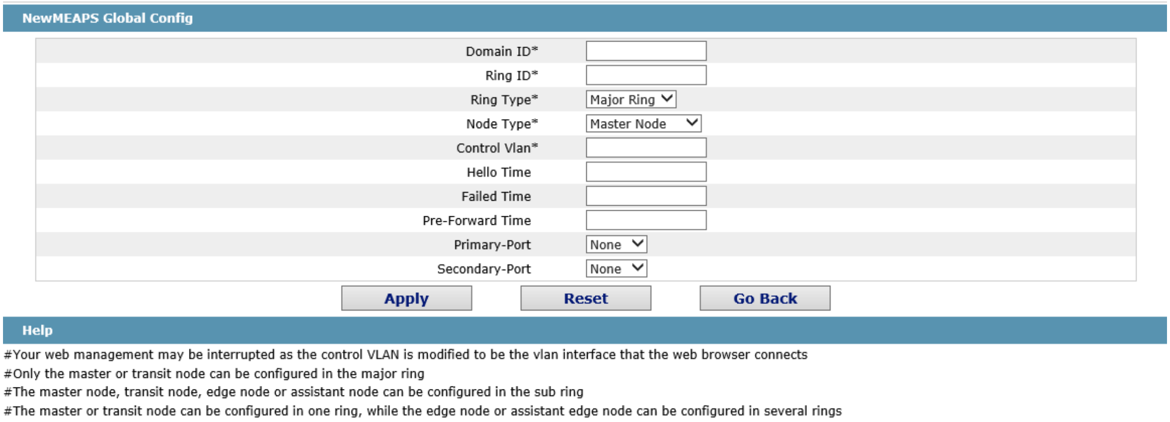
Step 3 Click “Edit” on the right and configure the time parameter and the primary and secondary port of the ring.

NOTE

- The system supports 4 MEAPS (0-3).
- One domain supports 8 rings (0-7).
- Once one MEAPS is configured, its Domain ID, ring ID, ring type, node type and control Vlan cannot be modified. If adjustment is needed, please delete the Ethernet ring and reset it.

5.11.2 MEAPS Ring Configuration

If you click New on the Multiple Ring Protection page or click Edit on the right, the New MEAPS Global Config page appears.



NewMEAPS Global Config

Domain ID*	
Ring ID*	
Ring Type*	Major Ring
Node Type*	Master Node
Control Vlan*	
Hello Time	
Failed Time	
Pre-Forward Time	
Primary-Port	None
Secondary-Port	None

Apply Reset Go Back

Help

#Your web management may be interrupted as the control VLAN is modified to be the vlan interface that the web browser connects
#Only the master or transit node can be configured in the major ring
#The master node, transit node, edge node or assistant node can be configured in the sub ring
#The master or transit node can be configured in one ring, while the edge node or assistant edge node can be configured in several rings

NOTE

In an existed MEAPS ring, its domain ID, ring ID, ring type, node type and control Vlan cannot be modified.

The primary ring can only be configured with the main node and the Transit node.

The secondary ring can be configured with the main node, the transit node, the edge node and the assistant edge node.

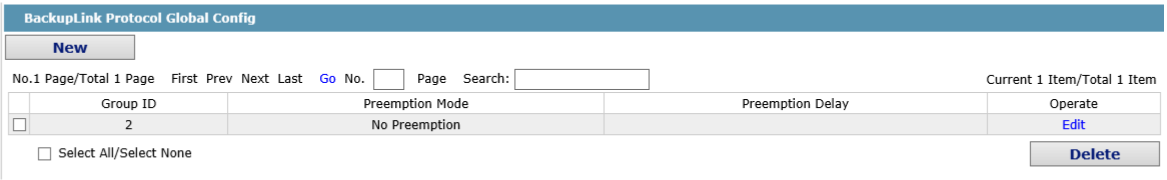
The primary node and the transit node can only be existed in one ring. The edge node and the assistant edge node can be existed in multiple rings simultaneously.

On the right drop box of “Primary-Port” and “Secondary-Port”, select one port respectively as the ring port or select None.

5.12 Backup Link Protocol Configuration

5.12.1 Backup Link Protocol Global Configuration

Step 1 Click **Layer-2 Config ->Backup Link Config ->Backup Link Protocol Global Config** on the navigation bar, the Backup Link Protocol Global Config page appears.

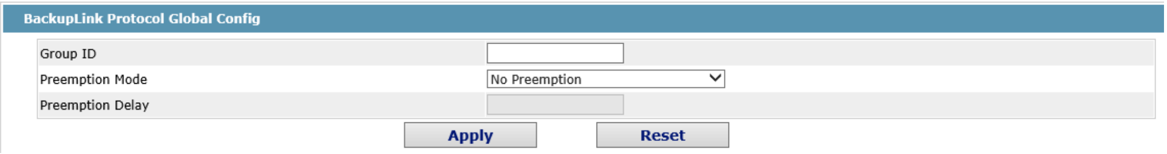

BackupLink Protocol Global Config
New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item
Select All/Select None
Delete

	Group ID	Preemption Mode	Preemption Delay	Operate
□	2	No Preemption		Edit

On the page, the current configured backup link groups are shown, including Preemption Mode and Preemption Delay.

Step 2 Click New to create a new link backup group.

Step 3 Click Edit on the right to configure Preemption Mode and Preemption Delay.



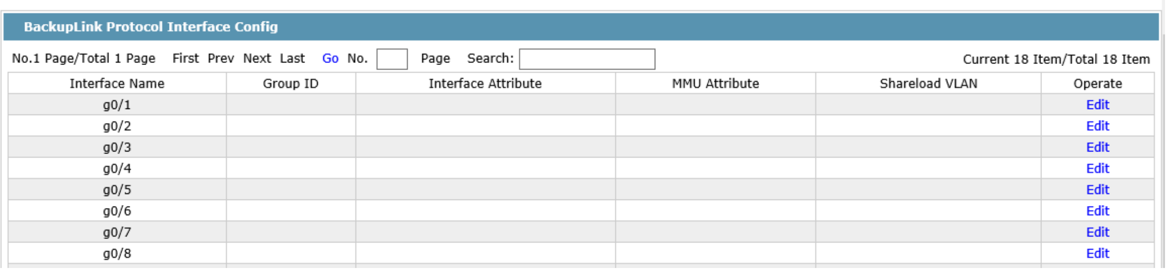
Group ID	
Preemption Mode	No Preemption
Preemption Delay	

NOTE

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

5.12.2 Backup Link Protocol Interface Configuration

Step 1 Click Layer-2 Config -> Backup Link Protocol Config -> Backup Link Protocol Interface Config on the navigation bar, the Backup Link Protocol Global Config page appears.



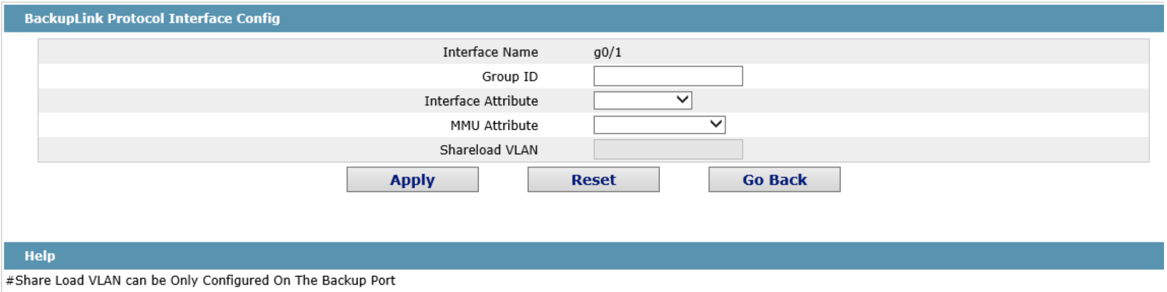
BackupLink Protocol Interface Config

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 18 Item/Total 18 Item

Interface Name	Group ID	Interface Attribute	MMU Attribute	Shareload VLAN	Operate
g0/1					Edit
g0/2					Edit
g0/3					Edit
g0/4					Edit
g0/5					Edit
g0/6					Edit
g0/7					Edit
g0/8					Edit

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

Step 2 Click Edit on the right to configure the Backup Link Protocol.



BackupLink Protocol Interface Config

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

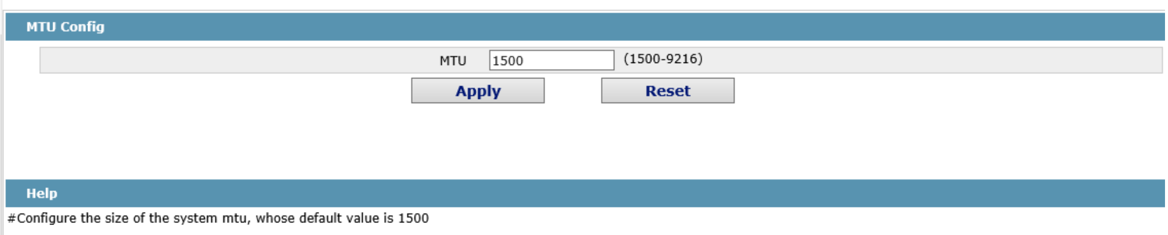
Help

#Share Load VLAN can be Only Configured On The Backup Port

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.

5.13 MTU Configuration

Click **Layer-2 Config -> MTU Config** on the navigation bar, the MTU Config page appears.



MTU Config

MTU 1500 (1500-9216)

Help

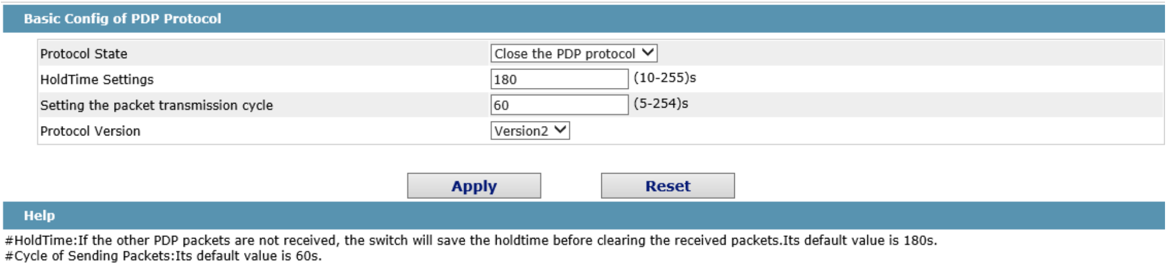
#Configure the size of the system mtu, whose default value is 1500

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

5.14 PDP Configuration

5.14.1 Configuring the Global Attributes of PDP

Click **Layer-2 Config -> PDP Config** in the navigation bar, the Global PDP Config page appears, as shown in the following figure.



Basic Config of PDP Protocol

Protocol State	Close the PDP protocol	
HoldTime Settings	180	(10-255)s
Setting the packet transmission cycle	60	(5-254)s
Protocol Version	Version2	

Help

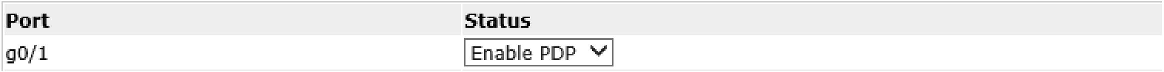
#HoldTime:If the other PDP packets are not received, the switch will save the holdtime before clearing the received packets.Its default value is 180s.
#Cycle of Sending Packets:Its default value is 60s.

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

The “HoldTime” parameter means the time to be saved before the router discards the received information if other PDP packets are not received.

5.14.2 Configuring the Attributes of the PDP Port

Click **Layer-2 Config -> PDP Config-> PDP Port Config** in the navigation bar, the Setting the attributes of the PDP port page appears, as shown in figure 5.



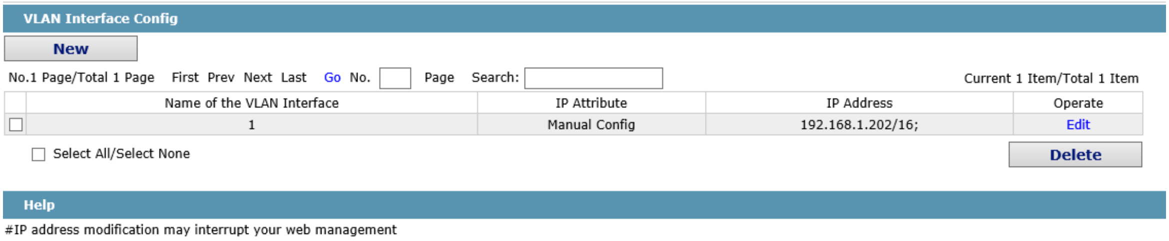
Port	Status
g0/1	Enable PDP

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

Chapter 6 Layer-3 Configuration

6.1 Vlan interface configuration

Click **L3 Config -> VLAN Interfaces and IP Addresses**, and enter the VLAN interface configuration page.



VLAN Interface Config

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

	Name of the VLAN Interface	IP Attribute	IP Address	Operate
□	1	Manual Config	192.168.1.202/16;	Edit

□ Select All/Select None

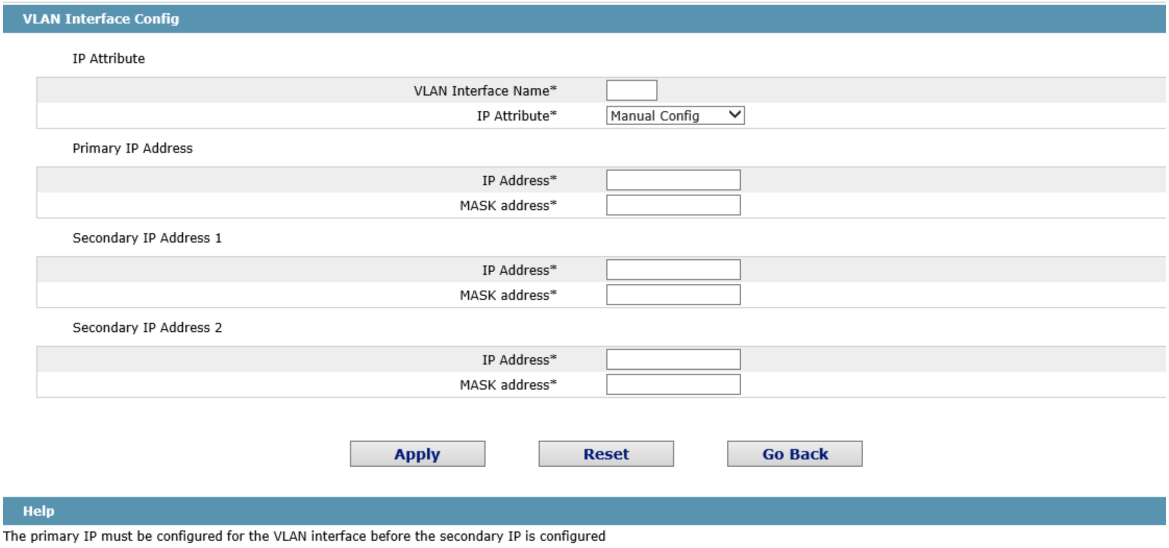
Delete

Help

#IP address modification may interrupt your web management

Click **New** to add a new VLAN interface. Click Cancel to delete a VLAN interface. Click Modify to modify the settings of a corresponding VLAN interface.

When you click New, the name of the corresponding VLAN interface can be modified; but if you click Modify, the name of the corresponding VLAN interface cannot be modified.



VLAN Interface Config

IP Attribute

VLAN Interface Name*	
IP Attribute*	Manual Config

Primary IP Address

IP Address*	
MASK address*	

Secondary IP Address 1

IP Address*	
MASK address*	

Secondary IP Address 2

IP Address*	
MASK address*	

Apply Reset Go Back

Help

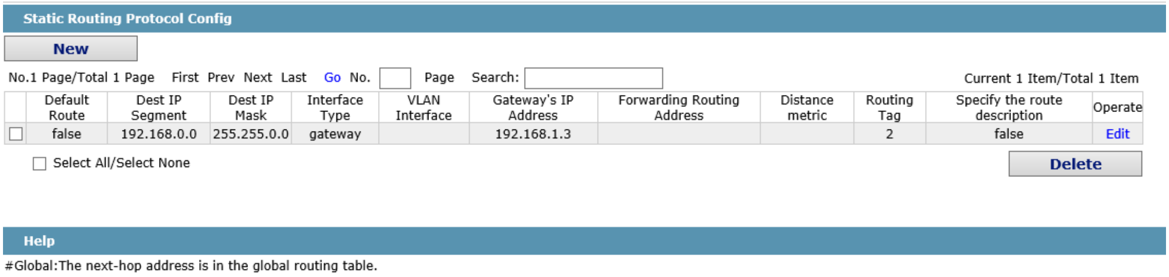
The primary IP must be configured for the VLAN interface before the secondary IP is configured

NOTE

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

6.2 Setting the Static Route

Click **Layer-3 Config -> Static Route Config**, the Static route configuration page appears.



Static Routing Protocol Config

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

	Default Route	Dest IP Segment	Dest IP Mask	Interface Type	VLAN Interface	Gateway's IP Address	Forwarding Routing Address	Distance metric	Routing Tag	Specify the route description	Operate
□	false	192.168.0.0	255.255.0.0	gateway		192.168.1.3			2	false	Edit

□ Select All/Select None

Delete

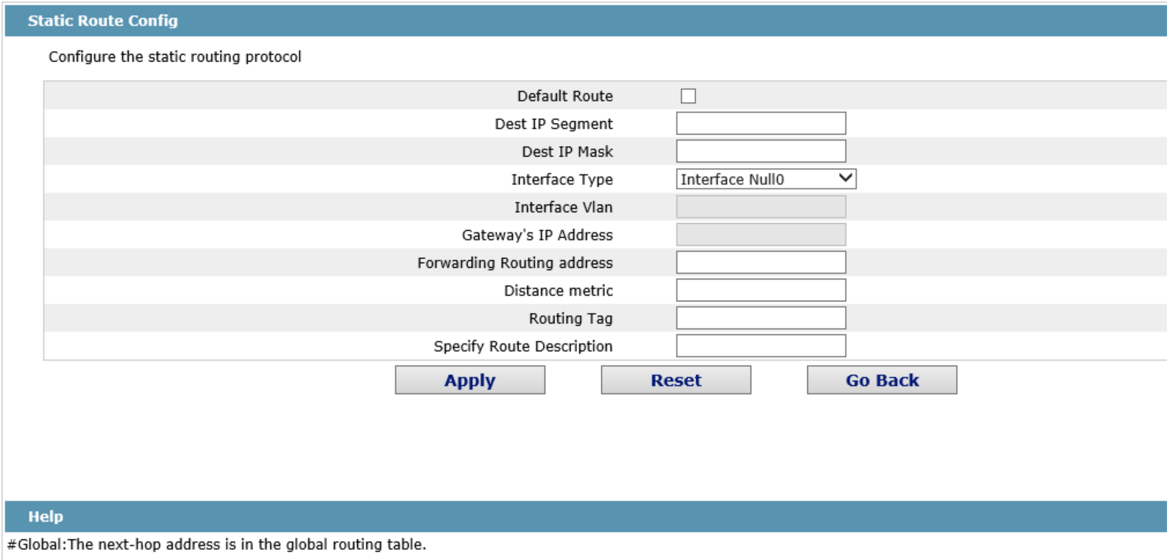
Help

#Global:The next-hop address is in the global routing table.

Click Create to add a static route.

If you click Edit, you can modify the current static route.

If you click Cancel, you can cancel the chosen static route.



Static Route Config

Configure the static routing protocol

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

Apply Reset Go Back

Help

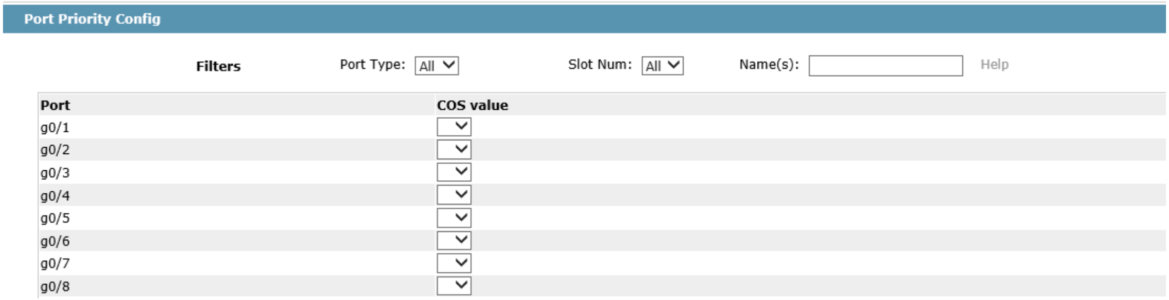
#Global:The next-hop address is in the global routing table.

Chapter 7 Advanced Configuration

7.1 QoS Configuration

7.1.1 Configuring QoS Port

Click **Advanced Config -> QoS -> Configure QoS Port**, the Port Priority Config page appears.



Port Priority Config

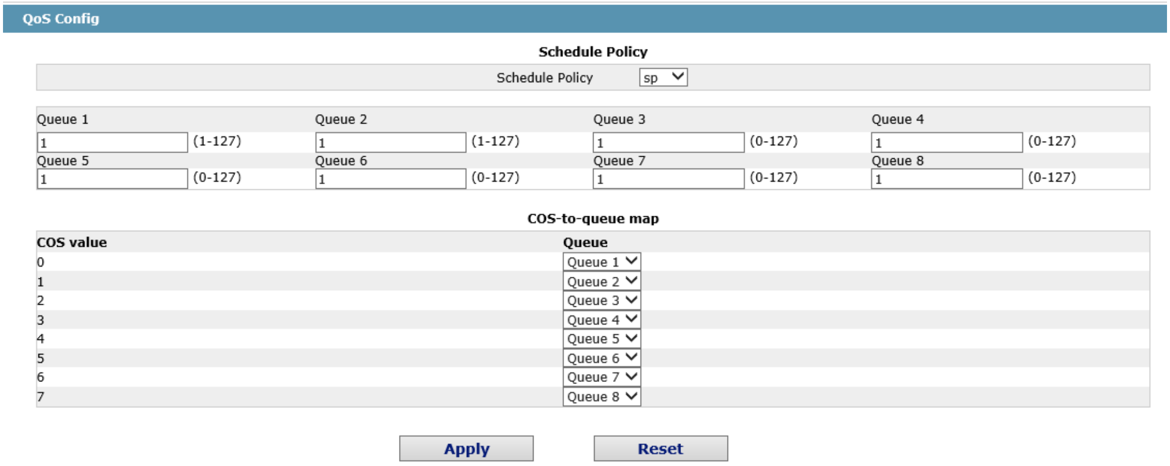
Filters Port Type: All Slot Num: All Name(s): Help

Port	COS value
g0/1	
g0/2	
g0/3	
g0/4	
g0/5	
g0/6	
g0/7	
g0/8	

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.

7.1.2 Global QoS Configuration

Click **Advanced Config -> QoS -> Configure QoS Port**, the Port Priority Config page appears.



QoS Config

Schedule Policy

Schedule Policy: sp

Queue 1		Queue 2		Queue 3		Queue 4	
1	(1-127)	1	(1-127)	1	(0-127)	1	(0-127)
Queue 5		Queue 6		Queue 7		Queue 8	
1	(0-127)	1	(0-127)	1	(0-127)	1	(0-127)

COS-to-queue map

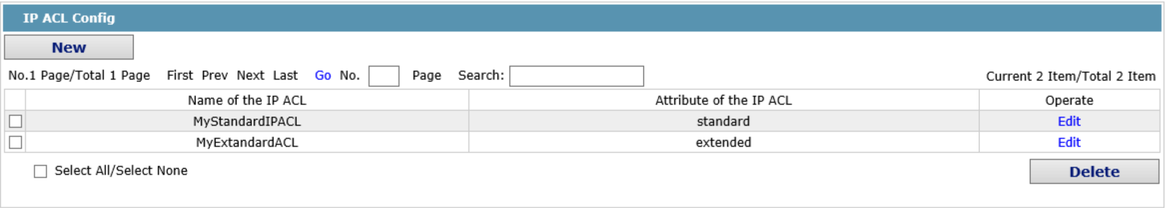
COS value	Queue
0	Queue 1
1	Queue 2
2	Queue 3
3	Queue 4
4	Queue 5
5	Queue 6
6	Queue 7
7	Queue 8

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

7.2 IP Access Control List

7.2.1 Setting the Name of the IP Access Control List

Click Advanced Config -> IP Access Control List -> IP Access Control List Config, the IP ACL configuration page appears.



IP ACL Config

New

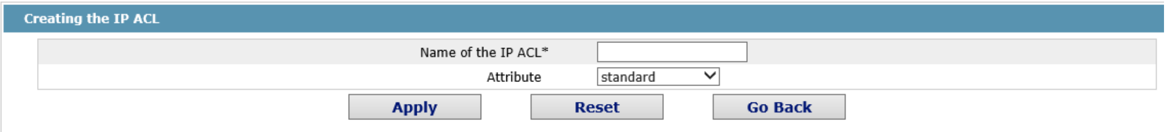
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 2 Item/Total 2 Item

	Name of the IP ACL	Attribute of the IP ACL	Operate
□	MyStandardIPACL	standard	Edit
□	MyExtandardACL	extended	Edit

□ Select All/Select None

Delete

Click New to add a name of the IP access control list. Click Cancel to delete an IP access control list.



Creating the IP ACL

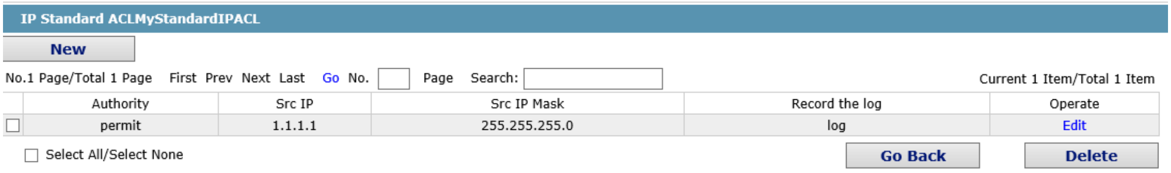
Name of the IP ACL*	
Attribute	standard

Apply Reset Go Back

If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

7.2.2 Setting the Rules of the IP Access Control List

- Standard IP access control list



IP Standard ACLMyStandardIPACL

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

	Authority	Src IP	Src IP Mask	Record the log	Operate
□	permit	1.1.1.1	255.255.255.0	log	Edit

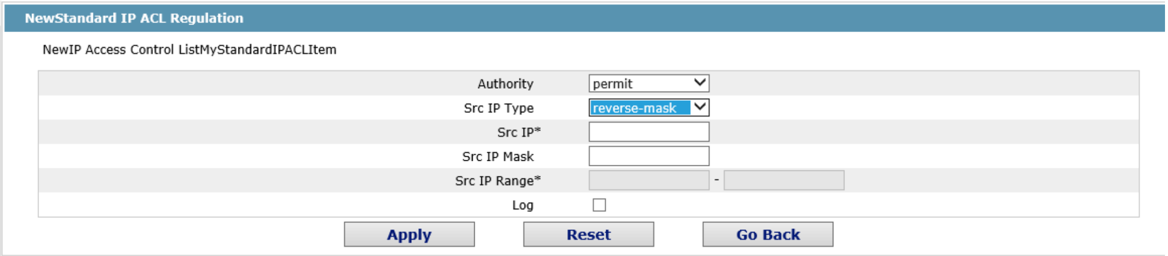
□ Select All/Select None

Go Back Delete

Click New to add a rule of the IP access control list.

Click Cancel to delete a rule of the IP access control list.

If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.



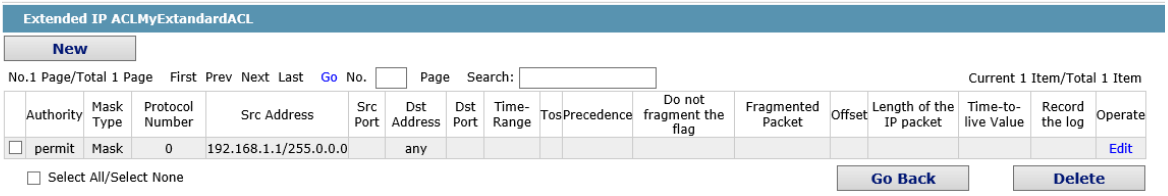
NewStandard IP ACL Regulation

NewIP Access Control ListMyStandardIPACLItem

Authority	permit
Src IP Type	reverse-mask
Src IP*	
Src IP Mask	
Src IP Range*	-
Log	□

Apply Reset Go Back

- Extended IP access control list



Extended IP ACLMyExtandardACL

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

	Authority	Mask Type	Protocol Number	Src Address	Src Port	Dst Address	Dst Port	Time-Range	Tos	Precedence	Do not fragment the flag	Fragmented Packet	Offset	Length of the IP packet	Time-to-live Value	Record the log	Operate
□	permit	Mask	0	192.168.1.1/255.0.0.0		any											Edit

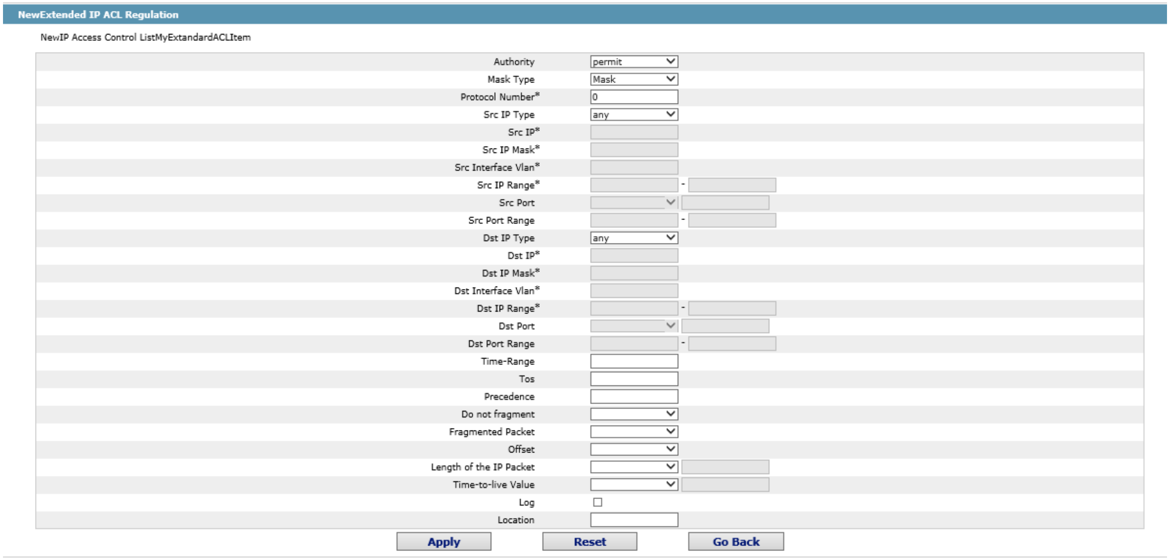
□ Select All/Select None

Go Back Delete

Click New to add a rule of the IP access control list.

Click Cancel to delete a rule of the IP access control list.

If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.



NewExtended IP ACL Regulation

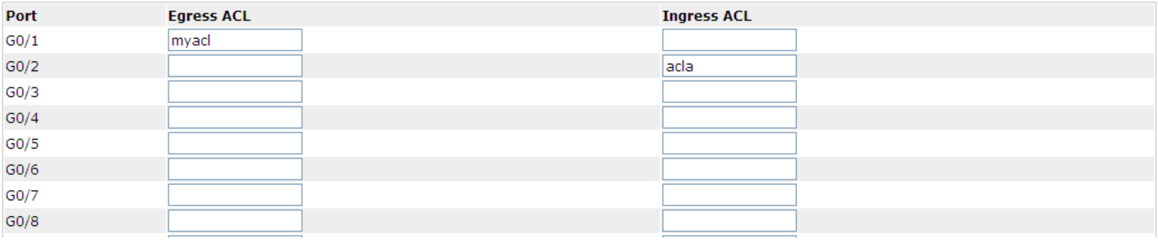
NewIP Access Control ListMyExtandardACLItem

Authority	permit
Mask Type	Mask
Protocol Number*	0
Src IP Type	any
Src IP*	
Src IP Mask*	
Src Interface Vlan*	
Src IP Range*	-
Src Port	
Src Port Range	-
Dst IP Type	any
Dst IP*	
Dst IP Mask*	
Dst Interface Vlan*	
Dst IP Range*	-
Dst Port	
Dst Port Range	-
Time-Range	
Tos	
Precedence	
Do not fragment	
Fragmented Packet	
Offset	
Length of the IP Packet	
Time-to-live Value	
Log	□
Location	

Apply Reset Go Back

7.2.3 Applying the IP Access Control List

Click Advanced Config -> IP Access Control List -> Applying the IP Access Control List, the Applying the IP access control list page appears.

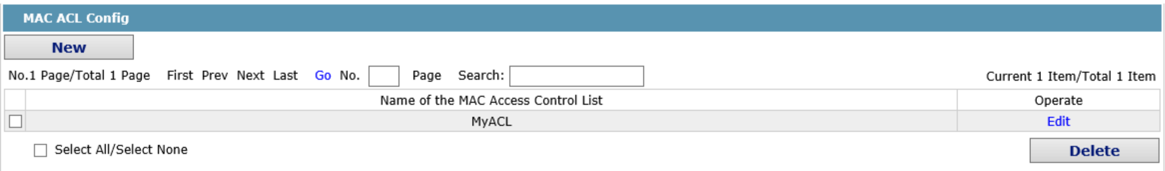


Port	Egress ACL	Ingress ACL
G0/1	myacl	
G0/2		acla
G0/3		
G0/4		
G0/5		
G0/6		
G0/7		
G0/8		

7.3 MAC Access Control List

7.3.1 Setting the Name of the IP Access Control List

Click Advanced Config -> MAC Access Control List -> MAC Access Control List Config, the MAC ACL configuration page appears.



MAC ACL Config

New

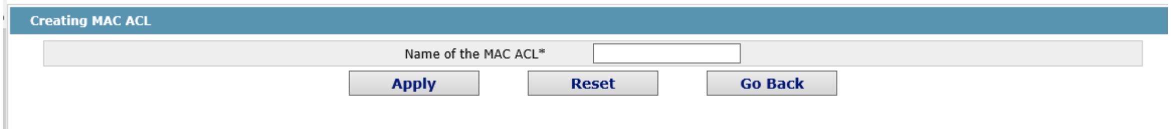
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

	Name of the MAC Access Control List	Operate
□	MyACL	Edit

□ Select All/Select None

Delete

Click New to add a name of the MAC access control list. Click Cancel to delete an IP access control list.



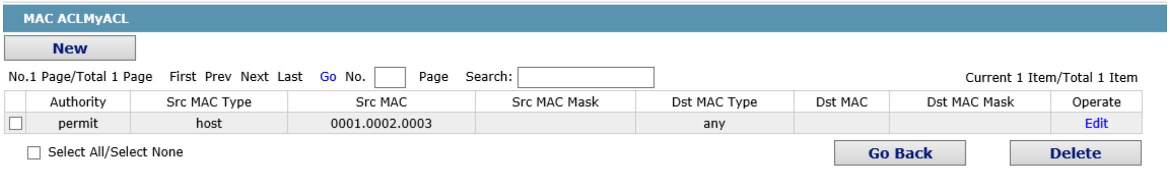
Creating MAC ACL

Name of the MAC ACL*

Apply Reset Go Back

7.3.2 Setting the Rules of the MAC Access Control List

If you click Modify, the corresponding MAC access control list appears and you can set the corresponding rules for the MAC access control list.



MAC ACLMyACL

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

	Authority	Src MAC Type	Src MAC	Src MAC Mask	Dst MAC Type	Dst MAC	Dst MAC Mask	Operate
□	permit	host	0001.0002.0003		any			Edit

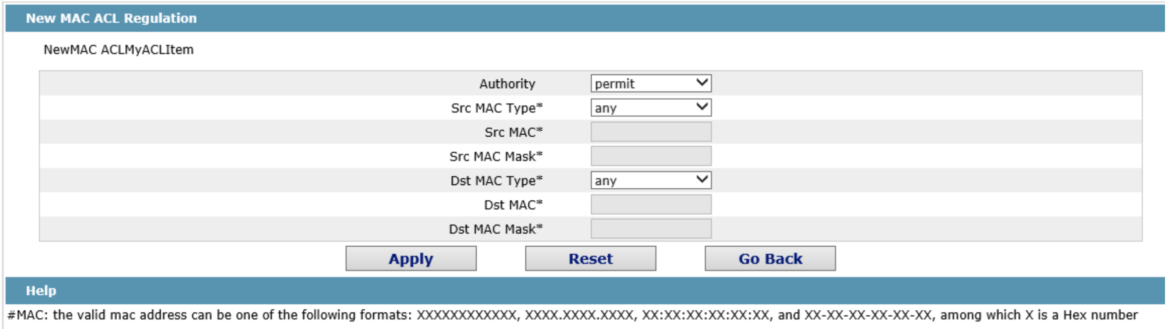
□ Select All/Select None

Go Back Delete

Click New to add a name of the MAC access control list.

Click Cancel to delete a rule of the IP access control list.

If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the MAC access control list.



New MAC ACL Regulation

NewMAC ACLMyACLItem

Authority	permit
Src MAC Type*	any
Src MAC*	
Src MAC Mask*	
Dst MAC Type*	any
Dst MAC*	
Dst MAC Mask*	

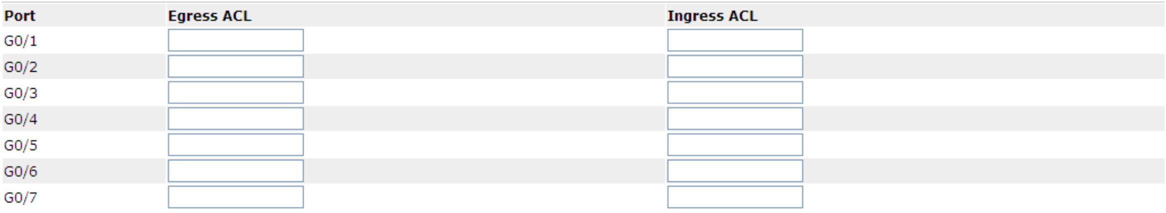
Apply Reset Go Back

Help

#MAC: the valid mac address can be one of the following formats: XXXXXXXXXXXX, XXXX.XXXX.XXXX, XX:XX:XX:XX:XX:XX, and XX-XX-XX-XX-XX-XX, among which X is a Hex number

7.3.3 Applying the MAC Access Control List

Click Advanced Config -> MAC Access Control List -> Applying The MAC Access Control List, the Applying the MAC access control list page appears.



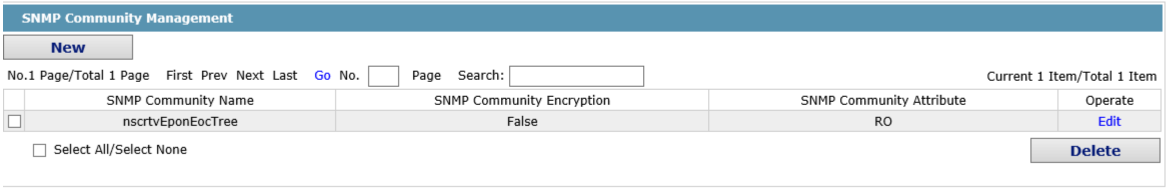
Port	Egress ACL	Ingress ACL
G0/1		
G0/2		
G0/3		
G0/4		
G0/5		
G0/6		
G0/7		

Chapter 8 Network Management Configuration

8.1 SNMP Configuration

Click **Network Management Config -> SNMP Management** in the navigation bar, the SNMP management page appears, as shown in the figure.

8.1.1 SNMP Community Management



SNMP Community Management

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

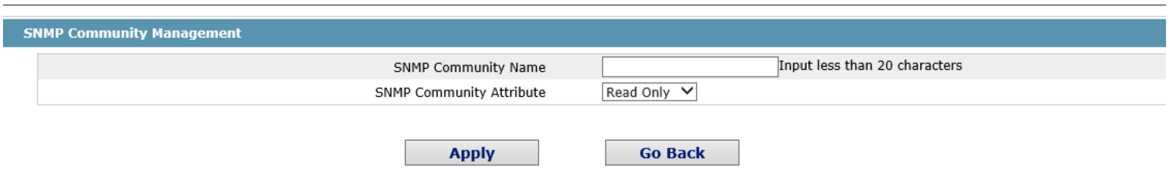
	SNMP Community Name	SNMP Community Encryption	SNMP Community Attribute	Operate
□	nscrtvEponEocTree	False	RO	Edit

□ Select All/Select None

Delete

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 New or Edit, you can switch to the configuration page of SNMP community.



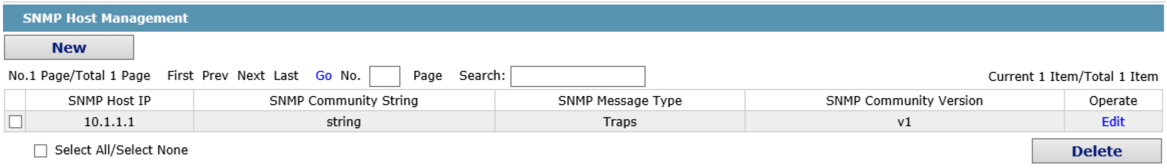
SNMP Community Management

SNMP Community Name	Input less than 20 characters
SNMP Community Attribute	Read Only

Apply Go Back

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.

8.1.2 SNMP Host Management



SNMP Host Management

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

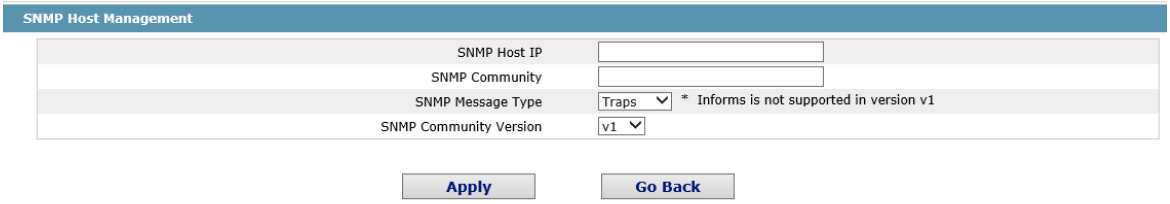
	SNMP Host IP	SNMP Community String	SNMP Message Type	SNMP Community Version	Operate
□	10.1.1.1	string	Traps	v1	Edit

□ Select All/Select None

Delete

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 New or Edit, you can switch to the configuration page of SNMP host.



SNMP Host Management

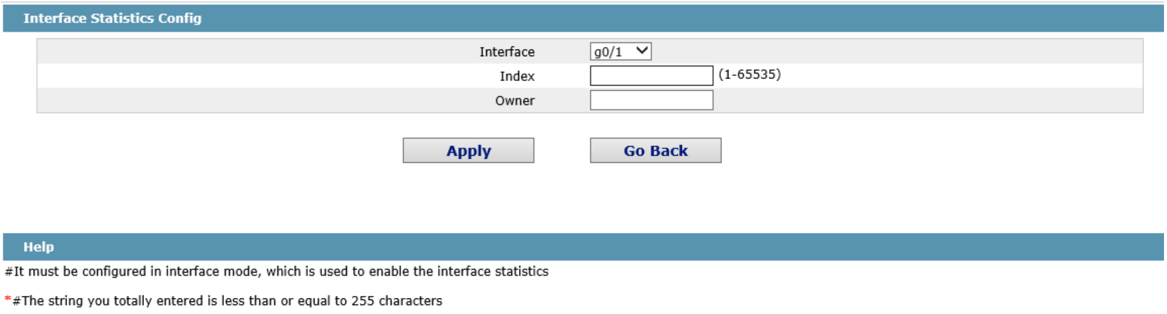
SNMP Host IP	
SNMP Community	
SNMP Message Type	Traps * Informs is not supported in version v1
SNMP Community Version	v1

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

8.2 RMON

8.2.1 RMON Statistic Information Configuration

Click Network Management Config -> Rmon -> Rmon Statistics -> New, the RMON Statistics page appears.



Interface Statistics Config

Interface	g0/1
Index	(1-65535)
Owner	

Help

#It must be configured in interface mode, which is used to enable the interface statistics

*#The string you totally entered is less than or equal to 255 characters

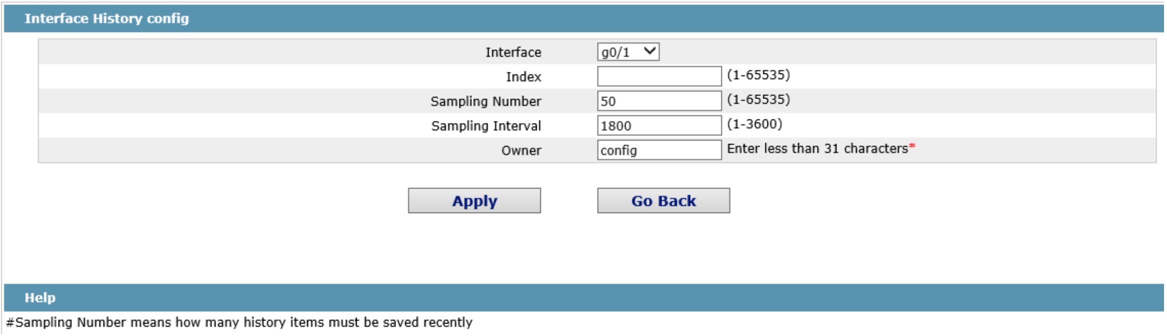
You need to set a physical port to be the reception terminal of the monitor data.

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.

8.2.2 RMON History Information Configuration

Click **Network Management Config** -> **RMON** -> **RMON History** -> **New**, the RMON history page appears.



Interface History config

Interface	g0/1	
Index		(1-65535)
Sampling Number	50	(1-65535)
Sampling Interval	1800	(1-3600)
Owner	config	Enter less than 31 characters*

Help

#Sampling Number means how many history items must be saved recently

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.

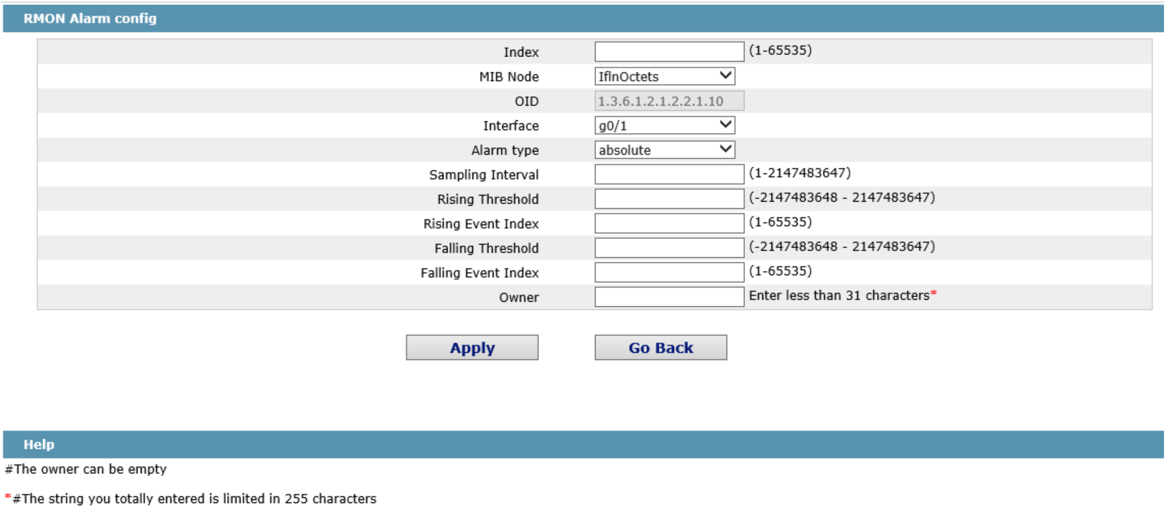
The sampling number means the items that need be reserved, whose default value is 50.

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.

8.2.3 RMON Alarm Information Configuration

Click Network Management Config -> Rmon -> Rmon Alarm -> New, the RMON Alarm page appears.



RMON Alarm config

Index		(1-65535)
MIB Node	IflnOctets	
OID	1.3.6.1.2.1.2.2.1.10	
Interface	g0/1	
Alarm type	absolute	
Sampling Interval		(1-2147483647)
Rising Threshold		(-2147483648 - 2147483647)
Rising Event Index		(1-65535)
Falling Threshold		(-2147483648 - 2147483647)
Falling Event Index		(1-65535)
Owner		Enter less than 31 characters*

Help

#The owner can be empty

*#The string you totally entered is limited in 255 characters

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.

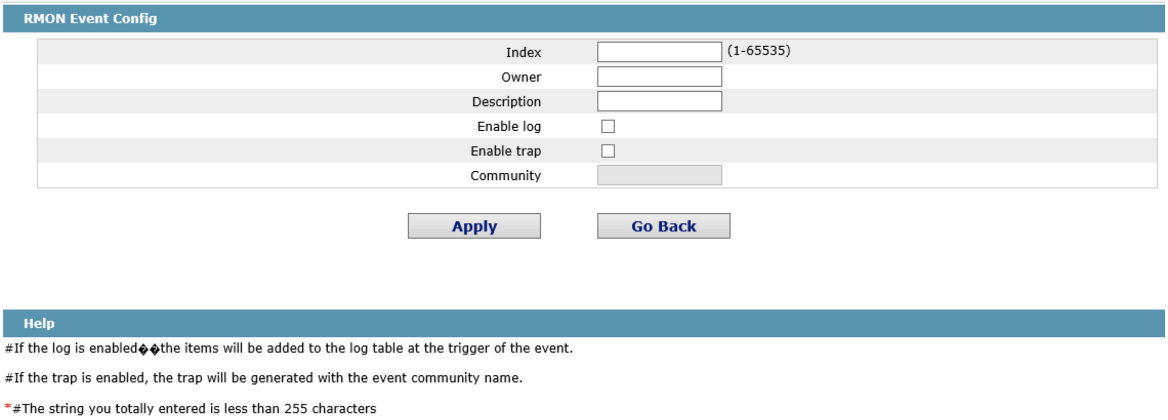
If the alarm type is absolute, the value of the MIB object will be directly minitored; if the alarm type is delta, the change of the value of the MIB object in two sampling will be monitored.

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.

8.2.4 RMON Event Configuration

Click Network Management Config -> RMON -> RMON Event -> New, the RMON event page appears.



Index	(1-65535)
Owner	
Description	
Enable log	□
Enable trap	□
Community	

#If the log is enabled��the items will be added to the log table at the trigger of the event.

#If the trap is enabled, the trap will be generated with the event community name.

*#The string you totally entered is less than 255 characters

The index corresponds to the rising event index and the falling event index that have already been configured on the RMON alarm config page.

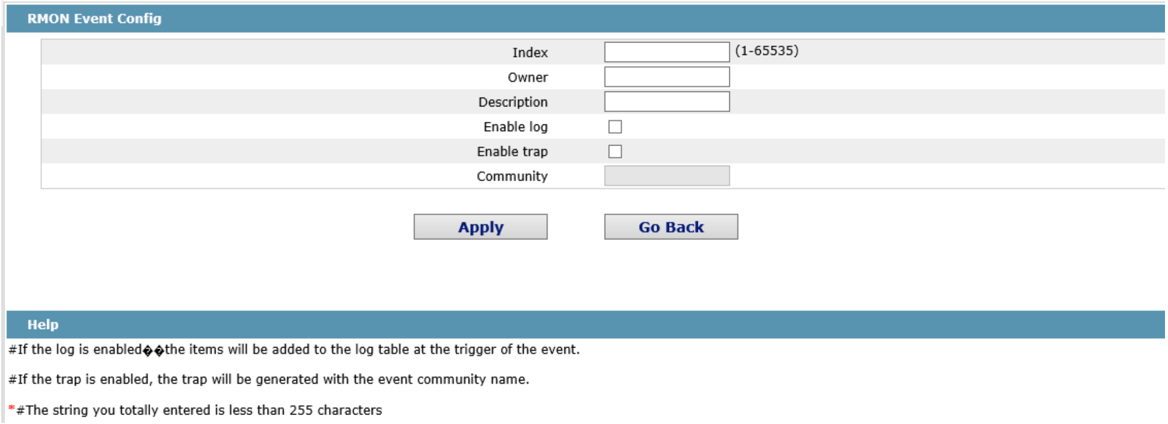
The owner is used to describe the descriptive information of an event.

"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.

Chapter 9 Diagnosis Tools

Click **Diagnosis Tools -> Ping**, the Ping page appears.



RMON Event Config

Index		(1-65535)
Owner		
Description		
Enable log	□	
Enable trap	□	
Community		

Help

#If the log is enabled��the items will be added to the log table at the trigger of the event.

#If the trap is enabled, the trap will be generated with the event community name.

*#The string you totally entered is less than 255 characters

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.

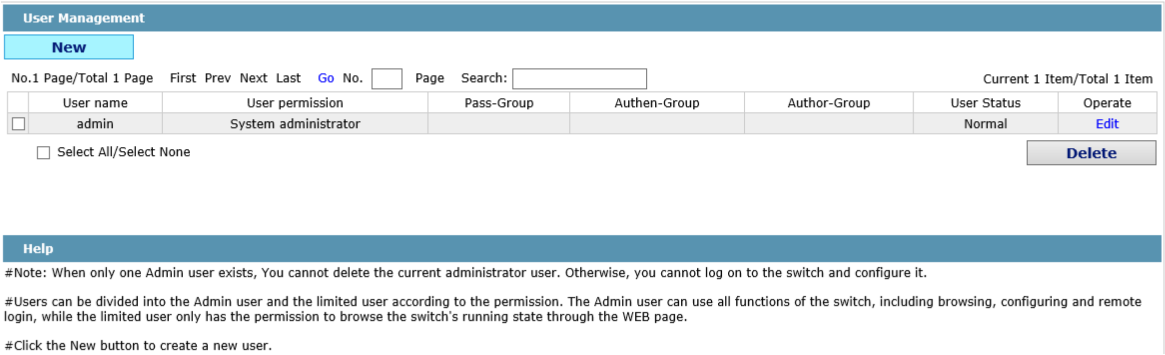
“Size of the PING packet” is used to set the length of the Ping packet which is transmitted by the device.

Chapter 10 System Management

10.1 User Management

10.1.1 User List

Click System Mgr.-> User Mgr., the User Management page appears.


User Management
New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item
□ Select All/Select None
Delete
Help

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

#Note: When only one Admin user exists, You cannot delete the current administrator user. Otherwise, you cannot log on to the switch and configure it.

#Users can be divided into the Admin user and the limited user according to the permission. The Admin user can use all functions of the switch, including browsing, configuring and remote login, while the limited user only has the permission to browse the switch's running state through the WEB page.

#Click the New button to create a new user.

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

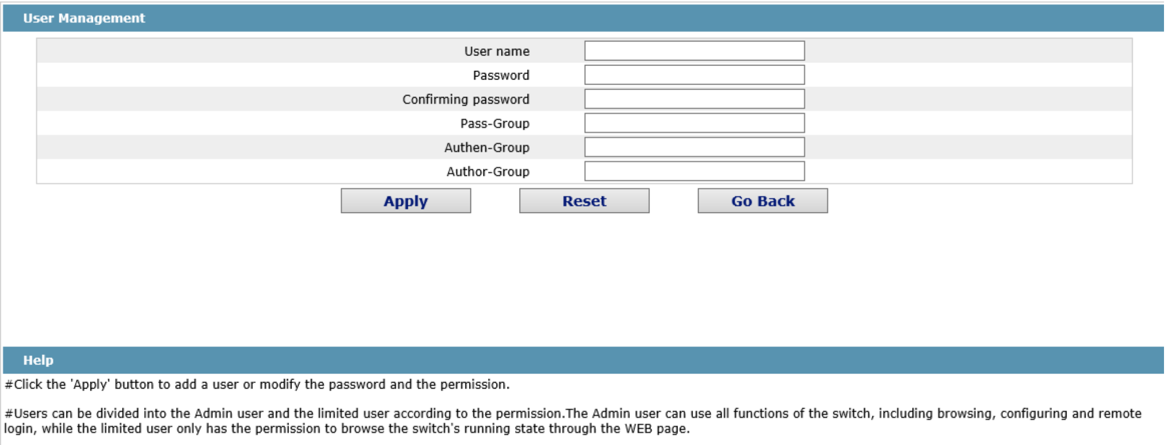
To modify the permission or the login password, click "Edit" on the right of the user list.

NOTE

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

10.1.2 Establishing a New User

Step 1 Click "New" on the User Management page, the Creating User page appears.



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

#Click the 'Apply' button to add a user or modify the password and the permission.

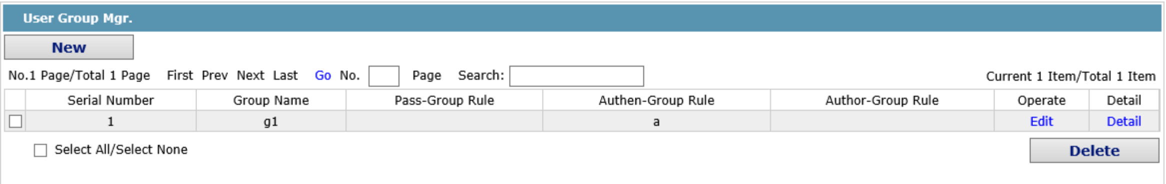
#Users can be divided into the Admin user and the limited user according to the permission.The Admin user can use all functions of the switch, including browsing, configuring and remote login, while the limited user only has the permission to browse the switch's running state through the WEB page.

Step 2 In the “User name” text box, enter a name, which contains letters, numbers and symbols except “?”, “\”, “&”, “#” and the "Space" symbol.

Step 3 In the “Password” textbox enter a login password, and in the “Confirming password” textbox enter this login password again.

10.1.3 User Group Management

Click the Tab page of user group management and enter user group management page.

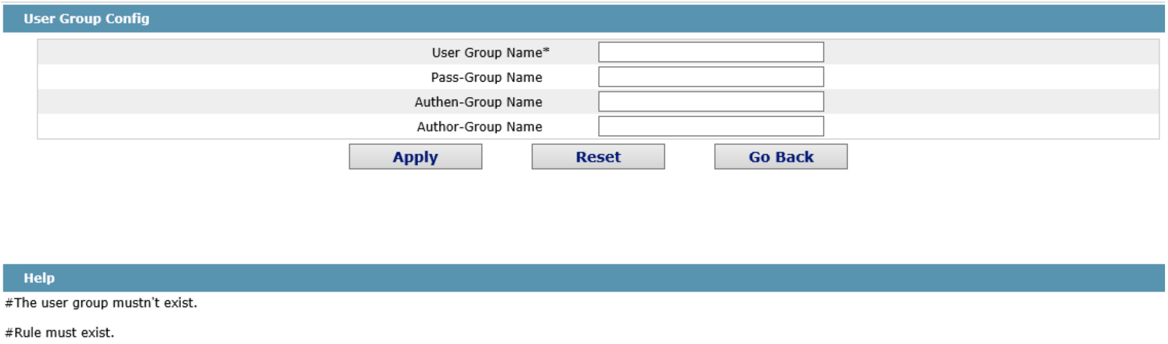

User Group Mgr.
New
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search:
Current 1 Item/Total 1 Item
Delete

	Serial Number	Group Name	Pass-Group Rule	Authen-Group Rule	Author-Group Rule	Operate	Detail
□	1	g1		a		Edit	Detail

□ Select All/Select None

Click “create new” to create a new user group.

Click “delete” to delete the user group.



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

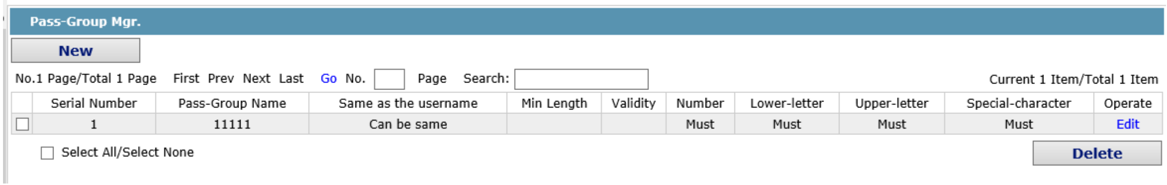
#The user group mustn't exist.

#Rule must exist.

The new user group name must be not used before. The password rule name, authentication rule name and authorization rule name must have been created, or you cannot create a new user group. Configure the password rule, authentication rule and authorization rule in other 3 tab pages.

10.1.4 Password Rule Management

Click password rule management Tab page to enter password rule management page.



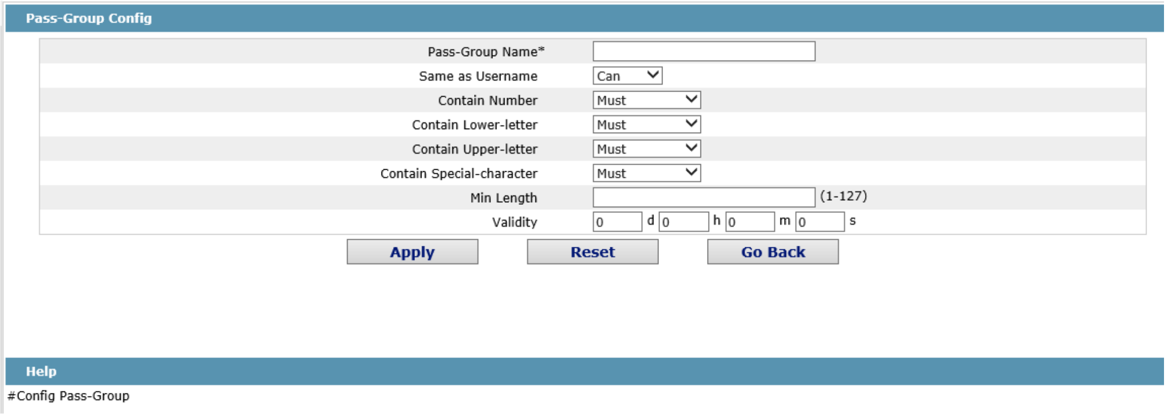
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

	Serial Number	Pass-Group Name	Same as the username	Min Length	Validity	Number	Lower-letter	Upper-letter	Special-character	Operate
□	1	11111	Can be same			Must	Must	Must	Must	Edit

□ Select All/Select None

Click “create new” to create new password rule.

Click “delete” to delete password rule.



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

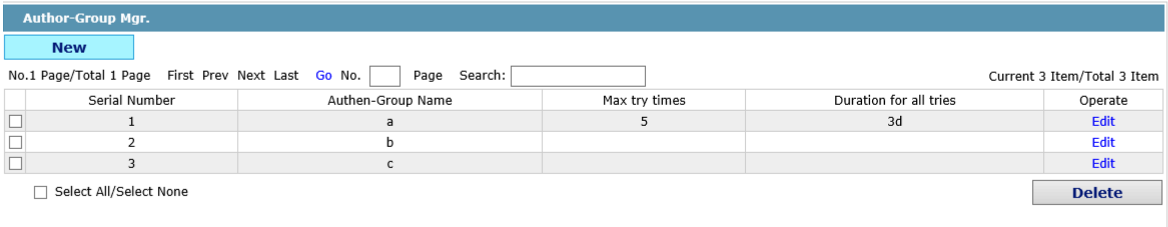
#Config Pass-Group

Set some password rules including whether the password can be the same with the user name, whether the password must contain numbers, lowercase, uppercase, special characters, the minimum length and the period of validity.

When the rule is created and applied to the user management, the user password will show invalid if the set password is not complied with the password rule, vice versa.

10.1.5 Authentication Rule Management

Click the Tab page of authentication rule management to enter authentication management page.



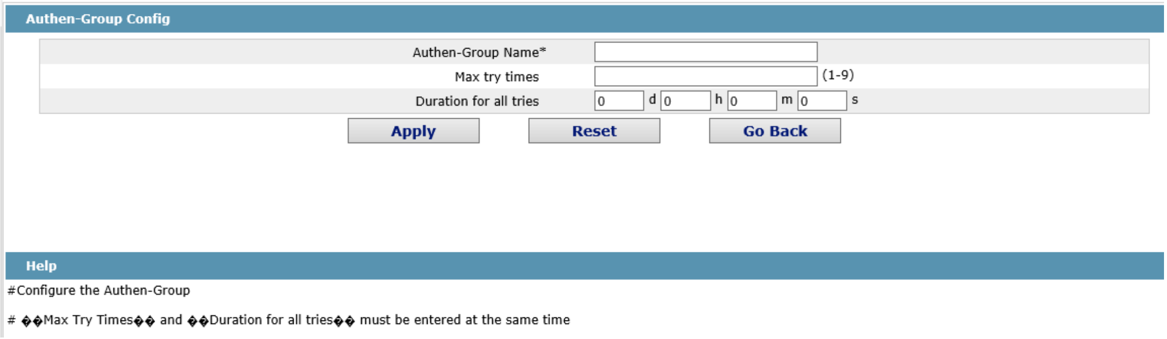
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 3 Item/Total 3 Item

	Serial Number	Authen-Group Name	Max try times	Duration for all tries	Operate
□	1	a	5	3d	Edit
□	2	b			Edit
□	3	c			Edit

□ Select All/Select None

Click “create new” to create the new authentication rule.

Click “delete” to delete the authentication rule.



Authen-Group Config

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

Help

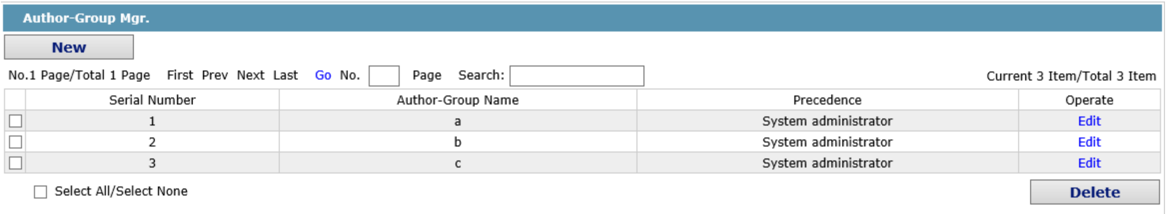
#Configure the Authen-Group

��Max Try Times�� and ��Duration for all tries�� must be entered at the same time

You can configure the maximum number of attempts and periods or you don’t, but you must configure them simultaneously or neither.

10.1.6 Authorization Rule Management

Click the Tab page of authorization rule and enter the authorization rule management page.



Author-Group Mgr.

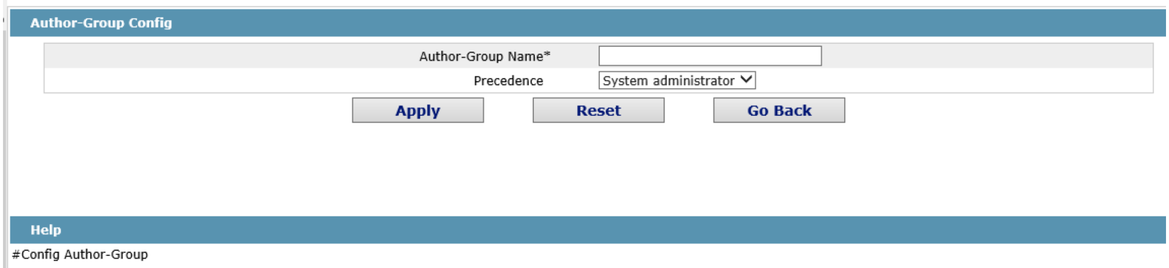
No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 3 Item/Total 3 Item

	Serial Number	Author-Group Name	Precedence	Operate
□	1	a	System administrator	Edit
□	2	b	System administrator	Edit
□	3	c	System administrator	Edit

□ Select All/Select None

Click “create new” to create new authorization rule.

Click “delete” to delete the authorization rule.



Author-Group Config

Author-Group Name*	
Precedence	System administrator

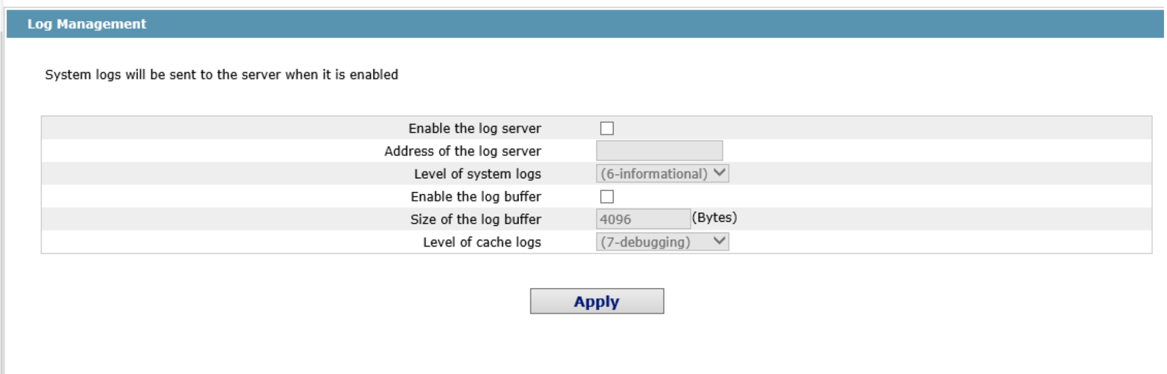
Help

#Config Author-Group

The authorization rule determines your permission of the administrator or the limited user. If you are the administrator, you have the administrator right. If you are the limited user, you can only but check the web.

10.2 Log Management

Click **System Mgr.-> Log Mgr.**, the Log Management page appears.



Log Management

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

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

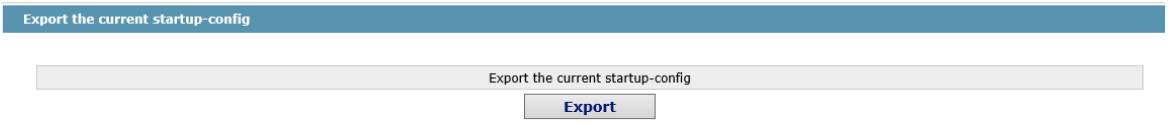
If “Enabling the log server” is selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the “Address of the system log server” textbox and select the log's grade in the “Grade of the system log information” dropdown box.

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.

10.3 Managing the Configuration Files

Click **System Mgr.-> Configuration file**, the Configuration file page appears.

10.3.1 Exporting the Configuration Information



Export the current startup-config

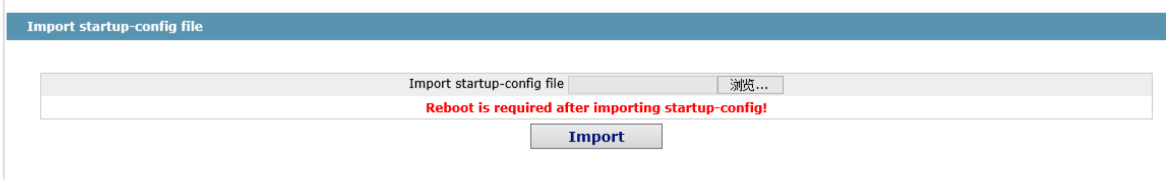
Export the current startup-config

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 and then select the “Save” option in the pop-up download dialog box.

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

10.3.2 Importing the Configuration Information



Import startup-config file

Import startup-config file 浏览...

Reboot is required after importing startup-config!

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.

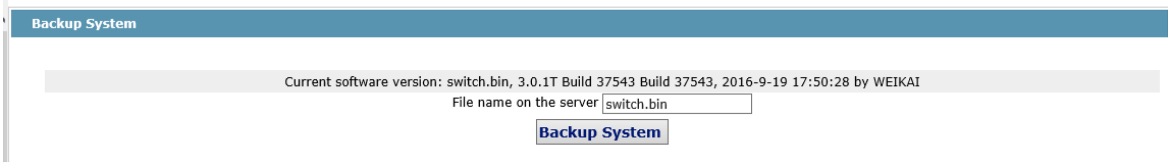
NOTE

- 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.
- 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.
- 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.

10.4 Software Management

Click **System Mgr. -> Software Update** in the navigation bar, and enter the device software management page.

10.4.1 Backup System Software



Backup System

Current software version: switch.bin, 3.0.1T Build 37543 Build 37543, 2016-9-19 17:50:28 by WEIKAI

File name on the server switch.bin

The current running software version is displayed in the page. If you need to backup the system, please click "backup system software", then select "save" in the pop-up file download dialog box and save the system profile to your computer disk, transferable data device or other positions in the network.

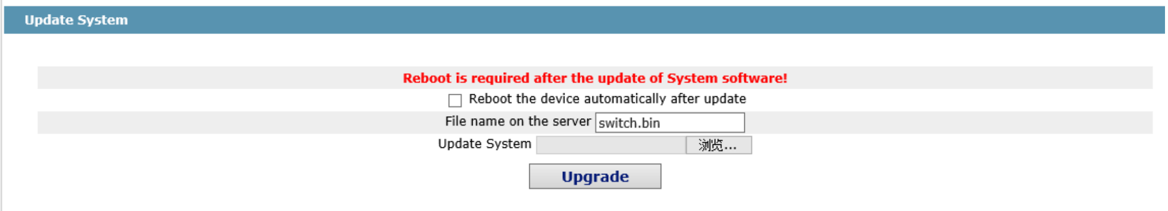
NOTE

Default name of the system profile is “Switch.bin”. You are suggested to change the default name to a name that easy to identify.

10.4.2 Update System Software

NOTE

- Please ensure your update system profile match with the device type. Otherwise, the system cannot operate normally.
- The system profile update may need 1 to 2 minutes. After clicking and confirming the “update” button, the profile will be upload to the device. Please be patient.
- Please do not restart or interrupt the device if errors occur in the update process, or the device cannot start up. Please try update again later.
- Please save the configuration and restart the device after updating, so that the new system can operate.



Update System

Reboot is required after the update of System software!

□ Reboot the device automatically after update

File name on the server: switch.bin

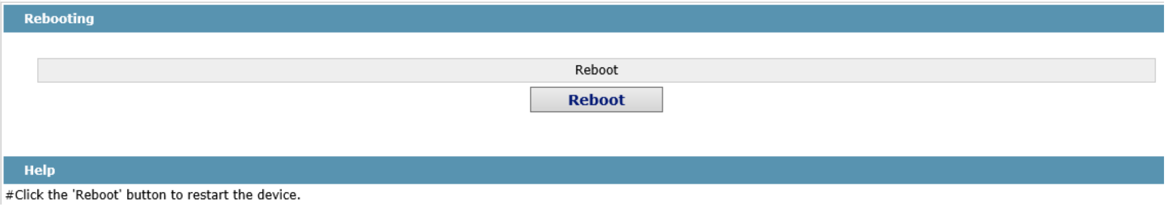
Update System: 浏览...

The update software is usually used for solving the existing problems or improving certain functions. You don’t need to update the system software regularly, if your device operates normally.

If your system needs to be update, please enter the full path of the new system profile into the text box right of “update system software” or click “browse” button to select new system profiles and click “update”.

10.5 Rebooting the Device

Click **System Mgr.-> Reboot,** the Rebooting page appears.



Rebooting

Reboot

Help

#Click the 'Reboot' button to restart 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.

First Choice for Security Professionals

www.hikvision.com