Gigabit Industry Managed PoE Switch

WEB Management Manual

8000110 Ver 5.0.8

Statement

Preface

This manual mainly describes the web page of industrial grade full Gigabit management PoE switch. Users can manage the switch through the web page of full Gigabit management PoE switch. This manual only briefly introduces the operation of each web page. Please refer to the user's operation manual for the introduction of each function of the full Gigabit management Ethernet switch。

The preface includes the following contents：

- Readers
- Product
- Product function

Readers

- Network planners
- On site technical support and maintenance person
- Network administrator responsible for network configuration and maintenance

Product

All Gigabit management Ethernet switch is designed and developed by our company. It is specially designed for the construction of high security and high performance network. The system adopts a new software and hardware platform, provides a comprehensive security protection system, perfect QoS strategy and rich VLAN functions, and has simple management and maintenance. It is an ideal convergence layer switch for office network, campus network, small and medium-sized enterprises and branches。

Product features

- Support IEEE 802.3x

- Support IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3z
- Support IEEE 802.3ad
- Support IEEE 802.3q 、IEEE 802.3q/p
- Support IEEE 802.1w、IEEE 802.1d 、EEE 802.1S
- Support 16K MAC address table, automatic update, two-way learning
- Support port based VLAN, up to 4096 VLAN
- Support 802.1Q standard VLAN
- Support STP Spanning tree protocol
- Support RSTP Fast spanning tree protocol
- Support MSTP Fast spanning tree protocol
- Support EPPS Ring network protocol
- Support EAPS Ring network protocol
- Support 802.1x Argumentation agreement
- Support 8 groups of aggregation, each group supports up to 8 ports
- Support bidirectional port image
- Support loop protection function, real-time detection, rapid alarm, accurate positioning, intelligent blocking and automatic recovery
- Support the isolation of downlink ports and communication with uplink ports
- Support half duplex control based on back pressure
- Support full duplex based on pause frame
- Support port based input / output bandwidth management
- Support IGMPv1/2/3 和 MLDv1/2 Snooping
- Support GMRP Agreement Registration
- Support multicast address management, multicast VLAN, multicast routing port and static multicast address
- Support DHCP Snoping
- Support storm suppression of unknown unicast, multicast, unknown multicast and broadcast type

- Support storm suppression based on bandwidth adjustment and storm filtering
- Support user port + IP address + MAC address
- Support ACL based on IP and MAC
- Support the security nature of the number of MAC addresses based on the port
- Support 802.1p port queue priority algorithm
- Support CoS / TOS, QoS tag
- Support WRR (Weighted Round Robin)，Weighted priority rotation algorithm
- It supports WRR, SP and WFQ priority scheduling modes
- Support auto mdix function, automatically identify through network cable and cross network cable
- Support port support automatic negotiation function (self negotiation transmission rate and duplex mode)
- Support upgrade package upload
- Support system log viewing
- Support web to restore factory configuration
- Support to open or close the port
- Support standard Poe scheduling management
- Support the function of automatic detection online equipment (automatic, no operation)
- Support web interface management
- Support cli management based on telnet and console
- Support SNMP V1/V2/V3 management
- Support SSHV1/V2 management
- Support RMON management

[Version update]

Ver 5.0.8

User experience Optimization

It solves the known problems and has faster response speed。

Perfect support for Chinese English one click conversion。

Optimize the related functions to make the management easier。

Catalog

一、WEB Page overview

1、WEB Characteristics of the visit

All Gigabit management Ethernet switch provides users with web access function. Users can access the switch through web browser to manage and configure the switch。The main features of the visit are：

- Easy access: users can easily access the switch from anywhere in the network。
- Users can use familiar Netscape communicator, Microsoft Internet Explorer and other browsers to access the web page of full Gigabit management Ethernet switch, and the web page is presented to users in graphical and tabular form。
- Gigabit management Ethernet switch provides rich web pages, through which users can configure and manage most of the functions of the switch。
- The classification and integration of web page functions is convenient for users to find relevant pages for configuration and management。

2、System requirements of WEB browsing

The system requirements of web browsing are shown in Table 1。

Table1：

Hardware and Software	**System requirements**
CPU	Pentium 586 up
Memory	128MB up
Resolution ratio	800x600 up
Color	256 color up
Browser	IE4.0 or above or Netscape 4.01 or above
Operating system	Microsoft® ,Windows95®,Windows10®,WindowsNT®, Windows2000®,WindowsXP®,WindowsME®, WindowsVista®, Windows7®, Windows8®,MAC, Linux,Unix operating system

Tips：

Microsoft®,Windows95®,Windows10®,WindowsNT®,Windows2000®,WindowsXP ®,Windows ME®, WindowsVista®, Windows7®, Windows8® is a registered trademark of Microsoft Corporation. All other product names, trademarks, registered trademarks and service marks are copyrighted by their respective owners.。

3、Login of web browsing session

The user needs to confirm before starting a web browsing session：

- The switch has been configured with IP. By default, the vlan1 interface IP address of the switch is 192.168.0.1，
- The subnet mask is 255.255.255.0。
- A host with a web browser has been connected to the network, and the host can ping the switch。
- After completing the above two tasks, the user can enter the address of the switch in the address bar of the browser and press enter to enter the web login page of the switch, as shown in Figure 1. When multi-user management is not enabled, users need to verify the password of the anonymous user (**admin**) when they log on to the web. Only when they enter the correct password can they access the web. The password of the anonymous user is **admin** by default。

If multi-user management is enabled and privileged users are configured in the system, the password of anonymous users will not take effect. Users do not verify the password of anonymous users when accessing the web, but verify the user name and password of multi-user management。

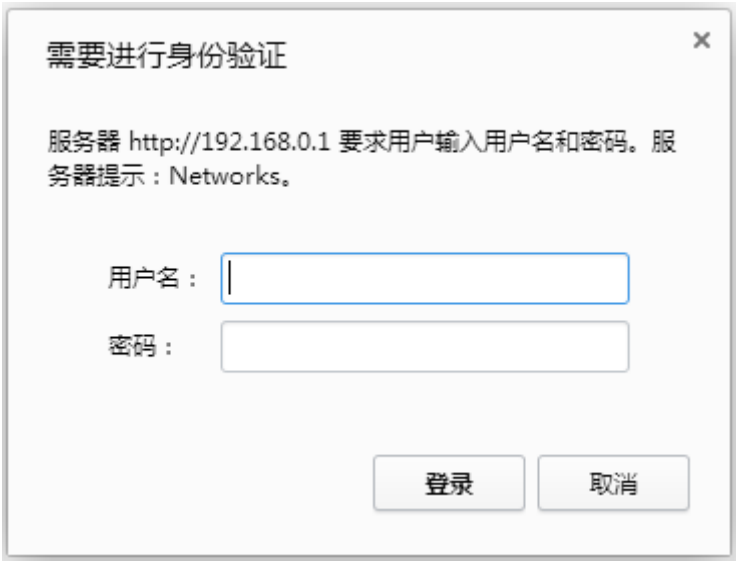


Figure 1 login page of web browsing session

4、Basic composition of WEB page

As shown in Figure 2, the web page is mainly composed of three parts: the title page, the navigation tree page and the main page。

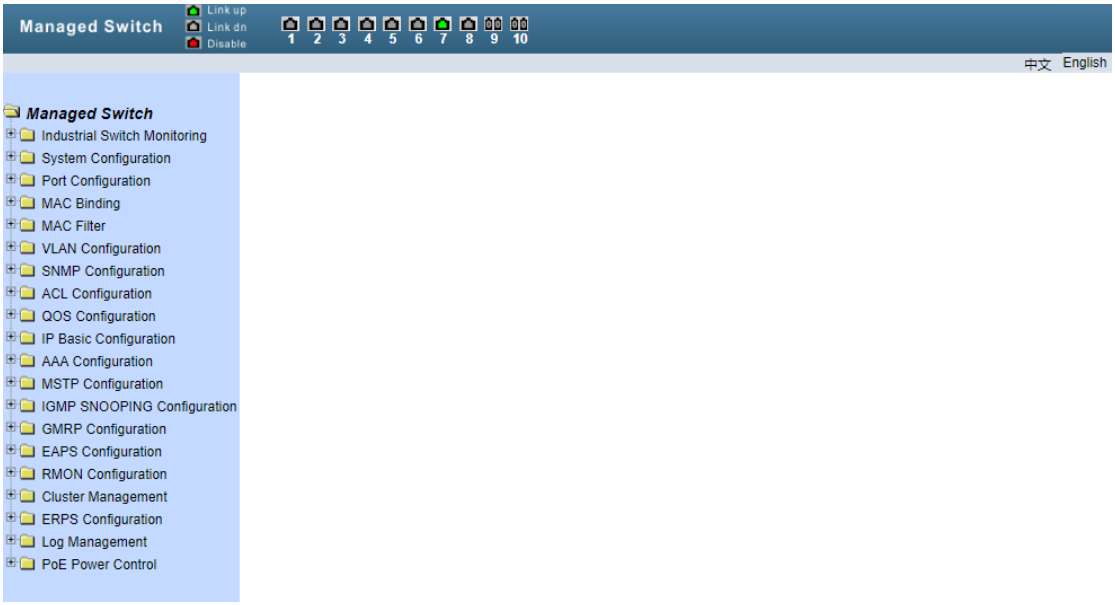


Figure 2 basic composition page of switch web page

Title Page The logo and real-time port status are shown in the following figure
The green light indicates that the port is connected;
The gray light indicates that the port is not connected;
The red light indicates that the port is closed (refer to figure 17 for specific settings)

Main page Used to display the page selected by the user from the navigation tree。

5、Navigation tree structure

Figure 3 shows the organizational structure of the navigation tree。

The navigation tree is located at the bottom left of each page, and the nodes of the web page are displayed in the form of tree. Users can easily find the web page to manage. According to the different functions of the web page, it is divided into different groups, each group includes one or more pages. Most of the page names in the navigation tree are the abbreviations of the page title at the top of the corresponding page。

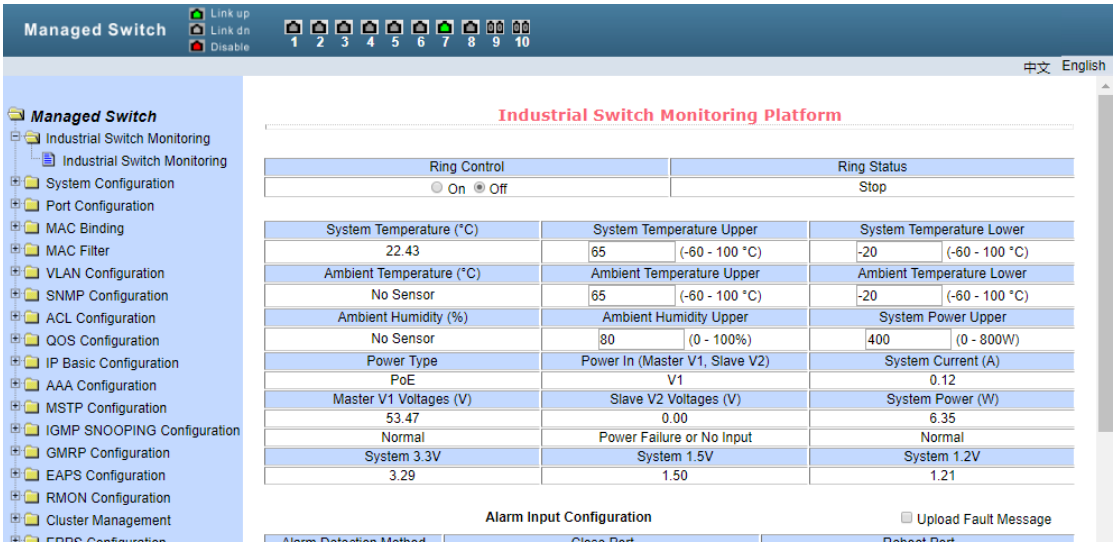


Figure 3 organization page of switch navigation tree

6、Page button introduction

There are some general buttons on the page, and the functions of these buttons are generally the same. Table 2 introduces the functions of these buttons。

Table 2：

Button	**Function**
Refresh	Update all fields on the page
Application	Put the updated value into memory. Because error checking is done by the web server,So there is no error checking before the user selects the button
Delete	Delete current record
Help	Open the help page to view the configuration description of each page

7、Error message

If the web server of the switch makes an error when processing the user's request, the corresponding error information will be displayed in a dialog box. For example, figure 4 shows an error message dialog。

图4 出错信息页面

8、Entry field

Some pages have an entry field in the leftmost column of the table, as shown in Figure 5, through which different rows in the table can be accessed. When you select a value in the entry field, the corresponding information of that line will be displayed in the first line. At this time, only that line can be edited, which is also called the active line. When a page is initially loaded, the entry field displays new and the activity behavior is empty。

If you want to add a new line, select new from the drop-down menu in the entry field, enter the new line information, and then press the apply key。

If you want to edit an existing row, select the corresponding row number from the drop-down menu of the entry field, edit the row as needed, and then press the apply key. You will see the corresponding changes displayed in the table。

If you want to delete a row, select the corresponding row number from the drop-down menu of the entry field, and then press the delete key, and the row will disappear from the table。

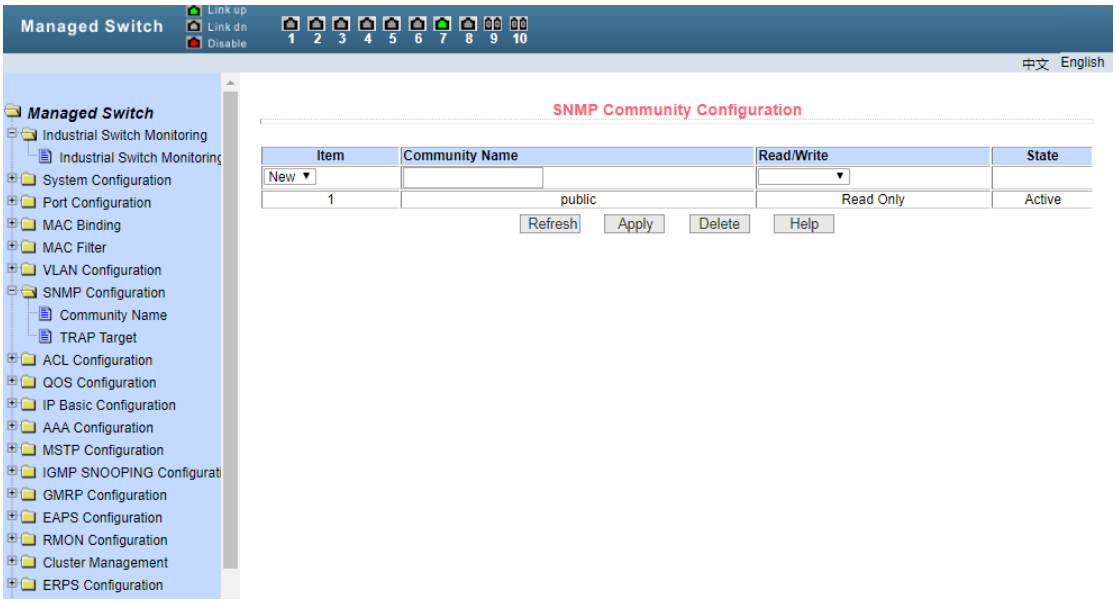


Figure 5 entry field page

9、State domain

Some pages have a status field in the rightmost column of the table, as shown in Figure 6, which displays the status of the row. The state field is read-only because all changes to the row state are processed internally. Once all the domain information in a row is valid, the state of the row will automatically become active。

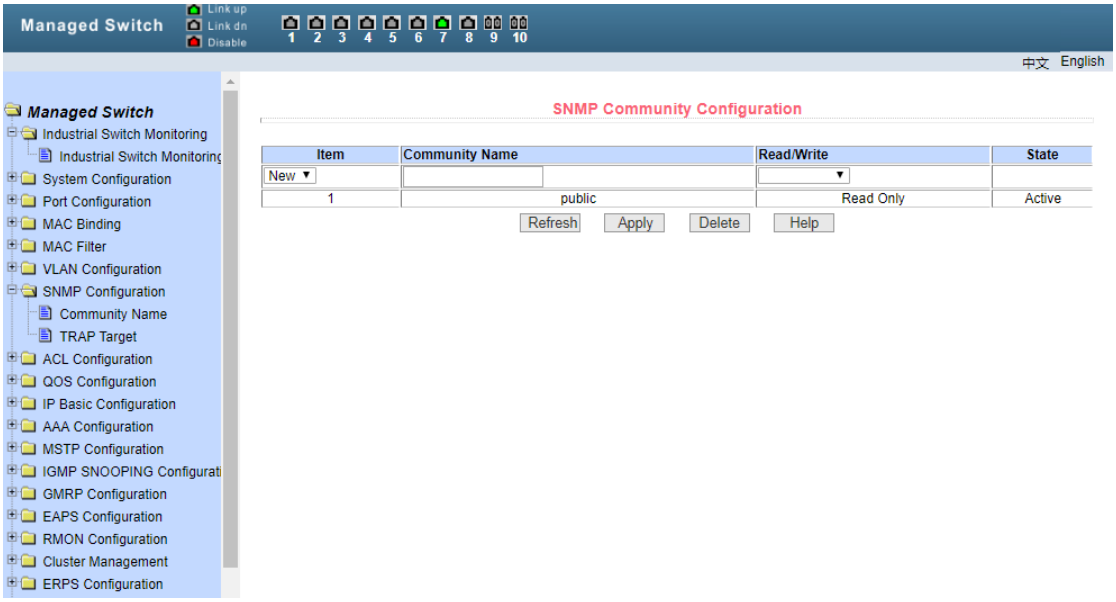


Figure 6 state field page

二、WEBPage introduction

1、Login Dialog

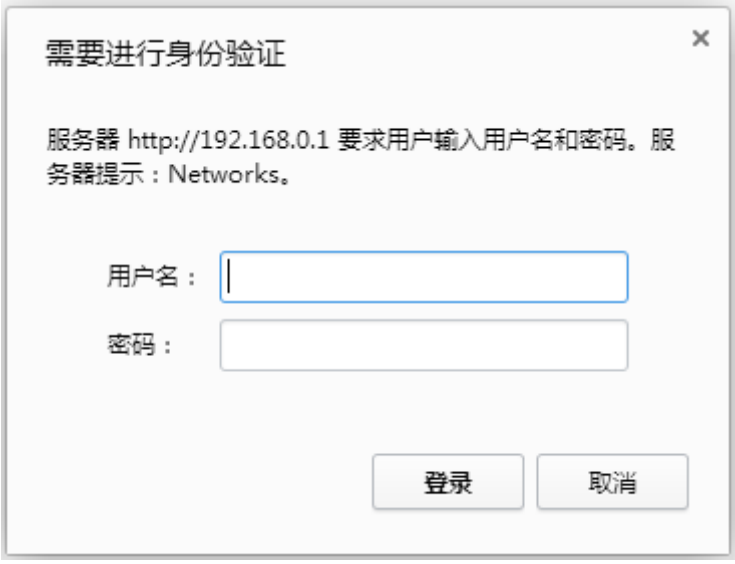


Figure 1-1 login page of web browsing session

Figure 7 shows the login dialog box, which is displayed when the user logs in to the web page for the first time. The user can enter the user name and password in the corresponding field, and then click OK to log in to the web server of the switch. Passwords are case sensitive, anonymous user passwords can be set up to 16 characters, while multiple user names and

passwords can be set up to 16 characters. The default user name of the management switch is the anonymous user name admin, the default password is the anonymous user password, and the anonymous user password is empty by default。

2、Main page

Figure 1-2 shows the web main page of the management switch. The page will be displayed after the user logs in to the web page。

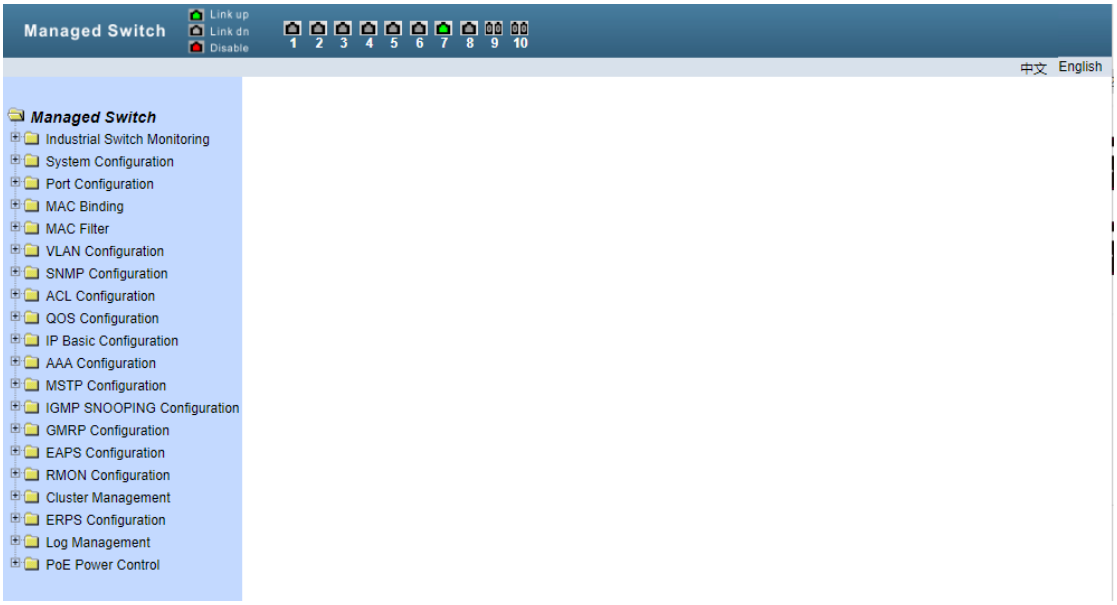
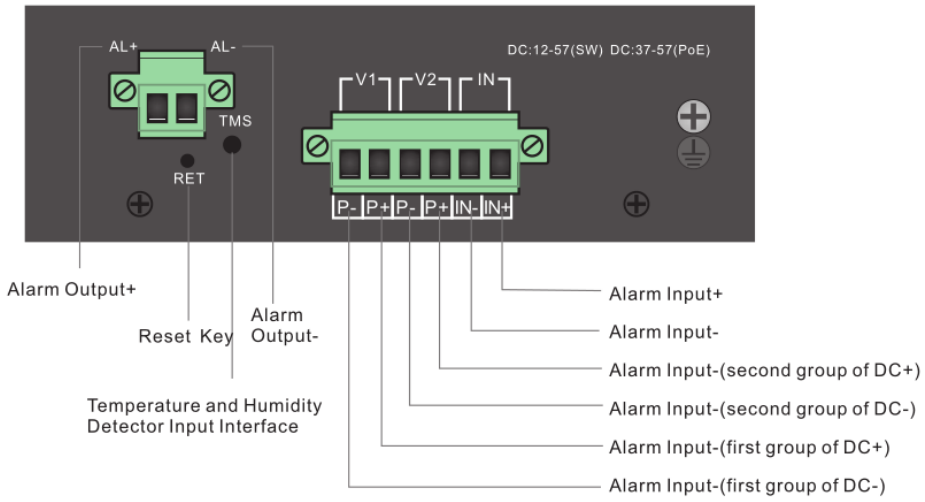


Figure 1-2 main page of switch

3、Industrial switch monitoring platform



Alarm detection mode

1.1 Off: the alarm is in off state, no alarm state output and action。

1.2 Low level alarm: when the alarm input changes from high level to low level, the alarm will be triggered. (higher than 5V, lower than 57V is high level, lower than 5V is low level)

1.3 High level alarm: when the alarm input changes from low level to high level, the alarm will be triggered. (higher than 5V, lower than 57V is high level, lower than 5V is low level)

（2）. Close port

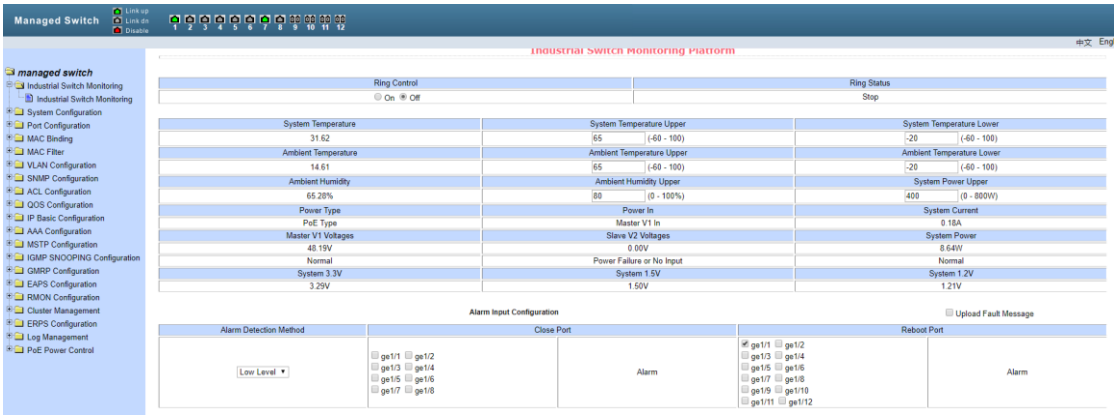
2.1 Select port: select the port to be activated after the alarm is triggered. After the alarm is released, the port action will return to the open state. For each trigger, select the port to restart once, and do not repeat。

2.2 Status box: alarm / normal

（3）. Restart port

3.1 Select port: select the port to be activated after the alarm is triggered. The port performs the port restart action once. For each trigger, select the port restart once and do not repeat。

3.2 Status box: alarm / normal



Alarm output configuration

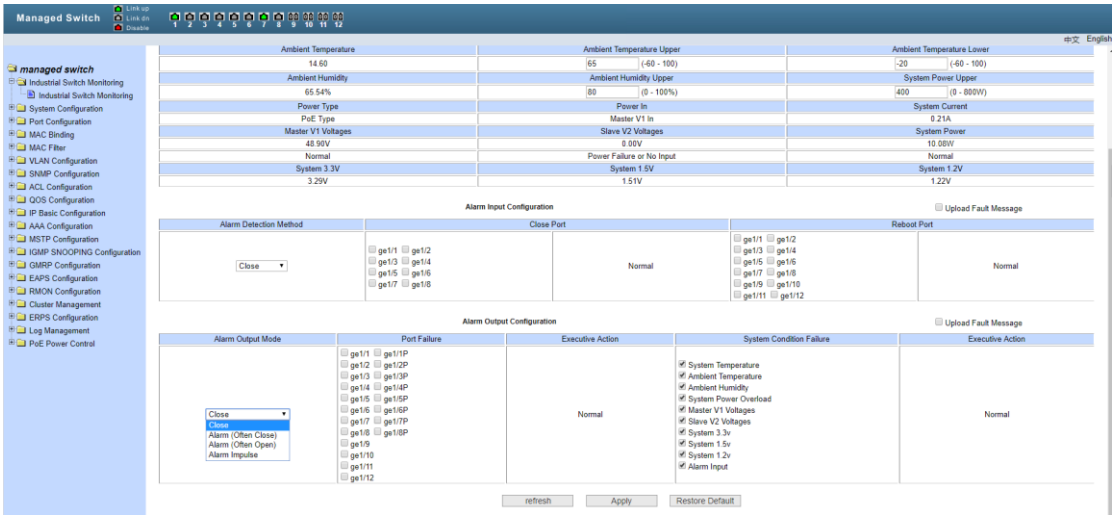
（1）. Alarm output mode

1.1 Turn off alarm: the alarm output is in the off state, and there is no alarm state output and action。

1.2 Alarm (normally closed): after the alarm is triggered, the alarm output is combined

1.3 Alarm (normally open): after triggering the alarm, the alarm output is open

1.4 Cycle alarm: after the alarm is triggered, the alarm output will open / close cycle



（2）. Port failure

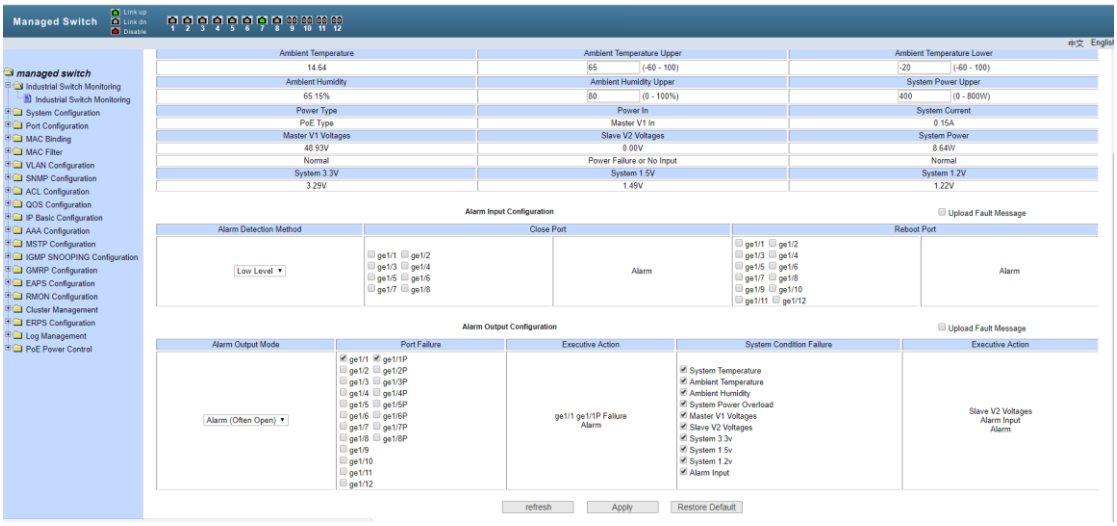
2.1 Select port

2.11：Data port: select the monitoring data port status. When the status is invalid, the alarm output will be triggered. When the status is normal, the alarm will be released。

2.12：PoE port: select the POE state of monitoring data. When the state fails, the alarm output will be triggered. When the state is normal, the alarm will be released。

（3）. Execution action

3.1 Status bar: failure alarm port display / normal



（4）. System condition failure

4.1 System temperature: that is, the temperature in the chassis. Set a temperature value, and if it exceeds this range, an alarm will be triggered

4.2 Ambient temperature: set a temperature value. If the temperature exceeds this range, an alarm will be triggered. The sensor needs to be selected

4.3 Environment humidity: set a humidity value. If it exceeds this range, an alarm will be triggered. Sensor is required

4.4 System power overload: set a power value, exceeding this range will trigger an alarm

4.5 V1 voltage of main power supply: trigger alarm through system monitoring judgment

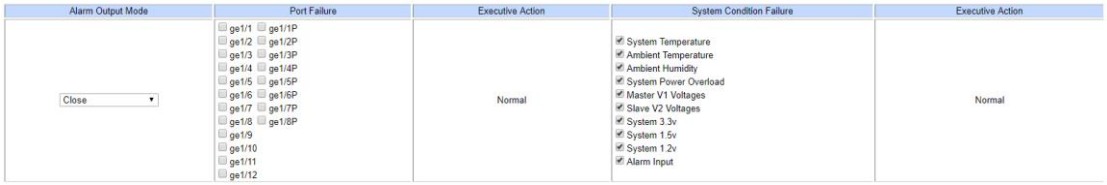
4.6 V2 voltage from power supply: trigger alarm through system monitoring judgment

4.7 System 3.3V: the alarm will be triggered if it exceeds the system monitoring judgment

4.8 System 1.5V: the alarm will be triggered if it exceeds the system monitoring judgment

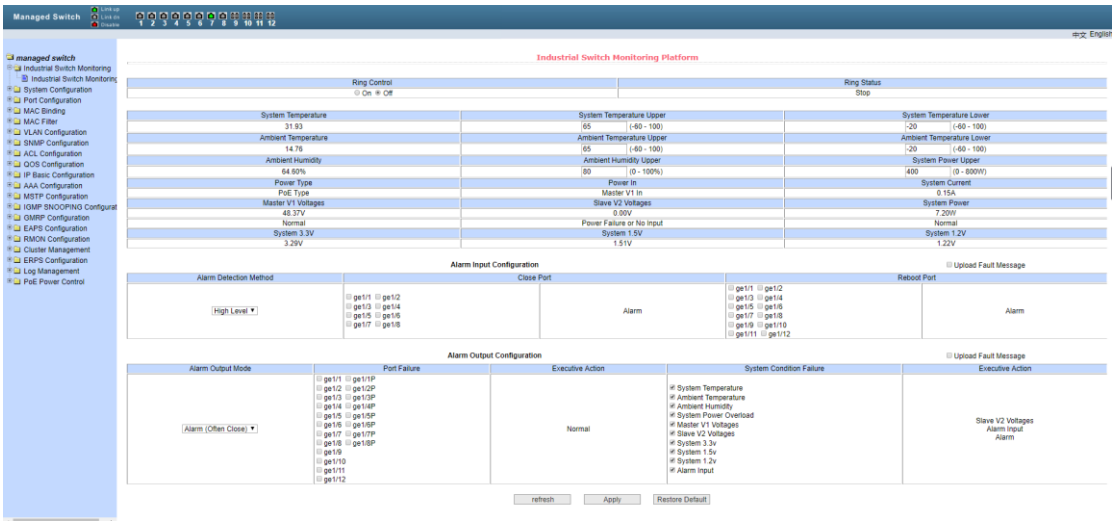
4.9 System 1.2V: the alarm is triggered by exceeding the system monitoring judgment

4.10 Alarm input: the alarm is triggered by the effective state of the alarm input, and the alarm input function needs to be enabled



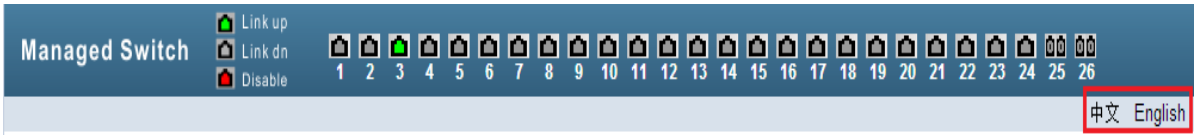
（5）. Execution action

5.1 Status bar: failure alarm port display / normal



4、System configuration

Language switch: switch between Chinese and English system interface easily through the language switch button in the upper right corner。



（1）Basic information

Figure 4-1 is the basic information configuration page, through which users can configure the basic information of the switch。

System description displays the description of system related parameters。

The system descriptor identification number shows the identification of the system in the network management。

The system version number shows the version number of the software currently used by the switch。

The number of network interfaces shows the current number of network interfaces in the switch。

The system startup time shows the time from the switch startup to the present。

The system clock displays the current clock of the system. The user can modify the current clock of the system and input the parameters of year, month, day, hour, minute and second。

The system name shows the system name of the switch in the network. Users can modify the system name。

The system location shows the physical location of the switch in the network, and the user can modify the system location。

The system contact display manages the contact person and contact information of the current node, and the user can modify the system contact information。

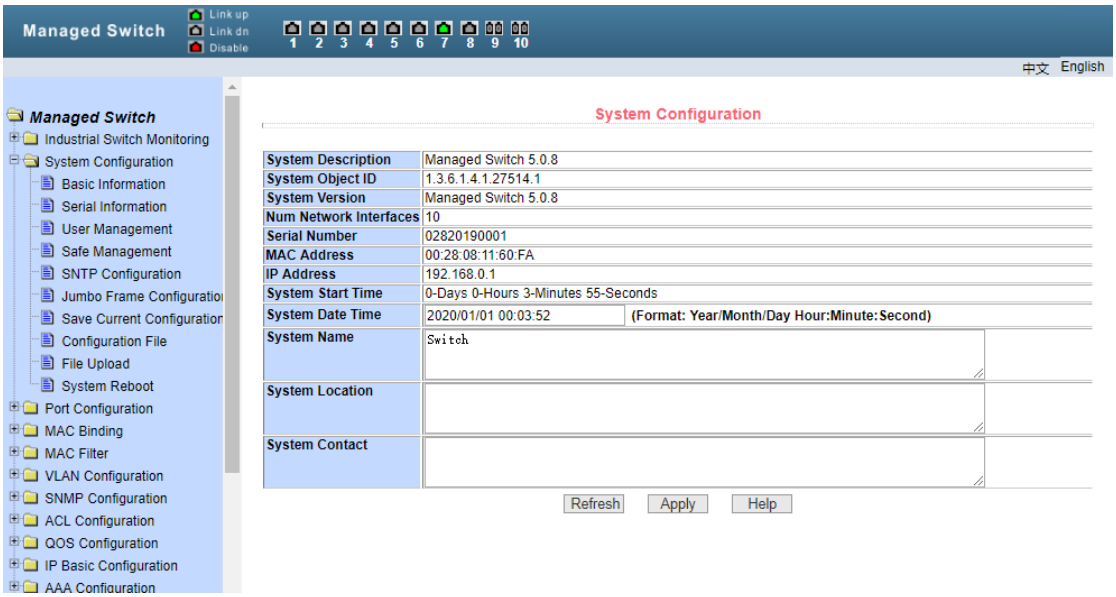


Figure 4-1 basic information page

（2）Serial port information

Figure 4-2 shows the serial port configuration page, which displays the serial port baud rate and other information related to the serial port. When the host manages the switch through the serial terminal (such as the super terminal of windows), the COM port configuration on the serial terminal must be consistent with the information on this page。

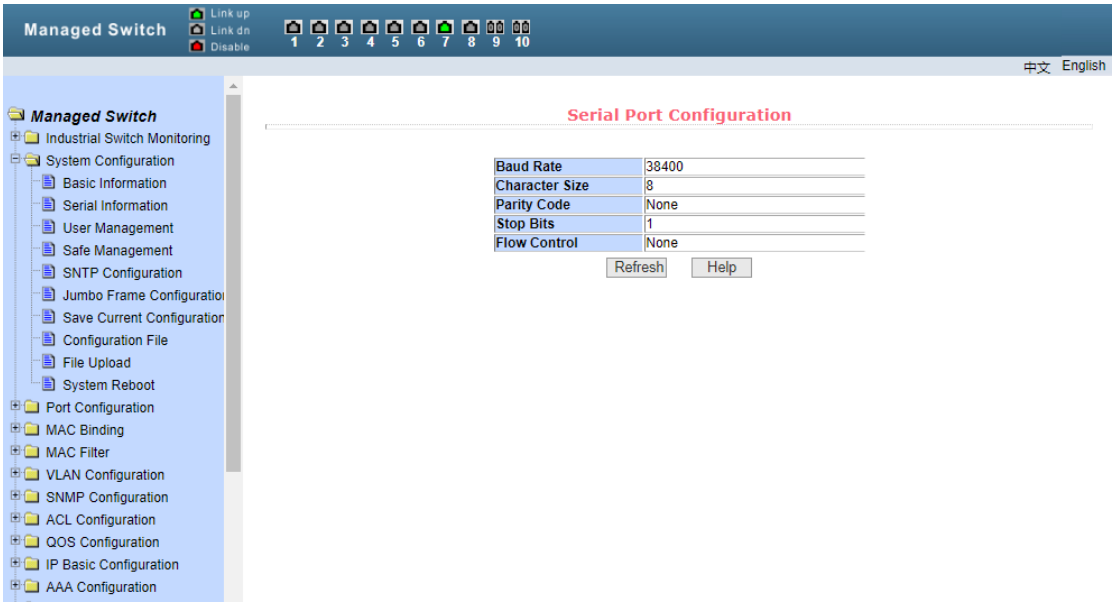


Figure 4-2 serial port information page

（3）user management

Figure 4-3 is the user management page. Through this page, users can modify the password of the switch's anonymous user (admin). Telnet and web use the same anonymous user password when multiple users are not enabled. Passwords are case sensitive and can be set up to 16 characters. If you want to change the password, the user needs to enter the new password twice. Once the user clicks the application key, the new password will be activated. At this time, if the switch does not enable multi-user, the login dialog box will be displayed (as shown in Figure 7). The user needs to log in to the web page again. The user must enter the new anonymous user password to log in to the web pag。

At the same time, users can configure multiple users through this page. The switch does not have multiple users by default, that is to say, the multi-user management function is not enabled by default. At this time, login does not need to verify the user name and password of multiple users. For Telnet, when a user name is added, the multi-user management function is enabled. When all users are deleted, the multi-user management function is turned off. For the web, when a user name is added, if it is a privileged user, the multi-user management function is enabled. When all privileged users are deleted, the multi-user management function is turned off. When the multi-user management function is enabled, the anonymous user password will not take effect. Logging in to telnet and web requires multi-user user user name and password verification. When the multi-user management function is turned off, if the anonymous user password is configured, login telnet and web need to verify the password of the anonymous user。

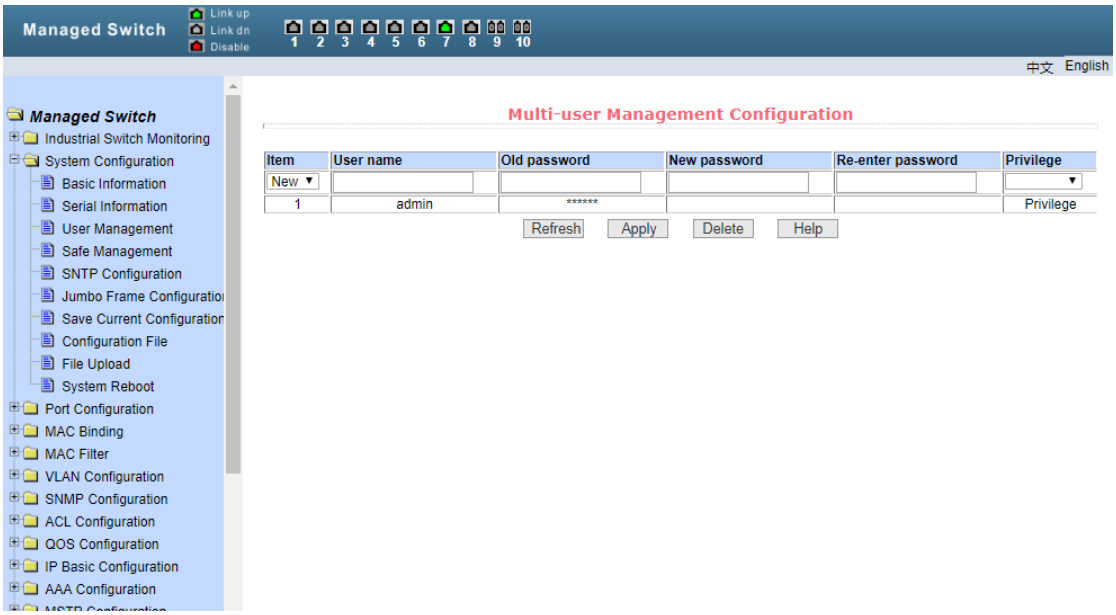


Figure 4-3 user management page

（4）Security management

Figure 4-4 is the security management configuration page. Through the configuration of this page, the administrator can control the network management services Telnet, web and SNMP, enable or disable these services, and connect these services with the ACL group of IP standard to implement source IP address control and control the host's access to these services。

By default, Telnet, web and SNMP services are turned on, and ACL filtering is not done, that is, all hosts can access the three services of the switch. If the administrator does not want to provide one or several services to other users for security, he can shut down one or several services. If the administrator only wants a specific host to access one or more of these services, he can do ACL filtering for one or more of these services. When a service wants to do ACL filtering, it needs to open the service and select an IP standard ACL group (1-99). At this time, the ACL group must exist。

It should be noted that if the administrator controls the web service on this page (such as turning off the web service), the user may no longer be able to use the web page. At this time, the administrator can log in to the switch through other ways and control the web service, so that the user can use the web page (such as turning on the web service)。

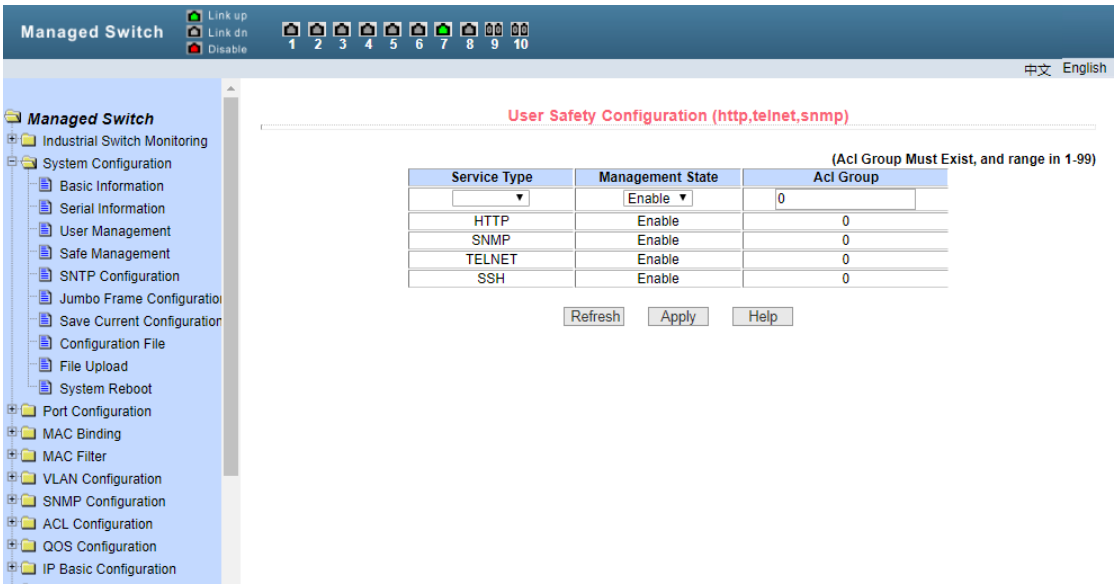


Figure 4-4 security management page

（5）SNTP　configuration

Figure 4-5 shows the SNTP configuration page, through which the administrator can configure and view the system clock。

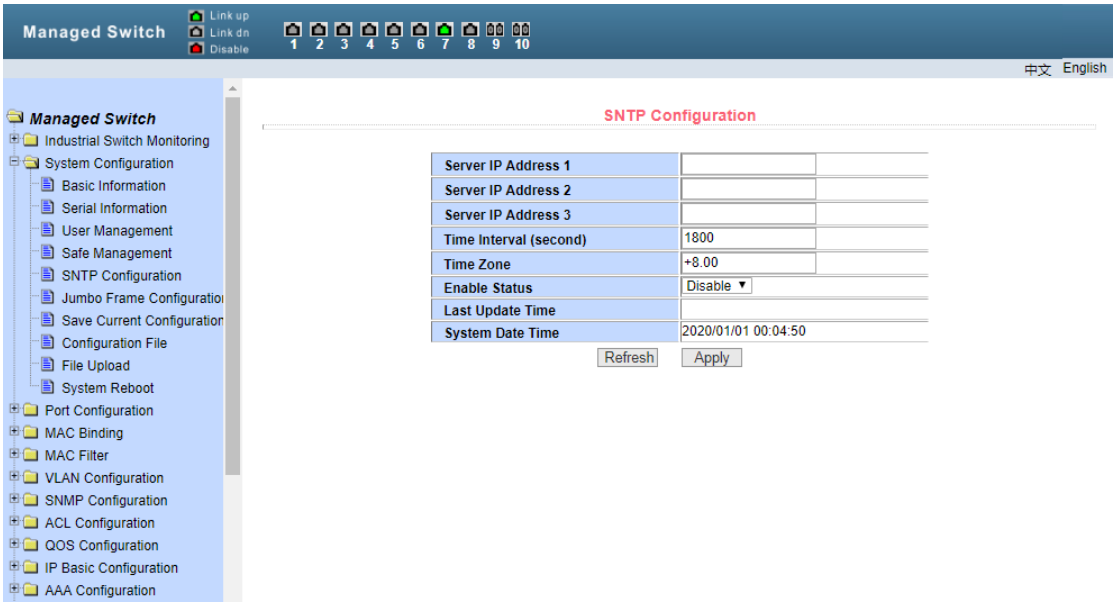


Figure 4-5 SNTP configuration page

（6）Giant sail configuration

Figure 4-6 is the giant sail configuration page, through which the administrator can configure and view the giant sail。

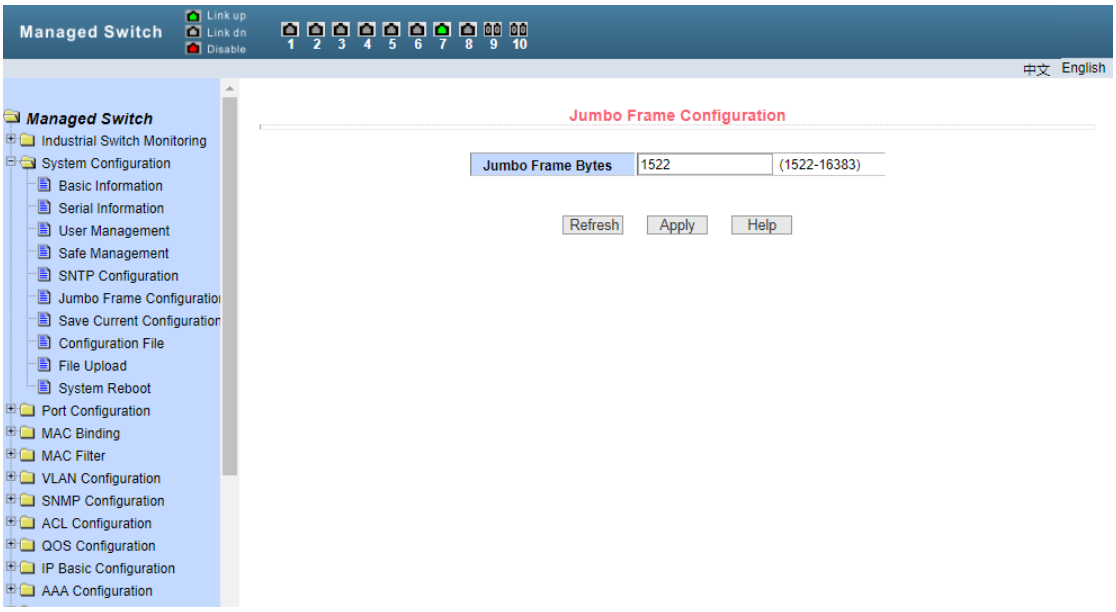


Figure 4-6 giant sail configuration interface

（7）Current　configuration

Figure 4-7 shows the current configuration page. Through this page, the user can view the current configuration of the switch. The save key stores the current configuration of the system into the configuration file. Because the memory operation needs to erase the flash chip, it takes a certain amount of time. When the user has made configuration on the page and hopes that the configuration will not be lost after restarting the switch, he must click the Save button in the current configuration page before exiting the page。

Figure 4-7 current configuration page

（8）Configuration file

Figure 4-8 shows the profile page. This page allows the user to view the initial

configuration of the system. The initial configuration is actually the configuration file in flash. When there is no configuration file in flash, the system starts with the default configuration. The delete key is used to delete the configuration file in flash. Click the delete key, a dialog box will pop up, and the dialog box will prompt the user whether to confirm to delete the configuration file. If yes, press the OK key on the dialog box, otherwise, press the cancel key. The download key is used to download the configuration file to the PC. Click the download button and a dialog box will pop up. The user can select the path of the save directory and save the configuration file. The file name of the downloaded configuration file is switch.cfg。

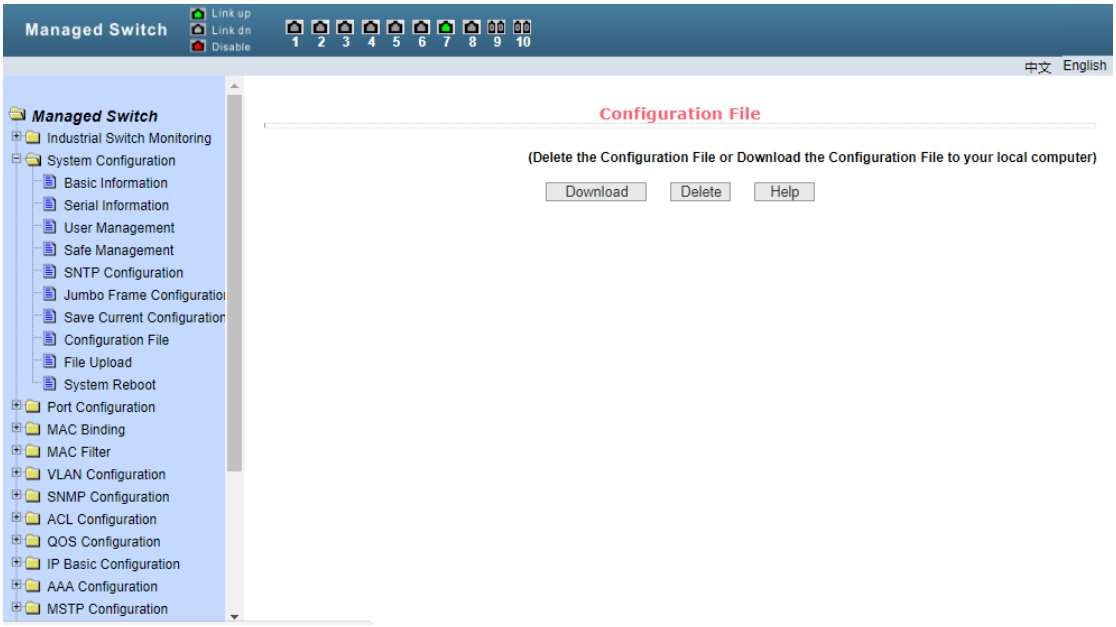


Figure 4-8 profile page

（8）File upload

Figure 4-9 shows the file upload page, through which users can upload configuration files and image files to the switch. Click Browse to select the directory path of the uploaded configuration file or image file on the PC. Click the upload button to upload the configuration file or image file. The suffix of the configuration file must be *. CFG, the image file must be provided by the manufacturer, and the file name suffix must be *. Img. Please do not click other pages or restart the switch before the transfer result page returns; otherwise, the file transfer will fail and the system will crash。

Figure 4-9 file upload page

（10）System reset

Figure 4-10 shows the system reset page through which the user restarts the switch.

When you click the restart button, a dialog box will pop up to prompt you whether you are sure to restart the switch. If you are sure, press OK, otherwise, press cancel. You will no longer be able to open web pages when you restart。

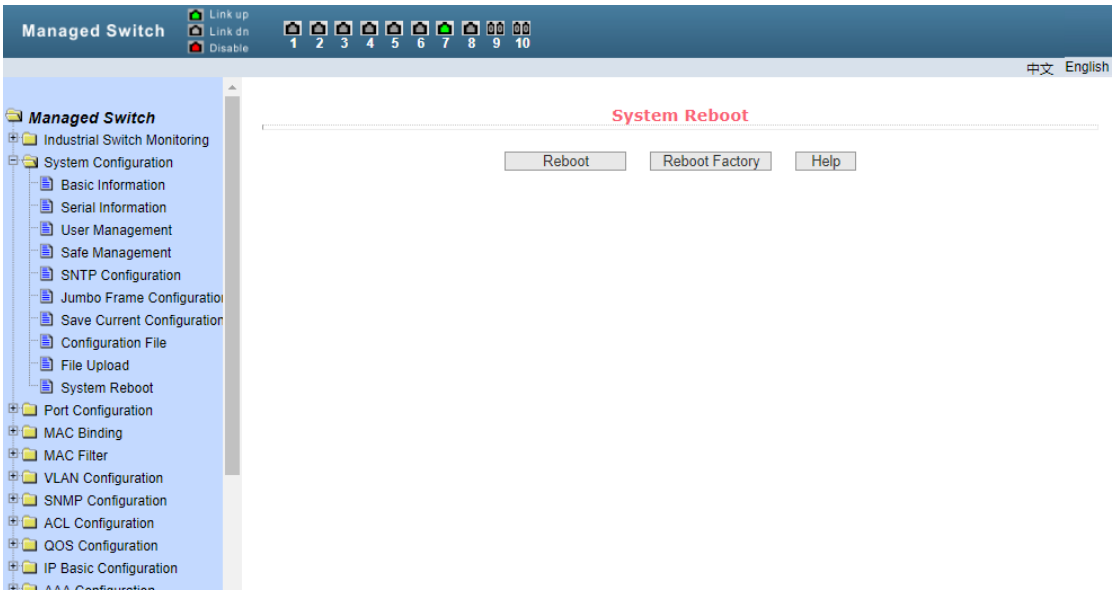


Figure 4-10 system reset page

5、Port configuration

（1）Universal port

Figure 5-1 shows the port configuration / port display page. Users can enable or disable ports, set port speed, or View basic information of all ports。

In order to set a specific port, the user needs to select the corresponding port name in the drop-down menu of the port. The port status is up by default. You can select down in the drop-down menu to disable the port. Users can also choose the drop-down menu of setting speed to set the speed of the port, such as forced half duplex 10m (half-10) for the port. Users can view other basic information of all ports through this page。

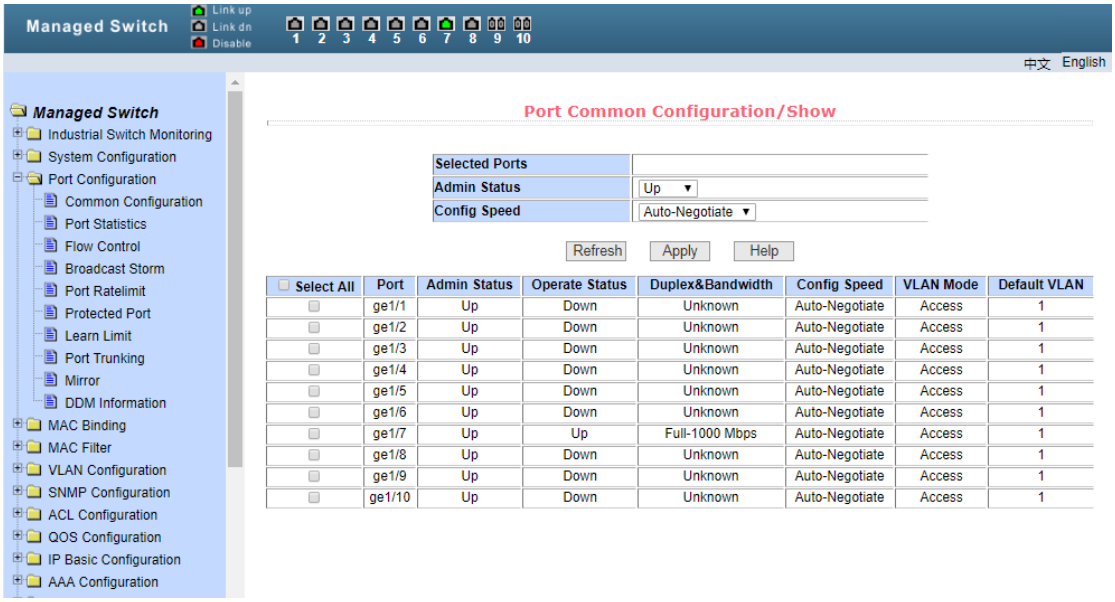


Figure 5-1 port configuration and port display page

（2）Port Statistics

Figure 5-2 shows the Port Statistics page. To view a specific port, the user needs to select the corresponding port name from the drop-down menu of the port. Users can view the statistical information of the port receiving and sending through this page。

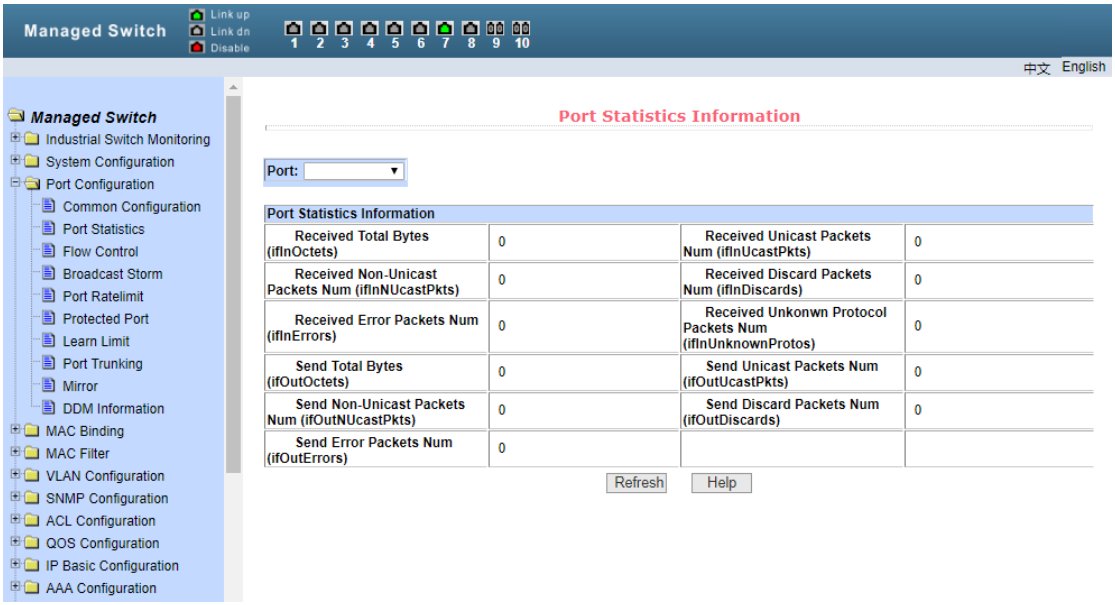


Figure 5-2 Port Statistics page

（3）Flow control

Figure 5-3 shows the flow control page. Users can open and close the flow control of each port through this page。

The flow control of a port can be turned on or off through the pull-down on or off of flow control. At the same time, you can view the flow control status of all ports through this page。

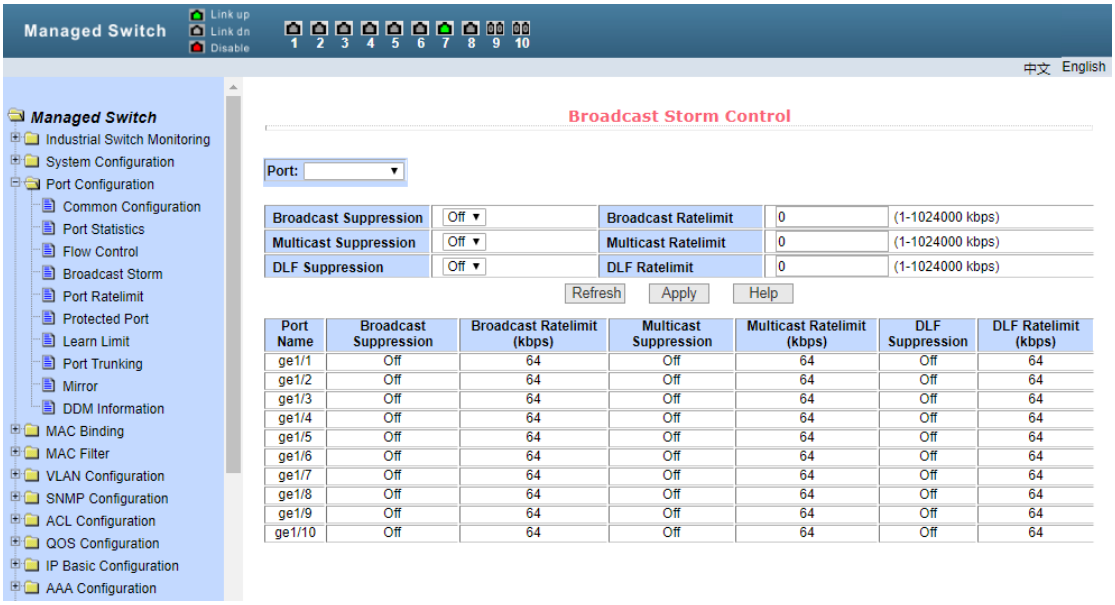


Figure 5-3 flow control page

（4）Broadcast storm

Figure 5-4 shows the broadcast storm control page. This page is used to configure the suppression function of broadcast packet, multicast packet and DLF packet。

Select the port you want to configure from the port drop-down bar. On and off are used to turn on and off the broadcast suppression, multicast suppression and DLF suppression. The inhibition rate item is used to configure the inhibition rate of the port, ranging from 1 to 1024000, in kbits. The rate of broadcast suppression, multicast suppression and DLF suppression is equal for the same port. At the same time, you can view the broadcast storm control configuration of all ports through this page。

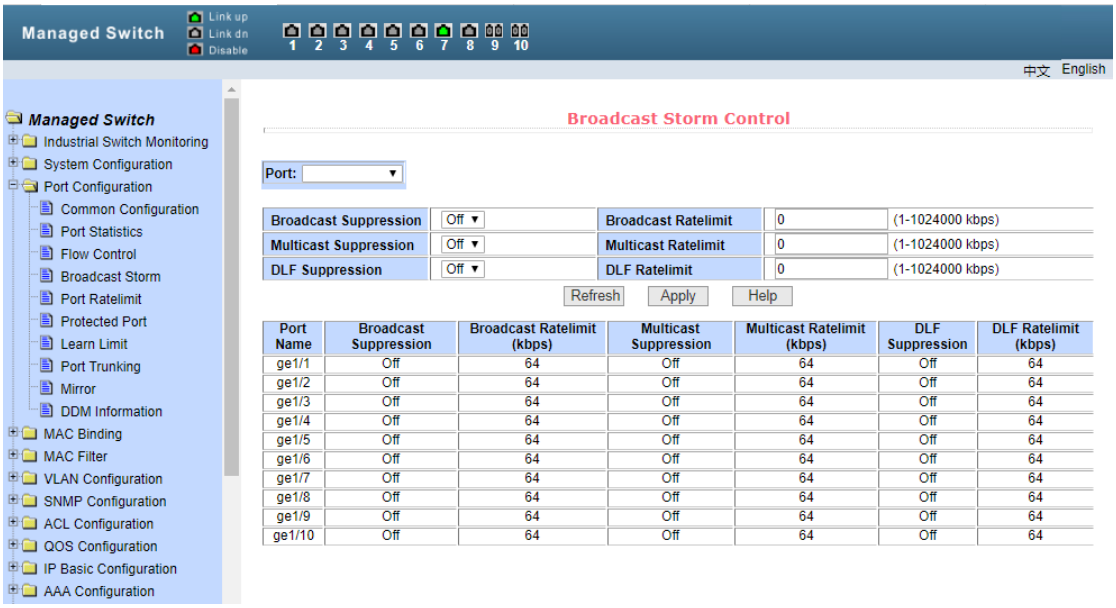


Figure 5-4 broadcast storm control page

（5）Port speed　limited

Figure 5-5 shows the port speed limit page. This page is used to configure the sending and receiving rate of the port。

Select the port you want to configure from the port drop-down bar. The bandwidth control of sending packets is used to configure and display the bandwidth control of sending packets. The range is 1-1024000, and the unit is kbits. After input, press the application key to take effect. If the port is not configured with bandwidth control, it is displayed as off. The corresponding cancel key is used to cancel the bandwidth control of sending packets. Received packet bandwidth control is used to configure and display the bandwidth control of received packets. The range is 1-1024000, and the unit is kbits. After input, press the application key to take effect. If the port is not configured with bandwidth control, it is displayed as off. The corresponding cancel key is used to cancel the bandwidth control of received packets。

If the port is configured with bandwidth control, it will be displayed in the list。

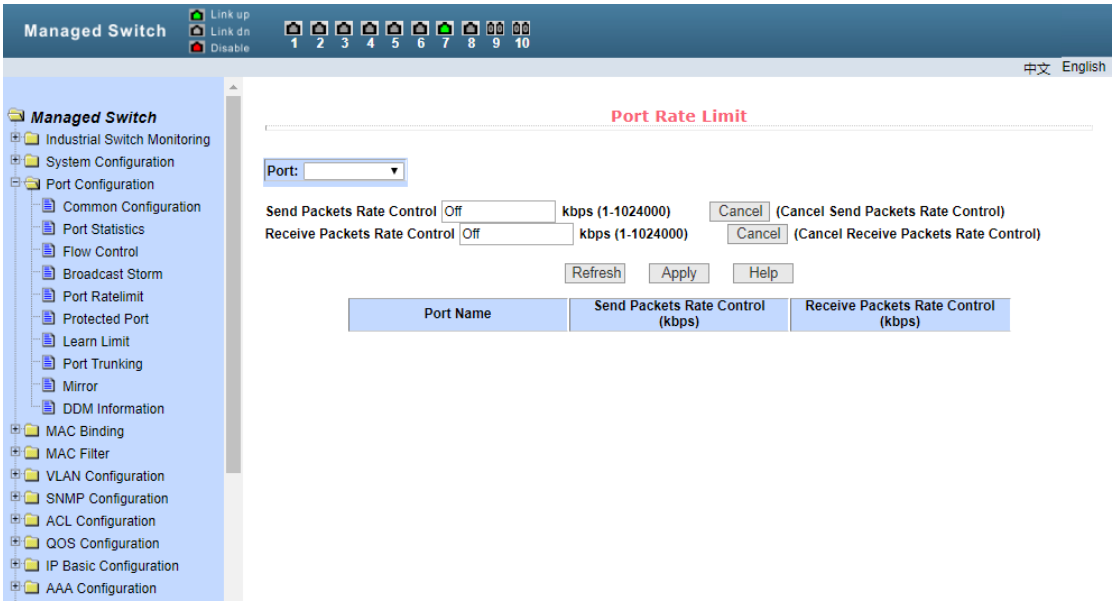


Figure 5-5 port speed limit page面

（6）Protection port

Figure 5-6 shows the protection port page. This page is used to configure the protection port。

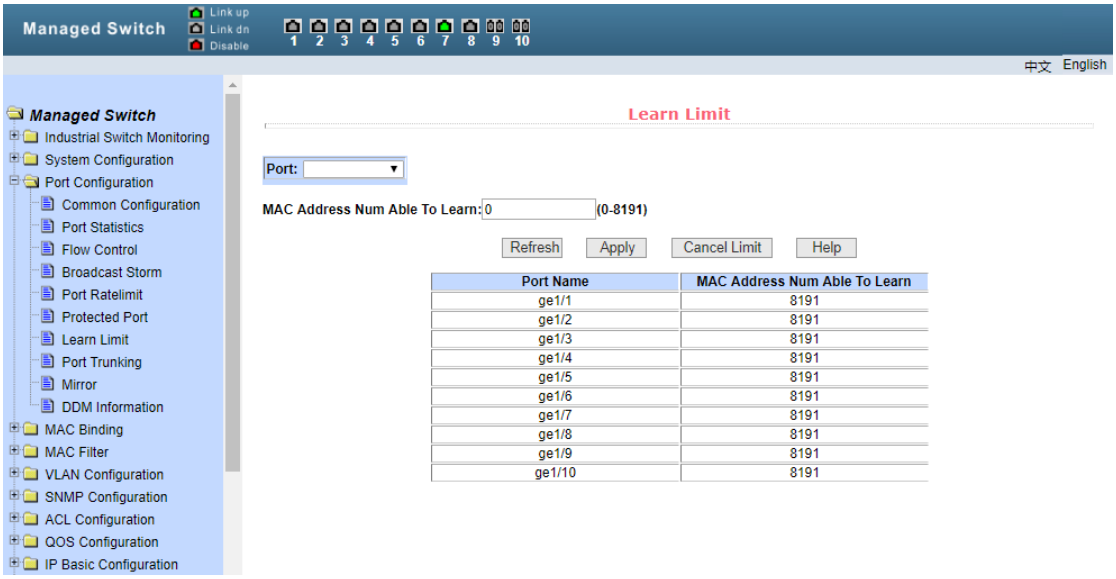


Figure 5-6 protection port page

（7）Learning restrictions

Figure 5-7 shows the port learning restriction page. This page is used to limit the number

of MAC addresses that the port can learn, and the range is 0-8191. The default value is 8191, which is also the maximum value, indicating that there is no learning limit configured for the port. The list shows the learning restrictions for all ports。

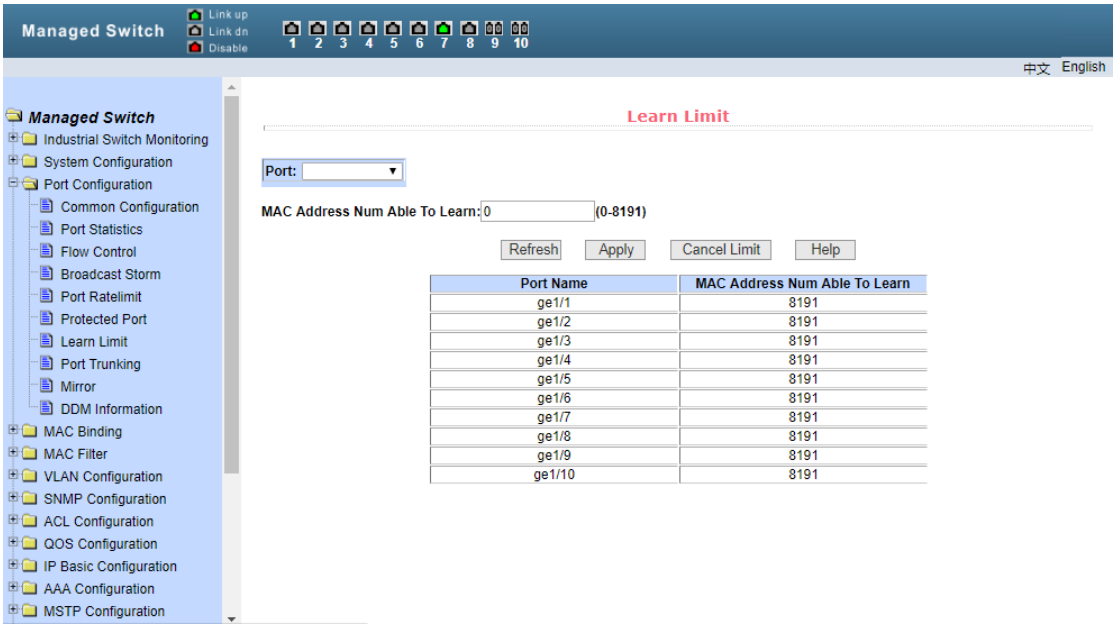


Figure 5-7 port learning restriction page

（8）Link aggregation

Figure 5-8 shows the port aggregation configuration page. This page allows the user to configure port aggregation. The page consists of four parts: trunk group ID selection, port aggregation method, configurable port and group member port。

In order to create or modify port aggregation, users need to select a trunk group ID from 1 to 8. The user clicks the corresponding trunk group ID in the list box, and the information of the trunk group is displayed in the group member port. To create a trunk group, select the corresponding ID in the trunk group ID and click "create trunk group". If the creation is successful, the created group will be marked with brackets in the ID display bar. If a trunk group is not created, it will be marked with brackets in the ID display bar. To set the port aggregation method, select an aggregation method from the drop-down box above the list, and click Set aggregation method. To add an aggregated port, select the aggregated port from the configurable ports and click the "member port = >" key. To delete a port from the existing aggregated ports, select the aggregated port from the group member ports and click the "non member port < =" key. To delete the entire trunk group, click the "delete trunk group" button。

In the process of page configuration, the configured aggregation method corresponds to the selected trunk group ID, and only the existing trunk group can configure the aggregation method; only the existing trunk can add or delete member ports; only when there is no member port can a trunk group be deleted。

The switch provides six port aggregation modes: Based on source MAC address, based on destination MAC address, based on source and destination MAC address, based on source IP address, based on destination IP address, based on source and destination IP address。

Managed switch supports up to 8 groups of port aggregation. Each group of port

aggregation supports up to 8 ports. Each trunk group can configure its own port aggregation method。

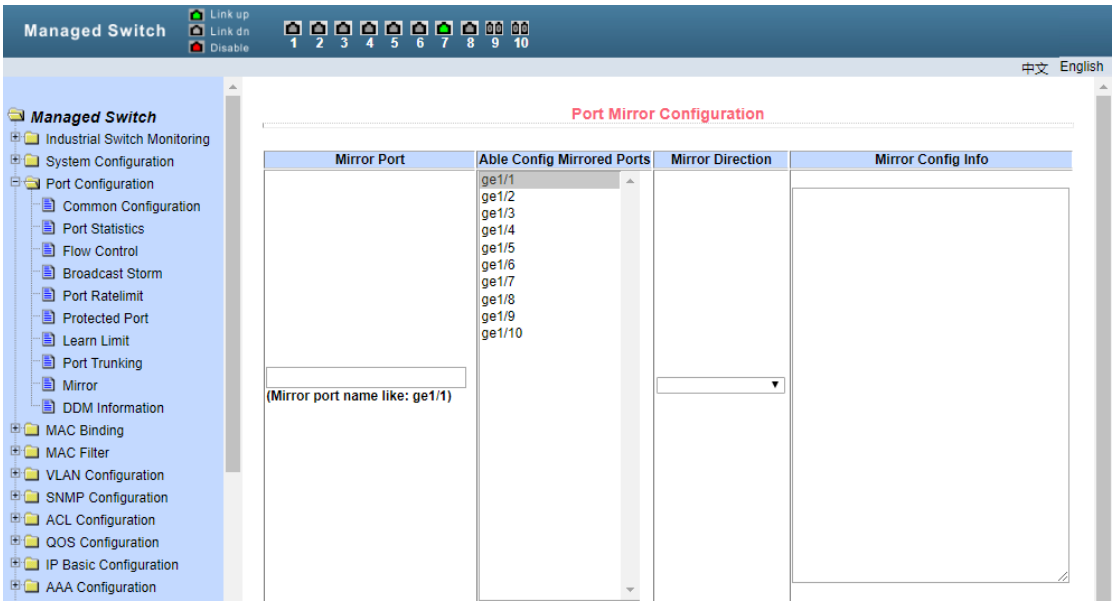


Figure 5-8 port aggregation configuration page

（9）Port Mirror

Figure 5-9 shows the port image configuration page, which allows users to configure port images. Port mirroring is used to monitor the output packets of the mirrored output port and the input packets of the mirrored input port. Only one mirror port can be selected, while multiple mirror output ports and mirror input ports can be selected. The page consists of four parts: monitoring port, configurable port, monitoring direction and image configuration information. When configuring an image port, first configure the image port from the listening port. There can only be one image port. Then select the mirrored port from the configurable ports, select the listening direction from the listening direction, and finally press the application key to take effect. The result will be displayed in the image configuration information。

When receive in the monitoring direction is selected, it means to monitor the received packets, transmit means to monitor the sent packets, both means to monitor all the sent and received packets, not_ Receive means to cancel listening to the received packets, not_ Transmit means to cancel the monitoring of the sent packets, neither means to cancel the monitoring of the received and sent packets, that is, to cancel the monitored port`。

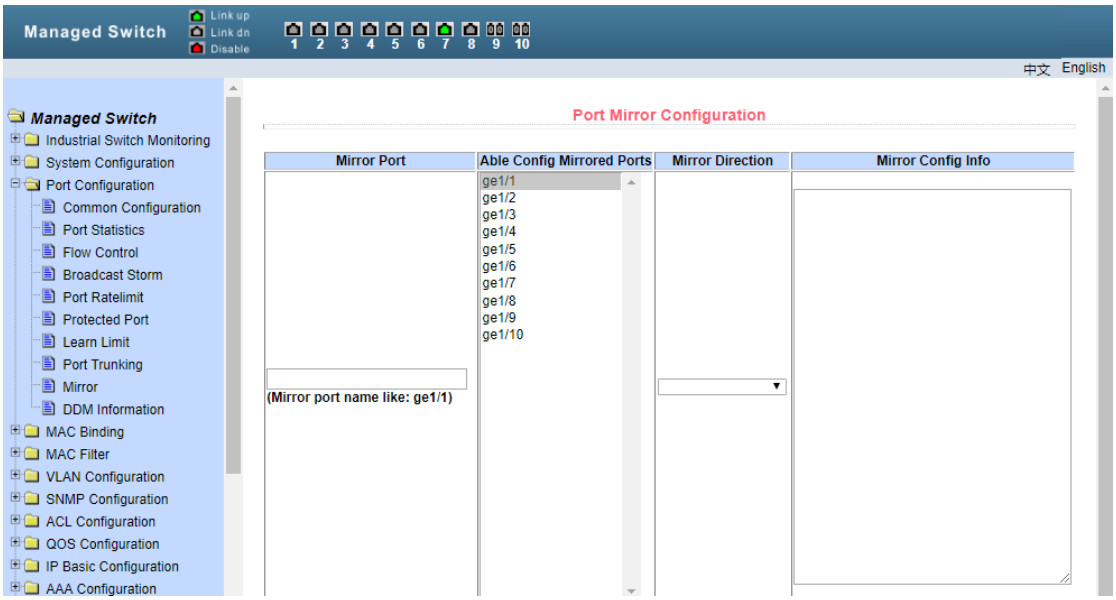


Figure 5-9 port image configuration page

（10）DDM information

Figure 5-10 shows the DDM display interface, which allows the switch to obtain port DDM information。

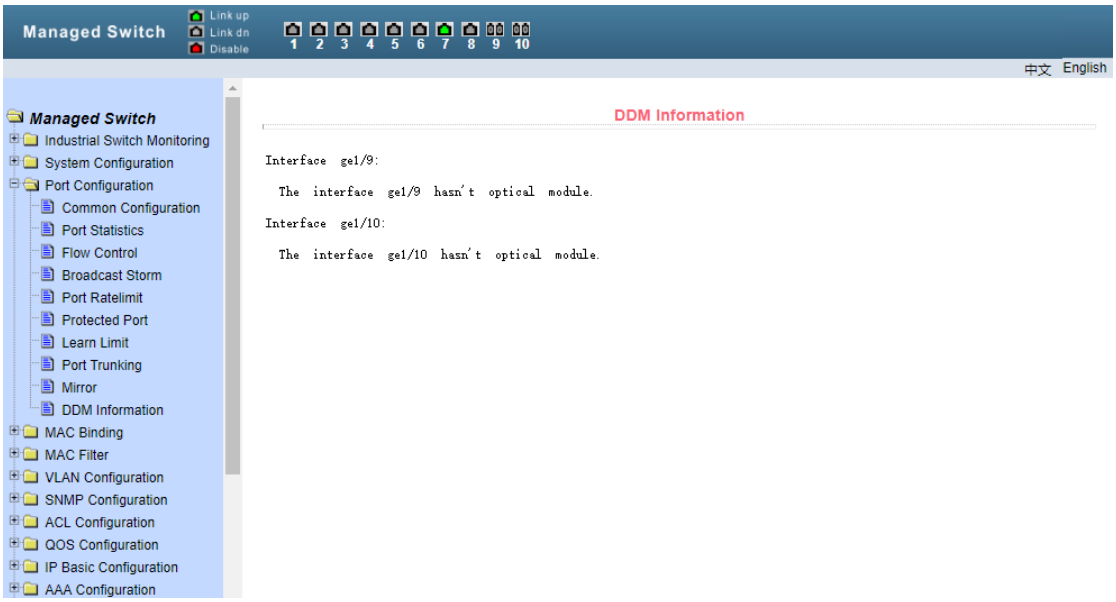


Figure 5-10 DDM display interface

6、MAC binding

（1）Mac binding configuration

Figure 6-1 shows the MAC binding configuration page. This page is used to realize the binding of port and MAC address。

The MAC item on the page is used to enter the bound MAC address, and the VLAN ID

item is used to enter the VLAN to which the MAC address belongs。

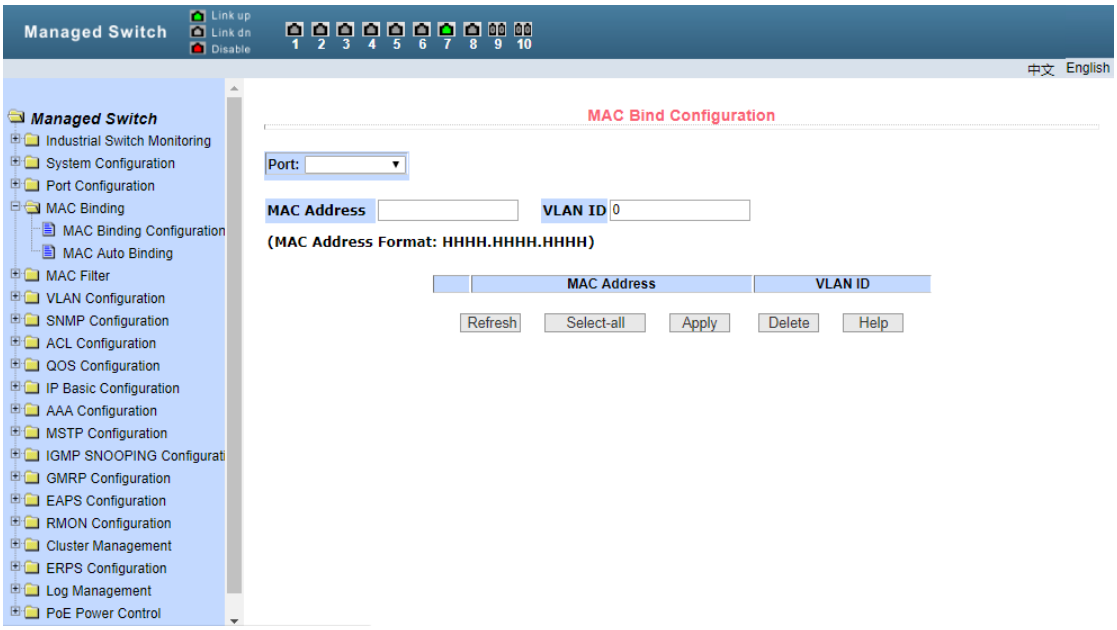


Figure 6-1 MAC binding configuration page

（2）Automatic conversion of MAC binding

Figure 6-2 shows the MAC binding automatic conversion page. This page is used to realize the port automatic binding MAC address。

Display the existing dynamic MAC address and VLAN of the port in the layer 2 hardware forwarding table. You can select one of the entries and convert it to a static binding。

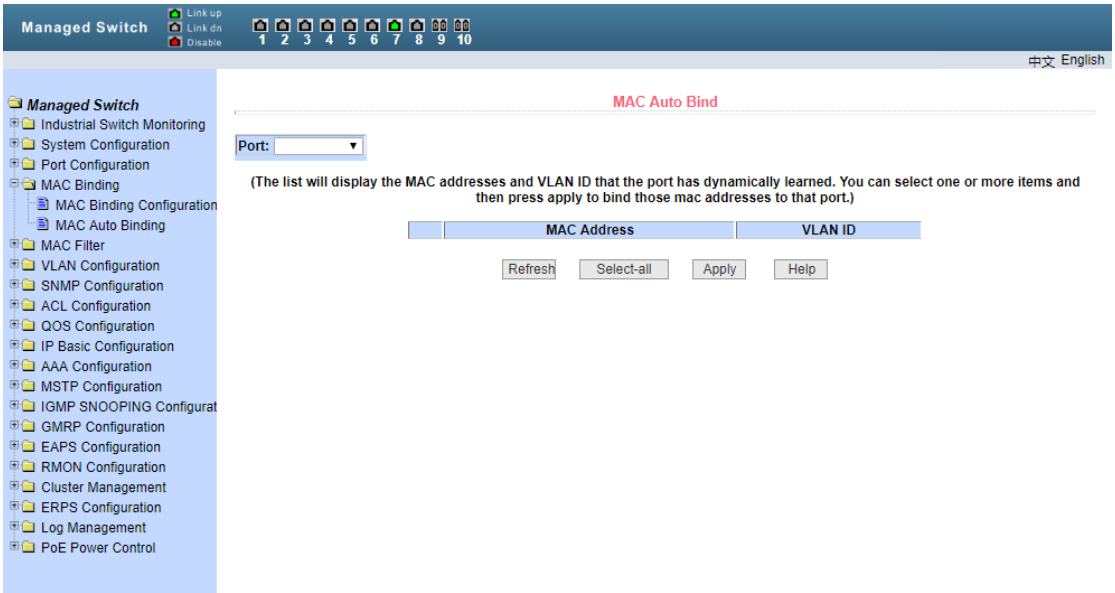


Figure 6-2 MAC binding automatic conversion page

7、MAC filter

（1）MAC Filter configuration

Figure 7-1 shows the MAC filter configuration page. This page is used to configure the filtering of MAC address by port。

The MAC item on the page is used to enter the filtered MAC address, and the VLAN ID item is used to enter the VLAN to which the MAC address belongs。

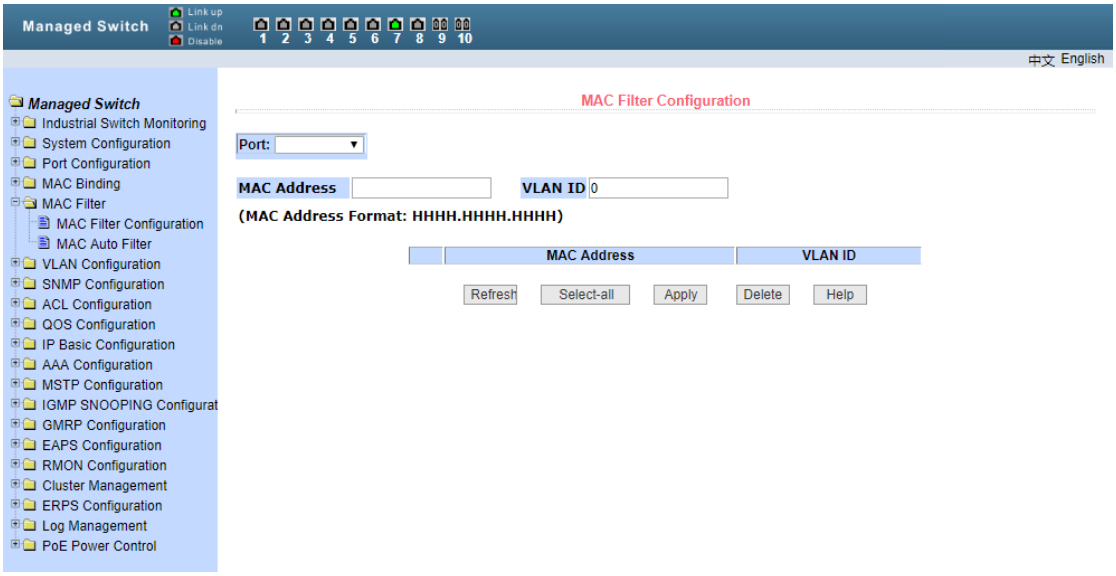


Figure 7-1 MAC filter configuration page

（2）Automatic conversion of MAC filter

Figure 7-2 shows the MAC filter automatic conversion page. This page is used to realize the port automatic binding MAC address。

Display the existing dynamic MAC address and VLAN of the port in the layer 2 hardware forwarding table. You can select the entries and convert them to a static filtering configuration。

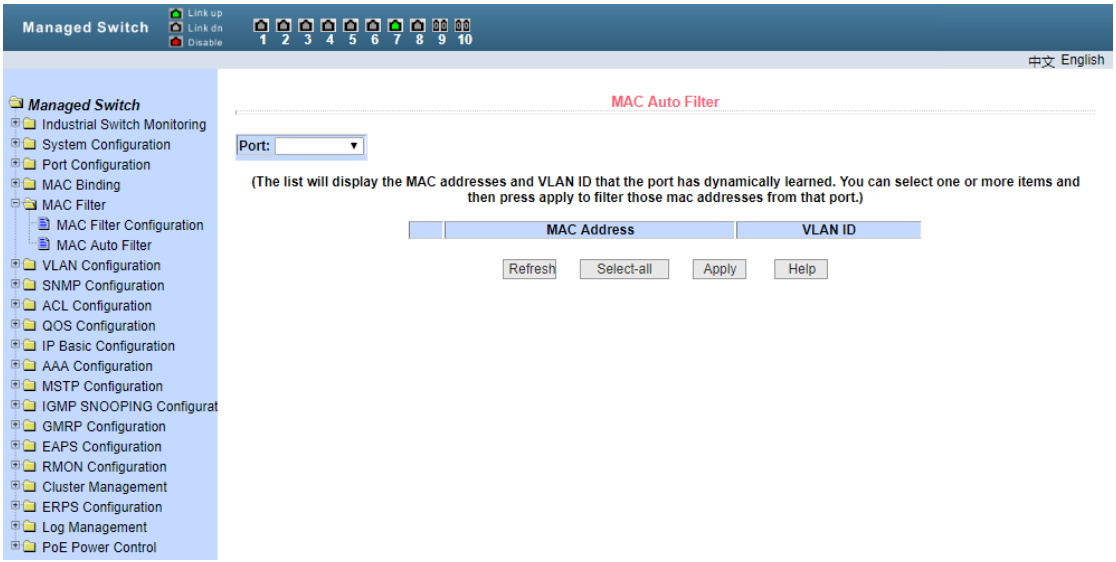


Figure 7-2 MAC filter automatic conversion page

8、VLAN Configuration

（1）VLAN infomation

Figure 8-1 shows the current VLAN information page. This page is read-only and displays the current VLAN, VLAN status and VLAN port members. All current VLANs will be displayed in the drop-down box, and the vid, status and port members of up to 30 VLANs will be displayed in the list. Select a VLAN from the drop-down box, and the information of up to 30 VLANs with vid greater than the VLAN will be displayed in the list. However, if there are no more than 30 VLANs, no matter which VLAN is selected from the drop-down box, the information of all VLANs will be displayed in the list。

A port may not be a VLAN member, it may be a tagged or untagged VLAN member. The meaning of the characters before the port of the page is as follows：

t tagged The port is a tagged member of this VLAN

u untagged The port is an untagged member of this VLAN

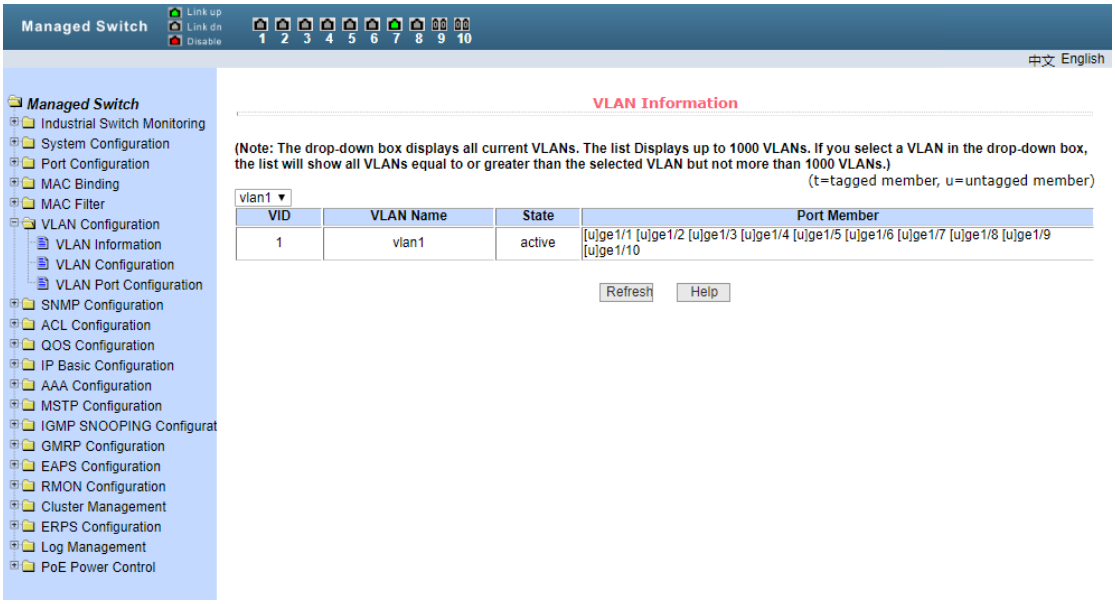


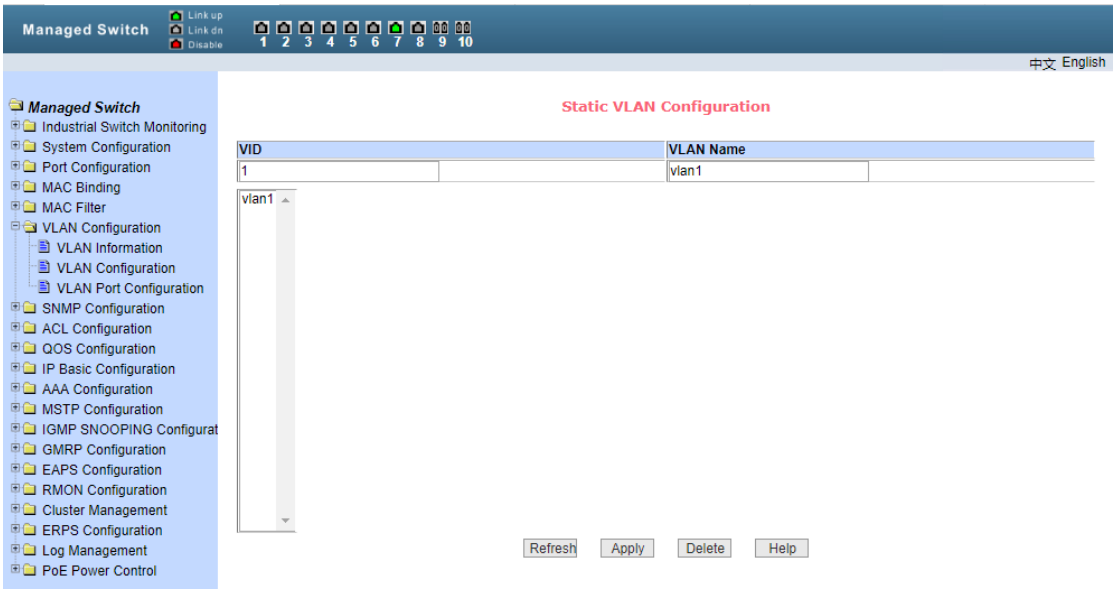
Figure 8-1 VLAN information page

（2）VLAN configuration

Figure 8-2 shows the static VLAN configuration page, which allows users to create VLAN。

If you want to create a new VLAN, the user enters vid in the active line, ranging from 2 to 4094. VLAN name is generated by the system according to VLAN ID and cannot be modified. Click the application key, and the list box will display the vid and VLAN name of the VLAN created by the user. The switch creates vlan1 by default, and vlan1 cannot be deleted。

If you want to delete a VLAN, you need to click the corresponding VLAN in the list box. The VLAN will be displayed in the active line. Click Delete to delete the VLAN. Meanwhile, the VLAN information will be removed from the list box。



（3）VLAN Port　configuration

Figure 8-3 shows the VLAN port configuration page, which is used to configure VLAN on the port and display the configuration results. This page is mainly composed of eight parts: port, mode, all current VLANs, VLAN of the port, key "default VLAN = >", "tagged = >", "untagged = >" and "non member < =".

Port is the port that specifies the VLAN to be configured。

Mode access specifies that the VLAN mode of the port is access mode. In this VLAN mode, the port is the untagged member of vlan1 by default, and the default VLAN of the port is 1. Hybrid specifies that the VLAN mode of the port is hybrid mode. In this VLAN mode, the port is the untagged member of vlan1 by default, and the default VLAN of the port is 1. Trunk specifies that the VLAN mode of the port is trunk mode. In this VLAN mode, the port is the tagged member of vlan1 by default, and the default VLAN of the port is 1。

All current VLANs refer to the currently created VLANs, which can be configured by ports. Users can select multiple VLANs from the list。

The VLAN of the port shows the result of VLAN port configuration, [P] indicates that the VLAN is the default VLAN of the port, [t] indicates that the port is a tagged member of the VLAN, [u] indicates that the port is a non tagged member of the VLAN. When deleting VLAN, users can select VLAN from the list。

Press "default VLAN = >" to configure the default VLAN of the port and select a VLAN from all the current VLANs。

Press "tagged = >" to configure that the port is a tagged member of the specified VLAN, and select one or more VLANs from all the current VLANs。

Press "untagged = >" to configure that the port is the untagged member of the specified VLAN, and select one or more VLANs from all the current VLAN。

Press "non member < =" to delete the port from the specified VLAN or VLANs. Instead of

being a member of these VLANs, select one or more VLANs from the VLANs to which the port belongs。

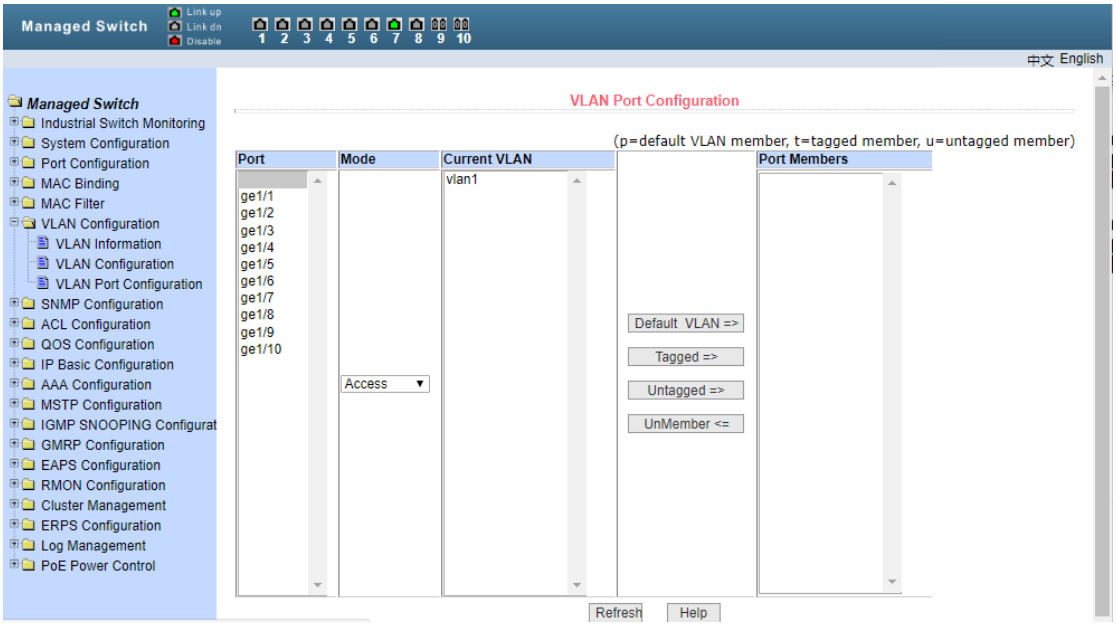


Figure 8-3 VLAN port configuration page

9、SNMP Configuration

（1）Community name

Figure 9-1 shows the SNMP community configuration page, which allows users to configure the name and read-write permissions of the common body of the switch. A total of 8 entries can be configured。

By default, the switch has a common body with a public name, which is read-only. Correspondingly, there is only one active entry on the page, the common body name is public, and the permission is read-only. When the switch needs to be managed by SNMP, it needs to configure a common body with read and write permissions。

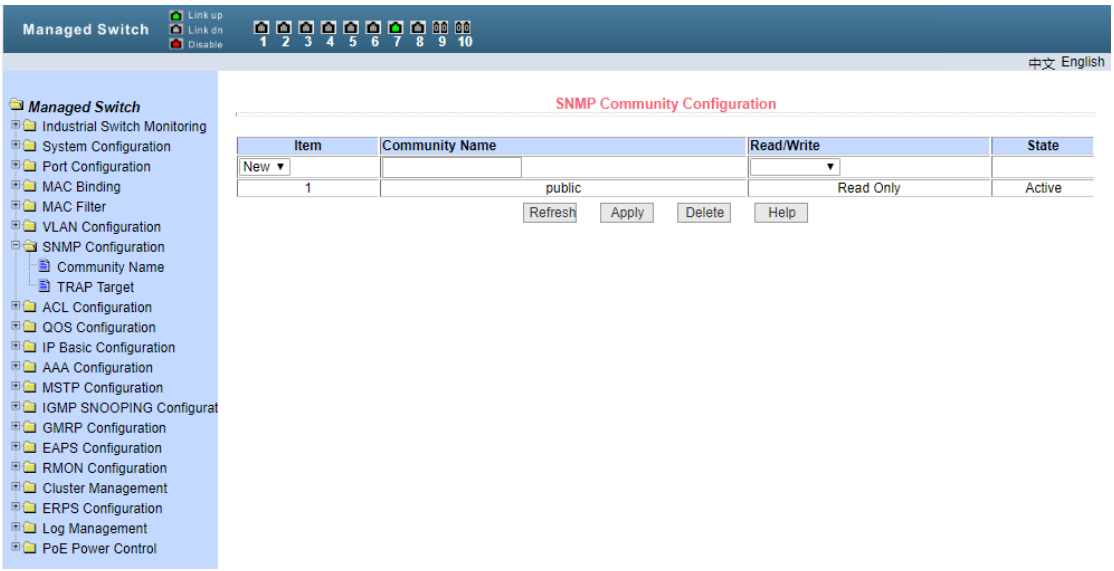


Figure 9-1 SNMP community configuration page

（2）TRAP Target

Figure 9-2 shows the trap target configuration page, which allows the user to configure the IP address of the workstation receiving the trap message and some parameters of the trap protocol package。

When configuring an entry, the name is used to enter the trap name, the transport IP address is used to enter the destination address, and the SNMP version is used to select the version of the trap package. If the setting is successful, the status in the entry will be displayed as active. If the configuration is successful, the SNMP trap function will work. In case of link up or link down, the switch will automatically send trap packets to the target address。

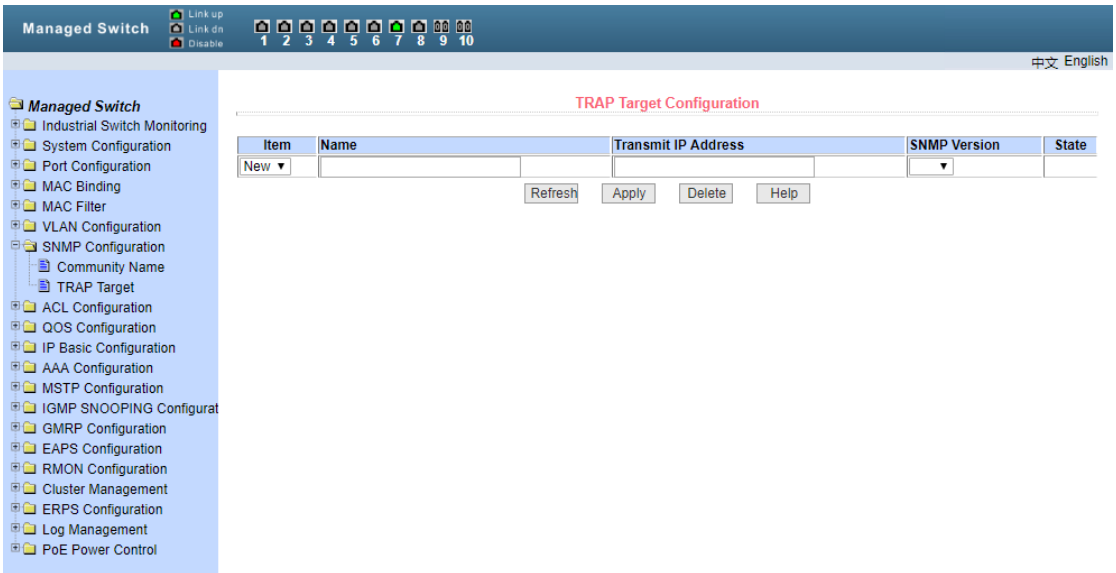


Figure 9-2 trap target configuration page

10、ACL Configuration

（1）Standard IP

Figure 10-1 shows the ACL standard IP configuration page, through which users can establish the rule base of ACL standard IP. Users can select an ACL group number (range 1-99, or 1300-1999) to create one or more rules in the group. The only fields that can be matched in a rule are the source IP address (masked)。

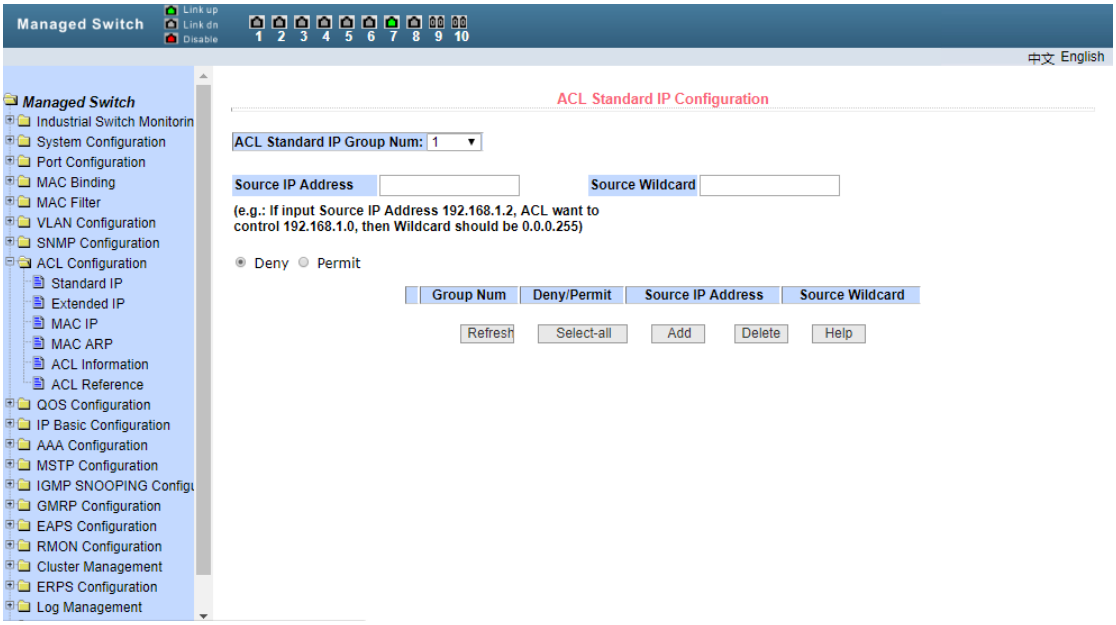


Figure 10-1acl standard IP configuration page

When users configure rules, the source IP address needs to be masked, and the rules can match the set of IP addresses. The mask of address is represented by inverse code. If the rules want to match the IP address range from 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1, and the mask is 0.0.0.255。

When users configure rules, each rule must have a filtering mode: allow or reject。

When users create a rule in a rule group, the system will automatically give the rule a rule number. When a rule in a rule group is deleted, other rules will remain unchanged, and the system will automatically sort the rules in a rule group. If you want to delete the whole rule group, you can first select all, and then click delete。

（2）Extend IP

Figure 10-2 shows the ACL extended IP configuration page, through which users can establish the rule base of ACL extended IP. Users can select an ACL group number (range 100-199, or 2000-2699) to create one or more rules in the group. The fields that can be matched in a rule are source IP address (masked), destination IP address (masked), protocol type (such as ICMP, TCP, UDP, etc.), source port and destination port (only valid for TCP and UDP protocols), TCP control flag。

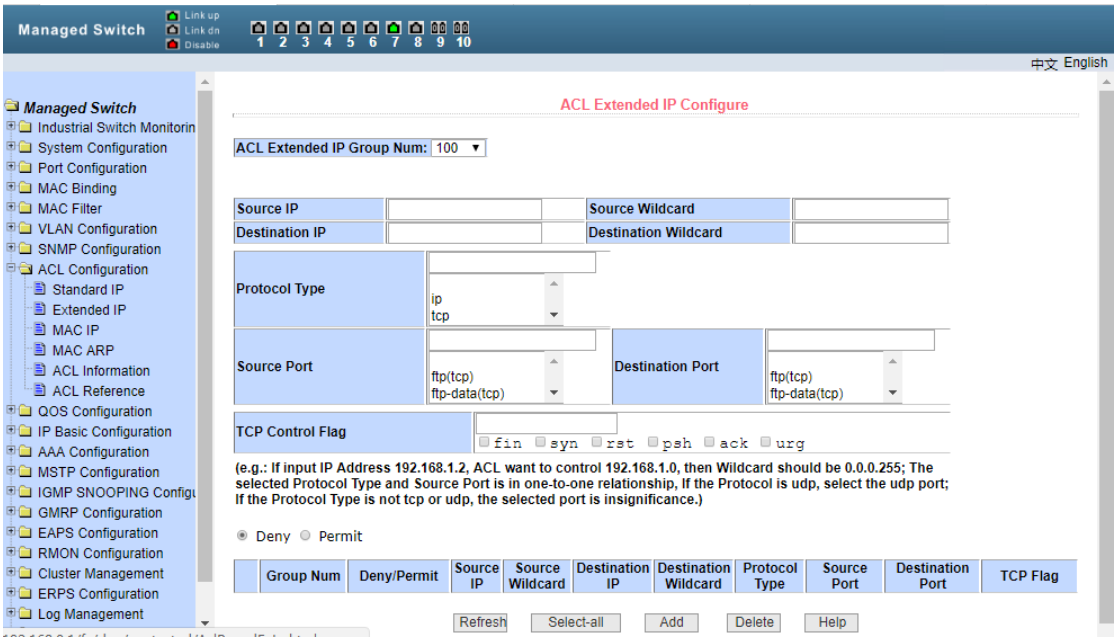


Figure 10-2 ACL extended IP configuration page

When users configure rules, both source IP address and destination IP address need to be masked. Rules can match the set of IP addresses. The mask of address is represented by inverse code. If the rules want to match the IP address range from 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1 and the mask is 0.0.0.255。

When users configure rules, each rule must have a filtering mode: allow or reject。

When users create a rule in a rule group, the system will automatically give the rule a rule number. When a rule in a rule group is deleted, other rules will remain unchanged, and the system will automatically sort the rules in a rule group. To delete the whole rule group, you can first select all, and then press the delete key。

（3）MAC IP

Figure 10-3 shows the ACL MAC IP configuration page, through which users can establish ACL MAC IP rule base. Users can select an ACL group number (ranging from 700 to 799) to create one or more rules in the group. The fields that can be matched in a rule are active MAC address (with address matching bit), source IP address (with address matching bit), destination IP address (with address matching bit), VLAN ID。

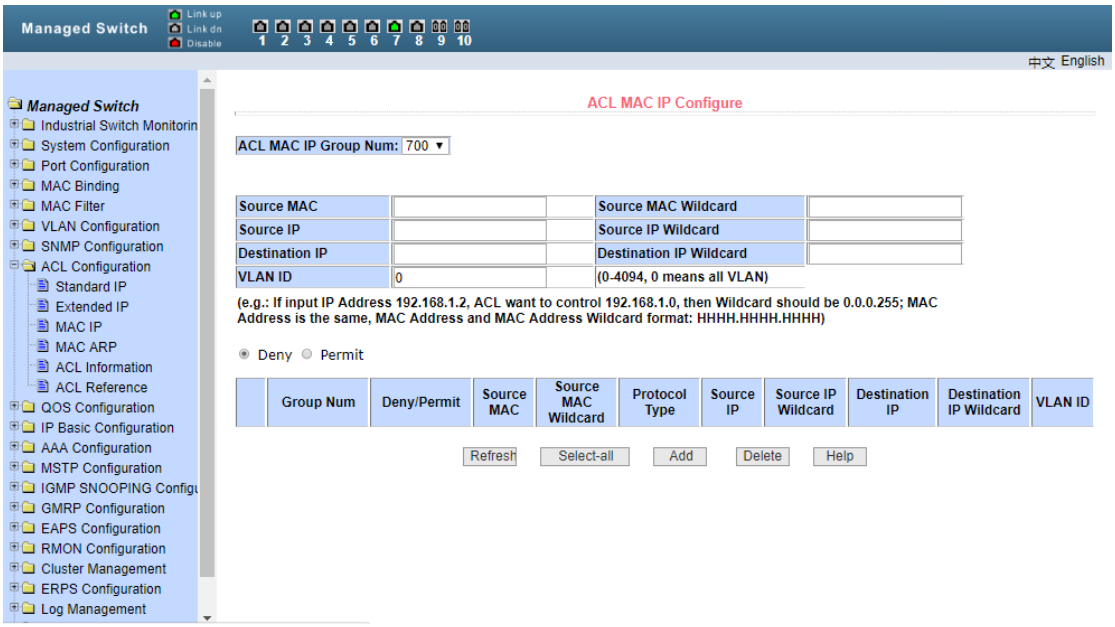


Figure 10-3 ACL MAC IP configuration page

When users configure rules, source MAC address, source IP address and destination IP address all need address matching bits. Rules can match the set of MAC address and IP address. For example, if the rule wants to match the IP address range 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1 and its mask is 0.0.0.255。

When users configure rules, each rule must have a filtering mode: allow or reject。

When users create a rule in a rule group, the system will automatically give the rule a rule number. When a rule in a rule group is deleted, other rules will remain unchanged, and the system will automatically sort the rules in a rule group. To delete the whole rule group, you can first select all, and then press the delete key。

When users configure rules, VLAN ID must be in the range of 0 to 4094, including 0 and 4094, where 0 represents all users。

（4）MAC ARP

Figure 10-4 shows the ACL MAC ARP configuration page, through which users can establish the ACL MAC ARP rule base. Users can select an ACL group number (ranging from 1100 to 1199) to create one or more rules in the group. The fields that can be matched in a rule are send MAC address (with address matching bit) and send IP address (with address matching bit)。

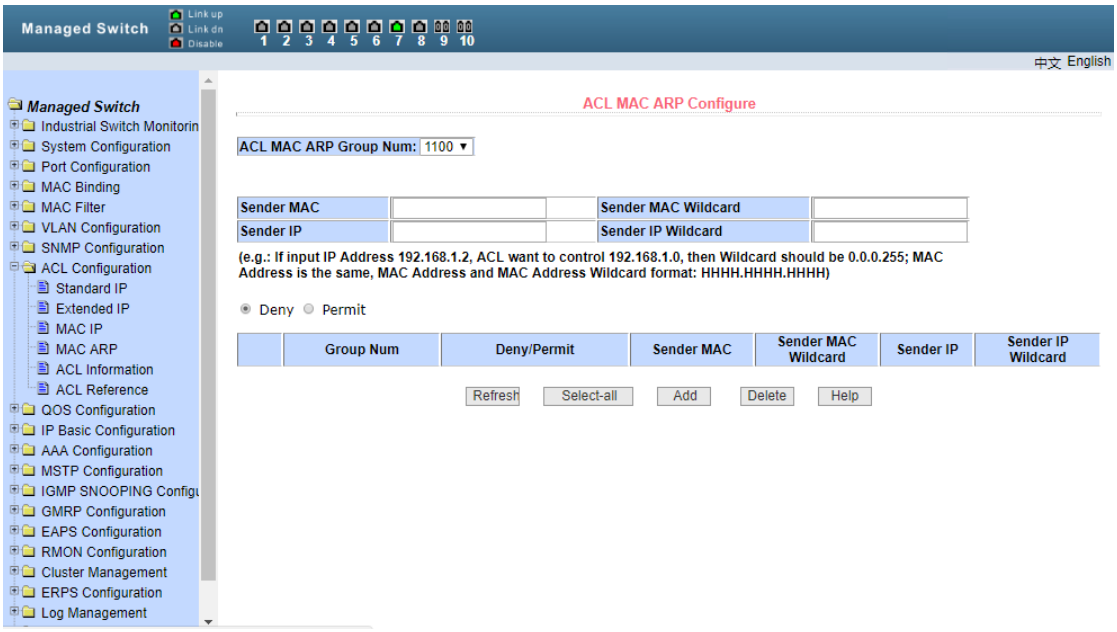


Figure 10-4 ACL MAC ARP configuration page

When the user configures the rules, both the sending MAC address and the sending IP address need address matching bits. The rules can match the set of MAC address and IP address. For example, if the rule wants to match the IP address range 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1 and its mask is 0.0.0.255。

When users configure rules, each rule must have a filtering mode: allow or reject。

When users create a rule in a rule group, the system will automatically give the rule a rule number. When a rule in a rule group is deleted, other rules will remain unchanged, and the system will automatically sort the rules in a rule group. To delete the whole rule group, you can first select all, and then press the delete key。

（5）Repository information

Figure 10-5 is the ACL repository information page, which displays all the rules and reference information configured in the current ACL。

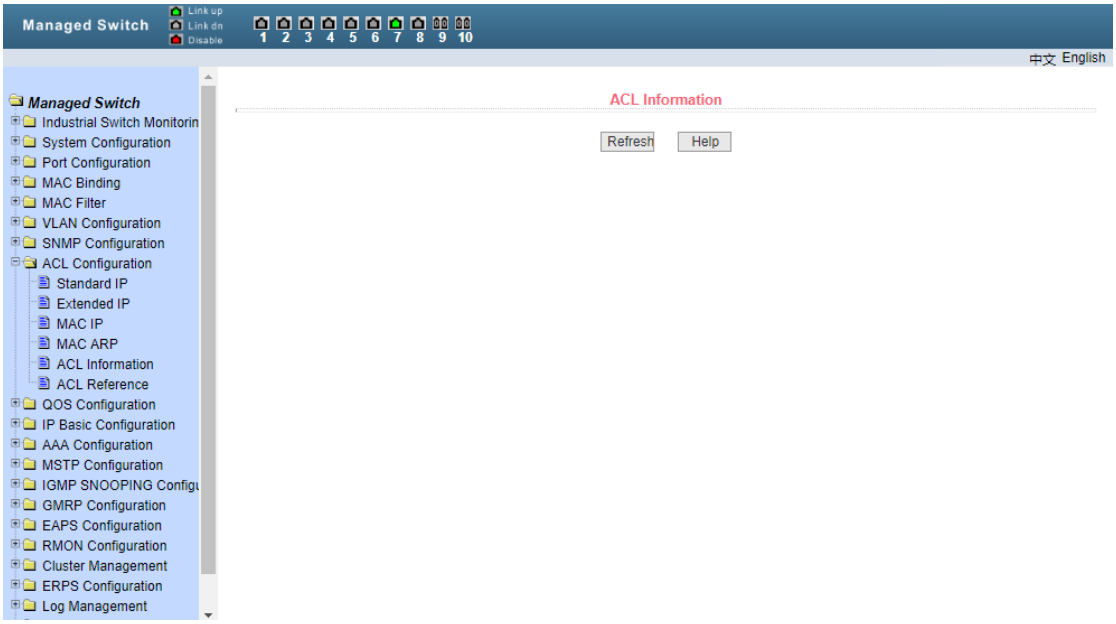


Figure 10-5 ACL repository information page

（6）ACL quote

Figure 10-6 is the ACL reference configuration page. Users can select an ACL rule group for a port through this page, and write the rules in the ACL rule group into the port hardware logic, so that the port can perform ACL filtering on the received packets according to these rules。

When selecting ACL rule groups for ports, you can select IP standard, IP extension, MAC IP, and MAC ARP ACL groups. The selected ACL rule group must exist. Select from the list of ACL rule groups and press the add key. To delete an ACL rule group, select an ACL rule group from the list of referenced rule groups and press the delete key。

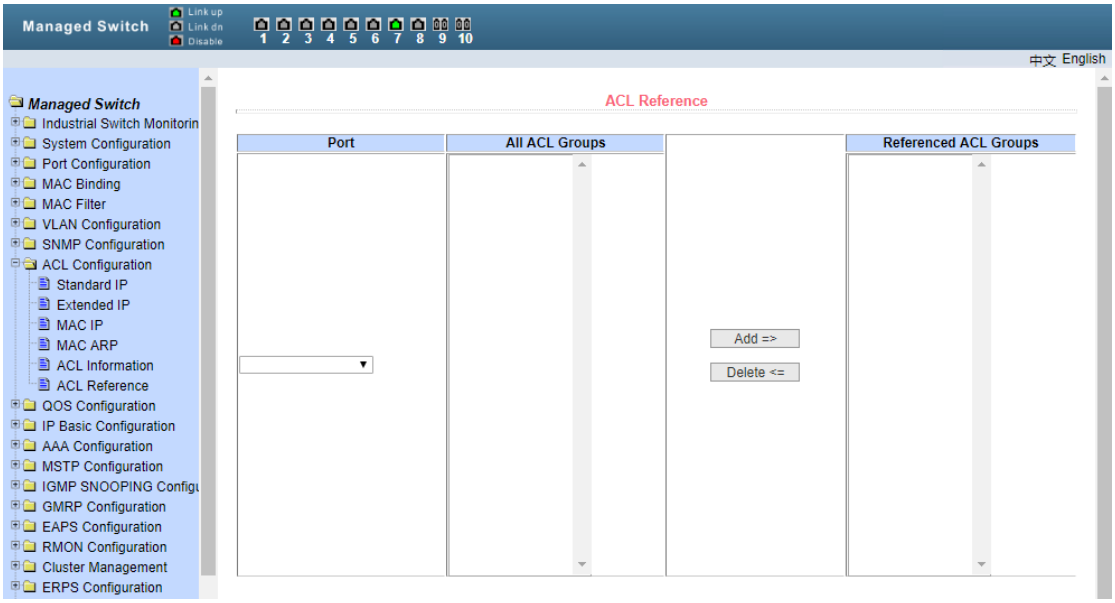


Figure 10-6 ACL reference configuration page

11、Qos Configuration

（1）Qos Application

Figure 11-1 shows the QoS application page, through which users can configure the QoS type of the port and modify the default user priority. The list is the real-time display port QoS type and user default priority。

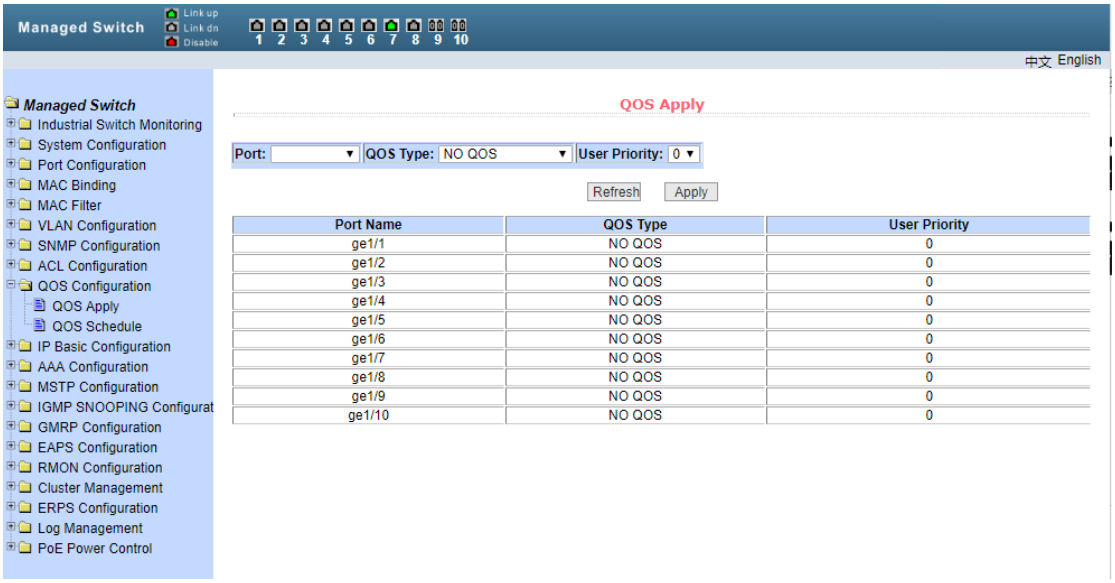


Figure 11-1 QoS application page

（2）Qos dispatch

Figure 11-2 shows the QoS scheduling page, through which users can configure the port QoS scheduling mode and modify the priority of the queue. The list shows the scheduling mode of the port and the weight value of each queue in real time。

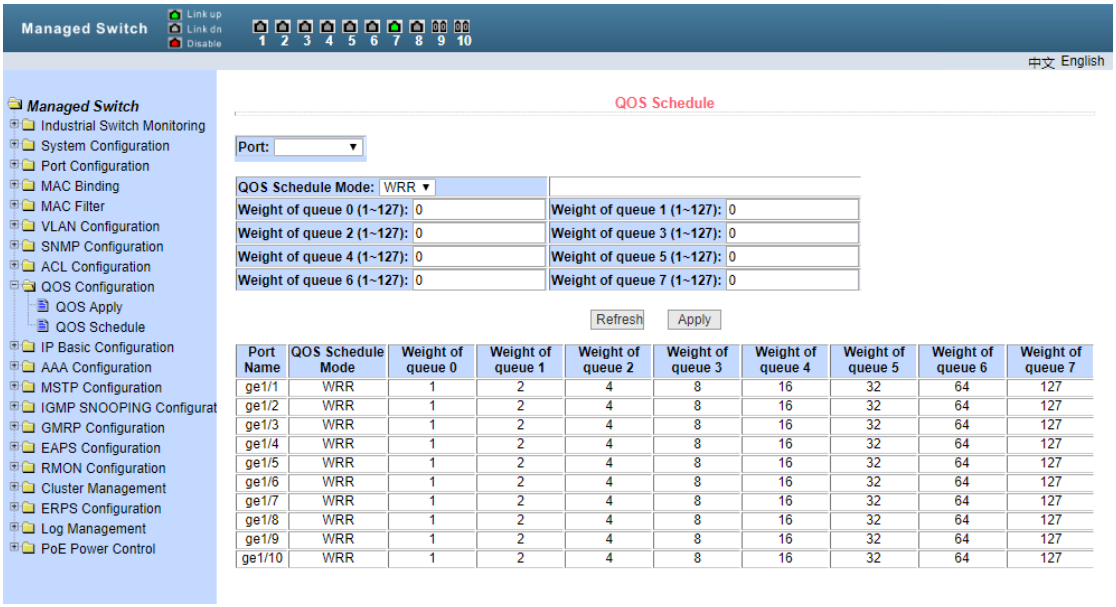


Figure 11-2 QoS scheduling page

12、IP basic information

（1）VLAN port

Figure 12-1 is the VLAN interface configuration page. Users can configure VLAN interface, delete VLAN interface, configure IP address of interface, delete IP address of interface and view interface information through this page. VLAN can only be set as an interface when it already exists, and the interface address can only be configured on the set interface。

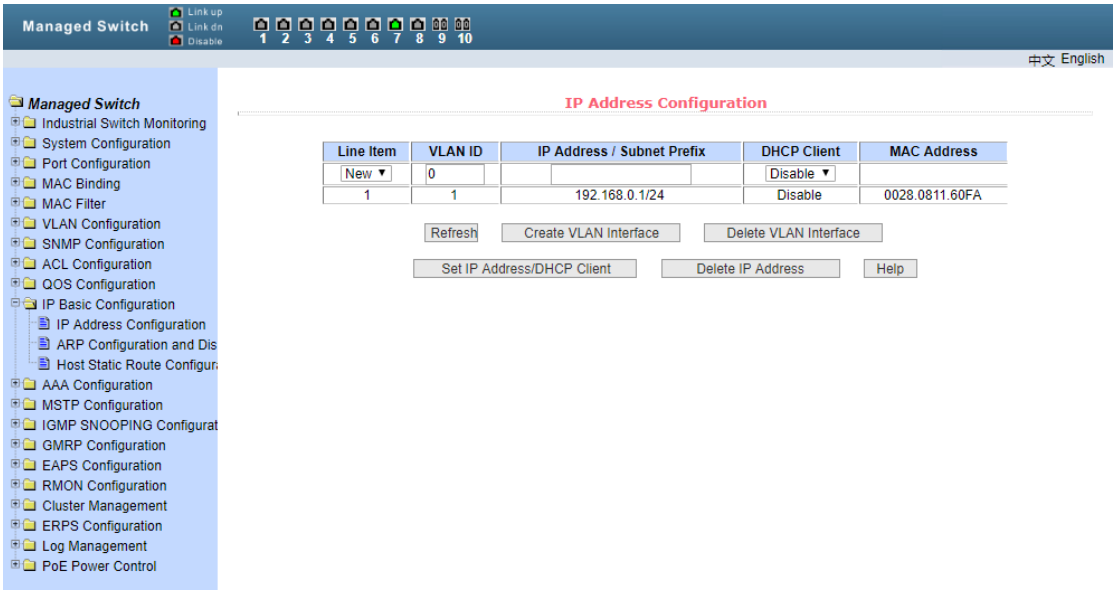


Figure 12-1 VLAN interface configuration page

The management switch has a vlan1 interface by default, which cannot be deleted. Only

one interface can be configured for a VLAN。

（2）ARP configuration and display

Figure 12-2 is the ARP configuration and display page. This page can display all the information of ARP table of the switch. At the same time, users can configure static ARP entries, delete ARP entries, and modify dynamic ARP entries to static ARP entries through this page。

When users configure a static ARP entry, they need to input IP address and MAC address. The MAC address must be unicast MAC address, and then click Add。

When deleting an ARP entry, users can choose to delete an IP ARP entry, a network segment ARP entry, all ARP entries, all dynamic ARP entries and all static ARP entries. To delete an ARP entry of an IP or a ARP entry of a network segment, enter the specified IP address or IP network segment in the input box. Click the delete button again。

When a dynamic ARP entry is changed to a static ARP entry, you can choose to change all or all the dynamic ARP entries in a network segment to a static ARP entry. For a network segment, you need to enter the specified network segment in the input box. Click the application button again。

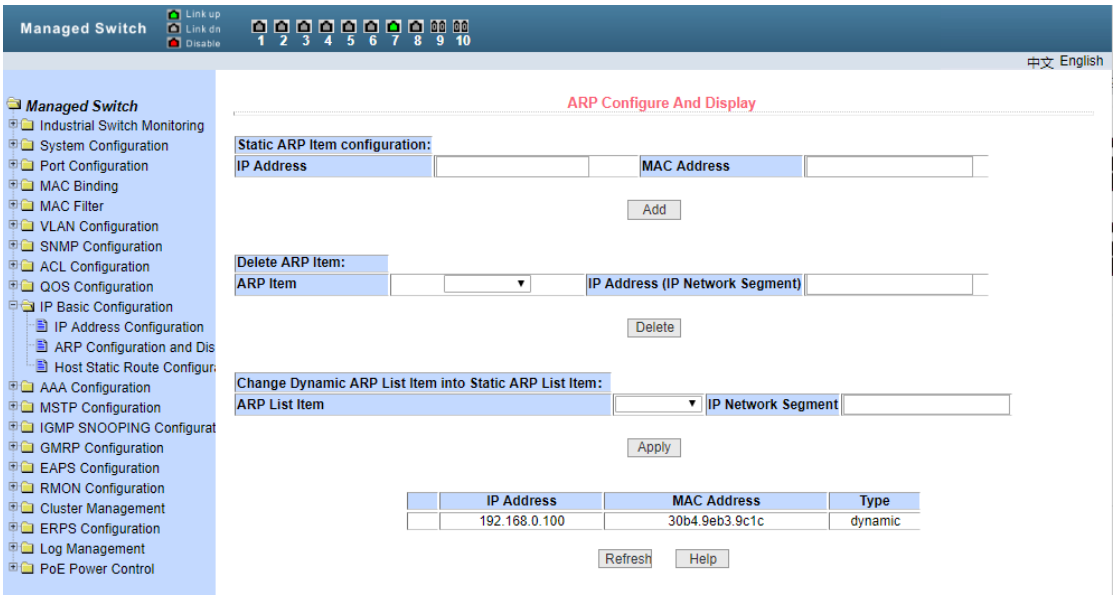


Figure 12-2 ARP configuration and display page

（3）Host static routing configuration

Figure 12-3 shows the host static routing configuration page. Users can add or delete the host static routing of the switch through this page. By default, the switch is not configured with host static route. Users can configure the default route through this page, that is, the route with destination address / subnet prefix of 0.0.0.0/0由。

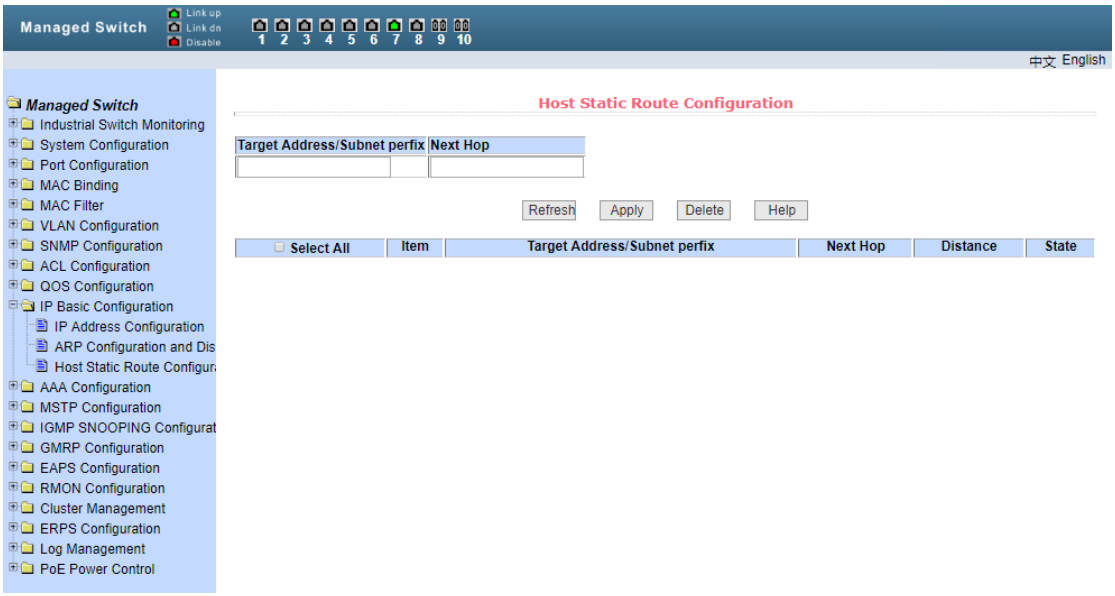


Figure 46 host static routing configuration page

13、AAA Configuration

（1）Tacacs+configuration

Figure 13-1 shows the TACACS + configuration page. Users can configure TACACS + related information, including enabling TACACS + function, configuring the IP address of TACACS + server, authentication type, and shared secret key。

Before using TACACS + function, TACACS + function must be enabled, which is not enabled by default。

To configure the IP address of the TACACS + server, this field must be set when using the TACACS + function。

Authentication type: two authentication types, PAP and chap, are provided. The default configuration is PAP authentication。

The shared key is used to set the encryption shared password between the switch and the TACACS + server. This field must be set when doing authentication and authorization, and it must be the same as that on the TACACS + server。

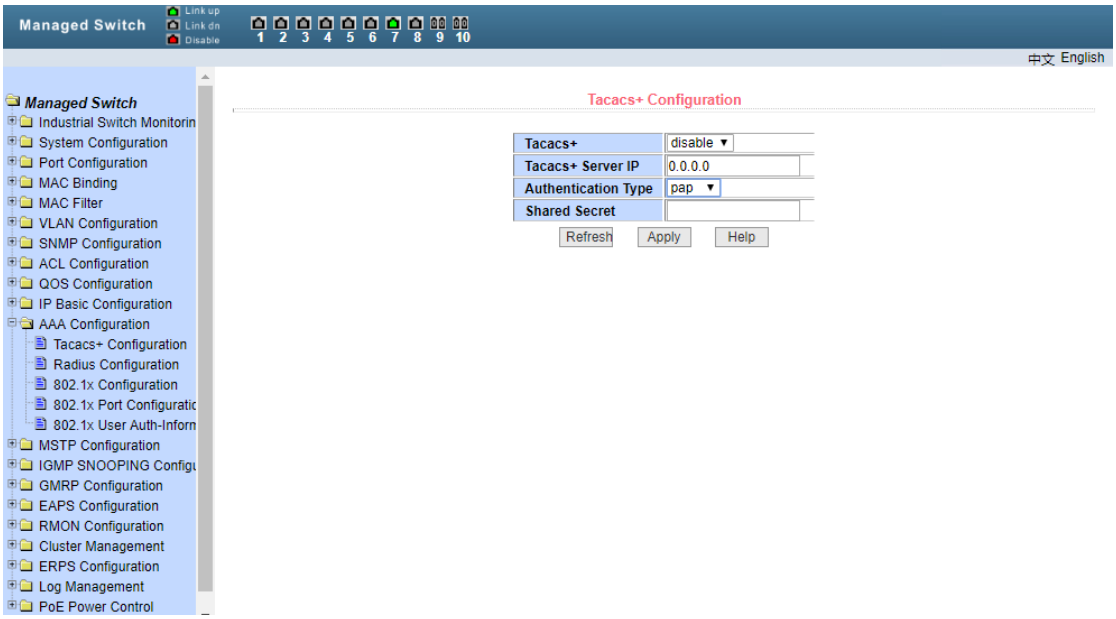


Figure 13-1 TACACS + configuration page

（2）Radius Configutation

Figure 13-2 shows the radius configuration page. Users can configure the information related to radius. The information that can be set includes：

- The IP address of the radius server. This field must be set when doing authentication and billing。
- The IP address of the radius server can be selected. If there is a spare radius server, this field can be set。
- Authentication UDP port, the default value is 1812, users generally do not need to modify this field。
- Whether to start billing or not, it is started by default, and it is generally required to start billing when doing authentication billing。
- The default value is 1813。
- The shared key is used to set the encrypted shared password between the switch and the radius server. This field must be set when doing authentication and billing, and it should be the same as the setting on the radius server。
- The user does not need to modify this field for manufacturer specific information。
- Users generally do not need to modify the three values of NAS port, NAS port type and NAS service type。
- Whether to start or turn off the roaming function of radius 。

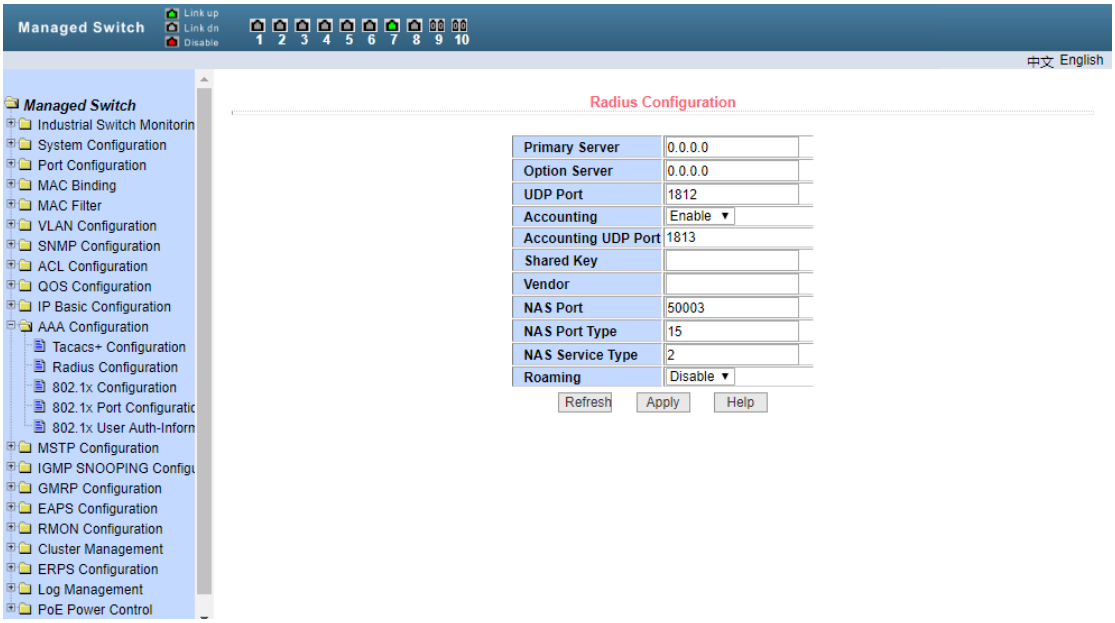


Figure 13-2 radius configuration page

（3）802.1x Configuration

Figure 13-3 shows the 802.1x configuration page, through which users can configure some information related to 802.1x, mainly including：

- Whether to start the 802.1x protocol. When doing authentication and billing, you must start the 802.1x protocol。
- Does the switch adopt the general authentication mode or the extended authentication mode。
- Whether to turn on the re authentication function is not turned on by default. It is decided according to the actual situation when making authentication charging. Turning on the re authentication function will make users more reliable when using authentication billing, but it will slightly increase the network traffic。
- Set the time interval of re authentication, which is valid only when the re authentication function is turned on. The default value is 3600 seconds. Set the value according to the actual situation when doing authentication billing, but the value should not be too small。
- The user does not need to modify this field。
- The user does not need to modify the TX period timer。
- Server timeout timer, users generally do not need to modify this field。
- The user does not need to modify this field。
- The number of Max requests. Generally, users do not need to modify this field。
- Display the size of reauth Max。
- Client Version，Client version number。
- Check Client，Whether to check the client's timed traffic packet after passing the authentication。

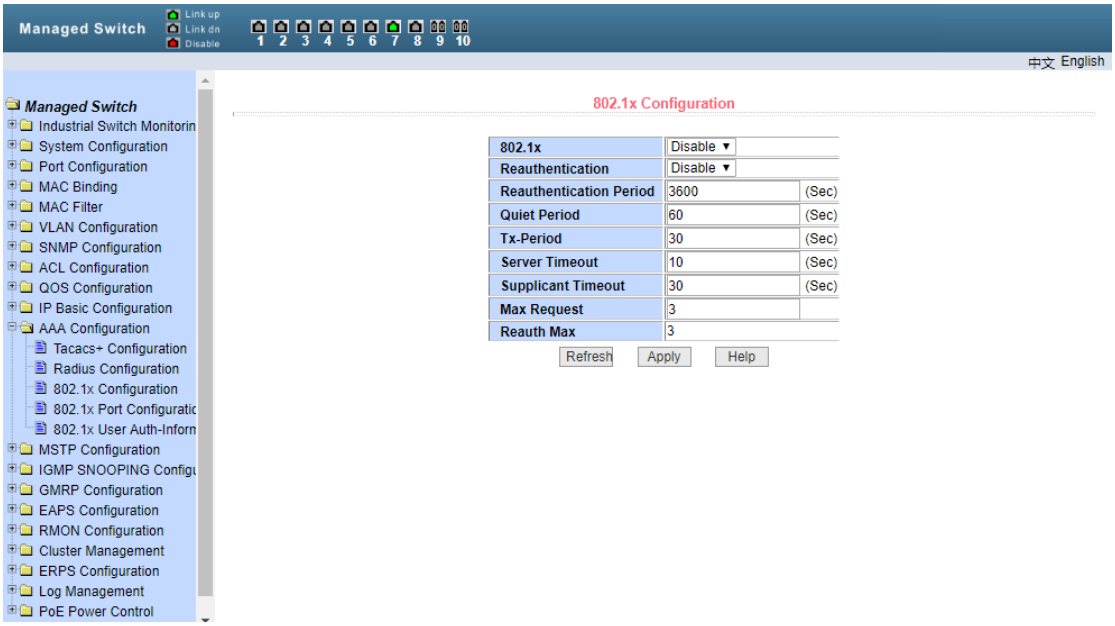


Figure 13-3 802.1x configuration page

（4）802.1x Port configuration

Figure 13-4 shows the 802.1x port configuration page, through which users can configure the 802.1x port mode and the maximum number of hosts supported, and view the 802.1x configuration of each port. 802.1x port mode includes four types: n / a state, auto state, force authorized state and force unauthorized state. When a port needs to do 802.1x authentication, the port should be set to auto state. If it can access the network without authentication, the port should be set to N / a state. The other two states are rarely used in practical applications。

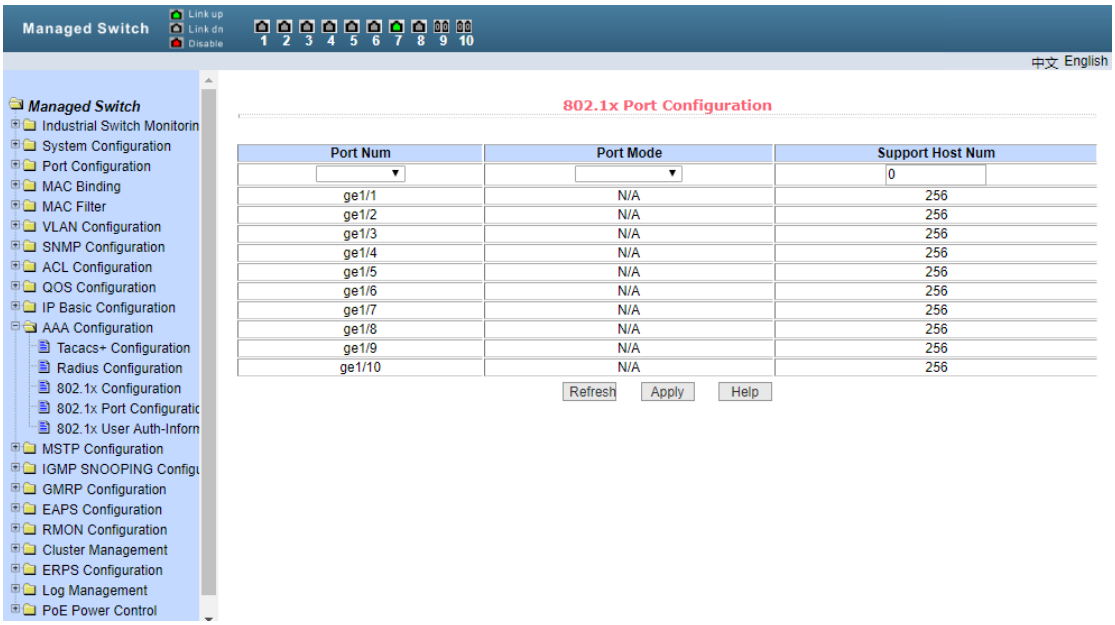


Figure 13-4 802.1x port configuration page

When doing 802.1x authentication, the maximum number of hosts that the port accesses by default is 256. Users can modify this field to support up to 256。

（5）802.1xUser authentication information

Figure 13-5 shows the 802.1x user authentication information page, through which users can view the status information of all users accessed under a certain port，

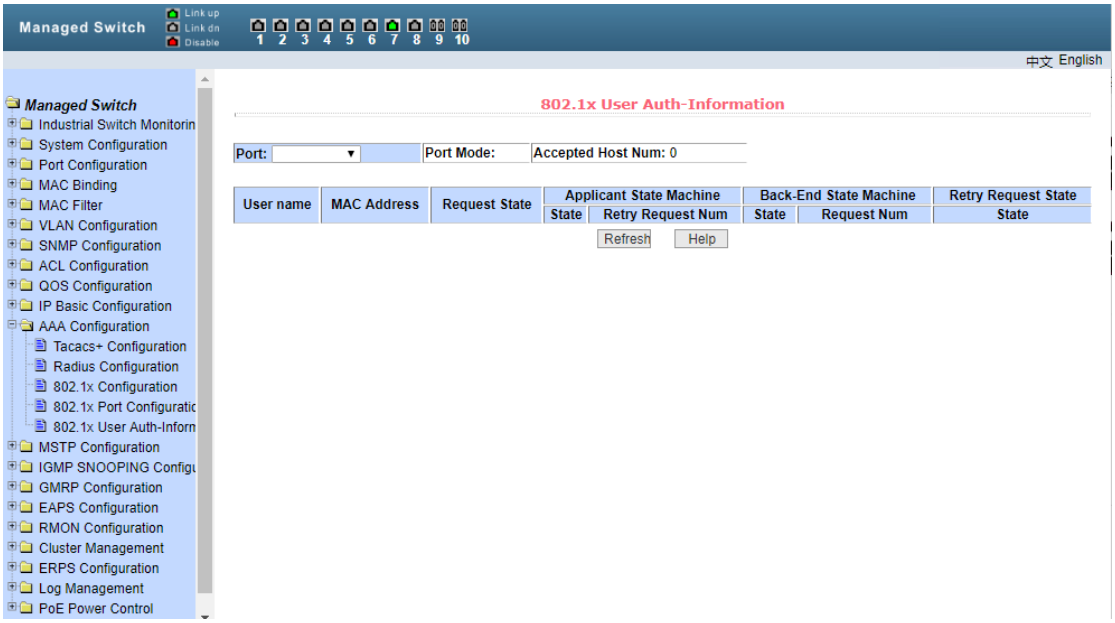


Figure 13-5 802.1x user authentication information page

14、MSTP Configuration

（1）Global configuration

Figure 14-1 shows the MSTP global configuration page, through which users can configure global MSTP parameters。

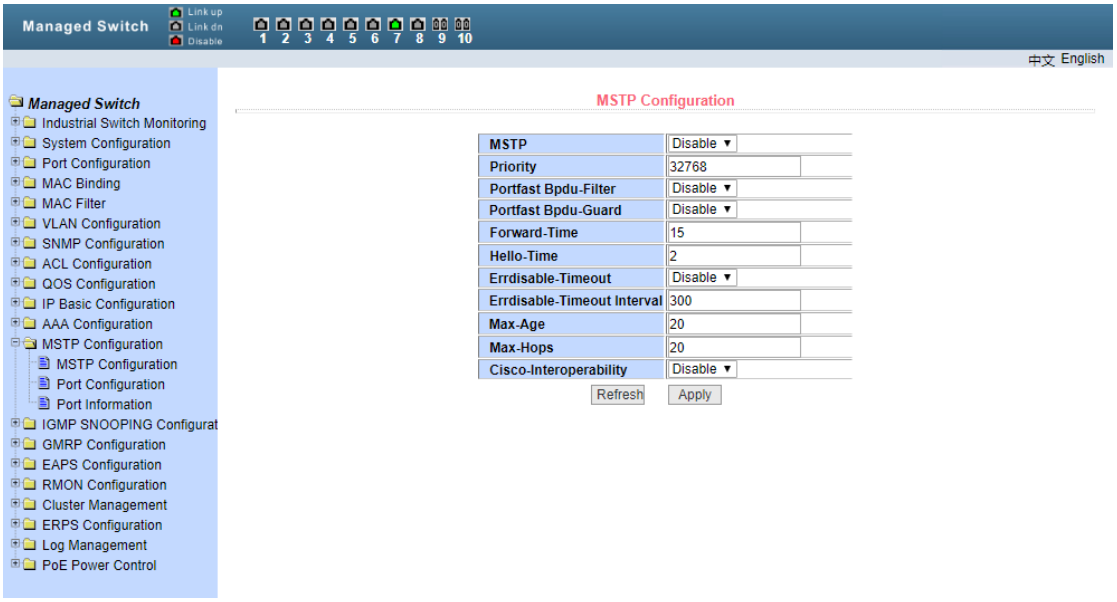


Figure 14-1 the MSTP global configuration page

（2）Port　configuration

Figure 14-2 shows the MSTP port configuration page, through which users can configure port MSTP parameters。

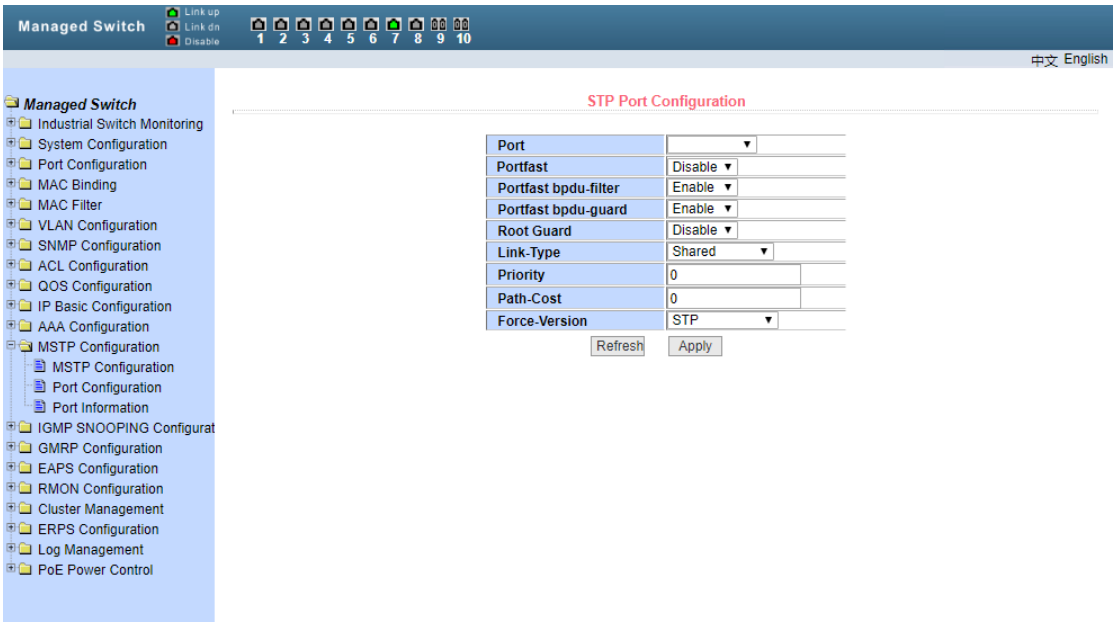
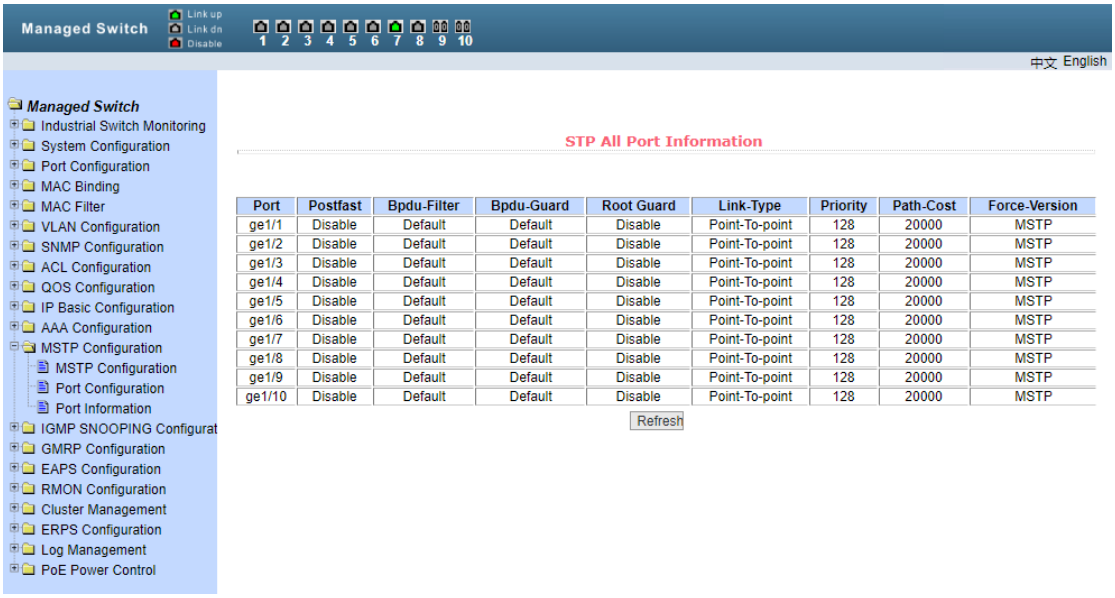


Figure 14-2 the MSTP port configuration page

（3）Port　information

Figure 14-3 is the MSTP port information page, through which users can view the specific state of MSTP port。



Figute14-3

15、IGMPSNOOPING CONFIGURATION

（1）IGMP SNOOPING　CONFIGURATION

Figure 15-1 shows the IGMP snooping configuration page, through which users can enable IGMP snooping。

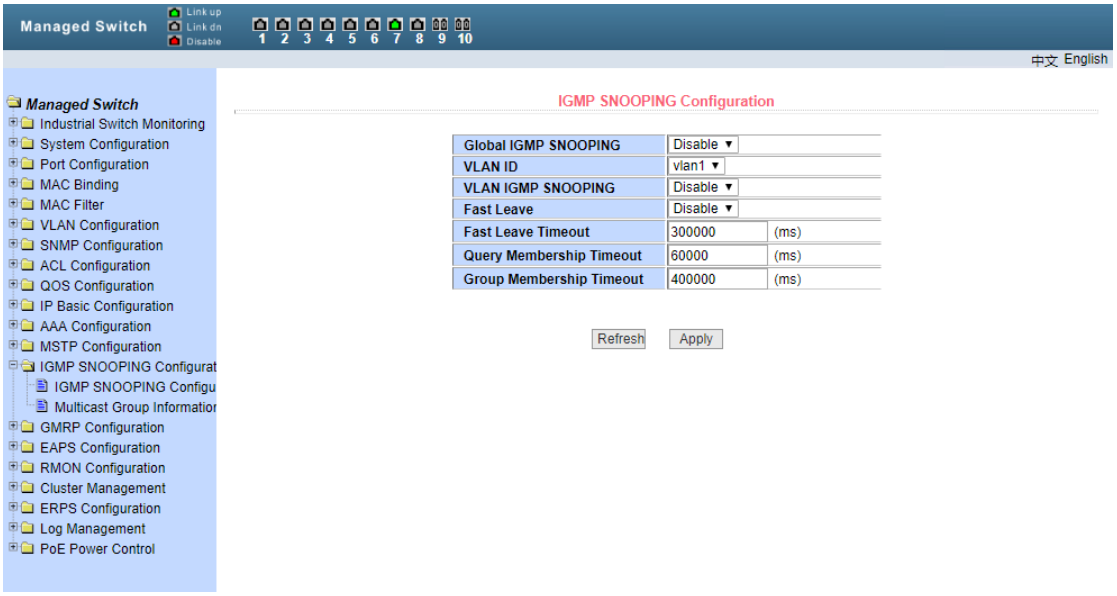


Figure15-1 IGMP SNOOPING

（2）Multicast group information

Figure 15-2 shows the multicast group information page, through which users can view IGMP snooping multicast program information。

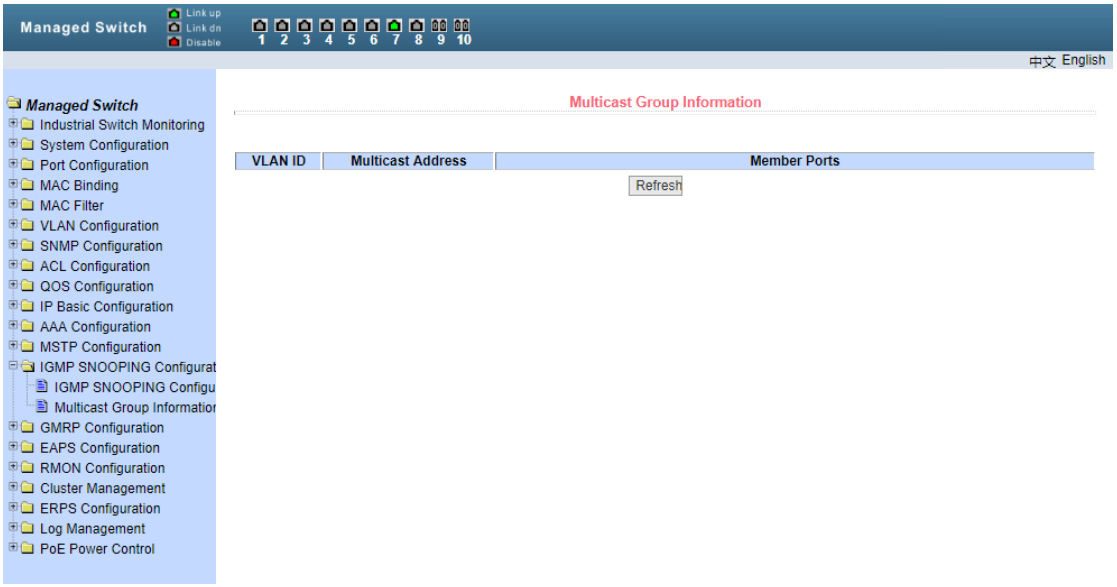


Figure 15-2

16、GMRP CONFIGURATION

（1）GMRP GLOBLE　CONFIGURATION

Figure 16-1 shows the GMRP global configuration page, through which users can enable GMRP。

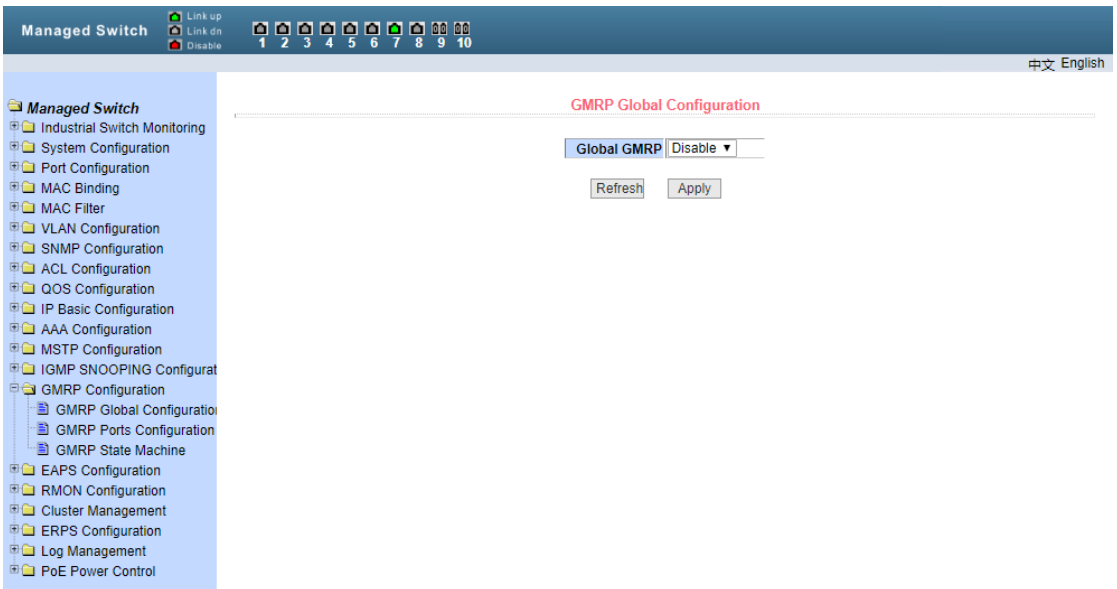


Figure 16-1 GMRP

（2）GMRP　Port　configuration

Figure 16-2 shows the GMRP port configuration page, through which users can enable port GMRP and view port information。

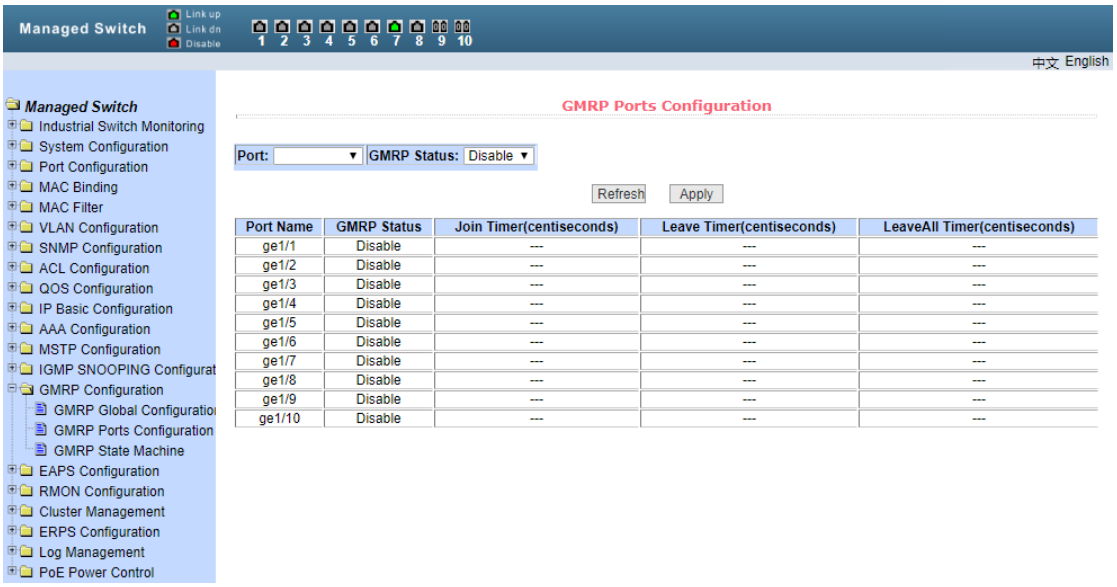


Figure 16-2 GMRP

（3）GMRPState machine

Figure 16-3 shows the GMRP state machine page, through which users can view the state machine information established by GMRP。

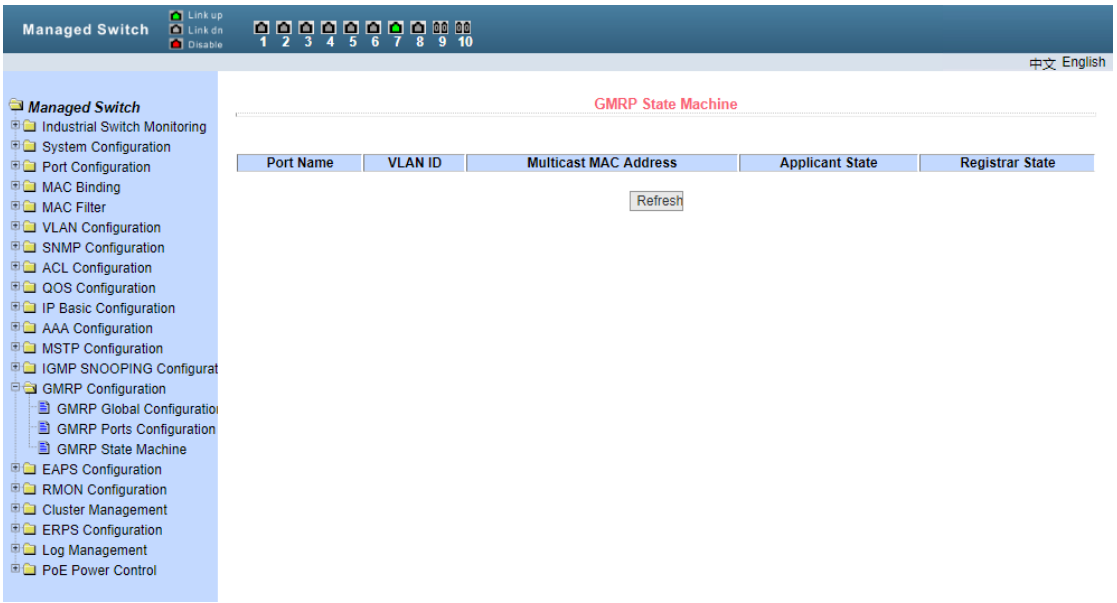


Figure 16-3 GMRP

17、EAPS Configuration

（1）EAPS　Configuration Figure17-1

This page is used to create and configure EAPs information, as well as to delete and display EAPs information。

EAPs ring number

Specific ring number, value range 1-16, can be selected according to the drop-down box

The creation status is "not created" and "created". If it is not created, it needs to be created first

There are two modes: master and transit, which can be configured according to specific needs

Main port EAPs main port, such as Fe1 / 1, GE1 / 1

Standby port - EAPs second port

Control VLAN? Control VLAN of EAPs ring, value 2-4094

VLAN protected by EAPs ring

The time interval of sending Hello message. The default is 1s

Fail time – the time of fault detection, the default is 3S

In the case of cross ring data forwarding and multi ring data forwarding, this function should be enabled. It is not turned on by default

Extreme interoperability is compatible with radical network devices. It is on by default

Enable status - EAPs ring enable status

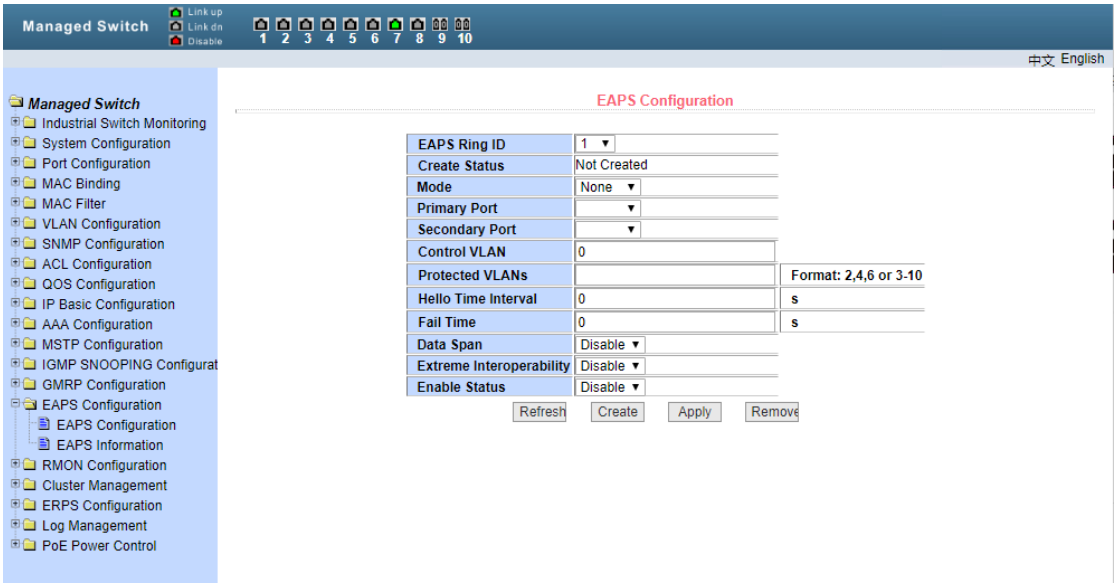


Figure17-1 EAPS

（2）EAPS information

Figure 17-2 shows the EAPs information page, through which users can view the EAPs configuration information。

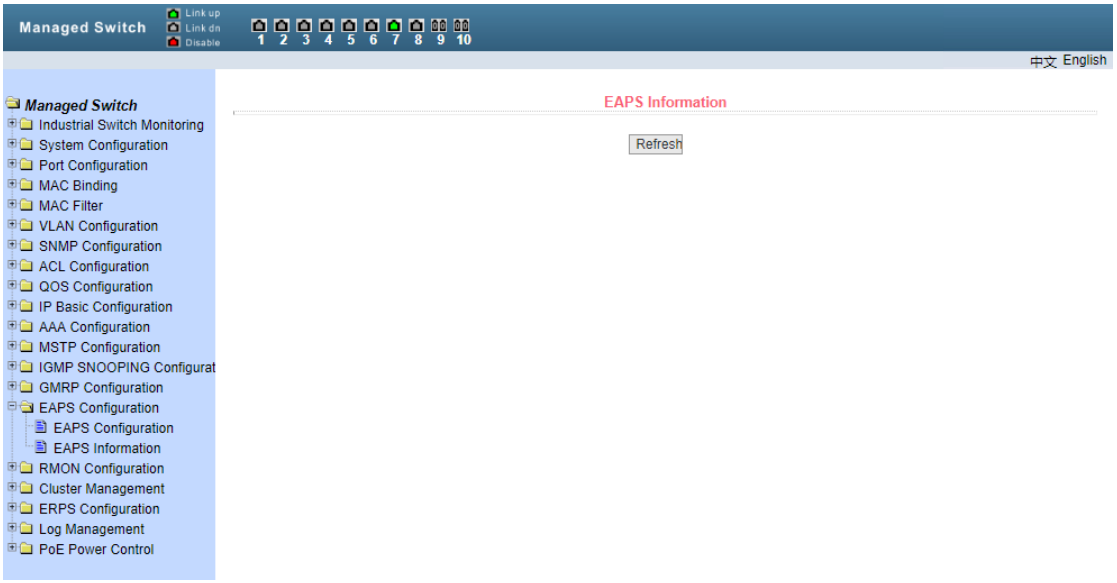


Figure17-2 EAPS

18、RMON configuration

（1）Statistics group configuration

Figure 18-1 shows the RMON statistics group configuration page. Users can configure RMON statistics group through this page. Select a port from the drop-down list to view the RMON statistics group configuration for that port. When not configured, the index number is 0, fill in the correct index number (range from 1 to 100), and the owner is optional. You can configure the RMON statistics group for this port. The statistics table shows the port statistics from the successful configuration。

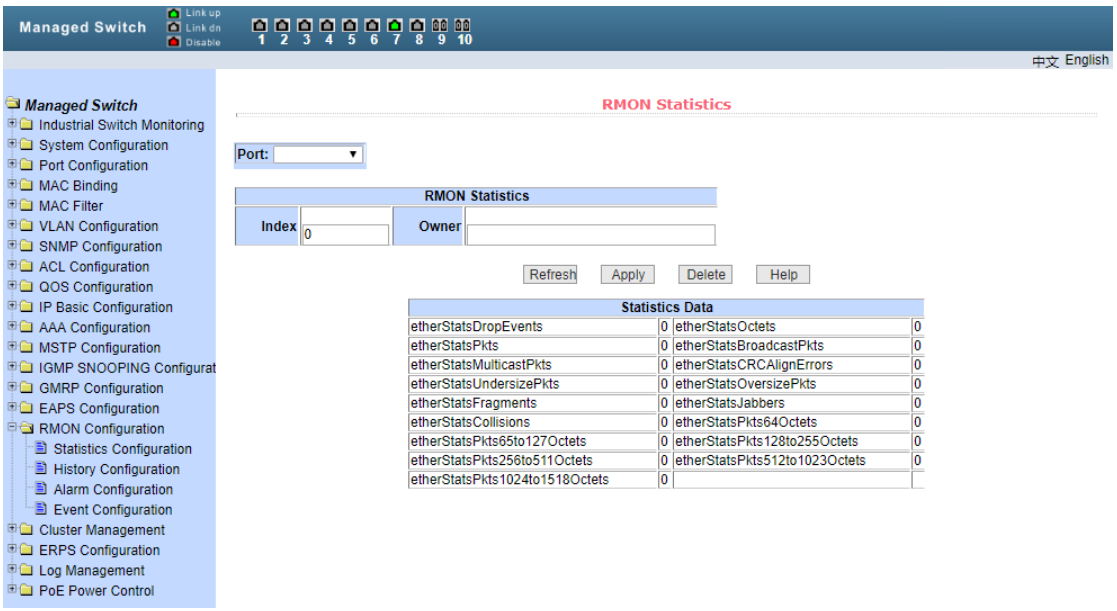


Figure18-1 RMON

（2）History group configuration

Figure 18-2 shows the configuration page of RMON history group. Users can configure RMON history group through this page. Select a port from the drop-down list to view the RMON history group configuration for that port. When it is not configured, the index number is 0, the correct index number (range 1 to 100), the interval, and the request buckets. If the owner is optional, the RMON history group can be configured for the port. Interval refers to the time interval of data collection, in seconds, ranging from 1 to 3600; request buckets is the allocated storage size, indicating how many records are stored, ranging from 1 to 100. The statistics table shows the historical data that has been collected since the successful configuratio。

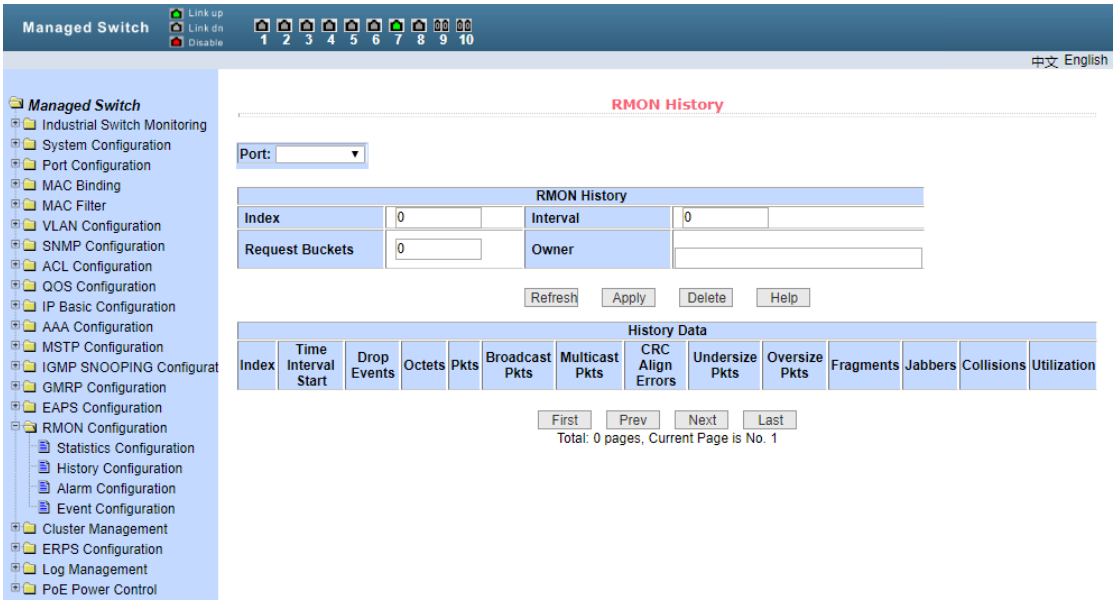


Figure18-2 RMON

（3）Alarm group configuration

Figure 18-3 is the configuration page of RMON alarm group. Users can create or modify RMON alarm group through this page. Select a configured alarm group from the drop-down list to view / configure its information, and select new to create it. The index number range is 1 to 60, and the interval range is 1 to 3600. In seconds, the monitoring object must fill in the MIB node. The comparison method can select absolute or delta. In addition, the upper and lower limit threshold values and event index must be filled in. The owner is optional. The alarm value is read-only and displays the sampling value of the last alarm. Event index refers to the index number of RMON event group, which must be configured in advance。

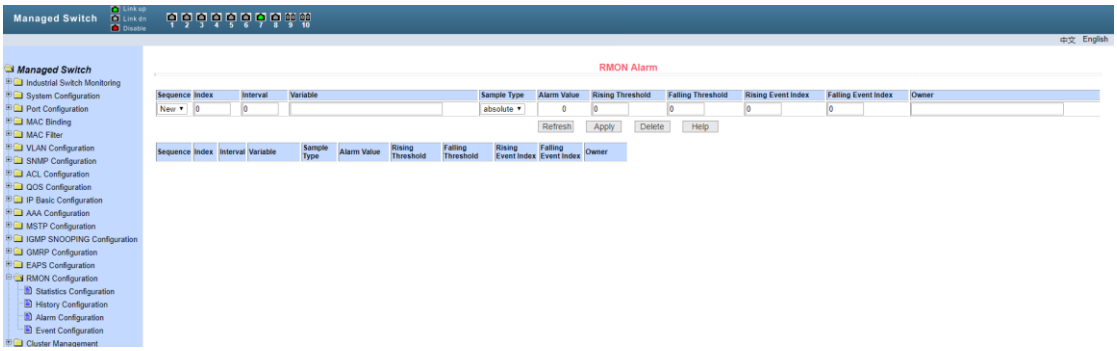


Figure18-3RMON

（4）Event group configuration

Figure 18-4 shows the RMON event group configuration page, through which users can create or modify RMON event groups. Select a configured event group from the drop-down list to view / configure its information, and select new to create it. The index number ranges from 1 to 60, and the description is in the form of string. The action can select none, log, SNMP trap or log and trap. The common body name does not work in this device, and the owner is optional. The last send time is read-only and displays the last time the event was sent。

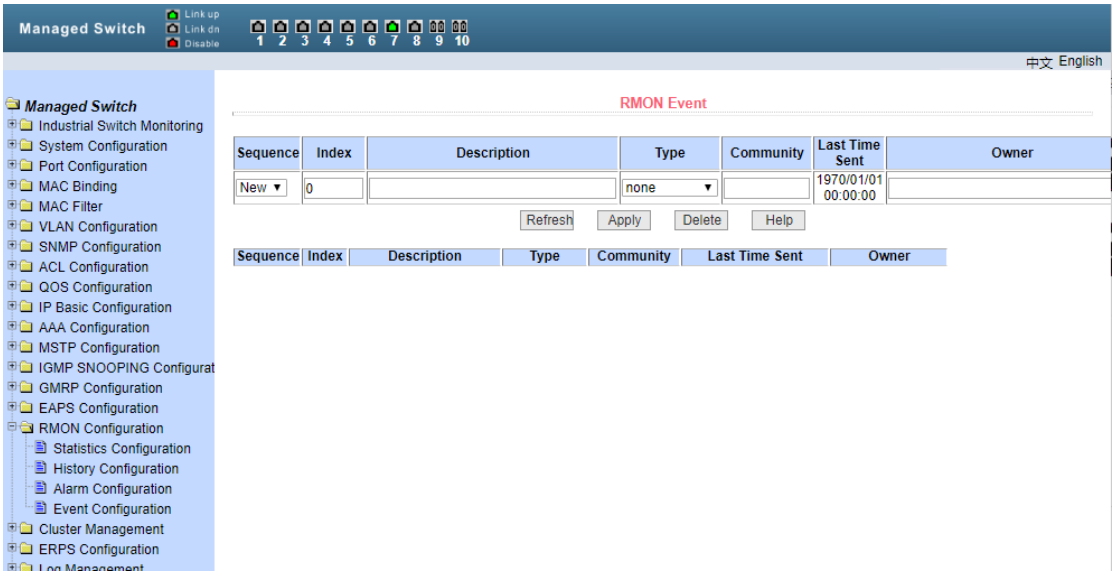


Figure18-4 RMON

19、Cluster management

（1）NDP configuration

Figure 19-1 shows the NDP configuration page, through which users can configure NDP. The information that can be set includes: select port, enable port NDP function, enable global NDP function, time interval of sending NDP message, and aging time of NDP message on

receiving device。

Port selection: the port can be selected according to the needs, and the NDP function of the port can be enabled. In order for NDP to work properly, it is necessary to enable both global and port NDP functions。

Configure the aging time of the NDP message sent by the device on the receiving device. The effective time range is 1-4096 seconds. The default configuration is 180 seconds。

The effective time range is 1-4096 seconds, and the default is 60 seconds。

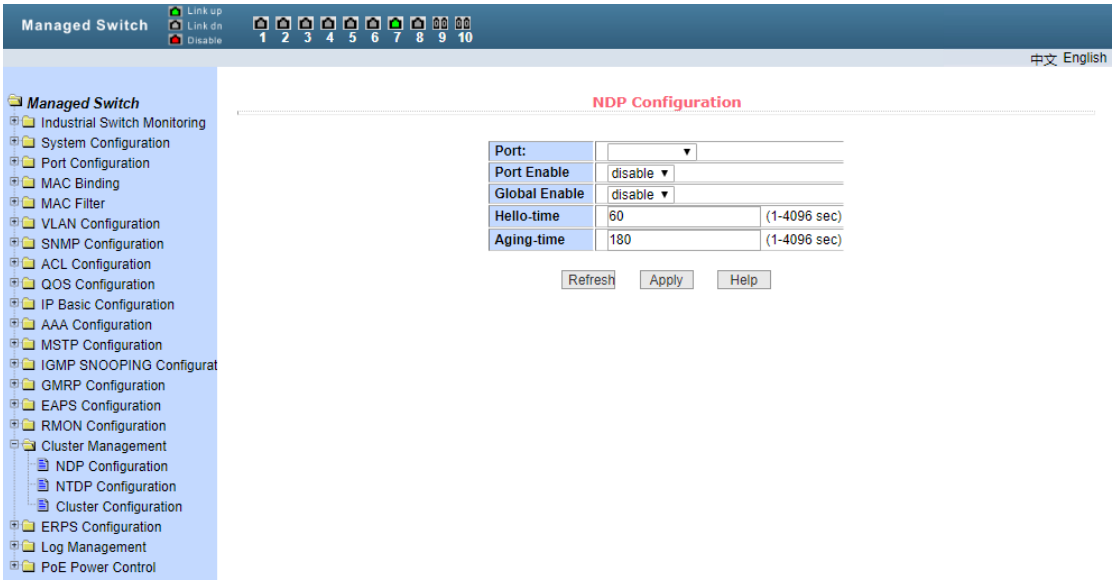


Figure19-1 NDP

（2）NTDP configuration

Figure 19-2 shows the ntdp configuration page, through which users can configure ntdp. The information that can be set includes: select port, enable port ntdp function, enable global ntdp function, scope of topology collection, time interval of timing topology collection, delay time of forwarding message of the first port, and delay time of forwarding message of other ports.

Port selection: the port can be selected according to the needs, and the port ntdp function can be enabled. In order for ntdp to run normally, it is necessary to enable both global and port ntdp functions.

Configure the range of topology collection. The valid range is 1-6. By default, the farthest device in the collected topology has 3 hops from the topology collection device.

Configure the time interval of timed topology collection. The valid range is 0-65535 minutes. The default configuration is 1 minute.

Configure the delay time of forwarding message on the first port, the effective range is 1-1000 MS, and the default configuration is 200 ms.

Configure the delay time of the first port forwarding message, the effective range is 1-100 MS, and the default configuration is 20 ms。

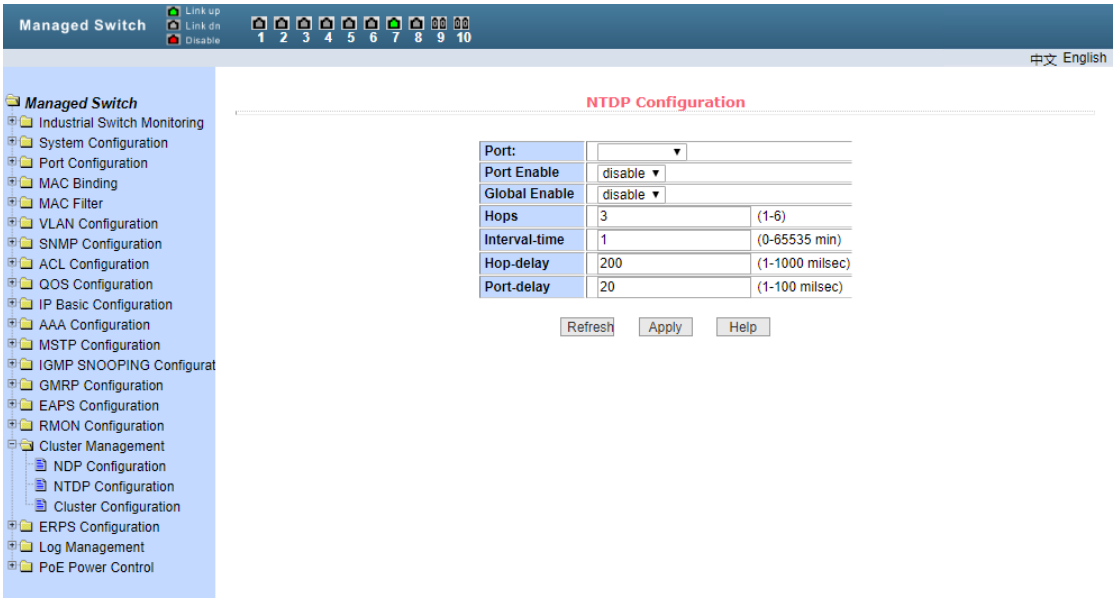


Figure19-2 NTDP

（3）Cluster configuration

Figure 19-3 shows the cluster configuration page. Users can configure the cluster and view the cluster member table through this page. The information that can be set includes: enable cluster function, configure and manage VLAN, address pool of cluster, time interval of handshake message sending, effective retention time of device, cluster name, method of joining cluster, delete cluster.

To enable the cluster function, it is necessary to enable the cluster function first.

Configuration management VLAN, the effective range is 1-4094, the default configuration is vlan1.

Configure the private IP address range used by the member devices in the cluster. The valid range of IP address is 0.0.0 ~ 255.255.255, and the valid range of mask length is 0 ~ 32.

Configure the time interval of handshake message sending, the effective range is 1-255 seconds, and the default configuration is 10 seconds.

Configure the effective retention time of the device. The effective range is 1-255 seconds. The default configuration is 60 seconds.

To establish a cluster, you need to configure the cluster name and select the way to join the cluster. There are two ways to join the cluster, manual and automatic. After the cluster is established, the automatic mode can be switched to manual mode, but manual mode cannot be switched to automatic mode. You can change the cluster name manually.

After the cluster is established, you can view member devices and candidate devices in the cluster member table. You can delete member devices or add candidate devices to member devices according to roles。

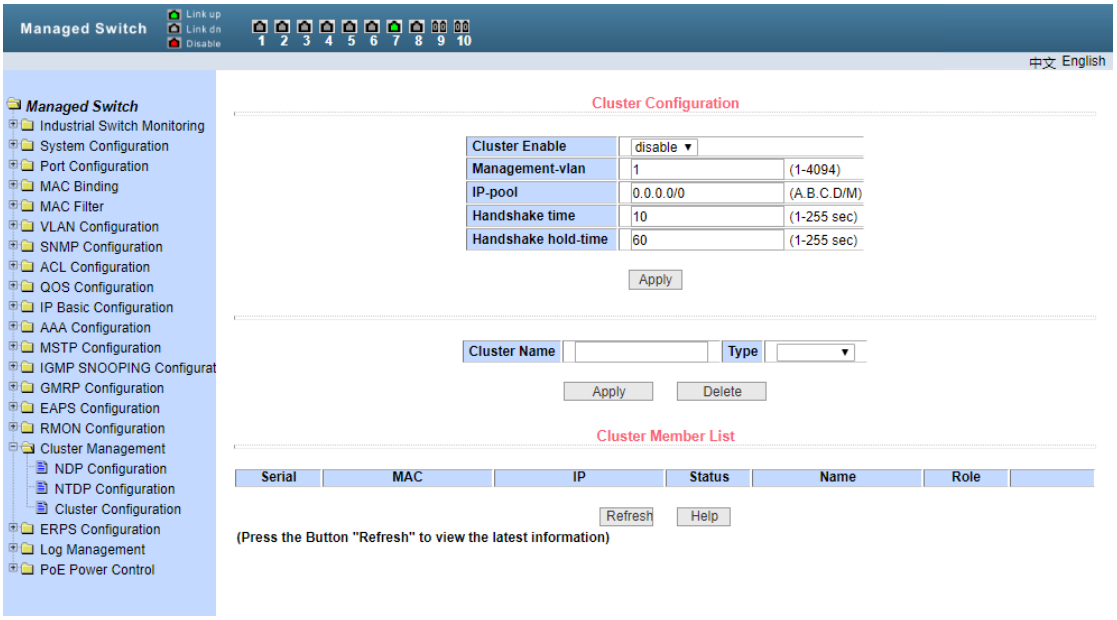


Figure19-3

20、ERPS configuration

（1）ERPS　configuration

Figure 20-1 is the ERPs configuration page. Users can use this page to enable ERPs functions, configure ERPs parameters, create and delete ERPs instances, ERPs rings and other applications.

ERPs instance creation and deletion (< 1-8 >)

ERPs instance node role － configure the role of a node in the ERPs ring, whether it is an interconnected node or a non interconnected node

ERPs ring number > create and delete ERPs rings (< 1-32 >)

Ring mode: configure ERPs ring mode, main ring or sub ring

Ring node mode: configure ERPs ring node mode, RPL owner node, RPL neighbor node or ordinary ring node

Configure and delete ERPs ring protocol VLAN (< 2-4094 >)

Data VLAN configuration ERPs ring data VLAN (< 1-4094 >)

Configure and delete ERPs ring port, RPL port or ordinary ring port

Recovery behavior configure ERPs ring recovery behavior, recoverable or unrecoverable

Hold off time configure the ERPs ring hold off time (< 0-10000 >), unit: ms, default to 0

Guard time configure the ERPs ring guard time (< 10-2000 >), unit: ms, the default is 500

WTR time > configure the WPR time of ERPs ring (< 1-12 >), unit: min, default is 5

WTB time configuration ERPs ring WTB time (< 1-10 >), unit: sec, default is 5

Sending time of protocol message: < 1-10 >, unit: sec, default is 5

Enable the ERPs ring to open or close the ERPs ring

Forced switching of ERPs ring port

Force manual ERPs ring port － force and clear manual ERPs ring port

Manual recovery: manual recovery when the irrecoverable behavior of ERPs ring is cleared or manual recovery before WTR / WTB expiration

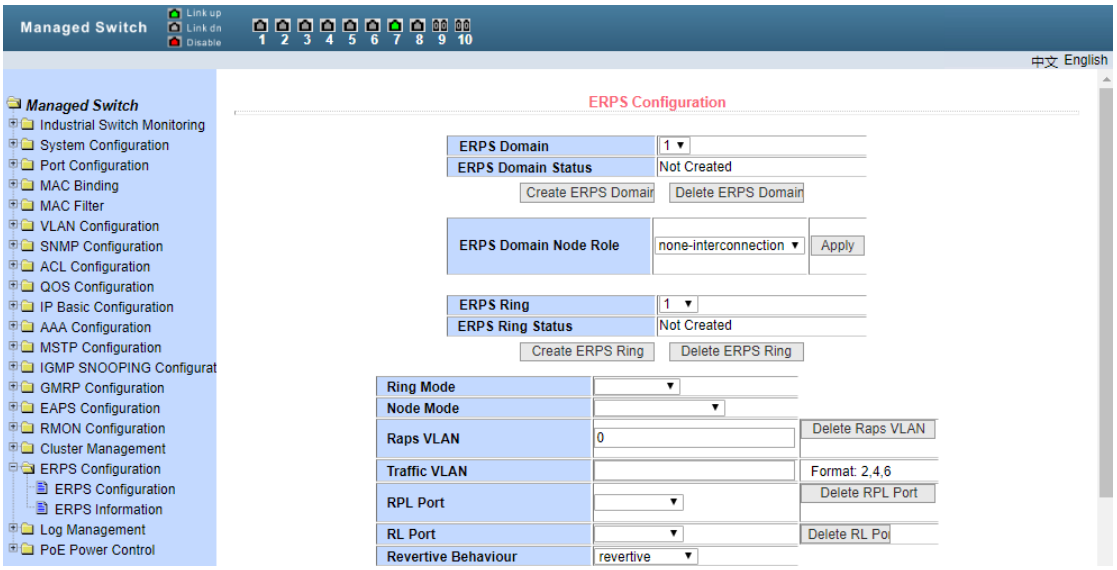


Figure20-1ERPS

（2）ERPS　information

Figure 20-2 shows the ERPs information page, through which users can view the ERPs configuration information。

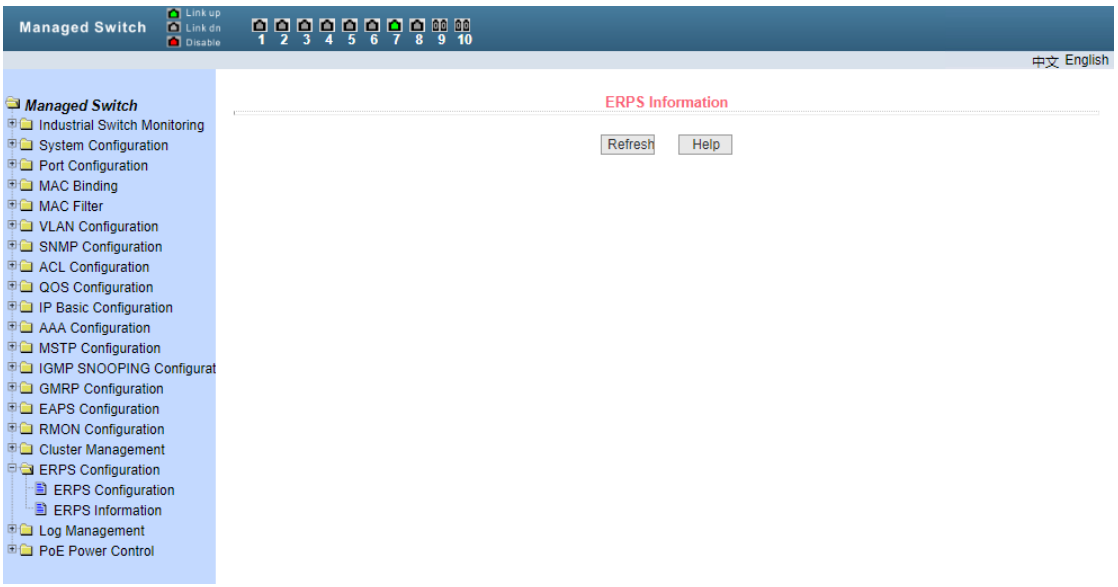


Figure 20-2 ERPS

21、Log management

（1）log information

Figure 21-1 shows the log information page, through which users can view the log. Select log priority from the drop-down list to view the log of this level. Click refresh to view the latest log。

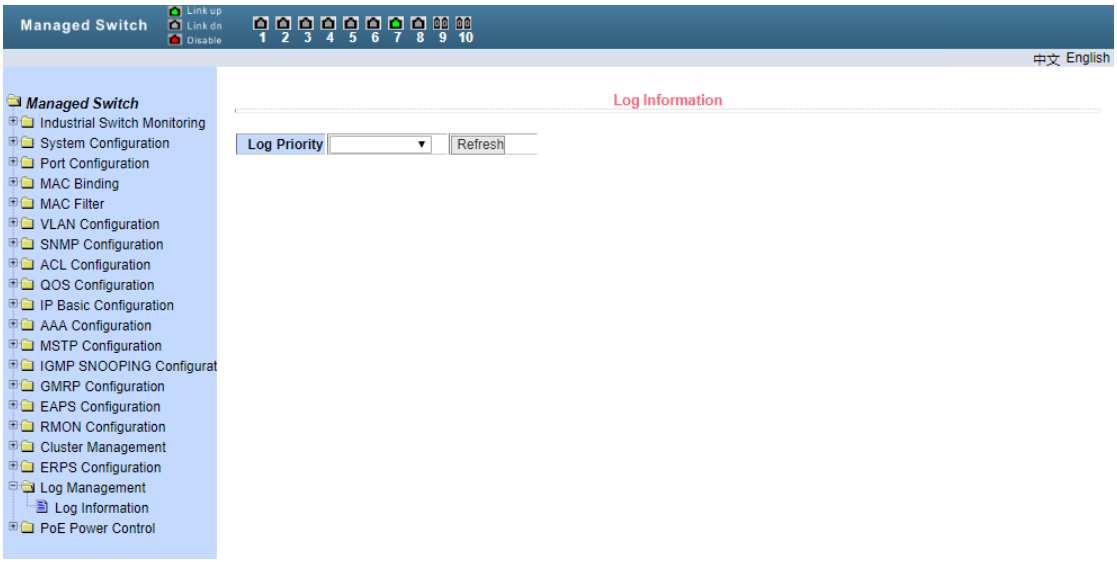


Figure 21-1

22、PoE port configuration

（1）PoE port configuration

Figure 22-1 shows the POE port configuration page. Through this page, you can configure the total power of the POE device (to be updated by the system), the single port power of the POE (to be updated by the system), and the POE on or off. Through this page, you can view the relevant information of the current Poe device

Poe port: select power supply port number (1-8)

Poe port status: enable or disable

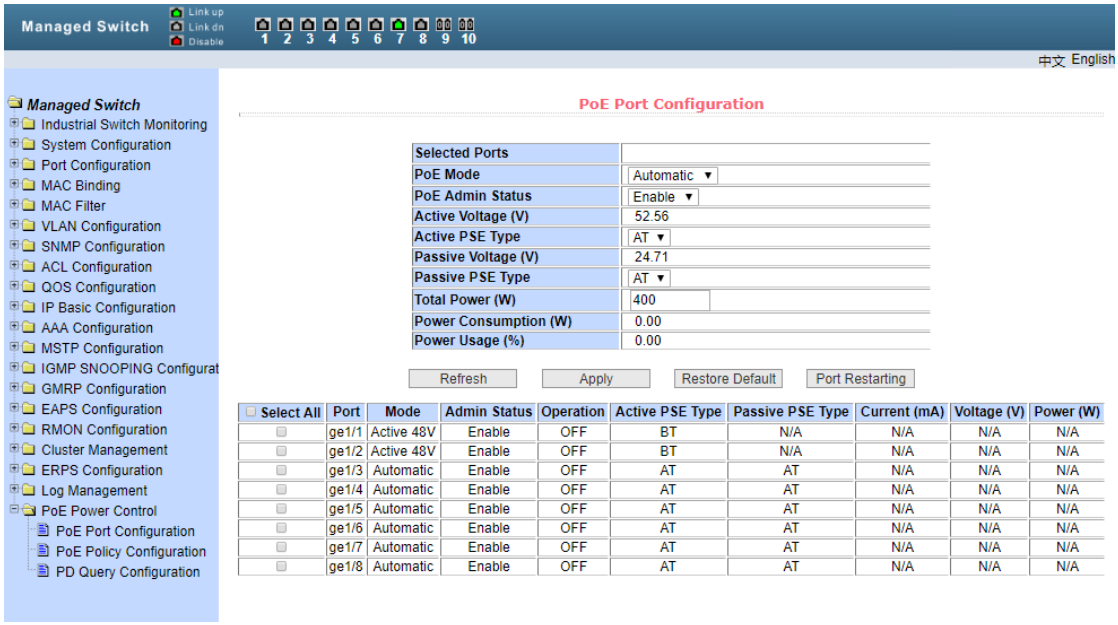


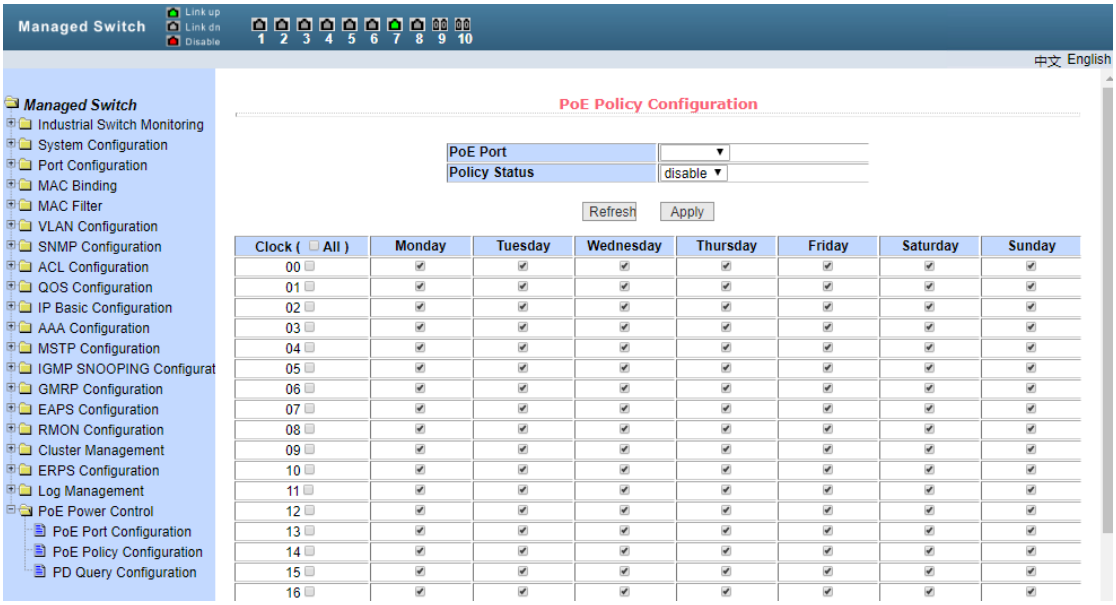
Figure 22-1 PoE

（2）POEScheduling configuration

Figure 22-2 shows the POE scheduling configuration page. Through scheduling management, Poe power supply can be turned on or off according to the actual demand. The control mode is hour + week。

Control port: used to select ports (1-8) for scheduling management

Control function: enable or disable



22-2 PoE Schedule configuration page

（3）PD Query configuration

Figure 22-3 shows the PD query configuration page. PD online device status detection can be realized through PD query configuration。。

Poe port: used to select the port connected with PD device to query

PD IP address: IP address of PD device。

PD query interval: the interval used to query PD devices (default 5 seconds)。

Maximum number of no response for PD query: used to query the maximum number of no response for PD device (3 times by default)）

Maximum time required for PD start: used to query the maximum time required for PD device start (default 120 seconds)

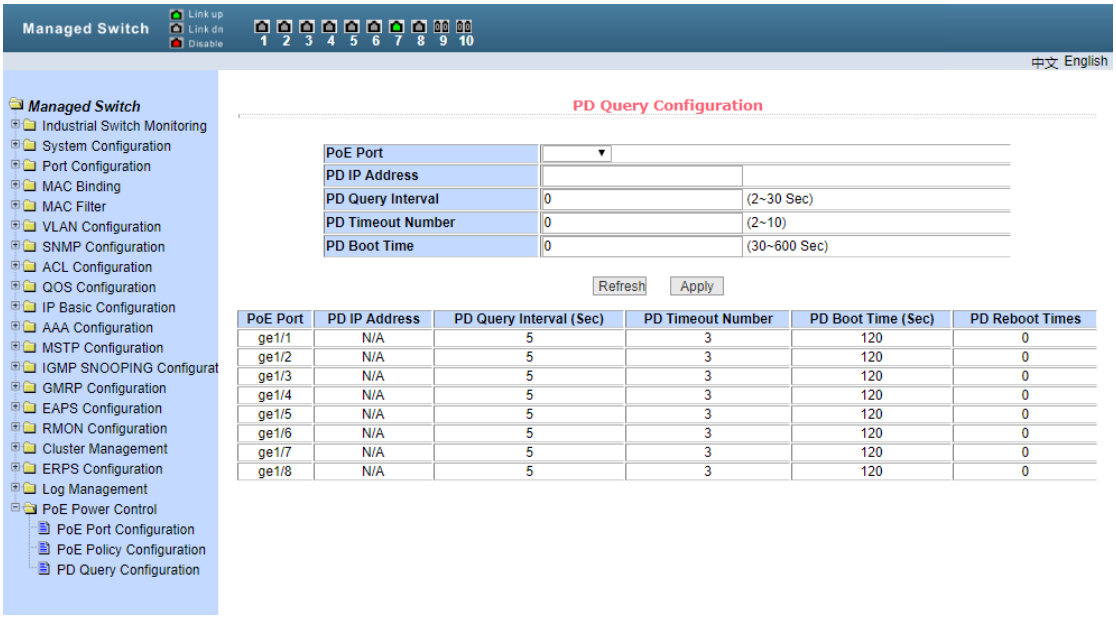


Figure 22-3 PD Query configuration page