Wi-Tek Managed PoE Switch Manual

Contents

Wi-Tek Managed PoE Switch Manual

一、 Overview of the Manual

This manual mainly describes the use manual page of WI-TEK Managed PoE Switch/NON-PoE Switch.The user can manage the switch through the WEB page of the switch. This manual only for each WEB page of the operation had a simple introduction. Please refer to the User Operation Manual for each function of the switch.

1、WEB access' characteristics

The switch provides the features of Web access for users.Users can access the switch through the Web browser and manage and configure the switch.The main characteristics of WEB access :

- Easy to access: Users can easily access the switch from anywhere on the network.
- Users can use the familiar Netscape Communicator and Microsoft Internet Explorer and other browsers to access the WEB page of the switch.WEB page is presented to the user in graphical and tabular form.
- The switch provides a rich WEB page,users can configure and manage most of the functions of the switch through these WEB pages.
- WEB page function’s classification and integration, user-friendly to find the relevant page for configuration and management.

2、WEB browsing' s system requirements

Web browsing' s system requirements shown in Table 1.

Table 1：

Hardware and Software	System Requirement
CPU	Pentium 586 above
RAM	128MB above
Resolution	800x600 above
Color	256 colors above
Browser	IE4.0 above or Netscape4.01 above
Operating System	Microsoft® ,Windows95®,Windows98®,WindowsNT®, Windows2000®,WindowsXP®,WindowsME®, WindowsVista®, Windows7®, Windows8®,MAC, Linux,Unix operating system

Note:

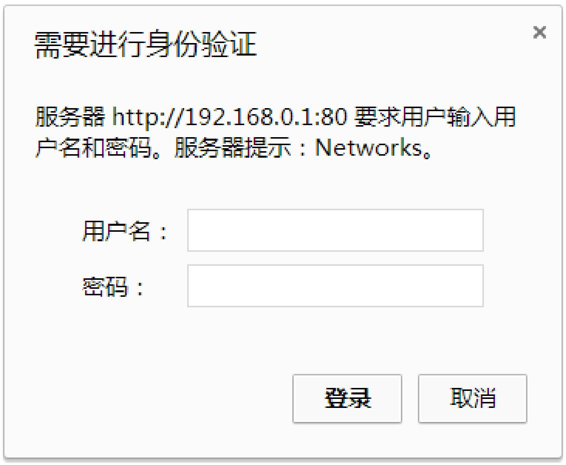
Microsoft®,Windows95®,Windows98®,WindowsNT®,Windows2000®,WindowsXP ®,Windows ME®, WindowsVista®, Windows7®, Windows8® are registered trademarks of Microsoft Corporation, all other product names, trademarks, registered trademarks and service marks, Copyright is held by their respective owners.

3、WEB browsing session login

Before you start a Web browsing session, you need to confirm:

- IP has been configured on the switch. By default, the interface IP address of the switch's VLAN1 is 192.168.0.1.
- The subnet mask is 255.255.255.0.
- A host computer with a Web browser installed has been connected to the network, and the host computer can PING through the switch.
- After the completion of the above two tasks, the user in the browser's address bar enter the address of the switch and press Enter to enter the switch Web login page,as shown in Figure 1,When multi-user management is not enabled, the user login to the Web when the need for anonymous user (admin) password verification,Only enter the correct password to access the Web, anonymous user password default to admin.

If the system is enabled for multi-user management and configured privileged users, the anonymous user password will not take effect, the user access to the Web does not do anonymous user password verification, but do multi-user management user name and password authentication.



需要进行身份验证

服务器 http://192.168.0.1:80 要求用户输入用户名和密码。服务器提示：Networks。

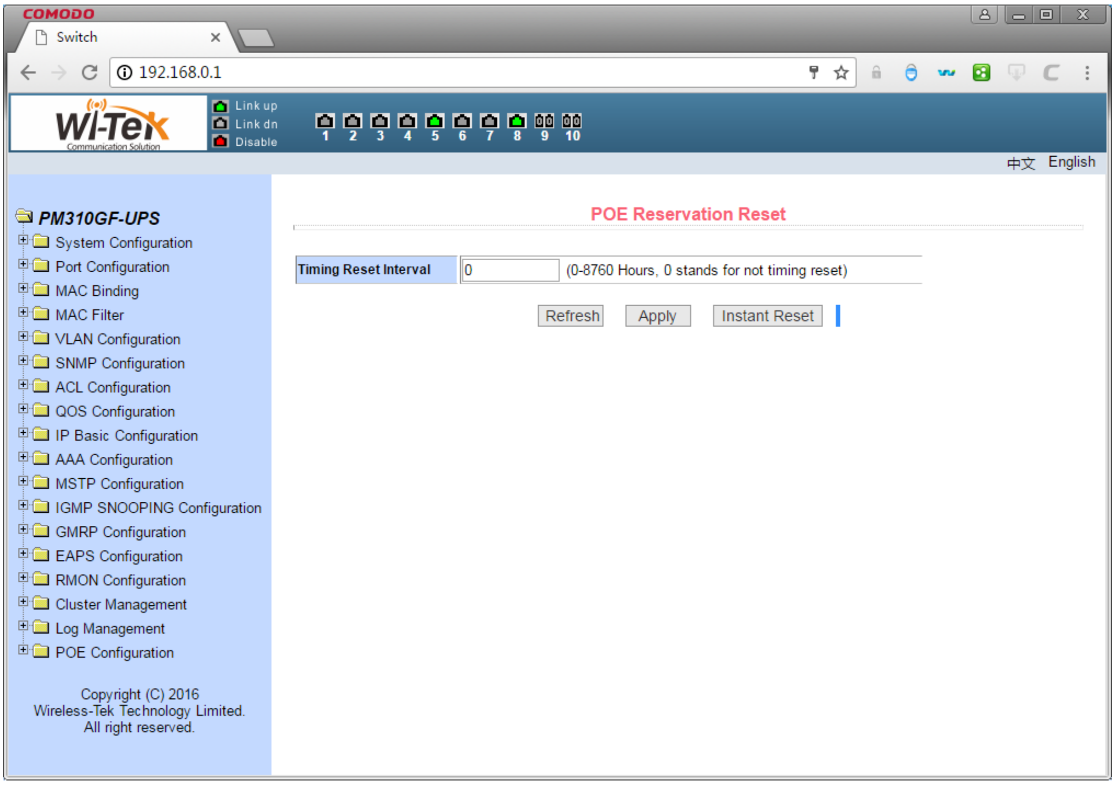
用户名：

密码：

Pic 1 WEB login page for browsing session

4、WEB page basic composition

Figure 2，The WEB page consists of three parts: the title page, the navigation tree page, and the main page.



POE Reservation Reset

Timing Reset Interval	0	(0-8760 Hours, 0 stands for not timing reset)

Copyright (C) 2016
Wireless-Tek Technology Limited.
All right reserved.

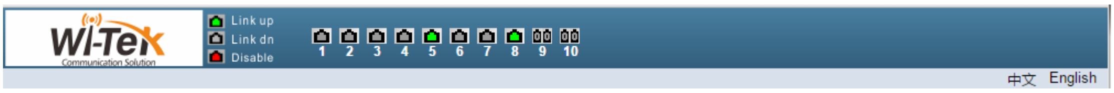
Pic 2 Switch Web page basic composition page

Title Page　Used to display the logo, and real-time port status as shown below

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 off (the specific setting is shown in Figure 17)

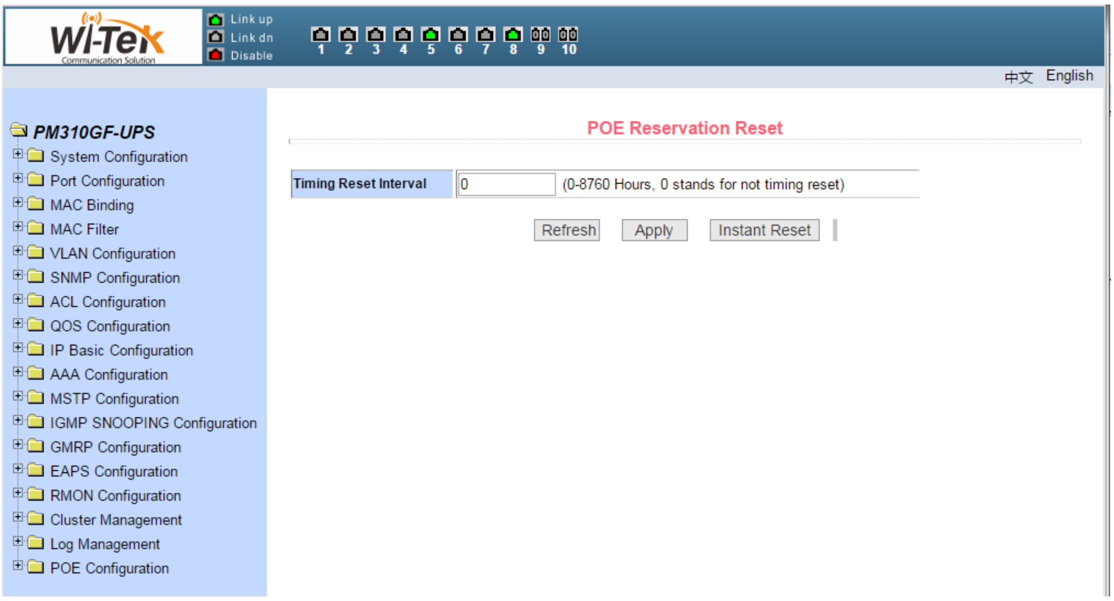


Main page　Used to display the page selected by the user from the navigation tree.

5、Navigation tree structure

Figure 3 shows the organization of the navigation tree.

The navigation tree is located at the bottom left of each page, displaying the nodes of the Web page in a tree, and the user can easily find the WEB page to be managed.According to the different functions of the page will be divided into different groups, each group includes one or more pages.Most web pages in the navigation tree are abbreviations of the page title at the top of the corresponding page.



POE Reservation Reset

Timing Reset Interval: 0 (0-8760 Hours, 0 stands for not timing reset)

Pic 3 Switch the navigation tree's organization page

6、Page button introduction

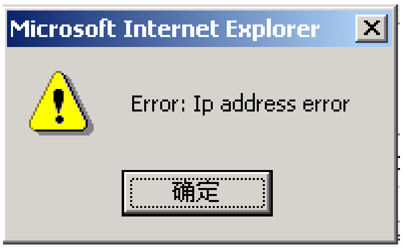
There are some general buttons on the page, the role of these buttons is generally the same, Table 2 on the role of these buttons to introduce.

Table 2：

Button	Effect
Refresh	Update all fields on the page
Application	Put the updated values in memory.Because the error check is done by the Web server, there is no error check before the user selects the button
Delete	Delete the current record
Help	Open the help page and view the configuration instructions for each page

7、Error message

If the switch's WEB server is in error when processing user requests, the corresponding error message is displayed in a dialog box.For example, Figure 4 shows an error message dialog box.



Microsoft Internet Explorer

Error: Ip address error

Pic 4 Error message's page

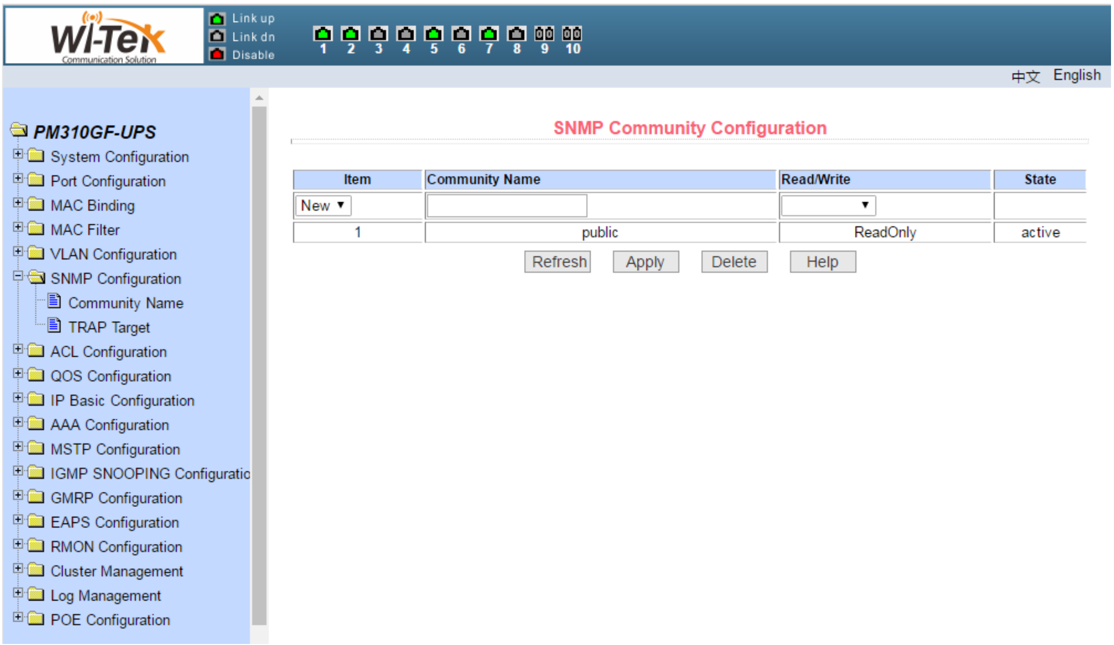
8、Entry field

There are some pages in the leftmost column of the table that have an entry field, as shown in Figure 5, through which you can access different rows in the table.When you select a value in the entry field, the corresponding information for that row is displayed on the first row, and only the row can be edited, which is also called the active row.When the first page is loaded, the entry field displays new, the active row is empty.

If you want to add a new row, select new from the drop-down menu of the entry field, enter the new row information, and press the Apply key.

If you want to edit an existing row, select the appropriate row number from the drop field menu of the entry field, edit the row as needed, and press the Apply key. You will see the corresponding change displayed in the table.

If you want to delete a row, select the corresponding row number from the drop-down menu in the entry field and press the Delete key. The row will disappear from the table.



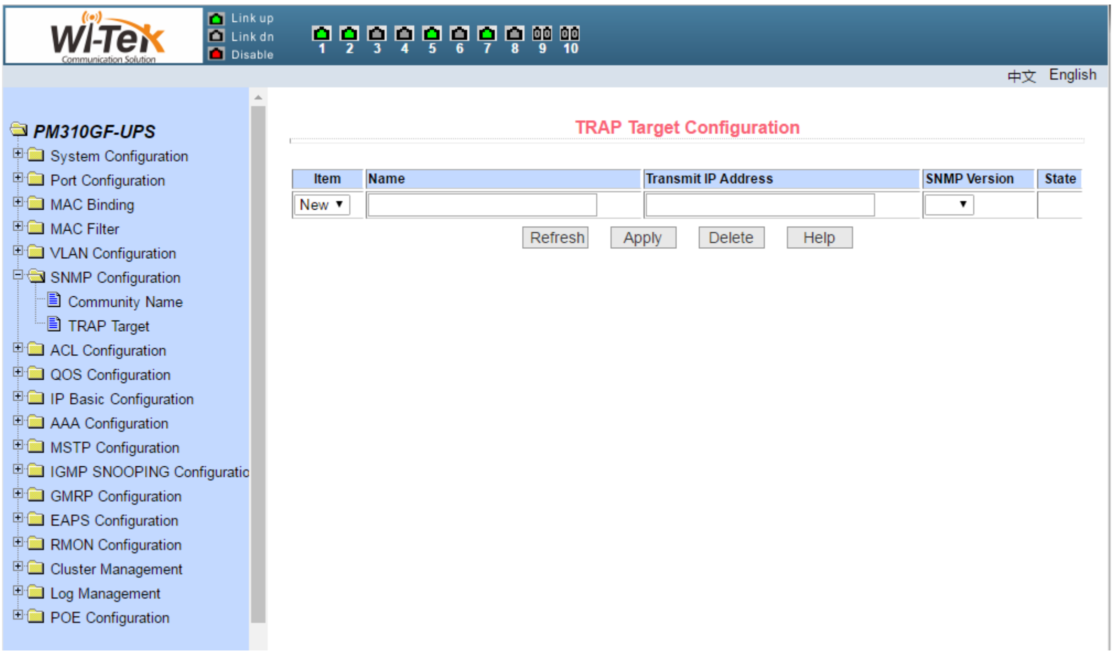
SNMP Community Configuration

Item	Community Name	Read/Write	State
New ▾		▾	
1	public	ReadOnly	active

Pic 5 Entry field's page

9、State field

There are some pages in the rightmost column of the table that have a status field, as shown in Figure 6, where the field shows the row state.Since all row state changes are processed internally, the status field is read-only.Once all the domain information in the row is valid, the row state becomes automatically active.



TRAP Target Configuration

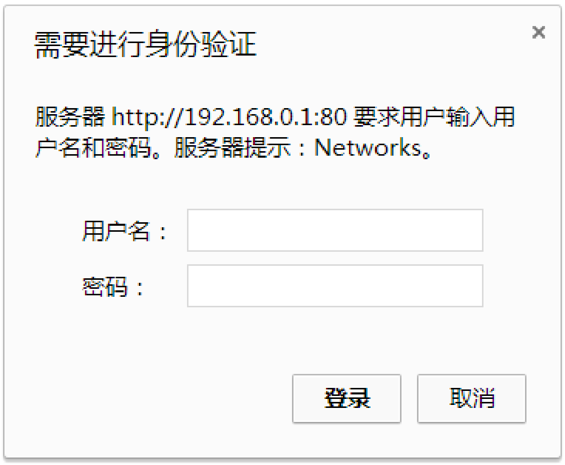
Item	Name	Transmit IP Address	SNMP Version	State
New ▾			▾	

Pic 6 State field's page

二、WEB PAGE INTRODUCTION

The WEB pages of the switch are organized into groups, each consisting of one or more Web pages. The following is an introduction to each page.

1、Login dialog box



需要进行身份验证

服务器 http://192.168.0.1:80 要求用户输入用户名和密码。服务器提示：Networks。

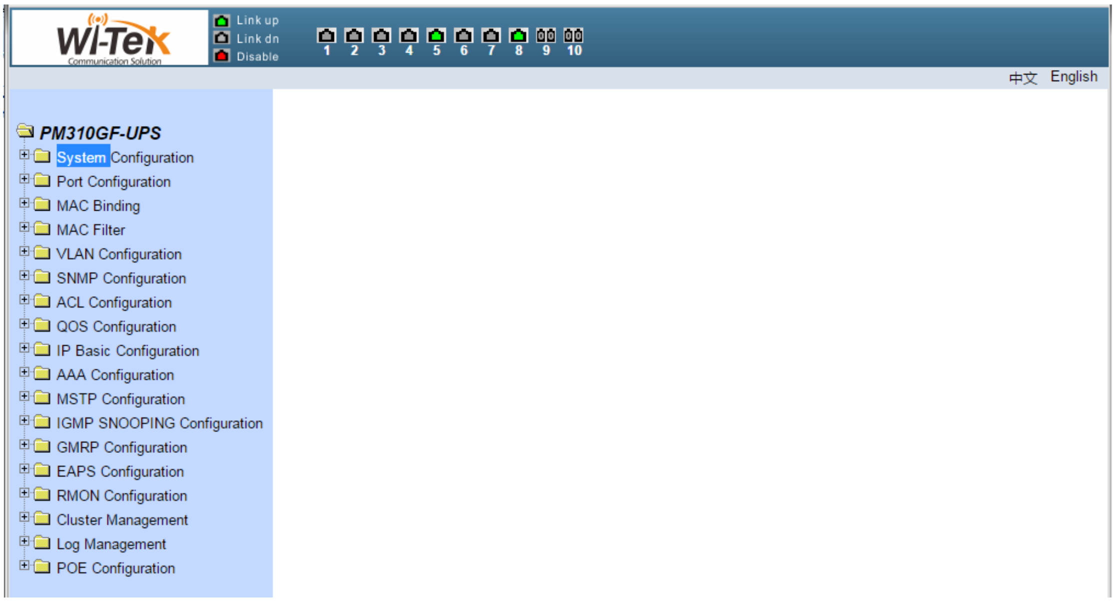
Pic 7 WEB Browse the session's login page

Figure 7 shows the login dialog box, which is displayed when the user first logs in to the web page.The user enters the user name and password in the corresponding field, and then clicks the OK key to log in to the Web server of the switch.Password is case-sensitive, anonymous user password can be set up to 16 characters, and multi-user name and password are up to 16 characters can be set.

The default user name for the switch is anonymous user name admin. The default password is anonymous user password. Anonymous user password is empty by default.

2、Main page

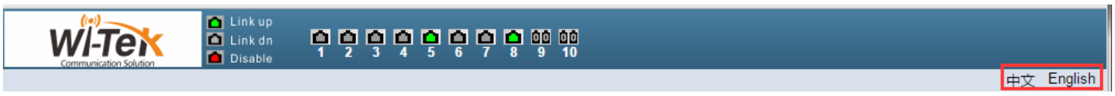
Figure 8 shows the WEB main page of the switch. The page will be displayed after the user logs in to the page.



Pic 8 Switch the main page

3、System Configuration

Language switching: switch buttons in the upper right corner and easily switch between Chinese and English system interfaces.



（1）Basic information page

Figure 9 shows the basic information configuration page where the user can configure the basic information for the switch.

System Description Displays a description of the system-related parameters.

The system descriptor identification number indicates the identity of the system in network management.

The system version number shows the version number of the current software used by the switch.

The number of network interfaces displays the current number of network interfaces in the switch.

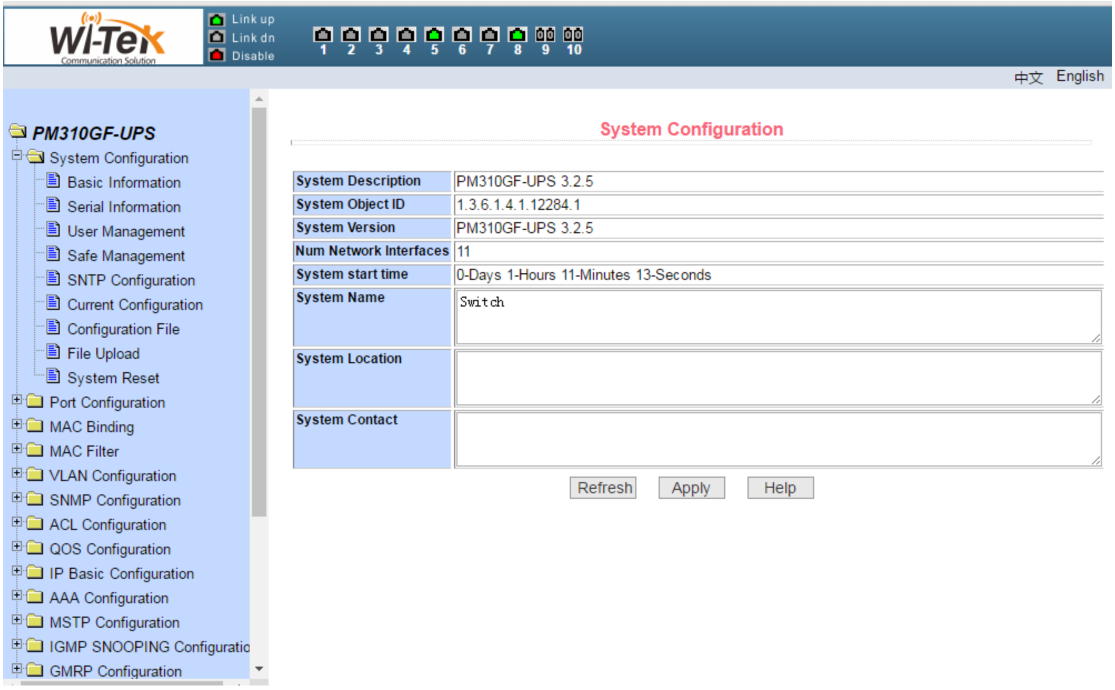
System Startup Time Displays the time the switch was started to the present time.

The system clock displays the current clock of the system. The user can modify the system's current clock and need to enter the year, month, day, hour, minute, and seconds parameters.

The system name displays the system name of the switch in the network. The user can modify the system name.

The system location displays the physical location of the switch in the network, and the user can modify the system location.

System contact display management of the current node contacts and contact information, the user can modify the system contact.



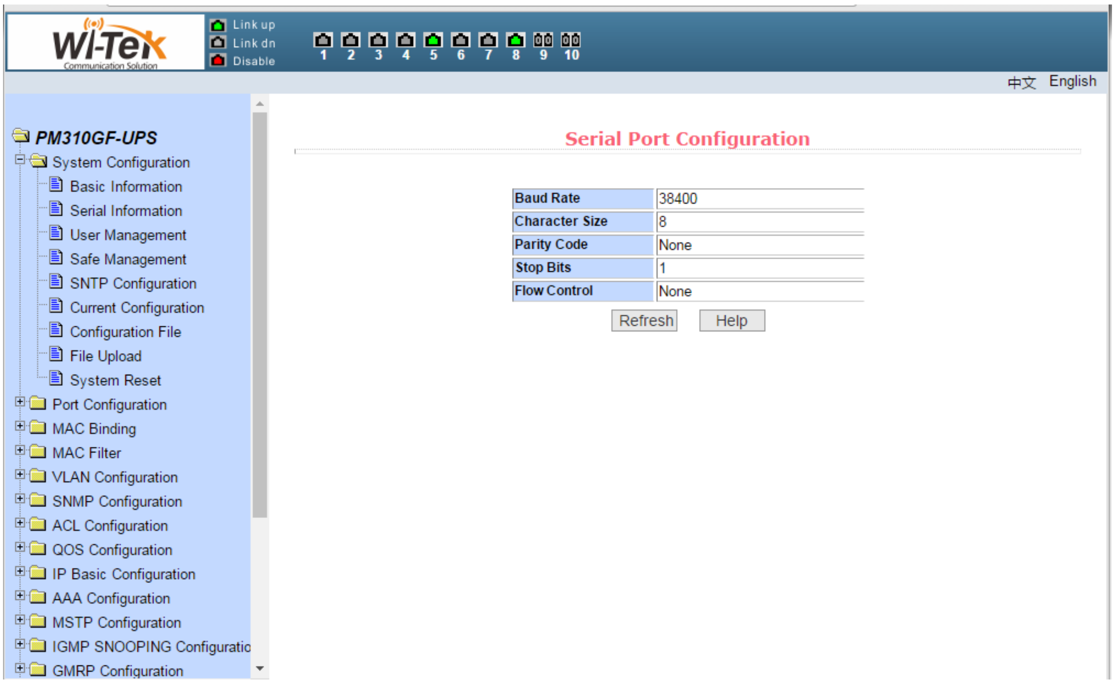
System Configuration

System Description	PM310GF-UPS 3.2.5
System Object ID	1.3.6.1.4.1.12284.1
System Version	PM310GF-UPS 3.2.5
Num Network Interfaces	11
System start time	0-Days 1-Hours 11-Minutes 13-Seconds
System Name	Switch
System Location	
System Contact	

Pic 9 Basic information page

（2）Serial port configuration page

Figure 10 shows the serial port configuration page, which shows the serial port baud rate and other information related to the serial port.When the host through the serial terminal (such as Windows HyperTerminal) to manage the switch, the serial port terminal COM port configuration must be consistent with the information on this page.



Serial Port Configuration

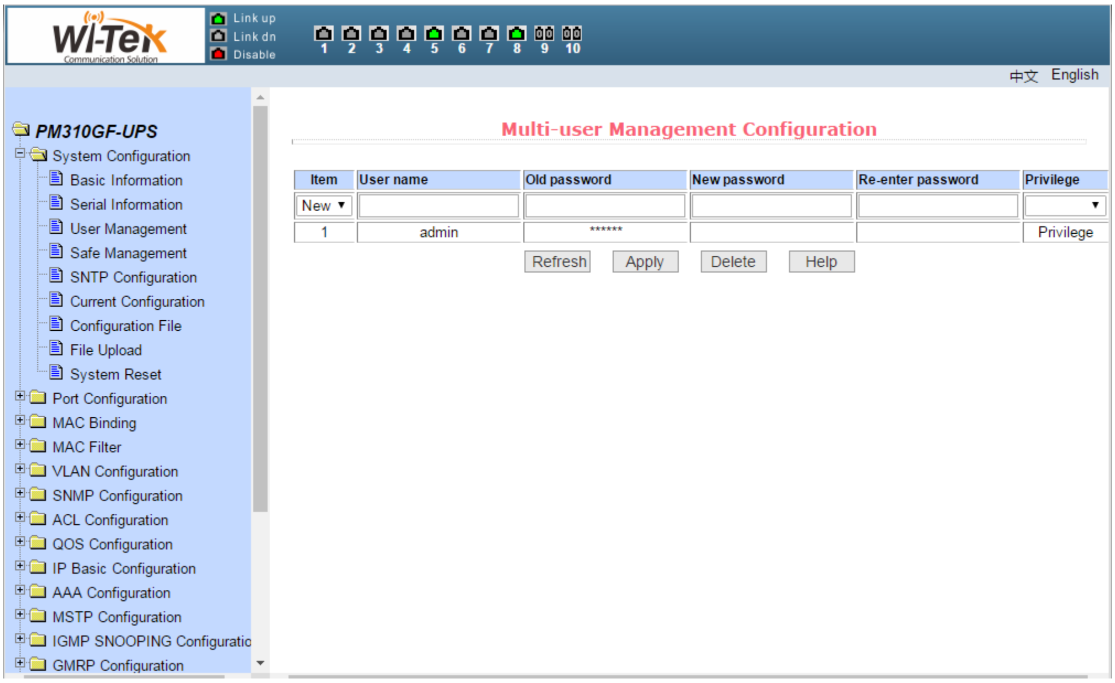
Baud Rate	38400
Character Size	8
Parity Code	None
Stop Bits	1
Flow Control	None

Pic 10 Serial port configuration page

（3）Multi-user management configuration page

Figure 11 shows the Multi-user management configuration page, through this page users can modify the switch's anonymous user (admin) password.Telnet and Web use the same anonymous user password when multiple users are not enabled.Passwords are case sensitive and you can set up to 16 characters at most.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 is activated,If the switch does not enable multi-user, will display the login dialog box (shown in Figure 7), the user needs to re-login page, the user must enter a new anonymous user password login WEB page.

At the same time through this page users can configure multiple users, the switch default no multi-user, that is the default does not enable multi-user management functions, then login does not require multi-user user name and password authentication.For Telnet, when adding a user name, the multi-user management function is enabled, and when all the users are deleted, the multi-user management function is turned off again.For the Web, when a user name is added, if be the privileged user,the multi-user management function is enabled, when all the privileged users are deleted, the multi-user management function is closed again.When the multi-user management function is enabled, the anonymous user password will not take effect, login Telnet and Web need to multi-user user name and password authentication.When the multi-user management function is closed, at this time if the anonymous user password is configured, login Telnet and Web need to anonymous user password verification.



Multi-user Management Configuration

Item	User name	Old password	New password	Re-enter password	Privilege
New ▾					▾
1	admin	******			Privilege

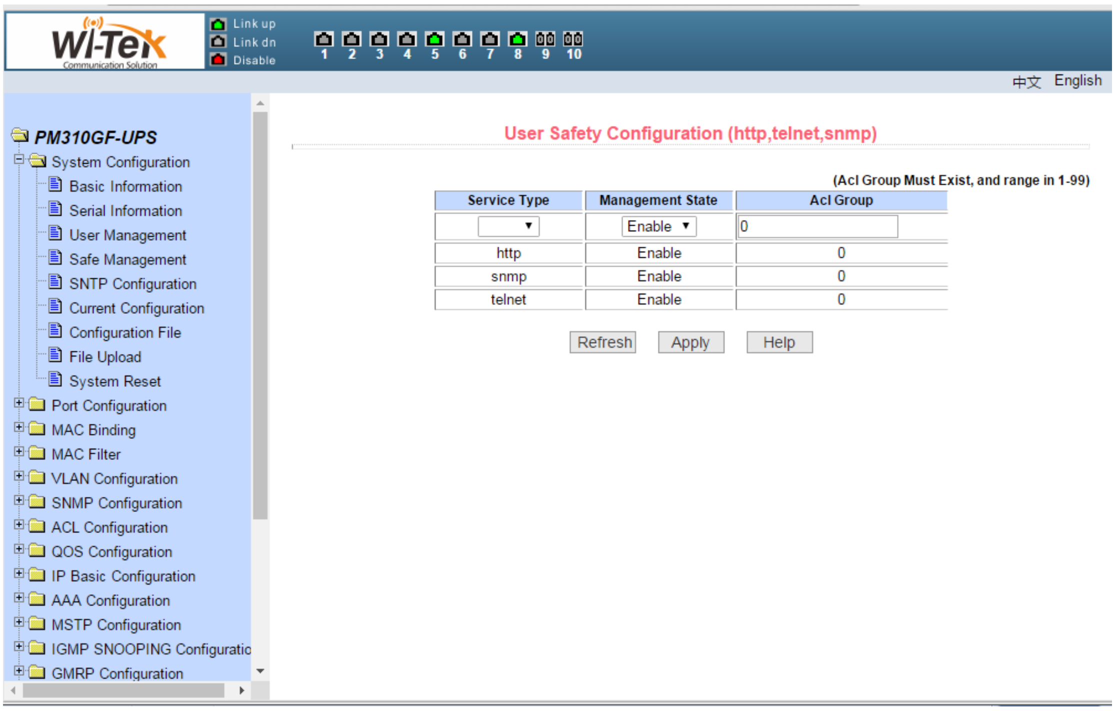
Pic 11 Multi-user management configuration page

（4）User safety configuration page

Figure 12 shows the user safety configuration page, through the configuration of the page, the administrator can control the network management services TELNET, WEB and SNMP control, you can open or close these services,These services can be linked with the IP standard ACL group, the implementation of source IP address control, control the host access to these services.

Switch by default TELNET, WEB and SNMP services are open, and do not do ACL filtering, that is, all the hosts can access the switch of these three services.If the administrator for security, do not want to provide other users one or several of these services, can shut down one or more of these services.Administrators only want a specific host to access one or more of these services, can one or several of these services do ACL filtering.When a service needs to do ACL filtering, you need to open the service and select an IP standard ACL group (1-99). The ACL group must exist.

It should be noted that if the administrator on this page to control the WEB service (such as the closure of WEB services) may make users can no longer use the WEB page,At this time through other ways to log on the switch and control WEB services so that users can use the WEB page (such as open the WEB service).



User Safety Configuration (http,telnet,snmp)

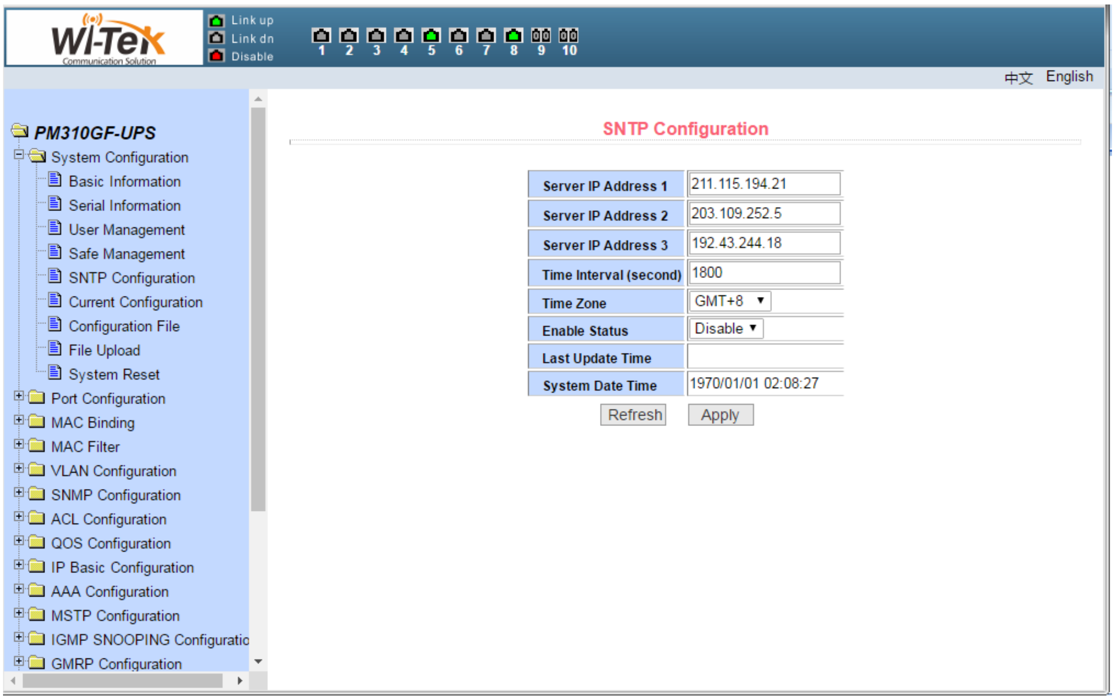
(Acl Group Must Exist, and range in 1-99)

Service Type	Management State	Acl Group
▾	Enable ▾	0
http	Enable	0
snmp	Enable	0
telnet	Enable	0

Pic 12 User safety configuration page

（5）SNTP configuration page

Figure 13 shows the SNTP configuration page, where the administrator can configure and view the system clock through configuration of the page.



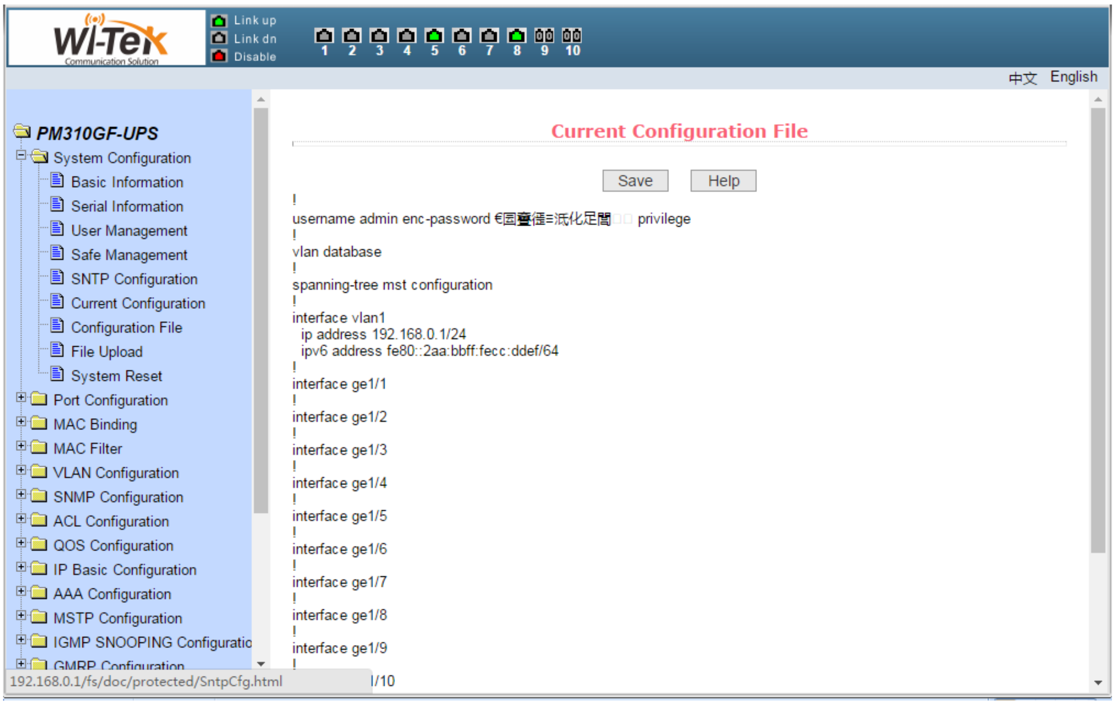
SNTP Configuration

Server IP Address 1	211.115.194.21
Server IP Address 2	203.109.252.5
Server IP Address 3	192.43.244.18
Time Interval (second)	1800
Time Zone	GMT+8 ▾
Enable Status	Disable ▾
Last Update Time	
System Date Time	1970/01/01 02:08:27

Pic 13 SNTP configuration page

（6）Current configuration file page

Figure 14 shows the current configuration file 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 storage operation needs to erase the FLASH chip, which takes a certain amount of time.When the user is configured on the page and want the configuration is not lost after restart the switch , you must click the Save button before exit the page in the current configuration page.

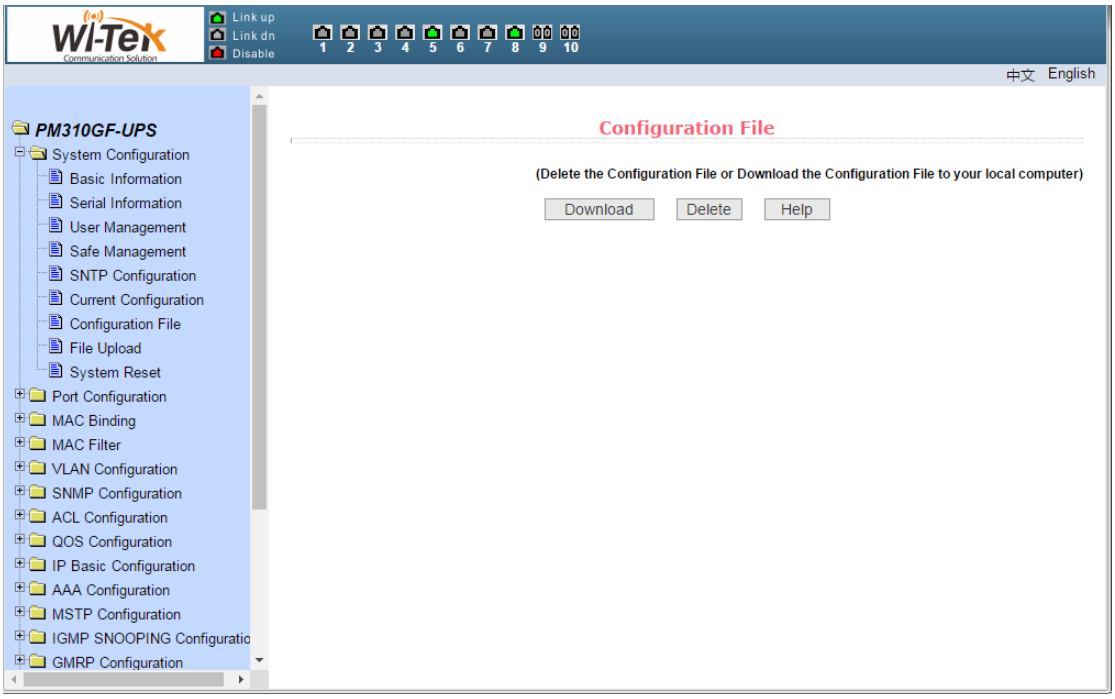


```
!
username admin enc-password €国亹徨=泜化足閭□□ privilege
!
vlan database
!
spanning-tree mst configuration
!
interface vlan1
  ip address 192.168.0.1/24
  ipv6 address fe80::2aa:bbff:fecc:ddef/64
!
interface ge1/1
!
interface ge1/2
!
interface ge1/3
!
interface ge1/4
!
interface ge1/5
!
interface ge1/6
!
interface ge1/7
!
interface ge1/8
!
interface ge1/9
!
l/10
```

Pic 14 Current configuration file page

（7）Configuration file page

Figure 15 shows Configuration file page.This page allows the user to view the initial configuration of the system.The initial configuration is actually the configuration file in the FLASH,When there is no configuration file in FLASH, the system is started with the default configuration.Delete key to delete the configuration file in FLASH.Click the delete button, will pop up a dialog box, the dialog box prompts the user whether to determine the deletion of the configuration file, if determined by the dialog box on the OK button, otherwise press the Cancel button.The download key is used to download the configuration file to the PC.Click the download button, will pop up a dialog box, the user chooses to save the directory path and save the configuration file. The file name of the downloaded configuration file is switch.cfg.



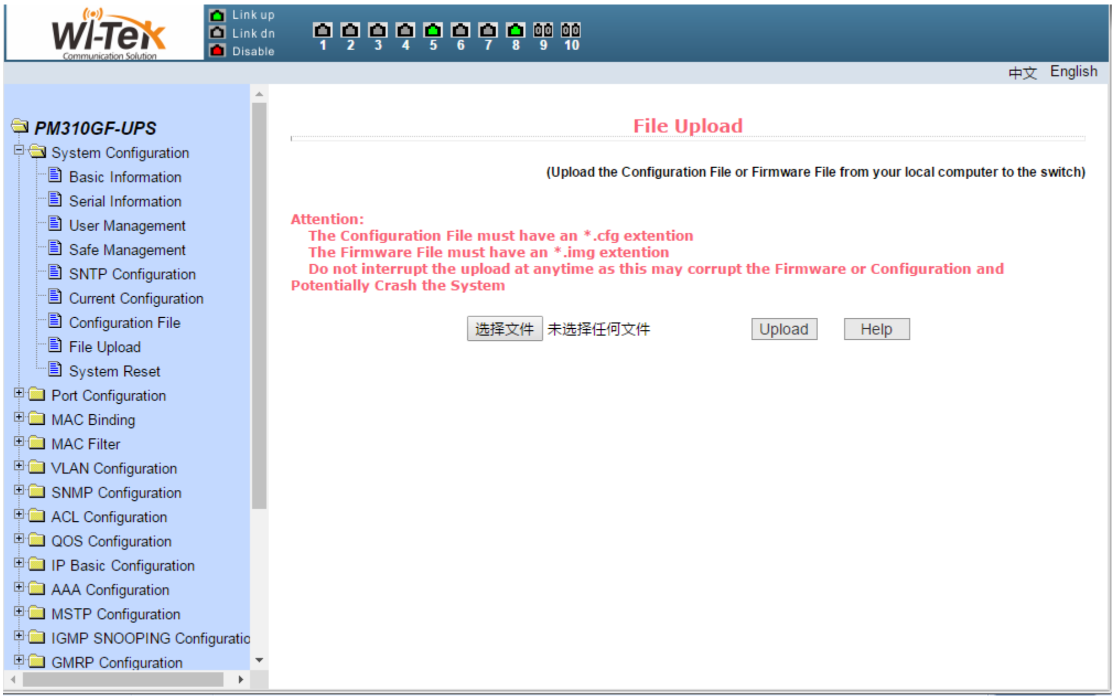
Configuration File

(Delete the Configuration File or Download the Configuration File to your local computer)

Pic 15 Configuration file page

（8）File upload page

Figure 16 shows the file upload page, through which users can upload configuration files and image files to the switch.Click the Browse button to select the directory path of the uploaded profile or image file on the PC.Click the upload key to upload the configuration file or image file. The configuration file suffix must be * .cfg. The image file must be provided by the manufacturer and the file name suffix must be * .img. Do not click on other pages or reboot the switch before the transfer results page returns. Otherwise, the file transfer failure causes the system to crash.



File Upload

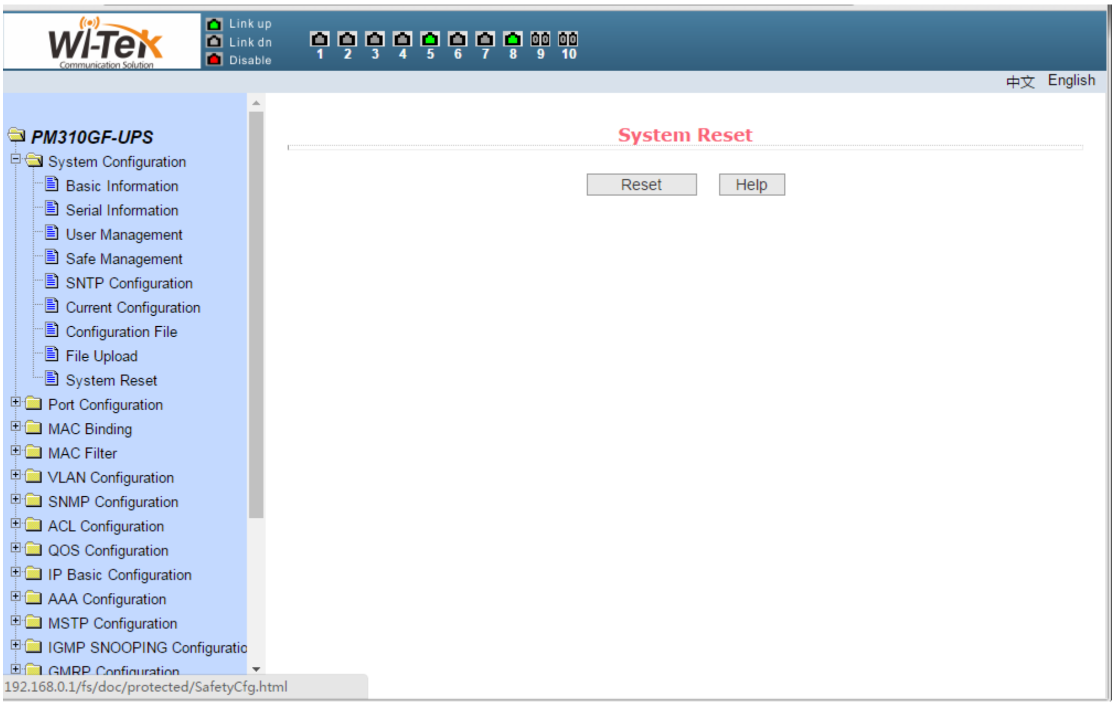
(Upload the Configuration File or Firmware File from your local computer to the switch)

Attention:
The Configuration File must have an *.cfg extention
The Firmware File must have an *.img extention
Do not interrupt the upload at anytime as this may corrupt the Firmware or Configuration and Potentially Crash the System

Pic 16 File upload page

（9）System reset page

Figure 17 shows the system reset page, through this page users to restart the switch.When you click the restart button, a dialog box will pop up prompting you if the user is sure to restart the switch. If OK, press the OK key. Otherwise, press the Cancel key.The Web page will no longer be opened when it is restarted.



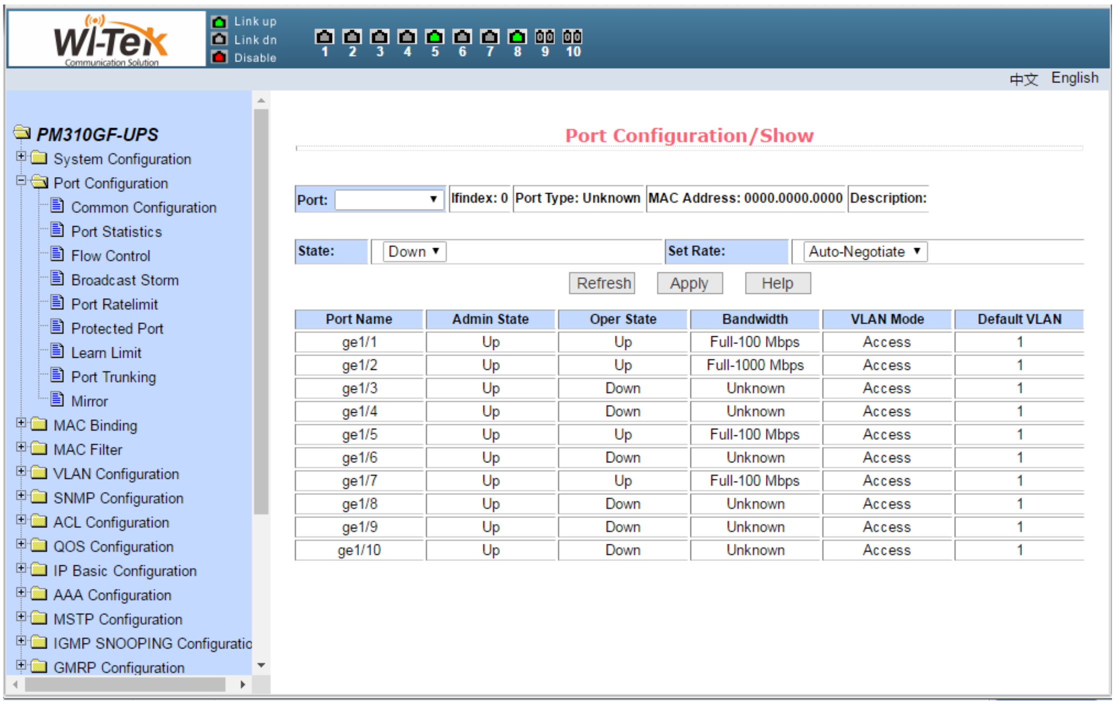
Pic 17 System reset page

4、Port configuration

（1）Port configuration/show page

Figure 18 shows the port configuration/show page.The user can enable or disable the port through this page, set the port speed, or view the basic information of all ports.

To set a specific port, select the appropriate port name in the drop-down menu for the user's port.Port status defaults to up, and you can select the down in the drop-down menu to disable the port.The user can also choose to set the speed drop-down menu to set the speed of the port, such as the mandatory semi-duplex for the port, 10M (half - 10), etc. Users can view other basic information for all ports from this page.



Port Configuration/Show

Port: ▾ | Ifindex: 0 | Port Type: Unknown | MAC Address: 0000.0000.0000 | Description:

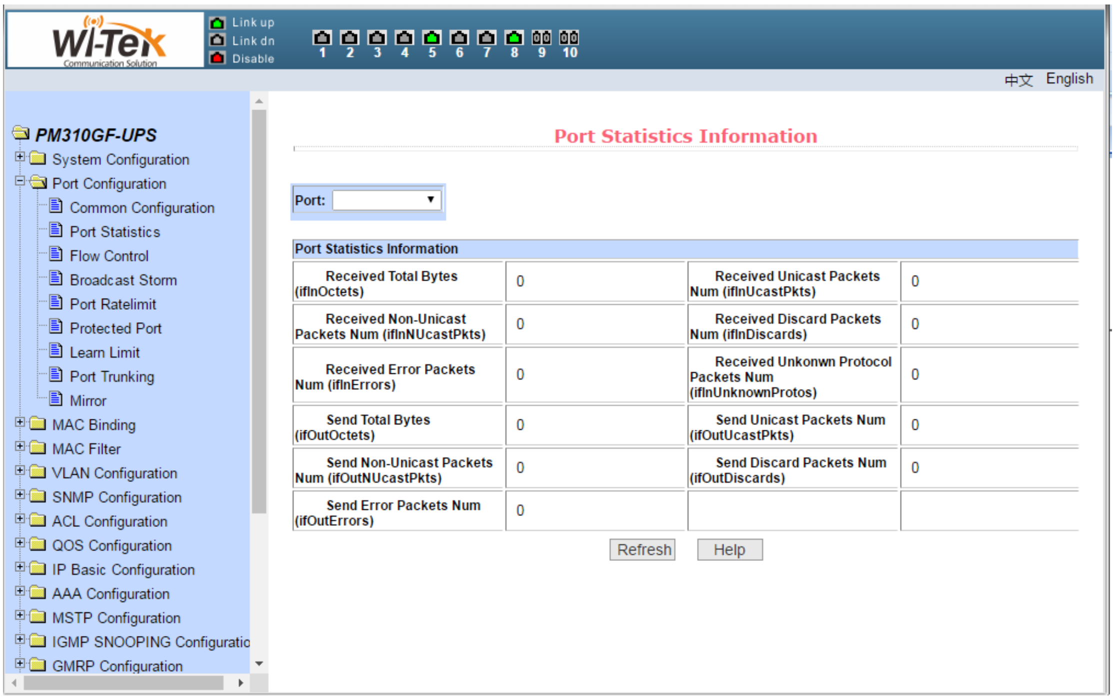
State: Down ▾ | Set Rate: Auto-Negotiate ▾

Port Name	Admin State	Oper State	Bandwidth	VLAN Mode	Default VLAN
ge1/1	Up	Up	Full-100 Mbps	Access	1
ge1/2	Up	Up	Full-1000 Mbps	Access	1
ge1/3	Up	Down	Unknown	Access	1
ge1/4	Up	Down	Unknown	Access	1
ge1/5	Up	Up	Full-100 Mbps	Access	1
ge1/6	Up	Down	Unknown	Access	1
ge1/7	Up	Up	Full-100 Mbps	Access	1
ge1/8	Up	Down	Unknown	Access	1
ge1/9	Up	Down	Unknown	Access	1
ge1/10	Up	Down	Unknown	Access	1

Pic 18 Port configuration/show page

（2）Port statistics information page

Figure 19 shows the port statistics information page.To view a particular port, select the appropriate port name in the drop-down menu for the user's port.Users can view the statistics of the port send and receive packet through this page.



Port Statistics Information

Port: ▾

Port Statistics Information

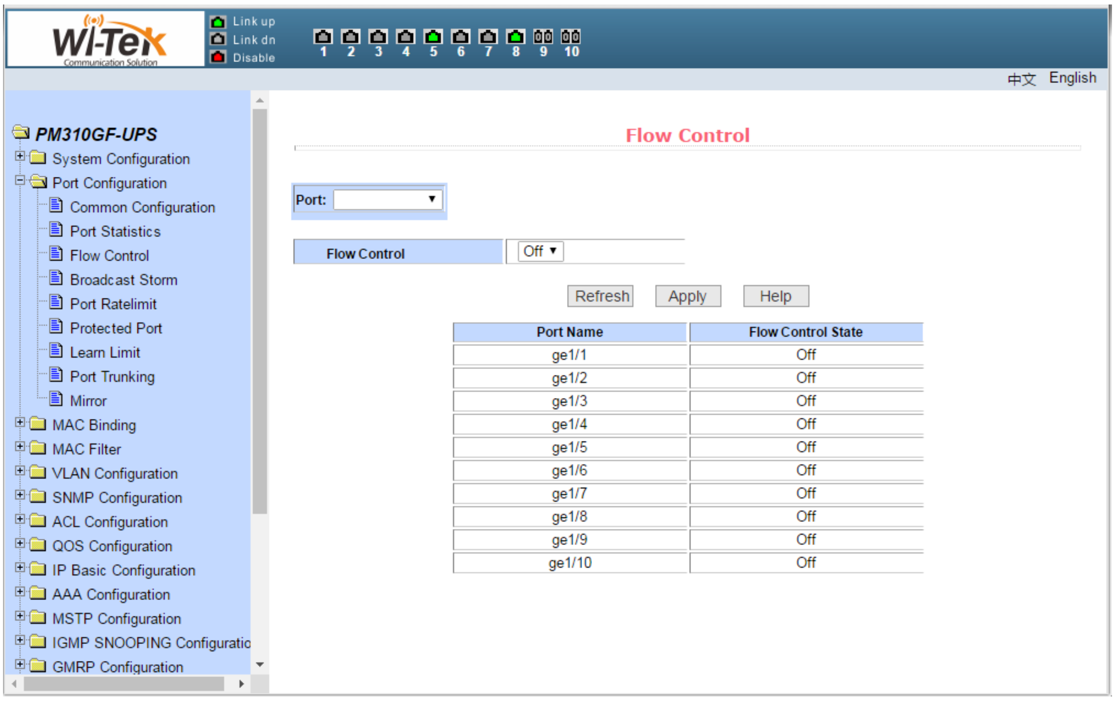
Received Total Bytes (ifInOctets)	0	Received Unicast Packets Num (ifInUcastPkts)	0
Received Non-Unicast Packets Num (ifInNUcastPkts)	0	Received Discard Packets Num (ifInDiscards)	0
Received Error Packets Num (ifInErrors)	0	Received Unkonwn Protocol Packets Num (ifInUnknownProtos)	0
Send Total Bytes (ifOutOctets)	0	Send Unicast Packets Num (ifOutUcastPkts)	0
Send Non-Unicast Packets Num (ifOutNUcastPkts)	0	Send Discard Packets Num (ifOutDiscards)	0
Send Error Packets Num (ifOutErrors)	0		

Pic 19 Port statistics information page

（3）Flow control page

Figure 20 shows the flow control page.The user can use this page to open or close the flow control for each port.

Through the drop-down on or off of the flow control to open or close a port flow control.At the same time through this page you can view the flow control status of all ports.



Flow Control

Port:

Flow Control: Off

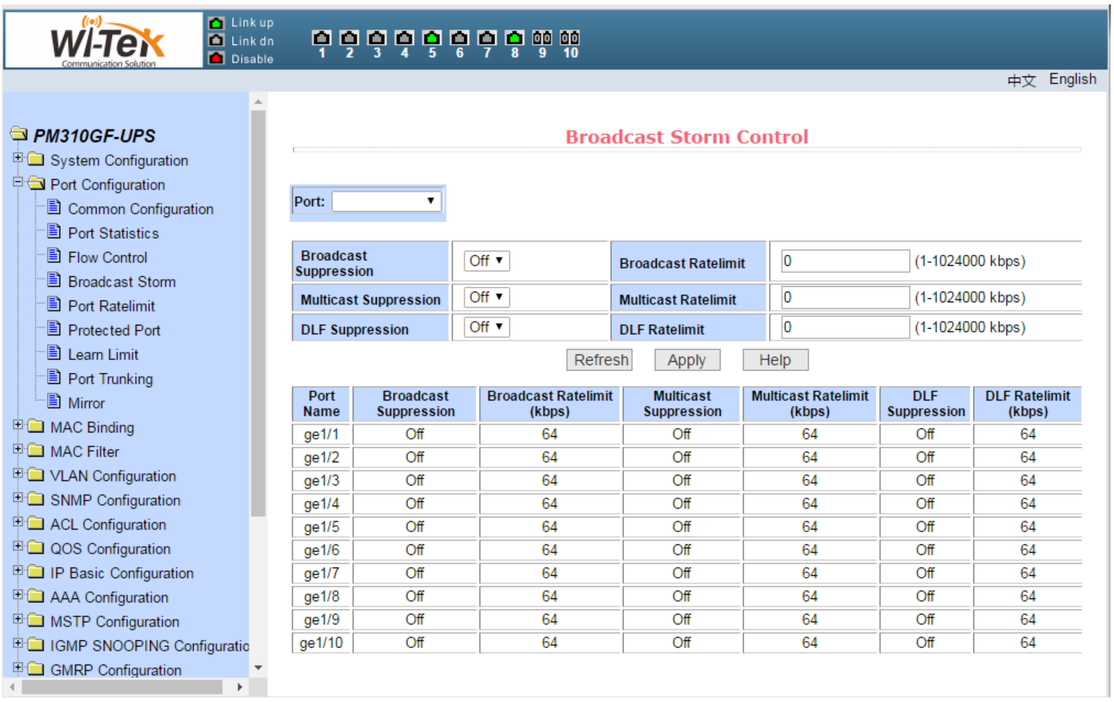
Port Name	Flow Control State
ge1/1	Off
ge1/2	Off
ge1/3	Off
ge1/4	Off
ge1/5	Off
ge1/6	Off
ge1/7	Off
ge1/8	Off
ge1/9	Off
ge1/10	Off

Pic 20 Flow control page

（4）Broadcast storm control page

Figure 21 shows the broadcast storm control page.This page is used to configure suppression the broadcast packets, multicast packets, and DLF packets on the port.

Select the port to be configured from the drop-down bar of the port.On and off to enable and disable broadcast suppression, multicast suppression, and DLF suppression of the port.The suppression rate term is used to configure the rate of suppression of the port, in the range of 1-1024000, in kbits.The suppression rates of broadcast suppression, multicast suppression, and DLF suppression on the same port are equal.At the same time, through this page, you can view all ports broadcast storm control configuration.



Broadcast Storm Control

Port:

Broadcast Suppression	Off	Broadcast Ratelimit	0	(1-1024000 kbps)
Multicast Suppression	Off	Multicast Ratelimit	0	(1-1024000 kbps)
DLF Suppression	Off	DLF Ratelimit	0	(1-1024000 kbps)

Port Name	Broadcast Suppression	Broadcast Ratelimit (kbps)	Multicast Suppression	Multicast Ratelimit (kbps)	DLF Suppression	DLF Ratelimit (kbps)
ge1/1	Off	64	Off	64	Off	64
ge1/2	Off	64	Off	64	Off	64
ge1/3	Off	64	Off	64	Off	64
ge1/4	Off	64	Off	64	Off	64
ge1/5	Off	64	Off	64	Off	64
ge1/6	Off	64	Off	64	Off	64
ge1/7	Off	64	Off	64	Off	64
ge1/8	Off	64	Off	64	Off	64
ge1/9	Off	64	Off	64	Off	64
ge1/10	Off	64	Off	64	Off	64

Pic 21 Broadcast storm control page

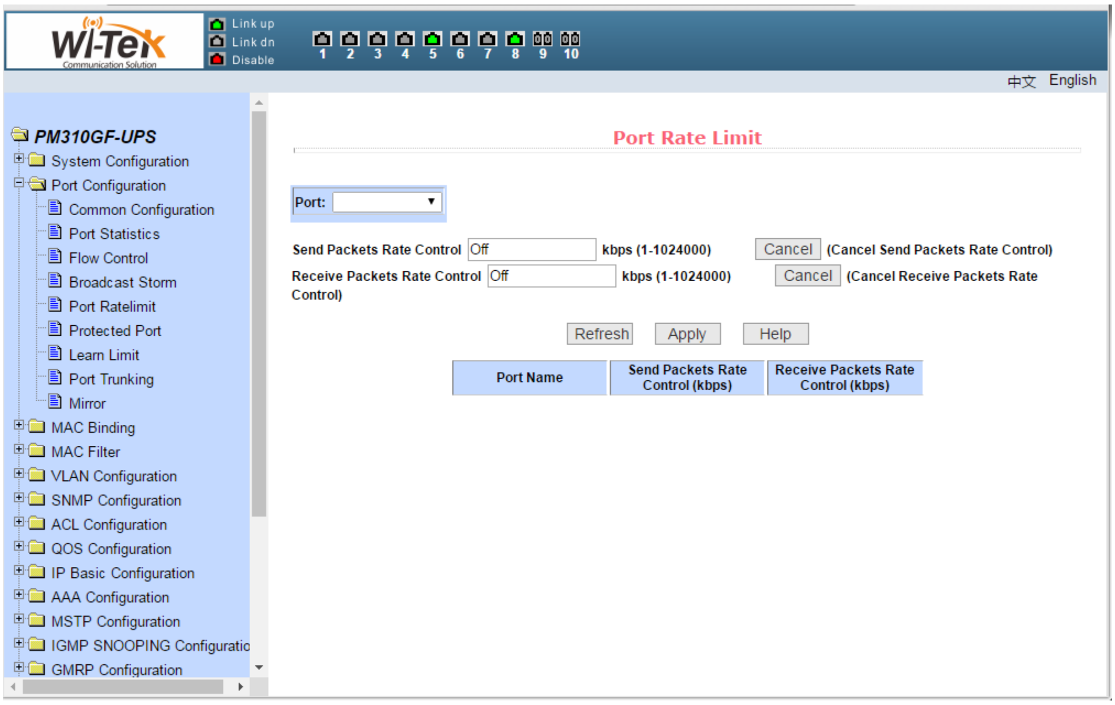
（5）Port rate limit page

Figure 22 shows the port rate limit page。This page is used to configure the rate at which ports are sent and received.

- Select the port to be configured from the drop-down bar of the port.The transmit packet bandwidth control is used to configure and display the bandwidth control of the sending data packet, in the range of 1-1024000, in kbits, after enter, 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 the sending data packet.The receive data packet bandwidth control is used to configure and display the bandwidth control of the received packet, in the range of 1-1024000, in kbits,after enter, 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 the receiving data packet.

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



Port Rate Limit

Port:

Send Packets Rate Control Off kbps (1-1024000) (Cancel Send Packets Rate Control)

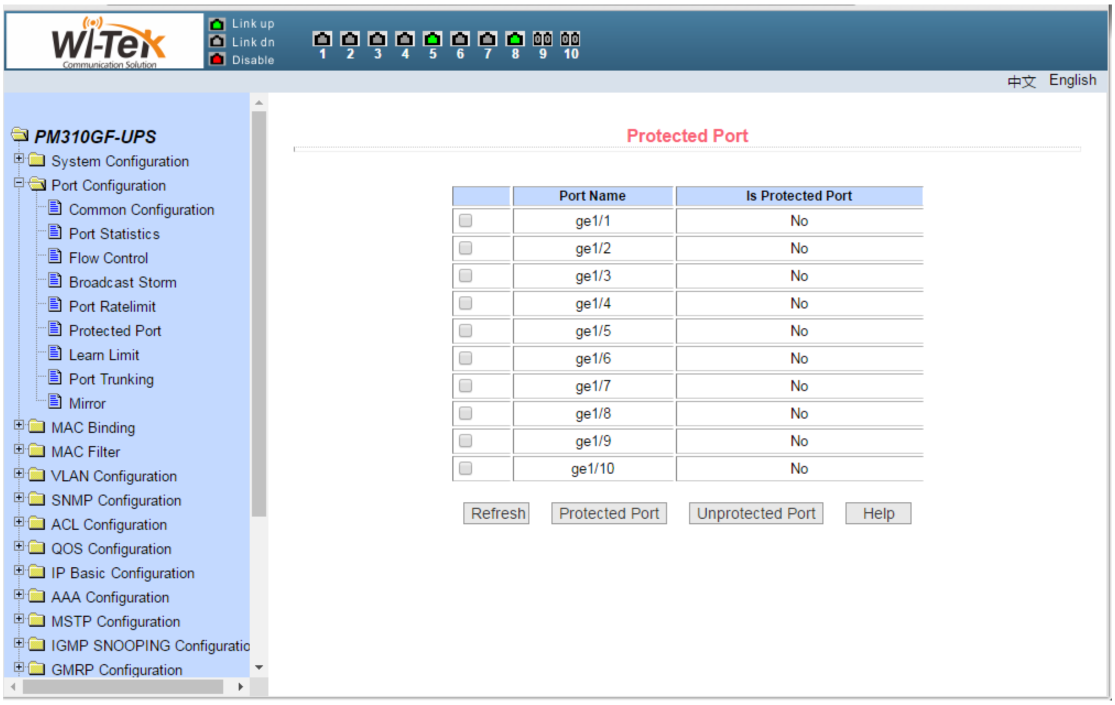
Receive Packets Rate Control Off kbps (1-1024000) (Cancel Receive Packets Rate Control)

Port Name	Send Packets Rate Control (kbps)	Receive Packets Rate Control (kbps)

Pic 22 Port rate limit page

（6）Protected port page

Figure 23 shows the protected port page。This page is used to configure the protection port.



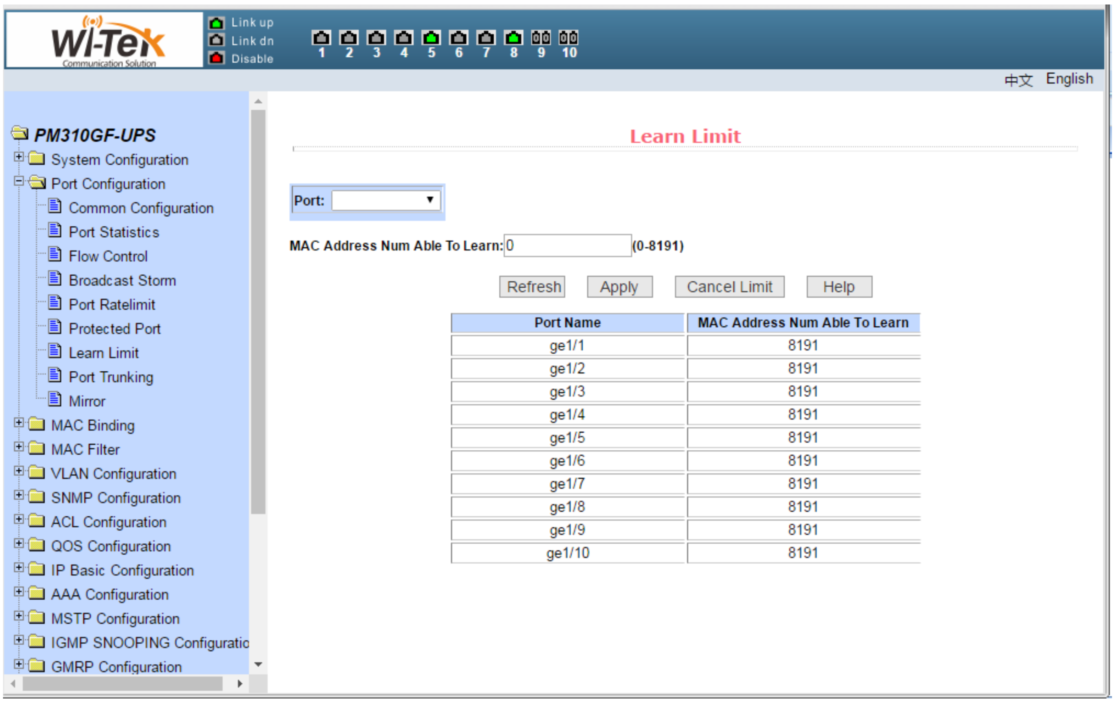
Protected Port

	Port Name	Is Protected Port
□	ge1/1	No
□	ge1/2	No
□	ge1/3	No
□	ge1/4	No
□	ge1/5	No
□	ge1/6	No
□	ge1/7	No
□	ge1/8	No
□	ge1/9	No
□	ge1/10	No

Pic 23 Protected port page

（7）Port learn limit page

- Figure 24 shows the port learn limit page。 This page is used to limit the number of MAC addresses that the port can learn. The range is 0-8191.The default value is 8191, which is also the maximum value, indicating that the port is not configured with learning restrictions.The list shows the learning limits for all ports.



Learn Limit

Port:

MAC Address Num Able To Learn: 0 (0-8191)

Port Name	MAC Address Num Able To Learn
ge1/1	8191
ge1/2	8191
ge1/3	8191
ge1/4	8191
ge1/5	8191
ge1/6	8191
ge1/7	8191
ge1/8	8191
ge1/9	8191
ge1/10	8191

Pic 24 Port learn limit page

（8）Port trunking configuration page

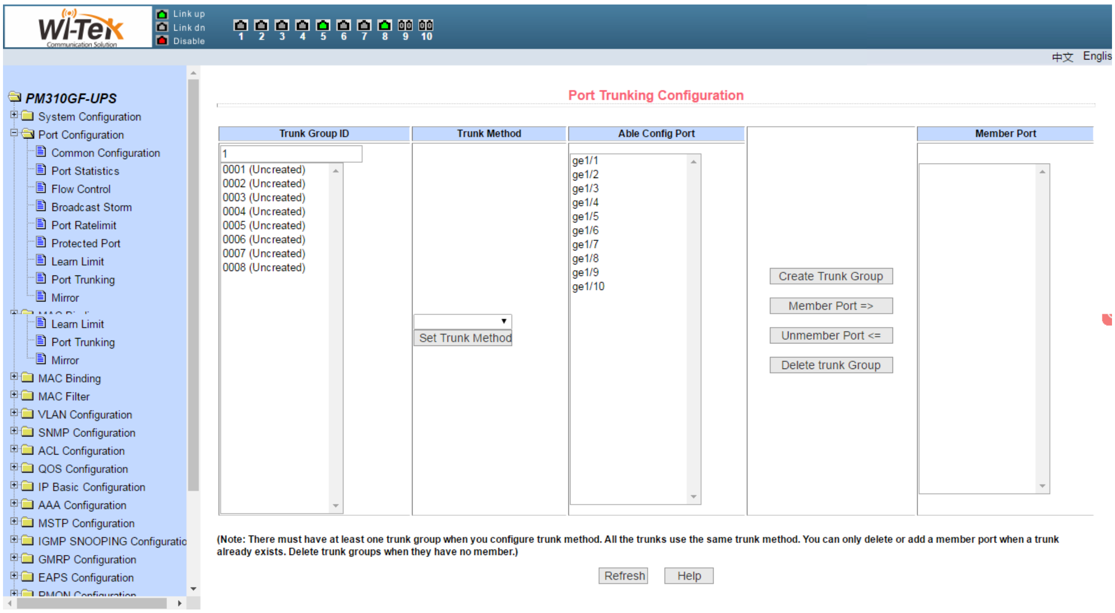
- Figure 25 shows the port trunking configuration page.This page allows the user to configure port aggregation.The page consists of four parts: Trunk group ID selection, set the aggregation method, configurable port and group member port.
- To create or modify port aggregation, the user needs to select a trunk group ID from ID 1 to 8.The user clicks the corresponding trunk group ID in the list box. 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, click the button "Create Trunk Group",if successful, the bracket annotation is created in the ID display bar. If a Trunk group is not created, the bracket annotation is not created in the ID display bar. To set the port aggregation method, select an aggregation method in the drop-down box above the list and click the "Set up aggregation method" button.To add an aggregated port, select the aggregated port in the configurable port and click the "Member Port =>" button.To remove a port from an existing port, select the aggregated port in the group member port and click the "Non-member port <=" key.To delete the entire Trunk group, click the

Delete Trunk Group key.

During the page configuration process, the aggregation method is configured to correspond to the selected trunk group ID. The existing Trunk group can configure the aggregation method. You can add or remove member ports on the existing Trunk. In the case of no member ports, To delete a Trunk group.

The switch provides six types of port aggregation: based on the source MAC address, based on the destination MAC address, based on the source and destination MAC addresses, based on the source IP address, based on the destination IP address, based on the source and destination IP addresses.

The switch supports up to eight groups of port aggregation. Each group of port aggregation supports up to eight ports. Each trunk group can configure its own port aggregation method.



Port Trunking Configuration

Trunk Group ID	Trunk Method	Able Config Port		Member Port
1 0001 (Uncreated) 0002 (Uncreated) 0003 (Uncreated) 0004 (Uncreated) 0005 (Uncreated) 0006 (Uncreated) 0007 (Uncreated) 0008 (Uncreated)		ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10		

(Note: There must have at least one trunk group when you configure trunk method. All the trunks use the same trunk method. You can only delete or add a member port when a trunk already exists. Delete trunk groups when they have no member.)

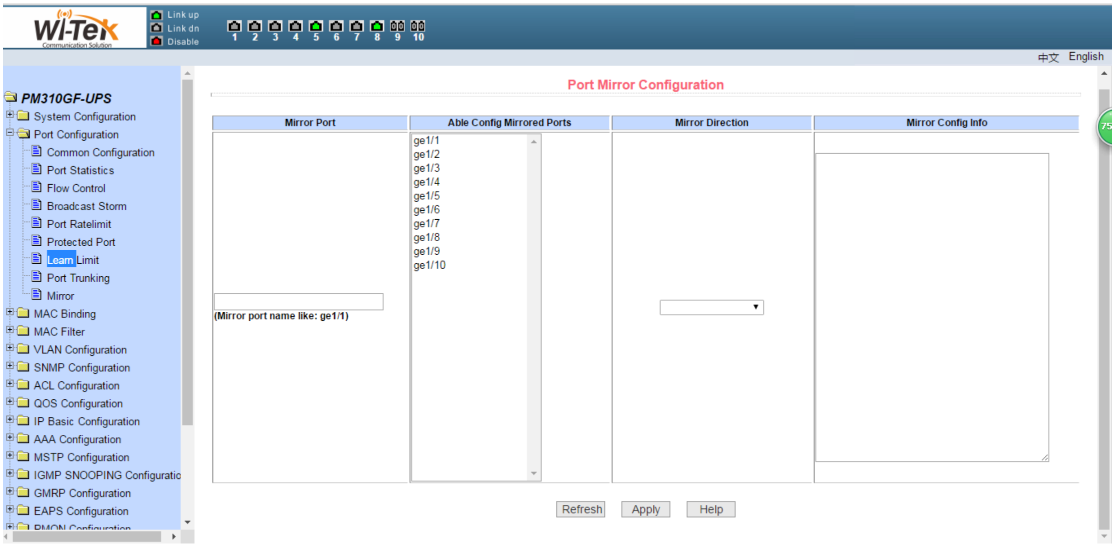
Pic 25 Port trunking configuration page

（9）Port mirror configuration page

- Figure 26 shows the Port mirror configuration page，This page allows the user to

  configure port mirroring.Port mirroring is through the mirror port to monitor the output of the mirror output port and the mirror input port input data packets.Mirror port can only select one, and the mirror output port and the mirror input port can choose multiple.The page consists of four parts: listening port, configurable port, listening direction and mirroring configuration information.Configure a mirroring port to configure a mirroring port from the listening port. Only one port can be selected from the listening port. Select the mirrored port from the configurable port, select the listening direction from the listening direction, and press the Apply key. The result will be The mirror configuration information is displayed.

When the RECEIVE in the listening direction is selected, it indicates that the received packet is received, TRANSMIT indicates the packet to be sent, BOTH indicates all the packets that are being sent and received, NOT_RECEIVE indicates that the received packet is canceled, NOT_TRANSMIT indicates that the packet is canceled Of the packet, NEITHER that cancel the monitor received and sent the packet, that is, to cancel the listening port.



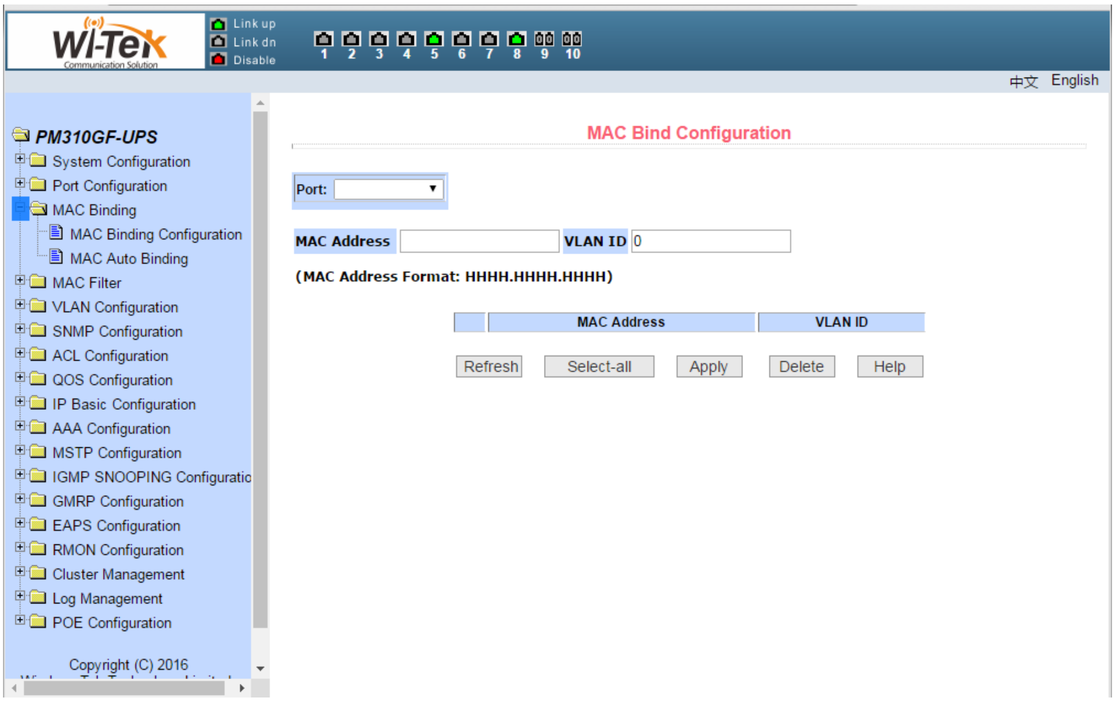
Pic 26 Port mirror configuration page

5、MAC Bind

（1）MAC bind configuration page

Figure 27 shows the MAC binding configuration page. This page is used to bind the port to the MAC address.

The MAC address on the page is used to enter the bound MAC address. The VLAN ID entry is used to enter the VLAN to which the MAC address belongs.



MAC Bind Configuration

Port:

MAC Address | VLAN ID 0

(MAC Address Format: HHHH.HHHH.HHHH)

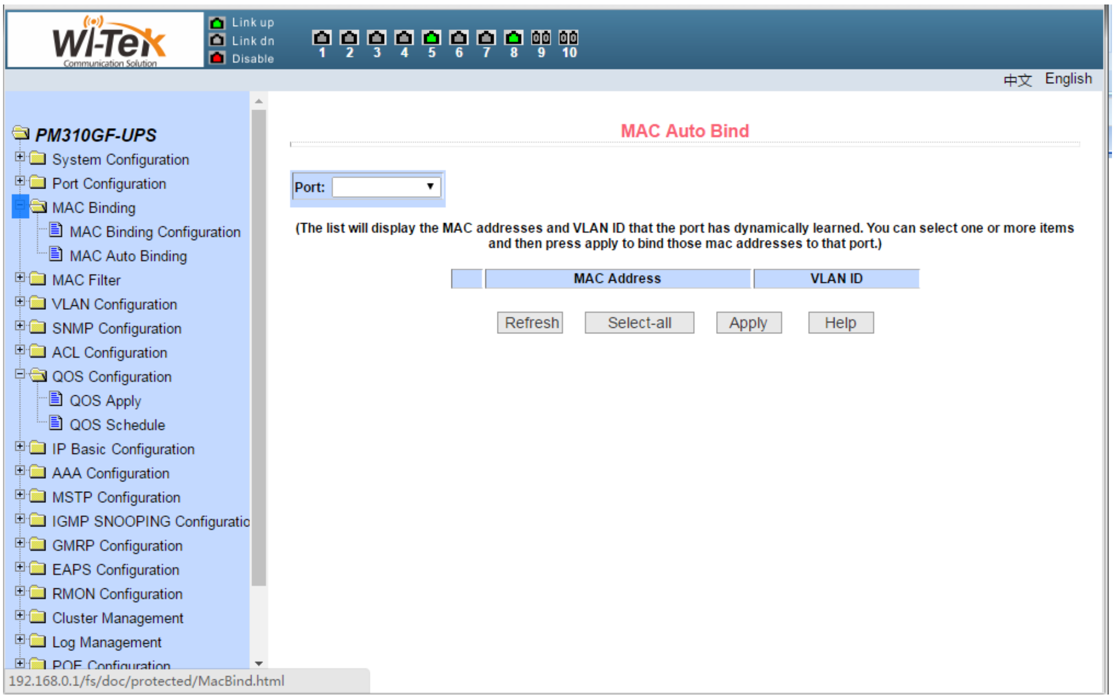
	MAC Address	VLAN ID

Pic 27 MAC bind configuration page

（2）MAC auto bind page

Figure 28 shows the MAC binding auto-conversion page. This page is used to implement the port automatically bind MAC address.

Displays the dynamic MAC address and the VLAN of the port in the two tier hardware forwarding table.You can select items from them and convert them into static bindings.



MAC Auto Bind

Port:

(The list will display the MAC addresses and VLAN ID that the port has dynamically learned. You can select one or more items and then press apply to bind those mac addresses to that port.)

	MAC Address	VLAN ID

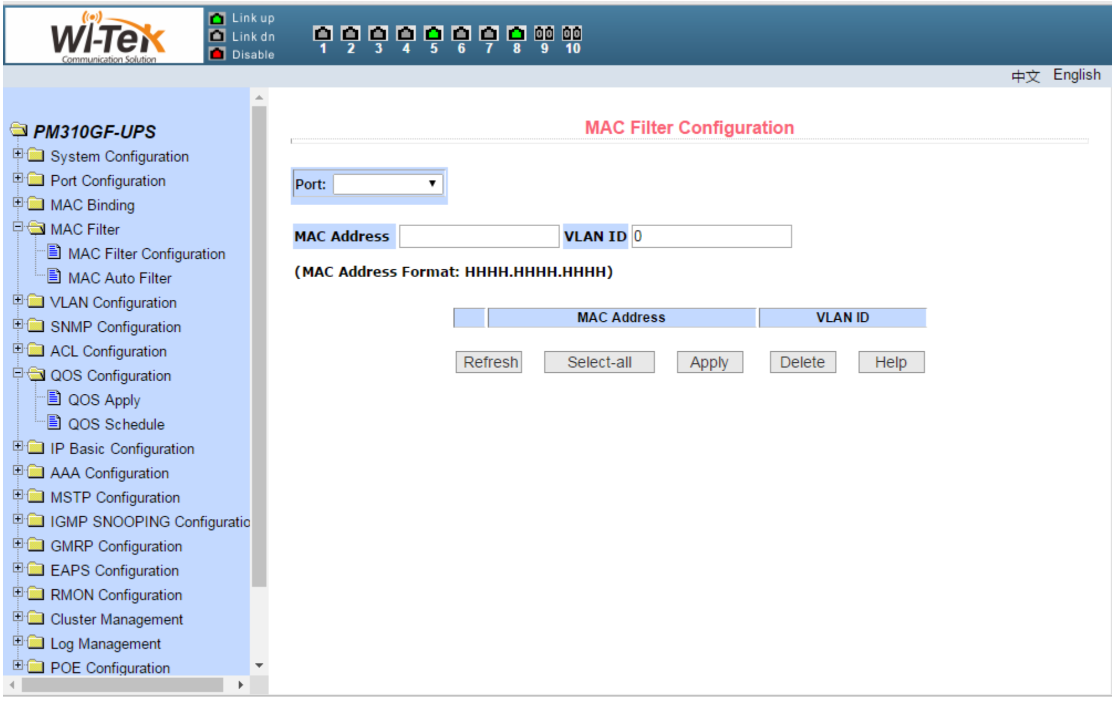
Pic 28 MAC auto bind page

6、MAC filter

（1）MAC filter configuration page

Figure 29 shows the MAC Filter Configuration page. This page is used to configure the port to filter the MAC address.

The MAC address on the page is used to enter the filtered MAC address. The VLAN ID entry is used to enter the VLAN to which the MAC address belongs.



MAC Filter Configuration

Port:

MAC Address: ____ VLAN ID: 0

(MAC Address Format: HHHH.HHHH.HHHH)

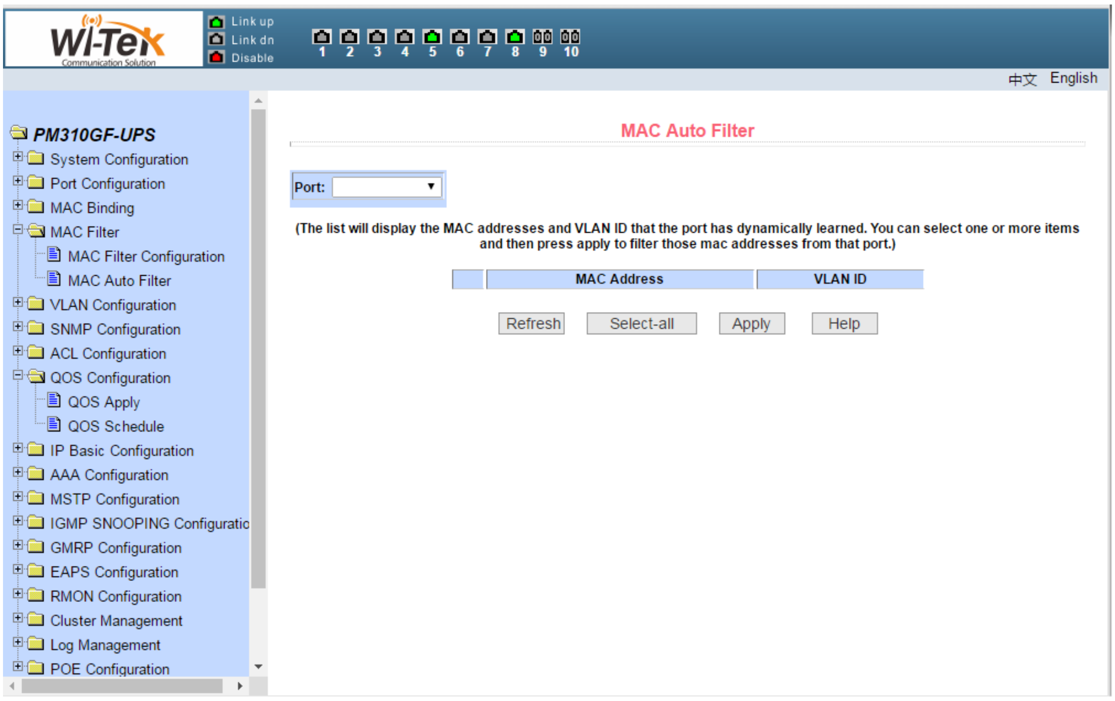
	MAC Address	VLAN ID

Pic 29 MAC filter configuration page

（2）MAC auto filter page

Figure 30 shows the MAC filter automatically convert the page. This page is used to implement the port automatically bind MAC address.

Display the dynamic MAC address and VLAN associated with the port in the Layer 2 hardware forwarding table. You can select an entry and convert it to a static filter configuration.



(The list will display the MAC addresses and VLAN ID that the port has dynamically learned. You can select one or more items and then press apply to filter those mac addresses from that port.)

	MAC Address	VLAN ID

Pic 30 MAC auto filter page

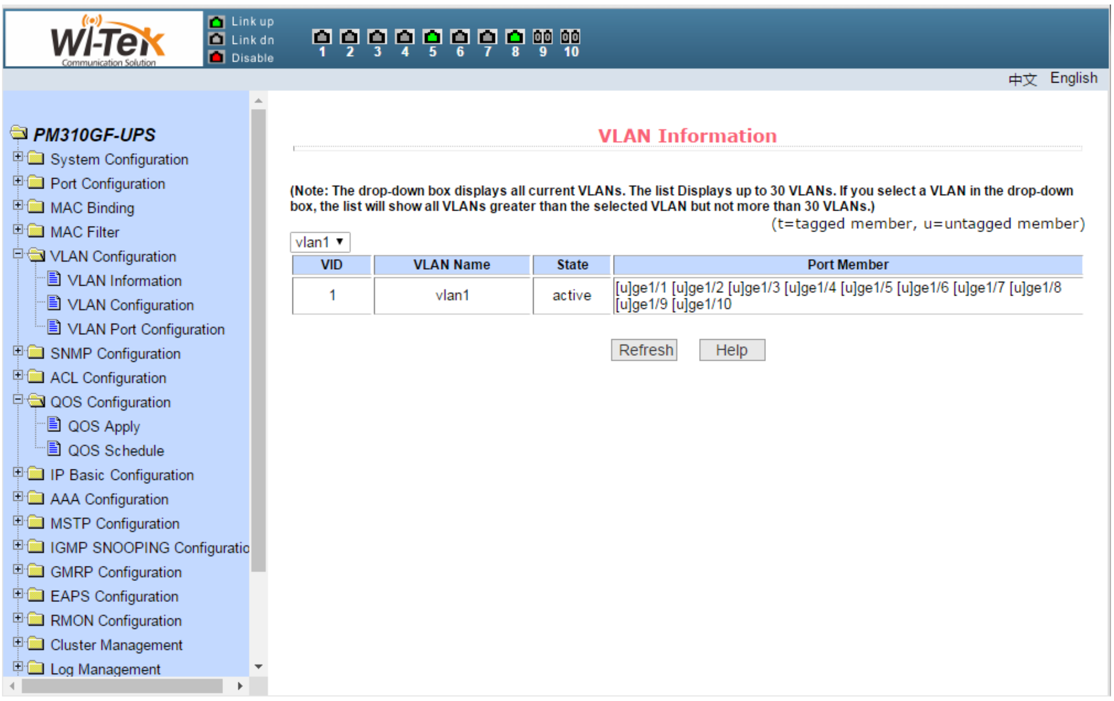
7、VLAN configuration

（1）VLAN information page

Figure 31 shows the current VLAN information page. The page is a read-only page that shows the current VLAN, VLAN status, and VLAN port members. Drop-down box will show all the current vlan, the list shows up to 30 vlan VID, state and port members.Select a vlan from the drop-down box, and the list will display information with a VID greater than 30 vlan for that vlan. But if all the vlan no more than 30, regardless of the drop-down box to choose which vlan, the list will show all the vlan information.

A port can not be a member of a VLAN, either a tagged member or a untagged member of a VLAN. The characters in the front of the page are as follows:

t	tagged	The port is a tagged member of this VLAN
u	untagged	The port is a untagged member of this VLAN



VLAN Information

(Note: The drop-down box displays all current VLANs. The list Displays up to 30 VLANs. If you select a VLAN in the drop-down box, the list will show all VLANs greater than the selected VLAN but not more than 30 VLANs.)

(t=tagged member, u=untagged member)

vlan1 ▾

VID	VLAN Name	State	Port Member
1	vlan1	active	[u]ge1/1 [u]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10

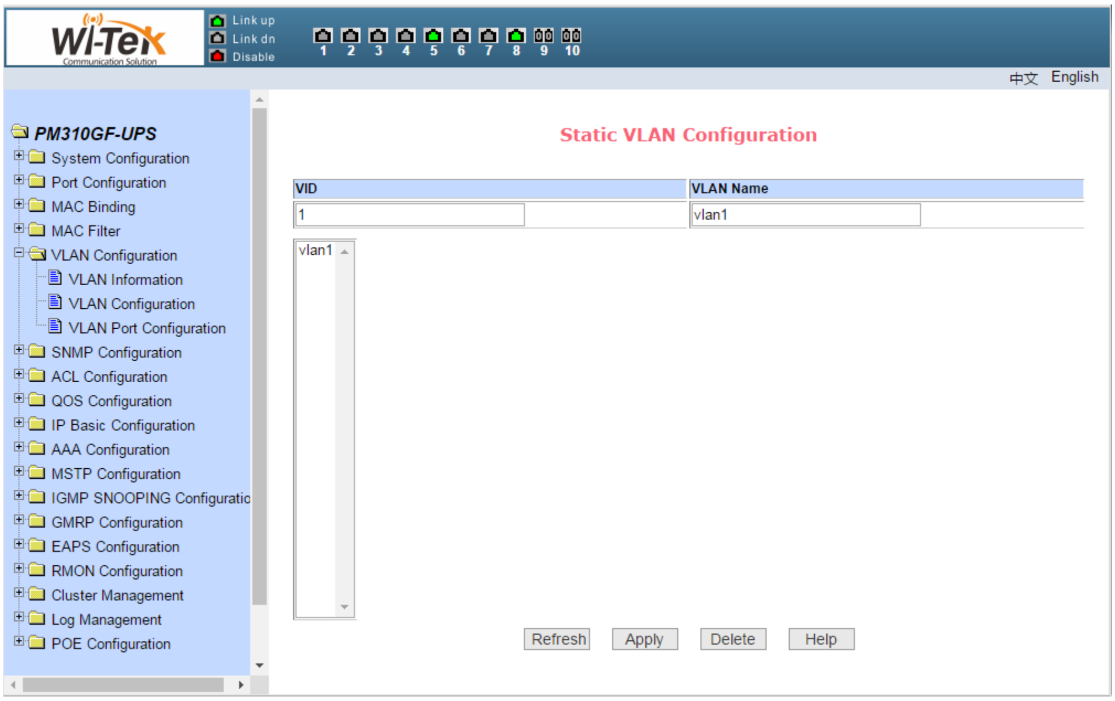
Pic32 VLAN information page

（2）Static VLAN conformation page

Figure 32 shows a static VLAN configuration page, which allows users to create VLAN.

If you want to create a new VLAN, the user enters a VID in the active line, ranging from 2 to 4094. The VLAN name is generated by the system according to the VLAN ID and can not be modified. Click the Apply key, and the list box displays the VID and VLAN name of the VLAN created by the user. The switch creates VLAN 1 by default, and VLAN 1 can not be deleted.

If you want to delete a VLAN, the user needs to click the corresponding VLAN in the list box. The VLAN will be displayed in the active line, click the Delete button to delete the VLAN, and the VLAN information will be removed from the list box.。



VID	VLAN Name
1	vlan1

vlan1

Pic 32 Static VLAN conformation page

（3）VLAN port configuration page

Figure 33 shows the VLAN port configuration page, which is used to configure VLAN on the port and display the results of the configuration. The page consists of eight parts: port, mode, all current VLAN, ports owned by VLAN, "default VLAN =>", "tagged =", "untagged =>" and "non-member <=".

The port is the port that specifies the VLAN to be configured.

Mode The port specifies the port's VLAN mode as ACCESS mode. In this VLAN mode, the port defaults to untagged members of VLAN1. The default VLAN of the port is 1. The VLAN mode of the hybrid port is HYBRID mode. In this VLAN mode, the port is the untagged member of VLAN1, and the default VLAN of the port is 1. The VLAN mode of the trunk port is Trunk mode. In this VLAN mode, the default port is the tagged member of VLAN1, and the default VLAN of the port is 1.

All the current VLAN are VLAN that can be created by the port. Users can select VLAN from the list.

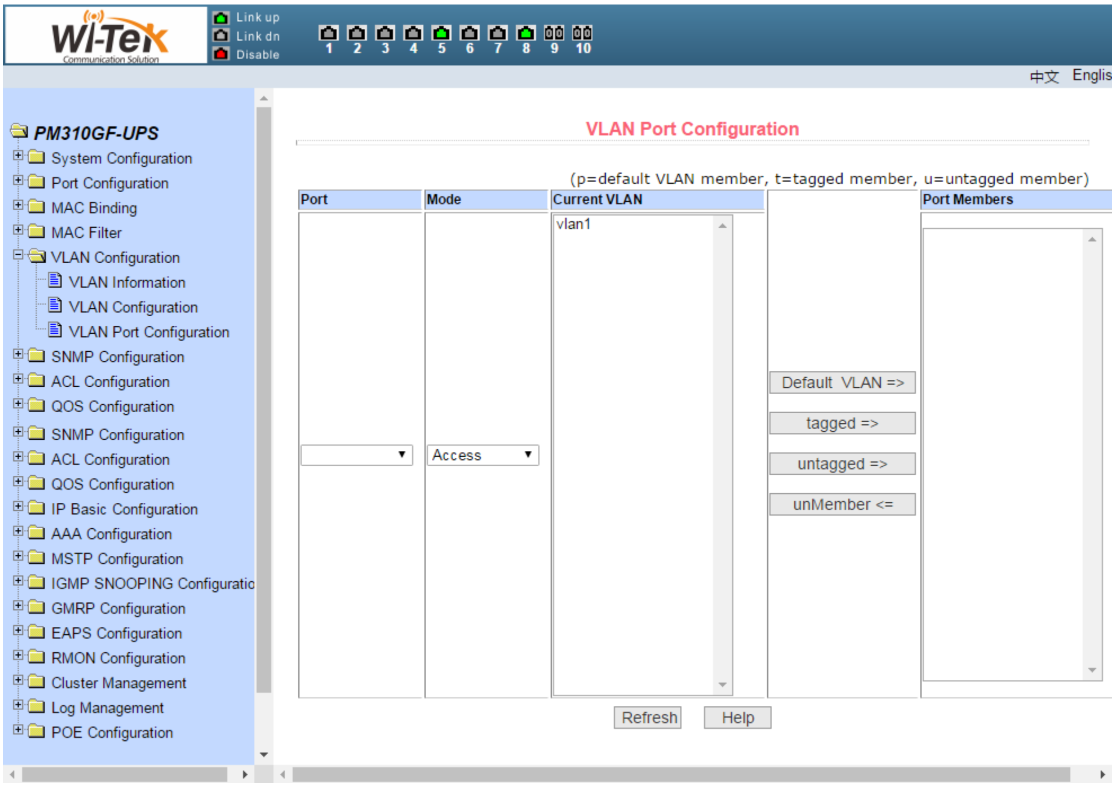
The port belongs to the VLAN to show the result of the VLAN port configuration. [P] indicates that the VLAN is the default VLAN of the port. [T] indicates that the port is a tagged member of the VLAN. [U] indicates that the port is a non-tagged member of the VLAN. When a VLAN is deleted, the user selects a VLAN from the list.

Press the default VLAN => Configure the default VLAN of the port and select a VLAN from all the current VLAN.

Press "tagged =>" to configure the port as a tagged member of the specified VLAN, and select one or more VLAN from all the current VLAN.

Press "untagged =>" to configure the port as an untagged member of the specified VLAN, and select one or more VLAN from all the current VLAN.

- The key "Non-member <=" removes the port from the specified one or more VLAN, is no longer a member of these VLAN, and selects one or more VLAN from the VLAN to which the port belongs.



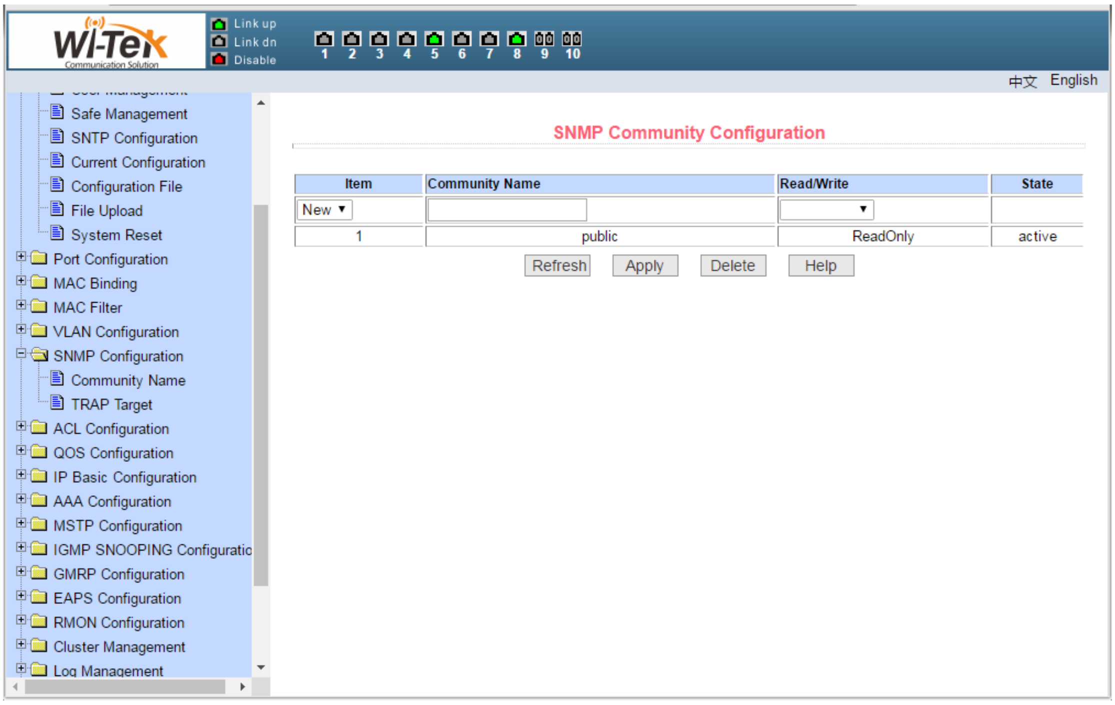
Pic 33 VLAN port configuration page

8、SNMP configuration

（1）SNMP community configuration page

Figure 34 shows the SNMP Community Configuration page, which allows the user to configure the name of the switch and the read and write permissions, and a total of eight entries can be configured.

By default, the switch has a public name of the common body, the common body is read-only permissions. Corresponding to this, there is only one active entry on the page, the common name is public, and the permissions are read-only. When the switch needs to be networked through SNMP, you need to configure a readable and writable community.



SNMP Community Configuration

Item	Community Name	Read/Write	State
New ▾		▾	
1	public	ReadOnly	active

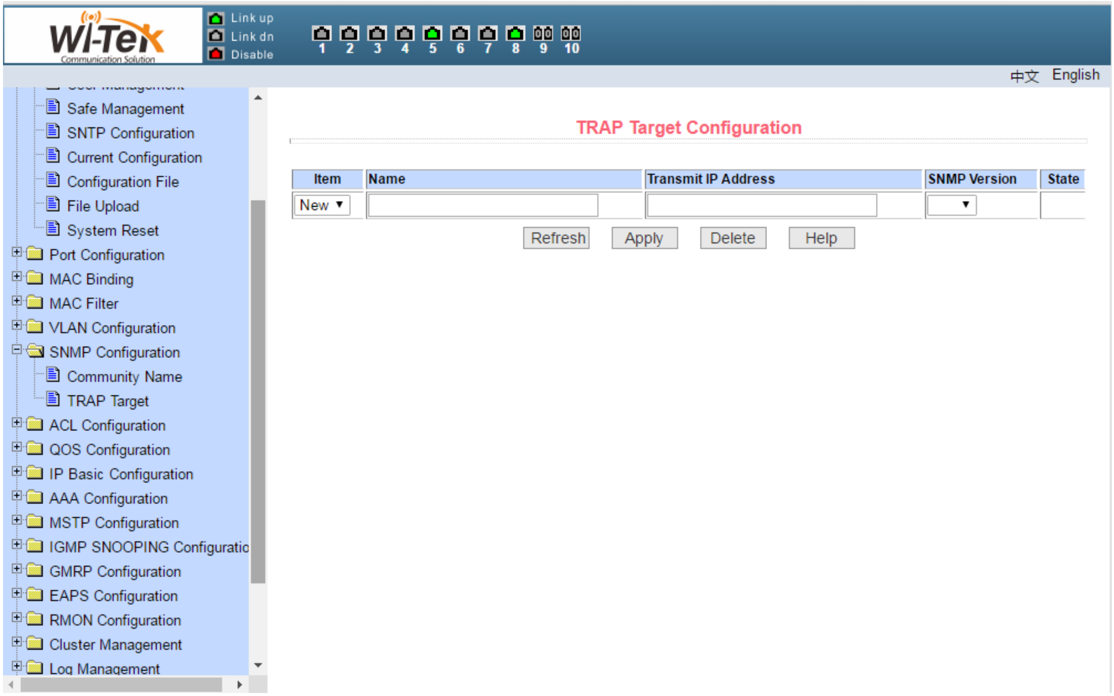
Pic 34 SNMP community configuration page

（2）TRAP target configuration page

Figure 35 shows the TRAP target configuration page, which allows the user to configure the IP address of the workstation that received 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 IP address is used to enter the destination address. The SNMP version is used to select the version of the TRAP packet. If the setting is successful, the status in the entry will be displayed as active. If the configuration succeeds, the SNMP TRAP function will take effect. In the event of link up or link down, the switch will automatically send the TRAP packet to the destination address.



TRAP Target Configuration

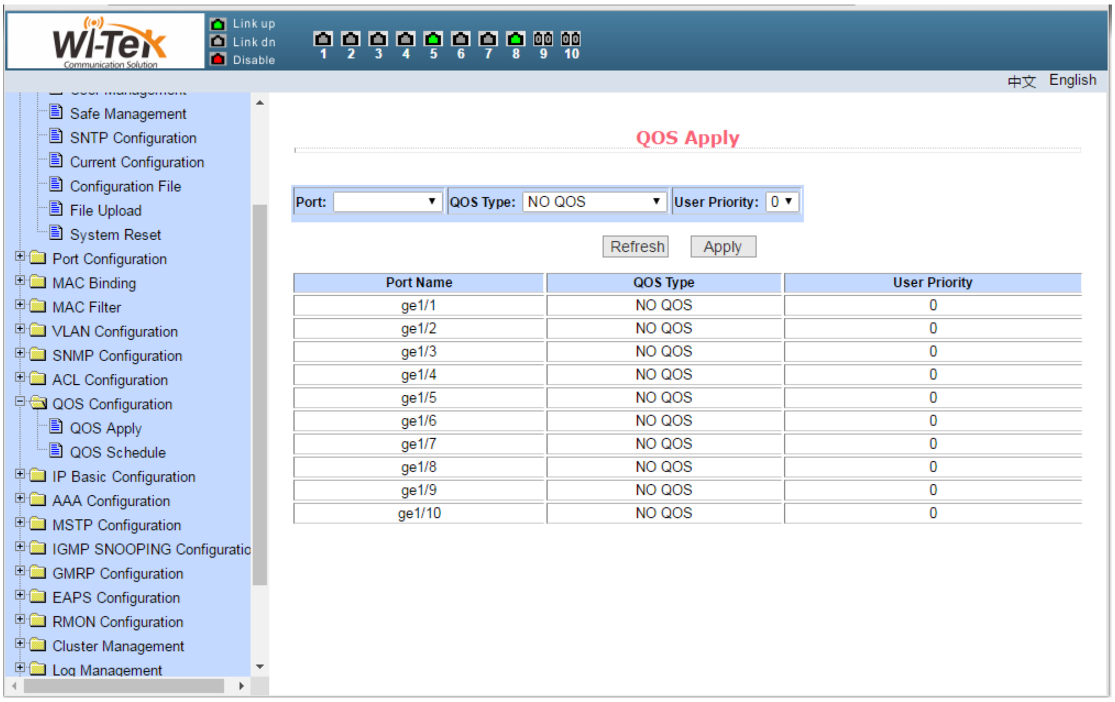
Item	Name	Transmit IP Address	SNMP Version	State
New ▾			▾	

Pic 35 TRAP target configuration page

9、Qos configuration

（1）Qos apply page

Figure 36 shows the Qos application page, the user can use this page to configure the port QOS type, but also can modify the default user priority. The list is the real-time display port Qos type and user default priority.



QOS Apply

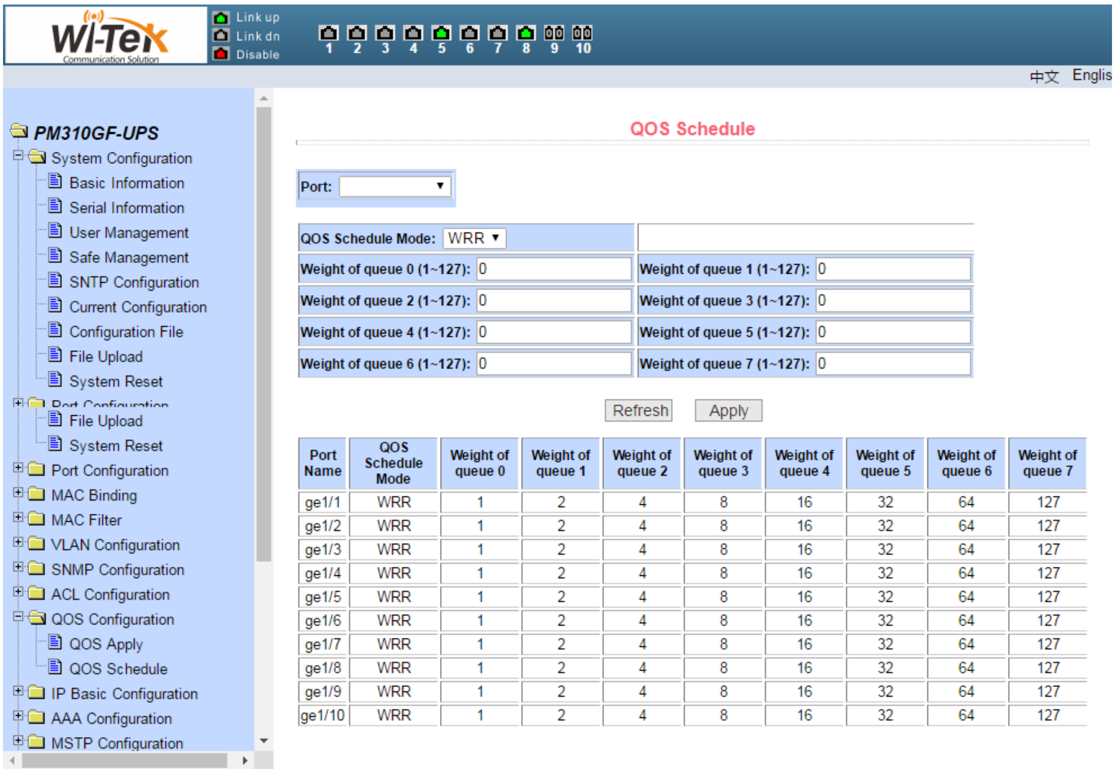
Port: QOS Type: NO QOS User Priority: 0

Port Name	QOS Type	User Priority
ge1/1	NO QOS	0
ge1/2	NO QOS	0
ge1/3	NO QOS	0
ge1/4	NO QOS	0
ge1/5	NO QOS	0
ge1/6	NO QOS	0
ge1/7	NO QOS	0
ge1/8	NO QOS	0
ge1/9	NO QOS	0
ge1/10	NO QOS	0

Pic 36 Qos apply page

（2）Qos schedule page

Figure 37 shows the Qos scheduling page, the user can use this page to configure the port QOS scheduling type, but also can modify the queue priority. The list is the real-time display port scheduling mode and the weight value of each queue.



QOS Schedule

Port:

QOS Schedule Mode: WRR

Weight of queue 0 (1~127): 0	Weight of queue 1 (1~127): 0
Weight of queue 2 (1~127): 0	Weight of queue 3 (1~127): 0
Weight of queue 4 (1~127): 0	Weight of queue 5 (1~127): 0
Weight of queue 6 (1~127): 0	Weight of queue 7 (1~127): 0

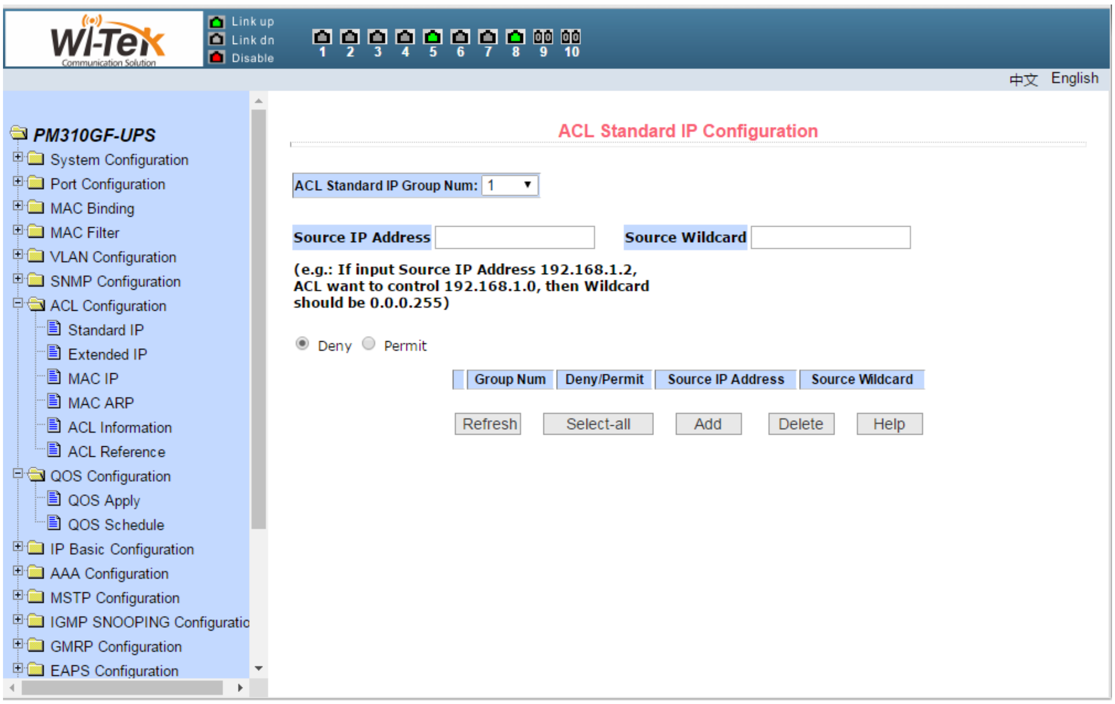
Port Name	QOS Schedule Mode	Weight of queue 0	Weight of queue 1	Weight of queue 2	Weight of queue 3	Weight of queue 4	Weight of queue 5	Weight of queue 6	Weight of queue 7
ge1/1	WRR	1	2	4	8	16	32	64	127
ge1/2	WRR	1	2	4	8	16	32	64	127
ge1/3	WRR	1	2	4	8	16	32	64	127
ge1/4	WRR	1	2	4	8	16	32	64	127
ge1/5	WRR	1	2	4	8	16	32	64	127
ge1/6	WRR	1	2	4	8	16	32	64	127
ge1/7	WRR	1	2	4	8	16	32	64	127
ge1/8	WRR	1	2	4	8	16	32	64	127
ge1/9	WRR	1	2	4	8	16	32	64	127
ge1/10	WRR	1	2	4	8	16	32	64	127

Pic 37 Qos schedule page

10、ACL configuration

（1）ACL standard IP configuration page

Figure 38 shows the ACL standard IP configuration page. You can use this page to create a rule base for ACL standard IP. The user can select an ACL group number (range between 1-99, or 1300-1999) to create one or more rules in the group. Fields that can be matched in a rule have only source IP addresses (with mask).



ACL Standard IP Configuration

ACL Standard IP Group Num: 1

Source IP Address ____ Source Wildcard ____

(e.g.: If input Source IP Address 192.168.1.2,
ACL want to control 192.168.1.0, then Wildcard
should be 0.0.0.255)

● Deny ○ Permit

Group Num	Deny/Permit	Source IP Address	Source Wildcard

Pic 38 ACL standard IP configuration page

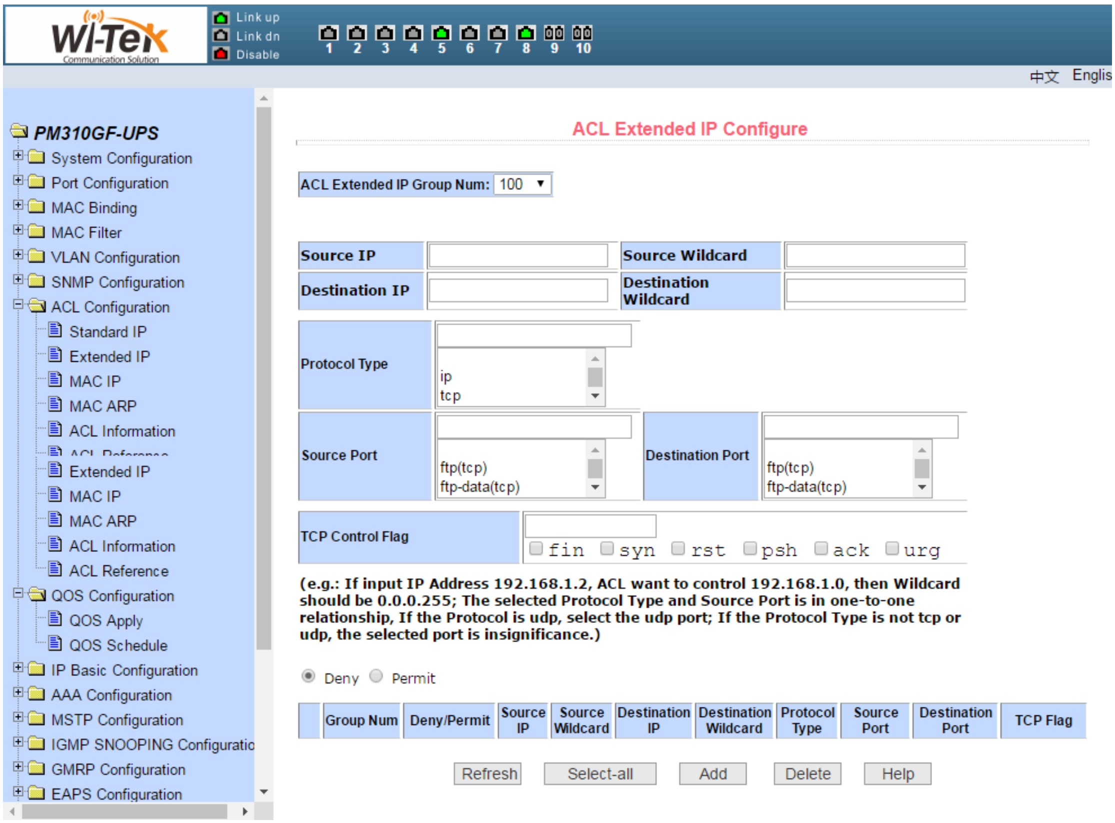
When a user configures a rule, the source IP address needs to be masked. The rule can match the set of IP addresses. The address mask is represented by an anti-code. If the rule matches the IP address range 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1 and its mask is 0.0.0.255.

When a user configures a rule, each rule must have a filtering mode: allow or deny.

When a user creates a rule in a rule group, the system automatically gives the rule a rule number. When a rule in a rule group is deleted, the other rules are not changed and the system automatically assigns a rule to a rule group Sort. If you want to delete the entire rule group, you can select all, and then click the Delete key.

（2）ACL extended IP configuration page

Figure 39 shows the ACL extension IP configuration page. You can use this page to create a rule base for ACL extension IP. The user can select an ACL group number (between 100-199, or 2000-2699) to create one or more rules in the group. (Such as ICMP, TCP, UDP, etc.), the source port, and the destination port (TCP and UDP only). The source IP address (masked), destination IP address (masked), protocol type (such as ICMP, TCP, UDP, etc.) Protocol valid), TCP control flag.



ACL Extended IP Configure

ACL Extended IP Group Num: 100

Source IP		Source Wildcard	
Destination IP		Destination Wildcard	

Protocol Type: ip, tcp

Source Port: ftp(tcp), ftp-data(tcp)

Destination Port: ftp(tcp), ftp-data(tcp)

TCP Control Flag: □ fin □ syn □ rst □ psh □ ack □ urg

(e.g.: If input IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255; The selected Protocol Type and Source Port is in one-to-one relationship, If the Protocol is udp, select the udp port; If the Protocol Type is not tcp or udp, the selected port is insignificance.)

● Deny ○ Permit

	Group Num	Deny/Permit	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol Type	Source Port	Destination Port	TCP Flag

Pic 39 ACL extended IP configuration page

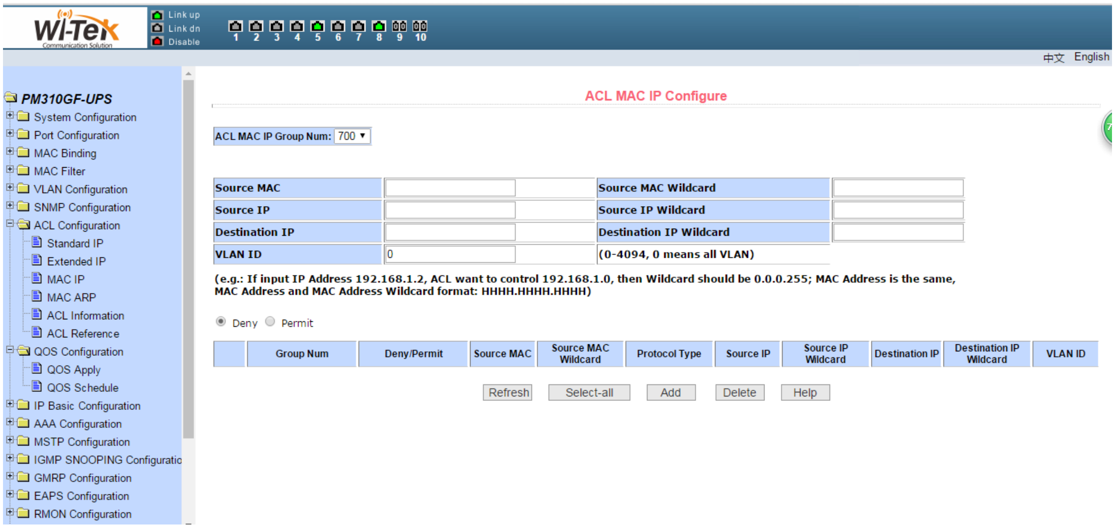
When a user configures a rule, the source IP address and destination IP address must be masked. The rule can match the set of IP addresses. The address mask is represented by an anti-code. If the rule matches the IP address range 192.168.0.0 to 192.168.0. 255, the IP address can be 192.168.0.1 and the mask is 0.0.0.255.

When a user configures a rule, each rule must have a filtering mode: allow or deny.

When a user creates a rule in a rule group, the system automatically gives the rule a rule number. When a rule in a rule group is deleted, the other rules are not changed and the system automatically assigns a rule to a rule group Sort. If you want to delete the entire rule group, you can select all, and then press the Delete key.

（3）ACL MAC IP configuration page

Figure 40 shows the ACL MAC IP configuration page. You can use this page to create a rule base for ACL MAC addresses. The user can select an ACL group number (in the range of 700-799) to create one or more rules in the group. Fields that can match the active MAC address (with address match bits), source IP address (with address match bit), destination IP address (with address match bit), and VLAN ID.



ACL MAC IP Configure

ACL MAC IP Group Num: 700

Source MAC		Source MAC Wildcard	
Source IP		Source IP Wildcard	
Destination IP		Destination IP Wildcard	
VLAN ID	0	(0-4094, 0 means all VLAN)	

(e.g.: If input IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255; MAC Address is the same, MAC Address and MAC Address Wildcard format: HHHH.HHHH.HHHH)

● Deny ○ Permit

	Group Num	Deny/Permit	Source MAC	Source MAC Wildcard	Protocol Type	Source IP	Source IP Wildcard	Destination IP	Destination IP Wildcard	VLAN ID

Pic 40 ACL MAC IP configuration page

When a user configures a rule, the source MAC address, source IP address, and destination IP address need to match the address. The rule can match the MAC address and the IP address. For example, if the rule matches 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.

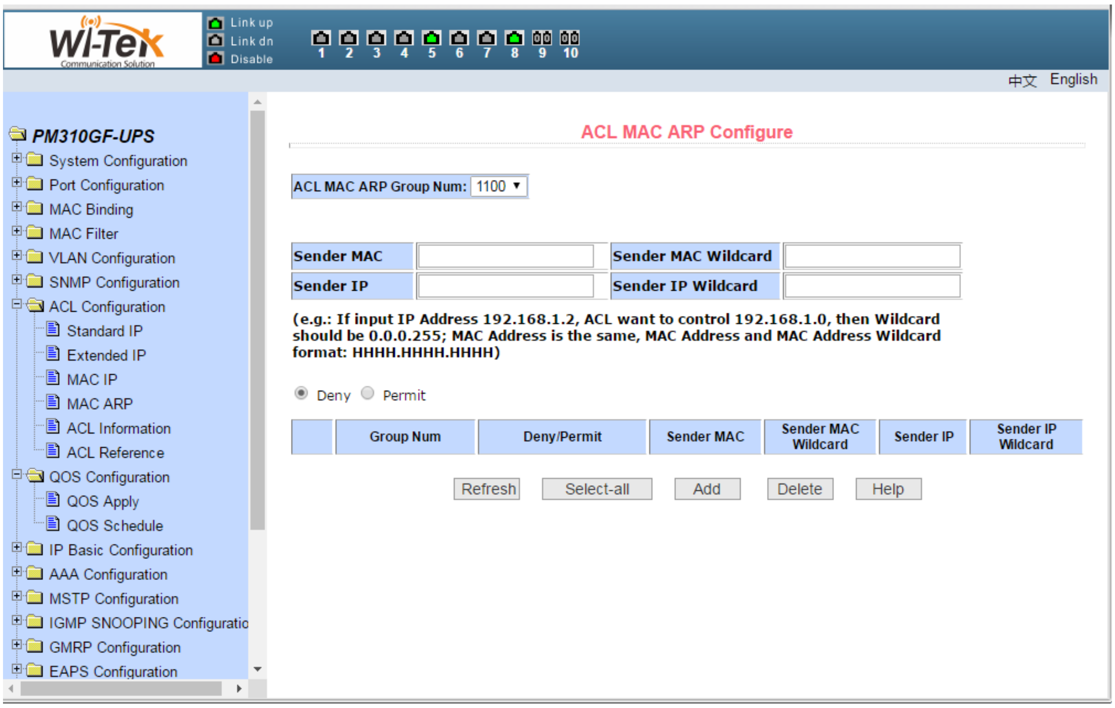
When a user configures a rule, each rule must have a filtering mode: allow or deny.

When a user creates a rule in a rule group, the system automatically gives the rule a rule number. When a rule in a rule group is deleted, the other rules are not changed and the system automatically assigns a rule to a rule group Sort. If you want to delete the entire rule group, you can select all, and then press the Delete key.

When a user configures a rule, the VLAN ID must be in the range 0 to 4094, including 0 and 4094, where 0 represents all.

（4）ACL MAC ARP configuration page

Figure 41 shows the ACL MAC ARP configuration page. You can use this page to create a rule base for ACL MAC ARP. The user can select an ACL group number (in the range of 1100-1199) to create one or more rules in the group. Fields that can be matched in a rule have ARP operation type, send MAC address (with address match bit), send IP address (with address match bit).



ACL MAC ARP Configure

ACL MAC ARP Group Num: 1100

Sender MAC		Sender MAC Wildcard	
Sender IP		Sender IP Wildcard	

(e.g.: If input IP Address 192.168.1.2, ACL want to control 192.168.1.0, then Wildcard should be 0.0.0.255; MAC Address is the same, MAC Address and MAC Address Wildcard format: HHHH.HHHH.HHHH)

● Deny ○ Permit

	Group Num	Deny/Permit	Sender MAC	Sender MAC Wildcard	Sender IP	Sender IP Wildcard

Pic 41 ACL MAC ARP configuration page

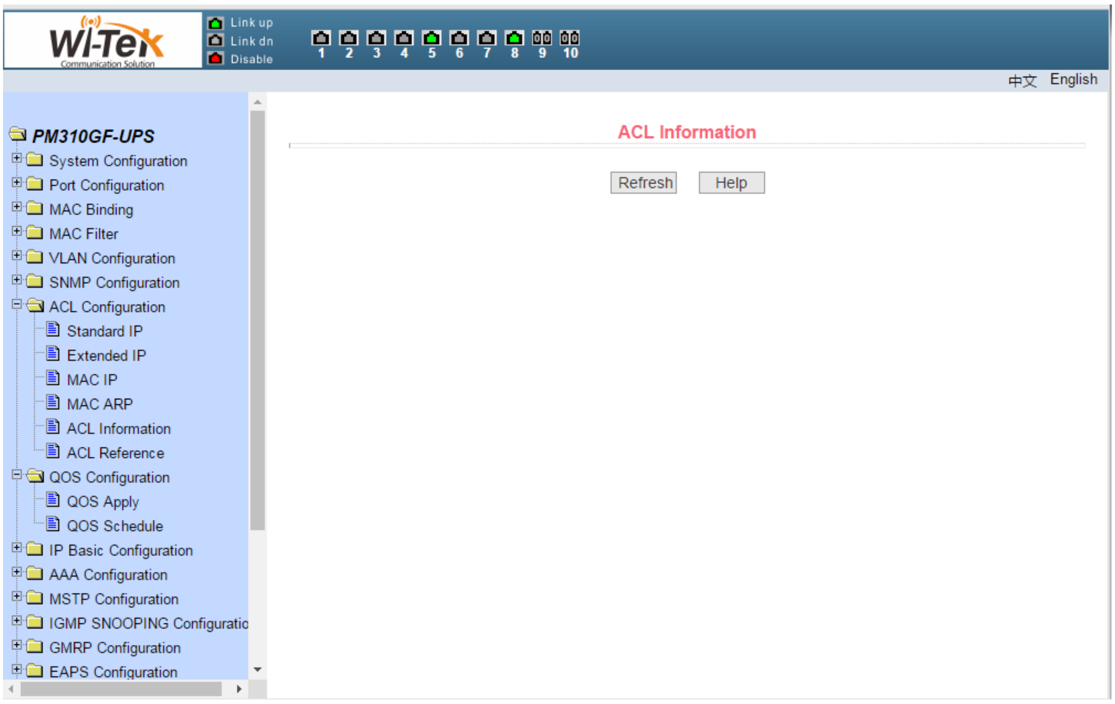
When a user configures a rule, the MAC address and the IP address are sent with an address matching bit. The rule can match the set of MAC address and IP address. For example, if the rule matches the IP address range 192.168.0.0 to 192.168.0. 255, the IP address can be 192.168.0.1 and its mask is 0.0.0.255.

When a user configures a rule, each rule must have a filtering mode: allow or deny.

When a user creates a rule in a rule group, the system automatically gives the rule a rule number. When a rule in a rule group is deleted, the other rules are not changed and the system automatically assigns a rule to a rule group Sort. If you want to delete the entire rule group, you can select all, and then press the Delete key.

（5）ACL resource information page

Figure 42 shows the ACL resource information page, which displays all the rules and references configured in the current ACL.

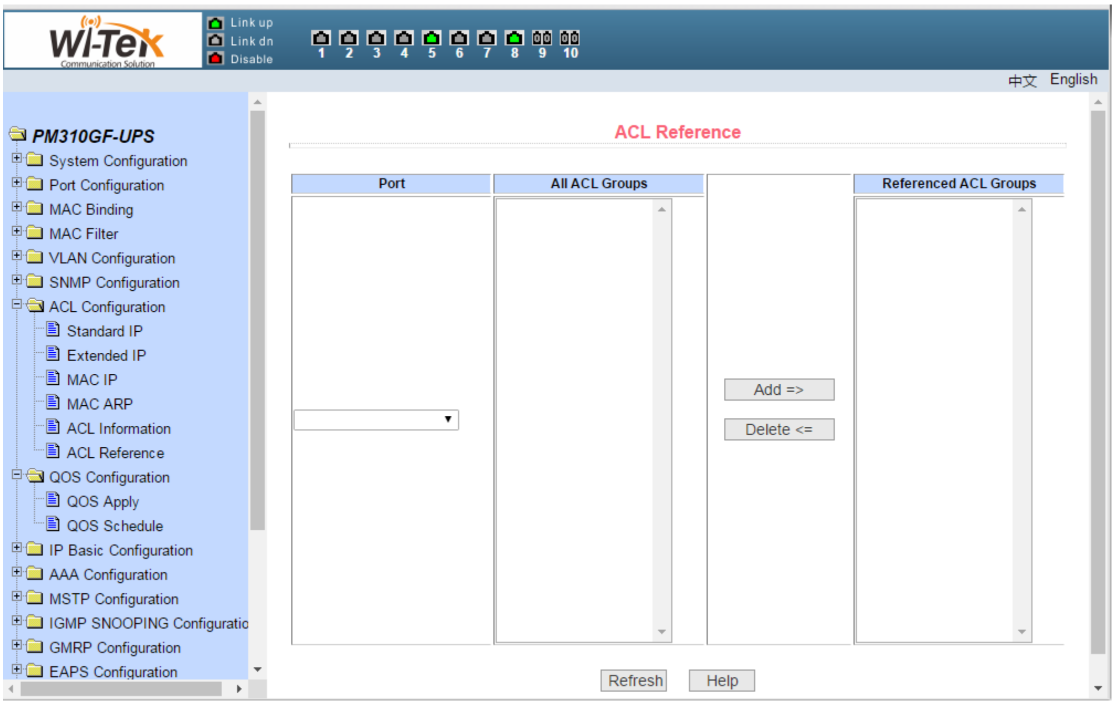


Pic 42 ACL resource information page

（6）ACL reference configuration page

Figure 43 shows the ACL reference configuration page. You can use this page to select an ACL group for a port and write the rules in this ACL group to the port hardware logic to enable the port to perform ACL filtering on the received packets according to these rules.

When selecting an ACL group on a port, you can select the IP standard, IP extension, MAC IP, and MAC ARP ACL. The selected ACL group must exist. Select the ACL rule group list and press the Add key. When deleting an ACL group, select an ACL group from the list of referenced rule groups and press the Delete key.

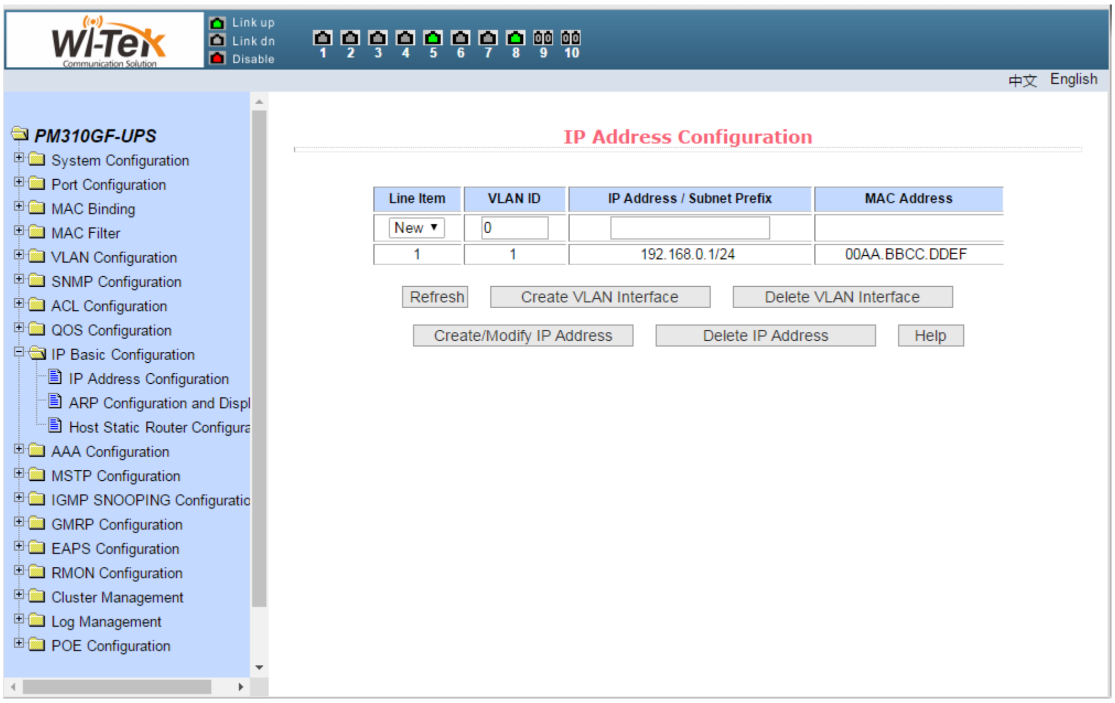


Pic 43 ACL reference configuration page

11、IP basic configuration

（1）VLAN interface configuration page

Figure 44 shows the VLAN interface configuration page. You can configure the VLAN interface, remove the VLAN interface, configure the IP address of the interface, delete the IP address of the interface, and view the interface information. Only when the VLAN already exists can it be set as an interface. Only the interface address can be configured on the configured interface.



IP Address Configuration

Line Item	VLAN ID	IP Address / Subnet Prefix	MAC Address
New ▾	0		
1	1	192.168.0.1/24	00AA.BBCC.DDEF

Pic 44 VLAN interface configuration page

The switch has a VLAN1 interface by default, and the interface can not be deleted. Only one interface can be configured for one VLAN.

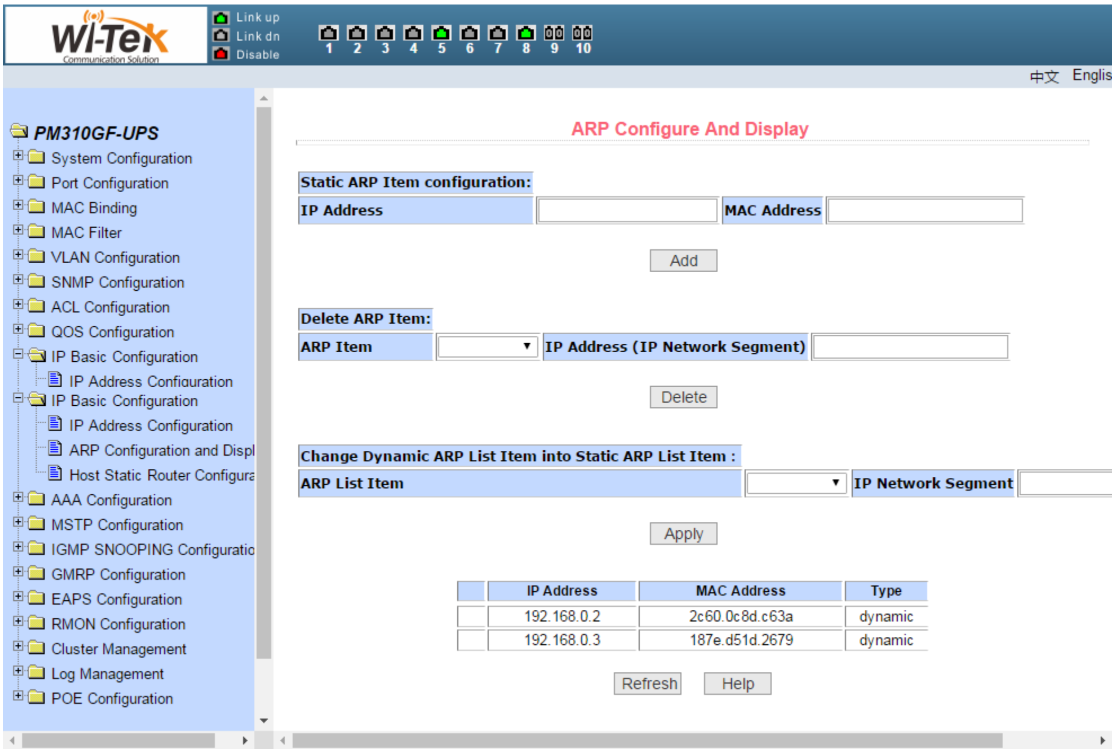
（2）ARP configuration and display page

Figure 45 shows the ARP configuration and display page. This page displays all the information of the ARP table of the switch. You can use this page to configure static ARP entries, delete ARP entries, and modify dynamic ARP entries to static ARP entries.

When you configure a static ARP entry, you need to enter the IP address and MAC address. The MAC address must be a unicast MAC address, and then click the Add key.

When a user deletes an ARP entry, you can choose to delete an ARP entry from one IP address, delete an ARP entry from one network segment, delete all ARP entries, delete all dynamic ARP entries, and delete all static ARP entries. The To delete an IP ARP entry or delete an ARP entry from a network segment, enter the specified IP address or IP segment in the input box. And then click the Delete key.

When a dynamic ARP entry is modified to a static ARP entry, you can choose to change the dynamic ARP entry in a network segment to a static ARP entry. For a network segment, enter the specified network segment in the input box. And then click the Apply button.



ARP Configure And Display

Static ARP Item configuration:

IP Address ____ MAC Address ____

Delete ARP Item:

ARP Item ____ IP Address (IP Network Segment) ____

Change Dynamic ARP List Item into Static ARP List Item :

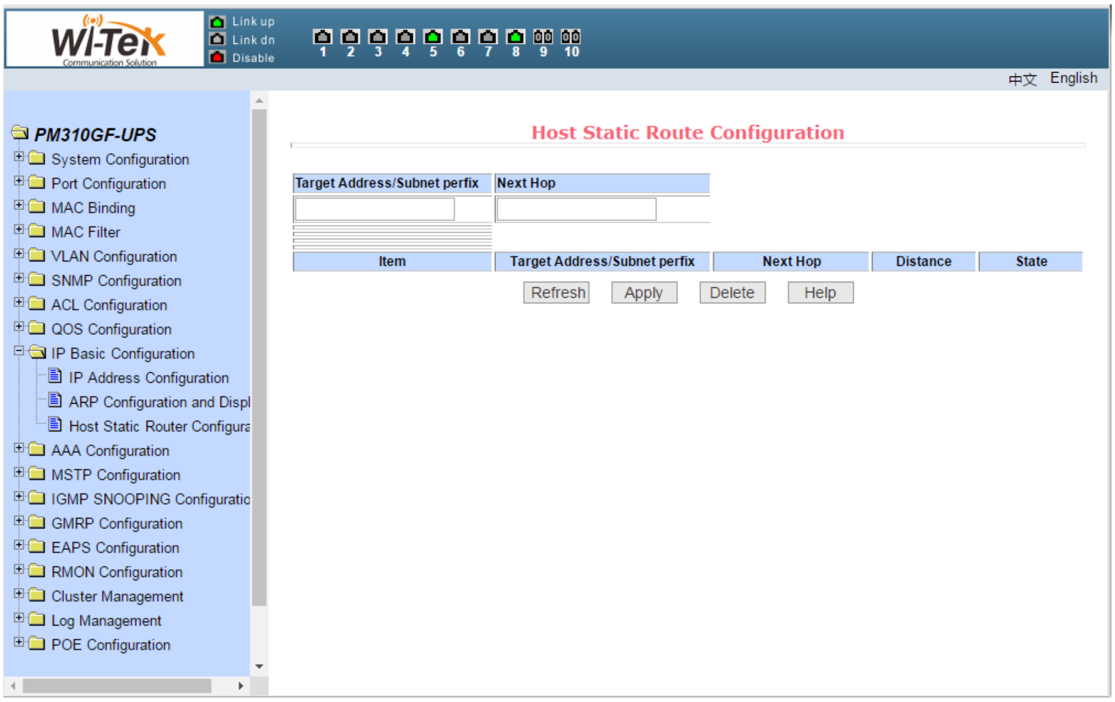
ARP List Item ____ IP Network Segment ____

	IP Address	MAC Address	Type
	192.168.0.2	2c60.0c8d.c63a	dynamic
	192.168.0.3	187e.d51d.2679	dynamic

Pic 45 ARP configuration and display page

（3）Host static route configuration page

Figure 46 shows the host static routing configuration page, the user can add and delete the host static route of the switch. By default, no static route is configured on the switch. You can use this page to configure a default route, that is, the destination / subnet prefix is 0.0.0.0/0.



Host Static Route Configuration

Target Address/Subnet perfix	Next Hop

Item	Target Address/Subnet perfix	Next Hop	Distance	State

Pic 46 host static route configuration page

12、AAA configuration

（1）Tacacs+configuration page

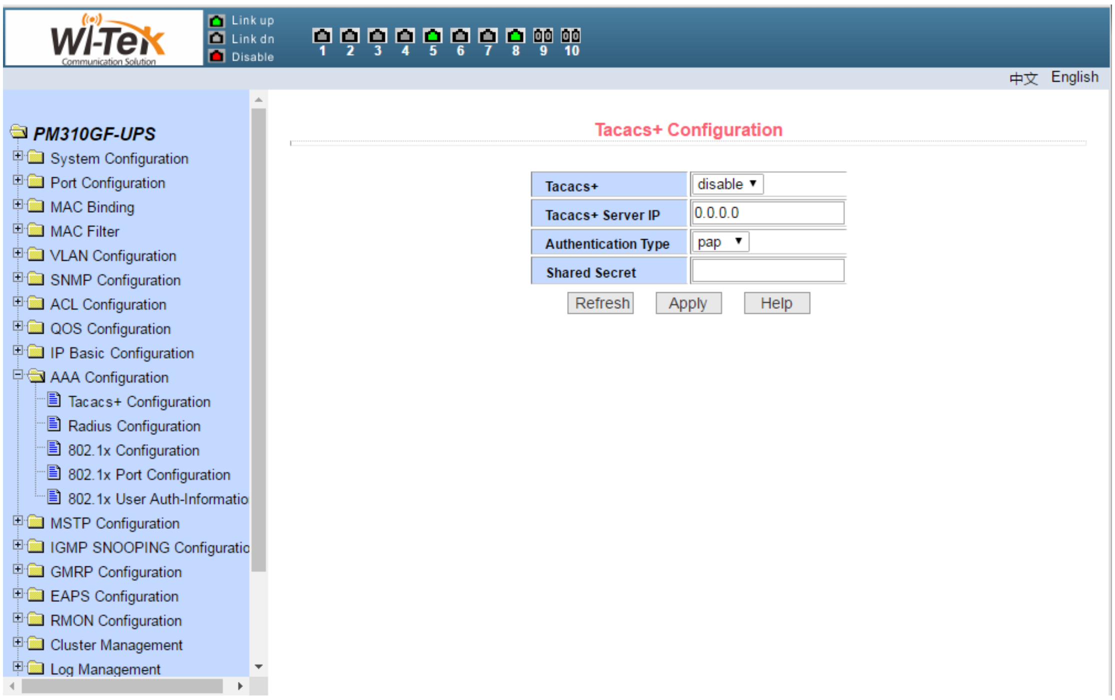
Figure 47 shows the Tacacs + configuration page. The user can configure information related to Tacacs +. The following information can be set: Enable Tacacs + function, configure the Tacacs + server IP address, authentication type, and shared secret key.

Before using the Tacacs + function, you must enable the Tacacs + function, which is configured by default.

Configure the IP address of the Tacacs + server, which must be set when using the Tacacs + feature.

Authentication type, providing PAP and CHAP authentication types. The default is PAP authentication.

Shared key, used to set the switch and Tacacs + server between the encrypted shared password, in the authentication authorization must set this field, and to the same as the Tacacs + server settings.



Tacacs+ Configuration

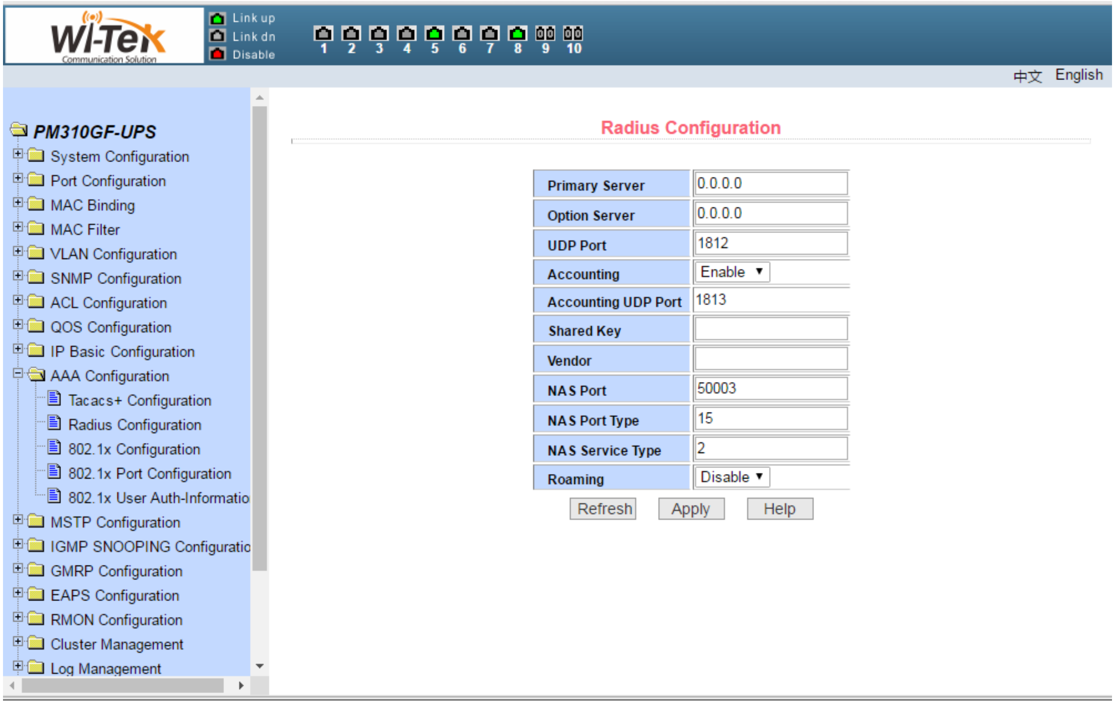
Tacacs+	disable
Tacacs+ Server IP	0.0.0.0
Authentication Type	pap
Shared Secret	

Pic 47 Tacacs+configuration page.

（2）Radius configuration page

Figure 48 shows the Radius configuration page, the user can configure information related to Radius, can set the information include:

- Radius server IP address, in the authentication and billing must be set when this field.
- Optional Radius server IP address, which can be set if there is an alternate Radius server.
- Authentication UDP port, the default value is 1812, the user generally do not need to modify this field.
- Whether to start billing, the default is to start, when doing the authentication and billing to start billing.
- Billing UDP port, the default value is 1813.
- Shared key, used to set the switch and the Radius server encryption between the shared password, in the authentication and billing must be set this field, and to the same settings on the Radius server.
- Vendor-specific information, users generally do not need to modify this field.
- NAS port, NAS port type, NAS service type, these three values users generally do not need to modify.
- Whether to start or turn off the roaming function of Radius.



Radius Configuration

Primary Server	0.0.0.0
Option Server	0.0.0.0
UDP Port	1812
Accounting	Enable
Accounting UDP Port	1813
Shared Key	
Vendor	
NAS Port	50003
NAS Port Type	15
NAS Service Type	2
Roaming	Disable

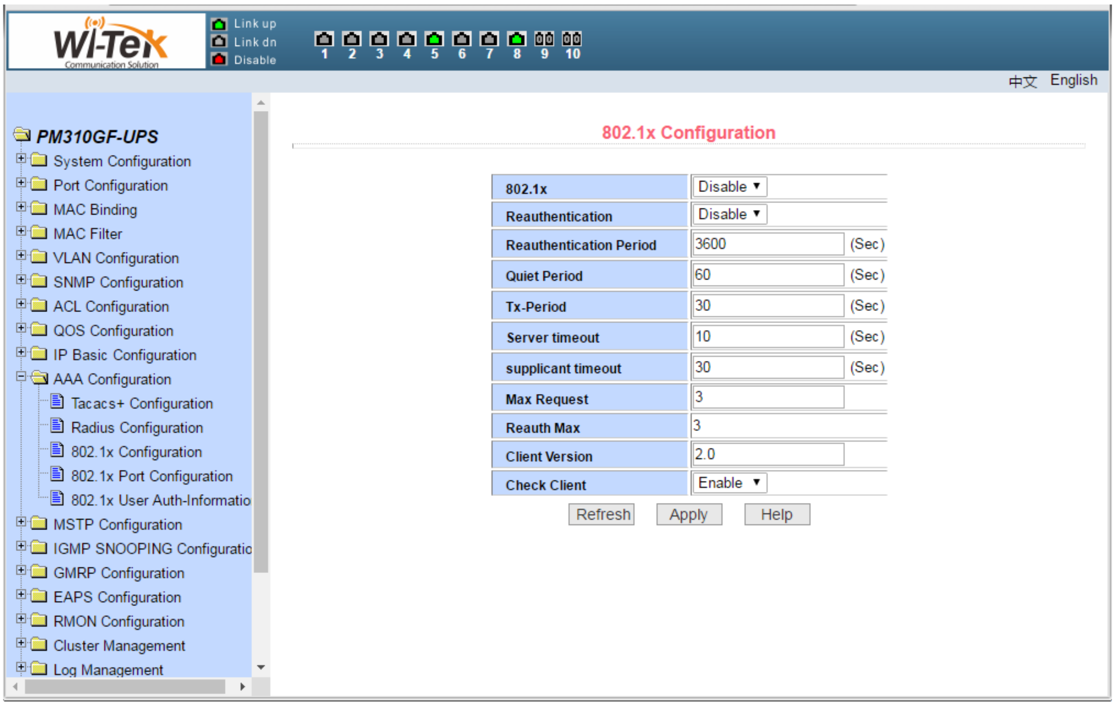
Pic 48 Radius configuration page

（3）802.1x configuration page

Figure 49 shows the 802.1x configuration page. You can configure 802.1x-related information through this page, including:

- Whether to start the 802.1x protocol, be sure to start the 802.1x protocol when doing authentication and accounting.
- Whether the switch is a common authentication method or an extended authentication method.
- Whether to open the re-authentication function, the default is not open, when doing the authentication and billing according to the actual situation to decide. Turning on the reauthentication function will make the user more reliable when using authentication and billing, but will slightly increase the traffic to the network.
- Set the re-authentication interval, only in the case of re-authentication function is enabled, the default is 3600 seconds, when doing authentication and billing according to the actual situation to set the value, but the value should not be too small.
- Quiet Period timer, the user generally does not need to modify this field.
- Tx-Period timer, the user generally does not need to modify this field.
- Server timeout timer, users generally do not need to modify this field.
- supplicant timeout timer, the user generally do not need to modify this field.
- The number of requests, users generally do not need to modify this field.
- Show Reauth Max size.
- Client version, client version number.

- Check Client, whether to check the client's timing traffic package after authentication has passed.



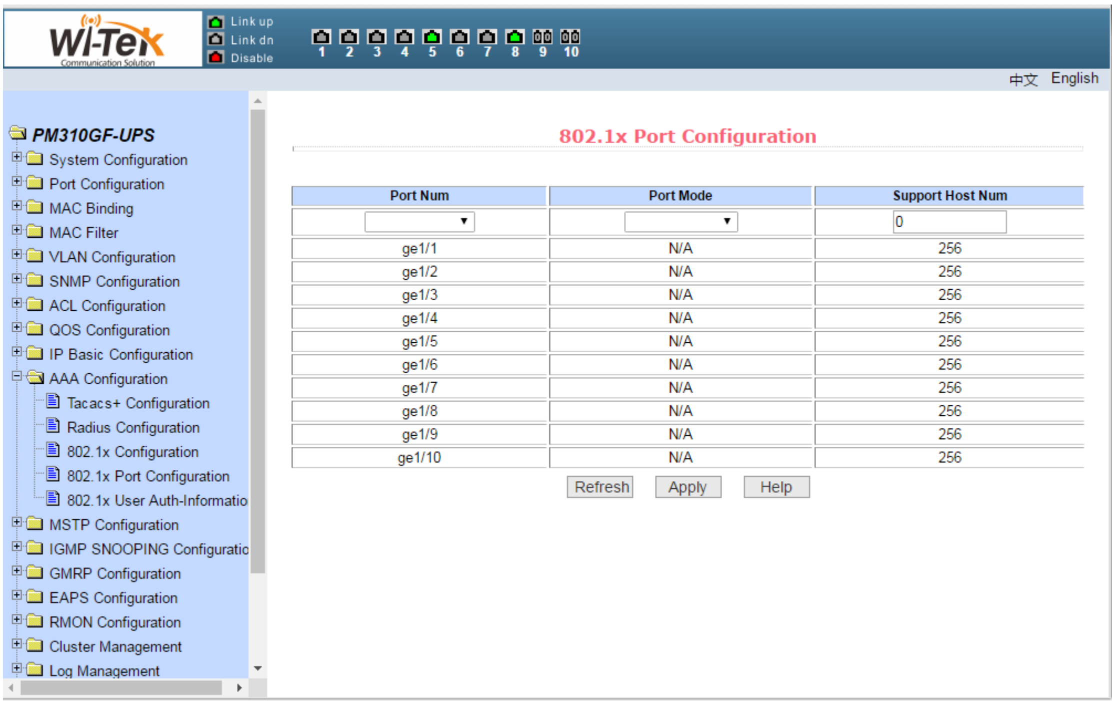
802.1x Configuration

802.1x	Disable ▾	
Reauthentication	Disable ▾	
Reauthentication Period	3600	(Sec)
Quiet Period	60	(Sec)
Tx-Period	30	(Sec)
Server timeout	10	(Sec)
supplicant timeout	30	(Sec)
Max Request	3	
Reauth Max	3	
Client Version	2.0	
Check Client	Enable ▾	

Pic 49 802.1x configuration page

（4）802.1x port configuration page

Figure 50 shows the 802.1x port configuration page. You can configure 802.1x port mode and the maximum number of hosts that can be configured. You can also view the 802.1x configuration of each port.The 802.1x port mode includes four types: N / A status, Auto state, Force-authorized status, and Force-unauthorized status.当When A port needs to be done to 802.1 x authentication, to the state of the port is set to Auto, if don't do certification can access the network, the state of the port is set to N/A, the other two state are seldom used in practical application.



802.1x Port Configuration

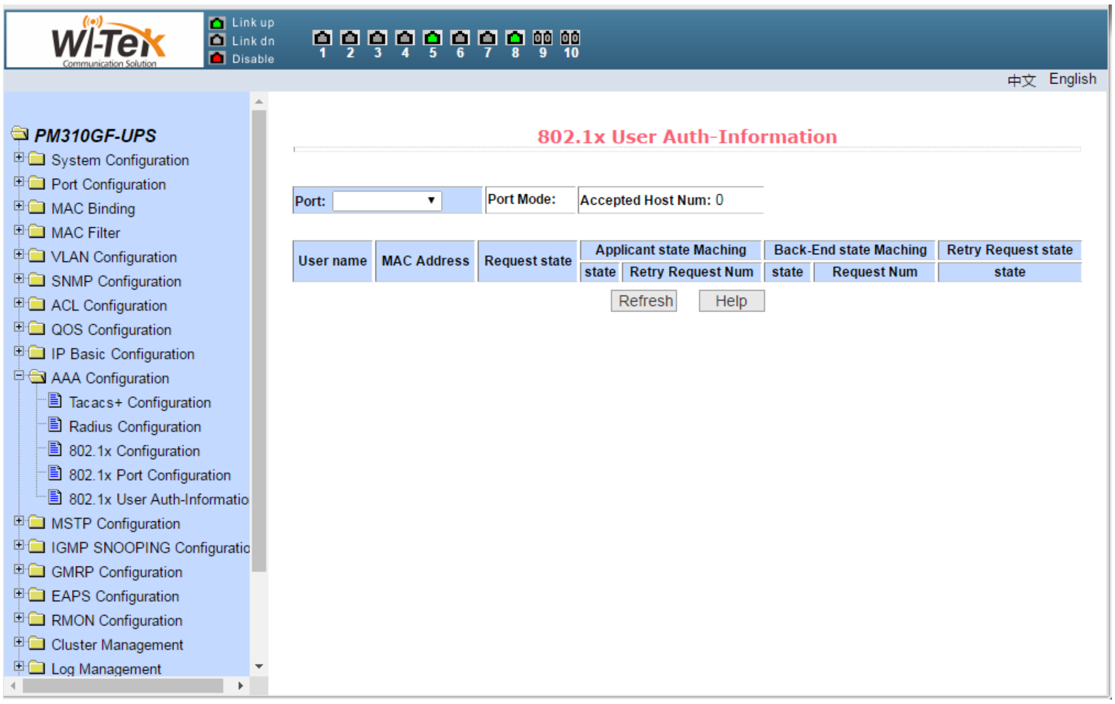
Port Num	Port Mode	Support Host Num
		0
ge1/1	N/A	256
ge1/2	N/A	256
ge1/3	N/A	256
ge1/4	N/A	256
ge1/5	N/A	256
ge1/6	N/A	256
ge1/7	N/A	256
ge1/8	N/A	256
ge1/9	N/A	256
ge1/10	N/A	256

Pic 50 802.1x port configuration page.

When 802.1x authentication is enabled, the maximum number of hosts that can be accessed by the port is 256, and the user can modify this field to support up to 256.

（5）**802.1x** user auth-information page

Figure 51 shows the 802.1x user auth-information page. You can view the status information of all users accessing a port through this page.



802.1x User Auth-Information

Port: | Port Mode: | Accepted Host Num: 0

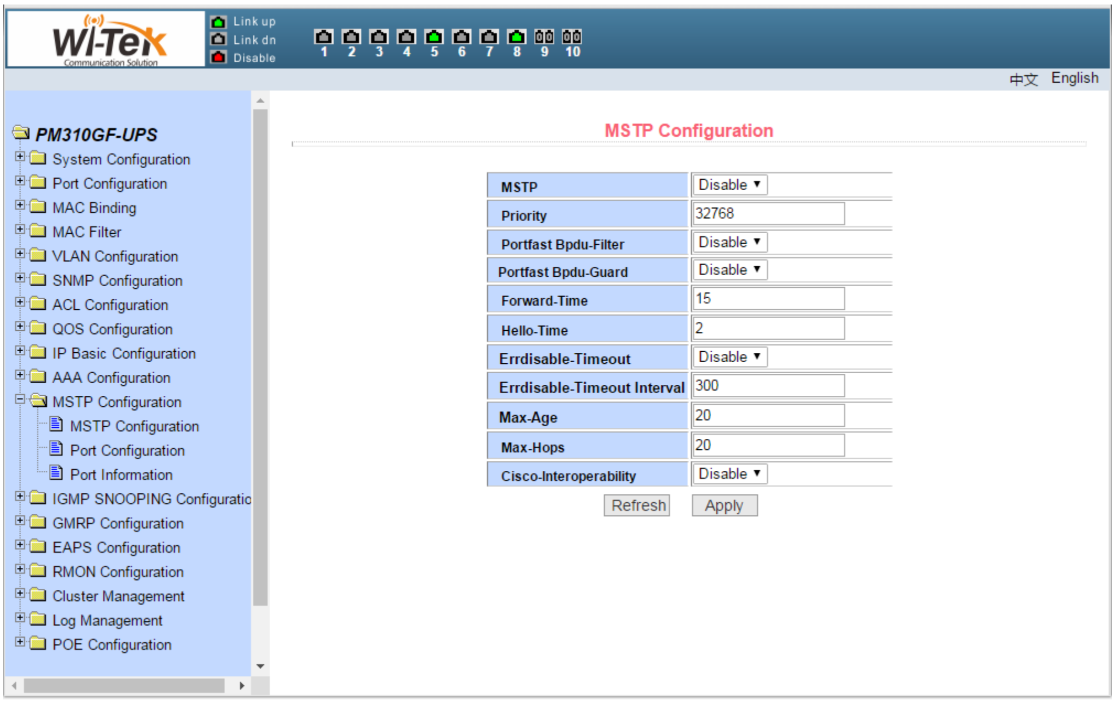
User name	MAC Address	Request state	Applicant state Maching		Back-End state Maching		Retry Request state
			state	Retry Request Num	state	Request Num	state

Pic 51 802.1x user auth-information page

13、MSTP configuration

（1）MSTP global configuration page

Figure 52 shows the MSTP global configuration page. You can configure global MSTP parameters through this page.



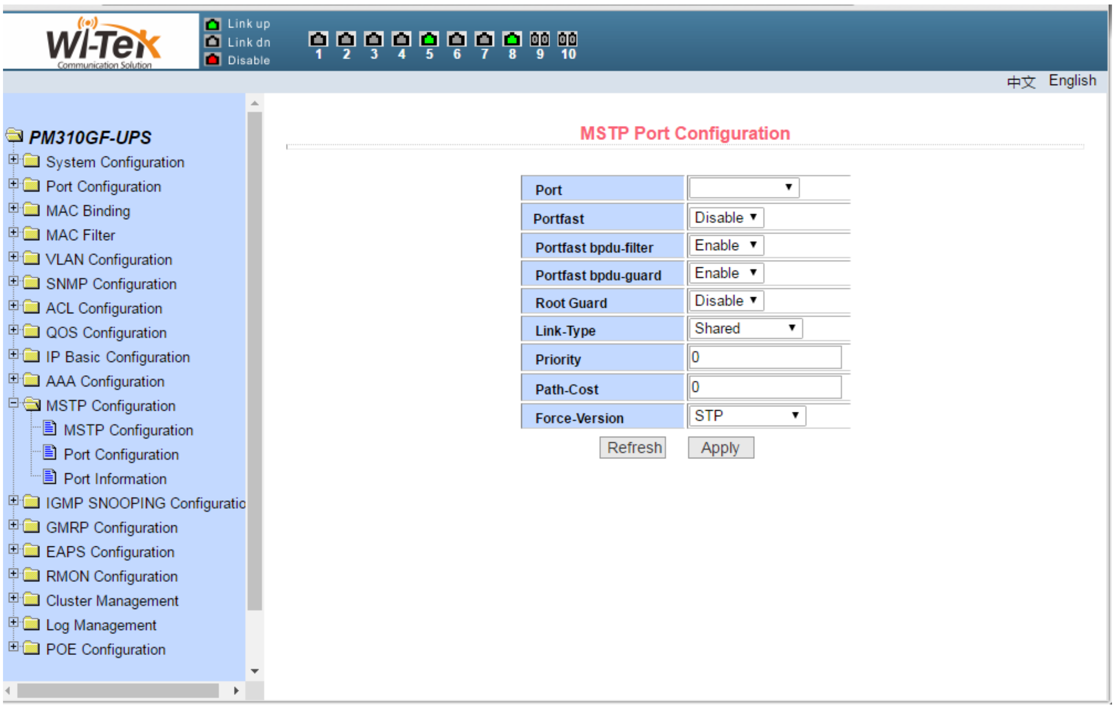
MSTP Configuration

MSTP	Disable
Priority	32768
Portfast Bpdu-Filter	Disable
Portfast Bpdu-Guard	Disable
Forward-Time	15
Hello-Time	2
Errdisable-Timeout	Disable
Errdisable-Timeout Interval	300
Max-Age	20
Max-Hops	20
Cisco-Interoperability	Disable

Pic 52 MSTP global configuration page

（2）MSTP port configuration page

Figure 53 shows the MSTP port configuration page. You can use this page to configure port MSTP parameters.



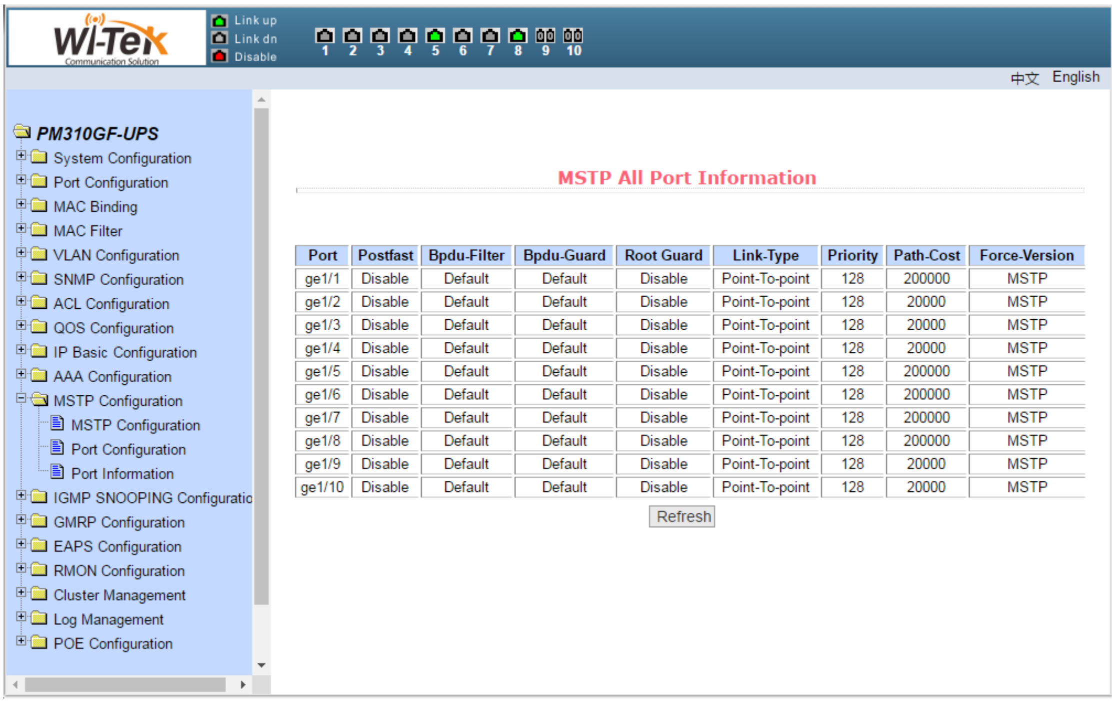
MSTP Port Configuration

Port	
Portfast	Disable
Portfast bpdu-filter	Enable
Portfast bpdu-guard	Enable
Root Guard	Disable
Link-Type	Shared
Priority	0
Path-Cost	0
Force-Version	STP

Pic 53 MSTP port configuration page

（3）MSTP port information page

Figure 54 shows the MSTP port information page. You can view the port MSTP status on this page.



MSTP All Port Information

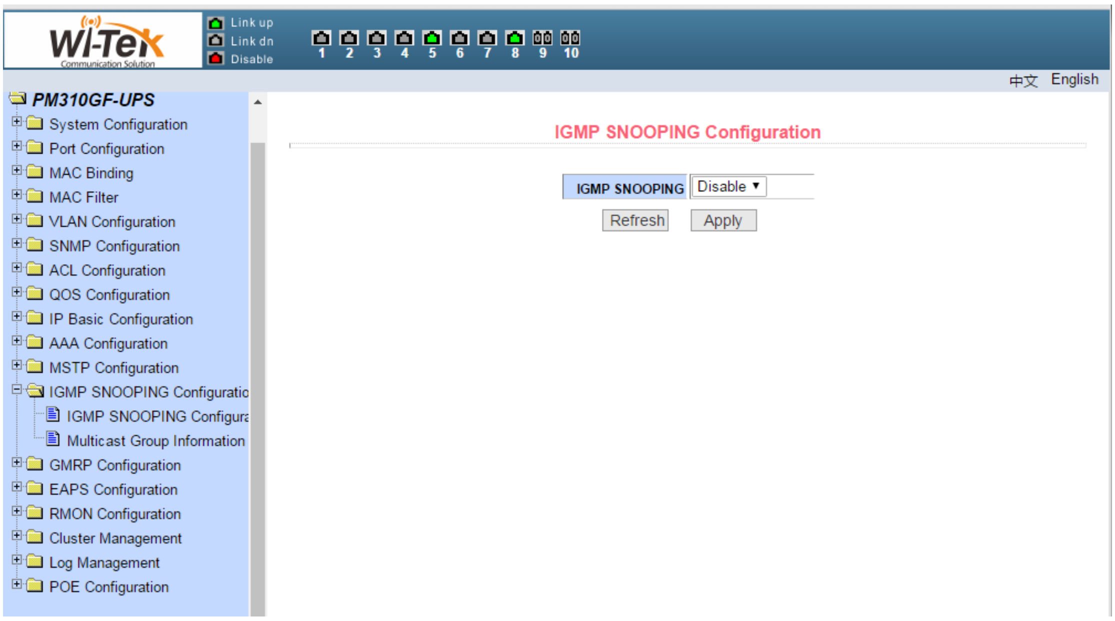
Port	Postfast	Bpdu-Filter	Bpdu-Guard	Root Guard	Link-Type	Priority	Path-Cost	Force-Version
ge1/1	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/2	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/3	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/4	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/5	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/6	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/7	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/8	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/9	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/10	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

Pic 54 MSTP port information page

14、IGMPSNOOPING configuration

（1）IGMPsnooping global configuration page

Figure 55 shows the IGMPsnooping global configuration page. You can enable IGMP snooping on this page.



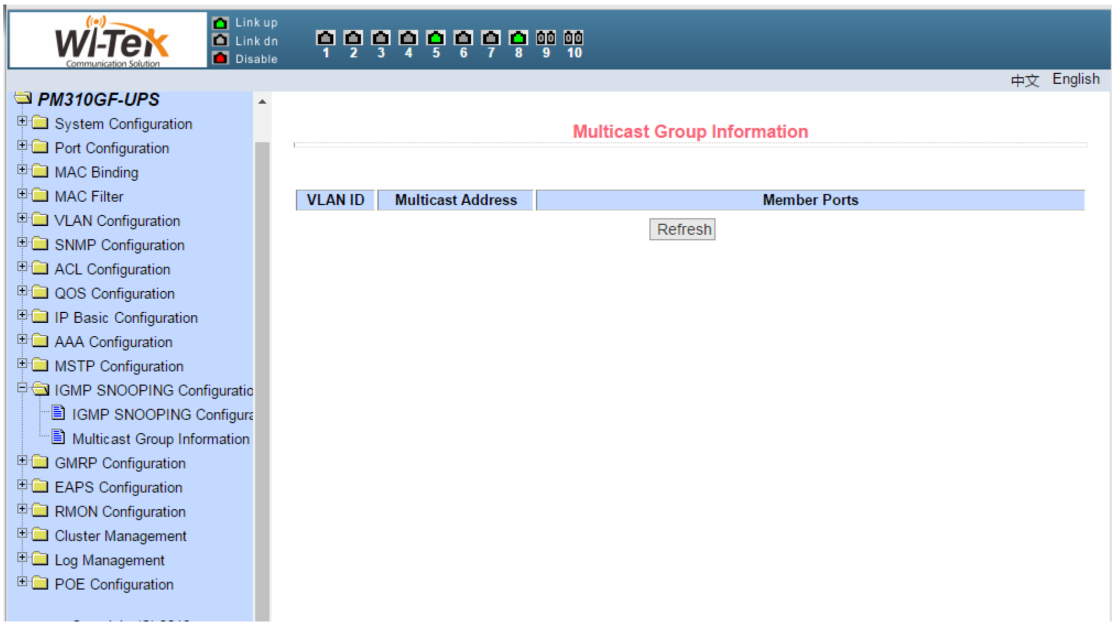
IGMP SNOOPING Configuration

IGMP SNOOPING	Disable

Pic 55 IGMPsnooping global configuration page

（2） Multicast group information page

Figure 56 shows the multicast group information page. You can view the igmp snooping multicast program information from this page.



Multicast Group Information

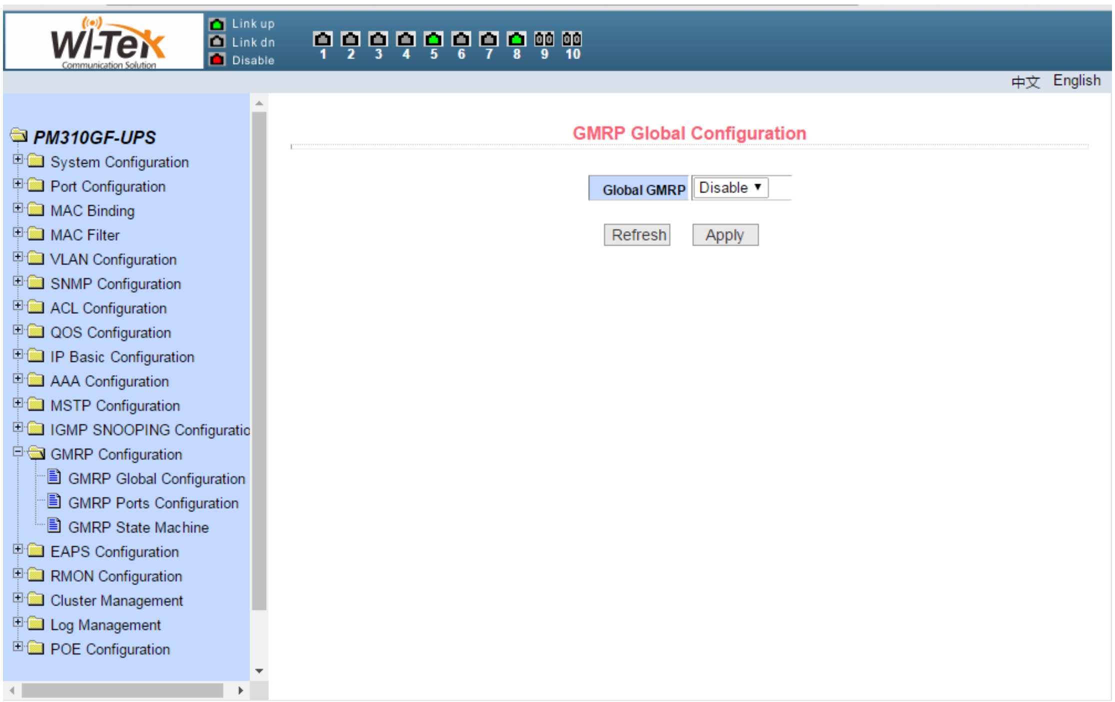
VLAN ID	Multicast Address	Member Ports

Pic 56 Multicast group information page

15、GMRP configuration

（1）GMRP global configuration page

Figure 57 shows the GMRP global configuration page. Users can enable GMRP through this page.



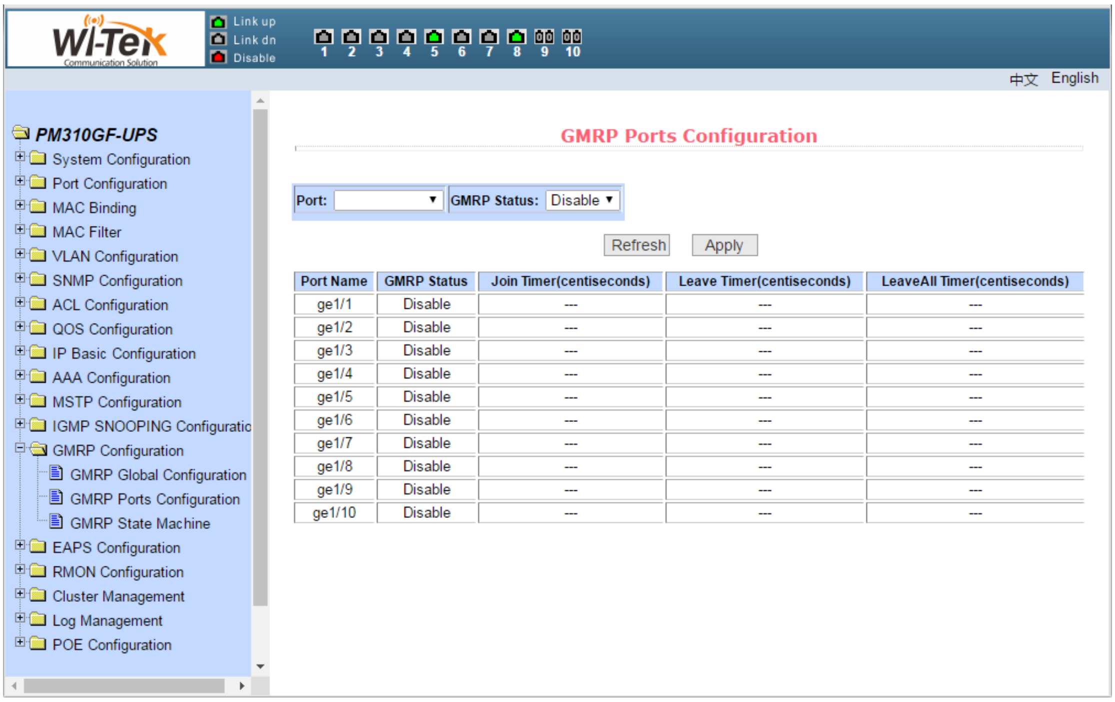
GMRP Global Configuration

Global GMRP: Disable

Pic 57 GMRP global configuration page

（2）GMRP port configuration page

Figure 58 shows the GMRP port configuration page.Users can use this page to enable port GMRP, and can view the port information.



GMRP Ports Configuration

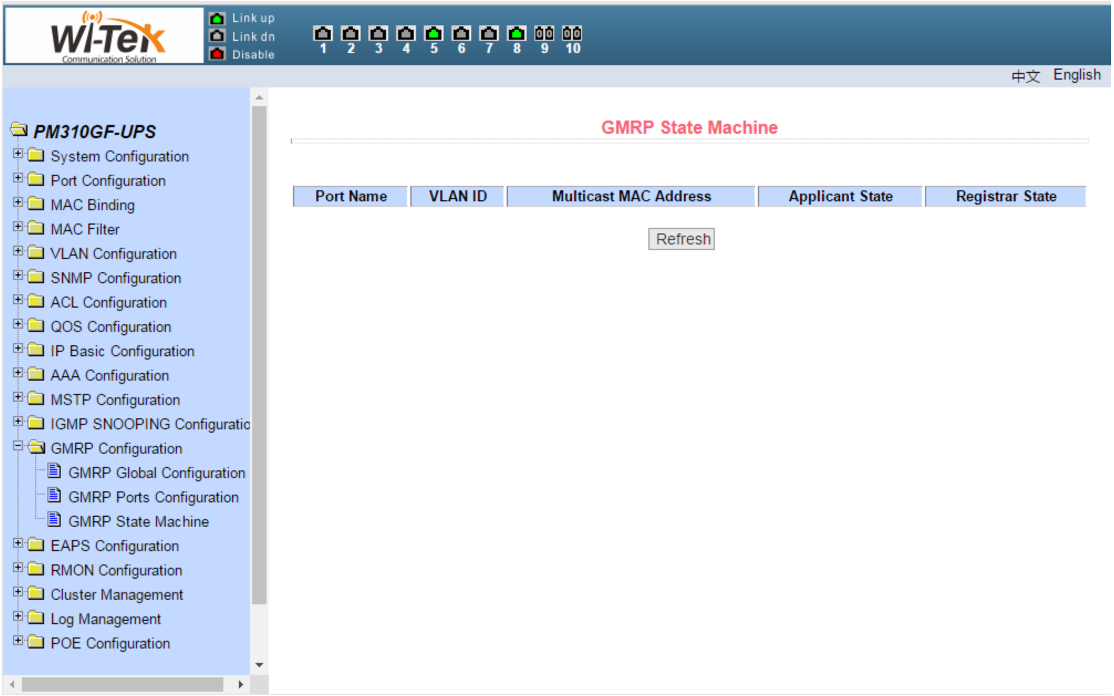
Port: [▾] GMRP Status: Disable ▾

Port Name	GMRP Status	Join Timer(centiseconds)	Leave Timer(centiseconds)	LeaveAll Timer(centiseconds)
ge1/1	Disable	---	---	---
ge1/2	Disable	---	---	---
ge1/3	Disable	---	---	---
ge1/4	Disable	---	---	---
ge1/5	Disable	---	---	---
ge1/6	Disable	---	---	---
ge1/7	Disable	---	---	---
ge1/8	Disable	---	---	---
ge1/9	Disable	---	---	---
ge1/10	Disable	---	---	---

Pic 58 GMRP port configuration page

（3）GMRP state machine page

Figure 59 is the GMRP state machine page.Users can view GMRP's state machine information from this page.



GMRP State Machine

Port Name	VLAN ID	Multicast MAC Address	Applicant State	Registrar State

Pic 59 GMRP state machine page

16、EAPS configuration

（1）EAPS configuration page

This page is used to create and configure EAPS information, and can also be used to delete and display EAPS information.

EAPS Ring ID　The specific ring ID, in the range of 1-16, can be selected according to the drop-down box

Create two types, Not Created and Created ,If you don't create it, you have to create the pattern Master and the Transit, The corresponding mode can be configured according to the specific needs

Main port　　EAPS Main port，such as：fe1/1、ge1/1

Alternate port　EAPS second port

Control vlan　EAPS ring control vlan, the value of 2-4094

Protected vlan　EAPS ring protection vlan

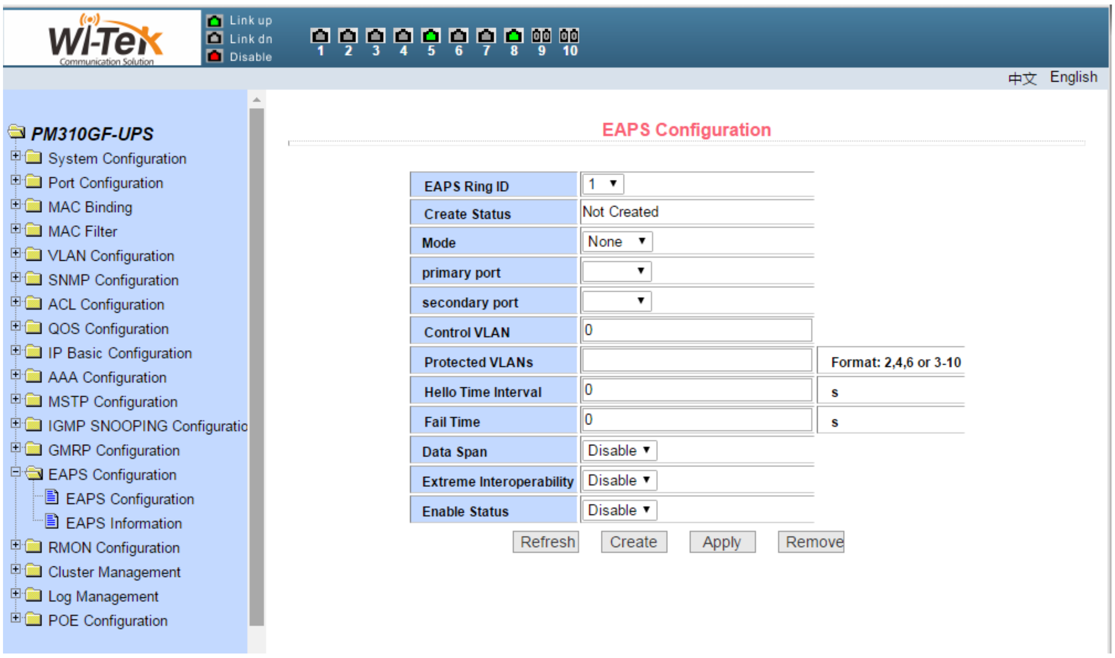
Hello time interval　 Hello message to send the time interval, the default is 1S

Fail time　Detection of the fault time, the default is 3S

Data is forwarded across the ring　　In the case of multiple rings, this function is required when data needs to be forwarded across the ring. The default is not turned on

EXtreme interoperability　　Compatibility with radical network devices, turned on by default

Enabled state　　The last EAPS ring is enabled



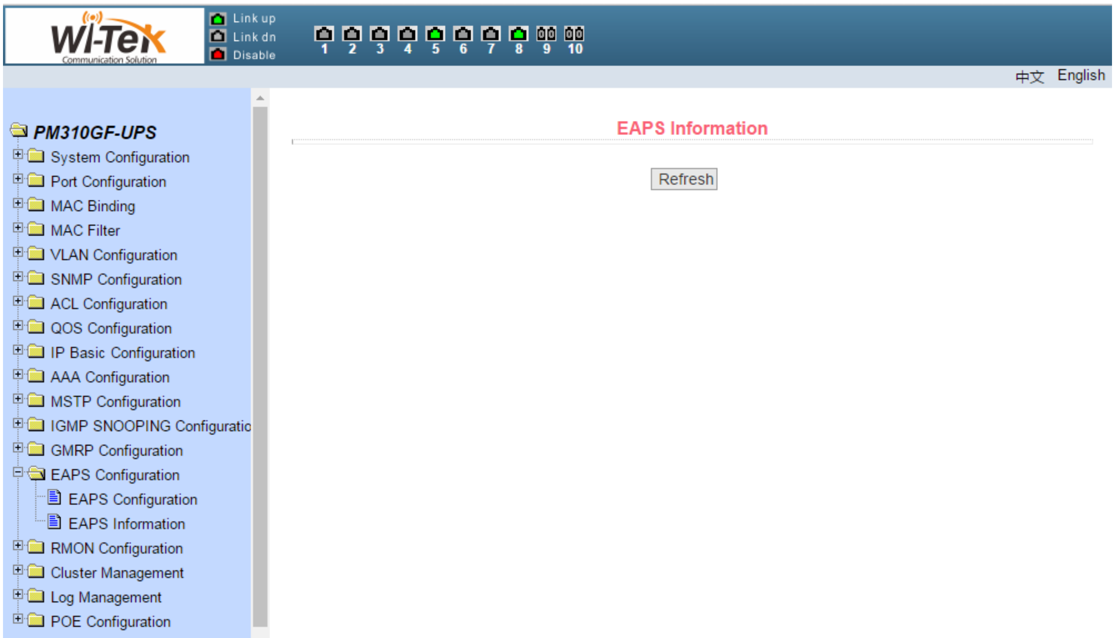
EAPS Configuration

EAPS Ring ID	1 ▾	
Create Status	Not Created	
Mode	None ▾	
primary port	▾	
secondary port	▾	
Control VLAN	0	
Protected VLANs		Format: 2,4,6 or 3-10
Hello Time Interval	0	s
Fail Time	0	s
Data Span	Disable ▾	
Extreme Interoperability	Disable ▾	
Enable Status	Disable ▾	

Pic 60 EAPS configuration page

（2）EAPS information page

Figure 61 shows the EAPS information page.Users can view EAPS configuration information from this page.

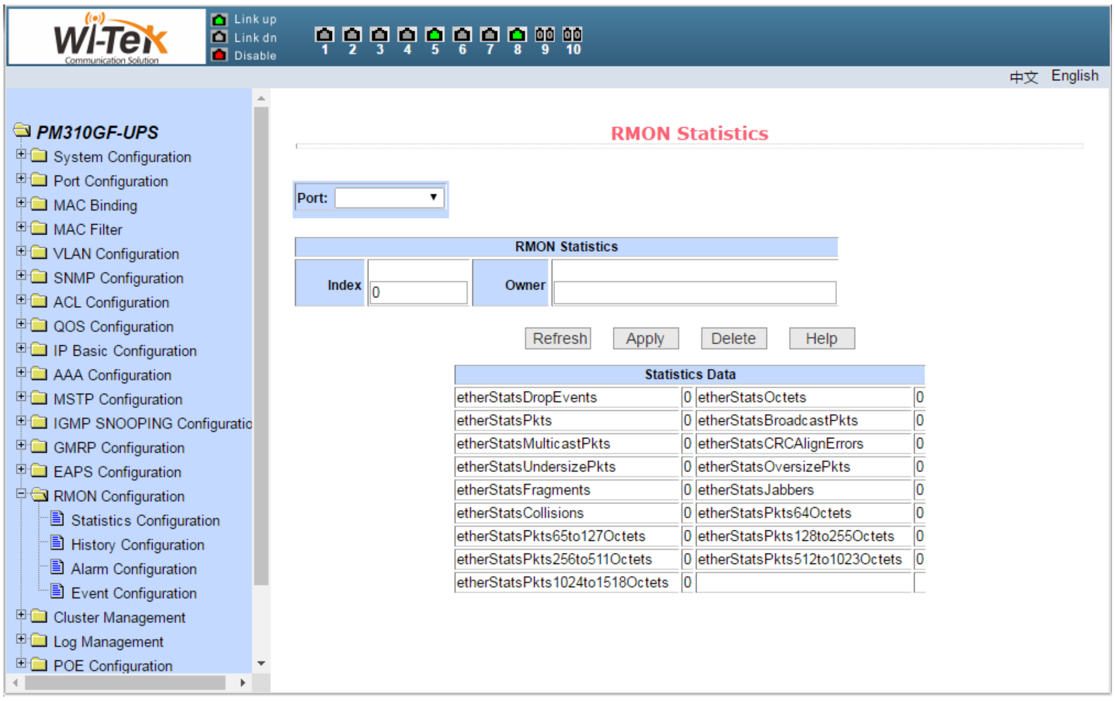


Pic 61 EAPS information page

17、RMON configuration

（1）**RMON** statistics group configuration page

Figure 62 shows the RMON statistics group configuration page.The user can configure the RMON statistics group through this page.Select a port from the drop-down list to view / configure the RMON statistics group configuration for that port.If the index number is 0, the correct index number (in the range of 1 to 100) is filled and the owner is optional. You can configure the RMON statistics group for the port.The statistics table shows the port statistics from the successful configuration.



RMON Statistics

Port:

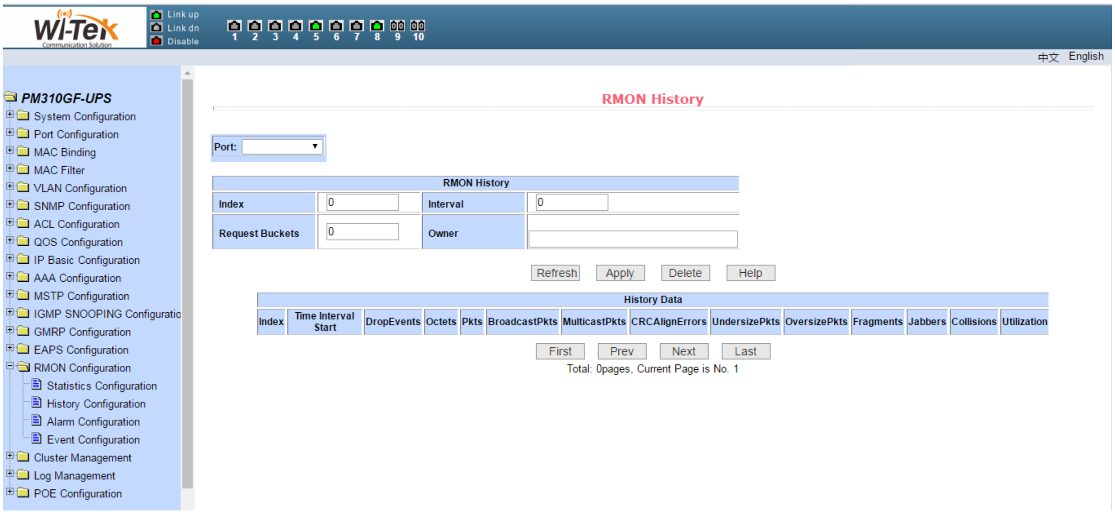
RMON Statistics			
Index	0	Owner	

Statistics Data			
etherStatsDropEvents	0	etherStatsOctets	0
etherStatsPkts	0	etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0	etherStatsCRCAlignErrors	0
etherStatsUndersizePkts	0	etherStatsOversizePkts	0
etherStatsFragments	0	etherStatsJabbers	0
etherStatsCollisions	0	etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0	etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0	etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0		

Pic 62 RMON statistics group configuration page

（2）RMON history group configuration page

Figure 63 shows the RMON history group configuration page.User can configure the RMON history group from this page.Select a port from the drop-down list to view / configure the RMON history group configuration for that port.If the index number is 0, the correct index number (in the range of 1 to 100), the interval, the request Buckets, and the owner is optional. You can configure the RMON history group for the port.Interval refers to the time interval for collecting data, in seconds, in the range of 1-3600; the request Buckets is the allocated storage size, indicating how many records are stored, the range is 1-100.The statistics table shows the historical data that has been acquired since the configuration was successful.



RMON History

Port:

RMON History			
Index	0	Interval	0
Request Buckets	0	Owner	

History Data

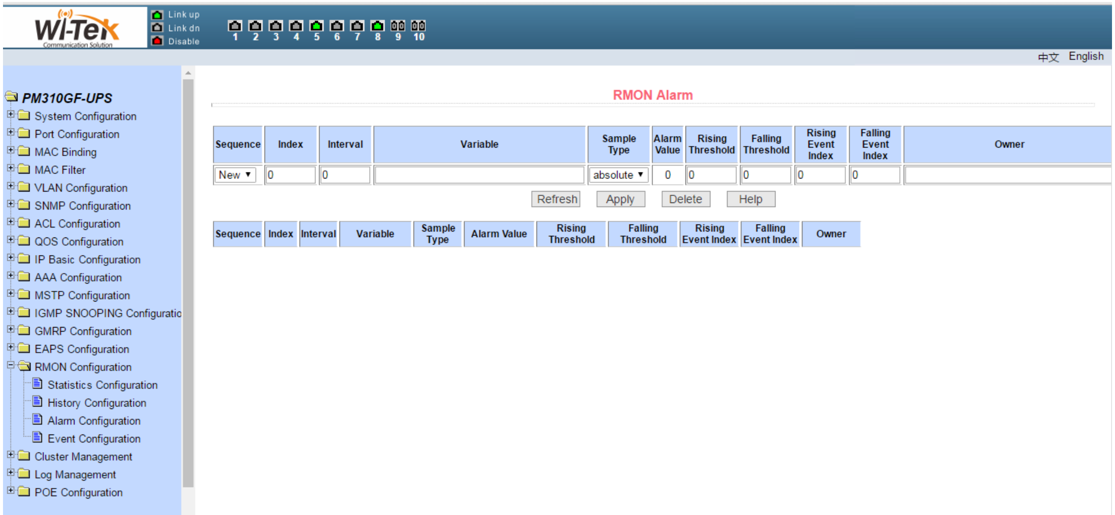
Index	Time Interval Start	DropEvents	Octets	Pkts	BroadcastPkts	MulticastPkts	CRCAlignErrors	UndersizePkts	OversizePkts	Fragments	Jabbers	Collisions	Utilization

Total: 0pages, Current Page is No. 1

Pic 63 RMON history group configuration page

（3）RMON alarm group configuration page

Figure 64 shows the RMON alarm group configuration page, where users can create or modify the RMON alarm group.Select a configured alarm group from the drop-down list to view / configure its information and select New to create it.The index range is 1 to 60, the interval is 1 to 3600, in seconds, the monitoring object must fill in the MIB node, the contrast can choose absolute or delta,Also must fill in the upper and lower threshold, the event index, the owner is optional.The alarm value is read-only and shows the sampled value when the last alarm was issued. The event index refers to the index number of the RMON event group and must be configured in advance.



RMON Alarm

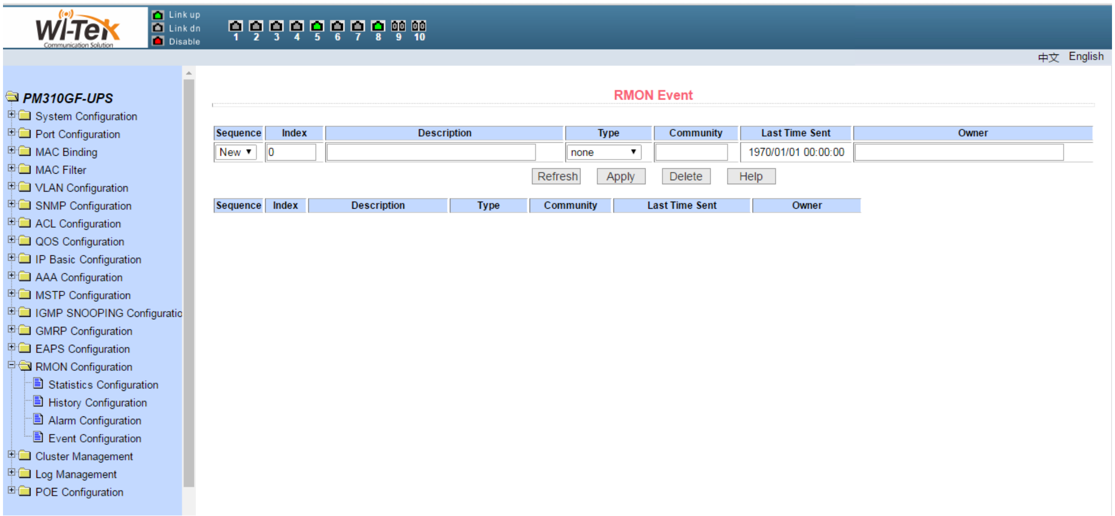
Sequence	Index	Interval	Variable	Sample Type	Alarm Value	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner
New	0	0		absolute	0	0	0	0	0	

Sequence	Index	Interval	Variable	Sample Type	Alarm Value	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner

Pic 64 RMON alarm group configuration page

（4）RMON event group configuration page

Figure 65 shows the RMON event group configuration page, where 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 range is 1 to 60, and the description is a string. The action can select none (no operation), log (log), SNMP-trap or log-and-trap.), The shared name does not work in this device, the owner is optional.The last send time is read-only, showing the last time the event was sent.



RMON Event

Sequence	Index	Description	Type	Community	Last Time Sent	Owner
New	0		none		1970/01/01 00:00:00	

Sequence	Index	Description	Type	Community	Last Time Sent	Owner

Pic 65 RMON event group configuration page

18、Cluster configuration

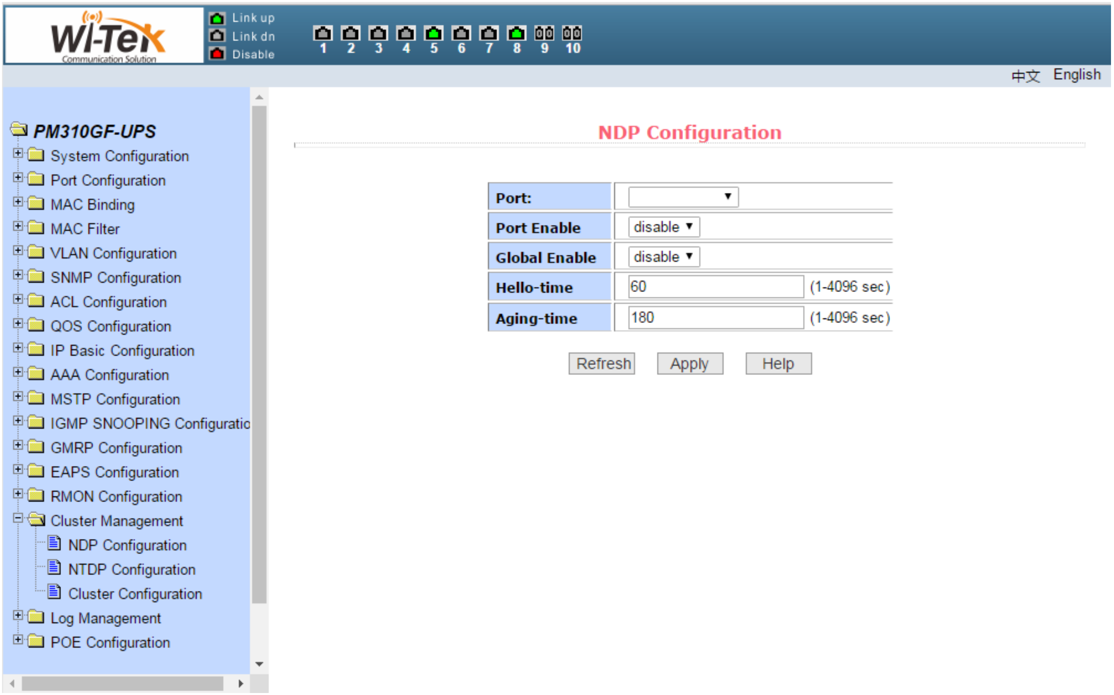
（1）NDP configuration page

Figure 66 shows the NDP configuration page, where users can configure NDP.The information that can be set includes: port selection, port NDP function, global NDP function, NDP packet sending interval, and aging time of NDP packets on the receiving device.

Port selection, select the port as required, and enable the port NDP function. NDP must run normally, and the NDP function of the global and port must be enabled at the same time.

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

Configure the interval for sending NDP packets, the valid time range is 1-4096 seconds, the default is 60 seconds.



NDP Configuration

Port:		
Port Enable	disable	
Global Enable	disable	
Hello-time	60	(1-4096 sec)
Aging-time	180	(1-4096 sec)

Pic 66 NDP configuration page

（2）NTDP configuration page

Figure 67 shows the NTDP configuration page, where users can configure NTDP. The information that can be set includes: Select port, enable port NTDP function, enable global NTDP function, topology collection range, time topology collection interval, first port forwarding packet delay time, and other port forwarding packets delay.

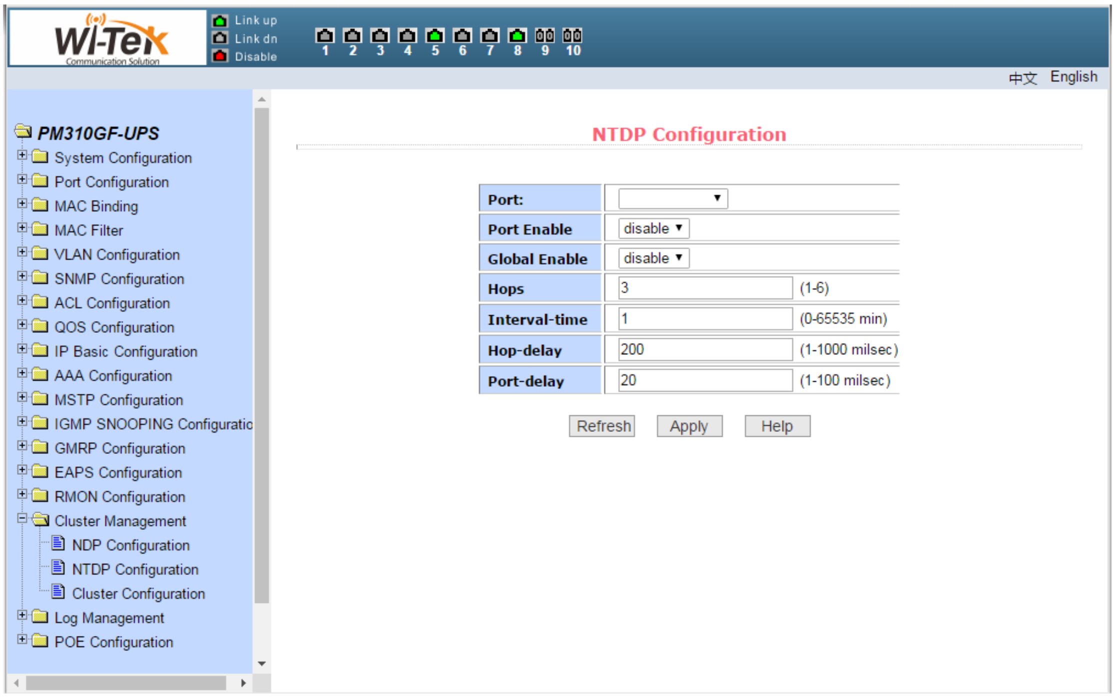
Port selection, you can select the port as required, and enable port NTDP function. NTDP to run normally, you must also enable the global and port NTDP function.

Configure the range of topology collection. The effective range is 1-6. In the default topology, the maximum hop count of the device is 3.

Configure the interval for collecting topology information. The effective range is 0-65535 minutes. The default configuration is 1 minute.

Configure the delay time for forwarding packets on the first port. The effective range is 1-1000 milliseconds. The default configuration is 200 milliseconds.

Configure the delay time for forwarding packets on the first port. The effective range is 1-100 milliseconds. The default configuration is 20 milliseconds.



NTDP Configuration

Port:	▾	
Port Enable	disable ▾	
Global Enable	disable ▾	
Hops	3	(1-6)
Interval-time	1	(0-65535 min)
Hop-delay	200	(1-1000 milsec)
Port-delay	20	(1-100 milsec)

Refresh Apply Help

Pic 67 NTDP configuration page

（3）Cluster configuration page

Figure 68 shows the cluster configuration page, the user can configure the cluster through this page and view the cluster member table.The information that can be set includes the functions of enabling the cluster, configuring the management VLAN, the address pool of the cluster, the interval for sending the handshake packets, the effective retention time of the device, the name of the cluster, the way of joining the cluster, and deleting the cluster.

Enable the cluster function and enable the cluster function to function normally. You must enable the cluster function first.

Configure a management VLAN with a valid range of 1-4094 and default to vlan1.

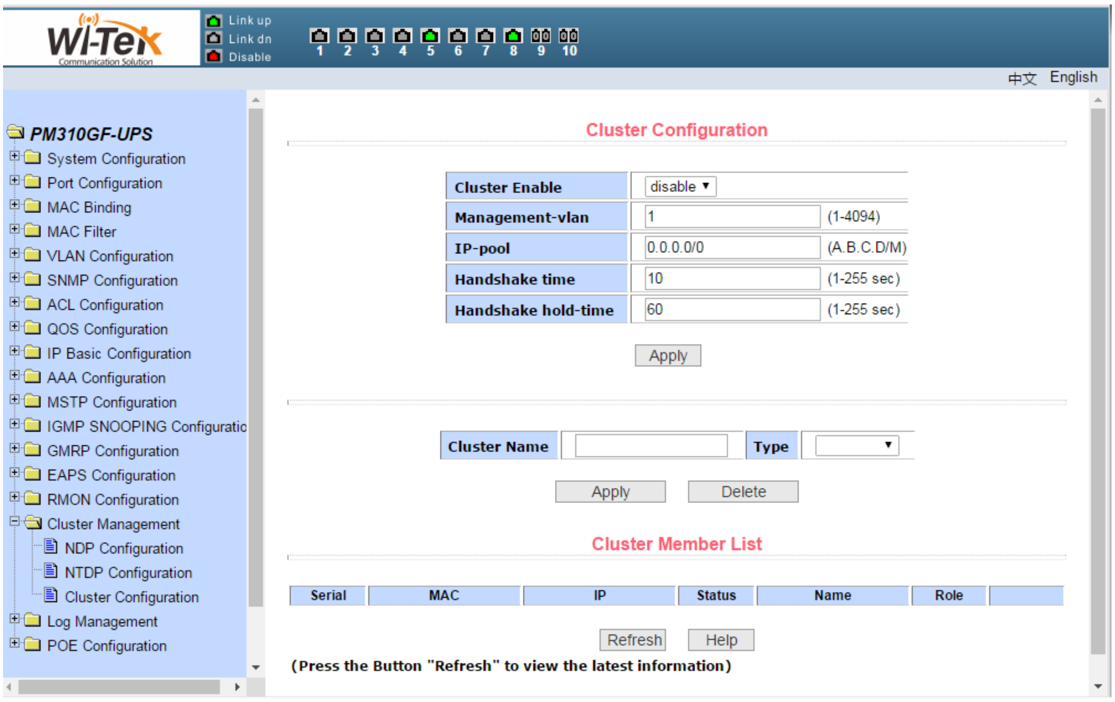
Configure the range of private IP addresses used by the member devices in the cluster. The effective range of the IP address is 0.0.0.0 ~ 255.255.255.255. The effective range of the mask length is 0 ~ 32.

The interval for sending the handshake packets is 1-255 seconds and the default 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, choose to join the cluster, the way to join both manual and automatic. After the cluster is set up, it can be automatically switched to manual, but manual can not be switched to automatic.Manual mode can change the cluster name.

After you create a cluster, you can view member devices and candidate devices in the cluster member table,you can add a member device or add a candidate device to a member device depending on the role.



Cluster Configuration

Cluster Enable	disable ▾	
Management-vlan	1	(1-4094)
IP-pool	0.0.0.0/0	(A.B.C.D/M)
Handshake time	10	(1-255 sec)
Handshake hold-time	60	(1-255 sec)

Apply

Cluster Name		Type	▾

Apply Delete

Cluster Member List

Serial	MAC	IP	Status	Name	Role	

Refresh Help

(Press the Button "Refresh" to view the latest information)

Pic 68 cluster configuration page

19、ERPSc configuration

（1）EAPS configuration page

Figure 69 shows the EAPS configuration page,Users can use this page to enable ERPS function, configure ERPS parameters, create and delete ERPS instance, ERPS ring and other applications.

ERPS instance Create and delete ERPS instances (<1-8>)

Node role Configure the role of the node in the ERPS ring, the internetwork node or the non-interconnected node

ERPS ring Create and delete ERPS rings (<1-32>)

Ring mode Configure ERPS ring mode, primary ring or subring

Node mode Configuration ERPS ring node mode, RPL owner node, RPL neighbor node or common ring node

Protocol VLAN configuration,delete ERPS ring protocol VLAN (<2-4094>)

Data VLAN Configuration ERPS Ring Data VLAN (<1-4094>)

Ring port Configuration, delete ERPS ring port, RPL port or common ring port

Restore Behavior Configure ERPS ring recovery behavior, recoverable or unrecoverable

hold-off Time Configure the ERPS loop hold-off time (<0-10000>), in ms, the default is 0

Guard Time Configure the ERPS ring guard time (<10-2000>), in ms, defaults to 500

Wtr Time Configure the ERPS ring wtr time (<1-12>), in min, default to 5

Wtb Time Configure the ERPS ring wtb time (<1-10>), in seconds, the default is 5

Protocol packet transmission time Configure the sending time of the ERPS ring protocol packets (<1-10>), in seconds, the default is 5

Enable ERPS ring Turn the ERPS ring on or off

Force to switch ERPS ring port Forced, clear to switch ERPS ring port

Force manual ERPS ring port Force, remove manual ERPS ring port

Manual recovery Handle recovery of ERPS ring's unrecoverable behavior or manual recovery before WTR / WTB expires

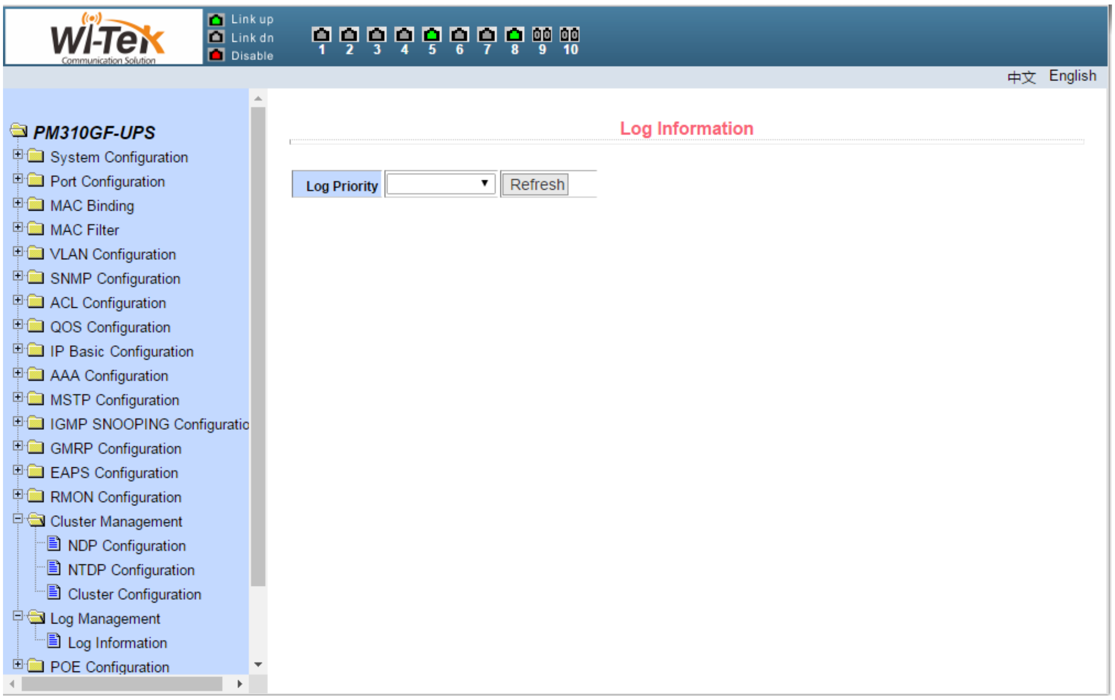
（2）ERPS information page

Figure 70 shows the ERPS information page, where users can view the ERPS configuration information.

20、Log management

（1）Log information

Figure 71 shows the log information page, the user can view the log through this page. Select the priority from the drop-down list, you can view the log of that level, click Refresh to view the latest log.



Pic 71 Log information page

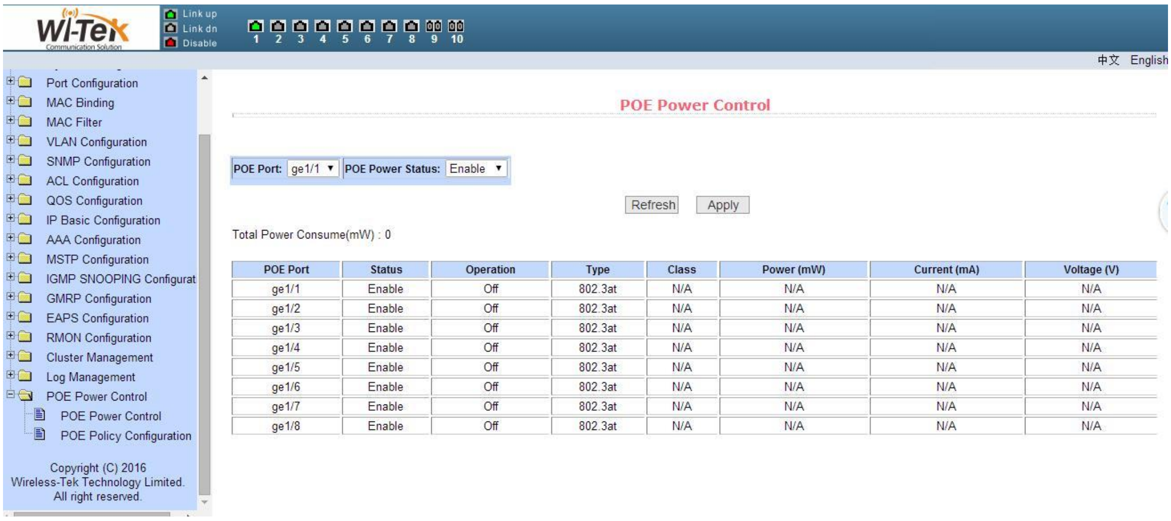
21、POE port configuration

（1）POE port configuration

Figure 72 shows the 48V 802.3af/at POE product configuration page. You can configure POE device total power (to be updated), POE single port power (to be updated), POE on or off;This page allows you to view information about the current POE device

POE port：Select the power supply port number (1-24)

POE commodity status：enable or disable



POE Port: ge1/1 POE Power Status: Enable

Total Power Consume(mW) : 0

POE Port	Status	Operation	Type	Class	Power (mW)	Current (mA)	Voltage (V)
ge1/1	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/2	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/3	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/4	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/5	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/6	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/7	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/8	Enable	Off	802.3at	N/A	N/A	N/A	N/A

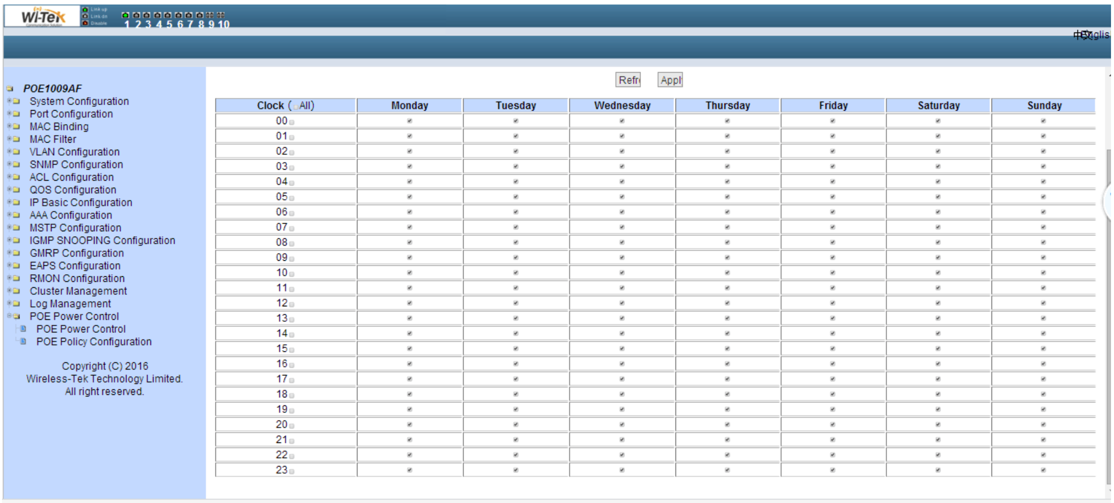
Pic 72 48V 802.3af/at POE product configuration page

（2）POE schedule configuration

Figure 73 shows the POE schedule configuration page. Through scheduling management, you can enable or disable POE power supply according to actual requirements. The control mode is hour + week mode.

Control port：Used to select the ports that need scheduled management (1-24)

control function：enable or disable



Clock (□ All)	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
00 □	☑	☑	☑	☑	☑	☑	☑
01 □	☑	☑	☑	☑	☑	☑	☑
02 □	☑	☑	☑	☑	☑	☑	☑
03 □	☑	☑	☑	☑	☑	☑	☑
04 □	☑	☑	☑	☑	☑	☑	☑
05 □	☑	☑	☑	☑	☑	☑	☑
06 □	☑	☑	☑	☑	☑	☑	☑
07 □	☑	☑	☑	☑	☑	☑	☑
08 □	☑	☑	☑	☑	☑	☑	☑
09 □	☑	☑	☑	☑	☑	☑	☑
10 □	☑	☑	☑	☑	☑	☑	☑
11 □	☑	☑	☑	☑	☑	☑	☑
12 □	☑	☑	☑	☑	☑	☑	☑
13 □	☑	☑	☑	☑	☑	☑	☑
14 □	☑	☑	☑	☑	☑	☑	☑
15 □	☑	☑	☑	☑	☑	☑	☑
16 □	☑	☑	☑	☑	☑	☑	☑
17 □	☑	☑	☑	☑	☑	☑	☑
18 □	☑	☑	☑	☑	☑	☑	☑
19 □	☑	☑	☑	☑	☑	☑	☑
20 □	☑	☑	☑	☑	☑	☑	☑
21 □	☑	☑	☑	☑	☑	☑	☑
22 □	☑	☑	☑	☑	☑	☑	☑
23 □	☑	☑	☑	☑	☑	☑	☑

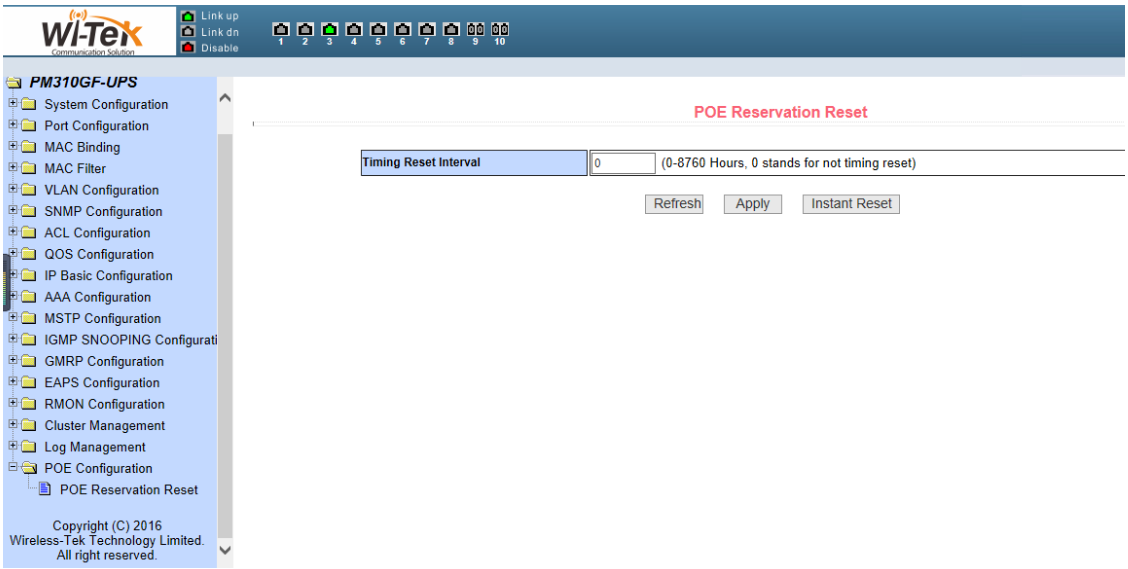
Pic 73 48V 802.3af/at　POE schedule configuration page

（3）POE Online detection (system to be updated)

Used to turn on or off the online detection device status detection, when the device when the machine is re-starting the device power supply.

（4）24V Passive POE Reset

For 24V Passive PoE model, you can reset all PoE Port at page, to finish restart your PD device like Wireless AP.



POE Reservation Reset

Timing Reset Interval	0	(0-8760 Hours, 0 stands for not timing reset)

Pic 74 24V Passive POE product PoE Port Reset