

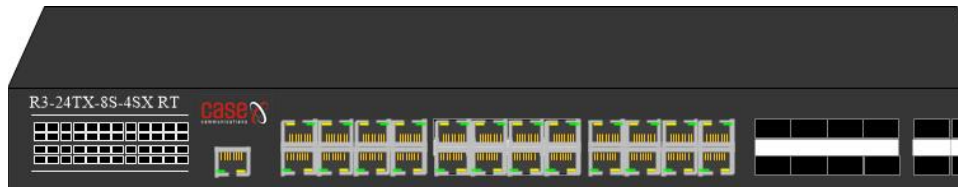
RT Series Switches

Web User Guide

R3 8TX 24S 4SX RT



R3 24TX 8S 4SX RT



This page left blank intentionally

Contents

1	Web Configuration Manual	1
1.1	Introduction to the web configurator	1
1.2	WEB system requirements for a PC and browser	1
1.3	Logging in to the browsing session	2
1.4	The Initial Logon Web Page	2
1.5	Introduction to page buttons	3
1.6	Error messages	3
1.7	Entry field	4
2	WEB Page introduction	5
2.1	System Configuration	5
2.2	IP address configuration	6
2.3	User Management Configuration	6
2.4	SNMP common configuration page	6
2.4	SNMP Trap Configuration	7
2.5	Log Information	7
3	Port Configuration	8
3.1	Basic port configuration	8
3.2	Port Statistics	8
3.3	Port storm suppression page	9
3.4	Port speed limit page	9
3.5	Link aggregation configuration page	10
3.6	Port mirroring configuration page	10
4	VLAN Configuration	11
4.1	VLAN	11
4.2	Access port configuration	11
4.3	Trunk port configuration	12
4.4	Hybrid port configuration	12
5	Security	18
5.1	MAC Configuration	18
5.2	MAC Address Automatic Binding	18
5.3	MAC Address filtering configuration	19
5.4	ACL Configuration	19
5.5	Expand IP Group ACL	20
5.6	Mac IP group ACL	20
5.7	MAC ARP group ACL	21
5.8	Port Application ACL	22
5.9	ACL Configuration Information	22
5.10	AAA Global Configuration	22

5.11	AAA Port configuration	23
5.12	AAA User information Menu	24
5.13	Local management security configuration	24
6	Multicast	25
6.1	IGMP	25
6.2	Multicast group information	25
7	Resilience Application	26
7.1	Spanning tree configuration	26
7.2	Spanning Tree Port configuration	26
7.3	ERPS Pre-defined configuration	27
7.4	ERPS Instance Configuration	27
7.5	ERPS Ring Configuration	28
7.6	ERPS Ring Information	29
7.7	ERPS Ring Example	30
8	IP Basic Configuration	32
8.1	VLAN Port Configuration	32
8.2	ARP Configuration	32
8.3	Static route configuration	33
9	System Tools	34
9.1	Saved configuration	34
9.2	Backup profile	34
9.3	Restore Profile	35
9.4	Software upgrade	35
9.5	Restore factory configuration	35
9.6	Restart	36

1. Web Configuration Manual

This manual describes the web pages that are used to configure switch.

This manual only gives a brief introduction to the operation of each web page, Please refer to the Installation and CLI Manual for additional information. This manual includes the following contents:

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

1.1. Introduction to the web configurator

This switch Web interface provides 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 S34024TR + 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.

1.2. WEB system requirements for a PC and browser

The system requirements to run the web browser for managing the switch are shown in the table below:

Hardware and software	System requirements
CPU	Pentium 586 above
Memory	128MB above
Resolution ratio	1024x768 above
Colour	256 colour above
Browser	Internet Explorer 8.0 Above or Firefox or Google Chrome or Opera...
Operating system	Microsoft® Windows XP® and up to Windows 11®, Linux, Unix operating system

Note:

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

1.3. Logging in to the browsing session

The user needs to confirm their IP Address 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.

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 interface. The default user is ' root' and the password is 'case'

Figure 1 login page of web browsing session

1.4. The Initial Logon Web Page

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

Figure 1.4

System Information	
Product Description	R3-8TX-24S-45X-RT
System Object ID	1.3.6.1.4.1.12284.103
Hardware Version	1.0
Firmware Version	3.5.7
Base MAC Address	00:82:44:1d:be:02
Serial Number	aaaa
CPU Utilization	14%
Memory Utilization	40%
System Uptime	00-Days 04-Hours 36-Minutes 10-Seconds
System Clock	2022/06/01 16:35:42 (Format: YYYY/MM/DD HH:MM:SS)

Title Page

Used to display the real-time port status, as shown in the figure below The green light indicates that the port is connected.

The grey light indicates that the port is disconnected.

The red light indicates that the port is closed

Category navigation page

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

Menu page

Display the menu selected by the user from the 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.

1.5. Introduction to page buttons

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

Table 2 Introduction to the buttons	
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

1.6. Error messages

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

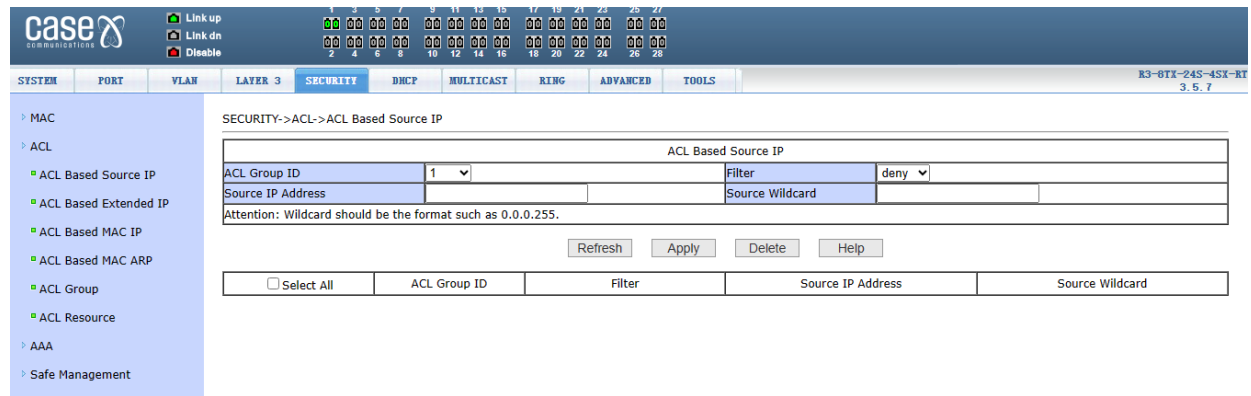


Figure 4 error message page

1.7. 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 1.7 Entry Field Page



The screenshot displays the RT Series Web Manual interface for configuring ACL Based Source IP. The top navigation bar includes tabs for SYSTEM, PORT, VLAN, LAYER 3, SECURITY, DHCP, MULTICAST, RING, ADVANCED, and TOOLS. The left sidebar shows a tree view with categories like MAC, ACL, and AAA. The main content area is titled 'SECURITY->ACL->ACL Based Source IP' and contains a form for configuring ACL Based Source IP. The form includes fields for ACL Group ID (set to 1), Filter (set to deny), Source IP Address, and Source Wildcard. Below the form are buttons for Refresh, Apply, Delete, and Help. At the bottom, there is a table with columns for Select All, ACL Group ID, Filter, Source IP Address, and Source Wildcard.

Select All	ACL Group ID	Filter	Source IP Address	Source Wildcard
<input type="checkbox"/>				

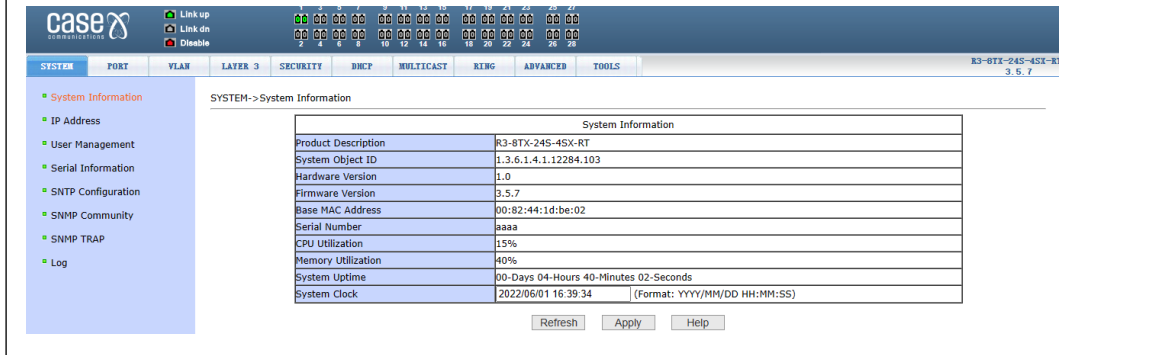
2. WEB Page introduction

The RT Series of Switches web pages are organized into groups, each group includes one or more web pages. These are described below

2.1. System Configuration

System information page

Figure 2.1a System Configuration



System Information	
Product Description	R3-8TX-24S-4SX-RT
System Object ID	1.3.6.1.4.1.12284.103
Hardware Version	1.0
Firmware Version	3.5.7
Base MAC Address	00:82:44:1d:be:02
Serial Number	aaaa
CPU Utilization	15%
Memory Utilization	40%
System Uptime	00-Days 04-Hours 40-Minutes 02-Seconds
System Clock	2022/06/01 16:39:34 (Format: YYYY/MM/DD HH:MM:SS)

Refresh Apply Help

The system information configuration page allows users to 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 Boot-Rom version information: the current Boot Rom version of the switch Reference MAC address: the base MAC address of the switch

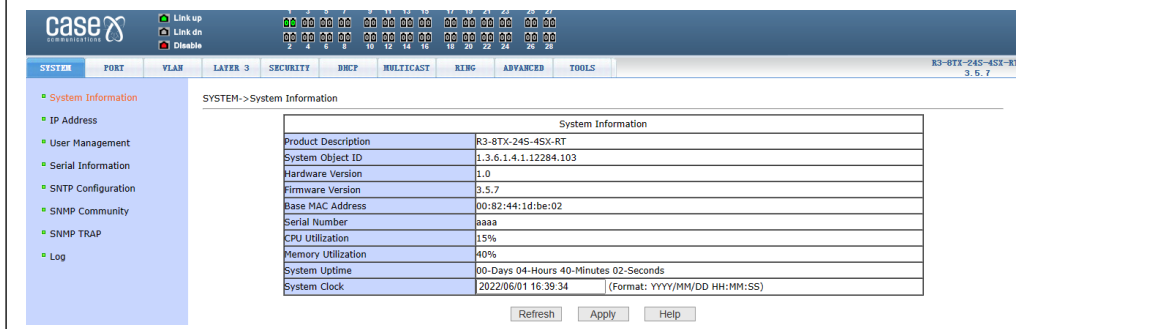
Serial number: the serial number of the switch

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

System start up time: the time the switch has been powered up

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

Figure 2.1b System Information



System Information	
Product Description	R3-8TX-24S-4SX-RT
System Object ID	1.3.6.1.4.1.12284.103
Hardware Version	1.0
Firmware Version	3.5.7
Base MAC Address	00:82:44:1d:be:02
Serial Number	aaaa
CPU Utilization	15%
Memory Utilization	40%
System Uptime	00-Days 04-Hours 40-Minutes 02-Seconds
System Clock	2022/06/01 16:39:34 (Format: YYYY/MM/DD HH:MM:SS)

Refresh Apply Help

2.2. IP address configuration

Figure 2.2 IP Address Configuration

SYSTEM- > IP Address

Admin VLAN	1
IP Address	192.168.42.240
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
MAC Address	00:82:44:1d:be:02

Attention: Please configure carefully. If WEB connection is interrupted after the configuration, please try establish a new connection with the new IP Address.

Refresh Apply Help

Figure 2.3 above shows 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.

2.3. User Management Configuration

Figure 2.3 – Managers configuration page

SYSTEM- > User Management

User Name	
User Level	normal
Password	
Confirm Password	

Attention: User name and password are case sensitive.

Refresh Apply Help

Item	User Name	User Level	Operation
1	admin	privilege	delete

Figure 2.3 above is used to configure the management information for the switch. The default user of the switch is admin, which cannot be deleted, and the default password is case, however the password can be modified.

2.4. SNMP common configuration page

Figure 2.4 SNMP Configuration

SYSTEM- > SNMP Community

Community Name	
Read and Write Purview	read-write

Refresh Apply Help

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

Figure 2.4 above shows the SNMP common configuration page, which allows the user to configure the name and read-write permissions of the SNMP Parameters 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.

2.4. SNMP Trap Configuration

Figure 2.5 SNMP Trap Configuration

Item	TRAP Name	Server IP Address	SNMP Version	Operation
------	-----------	-------------------	--------------	-----------

Figure 2.5 shows the SNMP trap configuration page, which allows users to configure the IP address of the workstation or network management system 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 entering and submitting the information, if the configuration is successful, the SNMP trap function will work. In the event of an SNMP Trap for example a link up or link down, the switch will automatically send trap packets to the target address (usually a Network Management system such as CaseView).

2.5. Log Information

Figure 2.6 Log Information

Priority	Log	Refresh	Help
----------	-----	---------	------

Figure 2.6 above shows 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.

3. Port Configuration

3.1. Basic port configuration

Figure 3.1 Basic port configuration

PORT->Basic Configuration

Basic Configuration						
Selected Port(s)						
Enable/Disable	<input type="checkbox"/>					
Speed/Duplex	<input type="checkbox"/>					
Flow Control	<input type="checkbox"/>					
Jumbo Frame Bytes	1522	(1522-12288)				

Refresh Apply Help

<input type="checkbox"/> Select All	Port	Link Status	Speed/Duplex	Enable/Disable	Flow Control	Jumbo Frame Bytes
<input type="checkbox"/>	1	100M/FULL	AUTO/AUTO	Enable	Disable	1522
<input type="checkbox"/>	2	---	AUTO/AUTO	Enable	Disable	1522
<input type="checkbox"/>	3	---	AUTO/AUTO	Enable	Disable	1522
<input type="checkbox"/>	4	---	AUTO/AUTO	Enable	Disable	1522
<input type="checkbox"/>	5	---	AUTO/AUTO	Enable	Disable	1522
<input type="checkbox"/>	6	---	AUTO/AUTO	Enable	Disable	1522
<input type="checkbox"/>	7	---	AUTO/AUTO	Enable	Disable	1522

Figure 3.1 above shows the basic port 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.

3.2 Port Statistics

Figure 3.2 Port Statistics

PORT->Port Statistics

Port	Send Packets Num	Send Octets Num	Received Packets Num	Received Octets Num	Error Packets Num	Discard Packets Num
1	22871	4172434	104612	14551818	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

Figure 3.2 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.

3.3 Port storm suppression page

Figure 3.3 Port storm suppression

PORT->Storm Control

Storm Control

Selected Port(s)

Broadcast Suppression

Multicast Suppression

DLF Suppression

Ratelimit (1-1024000 kbps)

Refresh Apply Help

<input type="checkbox"/> Select All	Port	Broadcast Suppression	Multicast Suppression	DLF Suppression	Ratelimit(kbps)
<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

Figure 3.3 above 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 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.

3.4 Port speed limit page

Figure 3.4 Port speed limiting

PORT->Port Rate

Port Rate

Selected Port(s)

Receive Packets Rate Control

Send Packets Rate Control

Refresh Apply Help

<input type="checkbox"/> 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	---	---

Figure 3.4 above 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 ticking the box. The speed limit range is 1-1024000, and the unit is kbits. If the ticked box is un ticked, the speed limit will not be limited. The list on the page shows the configuration information for all ports.

3.5

Link aggregation configuration page

Figure 3.5 – Link aggregation

Figure 3.5 above 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.

3.6

Port mirroring configuration page

Figure 3.6 – Port Mirroring

Figure 3.6 above shows the port mirroring configuration page, which allows users to configure port mirroring. Port mirroring listens to the output and input packets of the monitored port and sends them to the port undertaking the listening called 'The Mirror Port'. Only one mirror port can be selected, while multiple listening (mirrored) output ports and listening (mirrored) input ports can be selected. When configuring, select a mirror (listening) port first. Selecting "no mirroring" means cancelling 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 you can 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.

4. VLAN Configuration

4.1. VLAN Configuration

Figure 4.1 VLAN Configuration page

VLAN->VLAN Configuration

VLAN ID: (2-4094), format: 2-4 or 3,5,7

[U] untagged member of VLAN; [T] tagged member of VLAN
S static VLAN; D dynamic VLAN; S/D static and dynamic VLAN

VLAN ID	VLAN ID	Member	Operation
1	S	[U] : 1-28 [T] :	---

Page 1 / 1

Previous Next

Figure 4.1 above shows the VLAN configuration page. This page allows users to create VLANs and display all VLAN information.

To create a new VLAN ID entry, enter the required VLAN ID in the VLAN ID section of the page, this is a number ranging from 2 to 4094, and then click Apply. The switch creates VLAN1 by default, and VLAN1 cannot be deleted.

To delete a VLAN, click the corresponding Delete link in the VLAN list. Click the “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. It is possible for Trunk (Tagged) ports to be members of multiple VLANs, but Access (Untagged) ports are a member of a single 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 (Trunk port)
- U Untagged The port is an untagged member of this VLAN (Access port)

Note that this is an overview list of the VLAN and the member ports, configuring a port to be a member of a VLAN is made on other pages.

4.2. Access port configuration

Figure 4.2 Access Port Configuration page

VLAN->Access Port

Port

VLAN

1 3 5 7 9 11 13 15 17 19 21 23 25 27
2 4 6 8 10 12 14 16 18 20 22 24 26 28

Refresh Apply Help

Figure 4.2 above shows the Access Port configuration page, showing and configuring the port Access mode and VLAN.

When VLAN Access ports are untagged, that means that packets leaving the port will not have a VLAN tag attached and the packets coming into the port will not have a VLAN tag and the switch will add the relevant VLAN tag to the packet.

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 each port can only be set to a single VLAN ID, e.g. Port 1 is set to be on VLAN1 and if it is set to be on VLAN10 then it is no longer on VLAN1.

4.3. Trunk port configuration

Figure 4.3 Trunk Port Configuration Page

The screenshot shows the 'VLAN->Trunk Port' configuration page. The sidebar on the left has a blue background and contains the following menu items: SYSTEM, PORT, VLAN (highlighted), LAYER 3, SECURITY, DHCP, MULTICAST, RING, ADVANCED, and TOOLS. Under the 'VLAN' menu, there are sub-items: VLAN Configuration, Access Port, Trunk Port (highlighted in red), Hybrid Port, and GVRP Configuration. The main content area is titled 'VLAN->Trunk Port'. It contains a table with 28 columns representing VLANs (1 to 28) and a 'Port' column. Below the table, there are input fields for 'Default VLAN' and 'tagged VLAN (All)'.

Figure 4.3 above 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 the section 4.2 on access port configuration 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.

4.4. Hybrid port configuration

Figure 4.4 Hybrid port Configuration

The screenshot shows the 'VLAN->Hybrid Port' configuration page. The sidebar on the left has a blue background and contains the following menu items: SYSTEM, PORT, VLAN (highlighted), LAYER 3, SECURITY, DHCP, MULTICAST, RING, ADVANCED, and TOOLS. Under the 'VLAN' menu, there are sub-items: VLAN Configuration, Access Port, Trunk Port, Hybrid Port (highlighted in red), and GVRP Configuration. The main content area is titled 'VLAN->Hybrid Port'. It contains a table with 28 columns representing VLANs (1 to 28) and a 'Port' column. Below the table, there are input fields for 'Default VLAN', 'Tagged VLAN (All)', and 'Untagged VLAN (All)'.

Figure 4.4 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 the section 4.2 on access port configuration 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.

4.5. VLAN Configuration Examples

This example sets two Trunk ports carrying VLAN tagged traffic on through the network, 8 access ports set for VLAN1, 8 Access ports set for VLAN10, 8 Access ports set for VLAN20 and 2 Hybrid ports.

Note that if you set a port to be one type of VLAN port, e.g. an Access port, and later set it to be a different VLAN port type like Trunk then the original setting will be overwritten.

4.5.1 Configuring VLAN IDs

On the VLAN – VLAN Configuration page type in the required VLAN in the VLAN ID section as shown below, in this example that is 10 and click Apply

Figure 4.5.1a Configuring VLAN IDs

VLAN->VLAN Configuration

VLAN	
VLAN ID	10 (2-4094), format: 2-4 or 3,5,7

Refresh Apply Delete All Help

Repeat this with VLAN ID 20, after which the screen will show VLAN IDs 10 and 20 without any ports as members, as shown below:

Figure 4.5.1b Configured VLAN IDs

VLAN->VLAN Configuration

VLAN	
VLAN ID	(2-4094), format: 2-4 or 3,5,7

Refresh Apply Delete All Help

[U] untagged member of VLAN; [T] tagged member of VLAN
S static VLAN; D dynamic VLAN; S[D] static and dynamic VLAN

VLAN ID	VLAN ID	Member	Operation
1	S	[U] : 1-28 [T] :	---
10	S	[U] : [T] :	Delete
20	S	[U] : [T] :	Delete

Page 1 / 1

Previous Next

4.5.2 Configuring Access VLANs

On the VLAN – Access Port page select Port 9 (it will then be highlighted with a green square around the port) and then VLAN 10 and then click Apply, as shown below. Repeat this for ports 10 to 16

Figure 4.5.2a Configuring Access VLANs

VLAN->Access Port

Port	<div> <div>1</div><div>3</div><div>5</div><div>7</div><div>9</div><div>11</div><div>13</div><div>15</div><div>17</div><div>19</div><div>21</div><div>23</div><div>25</div><div>27</div> </div> <div> <div>2</div><div>4</div><div>6</div><div>8</div><div>10</div><div>12</div><div>14</div><div>16</div><div>18</div><div>20</div><div>22</div><div>24</div><div>26</div><div>28</div> </div>
VLAN	<input type="checkbox"/> 1 <input checked="" type="checkbox"/> 10 <input type="checkbox"/> 20

Refresh Apply Help

Then select Port 17 and then VLAN 20 and then click Apply, as shown below. Repeat this for ports 18 to 24.

Figure 4.5.2b Configured Access VLANs

VLAN->Access Port

Port	<div> <div>1</div><div>3</div><div>5</div><div>7</div><div>9</div><div>11</div><div>13</div><div>15</div><div>17</div><div>19</div><div>21</div><div>23</div><div>25</div><div>27</div> </div> <div> <div>2</div><div>4</div><div>6</div><div>8</div><div>10</div><div>12</div><div>14</div><div>16</div><div>18</div><div>20</div><div>22</div><div>24</div><div>26</div><div>28</div> </div>
VLAN	<input type="checkbox"/> 1 <input type="checkbox"/> 10 <input checked="" type="checkbox"/> 20

Refresh Apply Help

4.5.3 Configuring Trunk VLANs

On the VLAN – Trunk Port page select Port 27 (it will then be highlighted with a green square) and set Default VLAN to 1 and Tagged VLAN to both VLAN10 and VLAN20, so shown below. Repeat this for port 28.

Figure 4.5.3 Configuring Trunk VLANs

VLAN->Trunk Port

Port	<div> <div>1</div><div>3</div><div>5</div><div>7</div><div>9</div><div>11</div><div>13</div><div>15</div><div>17</div><div>19</div><div>21</div><div>23</div><div>25</div><div>27</div> </div> <div> <div>2</div><div>4</div><div>6</div><div>8</div><div>10</div><div>12</div><div>14</div><div>16</div><div>18</div><div>20</div><div>22</div><div>24</div><div>26</div><div>28</div> </div>
Default VLAN	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 10 <input type="checkbox"/> 20
tagged VLAN (<input type="checkbox"/> All)	<input type="checkbox"/> 1 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 20

Refresh Apply Help

Note that a Default VLAN **must** be configured. In this example we are using VLAN1 as the default, other network may use a different VLAN ID.

4.5.4 Configuring Hybrid VLANs

On the VLAN – Hybrid Port page select Port 25 and set the Default VLAN to 1, set Tagged VLAN as 10 only and then set Untagged VLAN as 20 only as shown below. Then click Apply.

Figure 4.5.4a Configuring Hybrid VLANs

VLAN->Hybrid Port

Port	<div> 1 3 5 7 9 11 13 15 17 19 21 23 25 27 2 4 6 8 10 12 14 16 18 20 22 24 26 28 </div>
Default VLAN	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 10 <input type="checkbox"/> 20
Tagged VLAN (<input type="checkbox"/> All)	<input type="checkbox"/> 1 <input checked="" type="checkbox"/> 10 <input type="checkbox"/> 20
Untagged VLAN (<input type="checkbox"/> All)	<input type="checkbox"/> 1 <input type="checkbox"/> 10 <input checked="" type="checkbox"/> 20

Refresh Apply Help

The select Port 26 and set Default VLAN to 1, set Tagged VLAN as 20 only and then set Untagged VLAN as 10 only as shown below. Then click Apply.

Figure 4.5.4b Configuring Hybrid VLANs

VLAN->Hybrid Port

Port	<div> 1 3 5 7 9 11 13 15 17 19 21 23 25 27 2 4 6 8 10 12 14 16 18 20 22 24 26 28 </div>
Default VLAN	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 10 <input type="checkbox"/> 20
Tagged VLAN (<input type="checkbox"/> All)	<input type="checkbox"/> 1 <input type="checkbox"/> 10 <input checked="" type="checkbox"/> 20
Untagged VLAN (<input type="checkbox"/> All)	<input type="checkbox"/> 1 <input checked="" type="checkbox"/> 10 <input type="checkbox"/> 20

Refresh Apply Help

Note that a Default VLAN must be set.

4.5.5 View VLAN Settings

On the VLAN – VLAN Configuration page the previously set VLAN settings can be viewed as seen below:

Figure 4.5.5 View VLAN Settings

VLAN->VLAN Configuration

VLAN			
VLAN ID		(2-4094), format: 2-4 or 3,5,7	

Refresh Apply Delete All Help

[U] untagged member of VLAN; [T] tagged member of VLAN
S static VLAN; D dynamic VLAN; S/D static and dynamic VLAN

VLAN ID	VLAN ID	Member	Operation
1	S	[U] : 1-8,25-28 [T] :	---
10	S	[U] : 9-16,26 [T] : 25,27-28	Delete
20	S	[U] : 17-25 [T] : 26-28	Delete

Page 1 / 1

Previous Next

This shows the following:

VLAN10 – Untagged on Ports 9 to 16 and 26 and also Tagged on Ports 25 and 27 to 28.

VLAN20 – Untagged on Ports 17 to 25 and also Tagged on Ports 26 to 28.

VLAN1 – Untagged on Ports 1 to 8 and also 25 to 28.

4.5.6 Adding IP Address to a VLAN

Sometimes you may need to add an IP Address to a VLAN, for example if you use VLAN10 in the network as a management VLAN.

Note that each VLAN need to have a unique IP address within a unique IP range. For example VLAN IP Address is 192.168.16.1/24 so VLAN10 IP address cannot be 192.168.16.1/24 or anything in the 192.168.16.XXX/24 range. VLAN10 could be IP Address 192.168.17.1/24 as this is in a separate IP range.

After configuring the VLANs, then the IP address for the VLAN, if required, can be configured on the Layer 3 – IP Basic – VLAN Interface page.

Figure 4.5.6a Adding IP Address to VLAN

LAYER 3->IP Basic->VLAN Interface

VLAN Interface			
VLAN ID			
IP Address / Subnet Prefix		(format: 192.168.0.1/24)	

Attention: Please configure carefully. If WEB connection is interrupted after the configuration, please try establish a new connection with the new IP Address.

Refresh Apply Help

VLAN ID	IP Address / Subnet Prefix	MAC Address	Operation
1	192.168.42.200/24	0000.6e03.0174	Delete

To set a VLAN IP Address enter the VLAN ID and then the IP Address with the CIDR Subnet Prefix (e.g. Subnet Mask 255.255.255.0 has the prefix /24)

For this example we type VLAN ID as 10 and IP Address as 10.1.1.1/24

Figure 4.5.6b Adding IP Address to VLAN

VLAN Interface	
VLAN ID	10
IP Address / Subnet Prefix	10.1.1.1/24 (format: 192.168.0.1/24)

Then press Apply.

Figure 4.5.6c VLAN IP Address summary

LAYER 3->IP Basic->VLAN Interface

VLAN Interface	
VLAN ID	
IP Address / Subnet Prefix	(format: 192.168.0.1/24)

Attention: Please configure carefully. If WEB connection is interrupted after the configuration, please try establish a new connection with the new IP Address.

Refresh Apply Help

VLAN ID	IP Address / Subnet Prefix	MAC Address	Operation
1	192.168.42.200/24	0000.6e03.0174	Delete
10	10.1.1.1/24	0000.6e03.0174	Delete

The Layer 3 – IP Basic – VLAN Interface screen will now show the VLAN10 tag has been added.

Note that the Management VLAN must not be deleted using this screen, access to management of the switch may be lost if this is done. In this example the Management VLAN is the default VLAN1.

4.5.6 How this example works

Equipment is connected to Port 9 and is configured to not use VLAN, i.e. is Untagged. Packets from this equipment arrive on Port 9 and the switch recognizes that the packets are Untagged and add a VLAN10 tag. This packet then goes to its destination.

If the destination is Port 10 of this switch then the switch will remove the VLAN10 tag and send the packet out on Port 10 as Untagged. If the destination is elsewhere on the network then it will be sent out of the switch on the relevant port, assuming that is Port 28 then the packet will be sent out of Port 28 as a Tagged packet with the VLAN10 tag still attached.

If a packet arrives on Port 28 destined for the equipment connected to Port 9, then the packet will have arrived with the VLAN10 tag already attached. The switch will remove the VLAN10 tag and send the packet out on Port 9 to the equipment.

Equipment is connected to Port 25 and is configured to use VLAN and Tagged with VLAN10. This equipment will send packets out with VLAN10 tag already attached. The switch will receive the packet and pass it onto its destination without modifying the VLAN 10 tag already attached to it.

All ports work in a similar way as described above. Each VLAN will be separate, so equipment connected to Port 9 on VLAN10 cannot communicate to equipment connected to Port 17 on VLAN20.

5 Security Configuration

5.1 MAC Configuration

Figure 5.1 MAC Configuration – Manual Binding of a Mac Address

Figure 5.1 above shows the MAC configuration page. This page is used to bind a 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.

5.2 MAC Address Automatic Binding

Figure 5.2 MAC Address Automatic Binding

Figure 5.2 above shows the MAC address auto binding page. This page is used to allow the switch to auto bind the 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.

5.3 MAC Address filtering configuration

Figure 5.3 MAC Address Filtering Configuration page

SYSTEM PORT VLAN LAYER 3 SECURITY DHCP MULTICAST RING ADVANCED TOOLS

MAC

- MAC Bind
- MAC auto Bind
- MAC Filter
- MAC Table

ACL

AAA

Safe Management

SECURITY->MAC->MAC Filter

Port

1	3	5	7	9	11	13	15	17	19	21	23	25	27
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Filter Information

MAC Address (Format: HHHH.HHHH.HHHH)

VLAN ID (1-4094)

Refresh Apply Delete Help

List MAC filtered on the selected port

☐ Select All

MAC Address	VLAN ID
-------------	---------

Figure 5.3 above 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.

5.4 ACL Configuration

Figure 5.4 ACL Configuration page

SYSTEM PORT VLAN LAYER 3 SECURITY DHCP MULTICAST RING ADVANCED TOOLS

MAC

- ACL
- ACL Based Source IP
- ACL Based Extended IP
- ACL Based MAC IP
- ACL Based MAC ARP
- ACL Group
- ACL Resource

SECURITY->ACL->ACL Based Source IP

ACL Based Source IP

ACL Group ID	1	Filter	deny
Source IP Address		Source Wildcard	

Attention: Wildcard should be the format such as 0.0.0.255.

Refresh Apply Delete Help

☐ Select All

ACL Group ID	Filter	Source IP Address	Source Wildcard
--------------	--------	-------------------	-----------------

Figure 5.4 above is the ACL page of a 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).

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.

5.5 Expand IP Group ACL

Figure 5.5 Expanded IP Group ACL Page

SYSTEM PORT VLAN LAYER 3 SECURITY DHCP MULTICAST RING ADVANCED TOOLS 3.5.7

> MAC

> ACL

- ACL Based Source IP
- ACL Based Extended IP
- ACL Based MAC IP
- ACL Based MAC ARP
- ACL Group
- ACL Resource

> AAA

SECURITY->ACL->ACL Based Extended IP

ACL Based Extended IP

ACL Group IP	100	Filter	deny
Source IP		Source Wildcard	
Destination IP		Destination Wildcard	
Protocol Type		Source Port	
Destination Port		TCP Flag	<input type="checkbox"/> fin <input type="checkbox"/> syn <input type="checkbox"/> rst <input type="checkbox"/> psh <input type="checkbox"/> ack <input type="checkbox"/> urg

Attention: Wildcard should be the format such as 0.0.0.255.

Refresh Apply Delete Help

<input type="checkbox"/> All	Group ID	Filter	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol Type	Source Port	Destination Port	TCP Flag
------------------------------	----------	--------	-----------	-----------------	----------------	----------------------	---------------	-------------	------------------	----------

Figure 5.5 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.

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.

5.6 Mac IP group ACL

Figure 5.6 MAC IP Group ACL Page

SYSTEM PORT VLAN LAYER 3 SECURITY DHCP MULTICAST RING ADVANCED TOOLS 3.5.7

> MAC

> ACL

- ACL Based Source IP
- ACL Based Extended IP
- ACL Based MAC IP
- ACL Based MAC ARP
- ACL Group
- ACL Resource

> AAA

> Safe Management

SECURITY->ACL->ACL Based MAC IP

ACL Based MAC IP

ACL Group ID	700	Filter	deny
Source MAC		Source MAC Wildcard	
Destination MAC		Destination MAC Wildcard	
Source IP		Source IP Wildcard	
Destination IP		Destination IP Wildcard	

Attention: IP Wildcard should be the format such as 0.0.0.255. MAC Wildcard format should be HHHH.HHHH.HHHH

Refresh Apply Delete Help

<input type="checkbox"/> All	Group ID	Filter	Source MAC	Source MAC Wildcard	Destination MAC	Destination MAC Wildcard	Source IP	Source IP Wildcard	Destination IP	Destination IP Wildcard
------------------------------	----------	--------	------------	---------------------	-----------------	--------------------------	-----------	--------------------	----------------	-------------------------

Figure 5.6 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).

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.

5.7 MAC ARP group ACL

Figure 5.7 MAC ARP Group ACL Page.

Figure 5.7 shows the ACL page of the MAC ARP group. The page includes a navigation menu on the left with options like MAC, ACL, and ACL Based Source IP. The main content area is titled "SECURITY->ACL->ACL Based MAC ARP" and contains a table for configuring ACL rules. The table has columns for ACL Group ID, Filter, Sender MAC, Sender MAC Wildcard, Sender IP, and Sender IP Wildcard. A "Filter" dropdown is set to "deny". Below the table are buttons for "Refresh", "Apply", "Delete", and "Help". At the bottom, there is a table with a "Select All" checkbox and columns for Group ID, Filter, Sender MAC, Sender MAC Wildcard, Sender IP, and Sender IP Wildcard.

Figure 5.7 is the ACL page of the 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)

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.

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.

5.8 Port Application ACL

Figure 5.8 Port Application ACL Page

Port	ACL Group configured	Operation	ACL Group applied
1		<div>Apply =></div> <div><= Delete</div> <div>Refresh</div> <div>Help</div>	
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

Figure 5.8 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 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.

5.9 ACL Configuration Information

Figure 5.9 ACL Configuration Information Page

ACL Resource

Figure 5.9 is the ACL configuration information page, which shows all the rules and reference information configured in the current ACL.

5.10 AAA Global Configuration

Figure 5.10 AAA Global Configuration

AAA Global Configuration	
802.1x	disable
Reauthentication	disable
Reauthentication Period	3600 (seconds)
RADIUS Server IP	0.0.0.0
Alternative RADIUS Server IP	0.0.0.0
Share Key	
Accounting Status	enable

Figure 5.10 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 server.
- Whether to start billing or not, it is started by default. When doing authentication billing, it is generally required to start charging.

5.11 AAA Port configuration

5.11 AAA Port configuration page

SYSTEM PORT VLAN LAYER 3 SECURITY DHCP MULTICAST RING ADVANCED TOOLS

SECURITY->AAA->AAA Port Configuration

AAA Port Configuration

Selected Port(s)

Port Mode Force-UnAuthorized

Support Host Num 256 (1-256)

Refresh Apply Help

<input type="checkbox"/> Select All	Port	Port Mode	Support Host Num
<input type="checkbox"/>	1	N/A	256
<input type="checkbox"/>	2	N/A	256
<input type="checkbox"/>	3	N/A	256
<input type="checkbox"/>	4	N/A	256
<input type="checkbox"/>	5	N/A	256
<input type="checkbox"/>	6	N/A	256
<input type="checkbox"/>	7	N/A	256

Figure 5.11 above 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.

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.

5.12 AAA User information Menu

Figure 5.12 AAA User Information page

SYSTEM PORT VLAN LAYER 3 SECURITY DHCP MULTICAST RING ADVANCED TOOLS

SECURITY->AAA->AAA User Information

AAA User Information					
User name	MAC Address	Authentication state	Authenticator state	Back-End state	Reauthentication state
<input type="button" value="Refresh"/> <input type="button" value="Help"/>					

Figure 5.12 above is the AAA user information page, through which users can view the status information of all users accessed under a certain port.

5.13 Local management security configuration

Figure 5.13 Local Management security configuration

SYSTEM PORT VLAN LAYER 3 SECURITY DHCP MULTICAST RING ADVANCED TOOLS

SECURITY->Safe Management->Safe Management

Safe Management

Service Type:

Management State:

ACL Group: (0-99, 0 means no ACL group is associated.)

Service Type	Management State	ACL Group	Number
HTTP	Enable	0	---
HTTPS	Enable	0	---
SNMP	Enable	0	---
TELNET	Enable	0	5
SSH	Enable	0	5

Figure 5.13 above 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, then these 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).

6 Multicast Configuration

6.1 IGMP Snooping Configuration

Figure 6.1 IGMP Snooping Configuration

IGMP SNOOPING Global Configuration	
Global IGMP SNOOPING	Disable
Unregistered Multicast Packets	Forward
Send Query Source IP	192.168.0.1
Send Query Version	V3

IGMP SNOOPING VLAN Configuration	
VLAN ID	VLAN 1
VLAN IGMP SNOOPING	Disable
Fast Leave	Disable
Fast Leave Timeout	300000 (>=0ms)
Query Membership Timeout	300000 (60000-300000ms)
Group Membership Timeout	400000 (>=0ms)
Querier	Disable
Query Interval	60000 (60000-125000ms)
Static Router Ports	(e.g : ge1/1,ge1/2)

Refresh Apply Help

Figure 6.1 above shows the IGMP snooping configuration page. Users can enable IGMP snooping through this page.

6.2 Multicast group information

Figure 6.2 Multicast group information page

VLAN ID	Address	Port
---------	---------	------

Refresh Help

Figure 6.2 above shows the multicast group information page, through which users can view IGMP snooping multicast information.

7 Resilience Applications

Note that only one of the following applications can be used on a switch, if ERPS (G.8032) is to be used then Spanning Treen cannot be enabled.

ERPS is widely known as G.8032 and is an ethernet ring protection that is now an adopted standard through the communication industry. ERPS is compatible with different models of Case switches.

ERPS sends administration packets over a configured VLAN that is only used for ERPS. An ERPS ring will have one link between the RPL Owner and the RPL Neighbour, this is known as the Ring Protection Link (RPL) Other links in the ring are known as Ring Links (RL)

With a working ring the RPL will be blocked by both the RPL Owner and RPL Neighbour so no traffic can pass over it. If the ring breaks for any reason administration packets are sent over the ERPS VLAN and the RPL Owner and RPL Neighbour both un block the RPL port to allow the ring to recover (bar the link or switch that has failed)

7.1 Spanning tree configuration

Figure 7.1 Spanning Tree Configuration

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

Figure 7.1 above shows the Spanning Tree global configuration page, through which users can configure the global Spanning Tree parameters. If Spanning Tree is to be used then enable Spanning Tree and set the required global values.

7.2 Spanning Tree Port configuration

Figure 7.2 Spanning Tree Port configuration page

Port Configuration							
Selected Port(s)							
Port Priority							
Path-Cost							
Force-Version	STP						
Portfast	disable						

<input type="checkbox"/> All	Item	Port	Priority	Path-Cost	Force-Version	Portfast	STP State
<input type="checkbox"/>	1	1	128	2000000	MSTP	disable	Forwarding
<input type="checkbox"/>	2	2	128	20000000	MSTP	disable	Blocked
<input type="checkbox"/>	3	3	128	20000000	MSTP	disable	Blocked
<input type="checkbox"/>	4	4	128	20000000	MSTP	disable	Blocked
<input type="checkbox"/>	5	5	128	20000000	MSTP	disable	Blocked
<input type="checkbox"/>	6	6	128	20000000	MSTP	disable	Blocked
<input type="checkbox"/>	7	7	128	20000000	MSTP	disable	Blocked
<input type="checkbox"/>	8	8	128	20000000	MSTP	disable	Blocked

Figure 7.2 above shows the port configuration page of Spanning Tree. Users can view the specific status of MSTP through this page. This page allow setting the required version of Spanning Tree as well as priority and patch cost for each port using Spanning Tree.

7.3 ERPS Pre-defined configuration

Figure 7.3 ERPS Configuration screen

Erps Predefined Configuration	
Status	disable ▼
Node Type	rpl-owner-node ▼

Refresh Apply Help

Figure 7.3 shows the ERPS predefined configuration page, which enables the ERPS predefined configuration. When this is enabled this presets certain settings for ERPS that cannot be modified, this makes it easier for someone unfamiliar with ERPS to configure a working ERPS mode.

Status - Enables a preset ERPS configuration.

Node Type - Configured the type of ERPS node this switch is, can be set to RPL Owner (effectively the Master node in the ring) or as a Ring Node.

7.4 ERPS Instance Configuration

Figure 7.4 ERPS Instance Configuration Page

ERPS Domain Configuration	
ERPS Domain	1 ▼
Domain Status	Not Created
Node Role	none-interconnection ▼

Refresh Apply Delete Help

Figure 7.4 above is the ERPS instance configuration page, which can be used to configure ERPS instances.

ERPS Domain – This is a drop down list of up to 8 separate ERPS configurations.

Domain Status – This shows if the instance has been created or not.

Node Role – This allows configuration of the ERPS instance to be Interconnection or Non-Interconnection. When set to Interconnection that shows that this switch is connected to more than 1 ERPS ring, the main ring and one or more sub-rings.

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.

7.5 ERPS Ring Configuration

Figure 7.5 ERPS Ring Config Page

ERPS Ring Configuration	
ERPS Ring	1
Ring Status	Not Created
Domain	
Ring Mode	
Node Mode	
Raps VLAN	0
Traffic VLAN	format: 2,4,6
RPL Port	
RL Port	
Revertive Behaviour	revertive
Hold-off Time	0 (<0-10000>, step 100, ms)
Guard Time	500 (<10-2000>, step 10, ms)
WTR Time	5 (<1-12>, min)
WTB Time	5 (<1-10>, sec)
Raps-send Time	5 (<1-10>, sec)
ERPS Ring Enable	disable
Forced Switch RPL Port	
Forced Switch RL Port	
Manual Switch Port	

Refresh Apply Delete Recover Help

Figure 7.5 above is the ERPS Ring configuration page, which can be used to configure each ERPS instance.

ERPS Ring – The Ring ID number (1 to 35)

Ring Status – Shows current status of the ring.

Domain – Drop down list showing the ERPS Domain this ERPS configuration belongs to.

Ring Mode – Selects if this ERPS ring is a Major Ring or a Sub-Ring. Note that Sub-Ring cannot be set for a switch with Node Role set to Non-Interconnection. A switch with Node Role set to Interconnection can have Ring Mode set to either Major Ring or Sub-Ring.

Node Mode – Selects RPL-Owner, RPL-Neighbour or Ring Node. RPL-Owner is the master of the ring and has an RPL port configured that is connected to the RPL-Neighbour.

RAPS VLAN – Sets the VLAN ID that will be used by the ERPS ring to send ERPS administration packets over. This VLAN must not be in use anywhere else in the ring network.

Traffic VLAN – Sets the VLAN IDs that can send packets over the ring, multiple VLANs can be set if the switch is configured to use more than one VLAN for traffic.

RPL Port – Set the port that will be used as the Ring Protection Link port and is connected to the RPL Owner or RPL Neighbour (if Node Mode is set to RPL Owner or RPL Neighbour) If Node Mode is set to Ring Node then the switch will treat this as a RL port. Note that both RPL and RL Ports need to be set and set to different ports)

RL Port – Set the port to be a Ring Link that will also be used for ERPS.

Revertive Behaviour – Sets Revertive or Non-Revertive mode. Revertive means that when failure recovery occurs the RPL Owner and Neighbour return the RPL port to blocking, this is standard operation. Non-Revertive means that on failure recovery the RPL port stays unblocked. It is recommended that Revertive is set.

Hold-off Time – This sets the delay between ERPS packets indicating a ring failure are received and the RPL Owner and Neighbour acting. Default and recommended value is 0.

Guard Time – After a failure has been recovered, the failed node will wait for the Guard Time duration to run before it sends the ERPS recover messages to the other switches in the ring. This gives the switch time to determine if the failure has genuinely recovered. Default is 500ms

WTR Time – The Wait To Restore Timer is used to verify that the ring recovery signal received by the RPL Owner and RPL Neighbour is not intermittent. This timer prevents the RPL from being continuously blocked and unblocked during a recovery period. If the recovery signal is received again the timer resets. Default value is 5S.

WTB Time – The Wait To Block timer is used to determine that there is no existing node failure condition before the RPL is blocked, i.e. the timer counts down and if another failure does not occur then the RPL is blocked after the timer finishes it's count. Default Value is 5S

RAPS-Send Time – This timer is used for the time between RAPS messages being sent showing a working ring. Default value is 5S.

ERPS Ring Enable – This setting enables or disables this instance of ERPS.

Forced Switch RPL Port – This option is always left blank. This is only used to force the specified port to be a blocked RPL port.

Force Switch RL Port – This option is always left blank. This is only used to force the specified port to be a RL port.

Manual Switch Port – This option is always left blank. This is only used to force a block on the specified port.

Refresh – refresh the screen to show the current configured options, note that any unsaved changes will be lost.

Apply – Apply the changes made to the configuration of this ERPS instance.

Delete – Delete the showed ERPS instance.

Recover - Force a recovery attempt for this ERPS instance. Note that button will only have an effect if there is an existing ring condition on this ERPS instance.

7.6 ERPS Ring Information

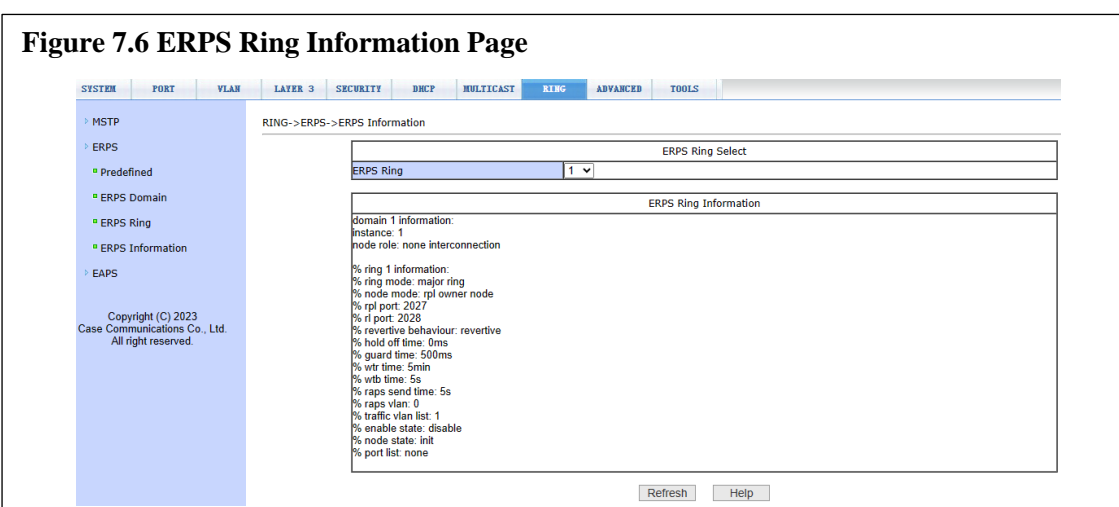


Figure 7.6 above is the ERPS Ring information page, which shows the current ERPS configuration.

7.7 ERPS Ring Example

Figure 7.7 ERPS Ring Example

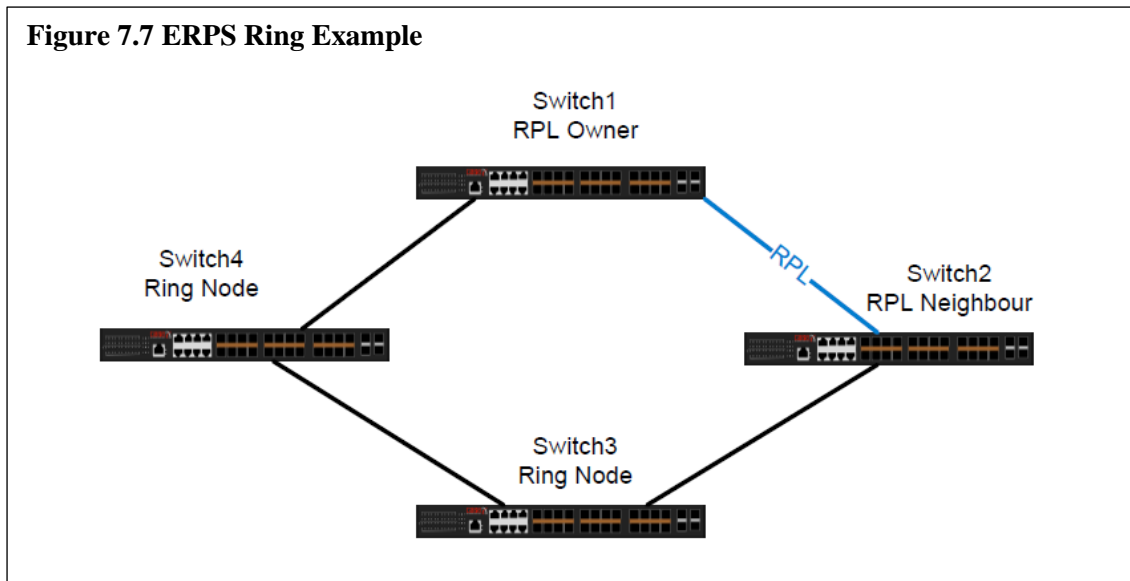


Figure 7.7 shows a network of 4 switches that are configured to operate an ERPS major ring. The ERPS configuration of the 4 switches are shown below, note that any option not shown is set to default value and only the ERPS configuration is shown.

7.7.1 Switch1 RPL Owner Configuration

ERPS Predefined

Status: Enable
Node Type: RPL-Owner Node

ERPS Domain

ERPS Domain: 1
Node Role: None-Interconnection

ERPS Ring

ERPS Ring: 1
Domain: 1
Ring Mode: Major-Ring
Node Mode: RPL-Owner
RAPS VLAN: 3001 – the VLAN to be used only for ERPS messages between switches in the ring
Traffic VLAN: 1 – all VLANs carrying traffic on the ring separated by a comma.
RPL Port: 27 – the port connected to the switch designated RPL Neighbour.
RL Port: 28 – port connected to a Ring Node switch.
Revertive Behaviour: Revertive
ERPS Ring Enable: Enable

7.7.2 Switch2 RPL Neighbour Configuration

ERPS Predefined

Status: Enable
Node Type: RPL-Neighbour Node

ERPS Domain

ERPS Domain: 1
Node Role: None-Interconnection

ERPS Ring

ERPS Ring: 1

Domain: 1

Ring Mode: Major-Ring

Node Mode: RPL-Neighbour

RAPS VLAN: 3001 – the VLAN to be used only for ERPS messages between switches in the ring

Traffic VLAN: 1 – all VLANs carrying traffic on the ring separated by a comma.

RPL Port: 28 – the port connected to the switch designated RPL Neighbour.

RL Port: 27 – port connected to a Ring Node switch.

Revertive Behaviour: Revertive

ERPS Ring Enable: Enable

Note: The RPL and RL port number – RPL port must always be between RPL Owner and RPL Neighbour.

7.7.3 Switch3 and Switch4 Ring Node Configuration

ERPS Predefined

Status: Enable

Node Type: Ring-Node

ERPS Domain

ERPS Domain: 1

Node Rol2: None-Interconnection

ERPS Ring

ERPS Ring: 1

Domain: 1

Ring Mode: Major-Ring

Node Mode: Ring-Node

RAPS VLAN: 3001 – the VLAN to be used only for ERPS messages between switches in the ring

Traffic VLAN: 1 – all VLANs carrying traffic on the ring separated by a comma.

RPL Port: 28

RL Port: 27

Revertive Behaviour: Revertive

ERPS Ring Enable: Enable

Note: The RPL and RL port must be configured on a Ring Node but can be connected to either another Ring Node switch, the RPL owner or RPL Neighbour.

7.7.4 ERPS Operation

With all nodes and connections between them working, the RPL port (in blue in the 7.7 drawing) will be blocked by the RPL Owner and RPL Neighbour. Traffic entering Switch2 destined to equipment connected to Switch1 will be passed through to Switch3, then Switch4 and onto Switch1.

If the connection between Switch3 and Switch4 fails, both switches send an ERPS message informing of the failure on the remaining ring port. Switch3 sends it to Switch2 and Switch4 send it to Switch1. Switch1 and Switch2 wait for a brief time to ensure that the failure is not intermittent and then unblock the RPL port. After that traffic can pass between Switch1 and Switch2 over this port.

When the connection between Switch3 and Switch4 recovers, both switches send an ERPS message informing of the recovery. Switch1 and Switch2 wait a brief amount of time to ensure that the recovery is not intermittent and then block the RPL port again.

8 IP Basic Configuration

8.1 VLAN Port Configuration

Figure 8.1 VLAN Port Configuration

SYSTEM PORT VLAN **LAYER 3** SECURITY DHCP MULTICAST RING ADVANCED TOOLS

> IP Basic

- VLAN Interface
- ARP Configuration
- Static Routes
- Routing Table

> RIP Configuration

> OSPF Configuration

> VRRP Configuration

LAYER 3->IP Basic->VLAN Interface

VLAN Interface

VLAN ID			
IP Address / Subnet Prefix	(format: 192.168.0.1/24)		

Attention: Please configure carefully. If WEB connection is interrupted after the configuration, please try establish a new connection with the new IP Address.

Refresh Apply Help

VLAN ID	IP Address / Subnet Prefix	MAC Address	Operation
1	192.168.42.240/24	0082.441d.be02	Delete

Figure 8.1 above shows 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. This switch has a VLAN1 interface by default, which cannot be deleted. A VLAN can only be configured with one interface.

8.2 ARP Configuration

Figure 8.2 ARP Configuration Page

SYSTEM PORT VLAN **LAYER 3** SECURITY DHCP MULTICAST RING ADVANCED TOOLS

> IP Basic

- VLAN Interface
- ARP Configuration
- Static Routes
- Routing Table

> RIP Configuration

> OSPF Configuration

> VRRP Configuration

LAYER 3->IP Basic->ARP Configuration

ARP Configuration

IP Address			
MAC Address	(format: HHHH.HHHH.HHHH)		

Refresh Apply Help

Item	IP Address	Mac Address	Type	Operation
1	192.168.42.13	b0:83:fe:53:06:41	Dynamic	Delete
2	192.168.42.9	f4:6d:04:9c:e0:5b	Dynamic	Delete
3	192.168.42.1	00:1d:aa:22:a8:10	Dynamic	Delete

Figure 8.2 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 deletes an ARP entry, click the corresponding delete link in the list.

8.3 Static route configuration

Figure 8.3 Static Route Configuration

SYSTEM

PORT

VLAN

LAYER 3

SECURITY

DHCP

MULTICAST

RING

ADVANCED

TOOLS

> IP Basic

VLAN Interface

ARP Configuration

Static Routes

Routing Table

> RIP Configuration

> OSPF Configuration

> VRRP Configuration

LAYER 3->IP Basic->Static Routes

Static Routes Configuration

Target Address/Subnet prefix		(format: 10.1.1.0/24)
Next Hop		

Attention: please use 0.0.0.0/0 to set default router.

Refresh

Apply

Help

Item	Target Address/Subnet prefix	Next Hop	State	Operation
------	------------------------------	----------	-------	-----------

Figure 8.3 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

9 System Tools

9.1 Saved configuration

Figure 9.1 Saved Configuration Page



Figure 9.1 above 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 a configuration change on the page to avoid that change being lost after the switch is restarted, the user must click the 'Save' button in the current configuration page before exiting the page.

9.2 Backup profile

Figure 9.2 Back-Up Profile Page

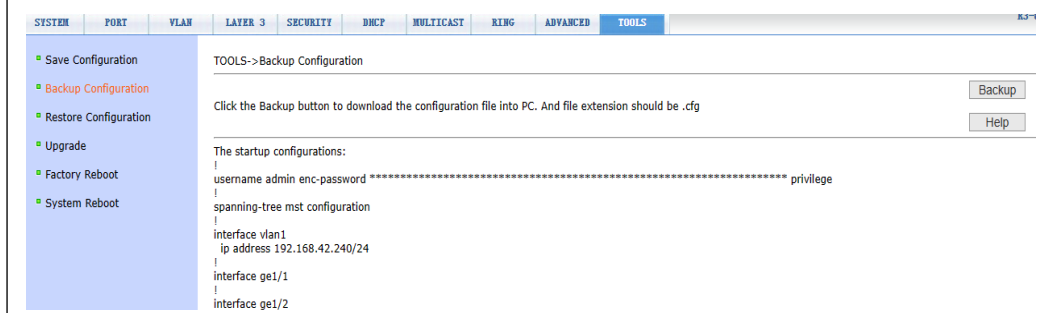


Figure 9.2 above shows the backup profile page. This page allows the user to view the initial configuration of the system. The initial configuration is actually the configuration file in flash. When there is no configuration file in flash, the default configuration is used when the system starts. Click 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

9.3 Restore Profile

Figure 9.3 Restore Profile Page

Figure 9.3 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 a system crash.

9.4 Software upgrade

Figure 9.4 Software Upgrade page

Figure 9.4 above 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

9.5 Restore factory configuration

Figure 9.5 Restore Factory Configuration page

Figure 9.5 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 switch will restart automatically to make the factory configuration effective. Please use the default IP address and password when logging in next time.

9.6 Restart Menu

Figure 9.6 Switch Restart Page

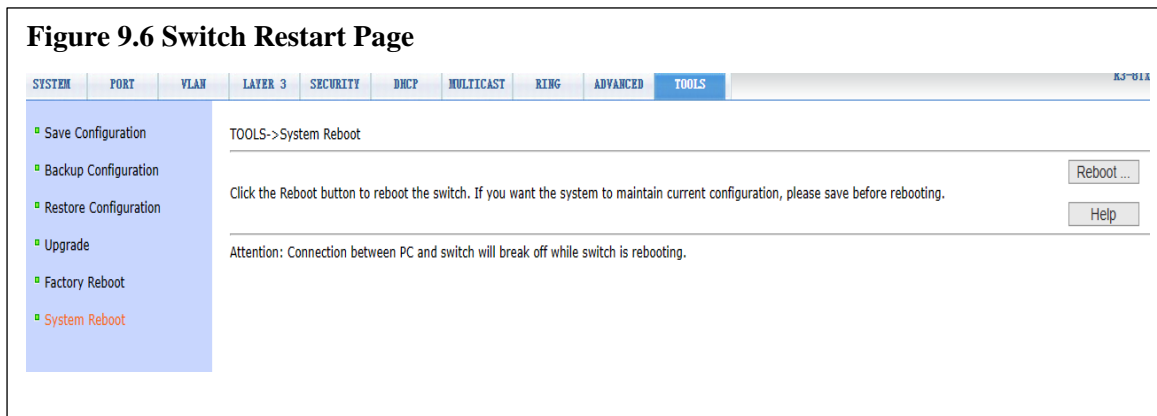


Figure 9.6 shows the restart page through which the user restarts the switch. When you click the restart button, a dialog box will pop up to prompt the user whether to restart the switch. If so, press the OK key, otherwise press the cancel key. You will no longer be able to open web pages when you restart the switch until its booted up.