



MANAGE SWITCH 24*10/100/1000M RJ45 PORTS + 4 SFP

User 'S Manual

CATALOG ERROR! BOOKMARK NOT DEFINED.

一、WEB DESCRIPTION..... 2

1、WEB CHARACTERISTICS OF THE ACCESS	2
2、WEB SYSTEM REQUIREMENTS FOR BROWSING	2
3、WEB LOGIN OF BROWSING SESSION	3
4、WEB BASIC COMPOSITION OF THE PAGE	3
5、INTRODUCTION TO PAGE BUTTONS	4
6、ERROR MESSAGE.....	4
7、ENTRY FIELD.....	5

二、WEB DESCRIPTION 5

1、SYSTEM CONFIGURATION	5
2、PORT CONFIGURATION.....	8
3、VLAN CONFIGURATION.....	11
4、SAFTY CONFIGURATION.....	13
(1) MAC configuration.....	13
(2) ACL configuration.....	14
(3) AAA configuration.....	17
(4) Local management security configuration.....	19
5、MULTICAST CONFIGURATION.....	20
(1) IGMP SNOOPING configuration.....	20
6、RELIABILITY APPLICATION.....	21
(1) Spanning tree configuration.....	21
(2) ERPS configuration.....	21
7、ADVANCED CONFIGURATION.....	23
(1) IP basic configuration	23
8、SYSTEM TOOL	25

Web page operation manual

This manual mainly describes the web page of the switch. Users can use the web page to manage the switch. This manual only gives a brief introduction to the operation of each web page, Please refer to << 24G-4S + >>user's Manual for function introduction. This manual mainly includes the following contents:

- 1、 Overview of web pages
- 2、 Introduction to web page

一、 Overview of web pages

1、 WEB Characteristics of the access

This switch provides Web access for users. Users can access the switch through the web browser to manage and configure the switch. The main characteristics of web access are :

- Easy access: users can easily access the switch from anywhere on the network.
- Users can visit the web pages of 24G-4S + switch with familiar browsers such as Firefox, Google Chrome, Opera and Microsoft Internet Explorer (version 8.0 and above). The web pages are presented to users in graphical and tabular form.
- This switch provides rich web pages, through which users can configure and manage most functions of the switch.
- The classification and integration of web page functions makes it easy for users to find relevant pages for configuration and management.

2、 WEB system requirements for browsing

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

Table 1:

Hardware and software	System requirements
CPU	Pentium 586 above
Memory	128MB above
Resolution ratio	1024x768 above
Color	256 color above
Browser	Internet Explorer 8.0 Above or Firefox or Google Chrome or Opera...
Operating system	Microsoft® Windows xp®/Windows Vista®/ Windows 7®/Windows 8®, Linux, Unix operating system

Notes:

Microsoft®, Windows xp®, Windows Vista®, Windows 7®, Windows 8® are a registered

trademark of Microsoft Corporation. All other product names, trademarks, registered trademarks and service marks are owned by their respective owners.

3、WEB login of browsing session

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

- The switch has been IP configured. By default, the interface IP address of vlan1 of the switch is 192.168.0.1,
- The subnet mask is 255.255.255.0.
- A host with a web browser installed is connected to the network, and the host can ping the switch.

After completing the above two tasks, the user can enter the address of the switch in the address bar of the browser and press enter to enter the web login page of the switch, as shown in Figure 1. Only the correct password can access the web. The default user is admin and the password is empty by default.



Figure 1 login page of web browsing session

4、WEB basic composition of the page

As shown in Figure 2, the web page is mainly composed of four parts: title page, category navigation page, menu page and main page.

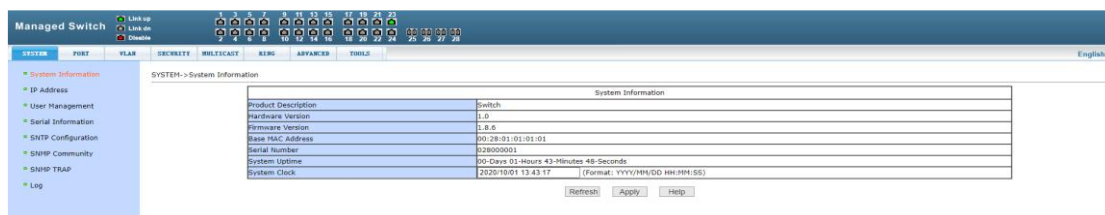


Figure 2 switch web page basic composition page

Title Page

Used to display logo and real-time port status, as shown in the figure below

The green light indicates that the port is connected;

The gray light indicates that the port is disconnected;

The red light indicates that the port is closed

Category navigation page

Web function classification entrance, users can click a button to view the corresponding classification menu, the right side of the page is the switch model version and login user name.

Menu page

Display the category menu selected by the user from the classification navigation page. There may be one or two level menus. Click the menu item to open the corresponding page.

Main page

Used to display the page selected by the user from the menu page.

5、Introduction to page buttons

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

Table 2:

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

6、Error message

If the web server of the switch has errors in processing user requests, the corresponding error information will be displayed in a dialog box. For example, figure 4 shows an error message dialog box.



Figure 3 error message page

7、Entry field

Some pages have an entry field at the beginning, as shown in Figure 5, through which you can access different items. When you select a value of an entry field, the corresponding information of that line is displayed on the page. At this time, the content of the line is edited, which is also called the active line.

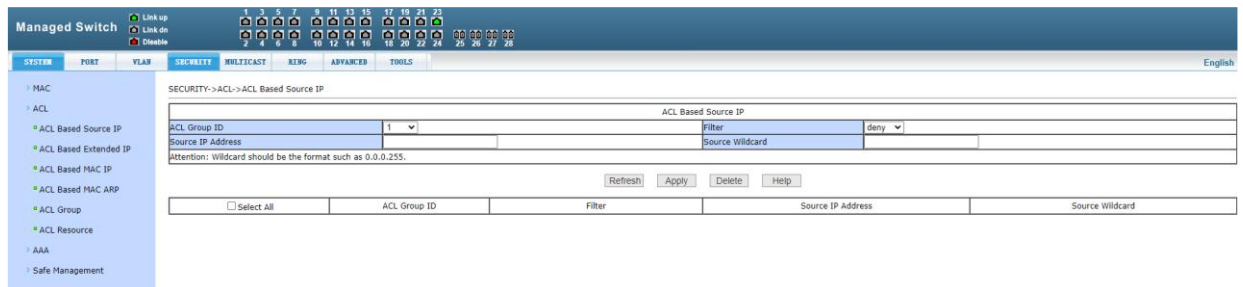


Figure 4 entry field page

二、WEB Page introduction

24G-4S+ The web pages of the switch are organized into groups, each group includes one or more web pages. Each page is introduced one by one.

1、SYSTEM CONFIGURATION

(1) System information page

Figure 5 is the system information configuration page, through which users can configure and view the system information of the switch.

Product model: product model description of the switch

Firmware version information: the firmware version currently used by the switch

Bootrom version information: the current bootrom version of the switch

Reference MAC address: the base MAC address of the switch

Serial number: the serial number of the switch

Serial port baud rate: the serial port baud rate used by the switch

System start up time: the time from switch start to now

System clock (modifiable): the current clock of the system. The parameters of year, month, day, hour, minute and second need to be input.

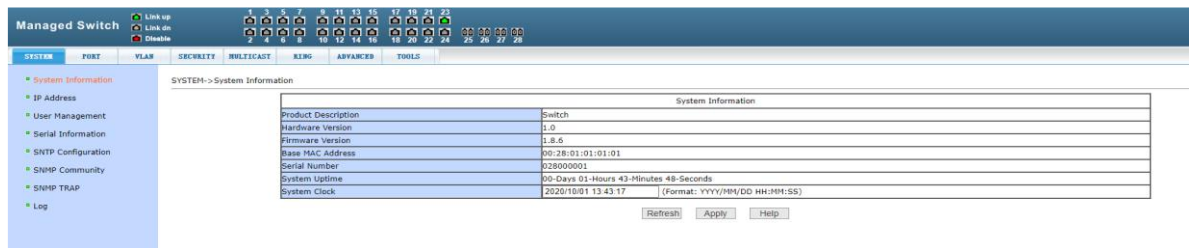


Figure 5 basic information page

(2) IP address configuration page

Figure 6 is the IP address configuration page. Users can configure the IP address, subnet mask and gateway address of the switch through this page. The management VLAN is 1 by default and cannot be modified.



Figure 6 IP address configuration page

(3) User management page

Figure 7 is the user management page, through which user information can be configured. The default user of the switch is admin, which cannot be deleted, but the password can be modified.

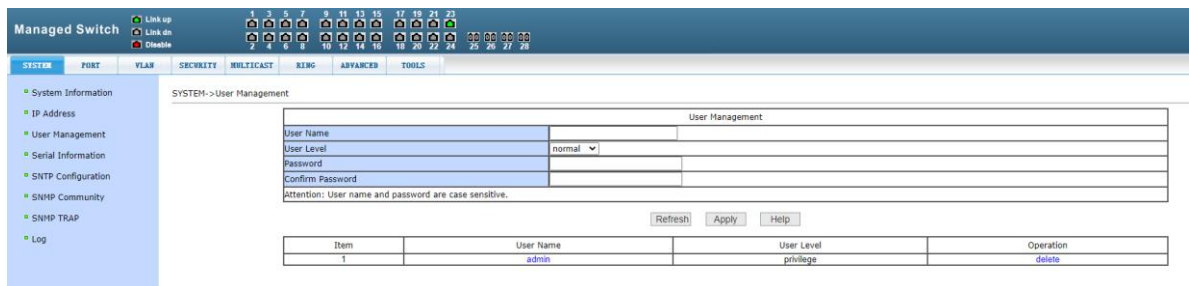


Figure 7 user management page

(4) SNMP common configuration page

Figure 8 is the SNMP common configuration page, which allows the user to configure the name and read-write permissions of the common body of the switch. A total of 8 entries can be configured.

By default, the switch has a public name common, which is read-only. When the switch needs to be managed by SNMP, it is necessary to configure a common body with readable and writable permissions.

The configured community cannot be modified or added with a duplicate name. However, you can click the corresponding delete link to delete the community, and then reconfigure it.



Managed Switch

SYSTEM -> SNMP Community

SNMP Community

Community Name:

Read and Write Privilege:

Item	Community Name	Read and Write Privilege	Operation
1	public	read-only	...

Figure 8 SNMP common configuration page

(5) SNMP TRAP CONFIGURATION PAGE

Figure 9 is the SNMP trap configuration page, which allows users to configure the IP address of the workstation receiving trap messages and some parameters of the trap protocol package.

Enter the trap name, trap server IP address, and select the version number. After submission, if the configuration is successful, the SNMP trap function will work. In case of link up or link down, the switch will automatically send trap packets to the target address.

The configured trap target cannot be modified or added with a duplicate name. However, you can click the corresponding delete link to delete the trap target and reconfigure it.



Managed Switch

SYSTEM -> SNMP TRAP

SNMP TRAP

TRAP Name:

Transmit Ip Address:

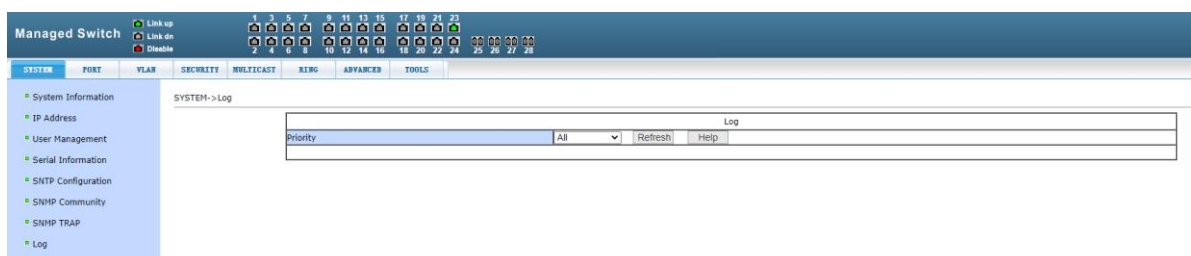
SNMP Version:

Item	TRAP Name	Transmit Ip Address	SNMP Version	Operation
------	-----------	---------------------	--------------	-----------

Figure 9 SNMP trap configuration page

(7) Log information

Figure 10 is the log information page through which users can view logs. Select the priority from the drop-down list to view the logs of this level. Click refresh to view the latest logs.



Managed Switch

SYSTEM -> Log

Log

Priority:

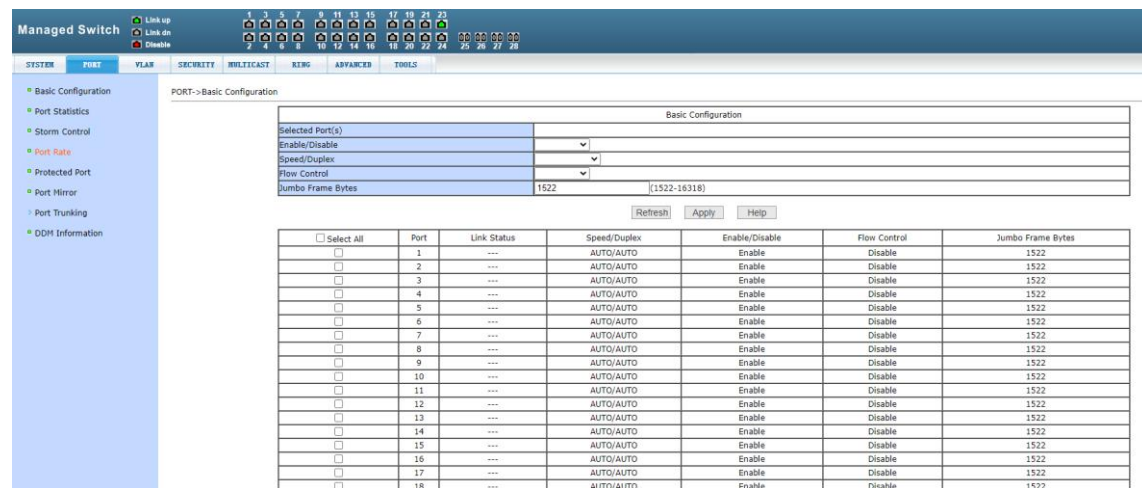
Figure 10 log information page

2、PORT CONFIGURATION

(1) Port basic configuration page

Figure 11 shows the port basic configuration page. Users can enable or disable ports, set port rate and flow control, or view basic information of all ports through this page.

To modify the port configuration, the user needs to check the left side of the corresponding port or use the "select all" function. The selected port will be displayed at the top of the page, and several consecutive ports are indicated by connection numbers. After successful setting, the selected port will be configured with the same parameters. The list on the page shows the configuration information for all ports.

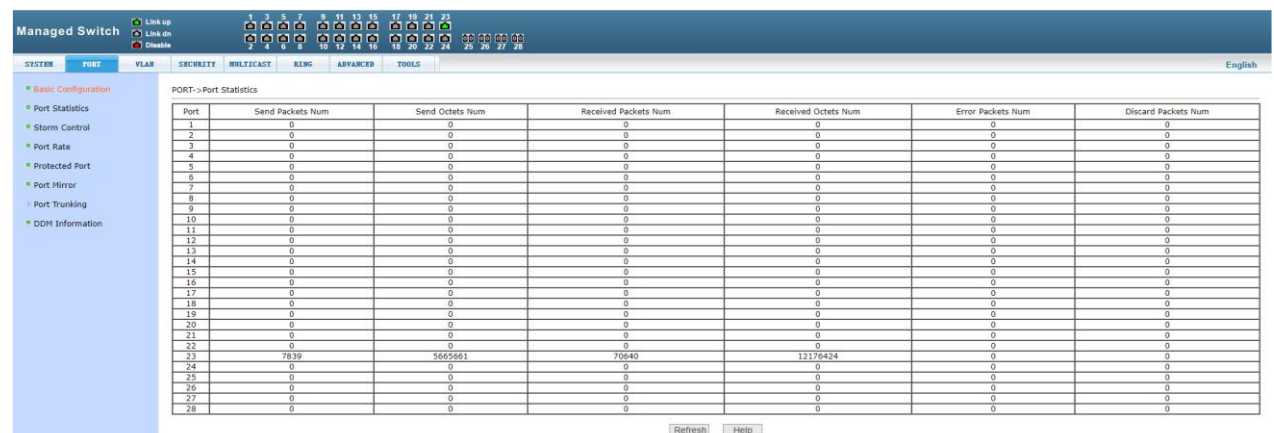


Port	Link Status	Speed/Duplex	Enable/Disable	Flow Control	Jumbo Frame Bytes
1	---	AUTO/AUTO	Enable	Disable	1522
2	---	AUTO/AUTO	Enable	Disable	1522
3	---	AUTO/AUTO	Enable	Disable	1522
4	---	AUTO/AUTO	Enable	Disable	1522
5	---	AUTO/AUTO	Enable	Disable	1522
6	---	AUTO/AUTO	Enable	Disable	1522
7	---	AUTO/AUTO	Enable	Disable	1522
8	---	AUTO/AUTO	Enable	Disable	1522
9	---	AUTO/AUTO	Enable	Disable	1522
10	---	AUTO/AUTO	Enable	Disable	1522
11	---	AUTO/AUTO	Enable	Disable	1522
12	---	AUTO/AUTO	Enable	Disable	1522
13	---	AUTO/AUTO	Enable	Disable	1522
14	---	AUTO/AUTO	Enable	Disable	1522
15	---	AUTO/AUTO	Enable	Disable	1522
16	---	AUTO/AUTO	Enable	Disable	1522
17	---	AUTO/AUTO	Enable	Disable	1522
18	---	AUTO/AUTO	Enable	Disable	1522

Figure 11 port configuration and port display page

(2) Port Statistics page

Figure 12 shows the Port Statistics page. The page lists the number of sent packets, sent bytes, received packets, received bytes, error packets, and dropped packets for all ports.



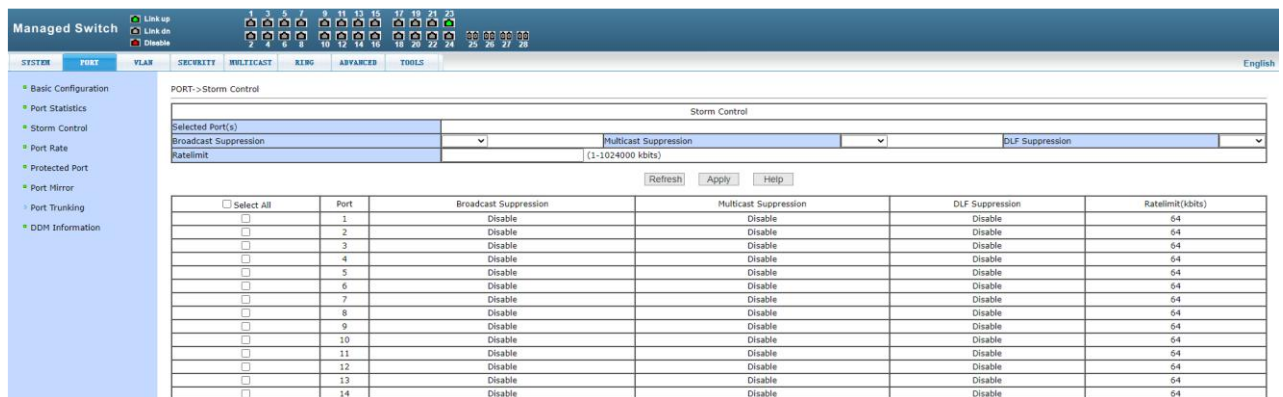
Port	Send Packets Num	Send Octets Num	Received Packets Num	Received Octets Num	Error Packets Num	Discard Packets Num
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	7839	5665861	70540	12176424	0	0
24	0	0	0	0	0	0
25	0	0	0	0	0	0
26	0	0	0	0	0	0
27	0	0	0	0	0	0
28	0	0	0	0	0	0

Figure 12 Port Statistics page

(3) Port storm suppression page

Figure 13 shows the port storm suppression page. This page is used to configure the suppression function of broadcast packets, multicast packets and DLF packets on ports.

Check the left side of the corresponding port, or select the port with the "select all" function to turn on and off the broadcast suppression, multicast suppression and DLF suppression of the port. The inhibition rate type item and inhibition rate item are used to select the inhibition rate type and inhibition rate value to be configured. The inhibition rate range is 1-1024000, and the unit is kbits. The inhibition rates of broadcast suppression, multicast suppression and DLF suppression can be configured independently. The list on the page shows the configuration information for all ports.



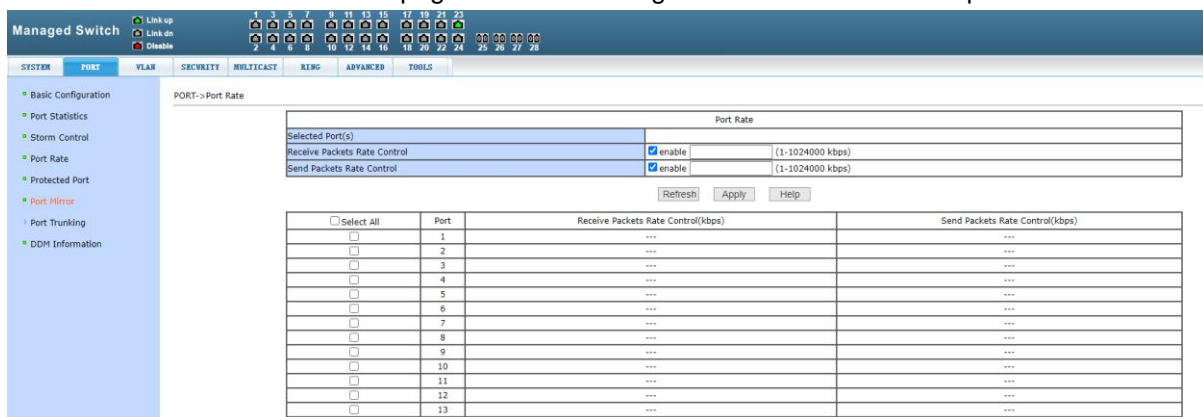
Select All	Port	Broadcast Suppression	Multicast Suppression	DLF Suppression	Rate Limit(kbits)
<input type="checkbox"/>	1	Disable	Disable	Disable	64
<input type="checkbox"/>	2	Disable	Disable	Disable	64
<input type="checkbox"/>	3	Disable	Disable	Disable	64
<input type="checkbox"/>	4	Disable	Disable	Disable	64
<input type="checkbox"/>	5	Disable	Disable	Disable	64
<input type="checkbox"/>	6	Disable	Disable	Disable	64
<input type="checkbox"/>	7	Disable	Disable	Disable	64
<input type="checkbox"/>	8	Disable	Disable	Disable	64
<input type="checkbox"/>	9	Disable	Disable	Disable	64
<input type="checkbox"/>	10	Disable	Disable	Disable	64
<input type="checkbox"/>	11	Disable	Disable	Disable	64
<input type="checkbox"/>	12	Disable	Disable	Disable	64
<input type="checkbox"/>	13	Disable	Disable	Disable	64
<input type="checkbox"/>	14	Disable	Disable	Disable	64

Figure 13 broadcast storm suppression page

(4) Port speed limit page

Figure 14 shows the port speed limit page. This page is used to configure the port access speed limit.

Check the left side of the corresponding port, or use the "select all" function to select the port. The speed limit of the in / out port can be opened separately by checking the box. The speed limit range is 1-1024000, and the unit is kbits. If the check is cancelled, the speed limit will not be limited. The list on the page shows the configuration information for all ports.



Select All	Port	Receive Packets Rate Control(kbps)	Send Packets Rate Control(kbps)
<input type="checkbox"/>	1	---	---
<input type="checkbox"/>	2	---	---
<input type="checkbox"/>	3	---	---
<input type="checkbox"/>	4	---	---
<input type="checkbox"/>	5	---	---
<input type="checkbox"/>	6	---	---
<input type="checkbox"/>	7	---	---
<input type="checkbox"/>	8	---	---
<input type="checkbox"/>	9	---	---
<input type="checkbox"/>	10	---	---
<input type="checkbox"/>	11	---	---
<input type="checkbox"/>	12	---	---
<input type="checkbox"/>	13	---	---
<input type="checkbox"/>	14	---	---

Figure 14 port speed limit page

(5) Link aggregation configuration page

Figure 15 shows the link aggregation configuration page. The page lists all ports vertically and all aggregation groups horizontally. To add a port to an aggregation group, just click the radio box at the intersection of the row and column, and the aggregation method can be selected at the bottom of each aggregation group. To cancel the aggregation configuration of the specified port, click the leftmost radio box corresponding to the port.

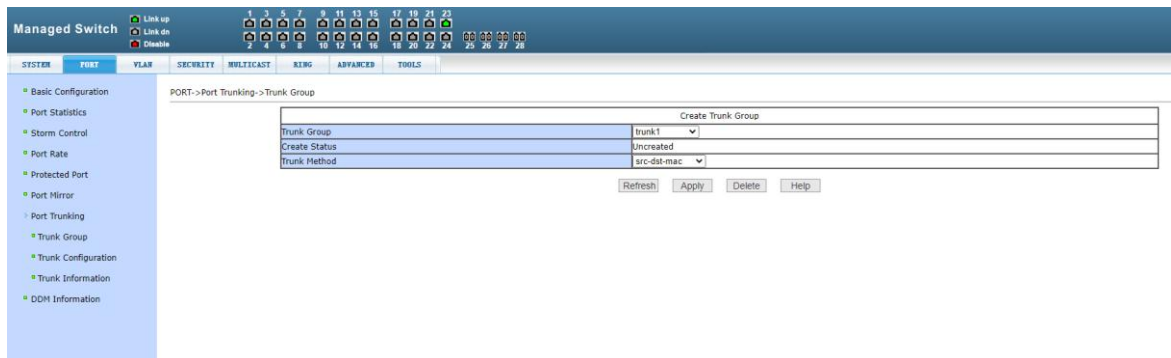


Figure 15 link aggregation configuration page

(6) Port image configuration page

Figure 16 shows the port mirroring configuration page, which allows users to configure port mirroring. Port mirroring is to listen to the output packets of the mirrored output port and the input packets of the mirrored input port through the mirror port. Only one mirror port can be selected, while multiple mirrored output ports and mirrored input ports can be selected. When configuring, select a mirror port first. Selecting "no mirroring" means canceling the mirror configuration. Then select the port and direction to be mirrored from other ports. When the input port in the listening direction is selected, it means to listen to the received packets, and the out port means to listen to the sent packets. If both are checked, it means to listen to all the packets sent and received.

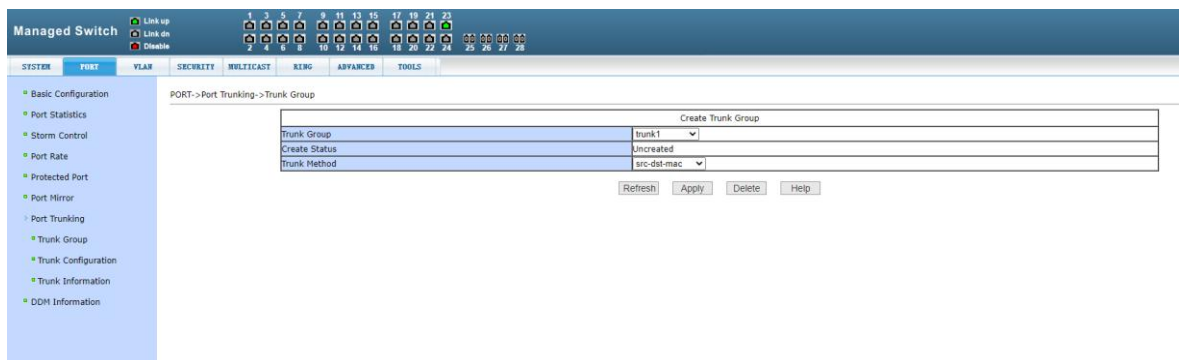


Figure 16 port image configuration page

3、VLAN CONFIGURATION

(1) VLAN CONFIGURATION PAGE

Figure 17 shows the VLAN configuration page. This page allows users to create VLANs and display all VLAN information.

If you want to create a new VLAN, enter vid in the active line, ranging from 2 to 4094. The switch creates vlan1 by default, and vlan1 cannot be deleted.

If you want to delete a VLAN, click the corresponding delete link in the VLAN list. Click "delete all" button to delete all VLANs except vlan1.

The VLAN list shows all VLANs that have been created, and indicates the port members of each VLAN. A port can not be a VLAN member, but can be a tagged or untagged member of a VLAN. The meaning of the characters in front of the port on the page is as follows:

- T tagged The port is a tagged member of this VLAN
- U untagged The port is an untagged member of this VLAN

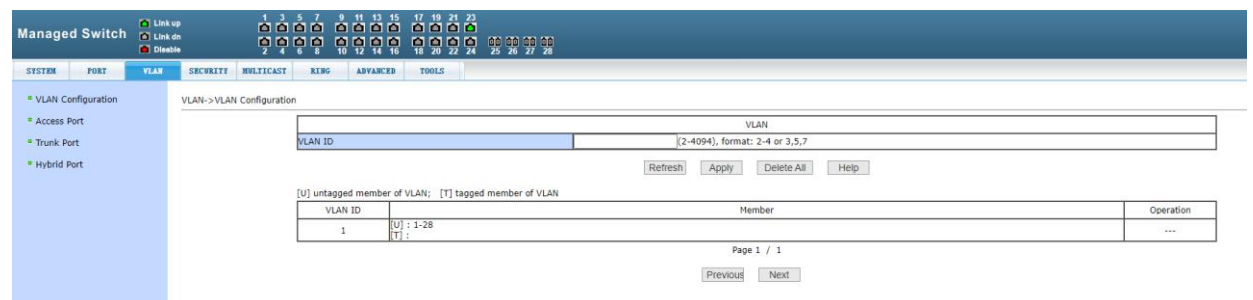


Figure 17 VLAN configuration page

(2) Access port configuration page

Figure 18 shows the access port configuration page, showing and configuring the port access mode and VLAN. Click on the port / VLAN page to see the port list, which can be divided into two parts. If the port is in access mode, its VLAN can be displayed when it is selected. If other VLANs are selected and applied, the VLAN of the port is changed. If the port is not in access mode, the port will be changed to access mode and VLAN will be set. Note that only one VLAN can be selected in access mode.

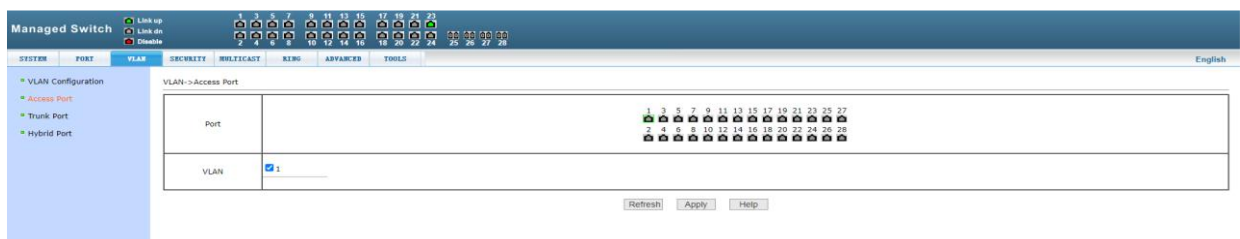


Figure 18 access port configuration page

(3) Trunk port configuration page

Figure 19 shows the trunk port configuration page, showing and configuring the port trunk mode and the VLAN it belongs to. This page is divided into two parts: port list and VLAN list. Please refer to Section 2 (access port configuration page) for port operation. If the port is in trunk mode, its VLAN can be displayed when it is selected. If other VLANs are selected and applied, the VLAN of the port is changed. If the port is not in trunk mode, the port will be changed to trunk mode and VLAN will be set after configuration. In trunk mode, multiple VLANs can be selected. If you need to select a continuous group of VLANs, first select the first one, hold down the shift key, and then select the last one.

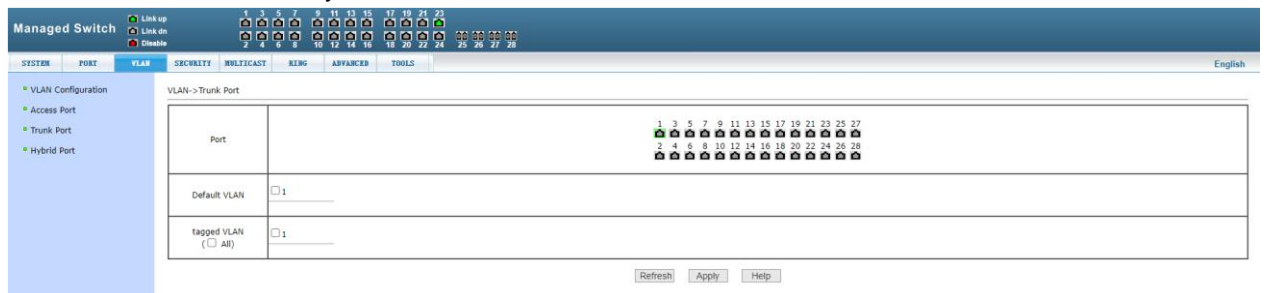


Figure 19 trunk port configuration page

(4) Hybrid port configuration page

Figure 20 shows the configuration page of hybrid port, showing and configuring the port hybrid mode and VLAN. This page is divided into two parts: port list and VLAN list. Please refer to Section 2 (access port configuration page) for port operation. If the port is in hybrid mode, its VLAN can be displayed when it is selected. If other VLANs are selected and applied, the VLAN of the port is changed. If the port is not in hybrid mode, the port will be changed to hybrid mode and VLAN will be set after configuration. If the number of VLANs is selected by default, only one VLAN or tagged VLAN can be selected.




Figure 20 configuration page of hybrid port

4、SAFTY CONFIGURATION

(1) MAC CONFIGURATION

① Manual binding page of MAC address

Figure 21 shows the MAC configuration page. This page is used to realize the binding of port and MAC address.

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

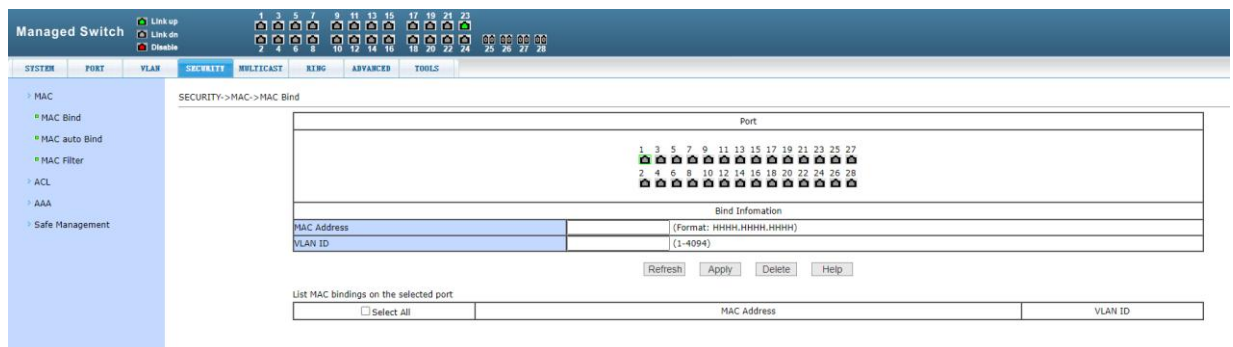


Figure 21 manual binding page of MAC address

② MAC address auto binding page

Figure 22 shows the MAC address auto binding page. This page is used to realize port auto binding MAC address.

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

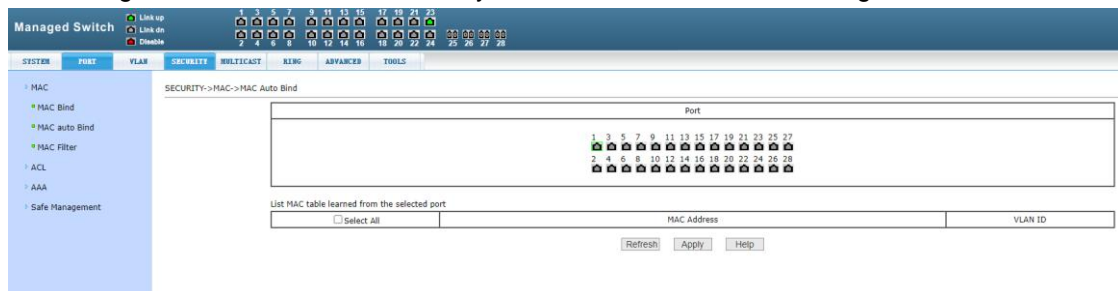


Figure 22 MAC address auto binding page

③ MAC address filtering configuration page

Figure 23 shows the MAC address filtering configuration page. This page is used to configure the port to filter MAC address.

The MAC item on the page is used to input the filtered MAC address, and the VLAN

number item is used to enter the VLAN to which the MAC address belongs.

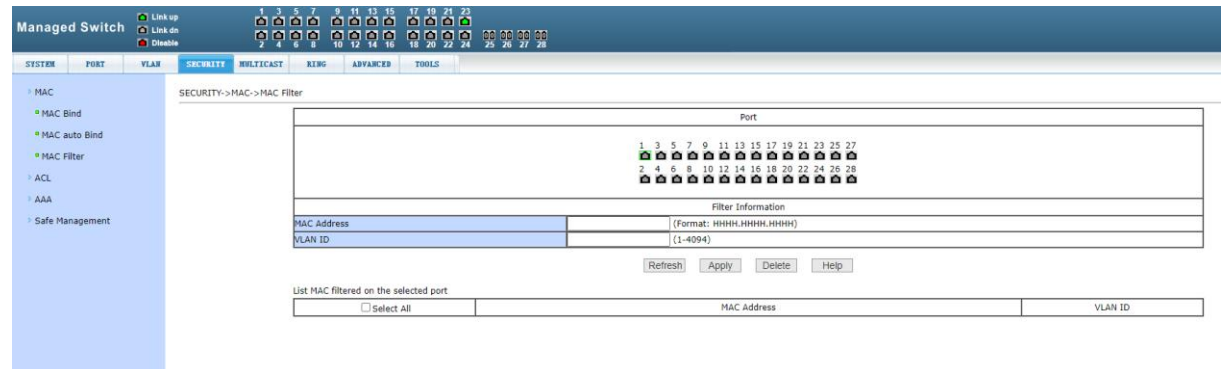


Figure 23 MAC address filtering configuration page

(2) ACL CONFIGURATION

① Standard IP group ACL page

Figure 24 is the ACL page of standard IP group, through which users can establish the rule base of ACL standard IP. Users can select an ACL group number (ranging from 1-99 or 1300-1999) to create one or more rules in the group. The only fields that can be matched in a rule are the source IP address (masked).

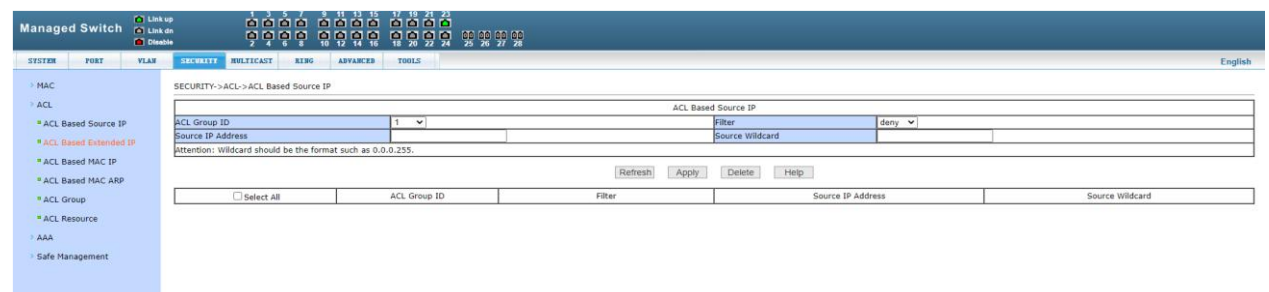


Figure 24 ACL page of standard IP group

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

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

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

② Expand IP group ACL page

Figure 25 shows the ACL page of the extended IP group, through which users can establish the rule base of ACL extended IP. Users can select an ACL group number (ranging from 100-199 or 2000-2699) to create one or more rules in the group. The fields that can be matched in a rule are active IP address (masked), destination IP address (masked), protocol type (such as ICMP, TCP, UDP, etc.), source port and destination port (only valid for TCP and UDP protocols), and TCP control flag.

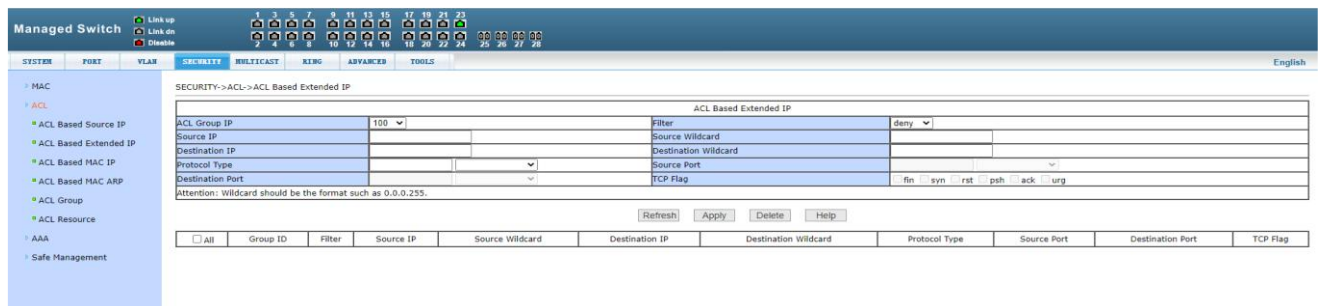


Figure 25 expand IP group ACL page

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

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

When a user creates a rule in a rule group, the system will automatically give the rule a rule number. When a rule in a rule group is deleted, other rules remain unchanged, and the system will automatically sort the rules in a rule group. If you want to delete the entire rule group, you can first select all and then press the delete key.

③ Mac IP group ACL page

Figure 26 is the ACL page of MAC IP group, through which users can establish ACL MAC IP rule base. Users can select an ACL group number (ranging from 700-799) to create one or more rules in the group. Fields that can be matched in a rule: active MAC address (with address matching bit), source IP address (with address matching bit), destination IP address (with address matching bit).

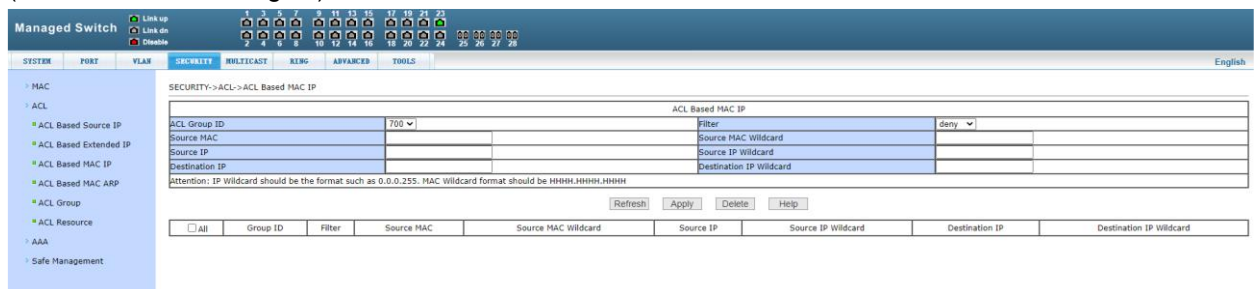


Figure 26 MAC IP group ACL page

When the user configures the rule, the source MAC address, the source IP address and the destination IP address all need to carry on the 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 users configure rules, each rule must have a filtering mode: allow or reject.

When a user creates a rule in a rule group, the system will automatically give the rule a rule number. When a rule in a rule group is deleted, other rules remain unchanged, and the system will automatically sort the rules in a rule group. If you want to delete the entire rule group, you can first select all and then press the delete key.

④ Mac ARP group ACL page

Figure 27 is the ACL page of MAC ARP group, through which users can establish ACL MAC ARP rule base. Users can select an ACL group number (ranging from 1100 to 1199) to create one or more rules in the group. The fields that can be matched in a rule are ARP operation type, sending MAC address (with address matching bit), and sending IP address (with address matching bit) .

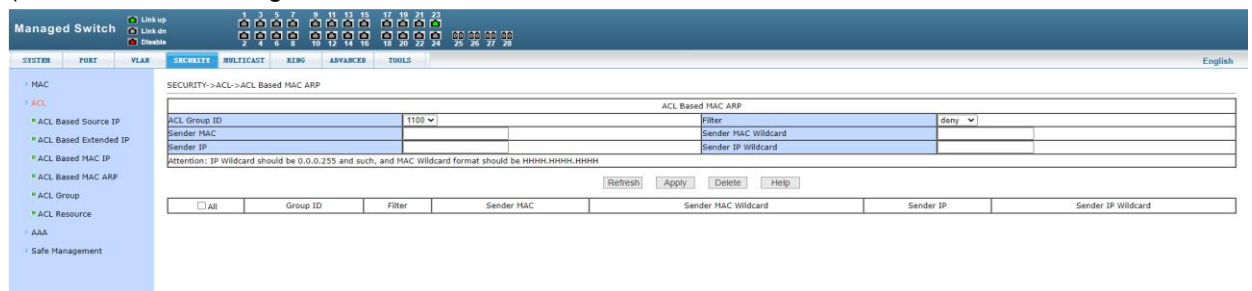


Figure 27 MAC ARP group ACL configuration page

When the user configures the rules, both the sending MAC address and the sending IP address should have address matching bits. The rules 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 users configure rules, each rule must have a filtering mode: allow or reject.

When a user creates a rule in a rule group, the system will automatically give the rule a rule number. When a rule in a rule group is deleted, other rules remain unchanged, and the system will automatically sort the rules in a rule group. If you want to delete the entire rule group, you can first select all and then press the delete key.

⑤ Port application ACL page

Figure 28 is the port application ACL page. Users can select an ACL group for a port through this page, write the rules in the ACL group into the port hardware logic, and make the port perform ACL filtering on the received packets according to these rules.

When selecting ACL group for port, you can select IP standard, IP extension, MAC IP, and MAC ARP ACL group. The selected ACL group must exist. Select from the ACL rule group list

and press add key. To delete an ACL group, select an ACL group from the list of referenced rule groups and press the delete key.

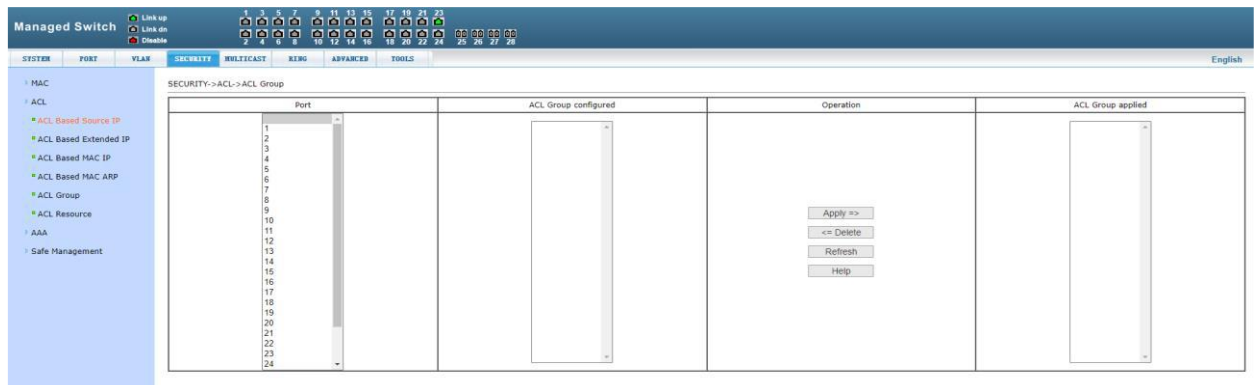


Figure 28 port application ACL page

⑥ ACL configuration information page

Figure 29 is the ACL configuration information page, which shows all the rules and reference information configured in the current ACL.

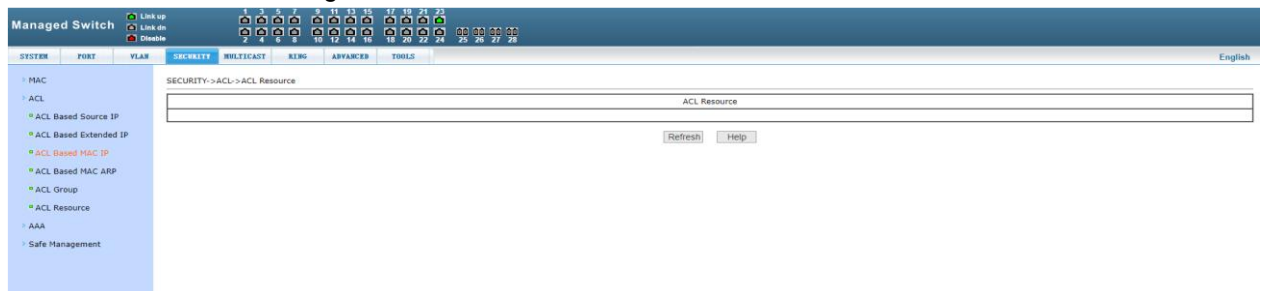


Figure 29 ACL configuration information page

(3) AAA CONFIGURATION

① AAA Global configuration page

Figure 30 shows the AAA global configuration page. Users can configure AAA related information, including:

- ☐ Whether to start 802.1x protocol or not, it must be started when doing authentication and accounting.
- ☐ Whether to turn on the re authentication function is not enabled by default. It is determined according to the actual situation when the authentication billing is made. Turning on the re authentication function will make users more reliable when using authentication billing, but will slightly increase the network traffic.
- ☐ Set the re authentication interval, which is valid only when the re authentication function is turned on. The default value is 3600 seconds. When doing

authentication billing, set the value according to the actual situation, but the value should not be too small.

- The IP address of radius server must be set in authentication billing.
- The IP address of the alternate radius server. If there is a standby radius server, this field can be set.
- The shared key is used to set the encrypted shared password between the switch and the radius server. This field must be set during authentication and billing, and it should be the same as that on the radius serve.
- Whether to start billing or not, it is started by default. When doing authentication billing, it is generally required to start charging.

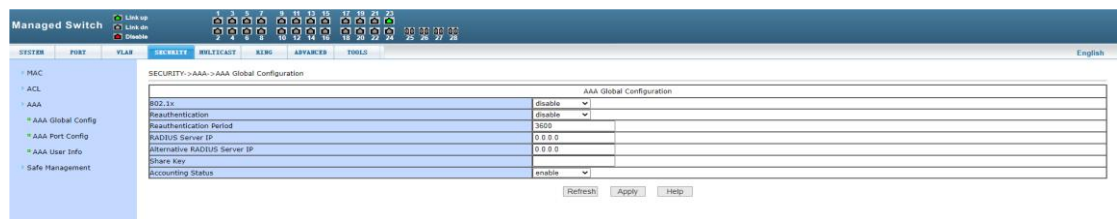


Figure 30 AAA global configuration page

② AAA Port configuration page

Figure 31 is the AAA port configuration page. Through this page, users can configure the authentication port mode and the maximum number of hosts supported, and view the configuration of each port. To modify the port AAA configuration, users need to check the left side of the corresponding port or use the "select all" function. The selected port will be displayed at the top of the page, and several consecutive ports are represented by connection numbers. After successful setting, the selected port will be configured with the same parameters. There are four types of AAA port modes: n / a state, auto state, force authorized state and force unauthorized state. When a port needs 802.1x authentication, the port should be set to auto state. If you can access the network without authentication, set the port to N / a state. The other two states are rarely used in practical applications.

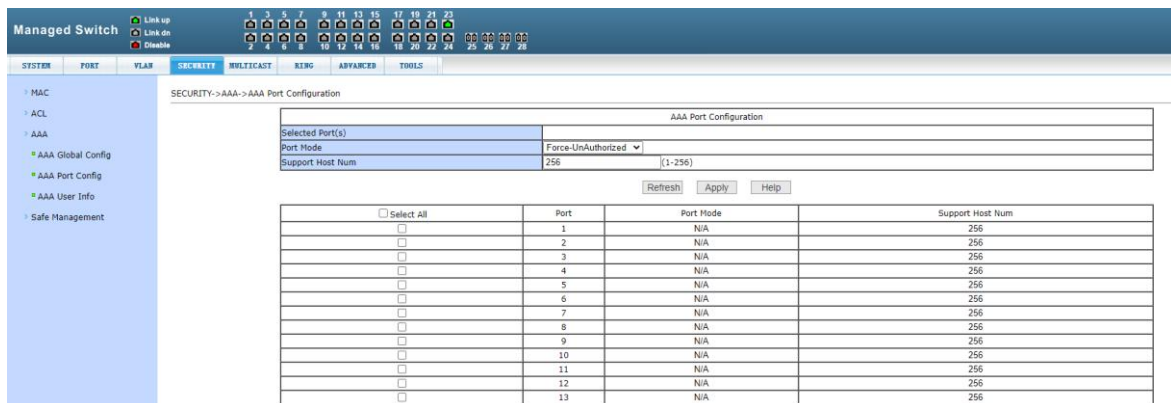


Figure 31 AAA port configuration page

When doing 802.1x authentication, the maximum number of hosts accessed by the port by default is 256. Users can modify this field to support 256 hosts at most.

③ AAA User information page

Figure 32 is the AAA user information page, through which users can view the status information of all users accessed under a certain port.



Figure 32 AAA user information page

(4) Local management security configuration

① Management rights configuration page

Figure 33 is the management authority configuration page. Through the configuration of this page, the administrator can control the network management services Telnet, web and SNMP, enable or disable these services, connect these services with ACL group of IP standards, implement source IP address control, and control host access to these service.

By default, Telnet, web and SNMP services are open, and ACL filtering is not performed. That is to say, all hosts can access the three services of the switch. If the administrator does not want to provide one or more services to other users for security, one or more services can be shut down. If the administrator only wants a specific host to access one or more services, one or more services can be filtered by ACL. When a service wants to perform ACL filtering, it is necessary to open the service and select an ACL group (1-99) of IP standard. At this time, the ACL group must exist.

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

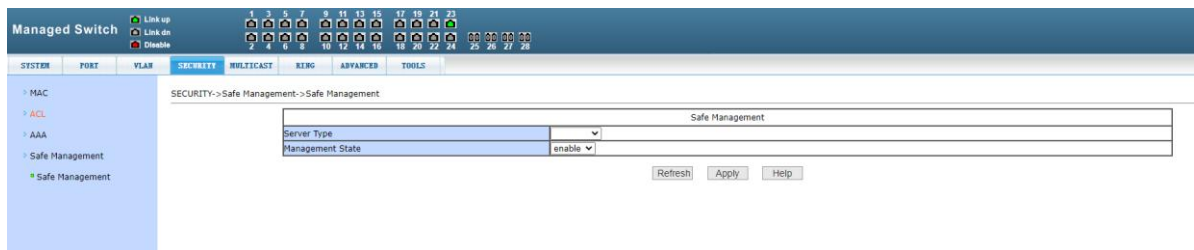


Figure 33 management rights new configuration page

5、Multicast configuration

(1) IGMP SNOOPING CONFIGURATION

① IGMP SNOOPING CONFIGURATION PAGE

Figure 34 shows the IGMP snooping configuration page. Users can enable IGMP snooping through this page.

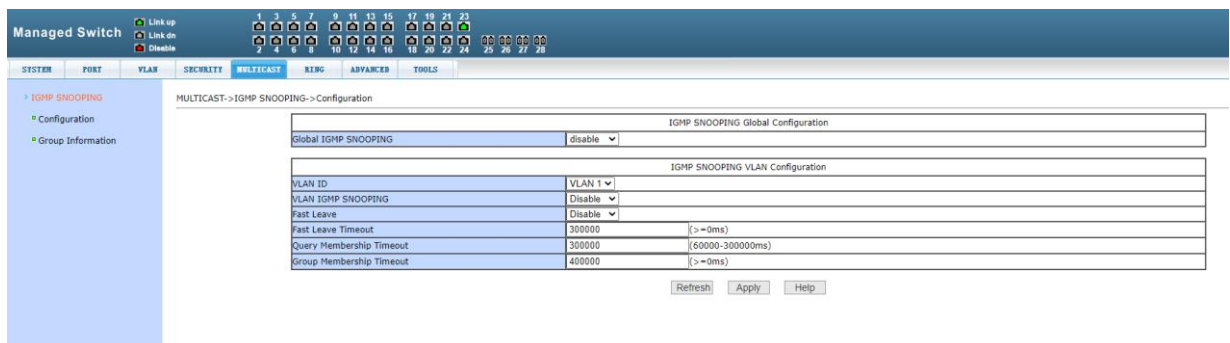


Figure 34 igmpssnooping configuration page

② Multicast group information page

Figure 35 is the multicast group information page, through which users can view IGMP snooping multicast information.

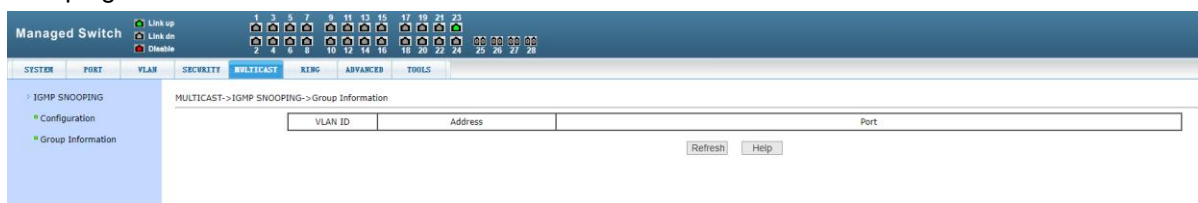


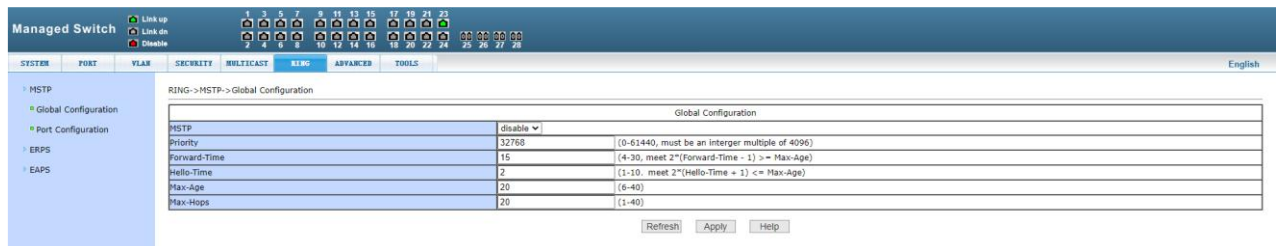
Figure 35 multicast group information page

6、Reliability Application

(1) Spanning tree configuration

① Spanning tree global configuration page

Figure 36 shows the spanning tree global configuration page, through which users can configure the global spanning tree parameters.

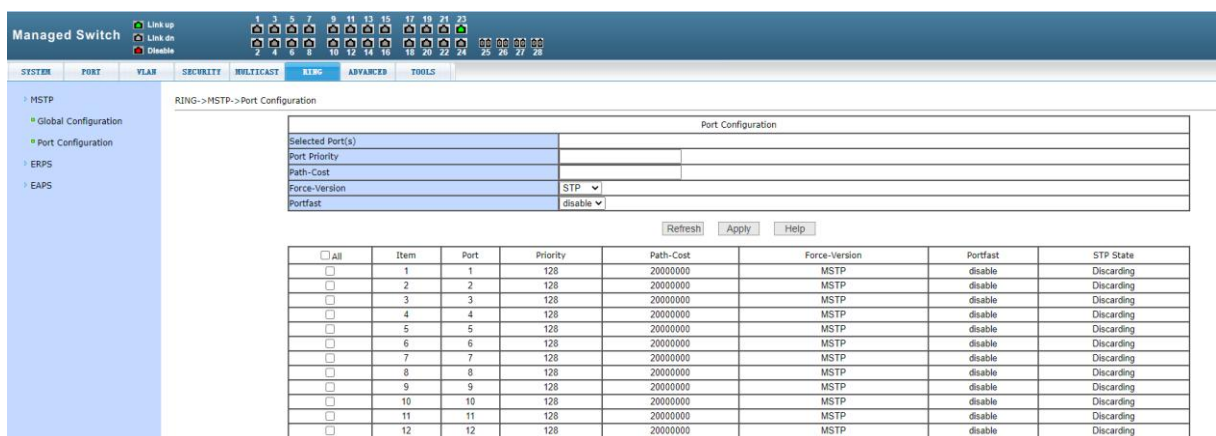


Global Configuration		
MSTP	disable	
Priority	32768	(0-61440, must be an integer multiple of 4096)
Forward-Time	15	(4-30, must be 2*(Forward-Time - 1) >= Max-Age)
Hello-Time	2	(1-10, must be 2*(Hello-Time + 1) <= Max-Age)
Max-Age	20	(6-40)
Max-Hops	20	(1-40)

Figure 36 global configuration page of spanning tree

② Spanning tree port configuration page

Figure 37 shows the port configuration page of spanning tree. Users can view the specific status of MSTP through this page.



Item	Port	Priority	Path-Cost	Force-Version	Portfast	STP State
1	1	128	20000000	MSTP	disable	Discarding
2	2	128	20000000	MSTP	disable	Discarding
3	3	128	20000000	MSTP	disable	Discarding
4	4	128	20000000	MSTP	disable	Discarding
5	5	128	20000000	MSTP	disable	Discarding
6	6	128	20000000	MSTP	disable	Discarding
7	7	128	20000000	MSTP	disable	Discarding
8	8	128	20000000	MSTP	disable	Discarding
9	9	128	20000000	MSTP	disable	Discarding
10	10	128	20000000	MSTP	disable	Discarding
11	11	128	20000000	MSTP	disable	Discarding
12	12	128	20000000	MSTP	disable	Discarding

Figure 37 spanning tree port configuration page

(2) ERPS CONFIGURAION

① ERPs predefined configuration page

Figure 38 shows the ERPs predefined configuration page, which enables the ERPs predefined configuration. When the ERPs predefined configuration is enabled, you can specify the node type: primary or transport.

Specific predefined configuration: ERPs instance number is 1, ERPs change number is 1,

ring mode is main ring mode, protocol VLAN is vlan3001, data VLAN is vlan1, RPL port is 51, RL port is 52, recovery behavior is recoverable, hold off time is 0, guard time is 500 ms, WTR time is 5 minutes, WTB time is 5 seconds, and protocol message sending time is 5 seconds.

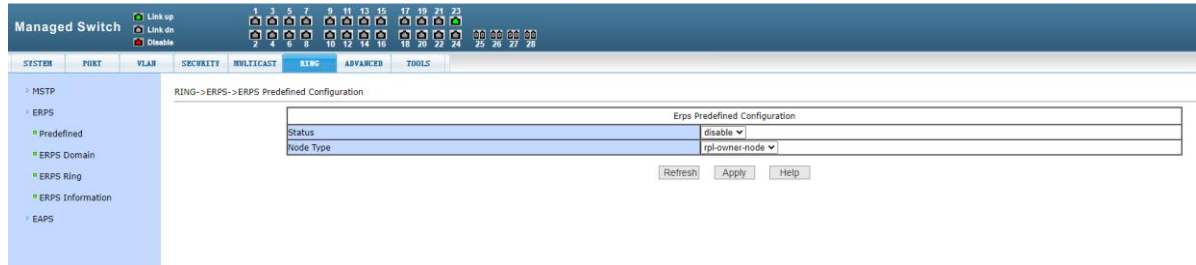


Figure 38 ERPs predefined configuration page

② ERPs instance configuration page

Figure 39 is the ERPs instance configuration page, which can be used to configure ERPs instances. When the instance is not created, click apply to create and specify the role; when the instance has been created but there is no associated ring, the role can be modified; if the instance has been created and associated with a ring, the instance cannot be modified. Click Delete to delete the selected instance. You can configure up to 8 instances.

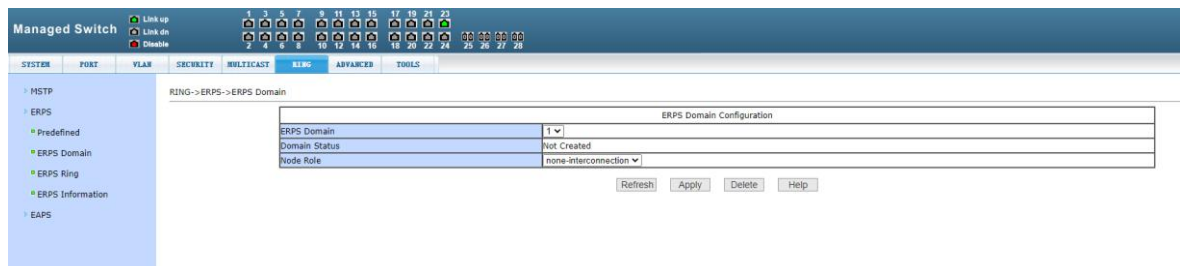


Figure 39 ERPs instance configuration page

③ ERPs ring configuration page

Figure 40 shows the ERPs ring configuration page, which allows you to create and configure ERPs rings. Select a ring. When the ring is not created, click the Apply button to create the ring and set the configuration information. If it has been created, the configuration information can be modified. Click the delete button to delete the selected ring. Rings must and can only be associated with one instance, and a maximum of 32 rings can be configured. When the ring fault is detected, click the manual recovery button to recover.

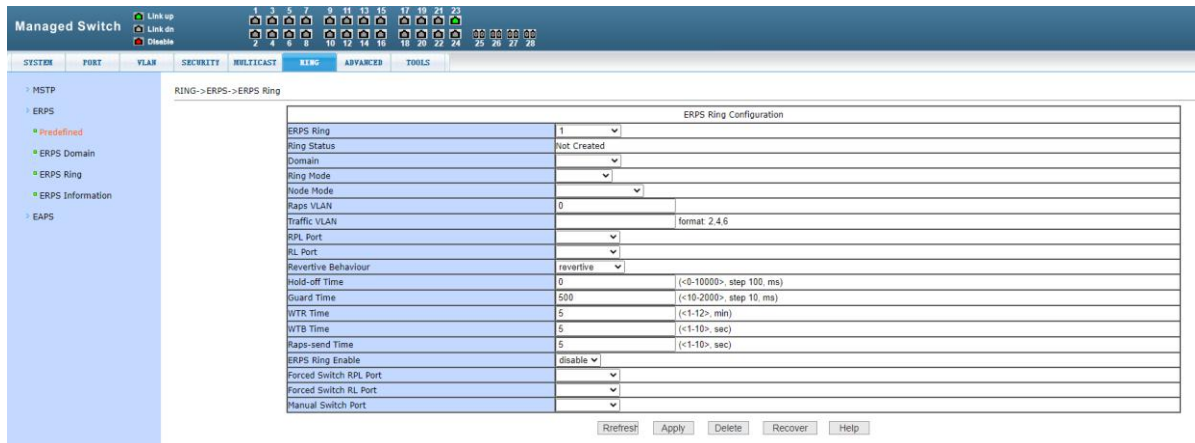


Figure 40 ERPs ring configuration page

④ ERPS MESSANGE PAGE

Figure 41 shows the ERPs information page. Selecting the ring number will display the configuration and status information of the relevant ERPs ring.

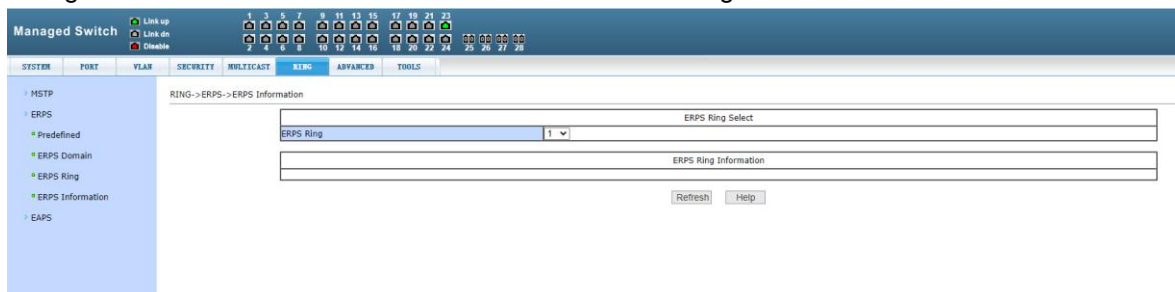


Figure 41 ERPs information page

7、Advanced configuration

(1) IP BASIC CONFIGURATION

① VLAN PORT CONFIGURAION PAGE

Figure 42 is the VLAN interface configuration page, through which users can configure the IP address of the interface, delete the IP address of the interface and view the interface information.

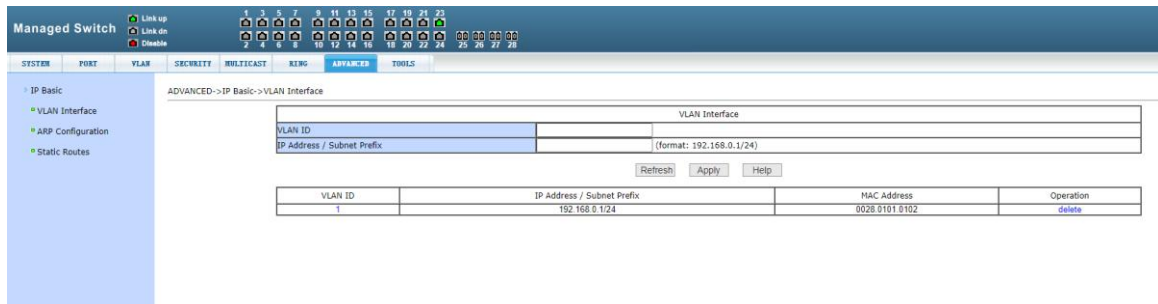


Figure 42 VLAN interface configuration page

This switch has a vlan1 interface by default, which cannot be deleted. A VLAN can only be configured with one interface.

② ARP CONFIGURATION PAGE

Figure 43 is the ARP configuration page, which can display all the information of the ARP table of the switch. At the same time, users can configure static ARP entries, delete ARP entries, and modify dynamic ARP entries to static ARP entries.

When configuring a static ARP entry, the user needs to input IP address and MAC address. MAC address must be unicast MAC address, and then click Apply button.

When the user is deleting an ARP entry, click the corresponding delete link in the list.

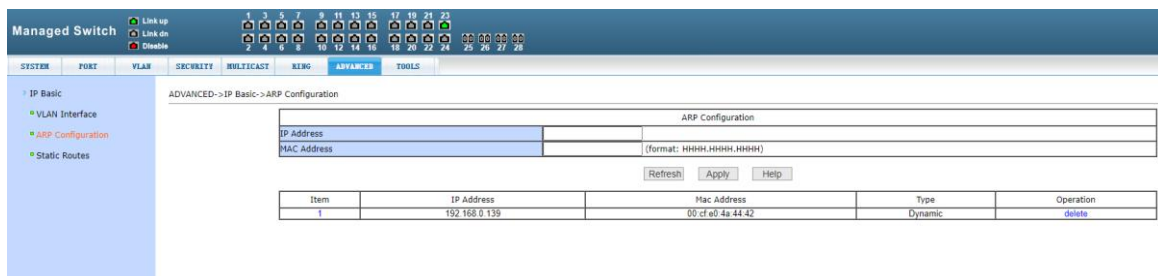


Figure 43 ARP configuration page

③ Static route configuration page

Figure 44 is the static route configuration page, through which users can add or delete static routes of switches. By default, the switch does not have a static route configured. Users can configure the default route through this page, that is, the route with destination address / subnet prefix of 0.0.0.0.

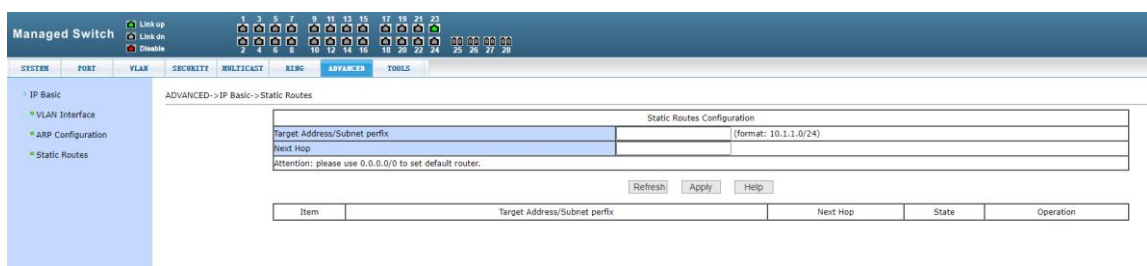


Figure 44 static route configuration page

8、SYSTEM TOOL

(1) Saved configuration page

Figure 45 shows the save configuration page. Through this page, users can view the current configuration of the switch. The Save button stores the current configuration of the system to the configuration file. Because the storage operation needs to erase the flash chip, which takes a certain amount of time. When the user has made the configuration on the page and hopes that the configuration will not be lost after the switch is restarted, the user must click the Save button in the current configuration page before exiting the page.

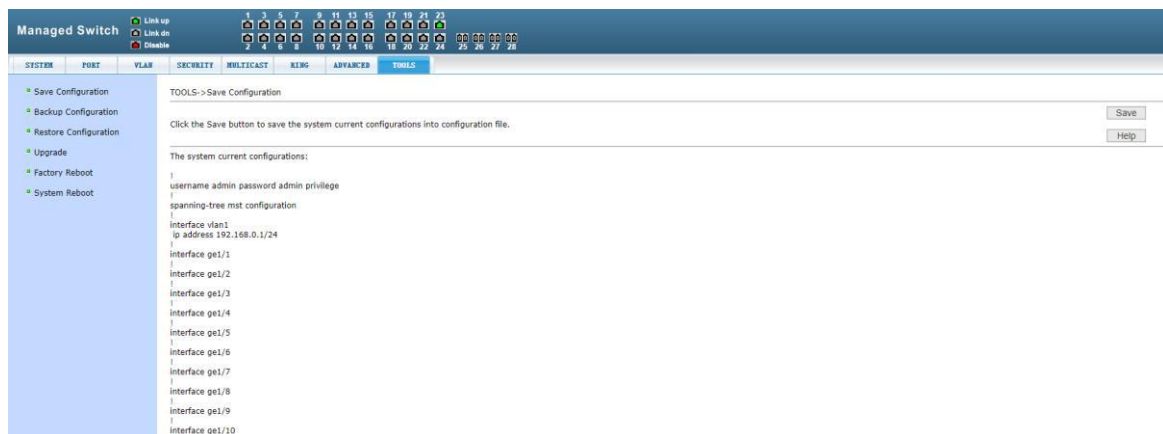


Figure 45 save configuration page

(2) Backup profile page

Figure 46 shows the backup profile page. This page allows the user to view the initial configuration of the system. The initial configuration is actually the configuration file in flash. When there is no configuration file in flash, the default configuration is used when the system starts. Click the Backup button, and a dialog box will pop up. The user can select the path to save the directory and save the configuration file. The file name of the downloaded configuration file is by default switch.cfg.



Figure 46 backup profile page

(3) Restore profile page

Figure 47 shows the recovery profile page, through which the user can upload the configuration file to the switch. Click the Browse button to select the directory path of the uploaded configuration file on the PC. Click the upload button to upload the configuration file. The suffix of the configuration file must be *. CFG. Before the transfer result page returns, please do not click on other pages or restart the switch; otherwise, it will cause file transfer failure and system crash.



Figure 47 restore profile page

(4) Software upgrade page

Figure 48 is the software upgrade page, through which users can upload image files to the switch. Click the Browse button to select the directory path of the uploaded image file on the PC. Click the upload button to upload the image file. It must be provided by the manufacturer and the suffix of the file name must be *. Img. Before the transfer result page returns, please do not click on other pages or restart the switch; otherwise, it will cause file transfer failure and system crash.



Figure 48 software upgrade page

(5) Restore factory configuration page

Figure 49 shows the restore factory configuration page. This page allows the user to delete the configuration file in flash to restore to the factory configuration. Click the restore factory configuration button, a dialog box will pop up to prompt the user whether to confirm. After restoring the factory configuration, the exchange machine will restart automatically to make the factory configuration effective. Please use the default IP address and password

when logging in next time.



Figure 49 restore factory configuration page

(5) Restart page

Figure 50 is the restart page through which the user restarts the switch. When you click the restart button, a dialog box will pop up to prompt the user whether to restart the switch. If so, press the OK key, otherwise press the cancel key. You will no longer be able to open web pages when you restart.

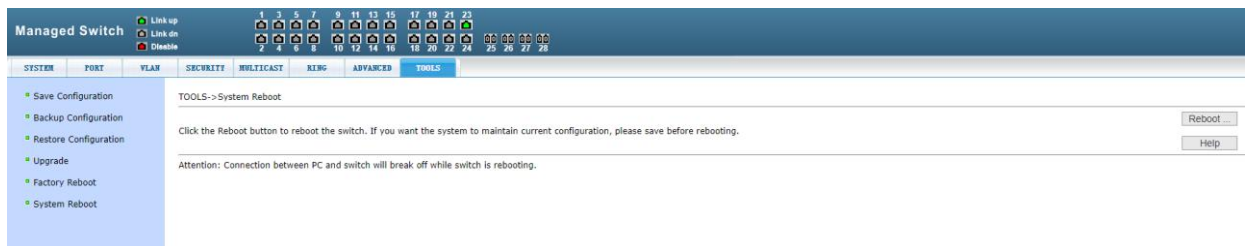


Figure 50 restart page