

## XonTel XT-1600G/XT-2400G PoE Switches

### Web Management User-Guide



## Contents

Chapter 1、WEB page overview.....	3
1、WEB Access features.....	3
2、WEB browsing system requirements.....	3
3、WEB browsing session landing.....	4
4、WEB page elements.....	5
5、The structure of Navigation tree.....	6
6、Page button Introduction.....	6
7、Error messages.....	7
8、Entry Field.....	7
9、Status Field.....	8
Chapter 2 WEB page introduction.....	9
1、Login dialog Box.....	9
2、Main Page.....	10
3、System Configuration:.....	11
4、Port Configuration.....	19
5、MAC binding.....	27
6、MAC filtering.....	28
7、VLAN Configuration.....	29
8、SNMP Configuration.....	32
9、ACL Configuraion.....	33
10、QoS Configuration.....	37
11、IP Basic Configuration.....	38
12、Certification. Authorization. Accounting (AAA) configuration.....	40
13、MSTP Configuration.....	44
14、IGMP SNOOPING configuration.....	45
15、GMRP Configuration.....	46
16、EAPS Configuration.....	48
17、RMON Configuration.....	49
18、Cluster Management.....	53
19、Log Management.....	56
20、PoE port configuration.....	57

# WEB page operating manual

This manual focus on describing the WEB page of XonTel XT-1600G/XT-2400G switches, the user can managed the XonTel XT-1600G/XT-2400G switches through WEB page. This manual only introduce the simple operations of the various WEB page of the various switches. This manual includes the following:

- 1, WEB page overview
- 2, WEB page description

## Chapter 1 、WEB page overview

### 1 、WEB Access features

- XonTel XT-1600G/XT-2400G switches provide users with Web access functionality. Via Web browser, users can access switches, manage and configure the switch. WEB accessing's main features are:
  - 1, Easy to access: Users can easily access on switch from anywhere using the network.
  - 2, users can visit the web pages of the switch by using the familiar Microsoft Internet Explorer and other browsers, WEB pages of graphical and tabular format presented to the user.
  - 3, Switch provides a wealth of WEB pages, the user can configure and manage vast majority of functions of the switch.
  - 4, WEB page' function classification &integration, make the user find the relevant pages to configuration and management.

### 2 、WEB browsing system requirements

Please see the form

1. Form 1 :

Hardware &Software	system requirements
<b>CPU</b>	Pentium 586 above
<b>Memory</b>	128MB above
<b>Resolution</b>	800x600 above
<b>Color</b>	256 colors above
<b>Browser</b>	IE4.0 above or Netscape4.01 above
<b>Operating system</b>	Microsoft® ,Windows95®,Windows98®,WindowsNT®, Windows2000®, WindowsXP®,WindowsME®, WindowsVista®, Linux,Unix ect.

**Note :**

Microsoft ®, Windows95 ®, Windows98 ®, WindowsNT ®, Windows2000 ®, WindowsXP ®, Windows ME ®, WindowsVista ® is a registered trademark of Microsoft Corp. All other product names, trademarks, registered trademarks and service marks, copyrights held by their respective owners.

### 3 、WEB browsing session landing

- Before start Web browsing session ,the user need to make sure:
  1. Has configure the IP of switch, under the default case, the switch VLAN1 interface IP address is **192.168.0.1**,
  2. Subnet mask is **255.255.255.0**.
  3. Has a Web browser installed on the host to connect to the network, and the host can PING-pass switches.
  4. After completing these two tasks, the user put the right address on the browser's address bar of the switch and press Enter to enter the switch after the Web login page, shown in Figure 1. When the multi-user management is not enabled, the user login need for anonymous Web user (**admin**) password for authentication, and only entered the correct password can access Web, anonymous user password by default is (**xontel**).

If the system enabled a multi-user management and configure the privileged user, the anonymous user's password will not force users to visit the Web. User access not do anonymous user's password authentication, but to do a multi-user management, user name and password authentication.



Figure 1

## 4 、WEB page elements

Shown in Figure 2, WEB page is mainly composed of three parts: title page, navigation tree page and main page

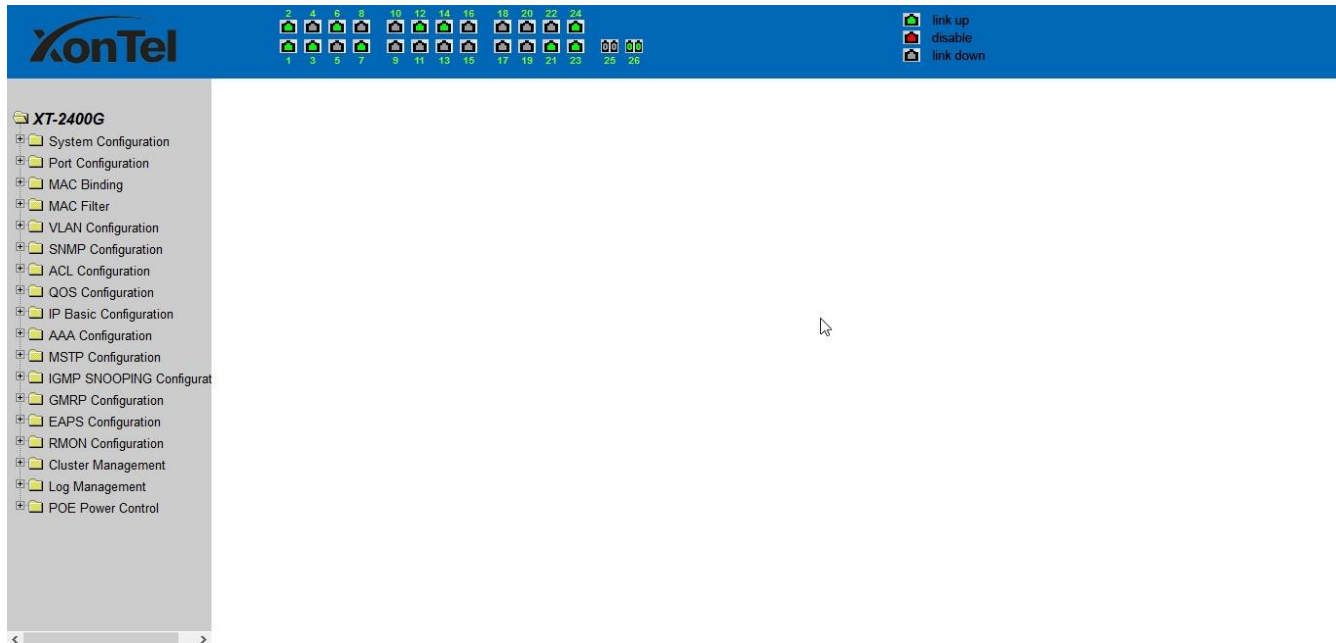


Figure 2

**Title page** is used to display the logo

**Main page** is used to display the user from the navigation tree, select the page

## 5 、 The structure of Navigation tree

Figure 3 shows the navigation tree organizational structure.

Navigation tree is located in the lower left of each page, using the tree display nodes of the WEB page, users can easily find the page you want to manage the WEB. According to a different web page functionality can be divided into different groups, each including one or more pages. Most of the navigation tree in the name of the corresponding web page top of page title abbreviation.

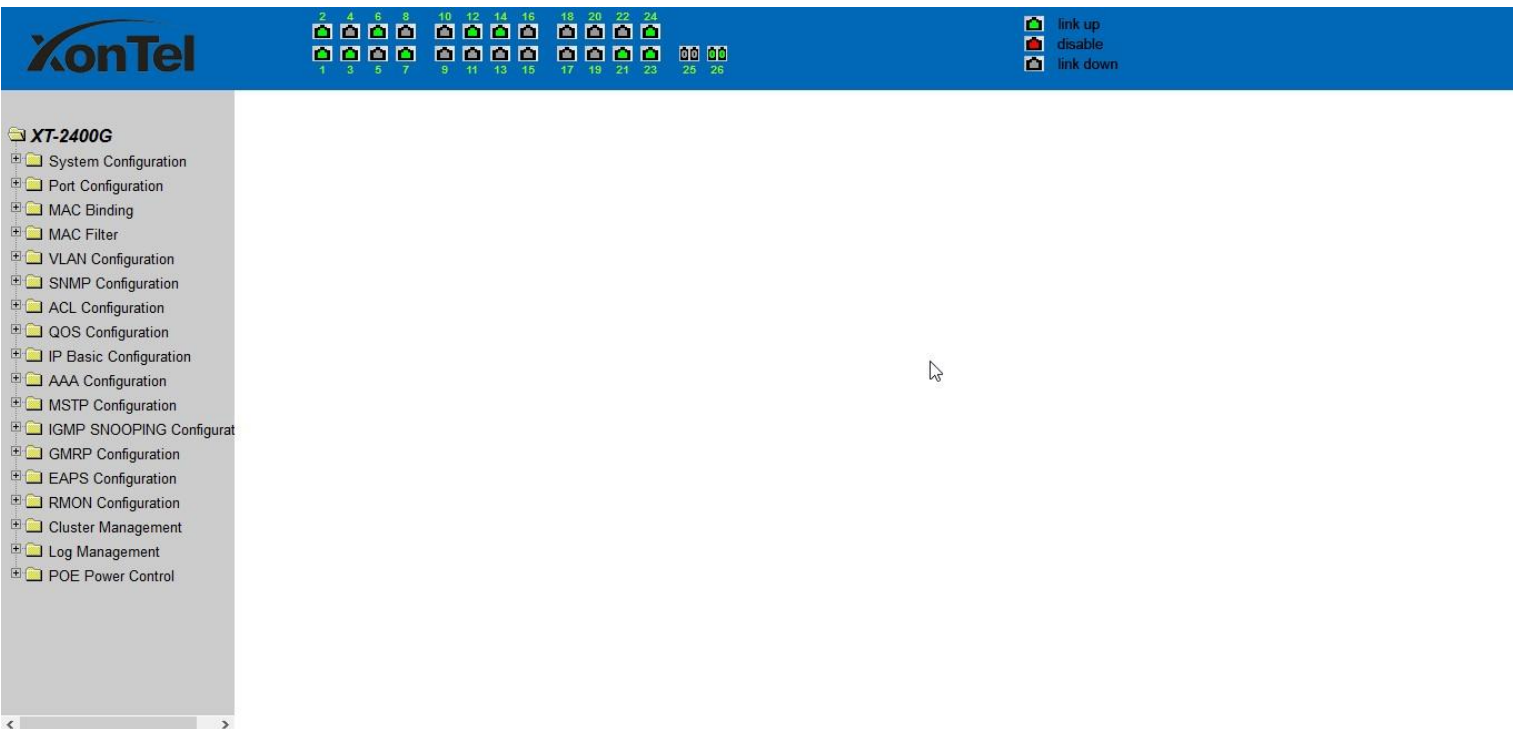


Figure 3

## 6 、 Page button Introduction

On the pages, here are some commonly used button, the role of these buttons are generally the same, form 2 on the role of these buttons are described:

Form 2 :

button	Effect.
Refresh	Update all fields on the page.
Apply	Numerical value will be updated into the memory. Because the error-checking should be implement by the Web Server, before the user selects the button will be no error checking.
Delete	Delete the current record.
Help	Open help pages, view the individual pages of the configuration instructions.

## 7 、 Error messages

If the switch WEB server error occurred while processing user requests, it will display a dialog box in the corresponding error message. For example, Figure 4 shows an error message dialog box.



Figure 4

## 8 、 Entry Field

Some pages of the most left column in the table has an entry field, as shown in Figure 5, through the field can access different rows in the table. When you choose a lines for the filed, which lines the corresponding information is displayed in the first line, then only the line can be edited, the line also known as the activities line. A time when it was first loaded, it shows the filed new, activity line is empty.

If want to add a new line , should select new from the drop-down menu of entry field, , enter the new line's information, and then press apply button.

If you want to edit the line already exists, it is necessary select the appropriate line number of the drop-down menu, according to need to edit the line, and then press the apply button, you will see a corresponding change in the table displayed.

If you want to delete a row, select the line number from entry field's drop-down menu, then press the delete key, this line will disappear from the table.

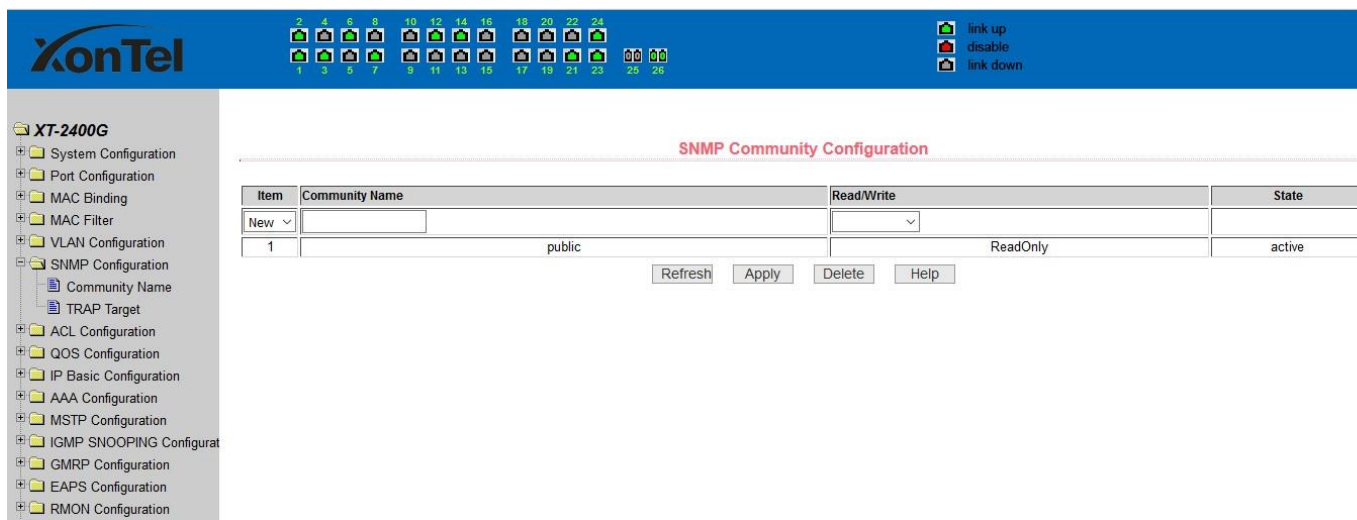


Figure 5

## 9 、 Status Field

Some pages of the most right column in the table there is a state field, as shown in Figure 6, the field displays the line status. Since all row state changes are processed in-house, so the status field is read-only. Once the line information of the entry filed into force, the line will automatically become the active state the status active.

The screenshot shows the XonTel web interface for the XT-2400G device. The top status bar displays 26 port icons, with a legend indicating 'link up' (green), 'disable' (red), and 'link down' (grey). The left navigation menu lists various configuration options under 'System Configuration' and 'Port Configuration'. The main content area is titled 'Port Statistics Information' and features a 'Port:' dropdown menu. Below this is a table with statistics for a selected 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 Unknown 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		

At the bottom right of the table, there are 'Refresh' and 'Help' buttons.

Figure 6 the web page of status field



## Chapter 2 WEB page introduction

XonTel XT-1600G / XT-2400G switches WEB pages organized into groups, each including one or more of the WEB pages. The following are introduced one by one on each page.

### 1 、Login dialog Box



Figure 7 WEB browsing session of the login page

Figure 7 shows the login dialog box, the logon dialog box will be displayed while the user login the web page at the first time. When the user filled out the correct user name and password, then click the Enter button can log on to the switch Web server. Passwords are case-sensitive, the anonymous user password can be maximum set up to 16 characters, while the multi-user name and password can be set up to 11 characters. Switch default user name is the anonymous user name **admin**, default password for the anonymous user's password, the anonymous user's password is **xontel**.

## 2 、 Main Page

Figure 8 shows the WEB main page of XonTel XT-1600G/XT-2400G switches. This page will be displayed after the user logs in web pages

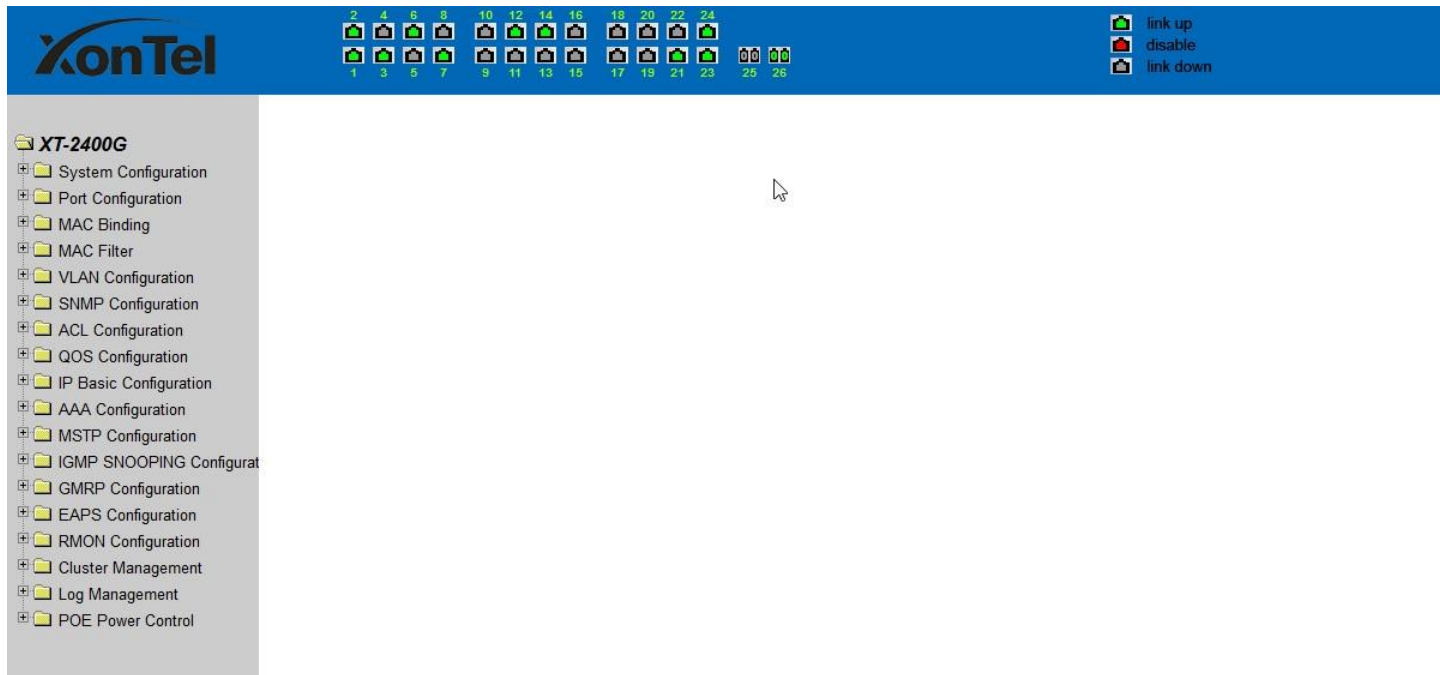


Figure 8 XonTel XT-1600G/XT-2400G POE switches main page

### 3 、 System Configuration:

#### ( 1 ) Basic information page

Figure 9 is the basic information of configuration page, users can configure the basic information for the switch.

System Description display the description of the relevant parameters of system.

System descriptor ID display system in the network identity management.

The system version number is displayed the current software version number of XonTel switches.

The number of switches interface displays the current number of interfaces in the switch.

The system start-up time display switches from start to the present time.

The system name as the switch's system name in the network, the user can modify the system name.

The systematic location as the switch's physical location showing at the network, the user can modify the system locations.

system contact show the contacts person and details of the current node, the user can modify the system contact.

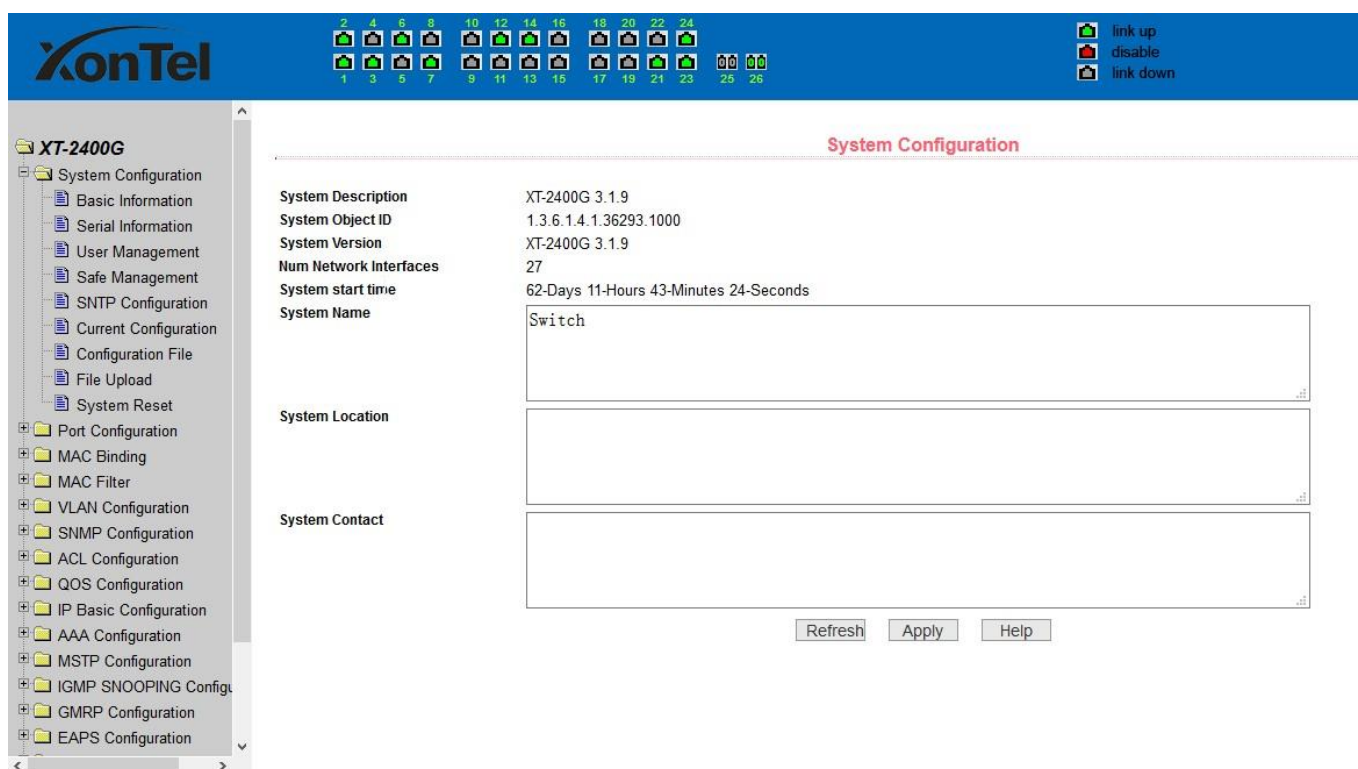


Figure 9 Basic information Page

## ( 2 ) Serial port information page

Figure 10 is a serial port configuration page, the page displays serial baud rate and other related information. When the host through the serial port terminals (such as Windows, HyperTerminal) to the management of switches, serial console on the COM port configuration must be consistent with this page information.

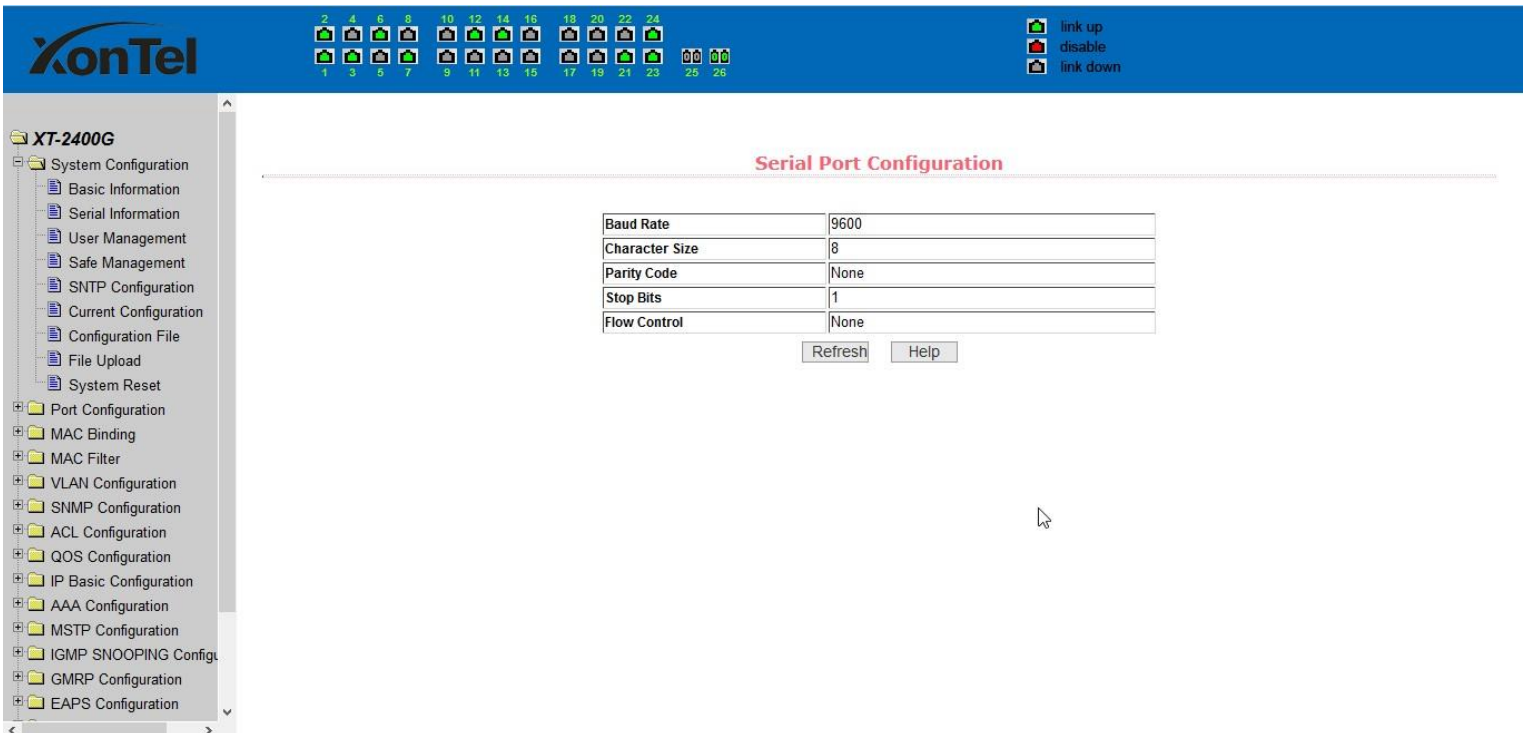


Figure 10 Serial port information page

### ( 3 ) User management page

Figure 11 is a user management page, the user can modify this switch anonymous user (**admin**) password, Telnet and the Web without opening a multi-user, and they all use the same anonymous user's password. Passwords are case-sensitive, and can be up to 16 characters. If you want to change your password, the user need to enter the new password twice, once the user clicks the application button, the new password is activated, then if the switch is not enabled multi-user, will display the login dialog box (as shown in Figure 7), require the user to re - Login the web page, with a new anonymous user password.

Meanwhile through this page user can configure the multi-user, switch if in the default is no multi-users that is, not enabled the multi-user management functionality, at this time does not require multi-user login user name and password authentication. For Telnet, when adding a user name, multi-user management features were enabled, and when removed all of the user, multi-user management functionality has been closed. For the Web, when adding a user name, if it is privileged user, multi-user management functionality was enabled, when all of the privileges users have been deleted, multi-user management functionality has been closed. When the multi-user management features enabled, the anonymous user's password will not take effect, log Telnet and the Web requires a multi-user user name and password authentication. When the multi-user management function is turned off, at this time if the configured anonymous user's password, log on Telnet, and Web need anonymous user's password authentication

The screenshot displays the XonTel web management interface. On the left is a navigation tree for the 'XT-2400G' device, with 'User Management' selected. The main content area has a blue header with port status indicators (1-26) and a legend for 'link up', 'disable', and 'link down'. Below the header, the 'Change Password' section contains a form with fields for 'User name' (admin), 'Old password', 'New password', and 'Re-enter password'. The 'Multi-user Management Configuration' section features a table with columns: Item, User name, Old password, New password, Re-enter password, and Privilege. The table lists the 'admin' user. Below the table are buttons for 'Refresh', 'Apply', 'Delete', and 'Help'.

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

Figure 11 user's management page

#### ( 4 ) Security Management Page

Figure 12 is **Security** management configuration page, through the page's configuration, , the administrator can control network management services TELNET, WEB and SNMP, you can open (enable) or off (disable) these services, these services can be mounted up with standards IP ACL group ,and the implementation of the source IP address control, control access to the host of these services

When the Switch default, Telnet, WEB and SNMP services are open and no ACL filtering, that is, all hosts have access to the switch of these three services. If the administrator for safety, do not want to provide one or several services, which can shut down one or several services. If the administrator only hope that the specified host could access one or several services, can do the ACL filtering for one or several services. As a service to do ACL filtering, you need to open the service, and to select an IP standard ACL group (1-99), the primary factor it's the ACL group must be present.

Note that, if the administrator on this page control the WEB services (such as closing WEB Services) may cause users to no longer use the WEB page, then you can log switches by other means and to control the use of WEB service allows users to WEB page (such as the Open the WEB service).

The screenshot displays the XonTel web interface for the XT-2400G switch. The left sidebar shows a tree view of configuration options, with 'System Configuration' expanded. The main content area is titled 'User Safety Configuration (http,telnet,snmp)'. It features a table with three columns: 'Service Type', 'Management State', and 'Acl Group'. The table lists three services: http, snmp, and telnet, all currently set to 'Enable' and associated with ACL group '0'. A note above the table states '(Acl Group Must Exist, and range in 1-99)'. Below the table are buttons for 'Refresh', 'Apply', and 'Help'. At the top right of the interface, there are status icons for 'link up', 'disable', and 'link down'.

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

Figure 12 Security management page



### ( 5 ) Configure the current page

Figure 13 is the current configuration page. The user can view the current configuration of the switch on this page. Save key is to store the current system configuration in the configuration file. Because the storage operation requires erase& write FLASH chips, which take up some time. When the user was configured on the page and hope to restart the switch from using these configurations are not lost, you must exit the page before the current configuration page, click the Save button.

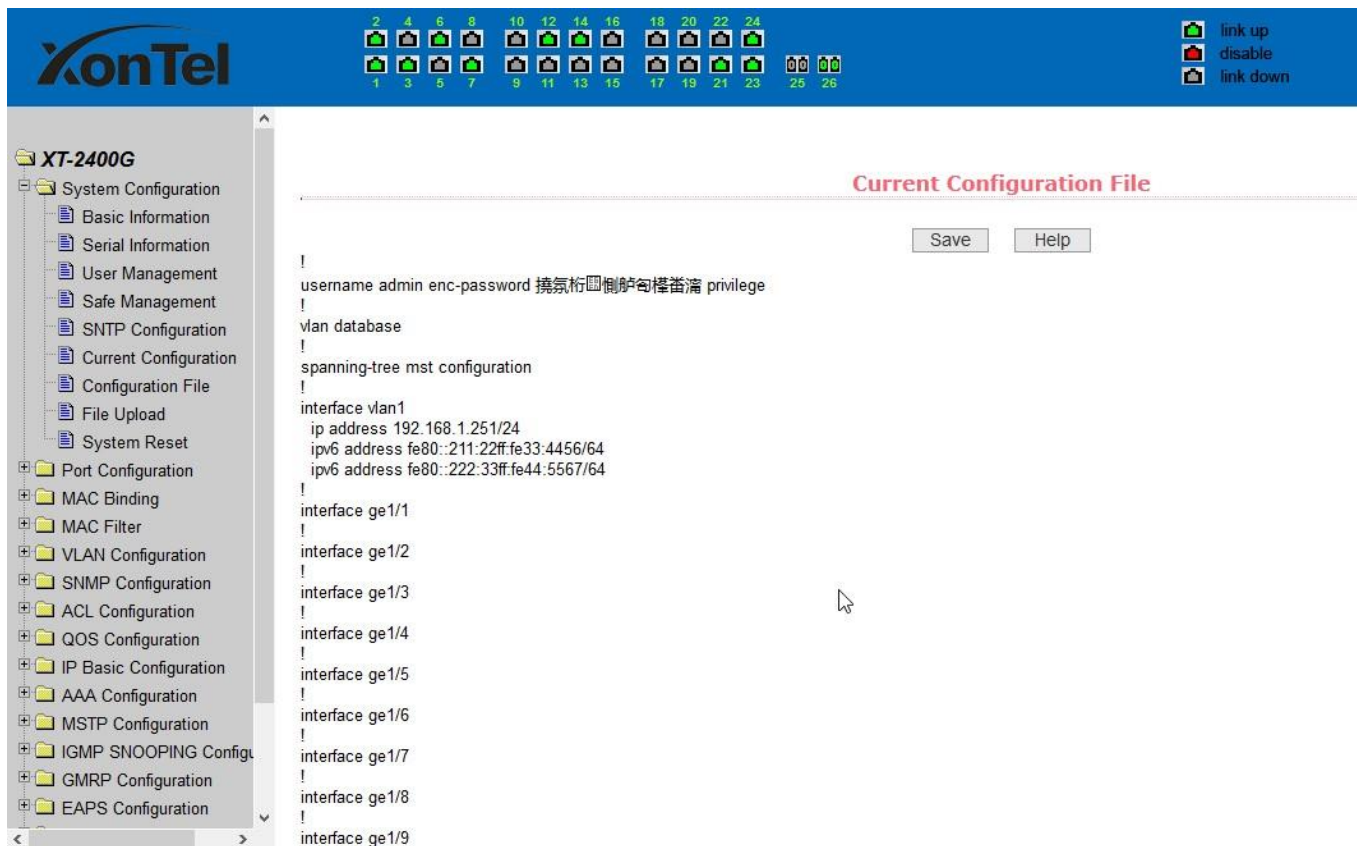


Figure 13 the current configuration page

### ( 6 ) Configuration file page

Figure 14 is profile configuration file page. This page allows users to view the system's initial configuration. The initial configuration is actually the configuration file in the FLASH, when the configuration file does not exist in FLASH, the system starts using the default configuration.

Delete key to delete the configuration file in the FLASH. Click the Delete button, will pop up a dialog box ,that will prompts the user sure to delete the configuration file or not, according to the dialog box to determine if it's ok, otherwise click Cancel button. Download button is used to downloaded a configuration file to the PC. Click to download button, will pop up a dialog box, users select Save and save the configuration file directory path. Download the configuration file names are as switch.cfg.

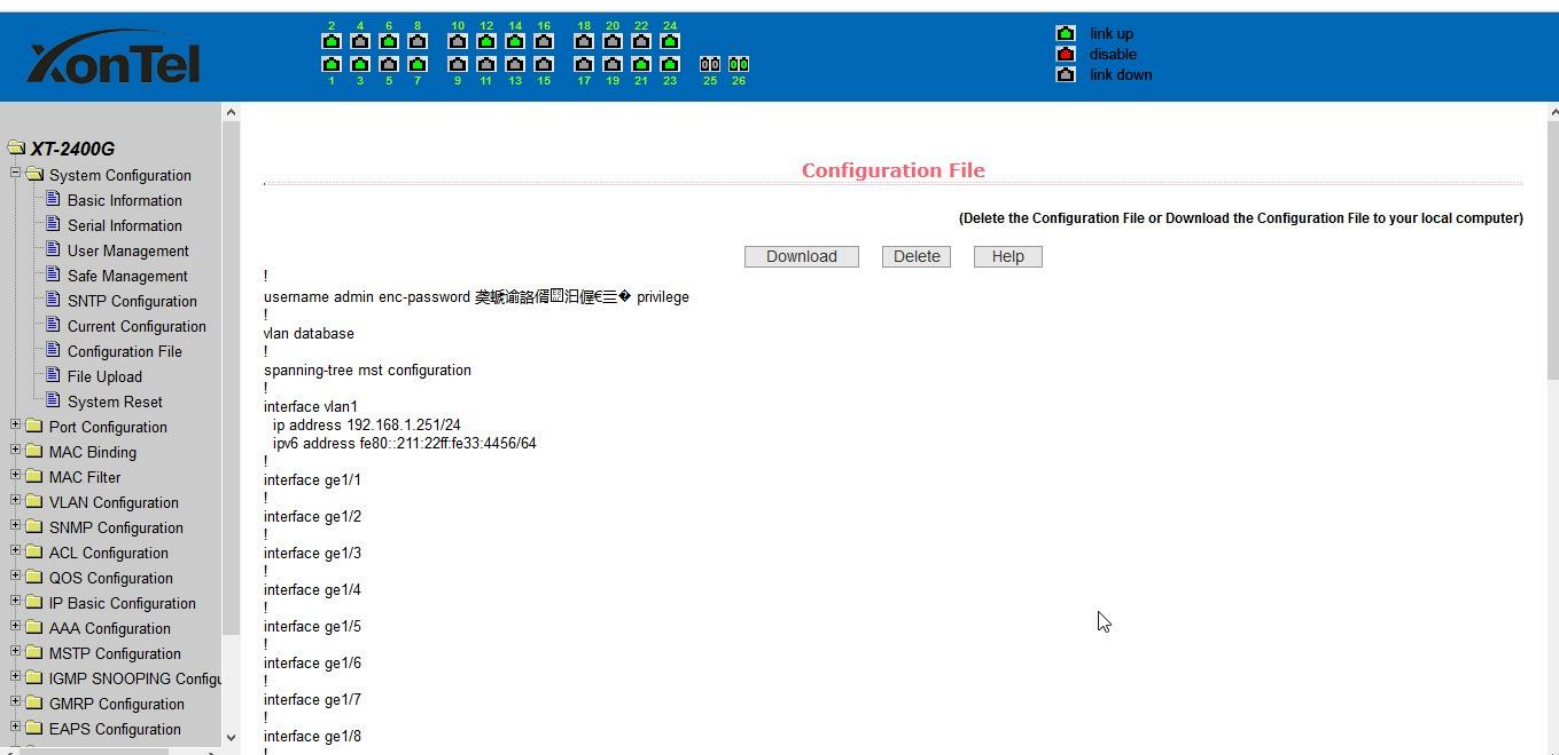


Figure14 Configuration file page



### ( 7 ) File upload page

Figure 15 is a file upload page, through this page a user can upload a configuration file and mapping files to the switch. Click the Browse button to select the upload configuration file or image file in the directory path on the PC. Click Upload button upload a configuration file or image file, configuration file extension must be \*.cfg, image file must be provided by the manufacturer and the file name extension must be \*.img. Transmission before the return of the results page, please do not click on other pages, or restart the switch; otherwise, the file transfer will lead to failure caused by system crashes.

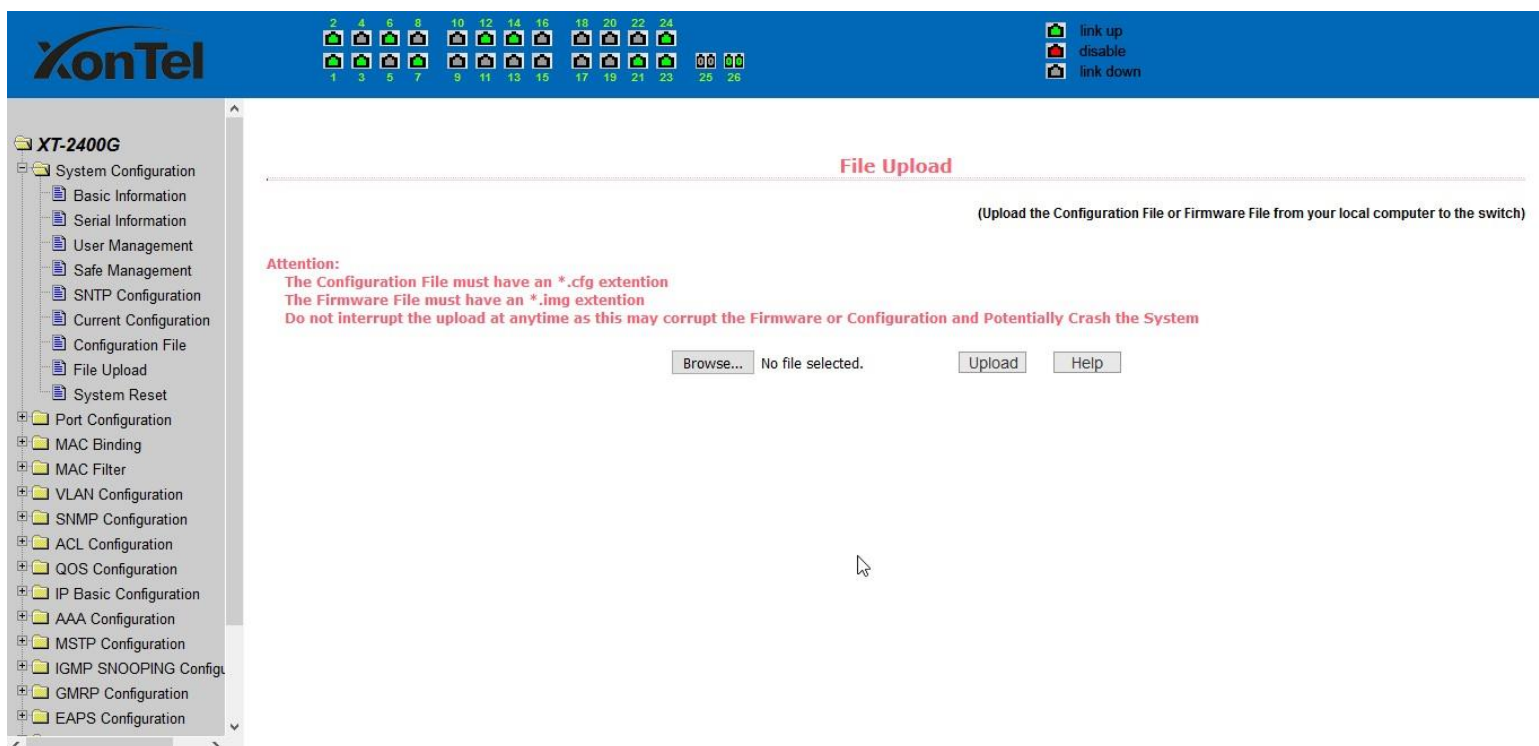


Figure 15 File Upload Page

### ( 8 ) System reset page

Figure 16 is system reset page, through this page users to restart the switch. When you click on Restart button, will pop up a dialog box that prompts the user to determine whether or restart the switch, if it is determined according to OK button, otherwise click Cancel button. Restart will no longer open the Web page.

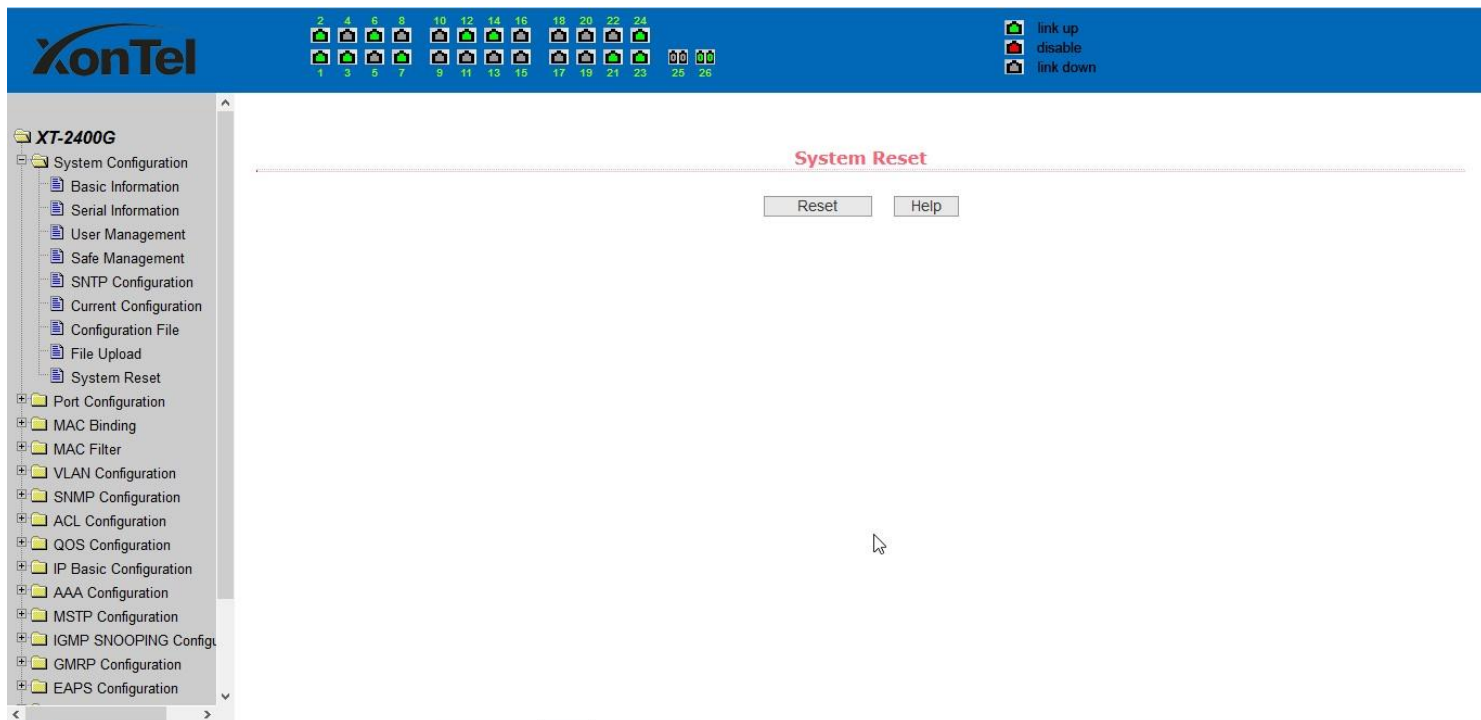


Figure16 System reset page

## 4 、Port Configuration

### ( 1 ) Port configuration / port -display page

Figure 17 is the port configuration / port -display page. Users can enable or disable the port to the page, set the port speed, or View all ports of the basic information.

To set a specific port, users need to select the appropriate port name on port drop-down menu,. The default port status is up, can select the drop-down menu -down to disable the port. Users can also choose to set the speed of the drop-down menu to set the speed of the port, such as the mandatory half-duplex port 10M (half-10) and so on. On this page the user can view all ports other basic information.

**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-100 Mbps	Access	1
ge1/3	Up	Up	Full-100 Mbps	Access	1
ge1/4	Up	Down	Unknown	Access	1
ge1/5	Up	Down	Unknown	Access	1
ge1/6	Up	Up	Full-1000 Mbps	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
ge1/11	Up	Down	Unknown	Access	1
ge1/12	Up	Up	Full-100 Mbps	Access	1

Figure 17 port configuration and port - display page

## ( 2 ) Port Statistics Page

Figure 18 is the port statistics information page. To view a particular port, users need to select the appropriate port name in the port drop-down menu. Users can view the statistics information of send and receive packets on this page.

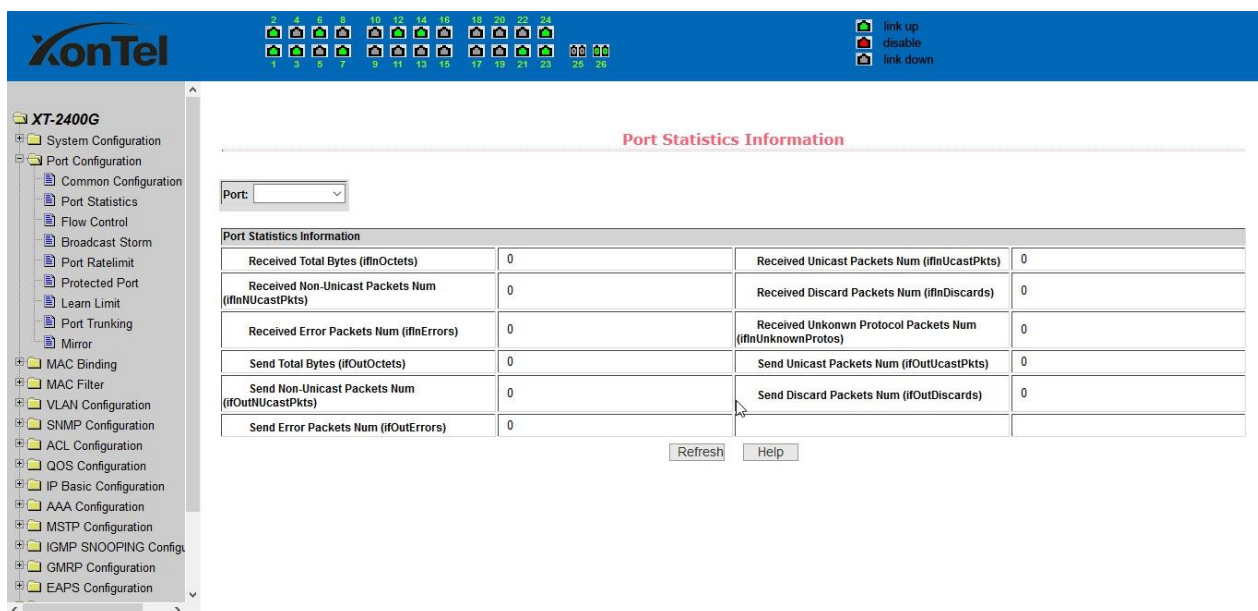


Figure 18 Port Statistics Page

## ( 3 ) Flow control page

Figure 19 is the flow control page. Users can enable and disable each port's send and receive flow control through this page.

Flow control by sending the side of the drop-down on or off to open or close the sending side of flow control, flow control through the receiving side of the drop-down on or off to open or close the receiver-side flow control, while on and off also shows the port to send side and receiving-side flow control is turned on or off.

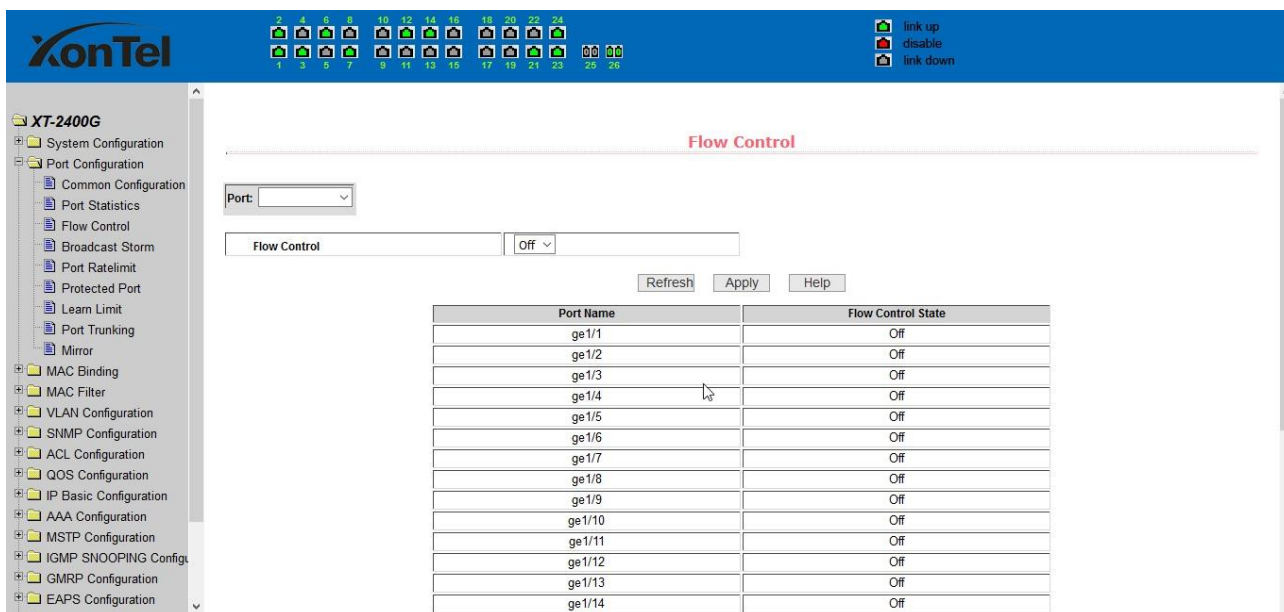


Figure 19 Flow control page

## ( 4 ) Broadcast storm control page

Figure 20 is the Broadcast Storm Control page. This page is used to do the suppression for configure port broadcast packets, multicast packets and DLF packet.

From the Port drop-down bar select to configure ports. Through the on and off key to open and close the port broadcast suppression, multicast, DLF inhibition and suppression. Inhibition rate is used to configure the port inhibition speed, range 1-1024000, unit kbps. The inhibition rate of the same port broadcast suppression, multicast and DLF inhibition is the same.

**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)

Refresh Apply Help

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
ge1/11	Off	64	Off	64	Off	64
ge1/12	Off	64	Off	64	Off	64

Figure 20 Broadcast Storm control Page



## ( 5 ) Port speed limits page

Figure 21 is the port speed- limit page. This page is used to configure the port send and receive rate

From the Port drop-down bar select the configure ports. Bandwidth control of the send data packets is used to configure and display the bandwidth control it, the range is 1-1024000, unit kbits, enter into force after the key press applications. If the port is not configured bandwidth control, shown as off. Cancel button is used to cancel the corresponding data packet to send bandwidth control. Receiving data packets is used to configure and display the bandwidth control of receive data packets control, the range is 1-1024000, unit kbits, enter into force after the key press applications. If the port is not configured bandwidth control, shown as off. Cancel button is used to cancel the corresponding receiving data packets bandwidth control

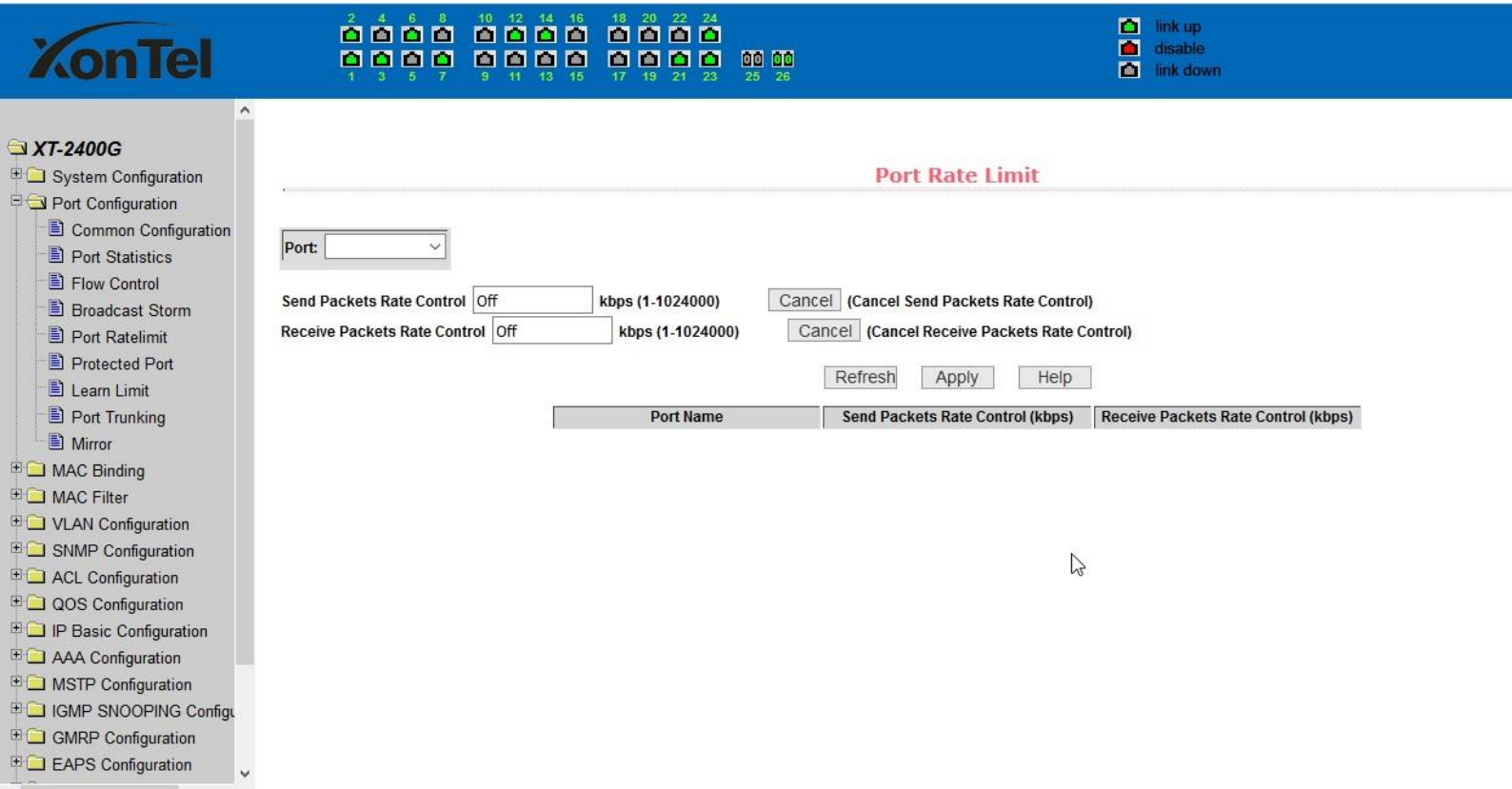


Figure 21 Port speed limit page

### ( 6 ) Port protection page

Figure 22 is the Port protection page. This page is used to configure the port for the protection port.

If the port is configured as a protected port, the ports can not exchange the data with each other, protected port only with non-protected port for data exchange.

**Protected Port**

	Port Name	Is Protected Port
<input type="checkbox"/>	ge1/1	No
<input type="checkbox"/>	ge1/2	No
<input type="checkbox"/>	ge1/3	No
<input type="checkbox"/>	ge1/4	No
<input type="checkbox"/>	ge1/5	No
<input type="checkbox"/>	ge1/6	No
<input type="checkbox"/>	ge1/7	No
<input type="checkbox"/>	ge1/8	No
<input type="checkbox"/>	ge1/9	No
<input type="checkbox"/>	ge1/10	No
<input type="checkbox"/>	ge1/11	No
<input type="checkbox"/>	ge1/12	No
<input type="checkbox"/>	ge1/13	No
<input type="checkbox"/>	ge1/14	No
<input type="checkbox"/>	ge1/15	No
<input type="checkbox"/>	ge1/16	No
<input type="checkbox"/>	ge1/17	No
<input type="checkbox"/>	ge1/18	No

Figure 22 protected port page

## ( 7 ) Port Learning restrain page

Figure 23 is the port learning restrain page. This page used to restrict the port can learn of the MAC address of the number, range is 0-8191. The default value is 8191, also is the maximum that the port is not configured the learning restrain

**Learn Limit**

Port:

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

Refresh Apply Cancel Limit Help

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
ge1/11	8191
ge1/12	8191
ge1/13	8191
ge1/14	8191
ge1/15	8191

Figure 23 Port Learning restrain page



### ( 8 ) Port Trunking configuration page

Figure 24 is the port trunking configuration page, this page allows the user to configure the port trunking. This page consists of four parts: port trunking ID selection, port trunking method selection, configurable ports and group members port.

To create or modify the port trunking, the user need to select a port trunking ID, port trunking ID from 1 to 3. The user clicks the list box the appropriate port trunking ID, the port trunking of information displayed in the group port. To create a Trunk group, select the appropriate ID in the port trunking ID, click the button "Trunk ID Settings." To set the port trunking method, select one port trunking method, click the button "polymerization Settings." To increase the trunking ports, the port can be configured to select the trunking port in the configurable, click on "members of the port =" "key. Aggregation from the existing port to remove a port group member ports in the trunking port selected, click on "non-member port" = "key. To delete the entire TRUNK group, then click the "Delete trunk group" button.

In page configuring process, at least one Trunk has been established then polymerization settings can take effect; configured Trunking method is also applied to all on the Trunk groups; in that already exist on the Trunk can add or remove Port members ; in the absence of the port members situation can delete a Trunk Group.

Switch provides three kinds of port trunking methods: Based on the source MAC address, based on the purpose MAC address, based on the source and purpose MAC addresses.

Switch maximum support 3 groups port trunking, can be configured to a maximum of three Trunk Group, Trunk 1 and Trunk 2 can not trucking Gigabit ports, and each group can be aggregated up to the same four attributes port. Trunk3 only be aggregated Gigabit ports, and up to 2 Gigabit ports can be aggregated. Port aggregation method is common to all of the Trunk.

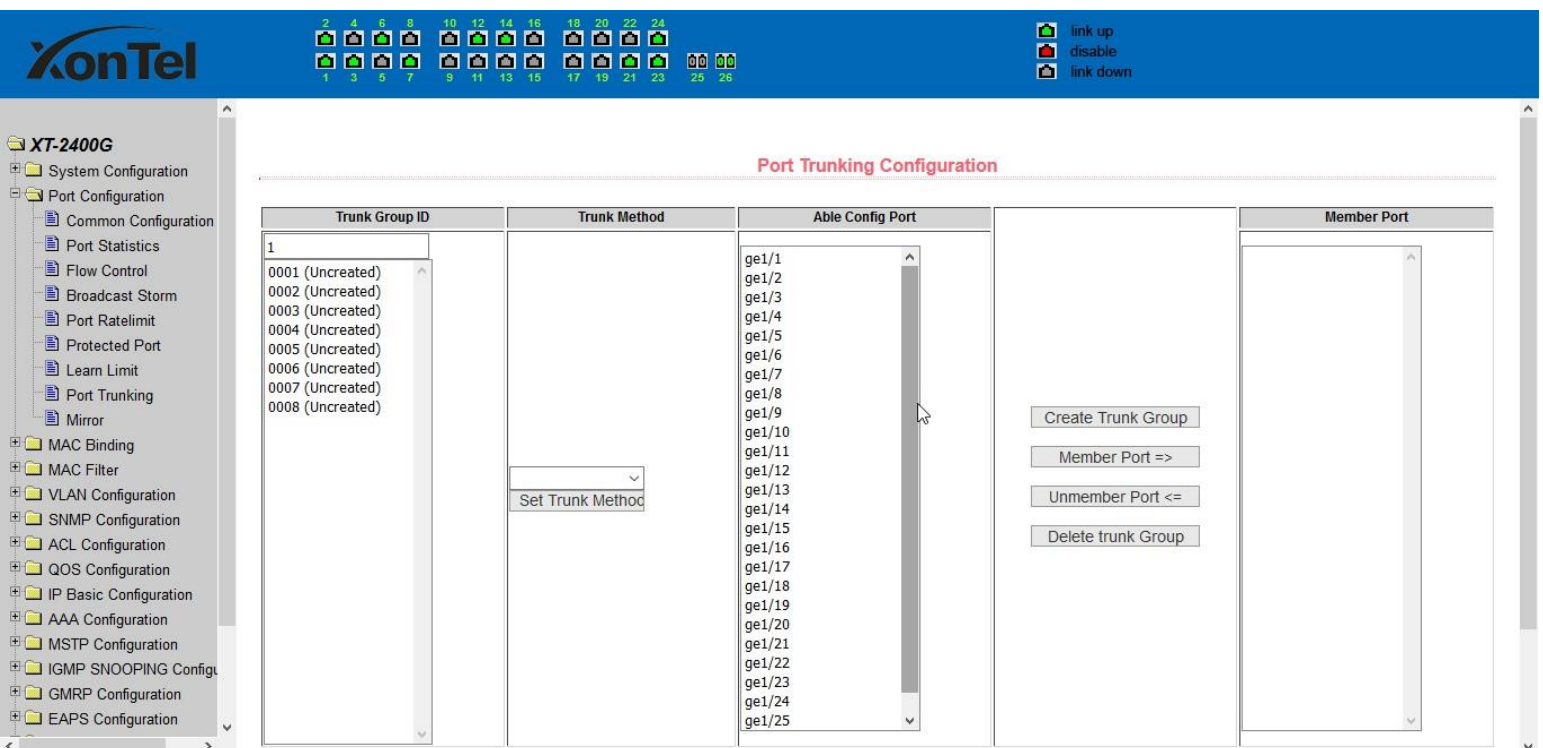


Figure 24 Port Trunking configuration page

### ( 9 ) Port mirroring configuration page

Figure 25 is the port mirroring configuration page .the page allows users to configure port mirroring. Port mirroring through the mirror port to monitor the data packets of being mirrored output port and the data packets of being mirrored input port mirroring Port can only choose one, being mirrored output port and being mirrored input port can select multiple. This page consists of four components: monitor port, configurable port, monitoring direction and mirror configuration information. When you start to configure a mirror port, firstly configured mirroring port from monitor ports, mirror ports can only have one, and then select the mirror port from the configurable port, select the monitor direction, and press the application key to entry into force, the results is displayed in the mirrored configuration information.

When choose the receive in direction of monitor, said monitor data packets received, transmit, said monitor data packets sent, both that monitor all data sent and received packets, not receive to cancel monitoring received data packets, not transmit to cancel monitor send data packets, neither cancels monitor data packets received and sent, that is canceling monitor port.

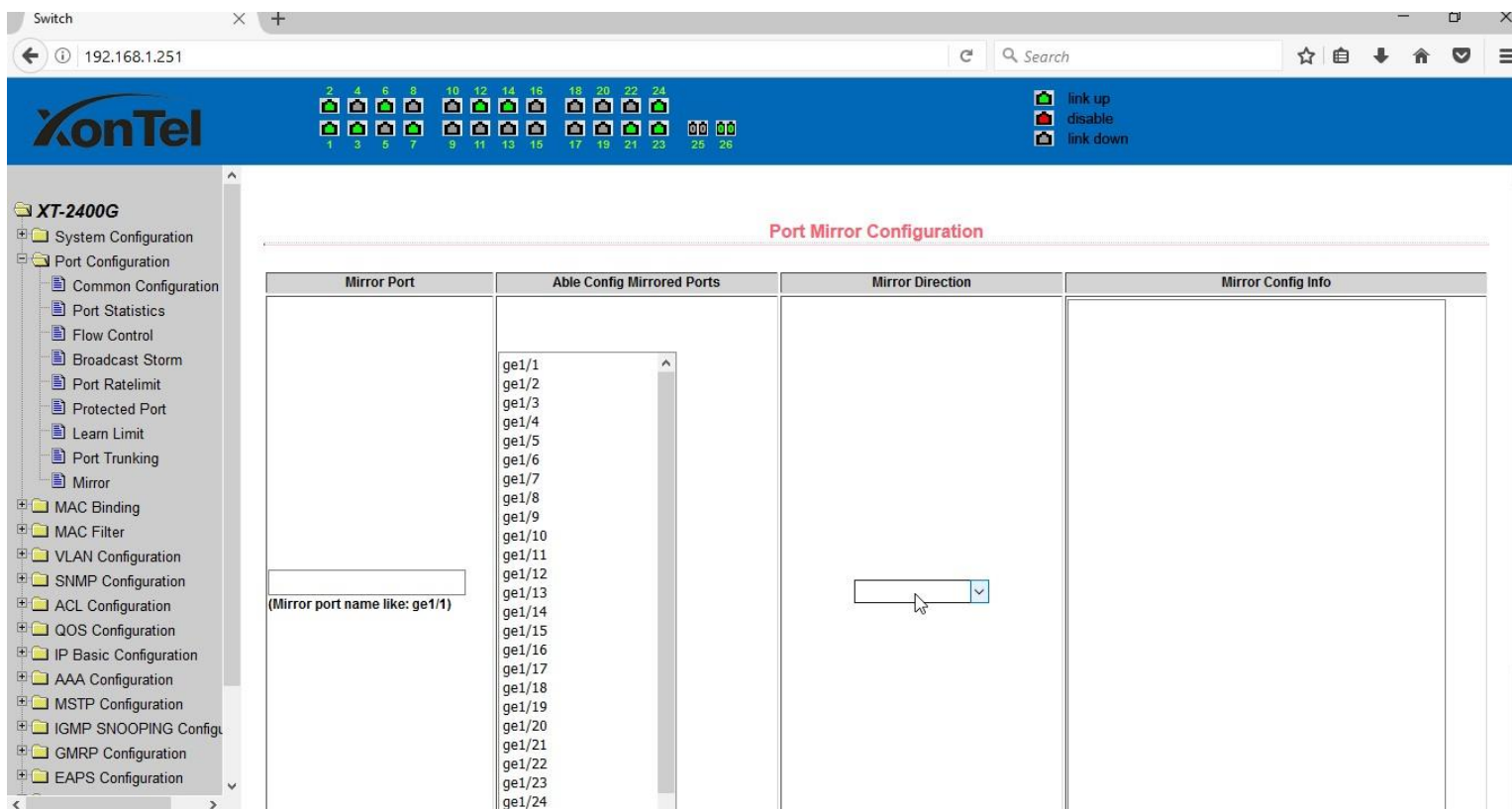


Figure 25 Port mirroring configuration page

## 5 、MAC binding

### ( 1 ) MAC binding configuration page

Figure 26 is the MAC binding configuration page. This page is used to achieve the port and MAC address binding.

MAC entries on the page is used to enter the MAC address binding, VLAN ID entry is used to enter the MAC address of VLAN.

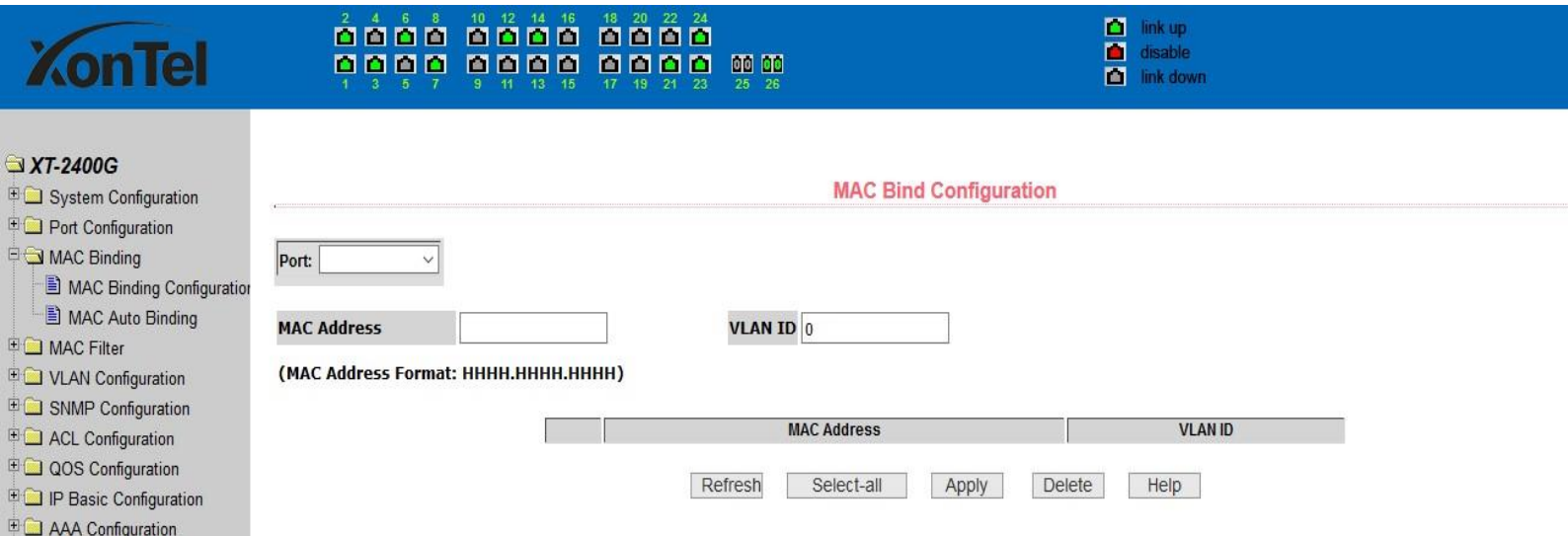


Figure 26 the MAC binding configuration page

### ( 2 ) MAC binding automatic conversion page

Figure 27 is the MAC binding automatic conversion page. This page is used to achieve the port MAC address auto-binding. Shows the hardware switch on the lay2 the exist port dynamic MAC address and affiliated VLAN. Can choose one of the entry and convert it into static binding.

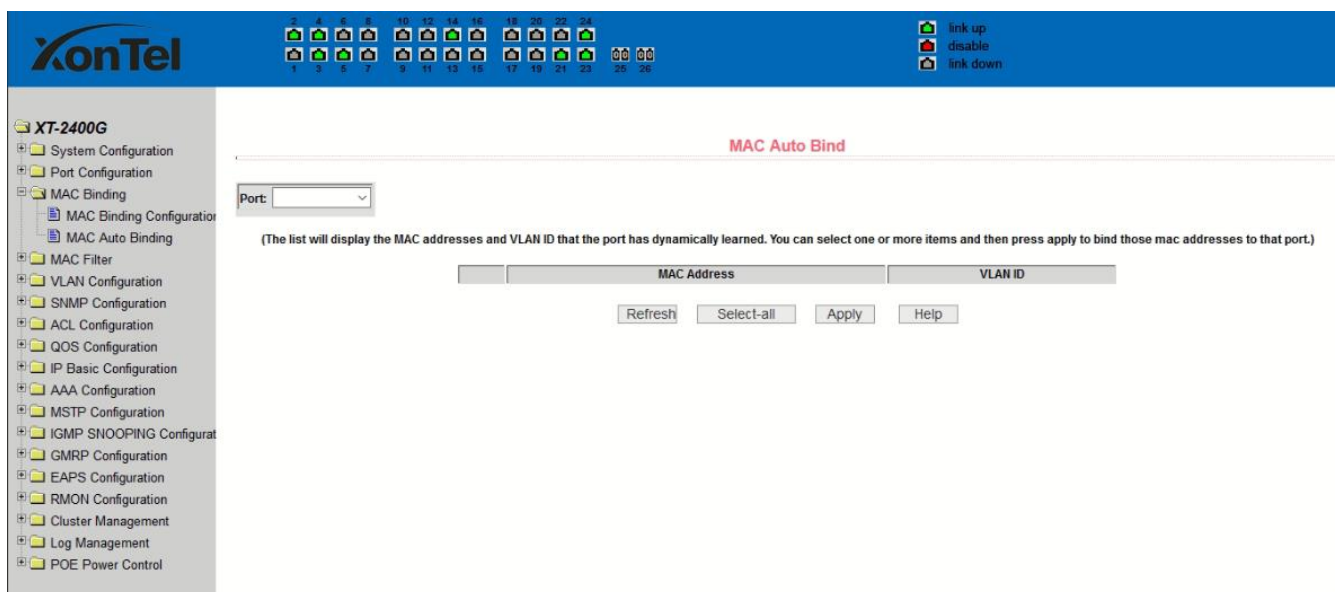


Figure 27 the MAC binding automatic conversion page

## 6 · MAC filtering

### ( 1 ) MAC filtering configuration page

Figure 28 is the MAC filtering configuration page. This page is used to configure the ports on the MAC address filtering.

MAC entries on the page is used to enter the MAC address filtering, VLAN ID entry is used to enter the MAC address affiliated VLAN.

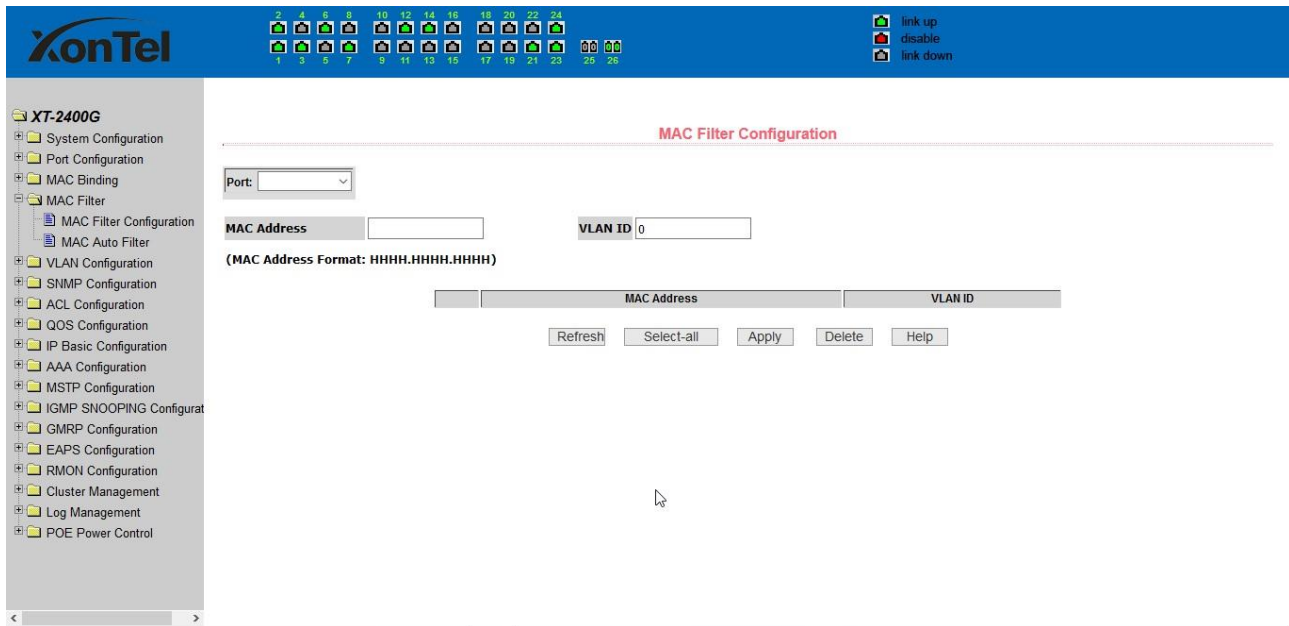


Figure 28 the MAC filtering configuration page

### ( 2 ) MAC filtering automatic conversion page

Figure 29 is the MAC filtering automatic conversion page. This page is used to achieve the port MAC address auto-binding.

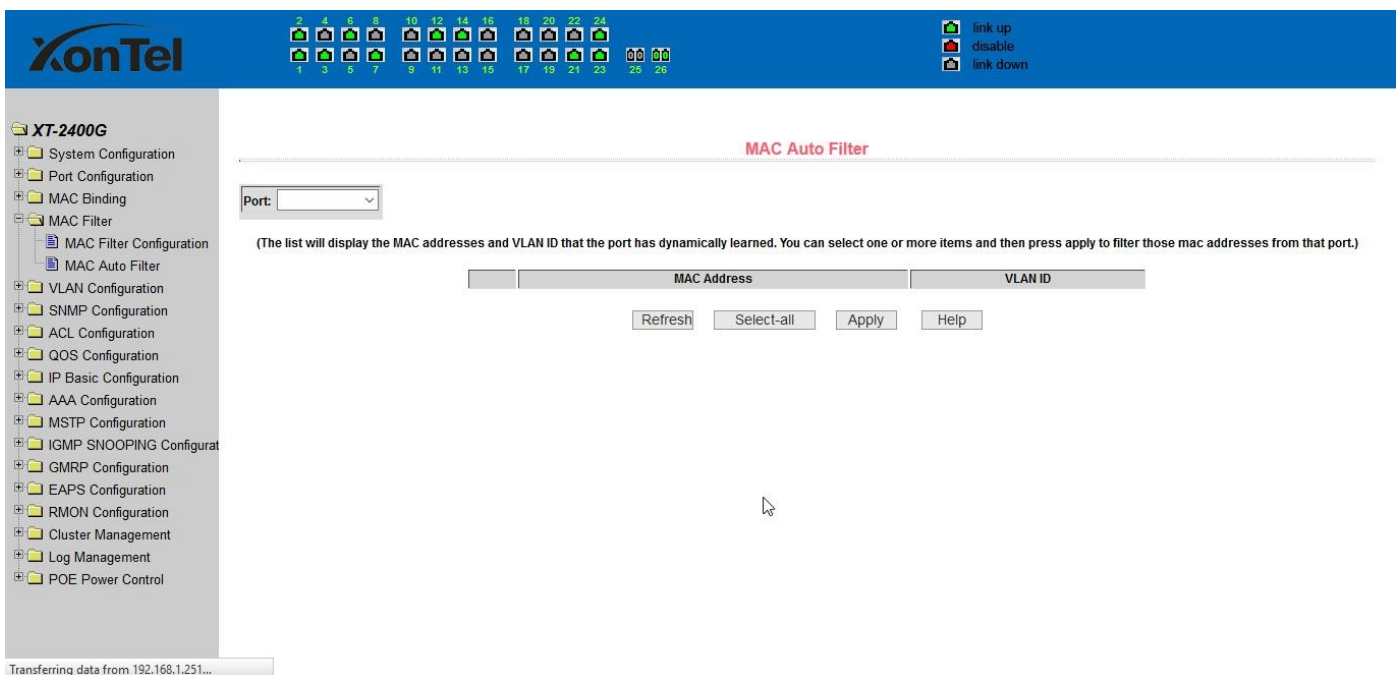


Figure 29 the MAC filtering automatic conversion page

## 7 · VLAN Configuration

### ( 1 ) VLAN information page

Figure 30 shows the current VLAN information page. This page is read-only page displays the current VLAN configuration information, including the VID, state and port members. Select VLAN from the drop-down VID, shows the port information of the Port VLAN members.

A port may not be a member of VLAN, which can be VLAN-tagged or untagged members. Please see the following info:

- t Tagged the port is the VLAN tagged member
- u Untagged the port is the VLAN untagged member

**XT-2400G**

System Configuration  
Port Configuration  
MAC Binding  
MAC Filter  
VLAN Configuration  
VLAN Information  
VLAN Configuration  
VLAN Port Configuration  
SNMP Configuration  
ACL Configuration  
QOS Configuration  
IP Basic Configuration  
AAA Configuration  
MSTP Configuration  
IGMP SNOOPING Configurat  
GMRP Configuration  
EAPS Configuration  
RMON Configuration  
Cluster Management  
Log Management  
POE Power Control

link up  
disable  
link down

### 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)

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 [u]ge1/11 [u]ge1/12 [u]ge1/13 [u]ge1/14 [u]ge1/15 [u]ge1/16 [u]ge1/17 [u]ge1/18 [u]ge1/19 [u]ge1/20 [u]ge1/21 [u]ge1/22 [u]ge1/23 [u]ge1/24 [u]ge1/25 [u]ge1/26

Refresh Help

Figure 30 VLAN information page



## ( 2 ) Static VLAN configuration page

Figure 31 is the static VLAN configuration page that allows users to create VLAN.

If you want to create a new VLAN, the user input VID on activity line, ranging from 2 to 4094. VLAN name is generated depend on VLAN ID and can not be modified. Click Apply button, then the list box displays the user-created VLAN's VID and VLAN name. Switch by default created VLAN1, and VLAN1 can not be removed

If you want to delete a VLAN, the user need to click the appropriate VLAN of the list box. The VLAN will be displayed in the activity line, click the Remove (Delete) key to delete the VLAN, the same time, the information of the VLAN to remove from the list box.

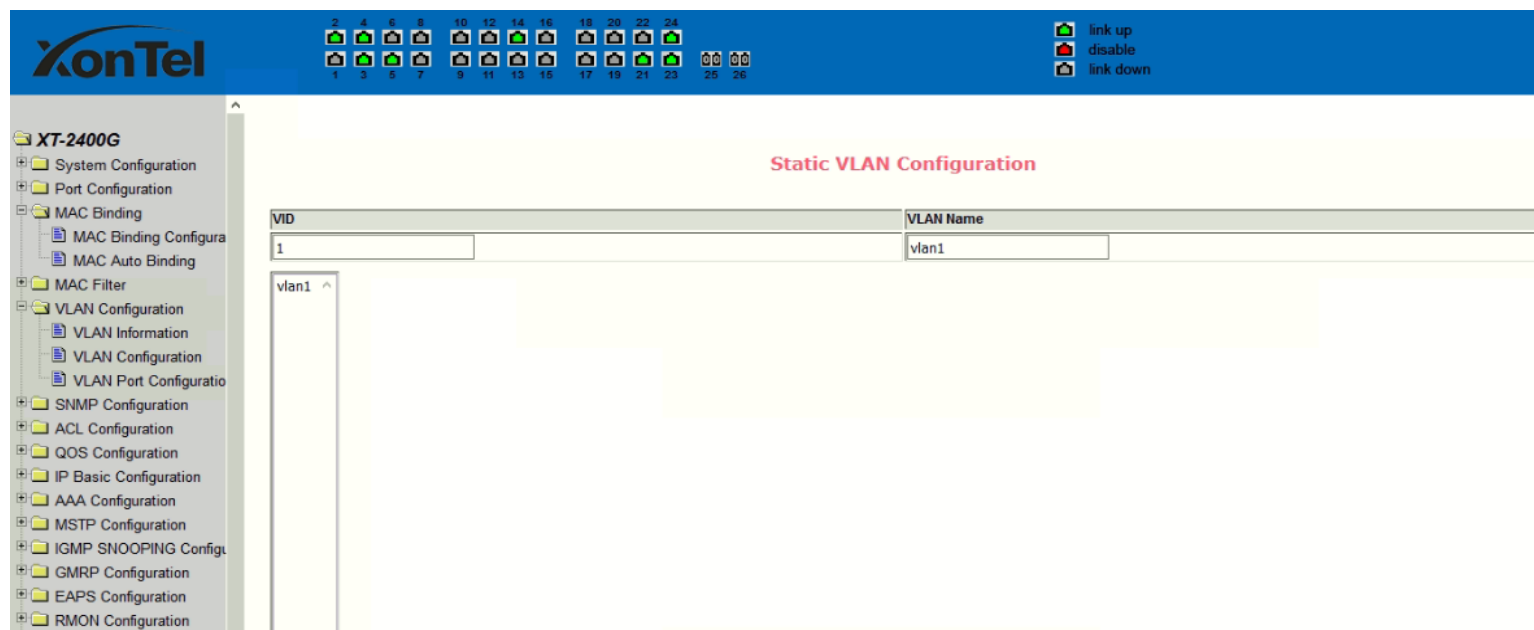


Figure 31 the static VLAN configuration page

### ( 3 ) VLAN port configuration page

Figure 32 is a VLAN port configuration page, which is used to configure the VLAN port configuration and display results. This page mainly consists of eight parts: port, mode, all current VLAN, port-owned VLAN, key "default VLAN =>", "tagged =>", "untagged =>" and "non-members" =.

Port is defined a designated port that will configure the VLAN

Mode Access designated the VLAN mode as the ACCESS mode, under this mode, the port default VLAN is the untagged member of VLAN1, the port's default VLAN is 1. Hybrid specified port VLAN mode HYBRID model, in this mode, the port default VLAN is the untagged member of VLAN1, the port's default VLAN is 1. Trunk specified port VLAN mode is Trunk mode, in which the port VLAN mode, the default is VLAN1 a tagged member of the port's default VLAN is 1.

All current VLAN that has been created VLAN, also it's can be configured VLAN, the user from the list select VLAN, can be multiple-choice.

VLAN Port-owned shows the results of VLAN port configuration, [p] indicates that the port VLAN is the default VLAN, [t] that the port is a VLAN tag members, [u] that the port is not tagged VLAN member. When you remove VLAN, the user from the list, select the VLAN, can be multiple-choice.

Button "default VLAN =>" to configure port the default VLAN, selected one VLAN from the current all the VLAN.

Button "tagged =>" Configured port is designated as a tagged member of VLAN, selected one or more VLAN from the current all VLAN.

Button "untagged =>" Configure VLAN port is a designated member of the untagged, selected one or more VLAN from the current all VLAN.

Button "non-members <=" to delete the port from the specified one or more of the VLAN ,no longer a member of the VLAN, from the port affiliated VLAN to selected one or more VLAN.

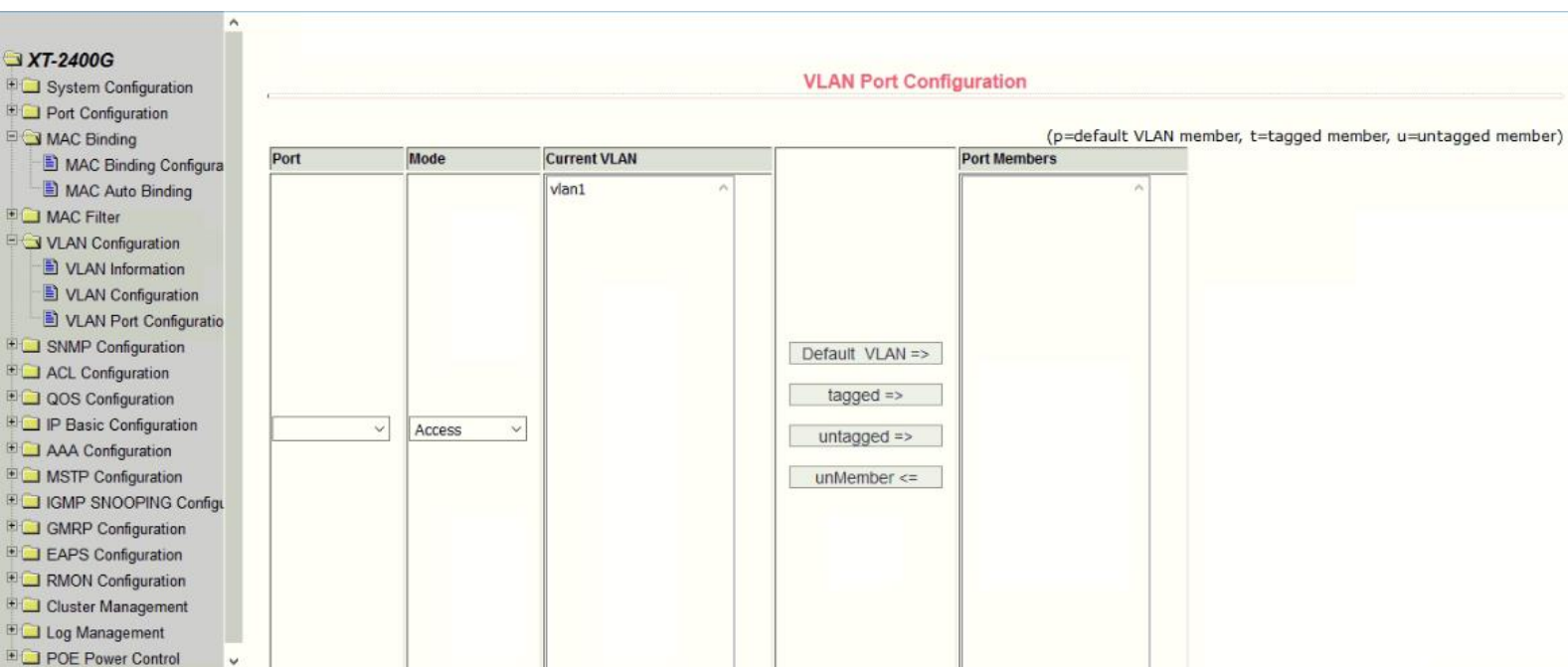


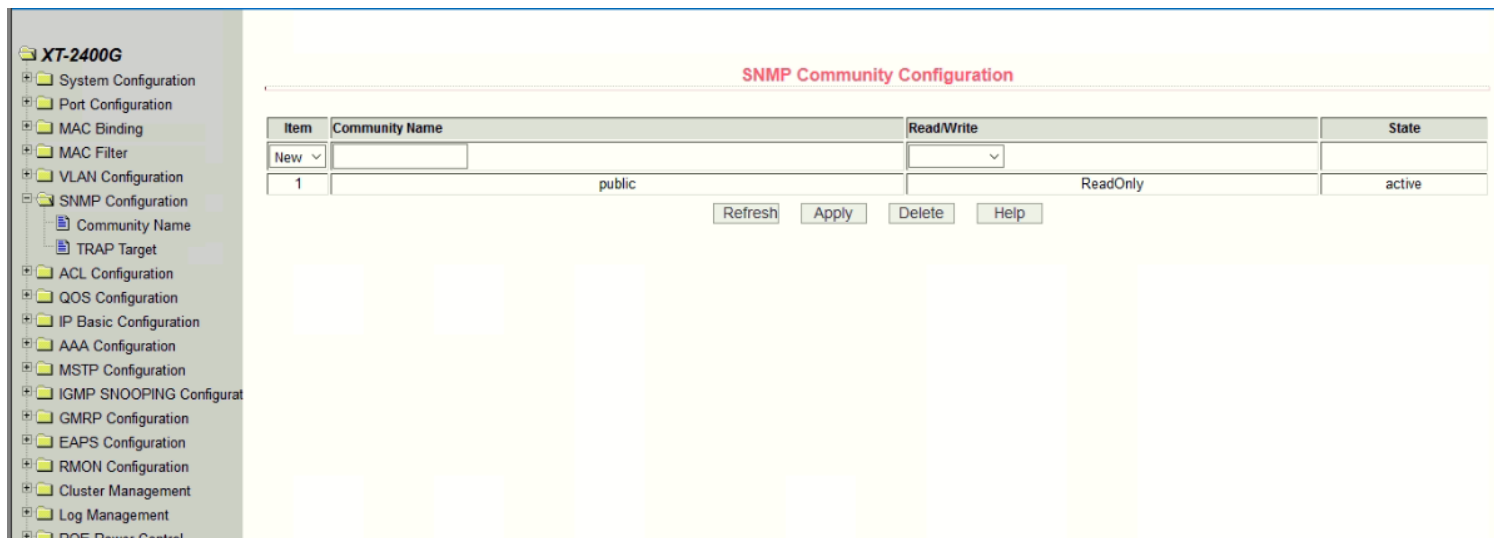
Figure 32 The VLAN port configuration page

## 8 · SNMP Configuration

### ( 1 ) SNMP share body configuration page

Figure 33 is a shared body of SNMP configuration page that allows users to configure the switch common body's name and read and write access, a total of 8 entries can be configured

By default, the switch there is a share name as named public, the common body is Read only access. With this correspondence, the activities of this page is only one entry, shared body names are public and access is read-only access. When the switch through SNMP for network management, you need to configure a read-write permissions to the shared body.



The screenshot shows the 'SNMP Community Configuration' page in the XonTel web interface. On the left is a navigation tree for the 'XT-2400G' device, with 'SNMP Configuration' expanded to show 'Community Name' and 'TRAP Target'. The main area has a title bar 'SNMP Community Configuration' and a table with columns: Item, Community Name, Read/Write, and State. The table contains one entry with Item '1', Community Name 'public', Read/Write 'ReadOnly', and State 'active'. Above the table is a 'New' button and a dropdown menu. Below the table are 'Refresh', 'Apply', 'Delete', and 'Help' buttons.

Item	Community Name	Read/Write	State
1	public	ReadOnly	active

Figure 33 SNMP Share body configuration page



## ( 2 ) TRAP target configuration page

Figure 34 is the TRAP target configuration page that allows users to configure the workstation to receive TRAP messages as well as the IP address of TRAP protocol packets of some of the parameters.

In the configuration entry, the name used to enter the TRAP name, IP address used to enter the target address, SNMP version used to select the version of the TRAP packet, if you set successful, it will show in the state to active. If the configuration was successful, SNMP TRAP functions will take effects, in the event of link up or link down, the switch will automatically send a TRAP packet to the target address.

Item	Name	Transmit IP Address	SNMP Version	State
New				

Refresh Apply Delete Help

Figure 34 the TRAP target configuration page

## 9 · ACL Configuration

### ( 1 ) IP Standard ACL configuration page

Figure 35 is the IP standard ACL configuration page. Users can through this page to build ACL standard IP-rule base. User can select an ACL group number, in the group to create one or more rules. In a rule can match only the source IP address field (with mask). The standard IP rules to control the source IP address packet forwarding.

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
-----------	-------------	-------------------	-----------------

Refresh Select-all Add Delete Help

Figure 35 The IP standard ACL configuration page

Users to configure the rules, the source IP address must be in with a mask, the rule can match the collection of IP addresses. The address mask is use anti-code , if the rule were to match the IP address range 192.168.0.0 to 192.168.0.255, then the IP address can be 192.168.0.1, and its mask of 0.0.0.255.

Users to configure the rules, each rule must have a filter mode: allow or deny.

The user to create a rule in the group, the system will automatically give the rule a rule number, when to delete a rule in the group 1 rules, other rules remain unchanged, and the system will automatically give the rule a rule group sort. If the user wants to delete the entire rule set, you can first select all, then click the delete key.

## ( 2 ) IP Extended ACL configuration page

Figure 36 is the IP extended ACL configuration page. The extended IP group is an extension of the standard IP rules. Control the packet forwarding via source IP, Destination IP, IP protocol type and service port.

**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
<input type="button" value="Refresh"/> <input type="button" value="Select-all"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>									

Figure 36 the IP Extended ACL configuration page

### ( 3 ) MAC IP ACL configuration page

Figure 37 is the MAC IP ACL configuration page. IP MAC group can be the IP packet source and destination MAC address and source and destination IP address control.

Figure 37 The MAC IP ACL configuration page

### ( 4 ) MAC ARP ACL configuration page

Figure 38 is the MAC ARP ACL configuration page. ARP group can be the type of the operation of the ARP packet, the sender MAC and the sender IP control.

Figure 38 The MAC ARP ACL configuration page

### ( 5 ) ACL information page

Figure 39 is the ACL information page, which displays the current ACL rules configured in all the information.

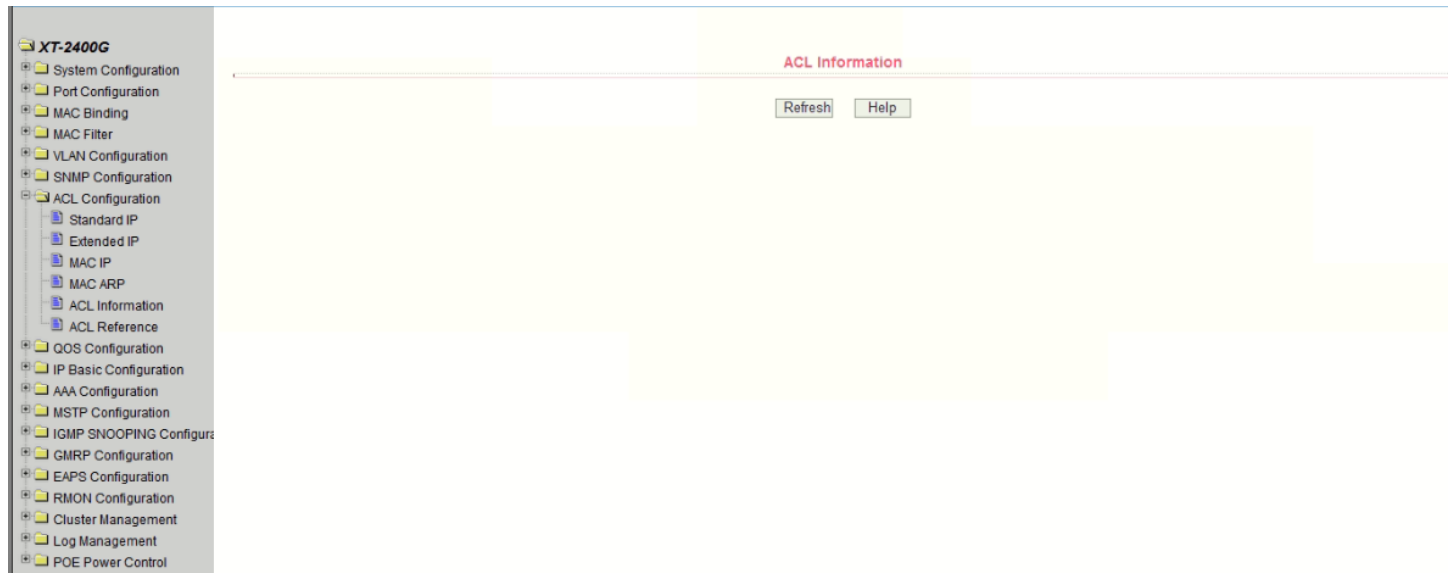


Figure 39 ACL resource library information page

### ( 6 ) ACL Reference

Figure 40 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.

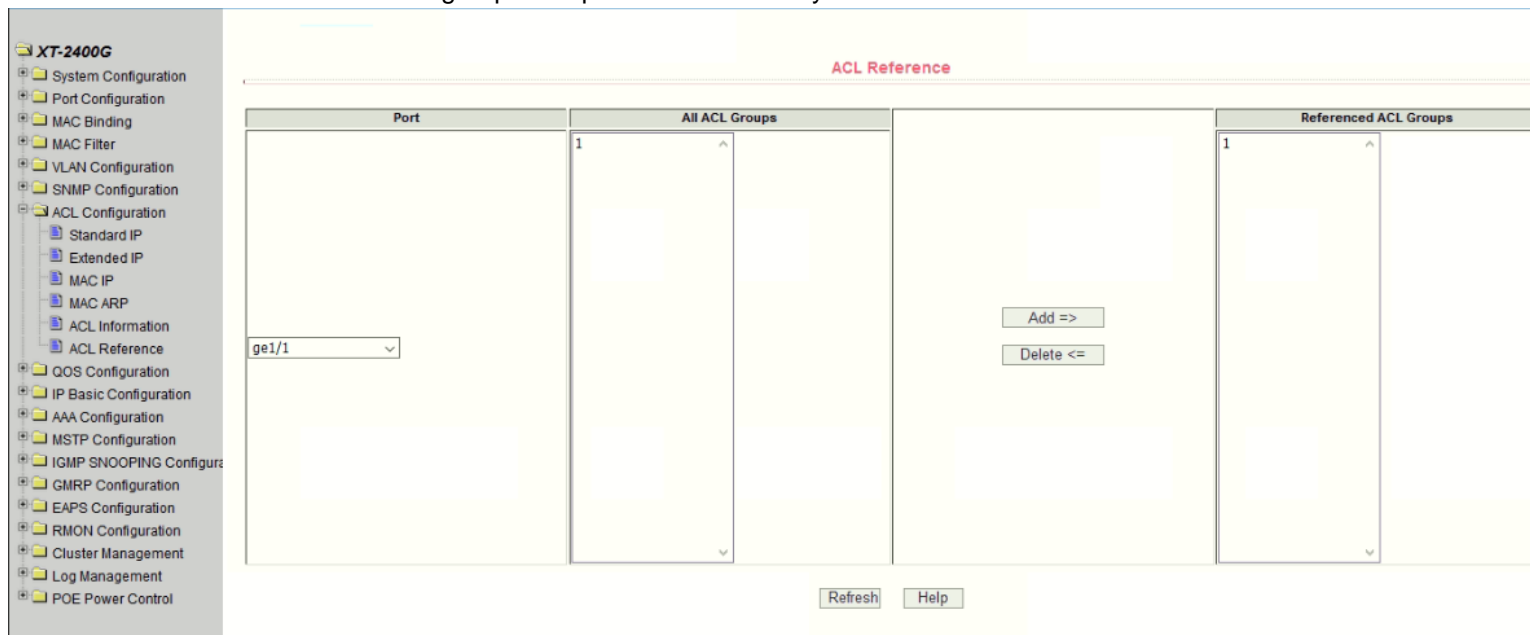


Figure 40 ACL Reference page

## 10 · QoS Configuration

### ( 1 ) QoS Apply Configuration Page

Figure 41 is a QoS Apply configuration page.

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
ge1/11	NO QOS	0
ge1/12	NO QOS	0
ge1/13	NO QOS	0

Figure 41 QoS Apply configuration page

### ( 2 ) QoS Schedule Configuration Page

Figure 42 is a QoS Schedule configuration page.

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
ge1/11	WRR	1	2	4	8	16	32	64	127
ge1/12	WRR	1	2	4	8	16	32	64	127

Figure 42 QoS Schedule configuration page

## 11 · IP Basic Configuration

### ( 1 ) VLAN Interface Configuration Page

Figure 43 is a VLAN interface configuration page, users can configure the VLAN interface through this page, delete VLAN interfaces, configure the interface IP address, remove the interface IP address, and view interface information. VLAN already exists can only be set when the interface can only be configured on the interface set interface address.

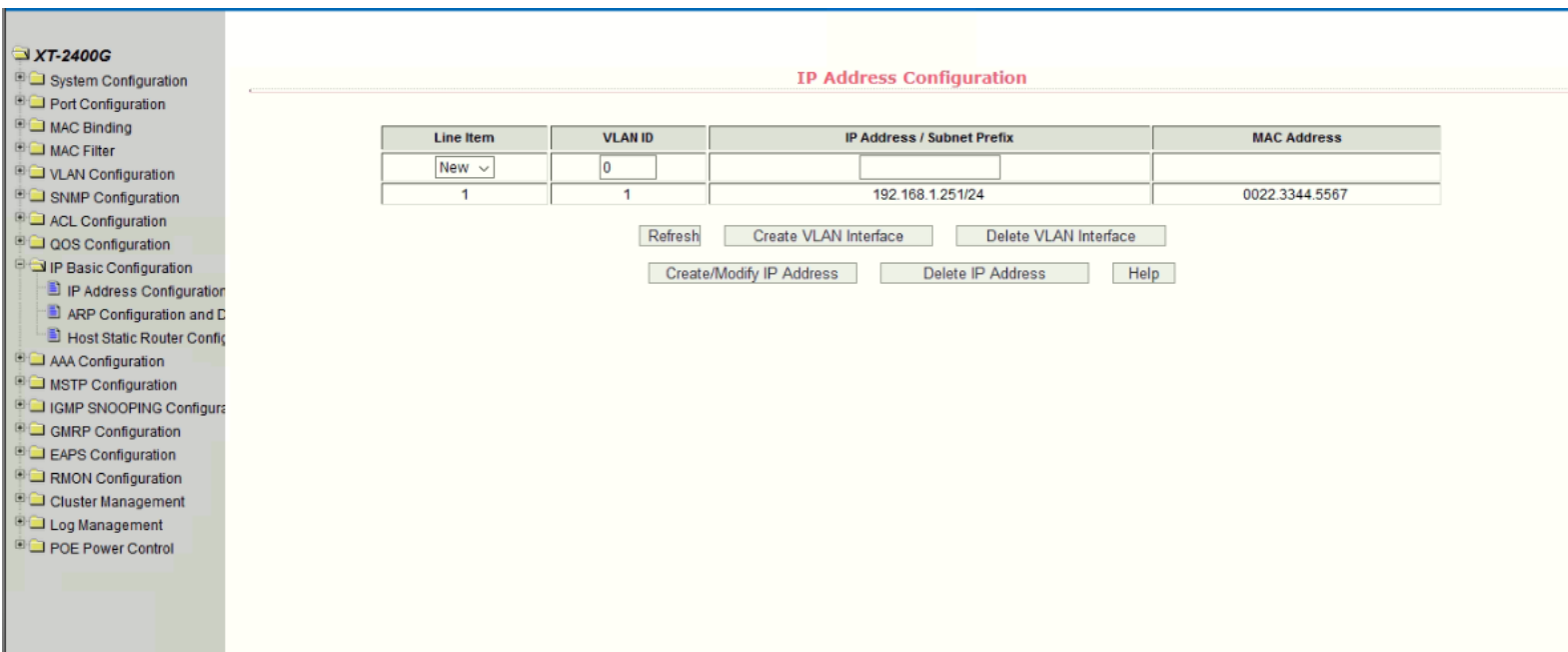


Figure 43 VLAN interface configuration page

XonTel switch in the default state have a VLAN1 interface, the interface can not be deleted. One can only configure a VLAN interface.

### ( 2 ) ARP configuration and display page

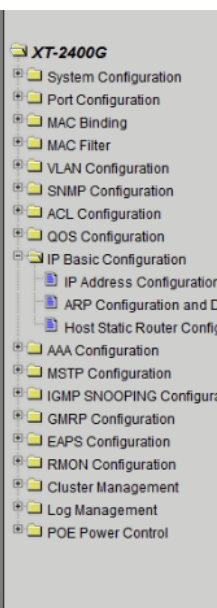
Figure 44 is the ARP configuration and display page, this page can display all of the information of the ARP table switch, while users can configure a static ARP entries on this page, delete ARP entries, and revised the dynamic ARP table entry to a static ARP table entry.

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

When a user delete an ARP entry, you can choose to delete an IP-ARP table entry, remove a segment of the ARP table entry, delete all of the ARP table entry, delete all dynamic ARP table entries and delete all of the static ARP table entry. For the deletion of an IP-ARP table entries, or delete a segment of the ARP table entry required to enter in the input box, specify the IP address or IP network segment. Then click the Delete button

When dynamic ARP table entry was revised to a static ARP table entry, you can choose to a particular network segment or all of the dynamic ARP table entry was revised to a static ARP table entry. For the situation to a network segment is required in the input box, enter the specified network segment. And then click Apply button.





### ARP Configure And Display

**Static ARP Item configuration:**  

IP Address	MAC Address
------------	-------------

Add

**Delete ARP Item:**  

ARP Item	IP Address (IP Network Segment)
----------	---------------------------------

Delete

**Change Dynamic ARP List Item into Static ARP List Item:**  

ARP List Item	IP Network Segment
---------------	--------------------

Apply

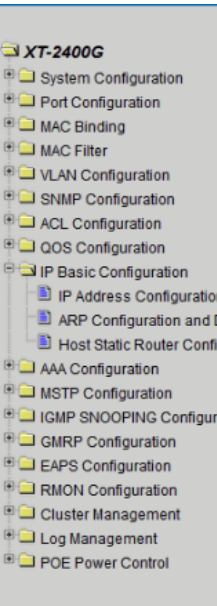
IP Address	MAC Address	Type
192.168.1.152	004f.4e62.994c	dynamic

Refresh Help

Figure 44 The ARP configuration and display page

### ( 3 ) Host Static Routing configuration page

Figure 45 is the host static route configuration page, the user can through this page to add, delete static routing switch hosts. By default, the XonTel XT-1600/XT-2400 switch is not configured to host a static route, the user can configure the default route through this page, that is the purpose of address / subnet prefix is 0.0.0.0 / 0 routing



### Host Static Route Configuration

Target Address/Subnet prefix	Next Hop
<input type="text"/>	<input type="text"/>

Item	Target Address/Subnet prefix	Next Hop	Distance	State

Refresh Apply Delete Help

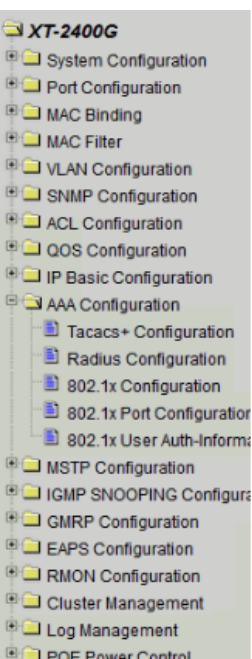
Figure 45 the host static route configuration page

## 12 · Certification. Authorization. Accounting (AAA) configuration

### ( 1 ) Tacacs+configuration page

Figure 46 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	

Figure 46 Tacacs+ configuration page



## ( 2 ) Radius Configuration Page

- Figure 47 is the Radius configuration page, users can configure with the Radius-related information, you can set information includes:
  1. Be sure to set the Radius server's IP address before do the authentication and accounting in this field,
  2. Optional Radius server IP address, if there is spare Radius server can set this field.
  3. Authentication UDP port, the default value is 1812, the user generally do not need to modify this field.
  4. Whether to activate the, the default is to start, and when you do authentication and accounting in general to start charging.
  5. Accounting UDP port, the default value is 1813.
  6. Shared secret key is used to setting the shared encryption password between the switch and the Radius server, so be sure to set the authentication and accounting in this field, and with the same settings on the Radius server.
  7. Vendor information, the users typically do not need to modify this field.
  8. NAS ports, NAS port type, NAS type of service, these three values do not change in general.
  9. Whether to on or off the roaming feature of Radius.

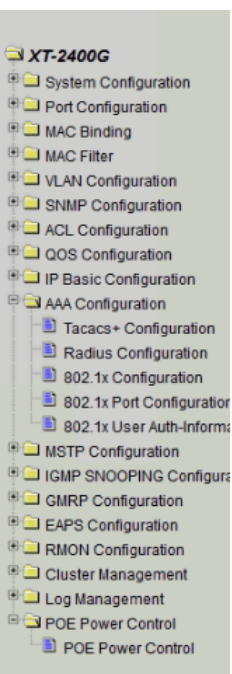
Radius Configuration	
Primary Server	0.0.0.0
Option Server	0.0.0.0
UDP Port	1812
Accounting	Enable ▾
Accounting UDP Port	1813
Shared Key	
Vendor	
NAS Port	50003
NAS Port Type	15
NAS Service Type	2
Roaming	Disable ▾

Refresh Apply Help

Figure 47 the Radius configuration page

### ( 3 ) 802.1x Configuration Page

- Figure 48 is the 802.1x configuration page, users can configure 802.1x related information on this page, including:
  - Whether to activate the 802.1x protocol, when doing authentication and accounting must be to start 802.1x protocol.
  - Switch is to adopt a common authentication method or the expansion of authentication.
  - Whether to open re-authentication function, the default is not open .when you do authentication and accounting based on the actual circumstances. Open the re-authentication feature will make users more reliable when using the authentication and accounting, but it will slightly increase the network traffic.
  - Setting re-certification time interval, only to re-open the case of authentication to be valid, the default is 3600 seconds, when you do authentication and accounting based on the actual situation to set the value, but the value is not too small.
  - Quiet Period Timer, users typically do not need to modify this field.
  - Tx-Period Timer, users typically do not need to modify this field.
  - Server timeout timer, users typically do not need to modify this field.
  - supplicant timeout timer, users typically do not need to modify this field.
  - Max Request number, users generally do not need to modify this field.
  - showing reauth Max size.
  - Client Version, the client version number.
  - Check Client, whether the certification passed then examine the client's regular flow of packets.



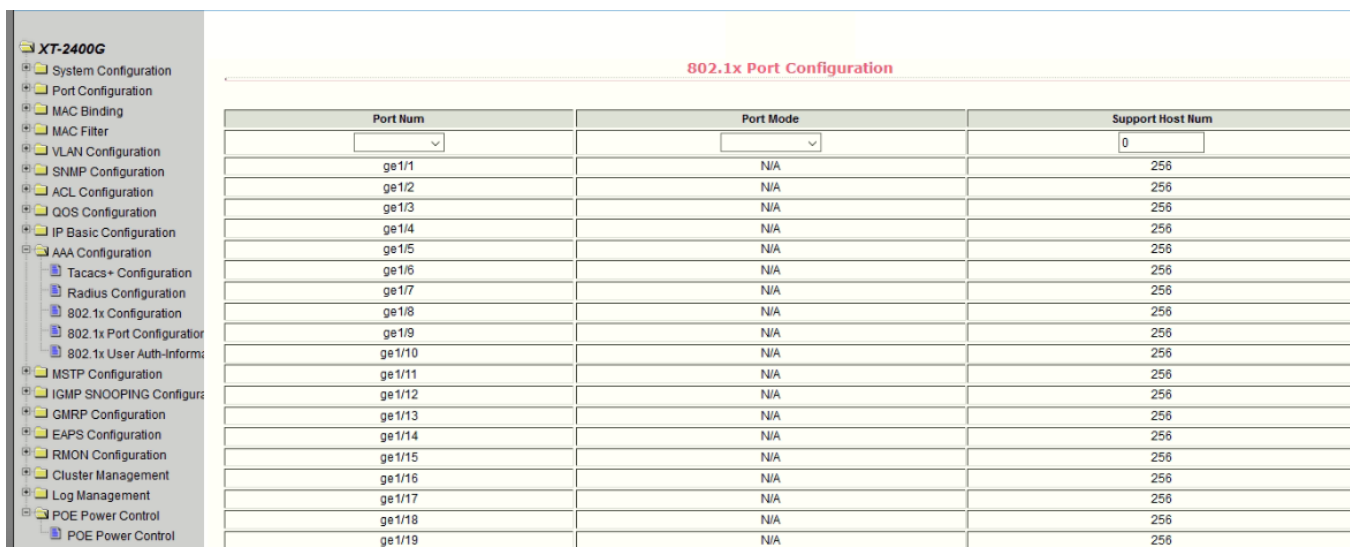
**802.1x Configuration**

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	▼

Figure 48 the 802.1x configuration page

#### ( 4 ) 802.1x port configuration page

Figure 49 is the 802.1x port configuration page, the user through this page to configure the support 802.1x port mode and hosts of the largest, at the same time you can view each port 802.1x configuration. 802.1x port model includes four types: N / A State, Auto state, Force-authorized state and Force-unauthorized state. When a port needs to do 802.1x Authentication need to set Auto state, if not do authentication to access the network, to set N / A state, the other two states are rarely used in practical applications



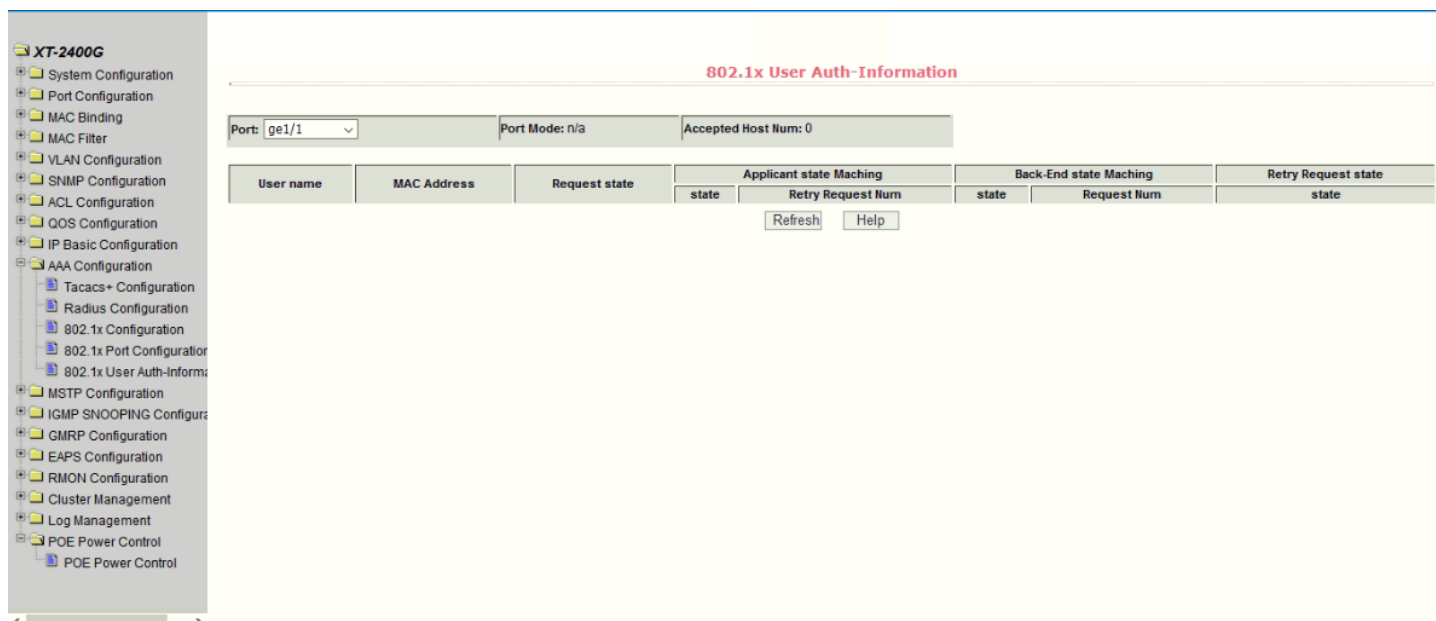
Port Num	Port Mode	Support Host Num
ge1/1	N/A	256
ge1/2	N/A	256
ge1/3	N/A	256
ge1/4	N/A	256
ge1/5	N/A	256
ge1/6	N/A	256
ge1/7	N/A	256
ge1/8	N/A	256
ge1/9	N/A	256
ge1/10	N/A	256
ge1/11	N/A	256
ge1/12	N/A	256
ge1/13	N/A	256
ge1/14	N/A	256
ge1/15	N/A	256
ge1/16	N/A	256
ge1/17	N/A	256
ge1/18	N/A	256
ge1/19	N/A	256

Figure 49 The 802.1x port configuration page

Doing 802.1x authentication, port access, the default maximum host number is 100, the user can modify this field, the biggest support to the 100.

#### (5) 802.1x user authentication information page

Figure 50 is 802.1x user authentication information page, the user can see through this page, under a certain port access for all users of the state information,



User name	MAC Address	Request state	Applicant state Matching		Back-End state Matching		Retry Request state
			state	Retry Request Num	state	Request Num	state
<div>Refresh Help</div>							

Figure 50 The 802.1x user authentication information page

## 13 · MSTP Configuration

### (1) MSTP configuration page

Figure 51 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 ▾
<input type="button" value="Refresh"/> <input type="button" value="Apply"/>	

Figure 51 MSTP configuration page

### (2) MSTP port configuration page

Figure 52 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	Disable ▾
Portfast bpdu-guard	Enable ▾
Root Guard	Disable ▾
Link-Type	Shared ▾
Priority	0
Path-Cost	0
Force-Version	STP ▾
<input type="button" value="Refresh"/> <input type="button" value="Apply"/>	

Figure 52 MSTP port configuration page

### (3) MSTP port information page

Figure 53 shows the MSTP port information page. You can view the port MSTP status on this page.

**XT-2400G**

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
- QOS Configuration
- IP Basic Configuration
- AAA Configuration
- MSTP Configuration
  - MSTP Configuration
  - Port Configuration
  - Port Information
- IGMP SNOOPING Configuration
- GMRP Configuration
- EAPS Configuration
- RMON Configuration
- Cluster Management
- Log Management
- POE Power Control

#### 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	20000	MSTP
ge1/2	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/3	Disable	Default	Default	Disable	Point-To-point	128	200000	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	20000	MSTP
ge1/7	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/8	Disable	Default	Default	Disable	Point-To-point	128	20000	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
ge1/11	Disable	Default	Default	Disable	Point-To-point	128	200000	MSTP
ge1/12	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/13	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/14	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/15	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/16	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/17	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/18	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/19	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/20	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

Figure 53 MSTP port information page

## 14、IGMP SNOOPING configuration

### (1) IGMP SNOOPING global configuration page

Figure 54 shows the IGMP snooping global configuration page. You can enable IGMP snooping on this page.

**XT-2400G**

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
- QOS Configuration
- IP Basic Configuration
- AAA Configuration
- MSTP Configuration
- IGMP SNOOPING Configuration
  - IGMP SNOOPING Configuration
  - Multicast Group Information
- GMRP Configuration
- EAPS Configuration
- RMON Configuration
- Cluster Management
- Log Management
- POE Power Control

#### IGMP SNOOPING Configuration

IGMP SNOOPING Disable

Figure 54 IGMP SNOOPING global configuration page

## (2) Multicast Group information page

Figure 55 shows the multicast group information page. You can view the igmp snooping multicast program information from this page.

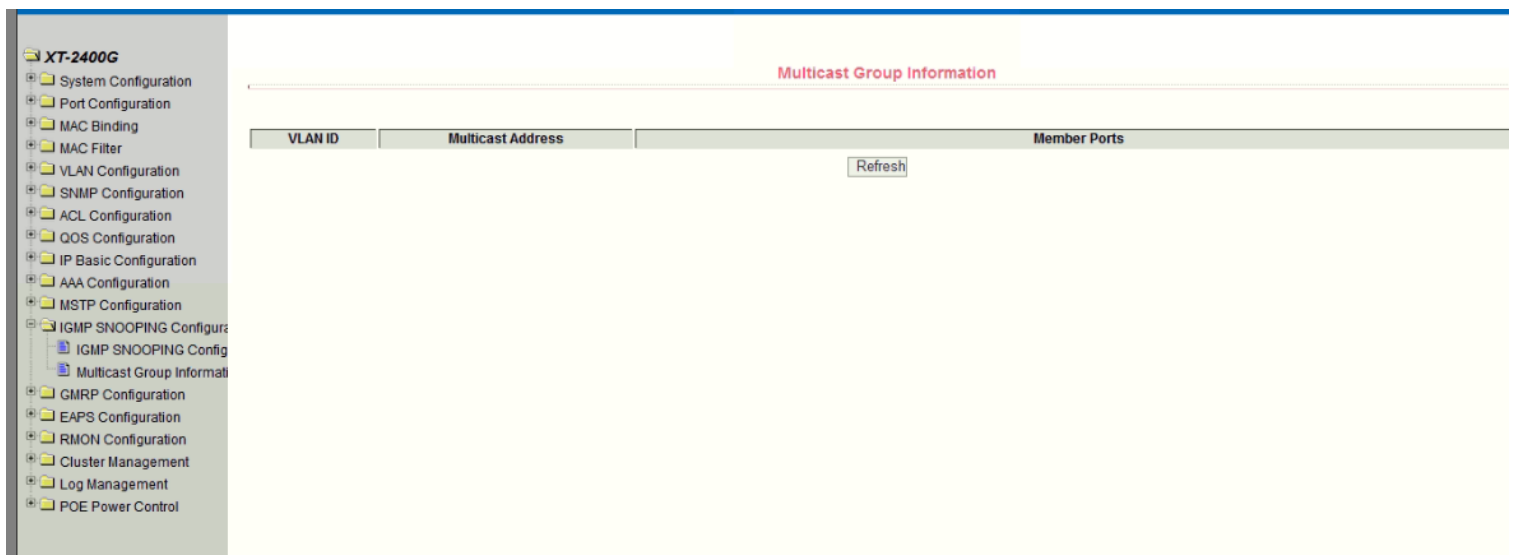


Figure 55 Multicast Group information page

## 15、GMRP configuration

### (1) GMRP global configuration page

Figure 56 shows the GMRP global configuration page. Users can enable GMRP through this page.



Figure 56 GMRP global configuration page



## (2) GMRP port configuration page

Figure 57 shows the GMRP port configuration page. Users can use this page to enable port GMRP, and can view the port information.

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	---	---	---
ge1/11	Disable	---	---	---
ge1/12	Disable	---	---	---
ge1/13	Disable	---	---	---
ge1/14	Disable	---	---	---
ge1/15	Disable	---	---	---
ge1/16	Disable	---	---	---

Figure 57 GMRP port configuration page

## (3) GMRP state machine page

Figure 58 is the GMRP state machine page. Users can view GMRP's state machine information from this page.

Port Name	VLAN ID	Multicast MAC Address	Applicant State	Registrar State

Figure 58 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** is 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.
- **Primary port** is EAPS Main port such as : fe1/1、ge1/1.
- **Secondary port** is EAPS Alternate port.
- **Control VLAN** is EAPS ring control vlan, the value of 2-4094

Protected vlan EAPS ring protection vlan.

- **Hello time interval** is the Hello message to send the time interval.
- **Fail time** is fault time detection.
- **Data Span** is forwarded across the ring In the case of multiple rings, this function is required when data needs to be forwarded across the ring.
- **Extreme interoperability** is the compatibility with radical network devices.
- **Enabled status** is used to enable EAPS ring.

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

Refresh Create Apply Remove

Figure 59 EAPS configuration page

## (2) EAPS information page

Figure 60 shows the EAPS information page. Users can view EAPS configuration information from this page.

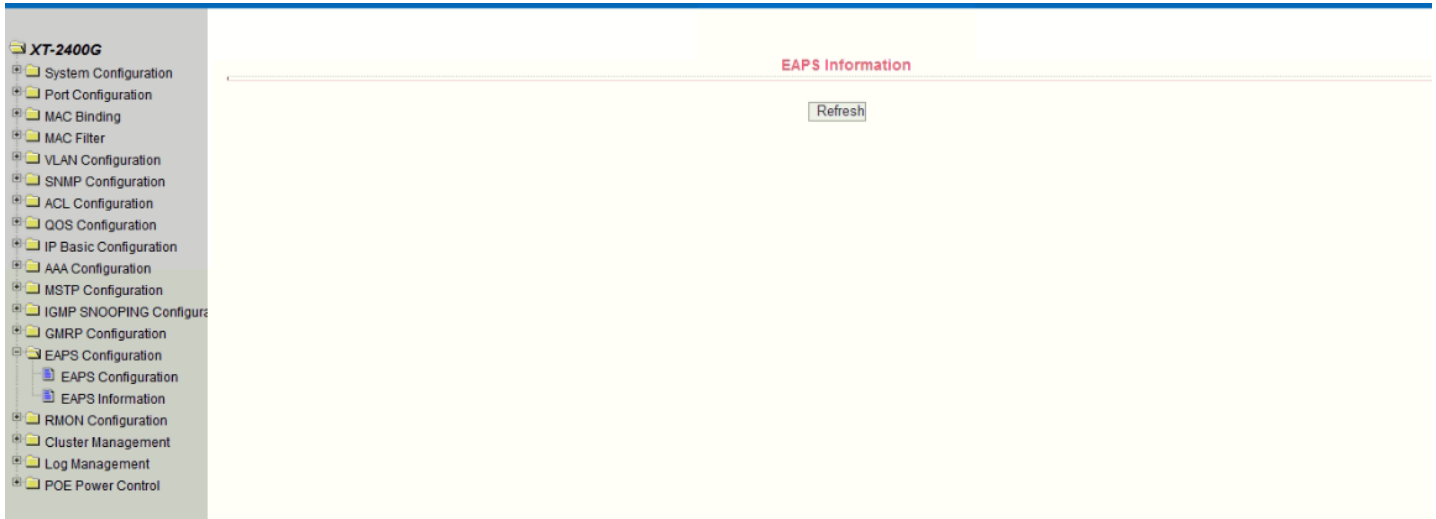


Figure 60 EAPS information page

## 17、RMON configuration

### (1) RMON Statistics configuration page

Figure 61 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.

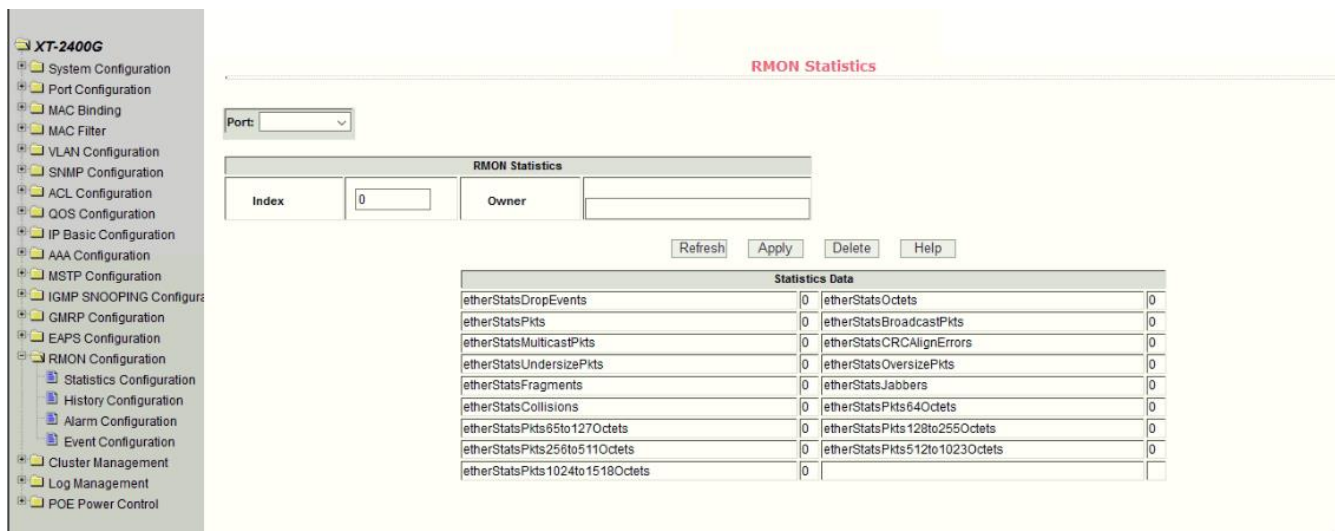


Figure 61 RMON Statistics configuration page

## (2) RMON History configuration page

Figure 62 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.

**XT-2400G**

- System Configuration
- Port Configuration
- MAC Binding
- MAC Filter
- VLAN Configuration
- SNMP Configuration
- ACL Configuration
- QOS Configuration
- IP Basic Configuration
- AAA Configuration
- MSTP Configuration
- IGMP SNOOPING Configuration
- GMRP Configuration
- EAPs Configuration
- RMON Configuration
  - Statistics Configuration
  - History Configuration
  - Alarm Configuration
  - Event Configuration
- Cluster Management
- Log Management

### RMON History

Port:

RMON History			
Index	<input type="text" value="0"/>	Interval	<input type="text" value="0"/>
Request Buckets	<input type="text" value="0"/>	Owner	<input type="text"/>

Refresh Apply Delete Help

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

First Prev Next Last

Total: 0pages, Current Page is No. 1

Figure 62 RMON History configuration page

### (3) RMON Alarm configuration page

Figure 63 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	

Refresh Apply Delete Help

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

Figure 63 RMON Alarm configuration page

#### (4) RMON Event configuration page

Figure 64 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	

Refresh Apply Delete Help

Sequence	Index	Description	Type	Community	Last Time Sent	Owner
----------	-------	-------------	------	-----------	----------------	-------

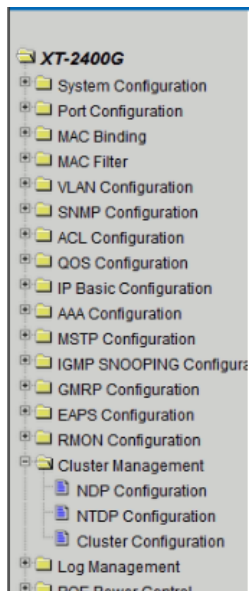
Figure 64 RMON Event configuration page



## 18. Cluster configuration

### (1) NDP configuration page

Figure 65 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:	<input type="text"/>	
Port Enable	<input type="text" value="disable"/>	
Global Enable	<input type="text" value="disable"/>	
Hello-time	<input type="text" value="60"/>	(1-4096 sec)
Aging-time	<input type="text" value="180"/>	(1-4096 sec)

Figure 65 NDP configuration page

## (2) NTDP configuration page

Figure 66 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.

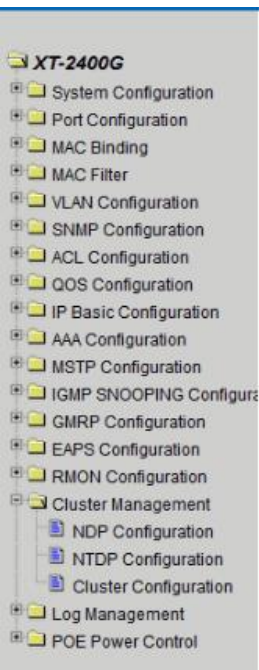
Port selection, you can select the port as required, and enable port NTDP function. NTDP to run normally, you must also enable the global and port NTDP function.

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:	<input type="text"/>	
Port Enable	disable <input type="button" value="v"/>	
Global Enable	disable <input type="button" value="v"/>	
Hops	<input type="text" value="3"/>	(1-6)
Interval-time	<input type="text" value="1"/>	(0-65535 min)
Hop-delay	<input type="text" value="200"/>	(1-1000 milsec)
Port-delay	<input type="text" value="20"/>	(1-100 milsec)

Figure 66 NTDP configuration page

### (3) Cluster configuration page

Figure 67 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**

Cluster Name:  Type:

Apply Delete

**Cluster Member List**

Serial	MAC	IP	Status	Name	Role
(Press the Button "Refresh" to view the latest information)					

Refresh Help

Figure 67 Cluster configuration page

## 19 · Log management

### ( 1 ) Log information

Figure 68 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.

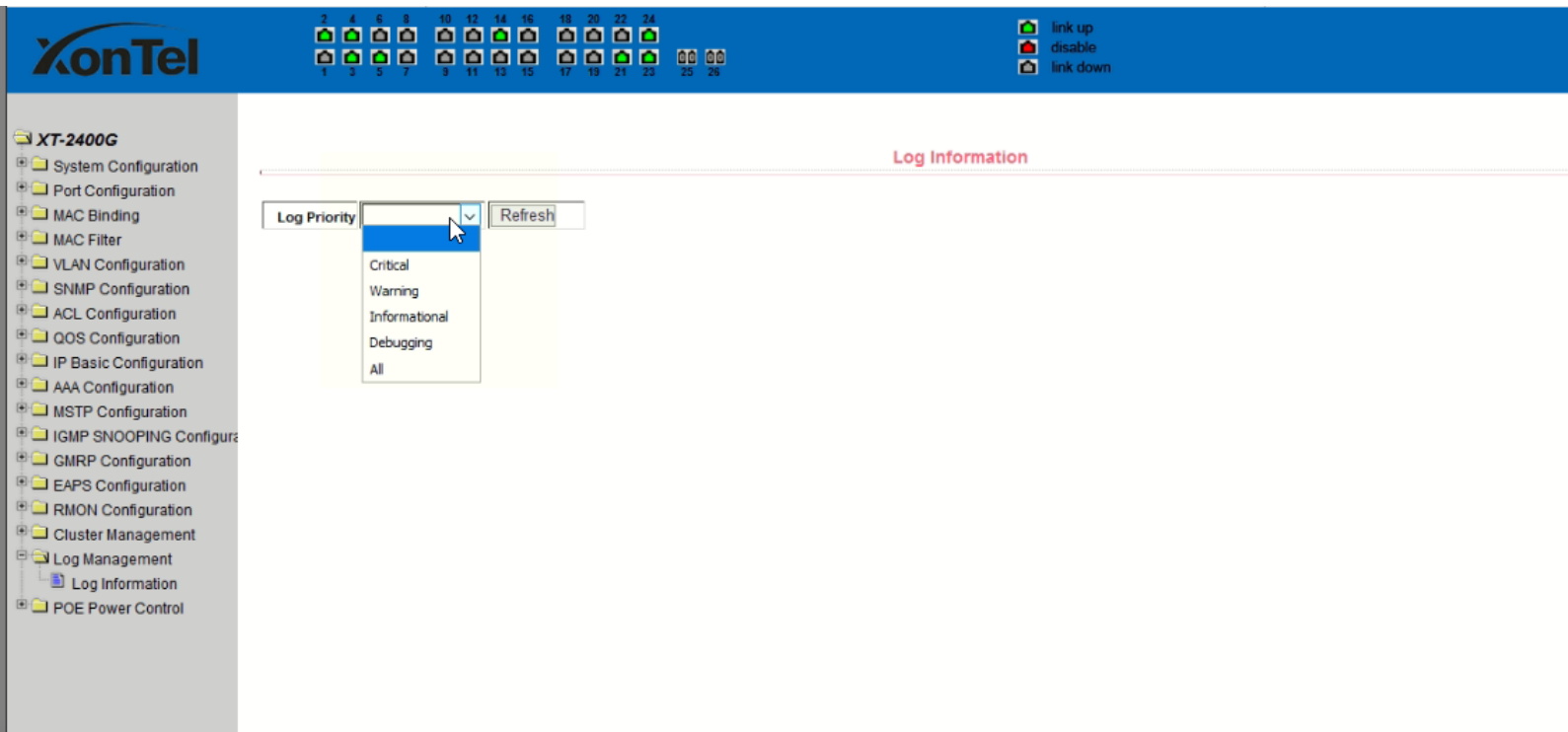


Figure 68 Log information page

## 20 · PoE port configuration

### ( 1 ) PoE port Configuration Page

- Figure 69 is the PoE port configuration / PoE-display page. Users can enable or disable the port's PoE function to the page, or View all ports of PoE information. Information can be seen in the following tables:

1 , Staus:Enable means PoE function is available disable means PoE function is close.

2 , Operation:Display the PoE ports ON or OFF

**POE Power Control**

POE Port:  POE Power Status:

Total Power Consume(mW) : 10547

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	On	802.3at	4	3392	64	53
ge1/4	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/5	Enable	On	802.3at	2	1431	27	53
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
ge1/9	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/10	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/11	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/12	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/13	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/14	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/15	Enable	Off	802.3at	N/A	N/A	N/A	N/A
ge1/16	Enable	Off	802.3at	N/A	N/A	N/A	N/A

Transfer data from 192.168.1.251

Figure 69 the PoE port configuration page