Zenty | Professional A/V Solution Provider

Web Management User Guide [V1.0]



48x1G PoE AV over IP Switch
ZT-420 I ZT-IPSW48P

ZENTY ®
9807 EMILY LANE
STAFFORD, TX 77477
(844) 200-1945
SUPPORT@ZENTY.COM

Table of Contents

1. WEB page overview 2
1.2 WEB Access features 2
1.3 WEB browsing system requirements 2
1.4 WEB browsing session landing 2
1.5 WEB page elements 3
1.6 The structure of Navigation tree 3
1.7 Page button Introduction 4
1.8 Error messages 4
1.9 Entry Field 4
2.0 Status Field 5
2. WEB page introduction 5
2.1 Login dialog Box 5
2.2 System Configuration: 6
2.3 Port configuration 11
2.4 VLAN Configuration 17
2.5 Security configuration 19
2.6 DHCP 27
2.7 Multicast configuration 31
2.8 RING 32
2.9 Advanced configuration 36
3.0 System tools 40

 Copyright © Zenty AV

WEB page operating manual

This manual focus on describing the WEB page of switch, the user can managed the switch through WEB page. This manual only introduce the simple opetations of the various WEB page of the switches. This manual includes the following:
1, WEB page overview
2, WEB page description

1. WEB page overview

1.2 WEB Access features

Switch provide users with Web access functionality. Via Web browser, users can access switches, manage and configure the switch. WEB accessing's main features are:

1, Easy to access: Users can easily access on switch from anywhere using the network.
2, users can visit the WEB pages of the switch by using the familiar Netscape Communicator and Microsoft Internet Explorer and other browsers, WEB pages of graphical and tabular format presented to the user.
3, Switch provides a wealth of WEB pages, the user can configure and manage vast majority of functions of the switch.
4, WEB page' function classification &integration, make the user find the relevant pages to configuration and management.

1.3 WEB browsing system requirements

Pls see the form 1。

Form 1：

Hardware & Software	**system requirements**
CPU	Pentium 586 above
Memory	128MB above
Resolution	800x600 above
Color	256 colors above
Browser	IE4.0 above or Netscape4.01 above
Operating system	Microsoft® Windows95®, Windows98®, Windows NT®, Windows 2000®,Windows XP®, Windows ME®, Windows Vista®, Linux, Unix ect.

Note：

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

1.4 WEB browsing session landing

Before start Web browsing session ,the user need to make sure:

1. has configure the IP of switch, under the default case, the switch VLAN1 interface IP address is 192.168.168.254,
2. subnet mask is 255.255.255.0.
3. has a Web browser installed on the host to connect to the network, and the host can PING-pass switches.
4. After completing these two tasks, the user put the right address on the browser's address bar of the switch and press Enter to enter the switch after the Web login page, shown in Figure 1. When the multi-user management is not enabled, the user login need for anonymous Web user (admin) password for authentication, and only entered the correct password can access Web, anonymous user password by default is empty.

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

 Copyright © Zenty AV



Figure 1

1.5 WEB page elements

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

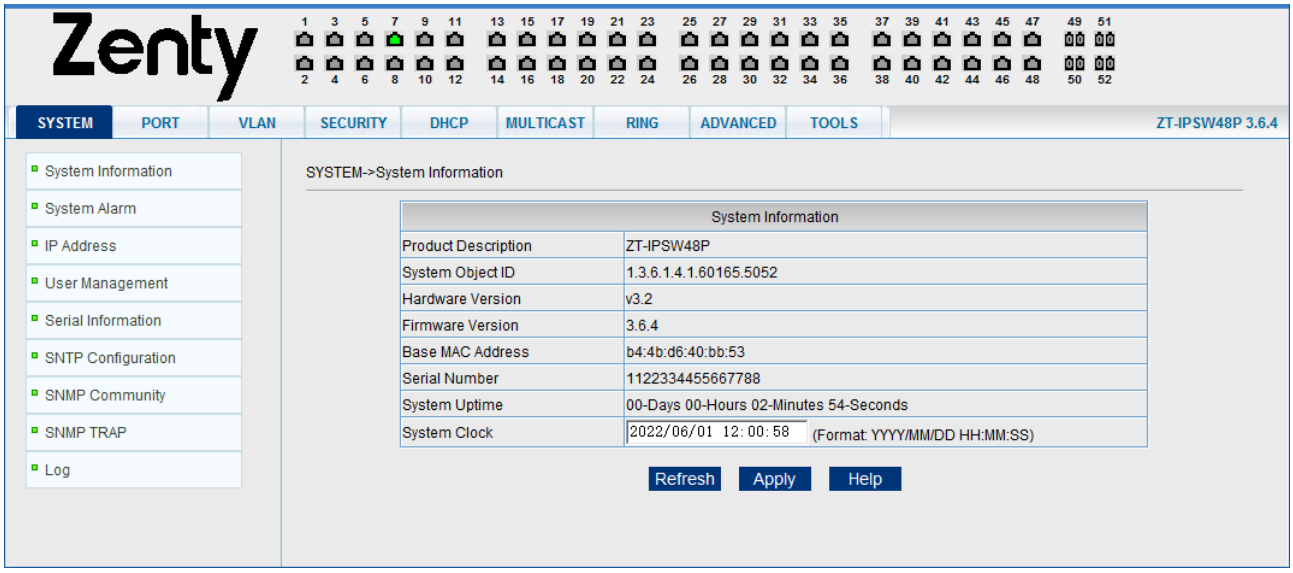


Figure 2

Title page is Used to display the logo

main page Is used to display the user from the navigation tree, select the page

1.6 The structure of Navigation tree

Figure 3 shows the navigation tree organizational structure.

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

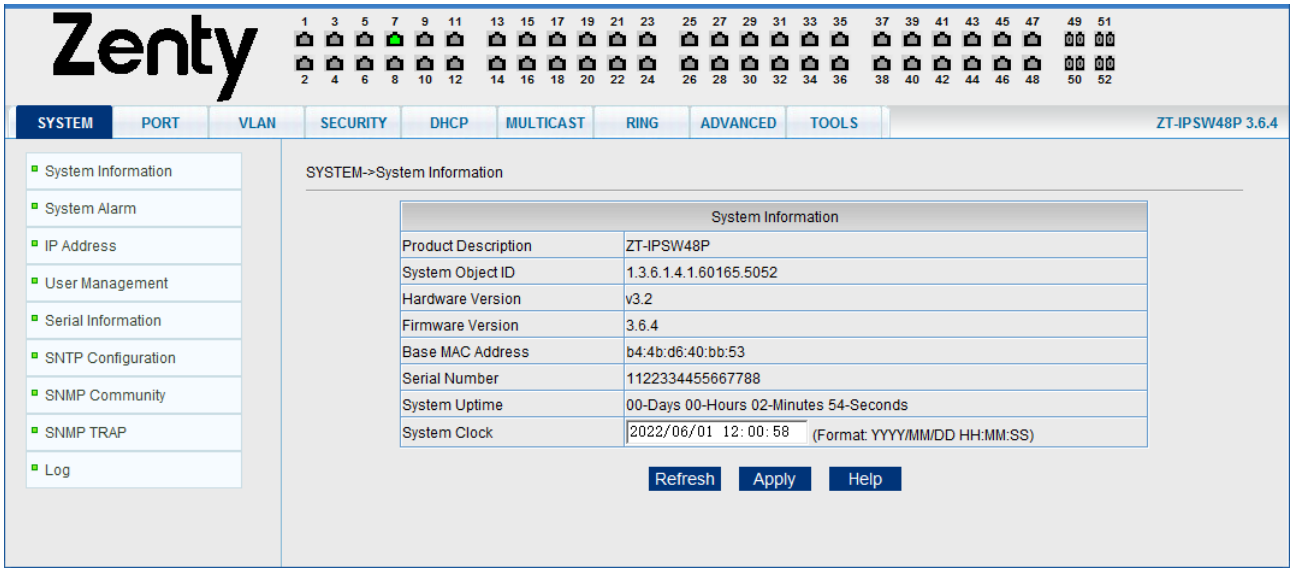


Figure 3

1.7 Page button Introduction

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

Form 2：

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

1.8 Error messages

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



Figure 4

1.9 Entry Field

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

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

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

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

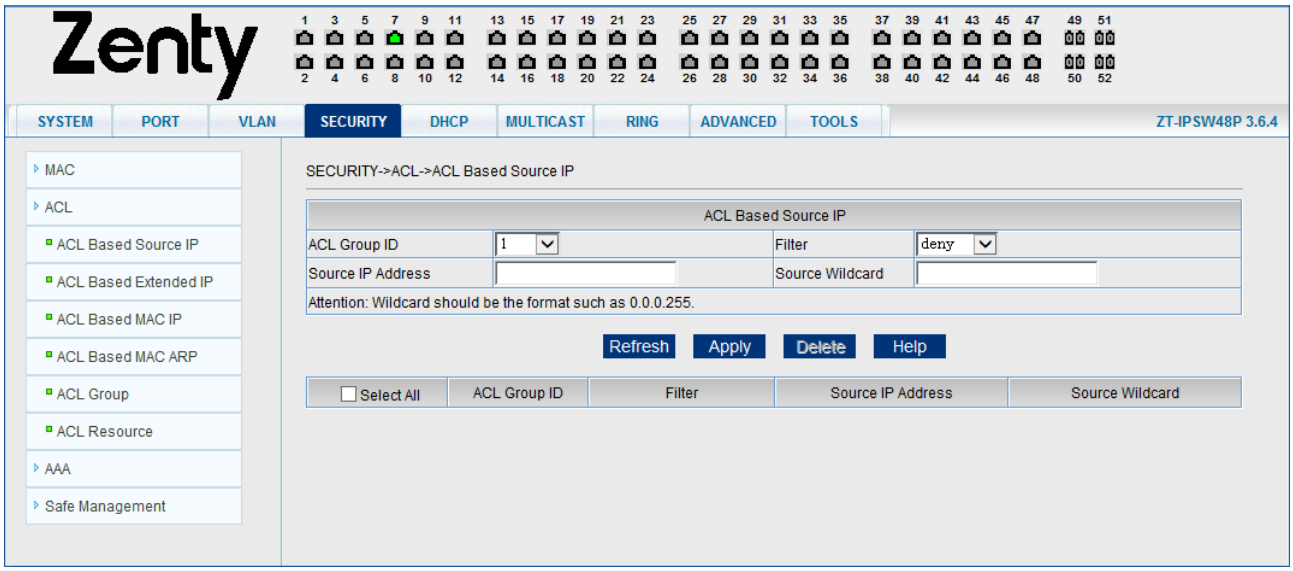
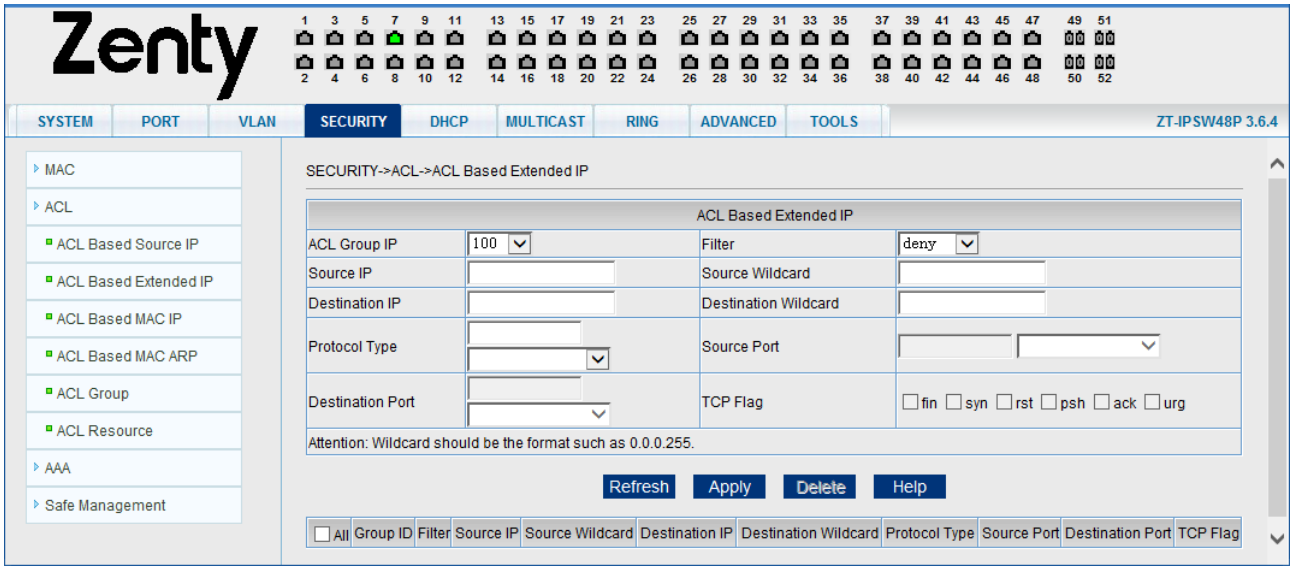


Figure 5

2.0 Status Field

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



the web page of status field

2. WEB page introduction

The WEB pages organized into groups, each including one or more of the WEB pages. The following are introduced one by one on each page.

2.1 Login dialog Box



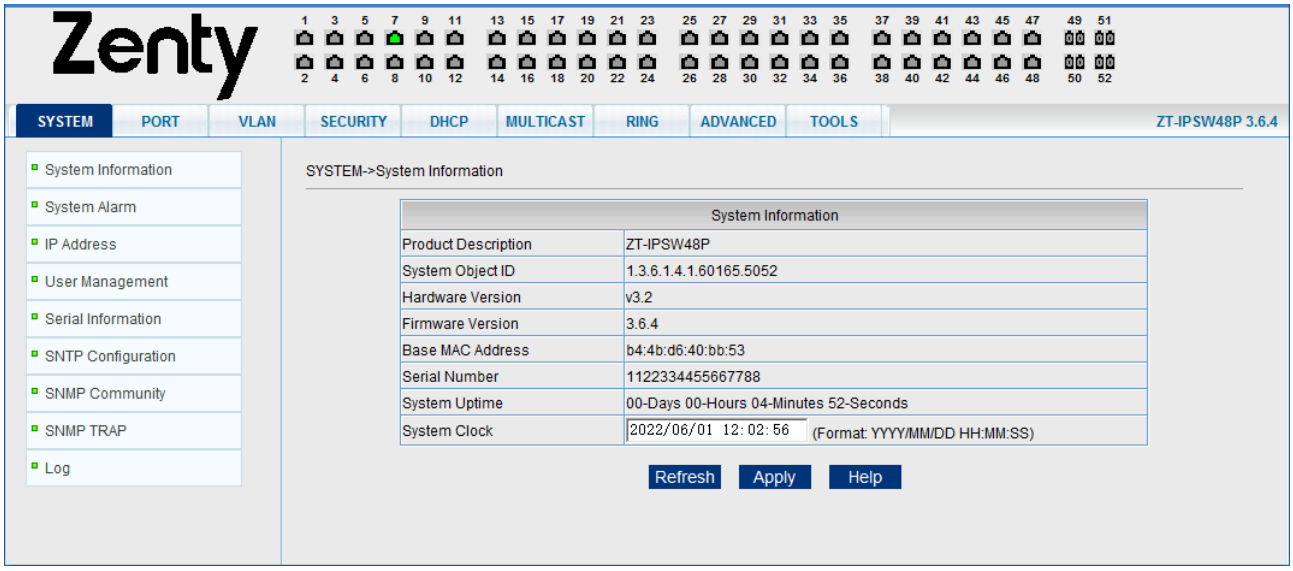
WEB browsing session of the login page

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

2.2 System Configuration:

（1）Basic information page

This page is used for display and configure some parameters of Switch system.



System Information Page

System Object ID: The SNMP system object ID of the switch.

Hardware Version: Version of switch current hardware.

Firmware Version: Version of switch current firmware.

Base MAC Address: Base MAC Address of switch

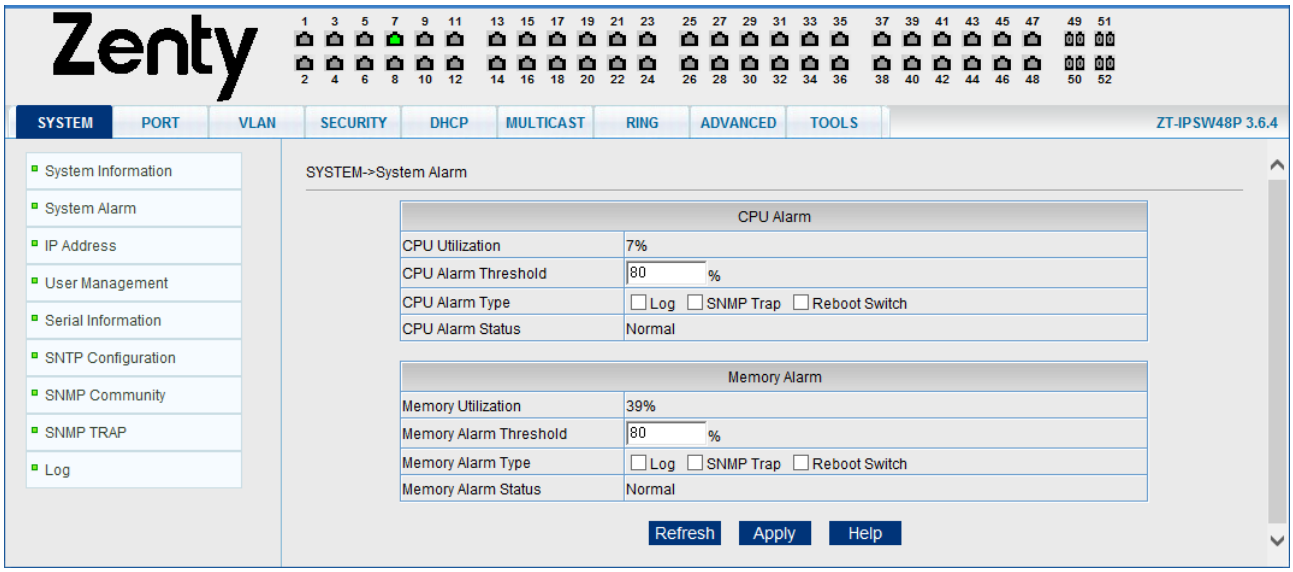
Serial Number: Serial Number of switch

System Uptime: Time from switch start to now.

System Clock: Current date and time. Need to input parameters as follow: year, month, day, hour, minute and second

（2）System Alarm

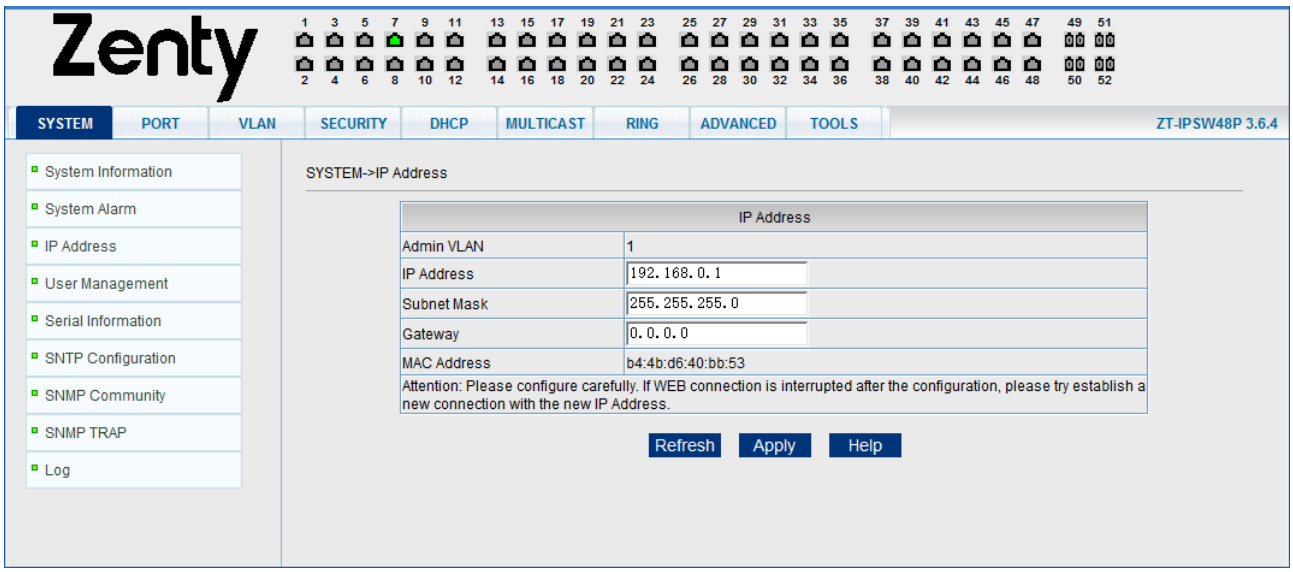
This page is used for dispaly and configure system alarm information, including CPU alarm and memory alarm.



CPU Utilization	**Current CPU utilization of the switch.**
CPU Alarm Threshold	When the CPU utilization of the switch is greater than the set CPU alarm threshold, an alarm is generated. When the CPU utilization of the switch is less than or equal to the set CPU alarm threshold, it retures to normal.
CPU Alarm Type	Set the output method for CPU alarm, including logs, SNMP trap packets or rebooting the switch.
CPU Alarm Status	Display whether the CPU is in a normal or alarm status.
Memory Utilization	Current memory utilization of the switch.
Memory Alarm Threshold	When the memory utilization of the switch is greater than the set memory alarm threshold, an alarm is generated. When the memory utilization of the switch is less than or equal to the set memory alarm threshold, it retures to normal.
Memory Alarm Type	Set the output method for memory alarm, including logs, SNMP trap packets or rebooting the switch.
Memory Alarm Status	Display whether the memory is in a normal or alarm status.

（3）IP address configuration page

This page is used to display and configure IP address in admin VLAN interface.



IP Address Configuration page

Admin VLAN: Admin vlan used on the switch.

IP Address: Current IP address on the switch.

Subnet Mask: Subnet mask for the IP Address.

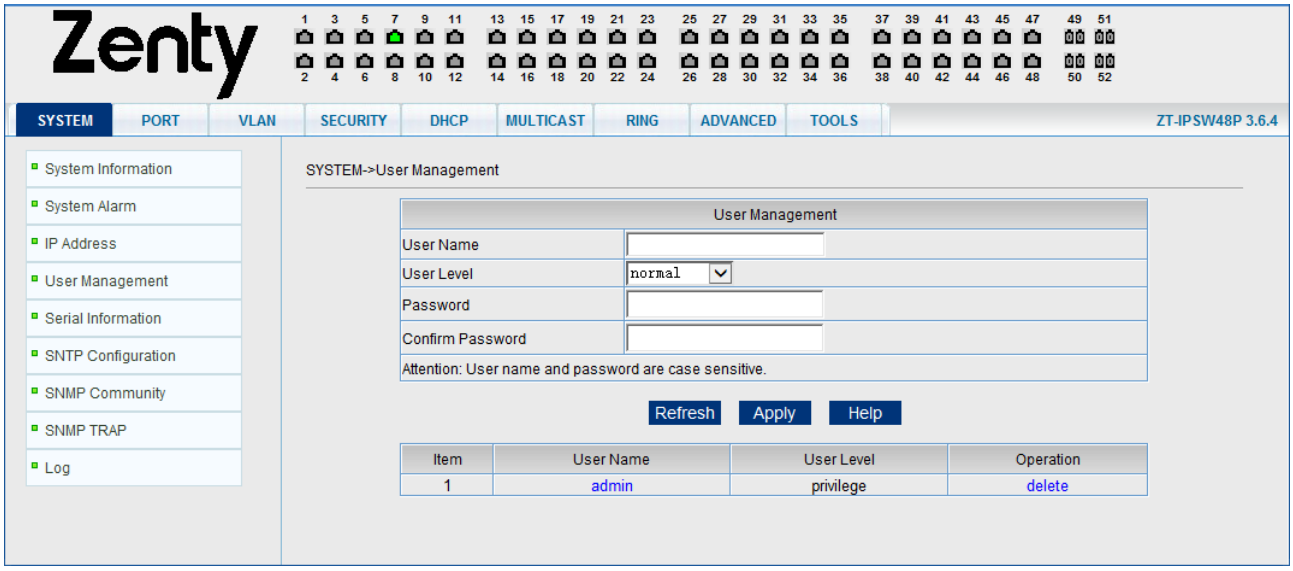
Gateway: Current switch gateway.

MAC Address: MAC address for admin vlan.

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

（4）User management page

Multi-user management not only ensures the safety of switch system, but also provides the ability to manage and maintain switch by multiple users simultaneously.



User Management page

Display and Configure User's Information:

User Name: Configure user name

User Level: The switch supports Two-Layer user: common user and privilege user.

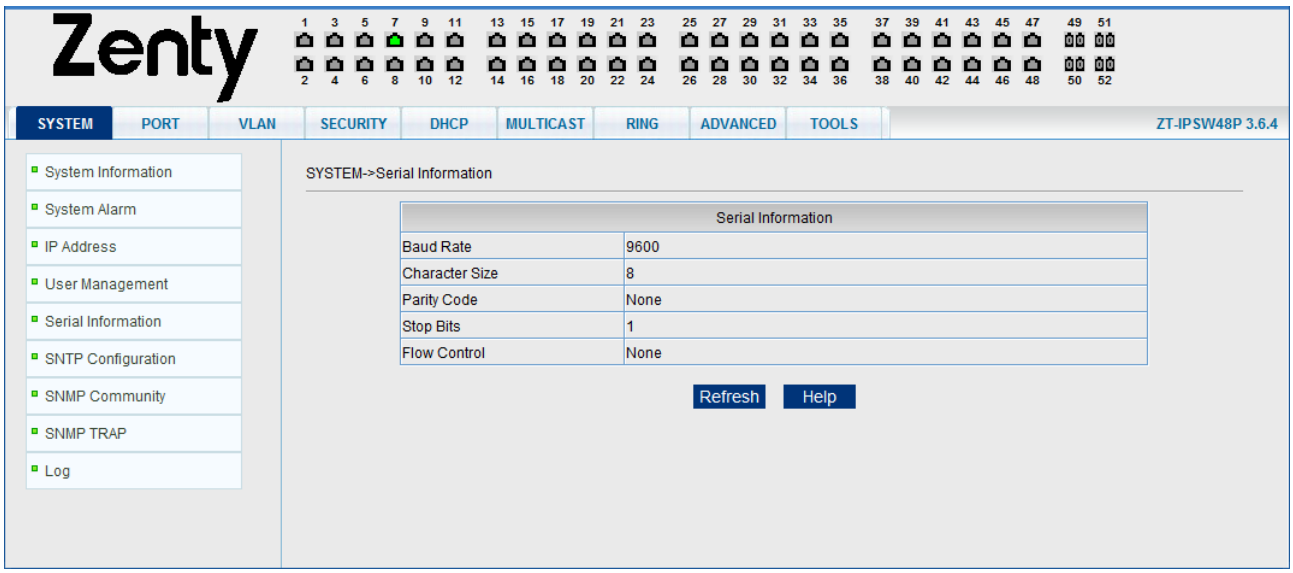
Password: Configure or change a user's password.

Confirm Password: Make sure two passwords matched.

Attention: *User's name and password is case-sensitive, please be careful when inputting.*

（5） Serial Information

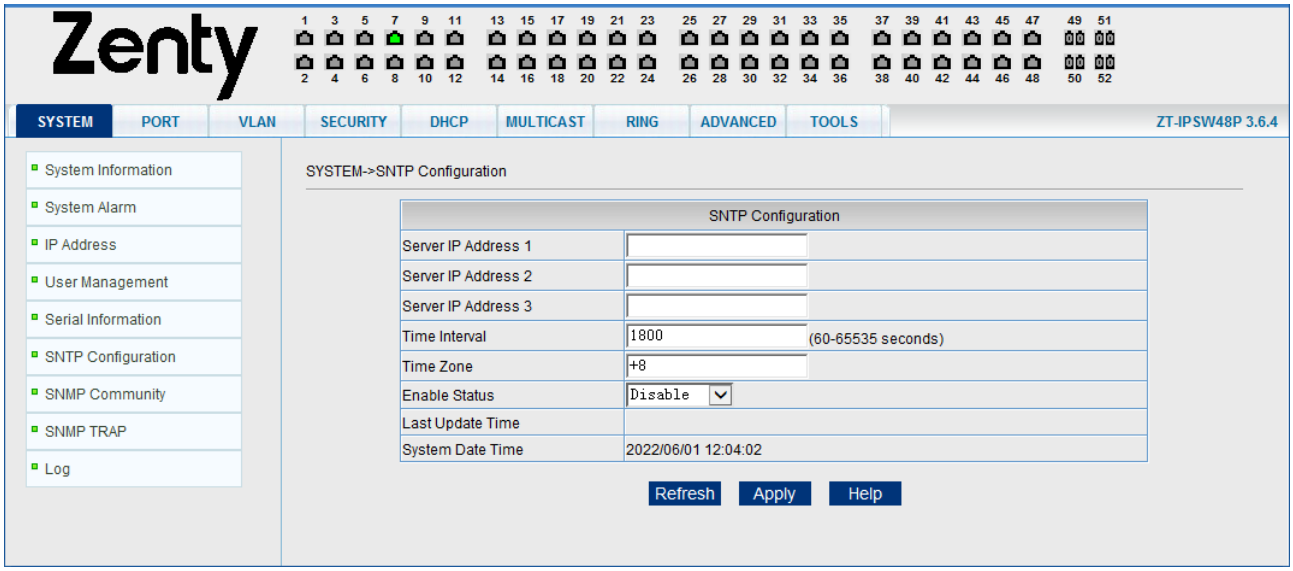
This page is used to display the serial information, including baud rate, character size, parity code, stop bits and flow control.



Serial information page

（6） SNTP Configuration

This page is used to configure and display SNTP protocol.



SNTP Configuration page

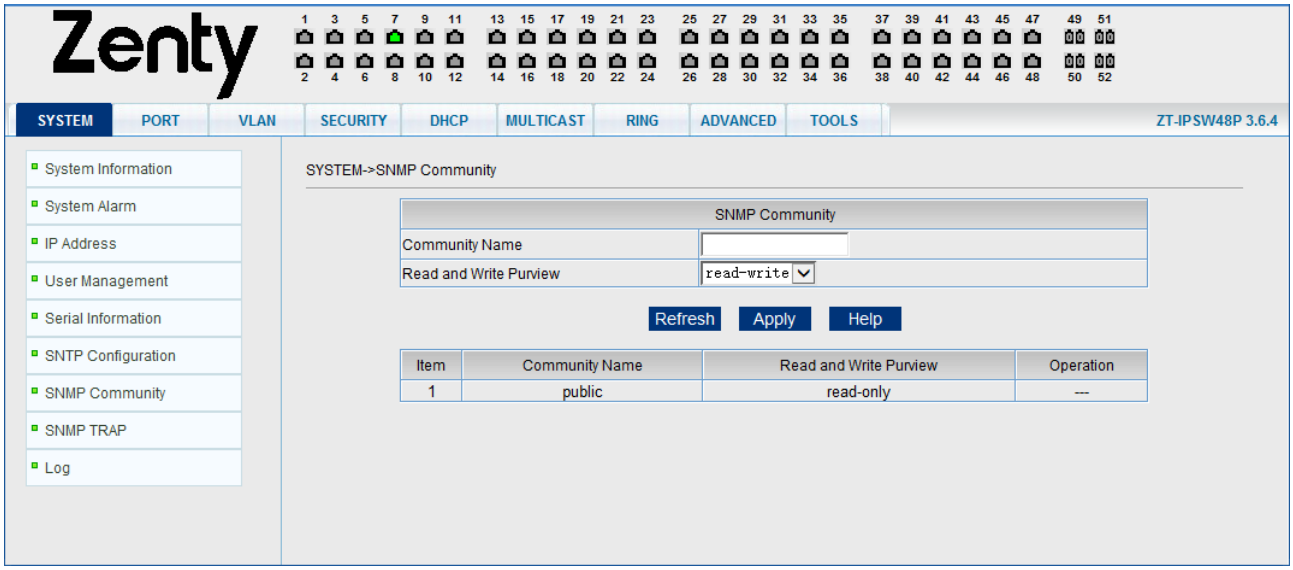
Server IP Address 1: One of the SNTP server address.
Server IP Address 2: One of the SNTP server address.
Server IP Address 3: One of the SNTP server address.
Time Interval: Set the SNTP synchronization time interval in seconds. The default is 1800s.
Time Zone: Set the time zone where the switch is located. The default is +8.
Enable Status: Enable or disable SNTP protocol.
Last Update Time: The time of the last SNTP synchronization.
System Date Time: The system current time.

（7）SNMP community configuration page

This page is used to configure and display community that accessing network.

By default, there is a public name of the common body for the switch, the common body is read-only permissions. When the switch needs to be managed through SNMP, you need to configure a readable and writable community.

Configured commons cannot be modified and cannot be duplicated with existing names. But you can click the corresponding delete link to delete the community, and then re-configure.



SNMP Community Configuration page

Community Name: Community Name

Read and Write Purview: read and write purview

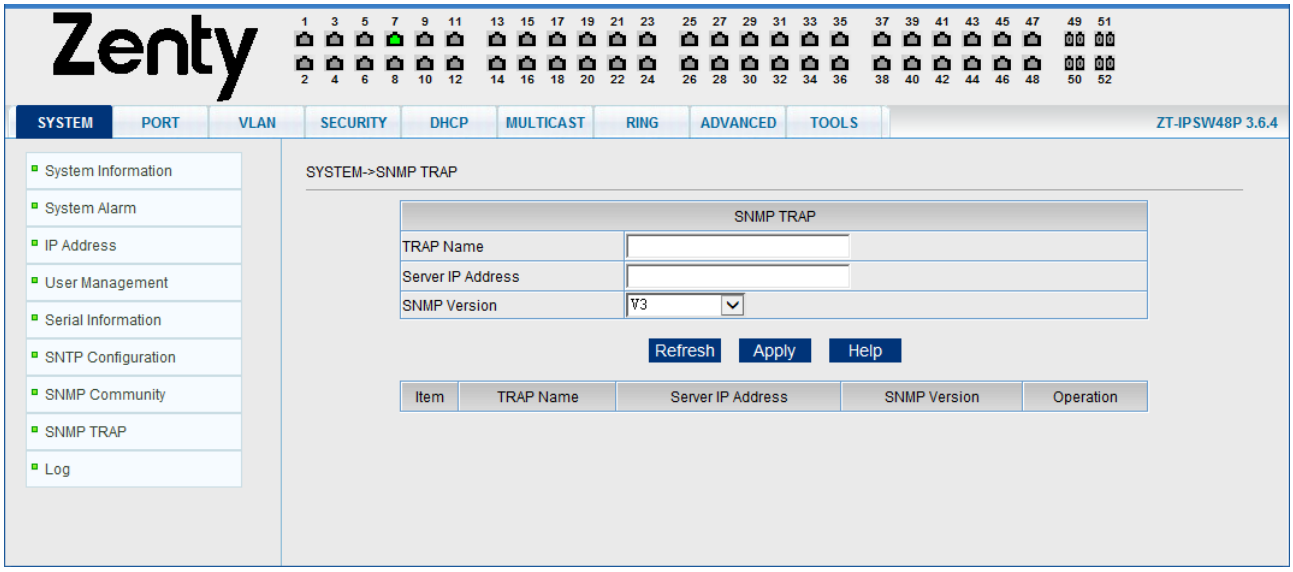
Attention: *The community name 'public' can't be deleted.*

（8）SNMP TRAP configuration page

This page used to configure and display the target of SNMP trap.

Enter the TRAP name, the IP address of the TRAP server, and select the version number. the SNMP TRAP function will take effect if the configuration is right. If the link up or link down occurs, the switch will automatically send the TRAP packet to the destination address.

The configured TRAP targets cannot be modified and cannot be duplicated with existing names. But you can click the corresponding delete link to delete the TRAP target, and then re-configure.



SNMP TRAP configuration page

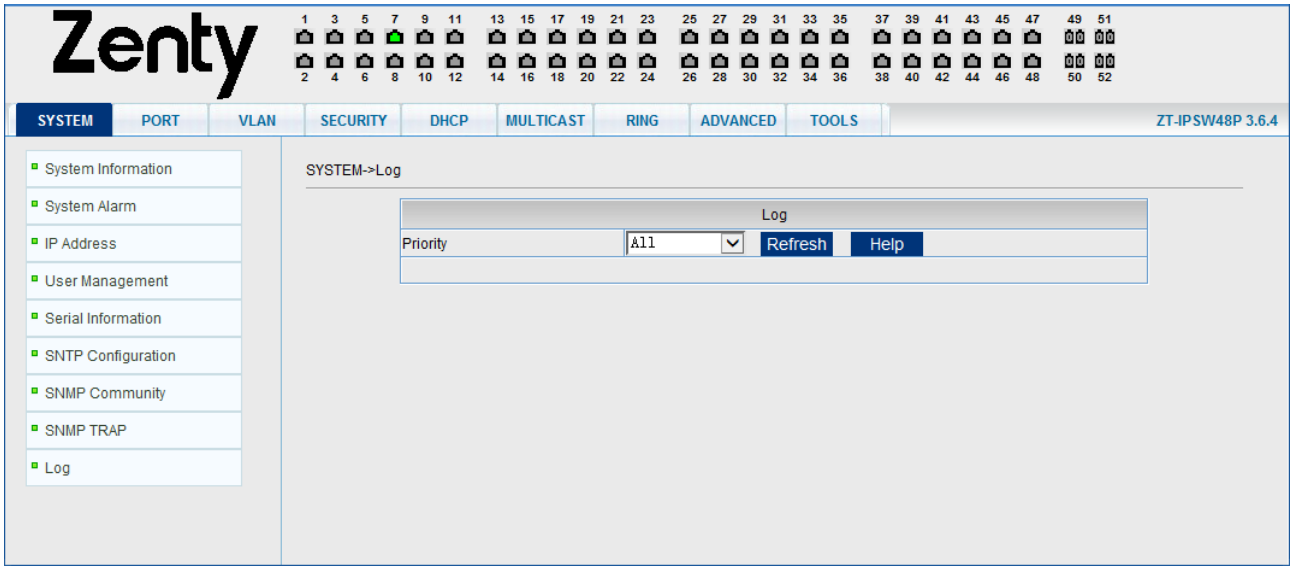
TRAP Name: TRAP target name.

Server IP Address: IP address of TRAP target.

SNMP Version: SNMP Version include v1, v2c and v3.

（9）log information

This page is used to view the log. The user can view the log through this page. Select the priority from the drop-down list, you can view the log of the level, click Refresh to view the latest log.



Log information page

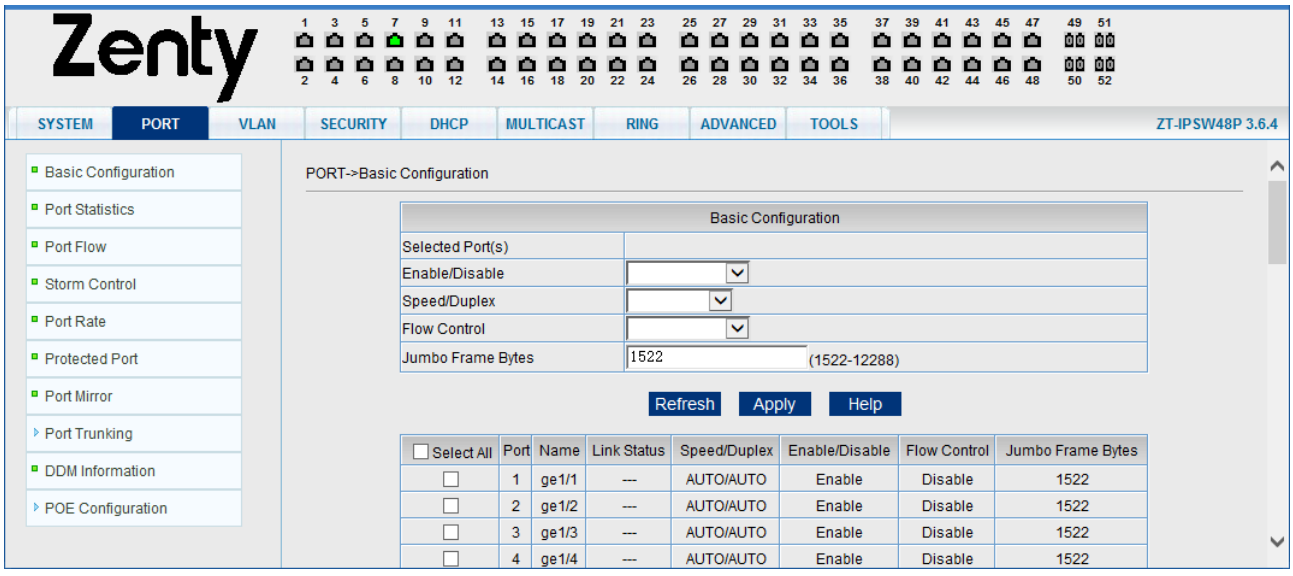
Priority: Priority of a log information indicate its importance. The following four different priorities shows the order from highest priority to lowest: Critical, Warning, Informational and Debugging.

2.3 Port configuration

（1）Port basic configuration page

This page is used to configure and display switch port basic information. The user can enable or disable the port through this page, set the port rate and flow control, or view the basic information of all ports.

To modify the port configuration, the user needs to check the left side of the corresponding port, or use the "Select" function, the selected port will be displayed at the top of the page, a few consecutive ports with the connection number. The selected ports are configured with the same parameters once the settings right. The list in the page shows the configuration information for all ports.



Port Basic configuration page

Select Port(s): Select Port(s) from the following list.

Enable/Disable: Enable or disable the port.

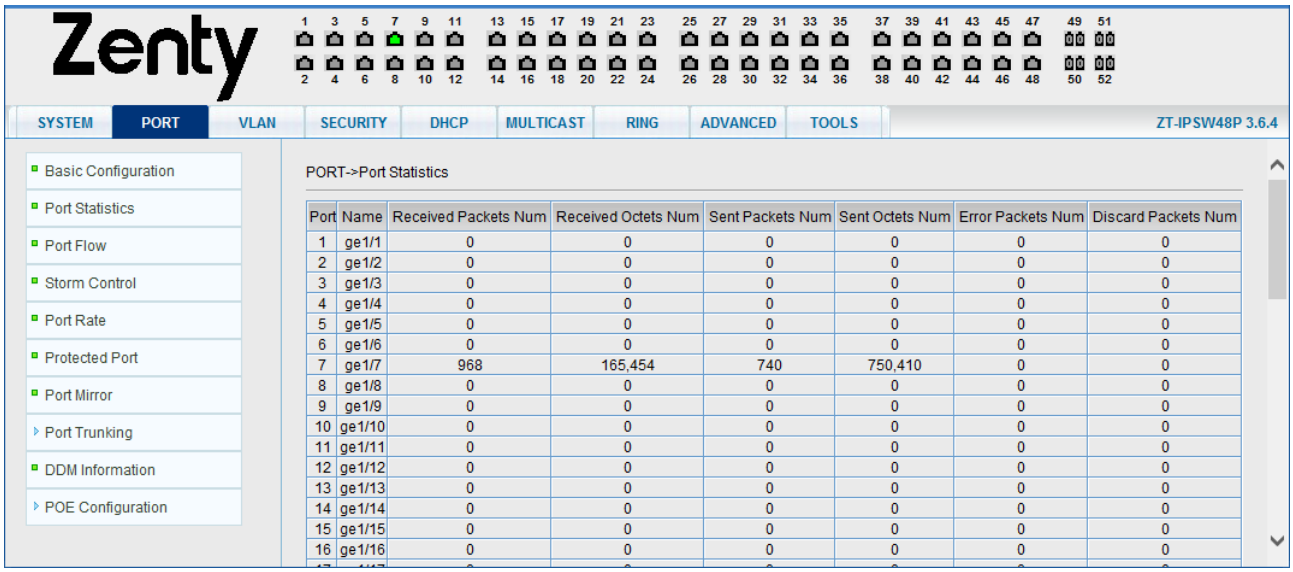
Speed/Duplex: Speed/Duplex: AUTO/AUTO, 10G/FULL, 1G/FULL, 100M/FULL, 100M/HALF, 10M/FULL, 10M/HALF

Flow Control: open or close to output flow control.

Jumbo Frame Bytes: Set the jumbo frame maximum bytes of the port.

（2）Port statistics page

This page is used to statistic receive and send data packets of all ports. The number of packets sent on all ports, the number of bytes sent and received, the packets received, the error packets, and the number of packets discarded.



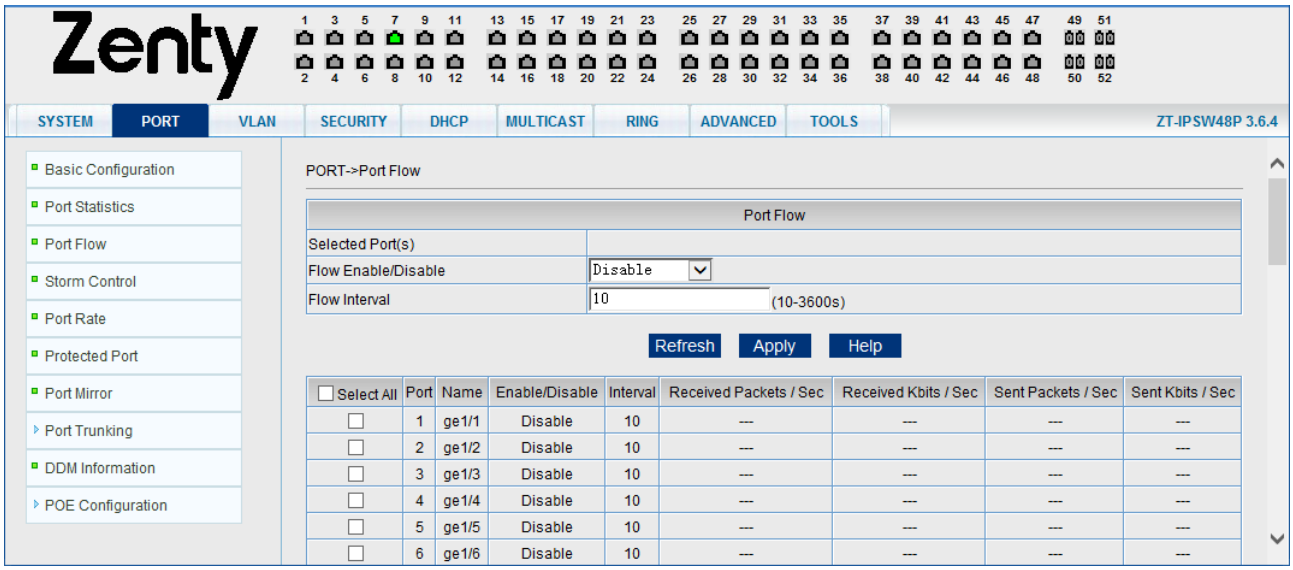
Port	Name	Received Packets Num	Received Octets Num	Sent Packets Num	Sent Octets Num	Error Packets Num	Discard Packets Num
1	ge1/1	0	0	0	0	0	0
2	ge1/2	0	0	0	0	0	0
3	ge1/3	0	0	0	0	0	0
4	ge1/4	0	0	0	0	0	0
5	ge1/5	0	0	0	0	0	0
6	ge1/6	0	0	0	0	0	0
7	ge1/7	968	165,454	740	750,410	0	0
8	ge1/8	0	0	0	0	0	0
9	ge1/9	0	0	0	0	0	0
10	ge1/10	0	0	0	0	0	0
11	ge1/11	0	0	0	0	0	0
12	ge1/12	0	0	0	0	0	0
13	ge1/13	0	0	0	0	0	0
14	ge1/14	0	0	0	0	0	0
15	ge1/15	0	0	0	0	0	0
16	ge1/16	0	0	0	0	0	0

Port Statistics page

Port statistical List: Display packets number, octets number, error packets number and discard packets number.

（3）Port Flow

This page is used to configure and display switch port flow informations.



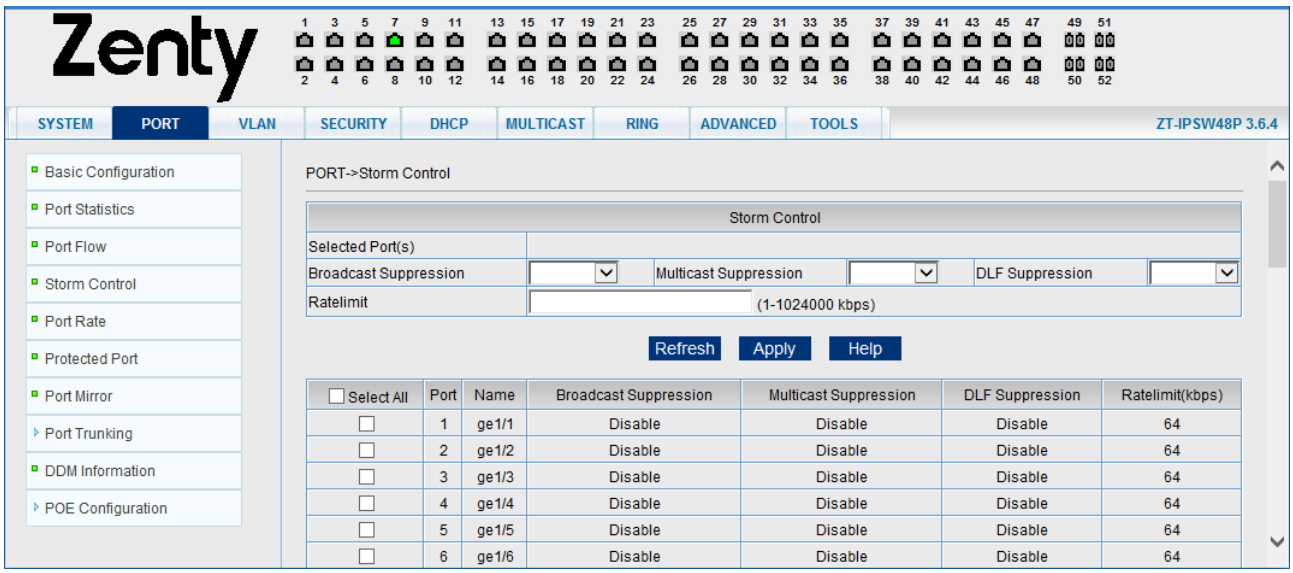
Select All	Port	Name	Enable/Disable	Interval	Received Packets / Sec	Received Kbits / Sec	Sent Packets / Sec	Sent Kbits / Sec
☐	1	ge1/1	Disable	10	---	---	---	---
☐	2	ge1/2	Disable	10	---	---	---	---
☐	3	ge1/3	Disable	10	---	---	---	---
☐	4	ge1/4	Disable	10	---	---	---	---
☐	5	ge1/5	Disable	10	---	---	---	---
☐	6	ge1/6	Disable	10	---	---	---	---

Select Port(s)	Select Port(s) from the following list.
Flow Enable/Disable	Enable or disable the flow of the selected ports.
Flow Interval	Set the flow interval of the selected ports.
List:Port, Name, Enable/Disable, Interval, Packets or Octets per second	Display switch port flow informations.

（4）Port storm suppression page

This page is used to configuration port Broadcast Suppression, Multicast Suppression, DLF Suppression and Ratelimit.

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



Storm Control page

Selected Port(s): Select port from the following checkbox list.

Broadcast Suppression: Open/close Broadcast Suppression

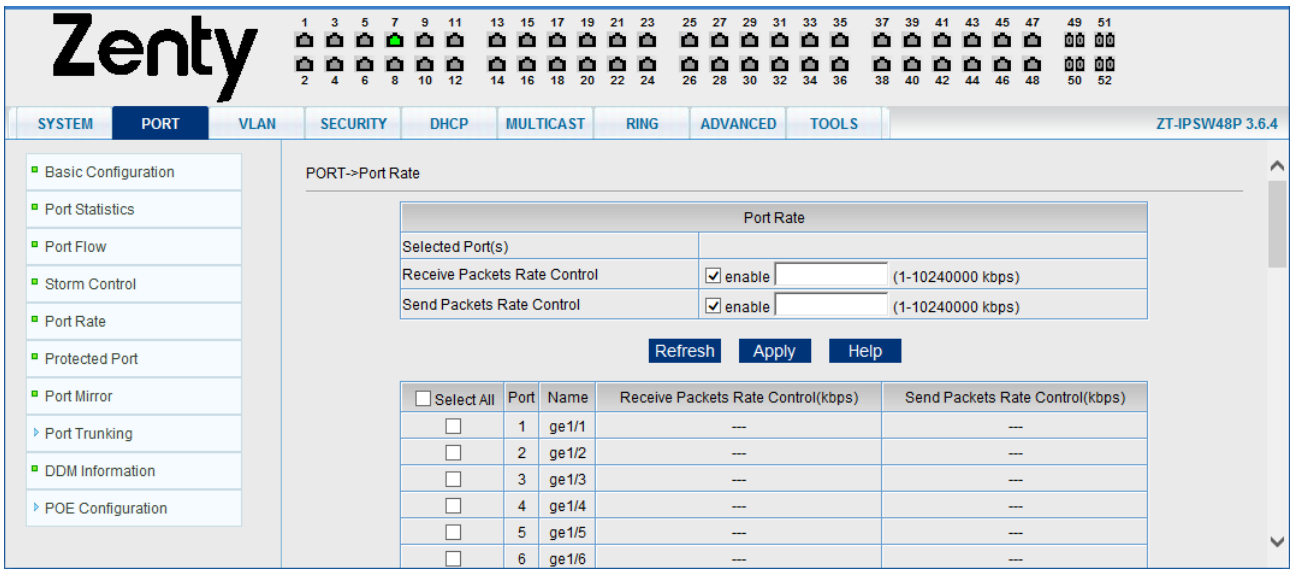
Multicast Suppression: Open/close Multicast Suppression

DLF Suppression: Open/close DLF Suppression

Ratelimit: Configuration rate of the port, range in 1-1024000(kbits)

（5）port speed limit page

This page is used to configuration port send and receive rate. Click the corresponding port on the left, or use the "select all" function select ports to tick alone port-in / port-out the speed limit, speed range from 1 to 1024000, the unit is kbits, the speed limit is not working when canceled click. The list in the page shows configuration information for all ports.



Port speed-limit page

Selected Port(s): Select port from the following checkbox list.

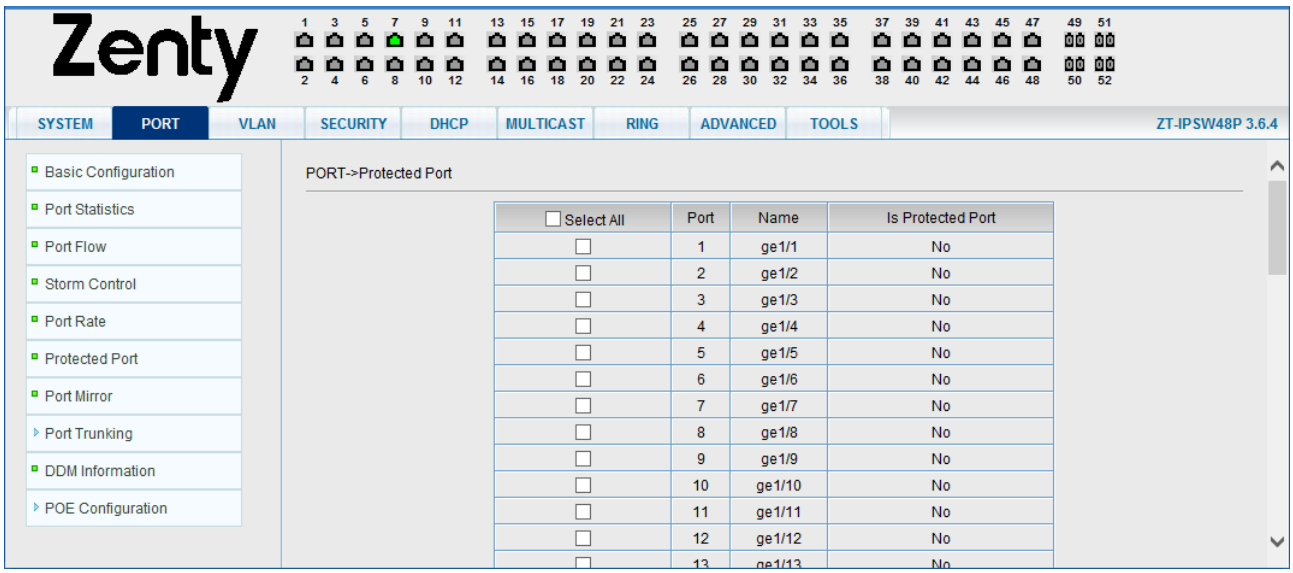
Receive Packets Rate Control: Config and display Receive Packet Wide Band Control, range in 1-1024000(kbits).

Send Packets Rate Control: Config and display Send Packet Wide Band Control, range in 1-1024000(kbits).

（6）Protected Port

This page shows the protection status of each port. Protected ports can only communicate with unprotected ports.

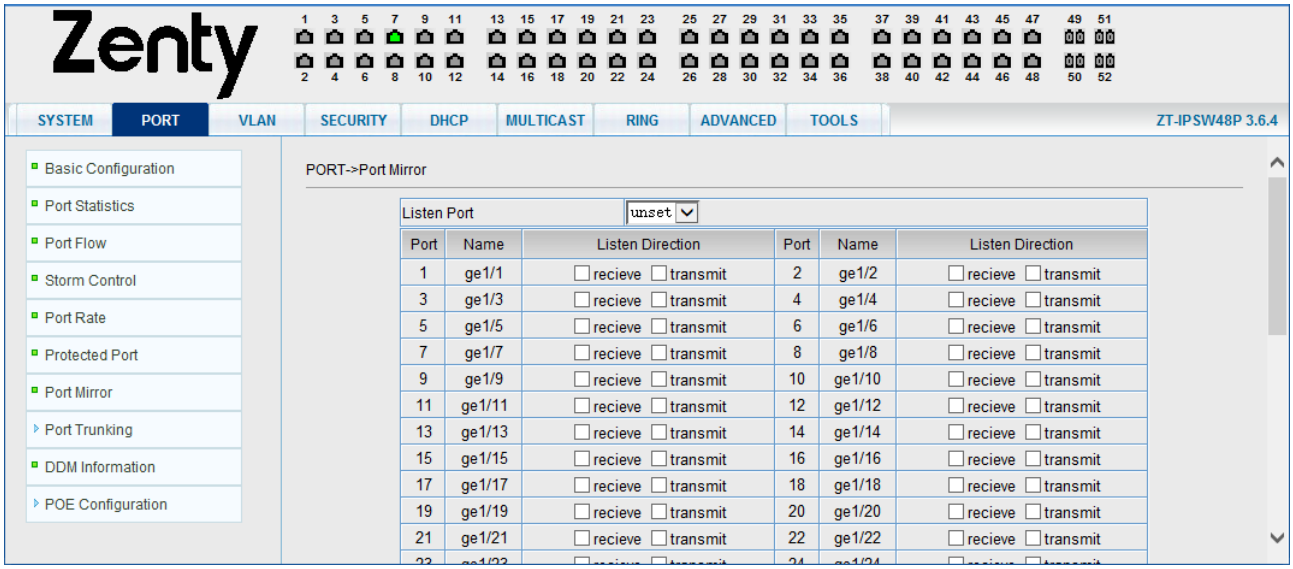
You can tick the ports and press "protected port" button to set the related protected ports. You can tick the ports and press "Unprotected port" button to clear the related protected ports.



Protected Port page

（7）Port mirroring configuration page

The page allows users to configure port mirroring. Port mirroring through the mirror port to monitor the data packets of being mirrored output port and the data packets of being mirrored input port. mirroring Port can only choose one, being mirrored output port and being mirrored input port can select multiple.



Port mirroring configuration page

Listen Port: Configure listen port. Only can have one listen port.

Able Configuration Port: Able to be listened port. Select from the following listen direction checkboxes.

Name: The port name that can be able to configure to listened port.

Listen Direction: Receive - listen received packets, Transmit - listen send packets

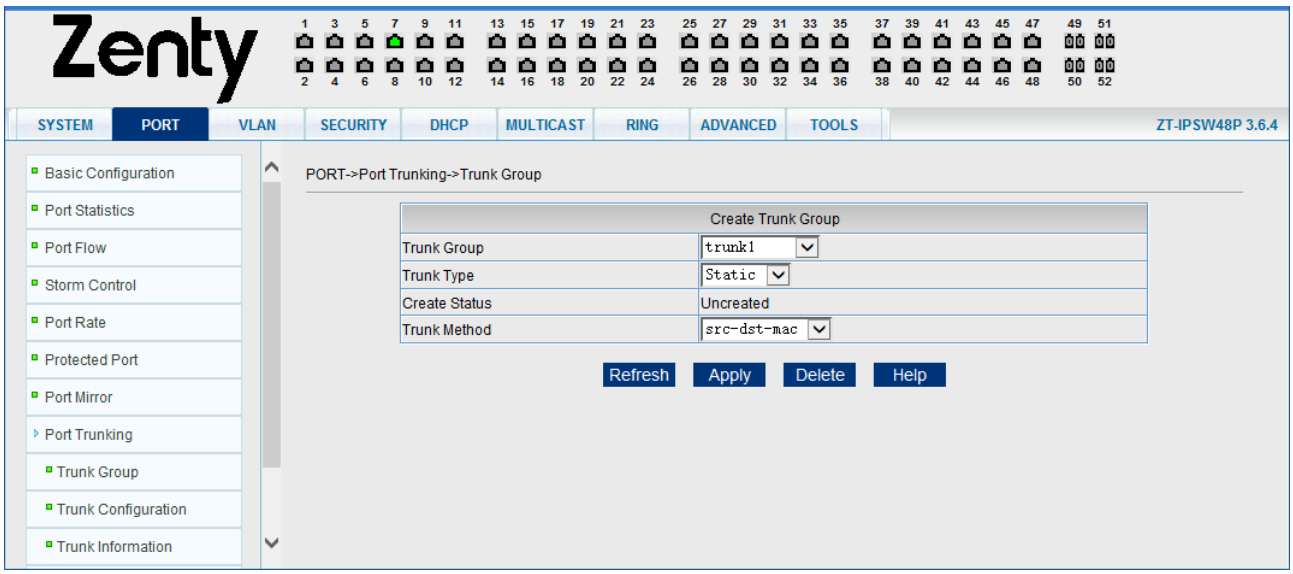
Apply: Active configuration.

Delete: Select unset option from Listen Port List and click the Apply button.

Attention: A port could not be listen and listened port at one time. There only one listen port, Listened port can be multiple.

（8）Create Trunk Group page

This a page of creating a link aggregation. Select the group you want to create from the pull-down menu and select the algorithm for link aggregation. The algorithm of link aggregation is based on source MAC, destination MAC, based on source and destination MAC at same time, source IP, destination IP, based on source and destination IP at same time.



Create Trunk Group page

Trunk Group: Create trunk Group, group ID is 1-32.

Trunk Type: Static trunk group or dynamic LACP trunk group.

Create Status: Uncreated or Created

Trunk Method: Configuration port load balance strategy.

src-mac - Based on source MAC balancing strategy.

dst-mac - Based on target MAC balancing strategy.

src-dst-mac - Based on source and target MAC balancing strategy.

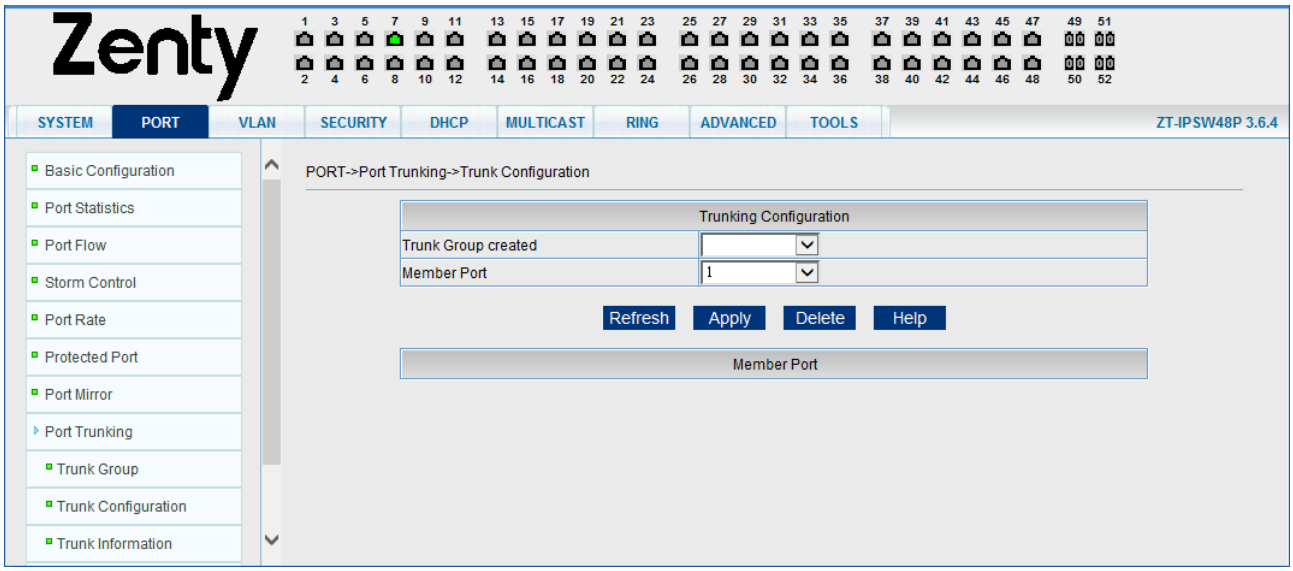
src-ip - Based on source IP balancing strategy.

dst-ip - Based on target IP balancing strategy.

src-dst-ip - Based on source and target IP balancing strategy.

（9）Trunking Configuration page

This is a link aggregation configuration page. Select the link aggregation group from the drop-down menu and select the port to join.



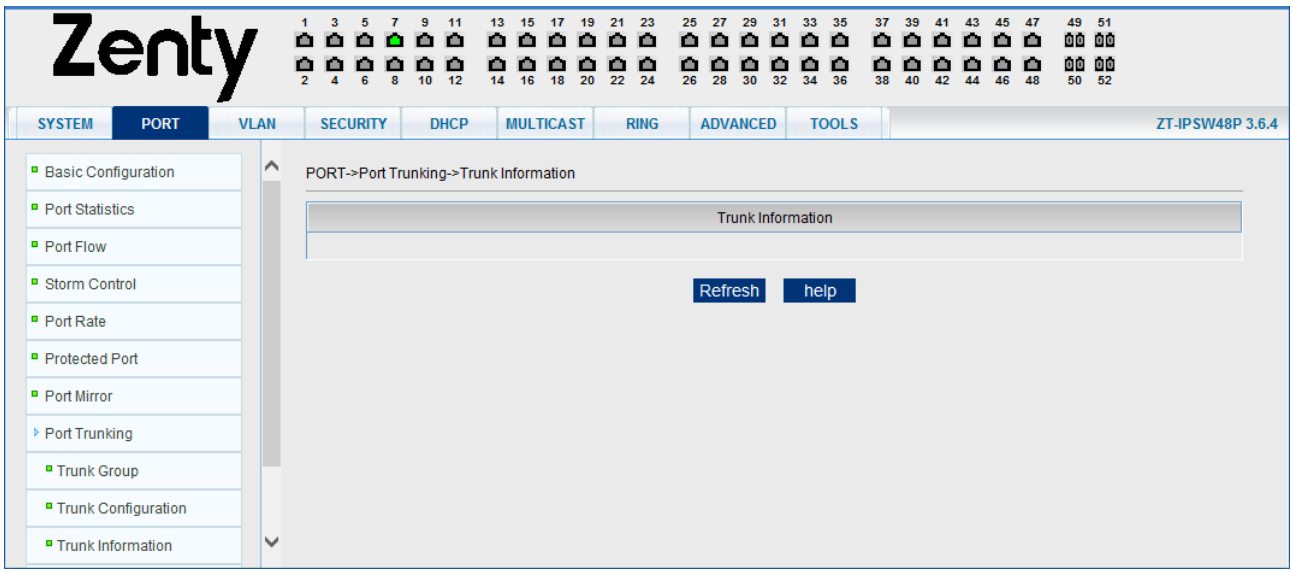
Trunking Configuration page

Trunk Group created: Display trunk groups those that already have been created

Member Port: Port able to be Trunk group member.

(10) Trunk Information page

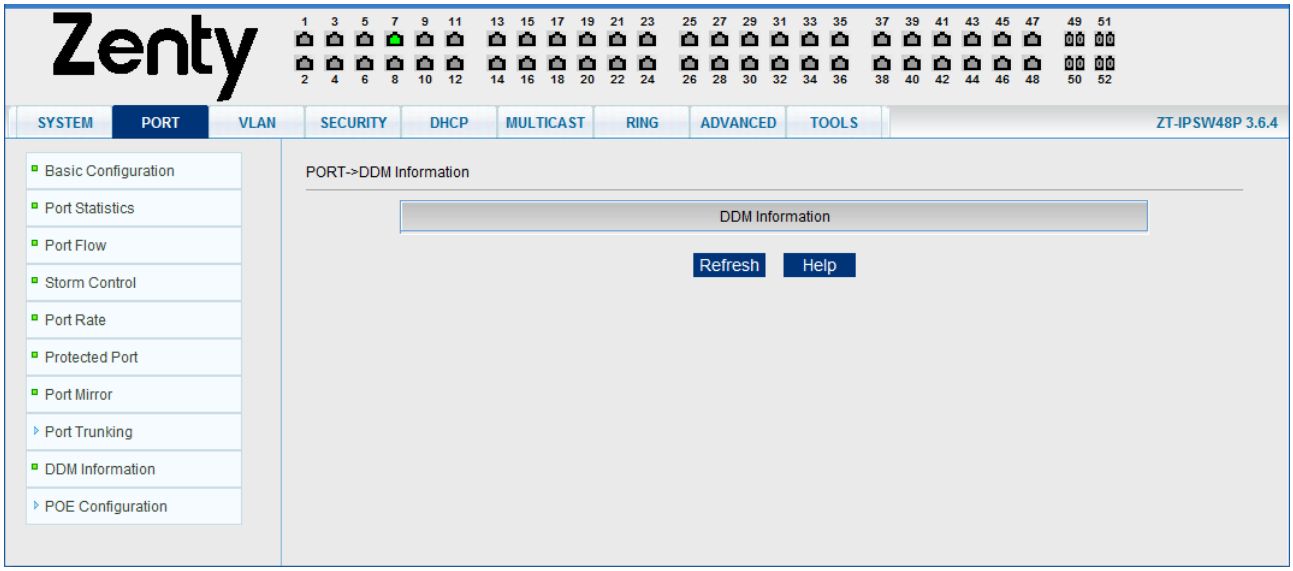
This page display All Information about trunking.



Trunk Information Page

(11) DDM Information

This page is used to display the DDM information of all ports with SFP or SFP+ optical modules inserted.



DDM information page

(12) PoE port configuration

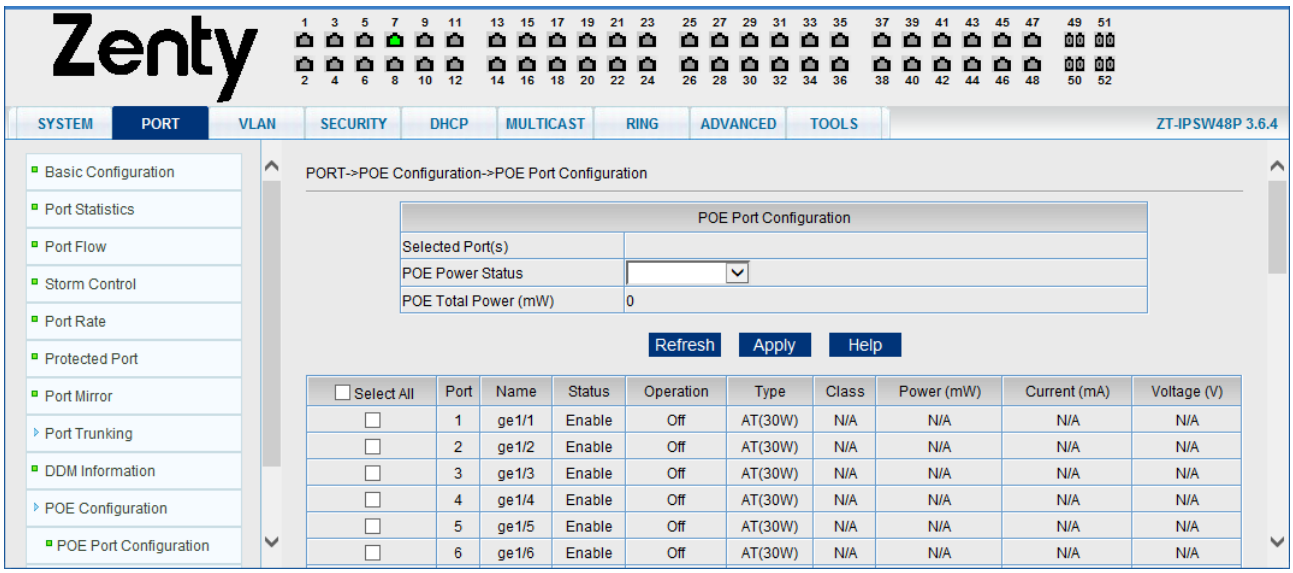
PoE port Configuration Page

The PoE port configuration / PoE-display page. Users can enable or disable the port's PoE function to the page, or View all ports of PoE information.

Information can be seen in the following tables:

1, Staus： Enalbe means PoE function is available；Disable means PoE function is close.

2, Operation： Displays the PoE ports ON or OFF



PoE port configuration page

2.4 VLAN Configuration

（1）VLAN configuration page

This page is used to create VLAN.

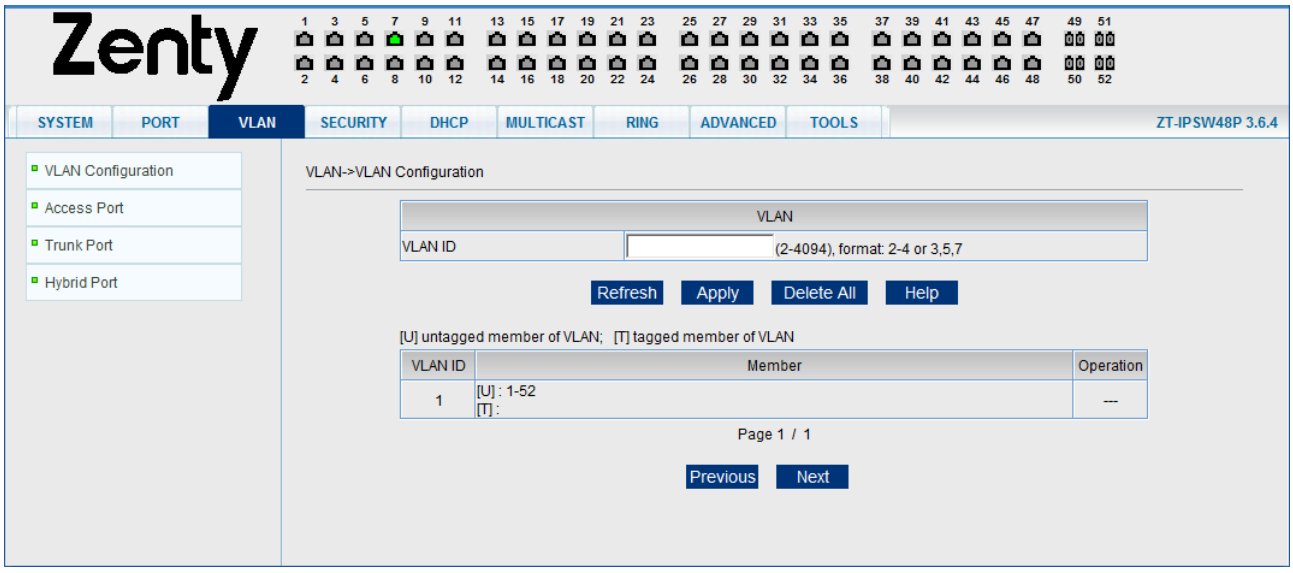
If you want to create a new VLAN, you can enter a VID in the active line, ranging from 2 to 4094. The switch creates VLAN 1 by default, and VLAN 1 cannot be deleted.

If you want 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 the VLANs that have been created and identifies the port members of each VLAN. A port cannot be a member of a VLAN. It can be a tagged or untagged member of a VLAN. The characters in the front of the page are as follows:

T (tagged): The port is a tagged member of this VLAN

U (untagged): The port is an untagged member of this VLAN



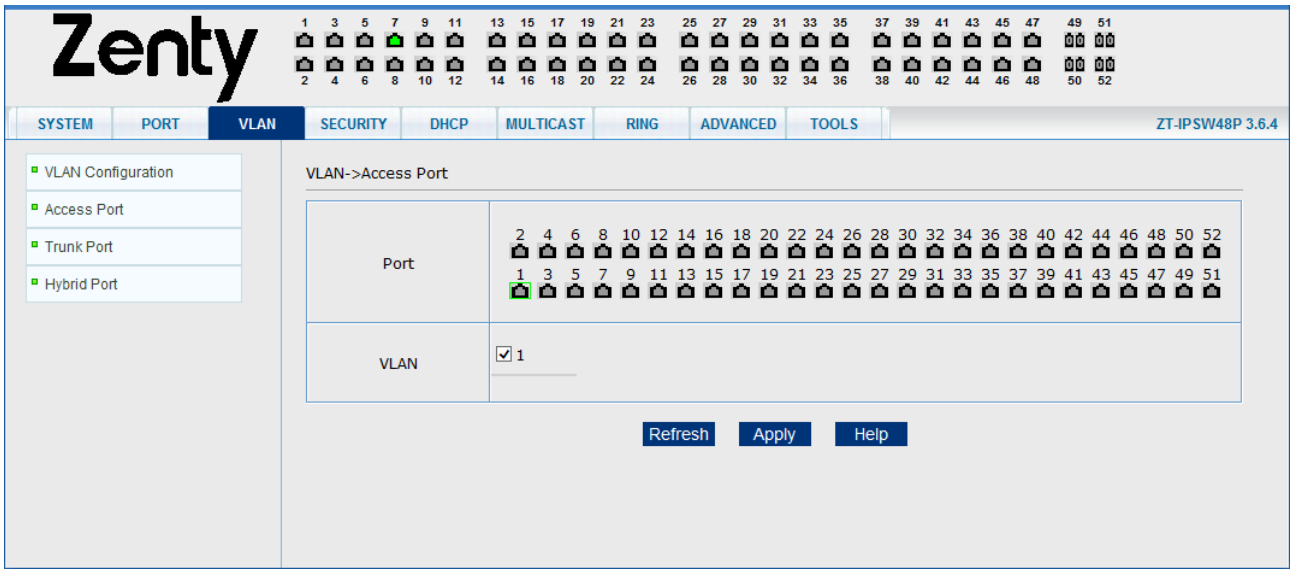
VLAN configuration page

（2）Access port configuration page

This page displays and configures the port access mode and the VLAN to which it belongs.

This page is divided into two parts: port list and VLAN list. The mouse on the port hover, you can see the port VLAN mode, click on a port to display / configure the port VLAN. If the port is in Access mode, it can display its VLAN, and you can select another VLAN then apply it. If the port is not in Access mode, the port is

changed to Access mode and VLAN is configured. Note that only one VLAN can be selected when in Access mode style.

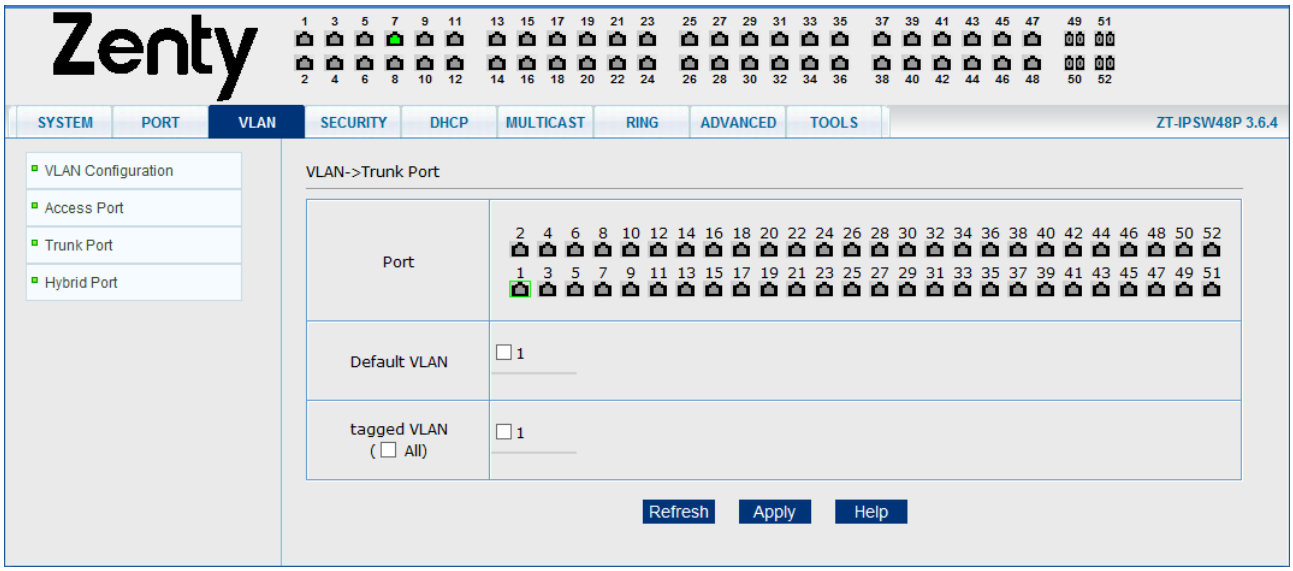


Access port configuration page

（3）Trunk port configuration page

This page displays and configures the port Trunk mode and the VLAN to which it belongs.

This page is divided into two parts: port list and VLAN list. The port part of the operation can refer to the second section (Access port configuration page). If the port is in trunk mode, it can display its VLAN, and you can select another VLAN than apply it. If the port is not in trunk mode, the port is configured with Trunk mode and VLAN. While in trunk mode, VLAN can be multi-selected. When need to select a group of consecutive VLAN, select the first, hold down the Shift key, then select the last one.

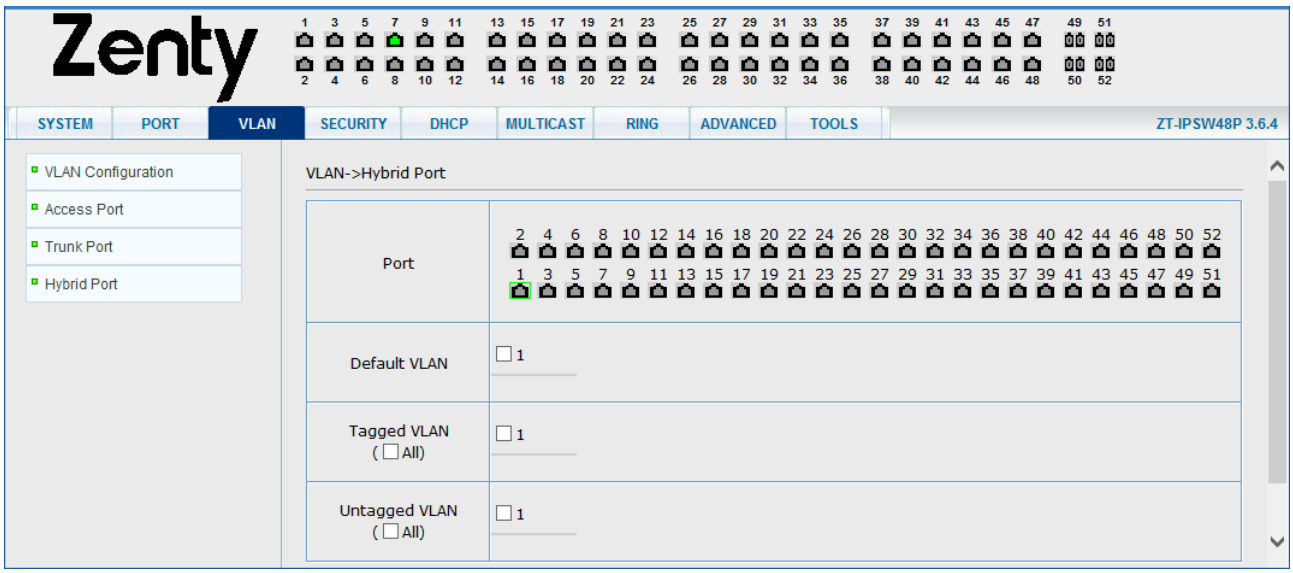


shows the trunk port configuration page

（4）Hybrid port configuration page

This page displays and configures the port hybrid mode and the VLAN to which it belongs.

This page is divided into two parts: port lists and VLAN list, the port part of the operation can refer to the second section (Access port configuration page). If the port is in hybrid mode, it can display its VLAN, and you can select another VLAN then apply it. If the port is not in the hybrid mode, the port is configured with the hybrid mode and the VLAN is configured. The default VLAN must be configured and only one can be selected. The tagged VLAN and the untagged VLAN can be selected in any number. However, for a VLAN, only one of the three modes can be selected. If a VLAN is configured with a tagged VLAN, the VLAN cannot be Specified as default VLAN or untagged VLAN, and so on.



Hybrid port configuration page

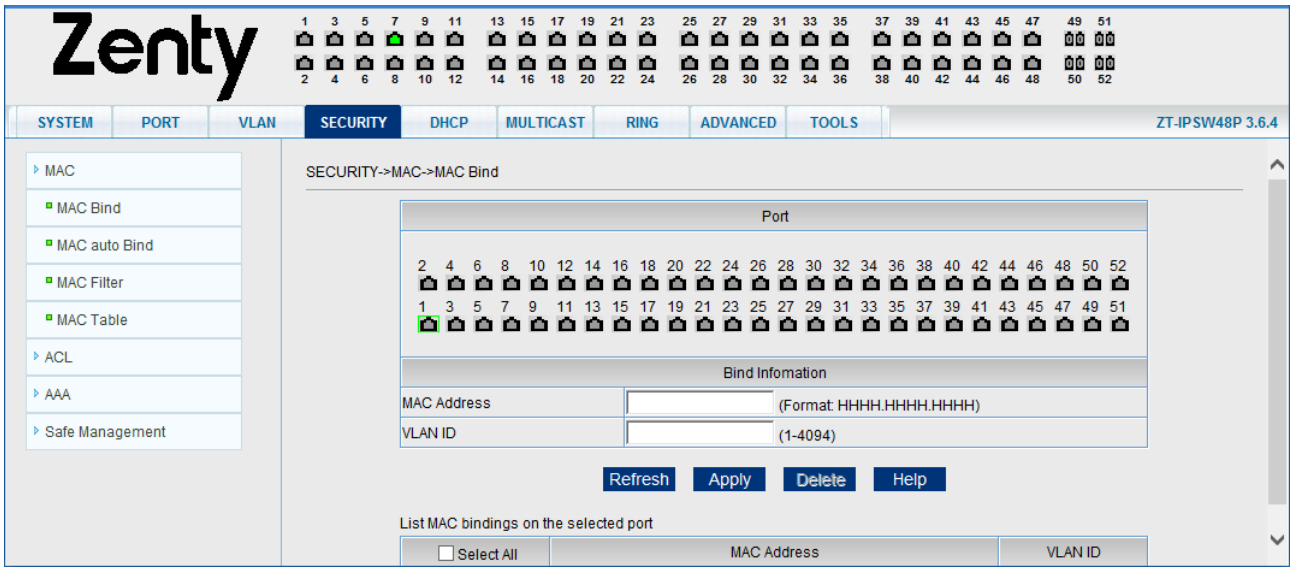
2.5 Security configuration

（1）MAC Configuration

1MAC address manual binding page

This page is used to achieve the port to the MAC address binding.

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

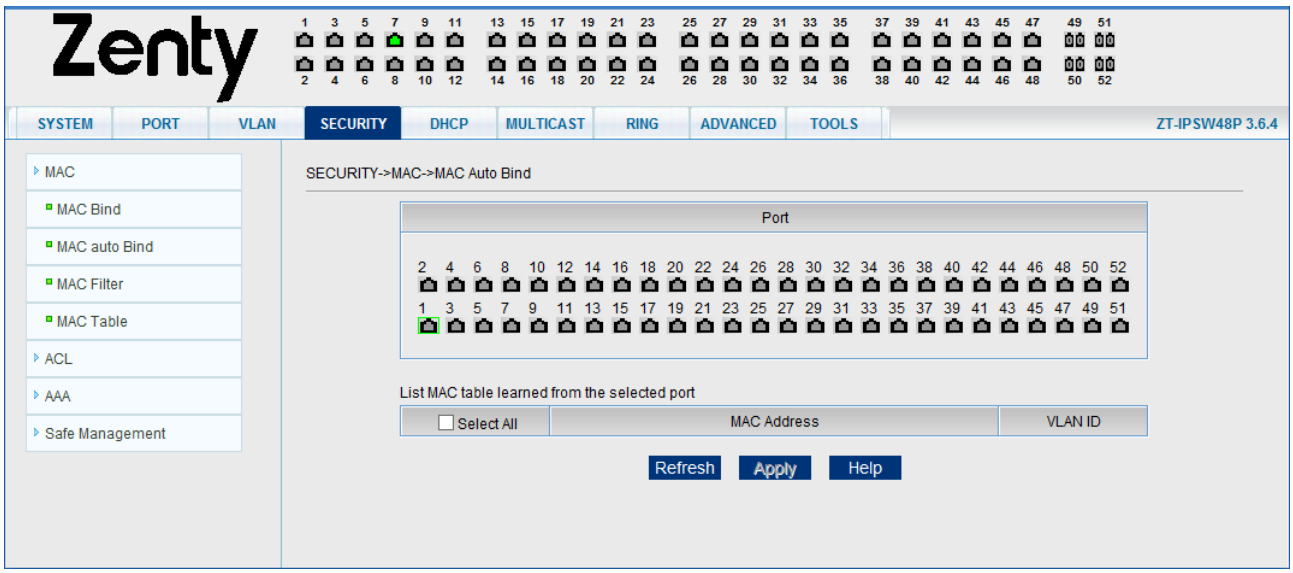


MAC address manual binding page

2 MAC binding automatic conversion page

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

Shows the hardware switch on the lay2 the exist port dynamic MAC address and affiliated VLAN. Can choose one of the entry and convert it into static binding.

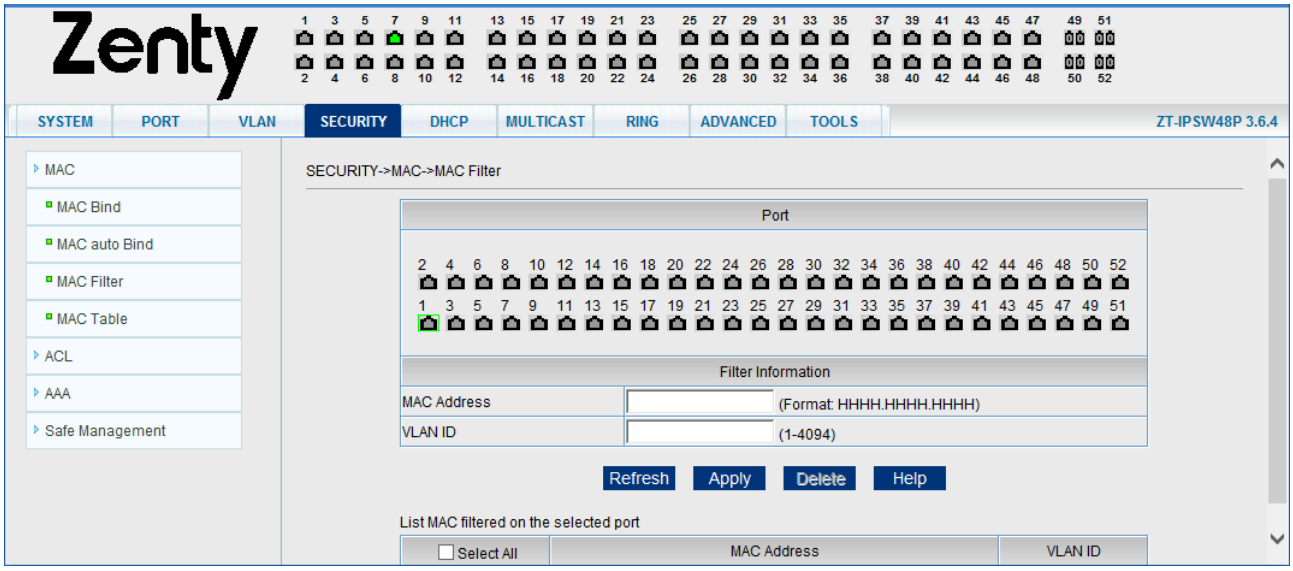


MAC address auto-binding page

3 MAC filtering configuration page

Figure 41 is the MAC filtering configuration page. This page is used to configure the ports on the MAC address filtering.

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

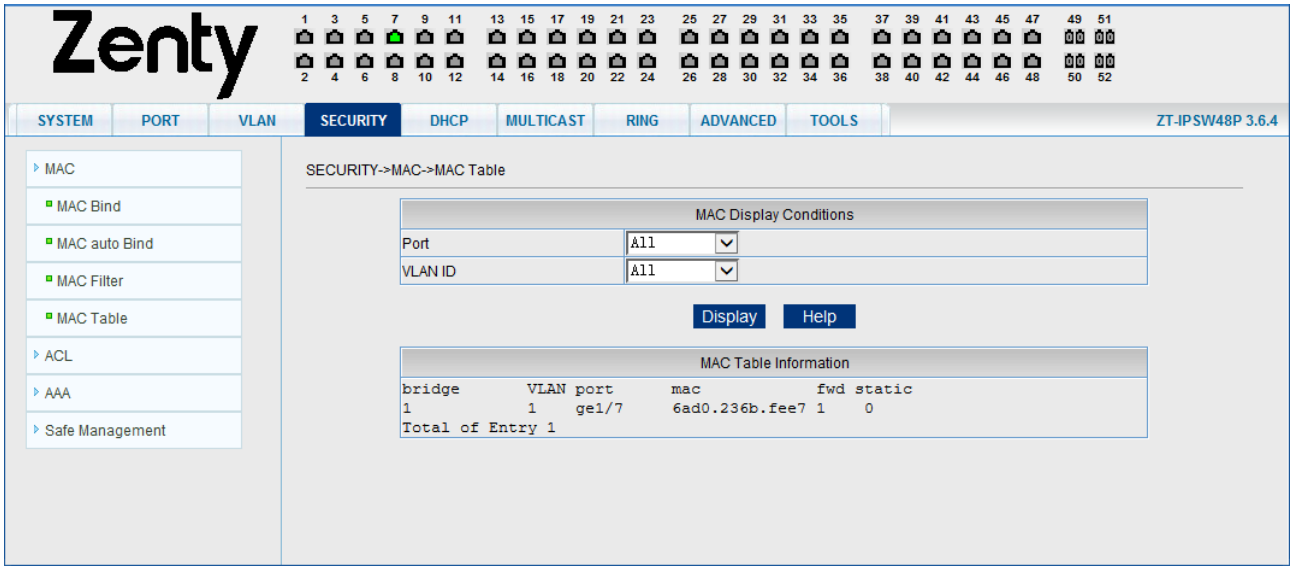


MAC Address Filtering Configuration page

4 MAC Table Information

This page is used to display MAC table information according to the conditions of port and VLAN id.

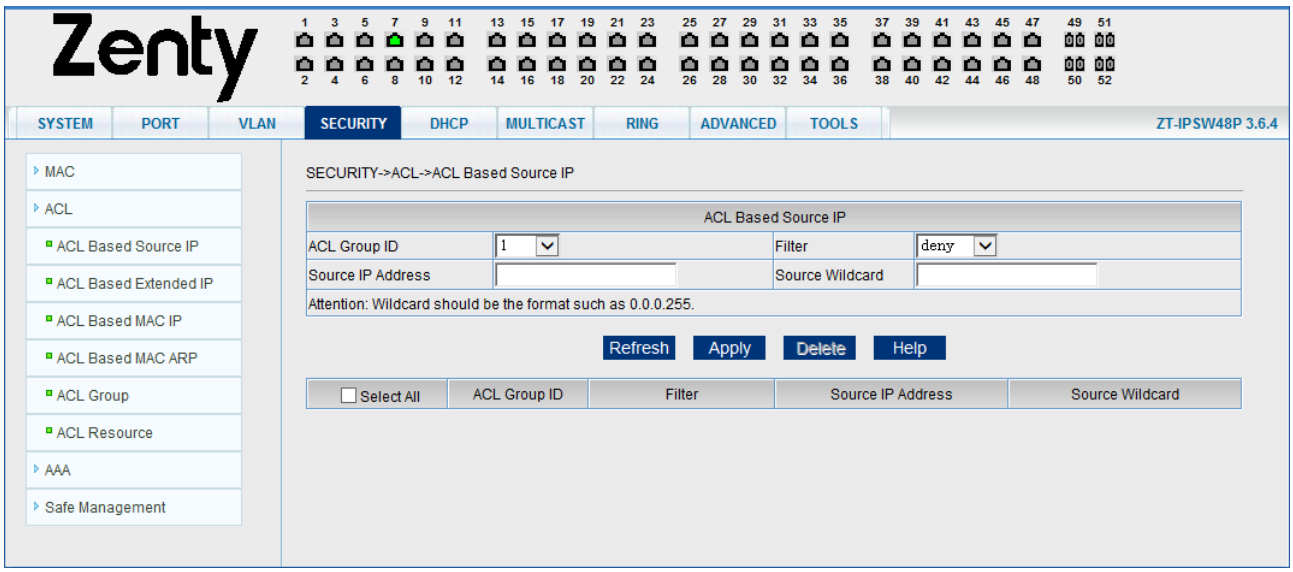
Port	All means to display the MAC addresses of all ports. others mean to display the the MAC addesses of a specified port.
VLAN ID	All means to display the MAC addresses of all VLANs. others mean to display the the MAC addesses of a specified VLAN.
MAC Table Information	Displaying the corresponding MAC table information according to the selection criteria.



（2）ACL Configuration

① IP Standard group ACL page

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



Standard IP Group ACL page

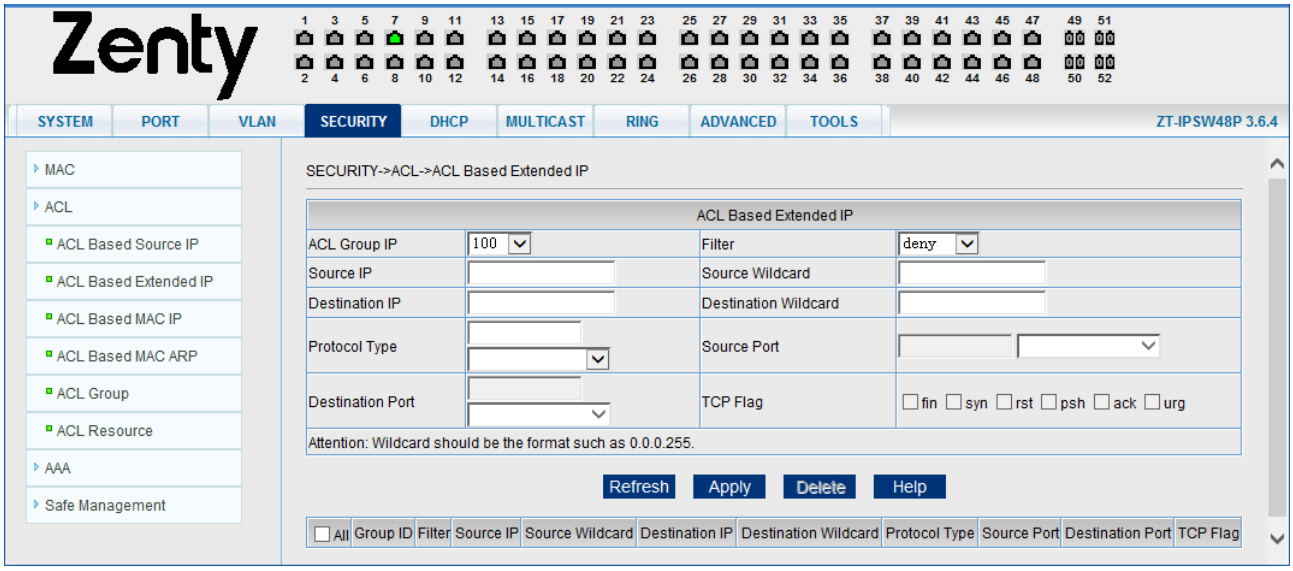
Users to configure the rules, the source IP address must be in with a mask, the rule can match the collection of IP addresses. The address mask is use anti-code, if the rule were to match the IP address range 192.168.168.0 to 192.168.168.255, then the IP address can be 192.168.168.254, and its mask of 0.0.0.255.

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

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

② IP Extended ACL configuration page

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



Extended IP Group ACL page

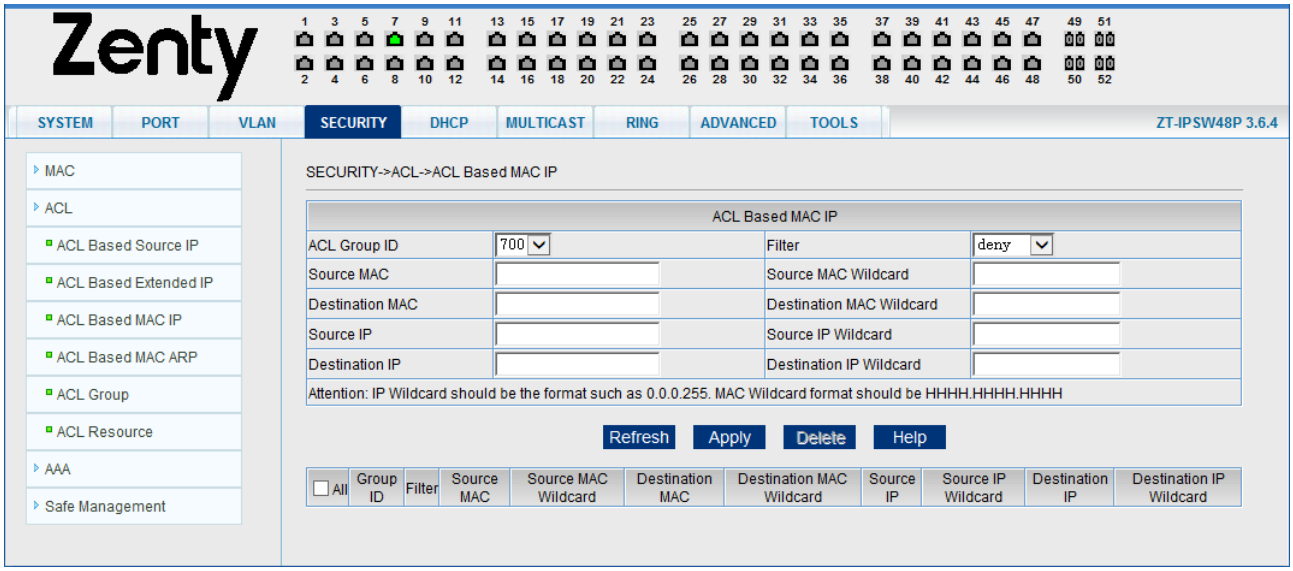
When a user configures a rule, the source IP address and destination IP address must be masked. The rule can match the set of IP addresses. The address mask is represented by an anti-code. If the rule matches the IP address range 192.168.168.0 to 192.168.168. 255, the IP address can be 192.168.168.254 and the mask is 0.0.0.255.

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

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

③ MAC IP group ACL page

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



MAC IP Group ACL page

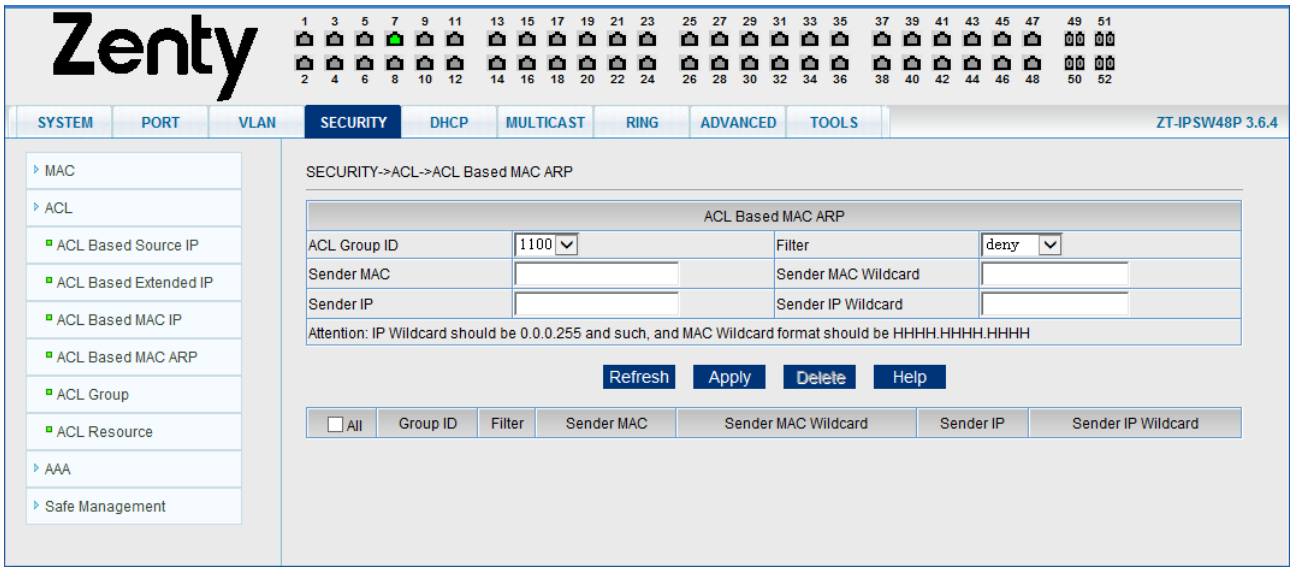
When configures a rule, the source MAC address, source IP address, and destination IP address need to match the address. The rule can match the set of MAC address and IP address. For example, if the rule matches the IP address range 192.168.168.0 to 192.168.168. 255, the IP address can be 192.168.168.254 and its mask is 0.0.0.255.

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

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

④ MAC ARP group ACL page

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



MAC ARP group ACL configuration page

When configures a rule, the MAC address and the IP address are sent with an address matching bit. The rule can match the set of MAC address and IP address. For example, if the rule matches the IP address range 192.168.168.0 to 192.168.168. 255, the IP address can be 192.168.168.254 and its mask is 0.0.0.255.

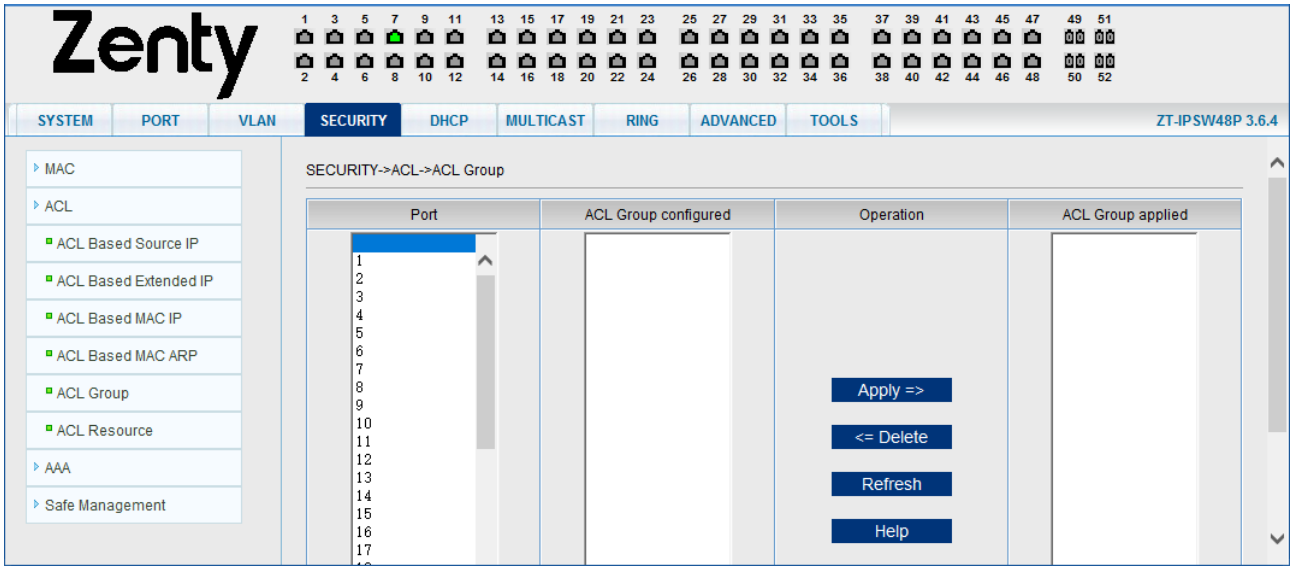
When configures a rule, each rule must have a filtering mode: allow or deny.

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

⑤ Port application ACL page

This shows the ACL application page for a port. Use this page to select an ACL group for a port and write the rules in this ACL group to the port hardware logic to enable the port to perform ACL filtering on the received packets according to these rules.

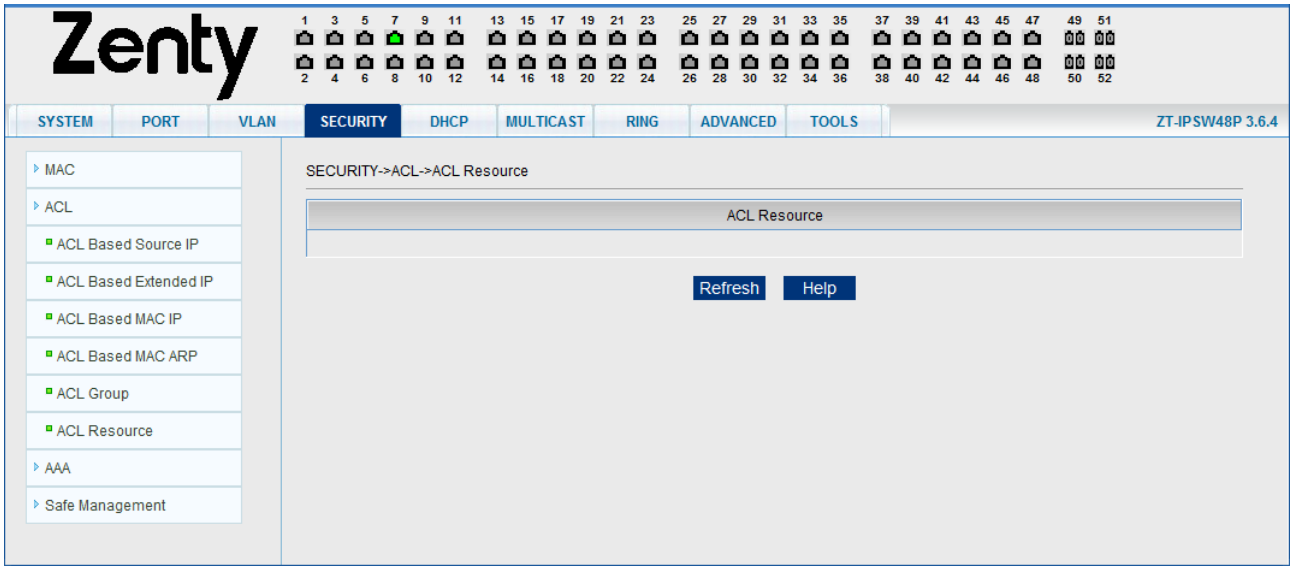
When selecting an ACL group on a port, select the IP standard, IP extension, MAC IP, and MAC ARP ACL. The selected ACL group must exist. Select the ACL rule group list and press the Add key. When deleting an ACL group, select an ACL group from the list of referenced rule groups and press the Delete key.



ACL application page for a port

⑥ ACL configuration information page

This shows the ACL configuration information page, which displays all the rules and references configured in the current ACL.

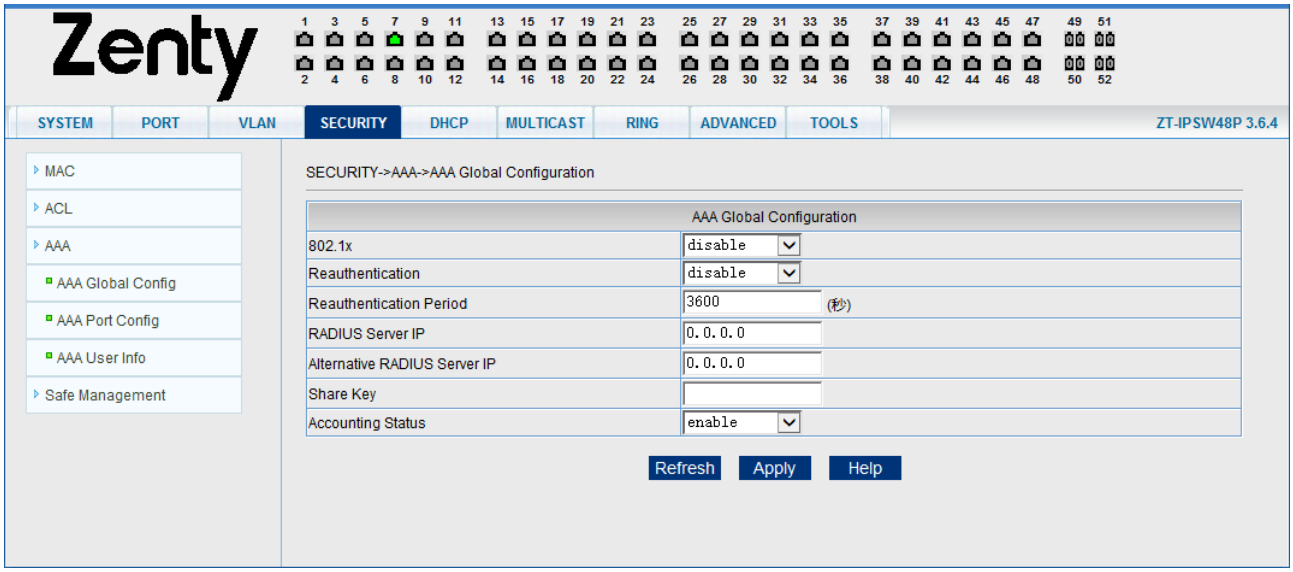


ACL configuration information page

（3）AAA configuration

① AAA global configuration page

This is the AAA global configuration page. It can configure the information related to AAA. The information that can be set includes:



AAA Global Configuration page

• Whether to enable 802.1x protocol or not, be sure to enable 802.1x protocol when doing authentication and accounting.

Whether to open the re-authentication function or not. the default is not open, in the authentication and billing according to the actual situation to decide. Turning on the reauthentication function will make the user more reliable when using authentication and billing, but will slightly increase the traffic to the network.

Set the re-authentication interval, only in the case of re-authentication function is enabled, the default is 3600 seconds, in the authentication and billing according to the actual situation to set the value, but the value should not be too small.

RADIUS server IP address, in the authentication and billing must be set when this field.

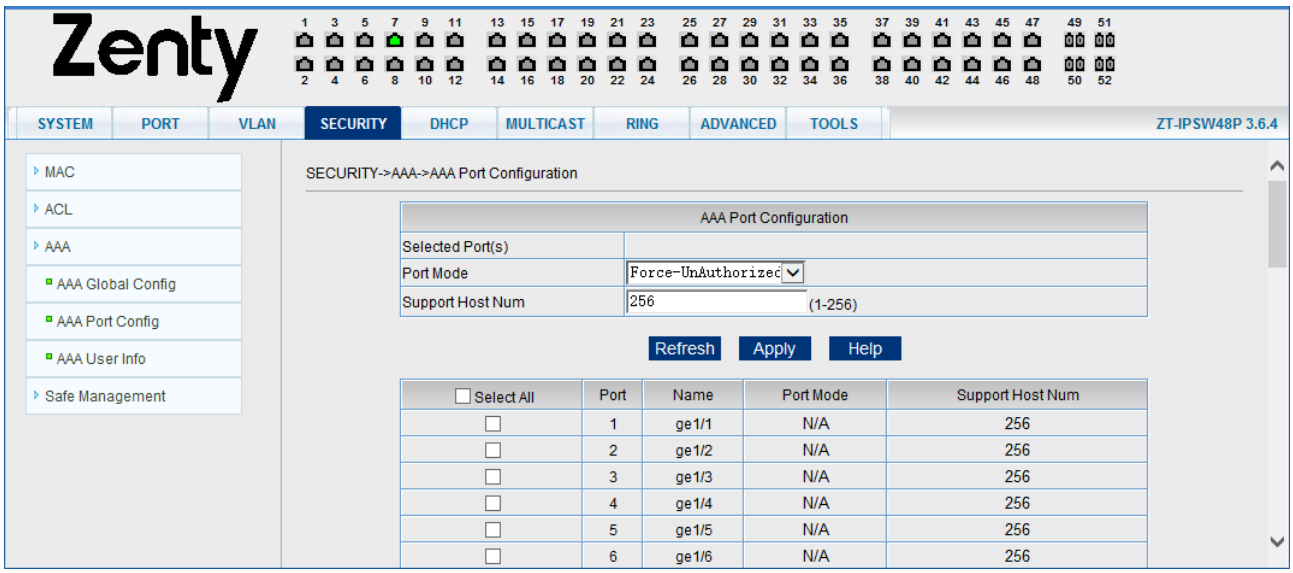
Standby RADIUS server IP address, which can be set if there is an alternate RADIUS server.

shared key, used to set the switch and the Radius server between the encrypted shared password, in the authentication and billing must be set this field, and to the same settings on the Radius server.

Whether to start billing, the default is to start, when doing the authentication and billing to start billing.

② AAA port configuration page

This shows the AAA port configuration page. Configure the authentication port mode and the maximum number of hosts supported by this page, and can view the configuration of each port. To modify the port AAA 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, several consecutive ports with the connection number. When the settings are successful, the selected ports are configured with the same parameters. The AAA port mode includes four types: N / A status, Auto status, Force-authorized status, and Force-unauthorized status. When a port needs to do 802.1x authentication, the port should be set to Auto state, if no authentication it can access the network, the port is set to N / A state, the other two states in the practical application rarely used.

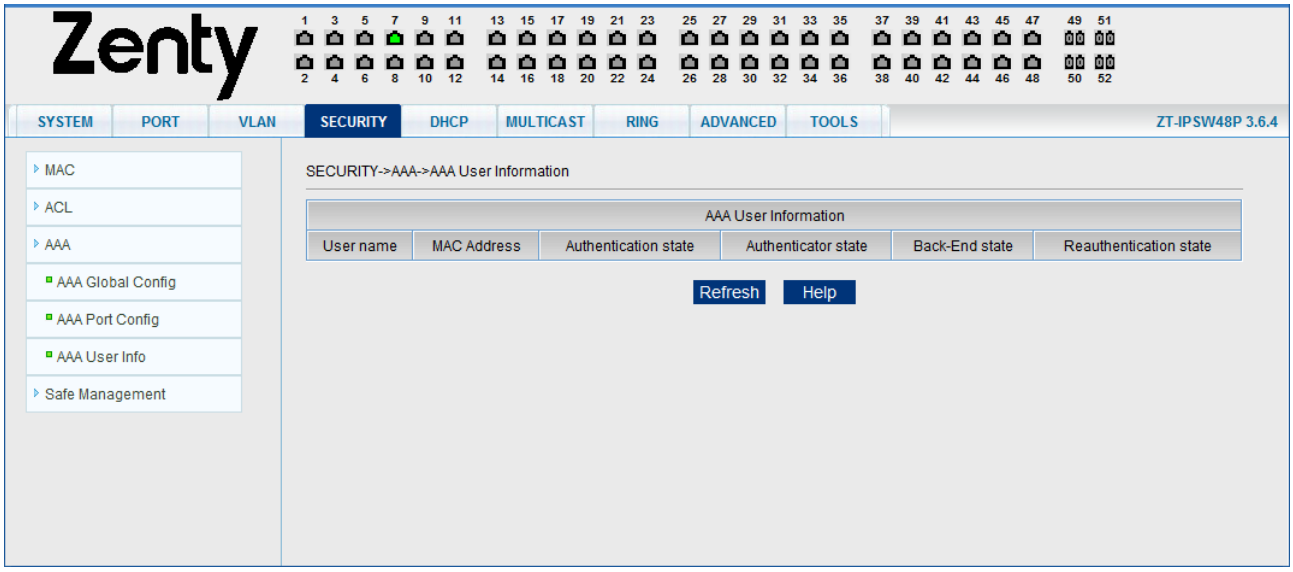


AAA port configuration page

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

③ AAA user information page

Figure 50 is the AAA user information page, the user can view the page under a port access to all users of the state information,

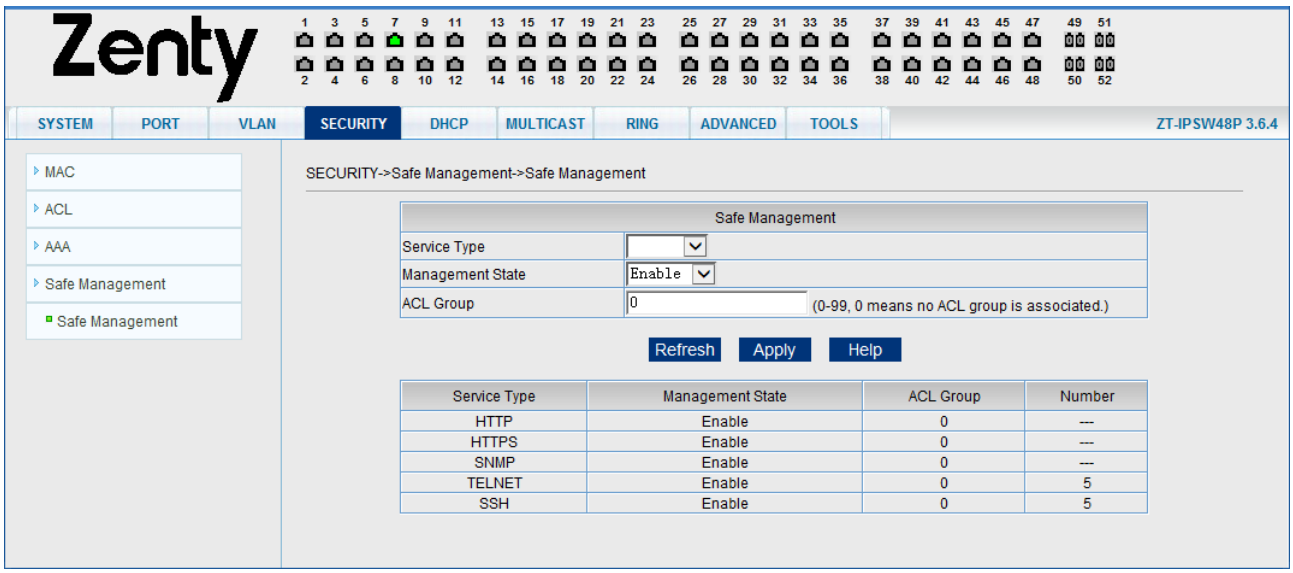


AAA user information page

（4）local management security configuration

① Safe Manage configuration page

This is the management rights configuration page, through the configuration of the page, the administrator can control the network management services TELNET, WEB and SNMP, can enable or disable these services, these services can be IP standard ACL Group up to implement the source IP address control, control the host access to these services.



Safe Management Configuration page

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

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

2.6 DHCP

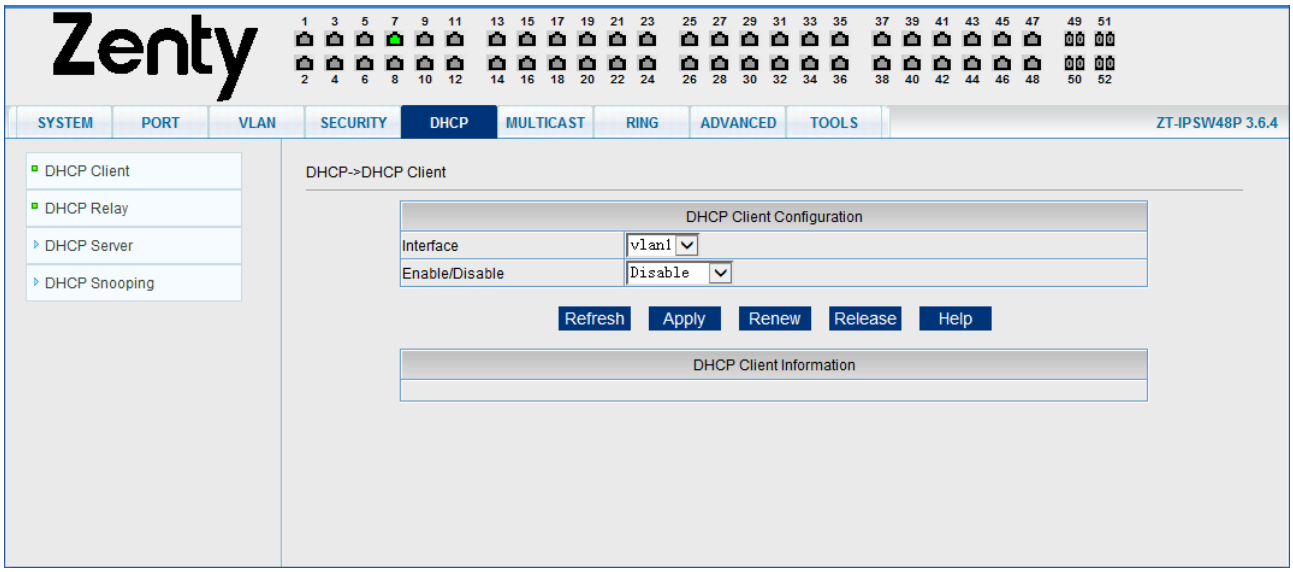
(1) DHCP Client

This page is used to configure DHCP client.

Interface: Select the layer 3 VLAN interface to be configured.

Enable/Disable: Enable or disable the DHCP client feature of the specified interface.

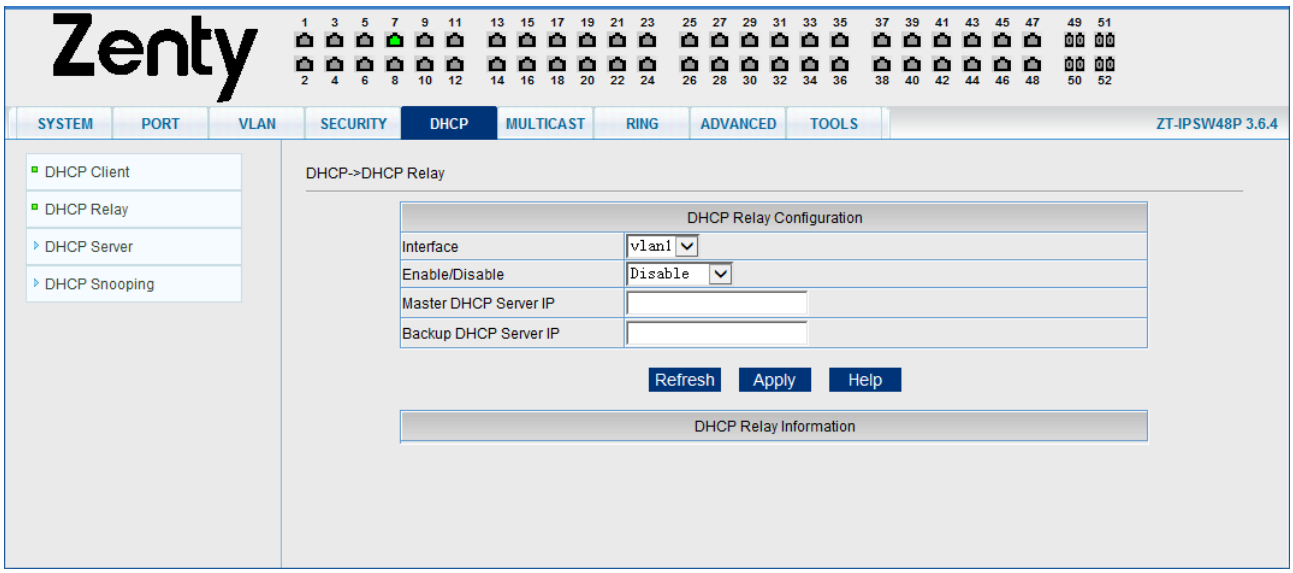
DHCP Client Information: Display the DHCP client information.



DHCP client Configuration page

(2) DHCP Relay

This page is used to configure DHCP relay.



DHCP Relay Configuration page

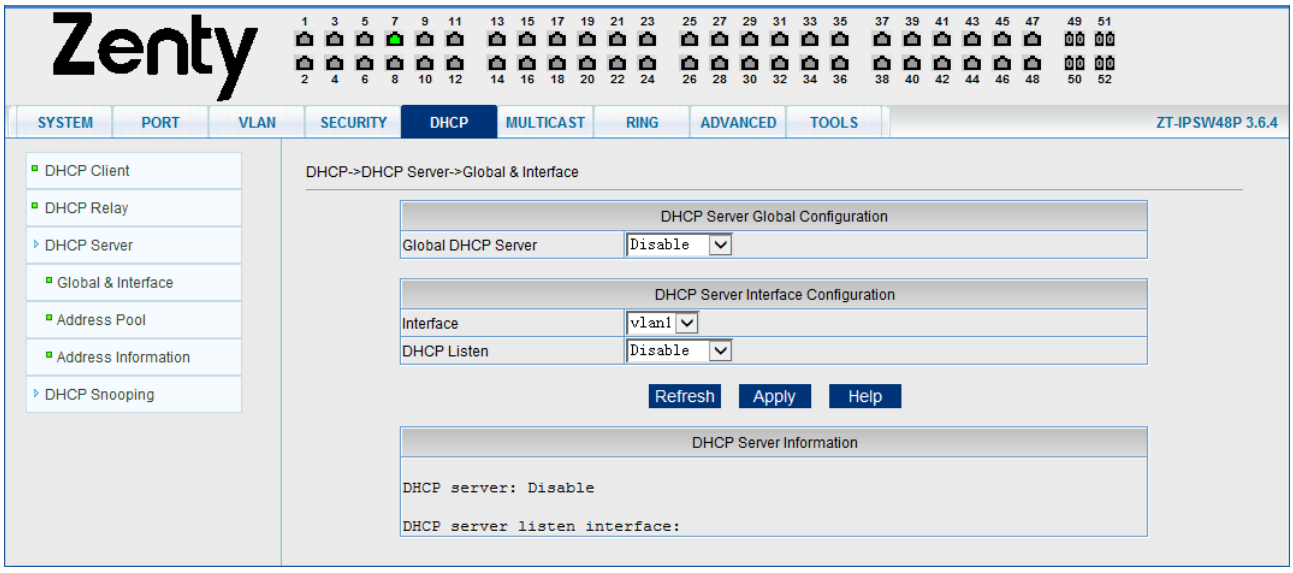
Interface: Select the layer 3 VLAN interface to be configured.
Enable/Disable: Enable or disable the DHCP relay feature of the specified interface.
Master DHCP Server IP: Set the master DHCP server IP address.
Backup DHCP Server IP: Set the backup DHCP server IP address.
DHCP Relay Information: Display the DHCP relay information.

(3) DHCP Server

① DHCP Server Global & Interface Configuration

This page is used to configure DHCP server, including global and interface configuration.

Global DHCP Server: Enable or disable global dhcp server.
Interface: Select the layer 3 VLAN interface to be configured.
DHCP Listen: Enable or disable the DHCP listen feature of the specified interface.
DHCP Server Information: Display the DHCP server global and interface configuration information.



DHCP Server Information page

② DHCP Server Address Pool Configuraiton

This page is used to configure DHCP server address pool.

Address Pool Name: To be created Set the address pool name to be created, then click "Create" button.
Address Pool Name: To be configured Select the address pool name to be configured.
Address Range: Set the range of IP addresses that can be assigned to DHCP clients in this address pool.

Subnet Mask: Set the subnet mask that this address pool can assign to DHCP clients.

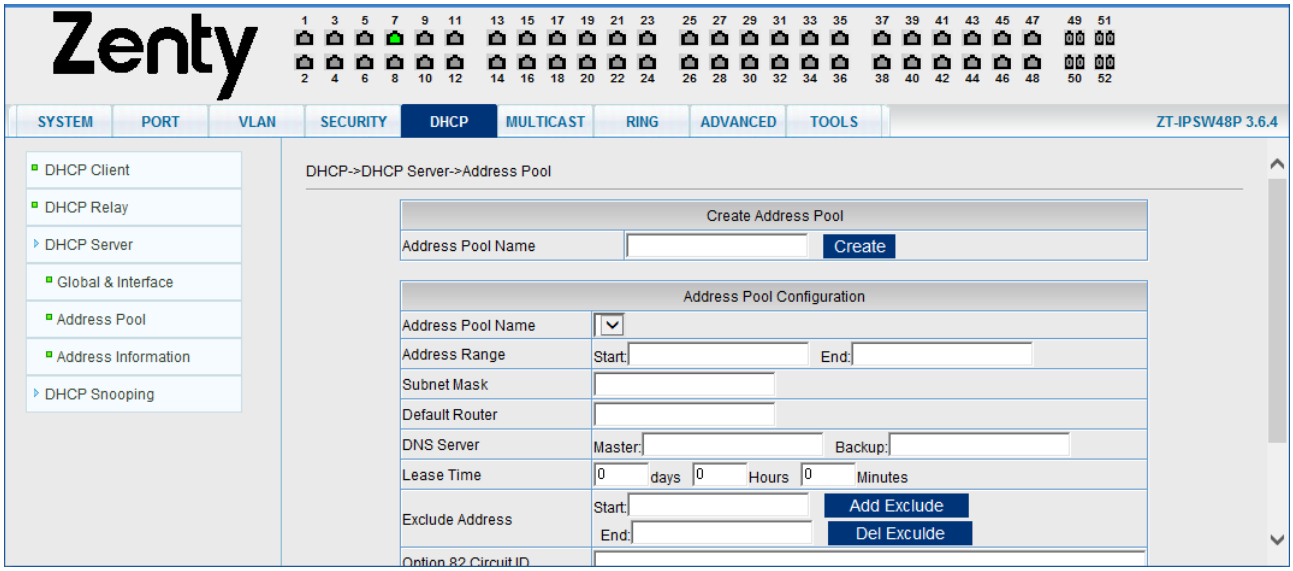
Default Router: Set the default router that this address pool can assign to DHCP clients.

DNS Server: Set the IP addresses of the DNS server that this address pool can assign to DHCP clients. You can set the master and backup DNS server IP addresses.

Lease Time: Set the lease time that this address pool can assign to DHCP clients. You can set a limited lease time of days, hours and minutes or select infinite lease time.

Exclude Address: Set the exclude address range to not be assigned to DHCP clients. You can add or delete exclude address by clicking the two buttons.

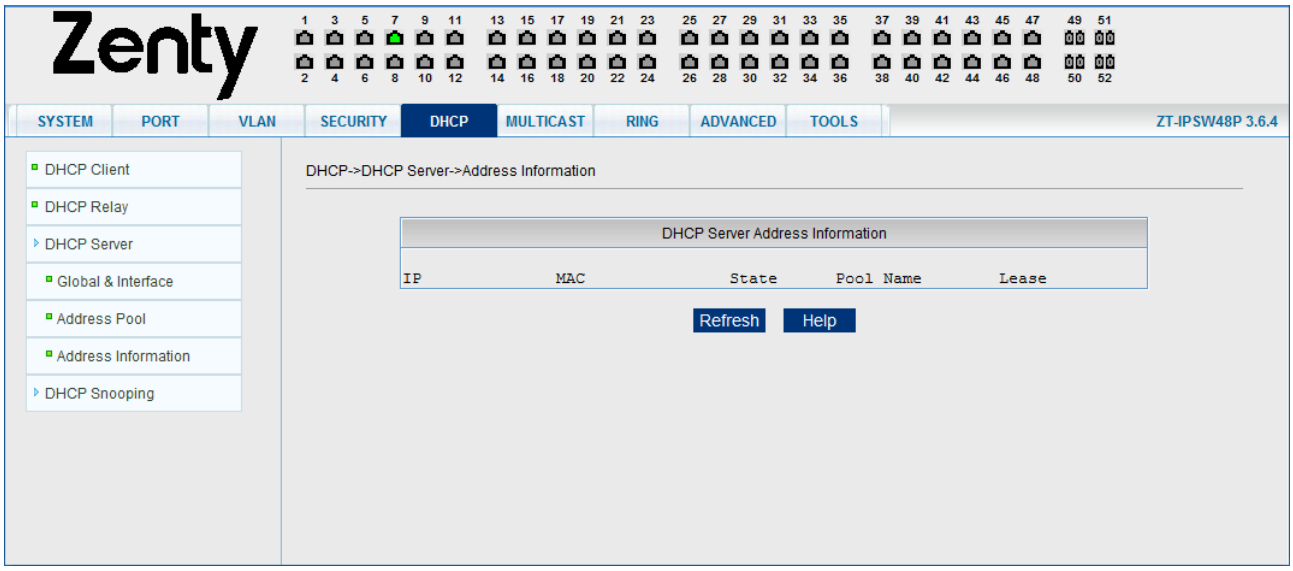
Option 82 Circuit ID: Set the option 82 circuit id applicable to the address pool.



Address Pool configuration page

③ DHCP Server Address Information

This page is used to display the IP address information being assigned or assigned to DHCP clients.



DHCP Server Address information page

（4）DHCP Snooping Global configuration

① Global Configuration

This page is used to configure global DHCP snooping.

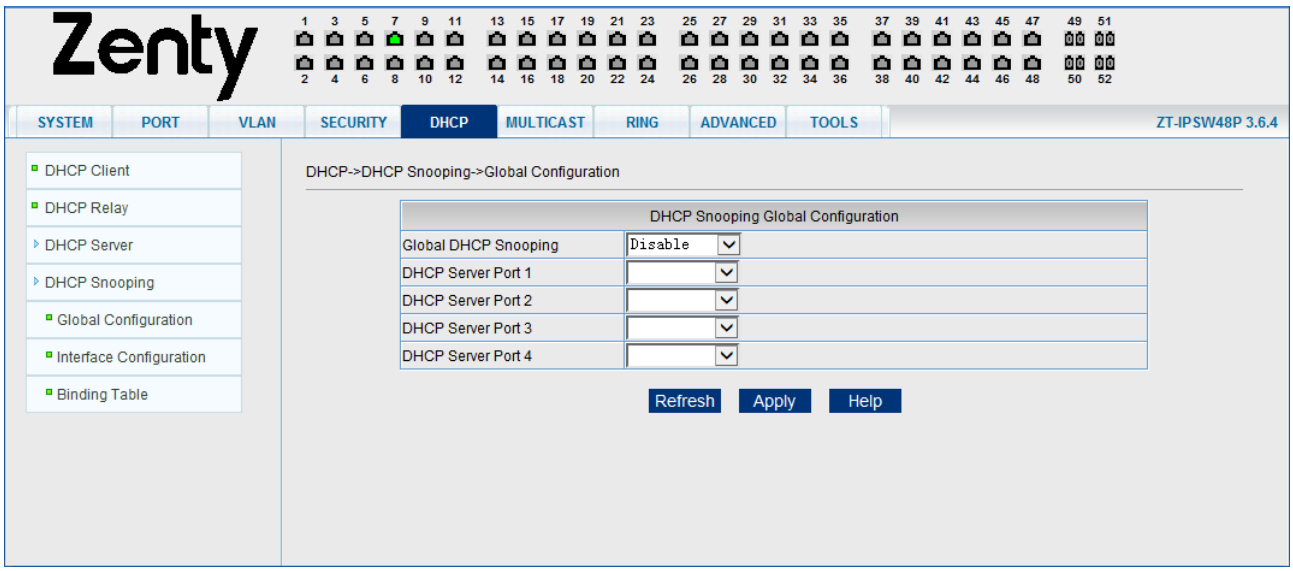
Global DHCP Snooping: Enable or disable global DHCP snooping.

DHCP Server Port 1: Select the trusted port to which the DHCP server is connected. Up to four DHCP server trusted ports can be selected.

DHCP Server Port 2: Select the trusted port to which the DHCP server is connected. Up to four DHCP server trusted ports can be selected.

DHCP Server Port 3: Select the trusted port to which the DHCP server is connected. Up to four DHCP server trusted ports can be selected.

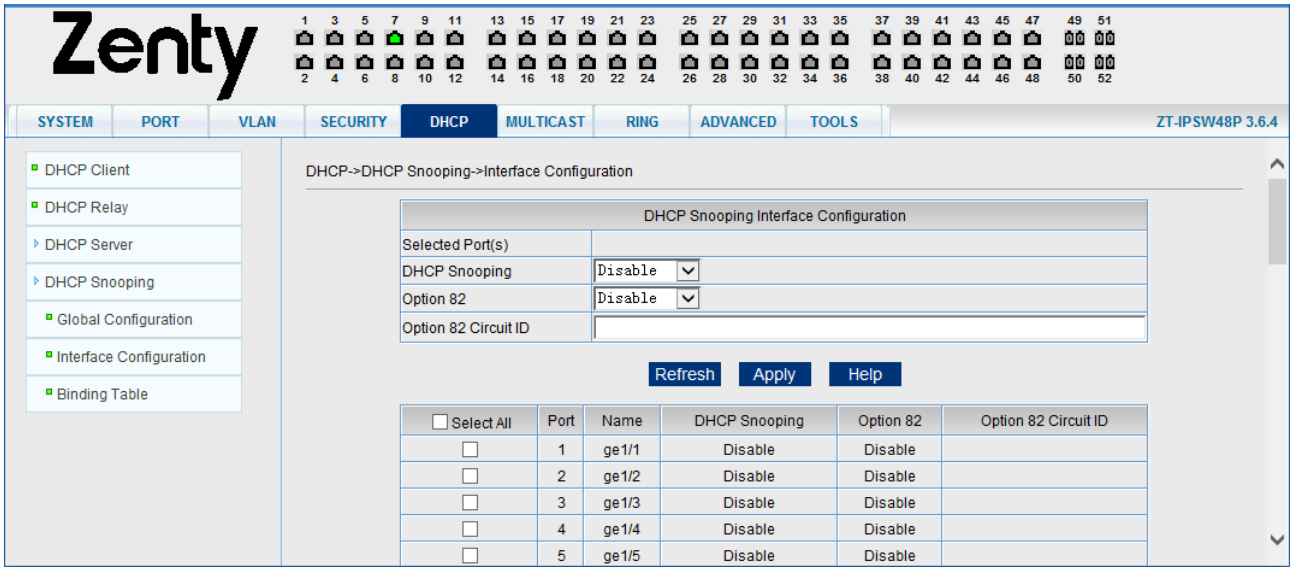
DHCP Server Port 4: Select the trusted port to which the DHCP server is connected. Up to four DHCP server trusted ports can be selected.



DHCP Snooping Global configuration page

② DHCP Snooping Interface Configuration

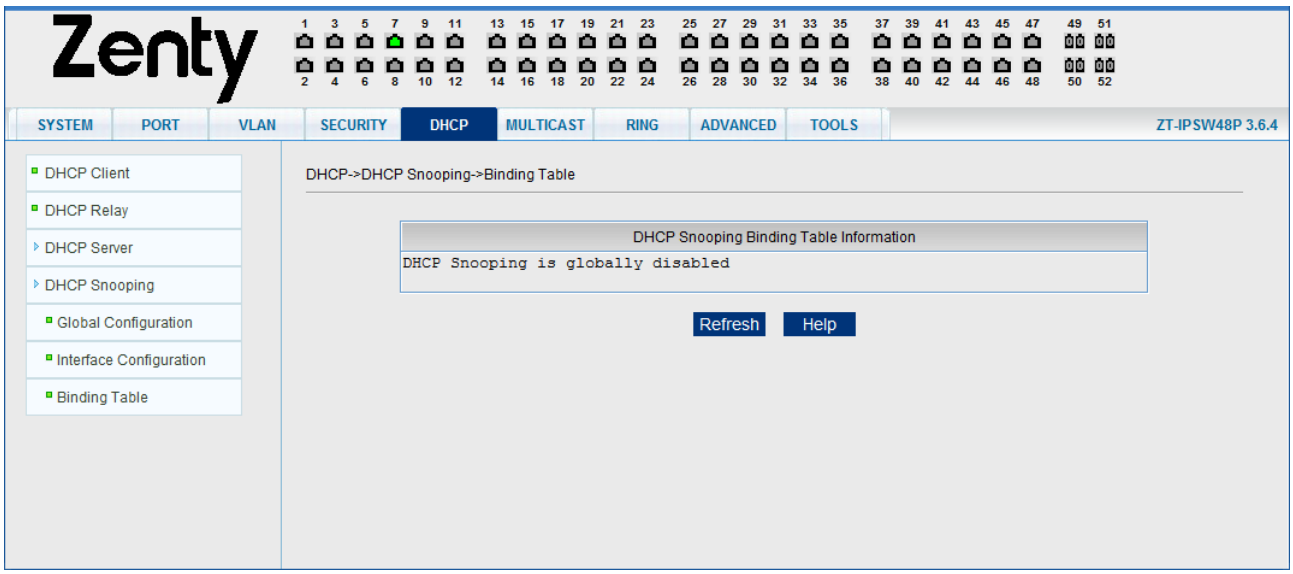
This page is used to configure DHCP snooping interface.



DHCP Snooping Interface Configuration page

③ DHCP Snooping Binding Table Information

This page is used to display DHCP snooping binding table information.



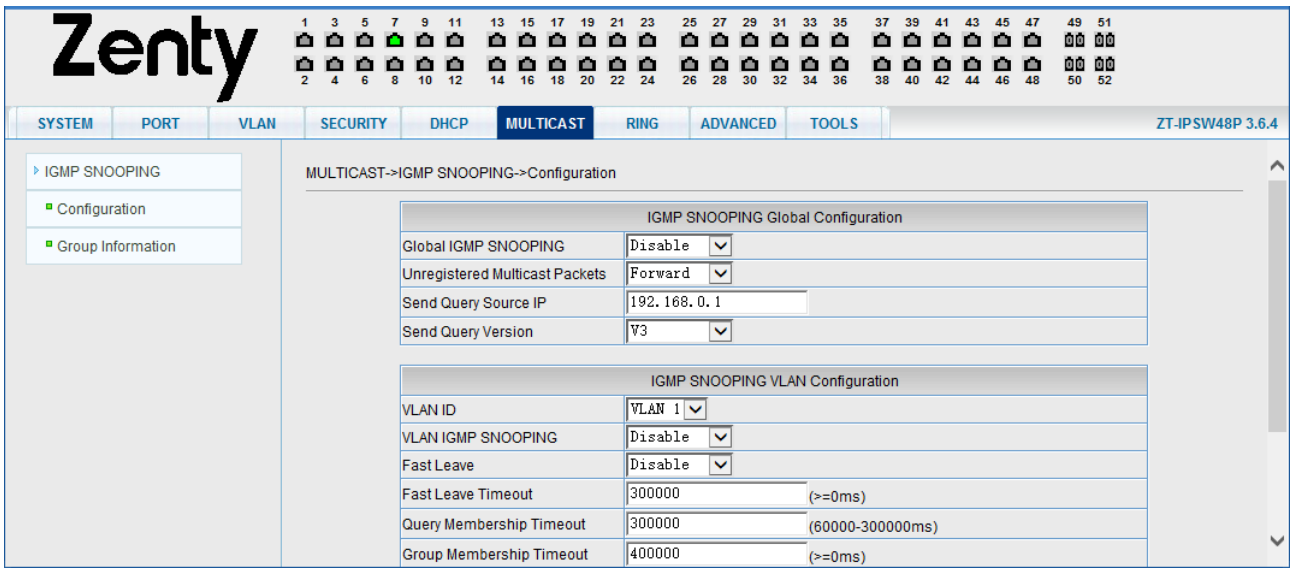
DHCP Snooping Binding Table Information

2.7 Multicast configuration

（1）IGMP SNOOPING configuration

① IGMP SNOOPING Configuration page

This is the IGMP SNOOPING configuration page. Users can enable IGMP Snooping on this page.

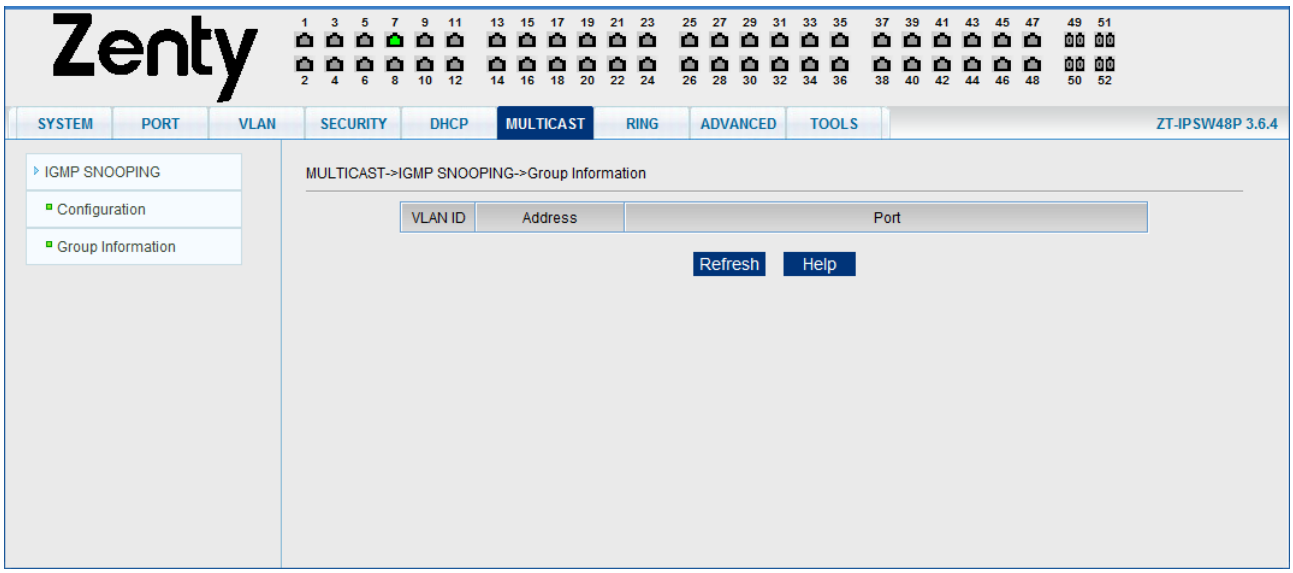


IGMP SNOOPING configuration page

Global IGMP SNOOPING: Enable or disable global-based IGMP snooping. The default value is disabled.
VLAN ID: Select a VLAN to do the following configuration.
VLAN IGMP SNOOPING: Enable or disable VLAN-based IGMP snooping.
Fast Leave: Enable or disable VLAN-based IGMP snooping fast leave function.
Fast Leave Timeout: Set VLAN-based IGMP snooping fast leave timeout.
Query Membership Timeout: Set VLAN-based IGMP snooping query membership timeout.
Group Membership Timeout: Set VLAN-based IGMP snooping group membership timeout.
Querier: Enable or disable the VLAN to send IGMP query packets.
Query Interval: Set the interval for sending IGMP query packets in this VLAN.

② Multicast Group Information

This page is used to display multicast group information.



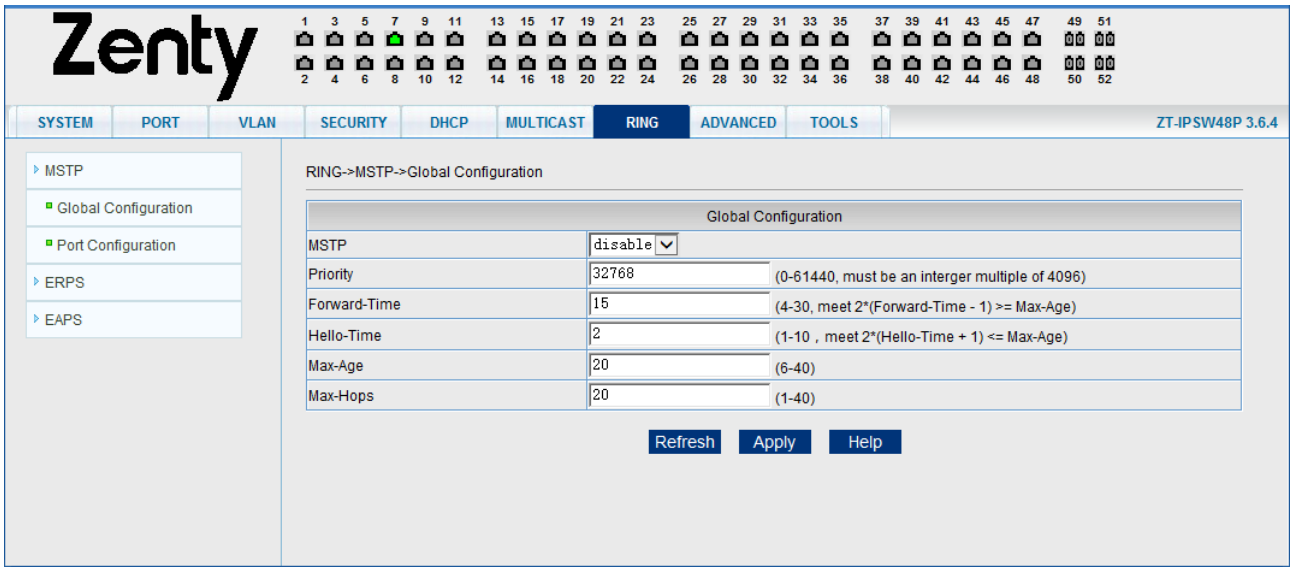
Multicast Group Information page

2.8 RING

（1）Spanning tree configuration

① Spanning tree global configuration page

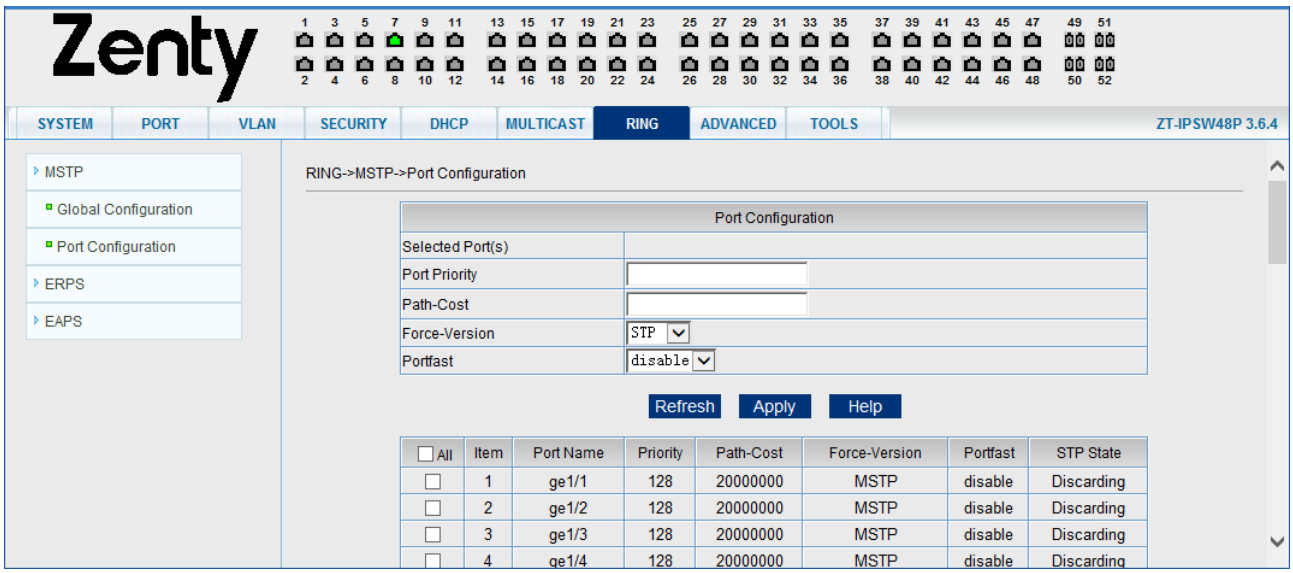
This is the spanning tree global configuration page, where users can configure global spanning tree parameters



Spanning Tree Global Configuration page

② Spanning tree port configuration page

This shows the spanning tree port configuration page. Users can view the port MSTP status on this page.



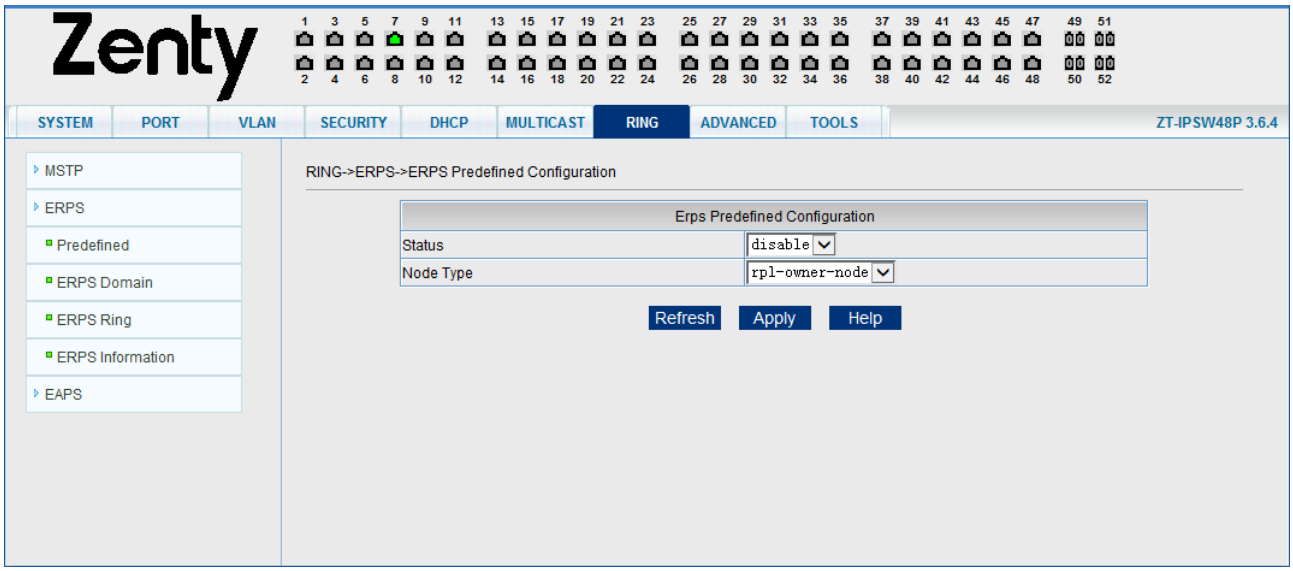
Spanning tree port configuration page

（2）ERPS configuration

① ERPS predefined configuration page

This is the ERPS Predefined Configuration page, which enables the ERPS pre-configuration configuration. When enable the ERPS predefined configuration, can specify the node type: the master node or the transit node.

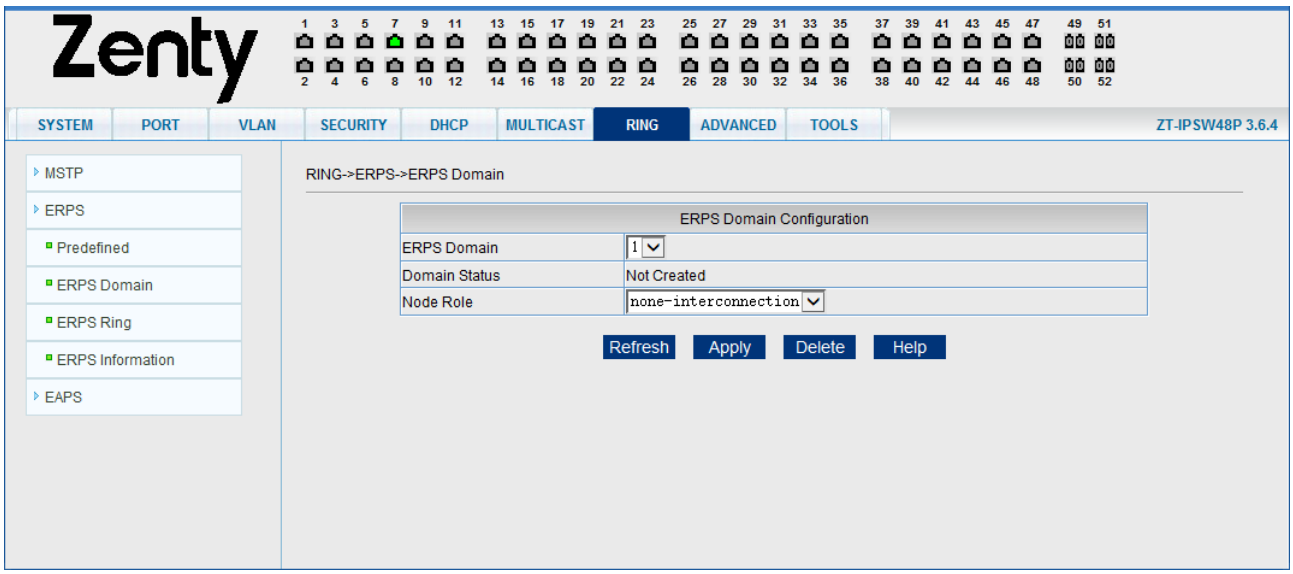
For example, the ERPS instance number is 1, the ERPS mode is 1, the ring mode is the primary ring mode, the protocol VLAN is VLAN3001, the data VLAN is VLAN1, the rpl port is 51, the rl port is 52, and the recovery behavior is re- coverable, Hold-off time is 0, guard time is 500 milliseconds, wtr time is 5 minutes, wtb time is 5 seconds, protocol message transmission time is 5 seconds.



ERPS predefined configuration page

② ERPS instance configuration page

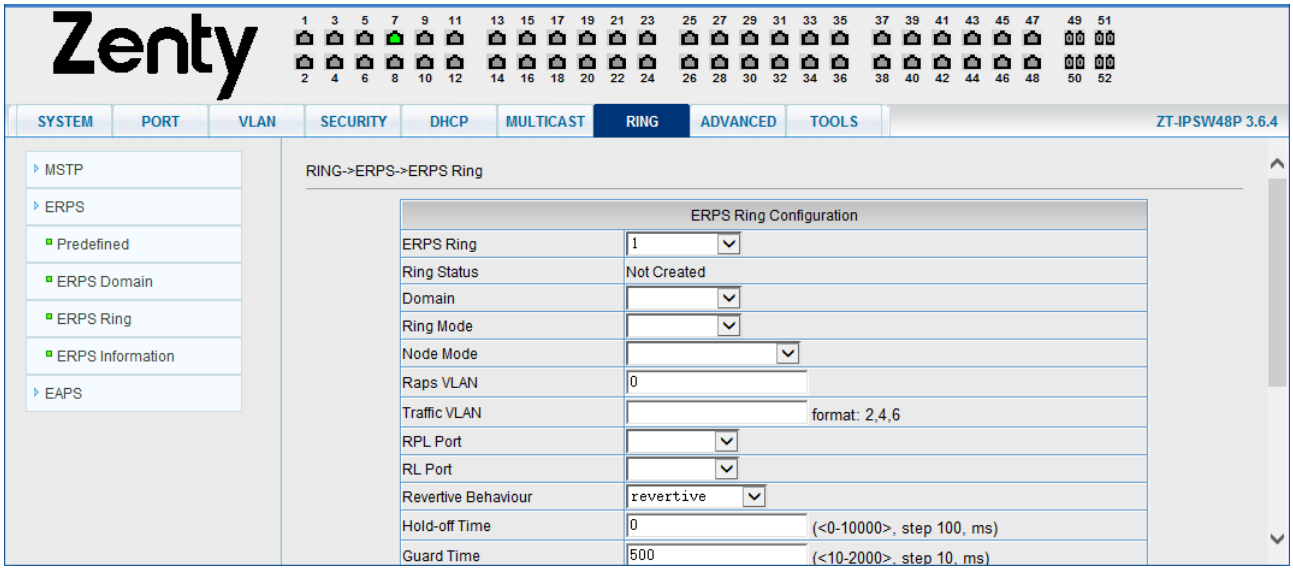
This is the ERPS Instance Configuration page, where you can configure ERPS instances. When an instance is not created, click the Apply button to create and specify a role; if the instance has been created and has no associated ring, the role can be modified; if the instance has been created and the ring is associated, the instance can not be modified. Click the Delete button to delete the selected instance. It can configure up to 8 instances.



ERPS instance configuration page

③ ERPS ring configuration page

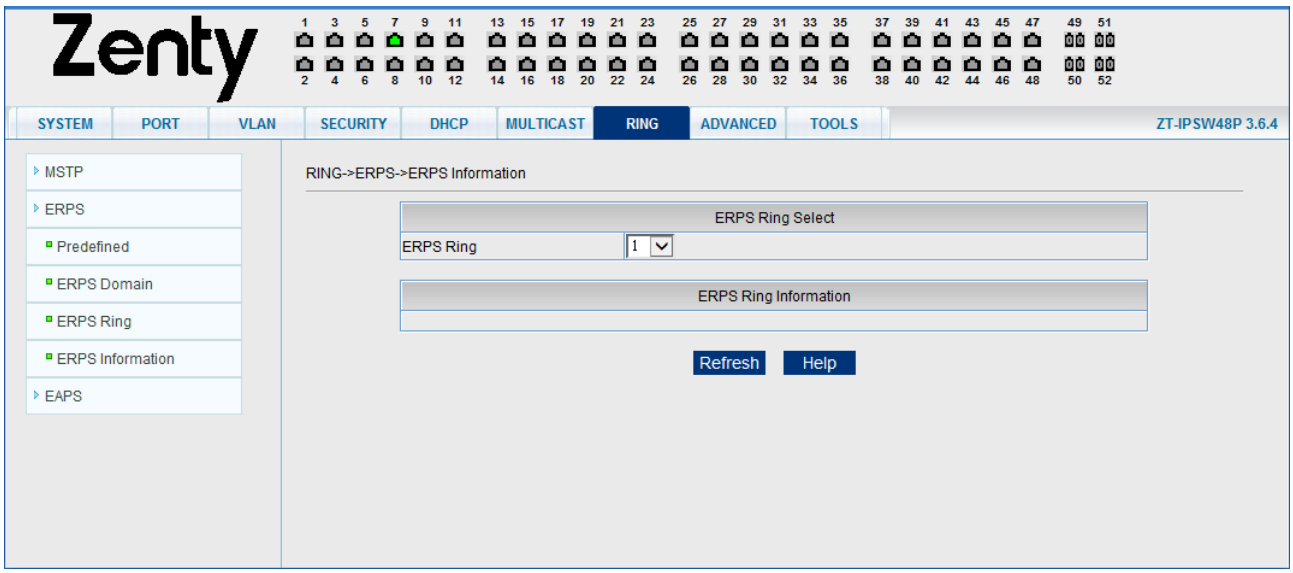
This is the ERPS ring configuration page, through which user can create and configure an ERPS ring. Select a ring, when the ring is not created, click the Apply button to create the ring and set the configuration information, has been created to modify the configuration information. Click the Delete button to delete the selected ring. The ring must and can only be associated with an instance, and up to 32 loops can be configured. When a ring failure is detected, click the Manual Restore button to resume.



ERPS ring configuration page

④ ERPS information page

This is the ERPS information page, and the selected ring number displays the configuration and status information of the associated ERPS ring.



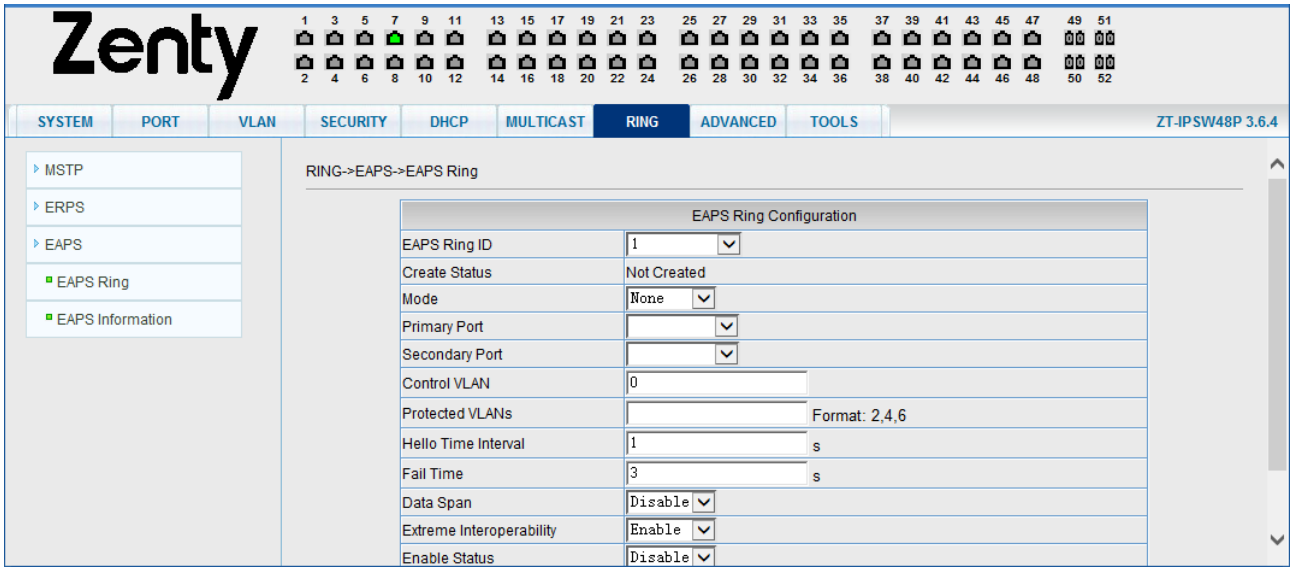
RPS information page

（3）EAPS configuration

① EAPS configuration page

This is an EAPS configuration page, through which you can configure some EAPS related information, including:

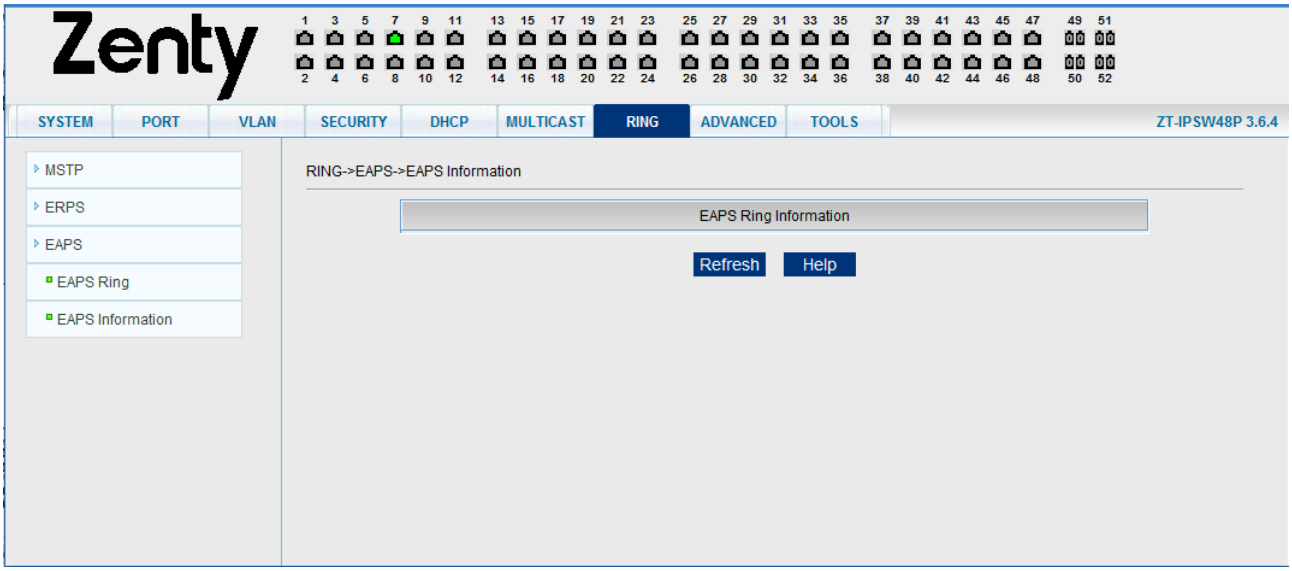
- Select an EAPS ring number.
- Configure the operating node mode of an EAPS Domain.
- Configure Primary Port of EAPS Domain.
- Configure Secondary Port of EAPS Domain.
- Configure a control VLAN for EAPS Domain.
- Add one or more protected VLANs of the EAPS Domain.
- Configure an EAPS Domain to periodically send HEALTH packets. Hello-timer must be less than fail-time.
- Set the fail-period timer of one EAPS domain to expire.
- Enable or disable compatibility with Extreme devices.
- Whether to enable



EAPS Configuration Page

② EAPS information page

This is an EAPS information page, through which users can view some EAPS related information.

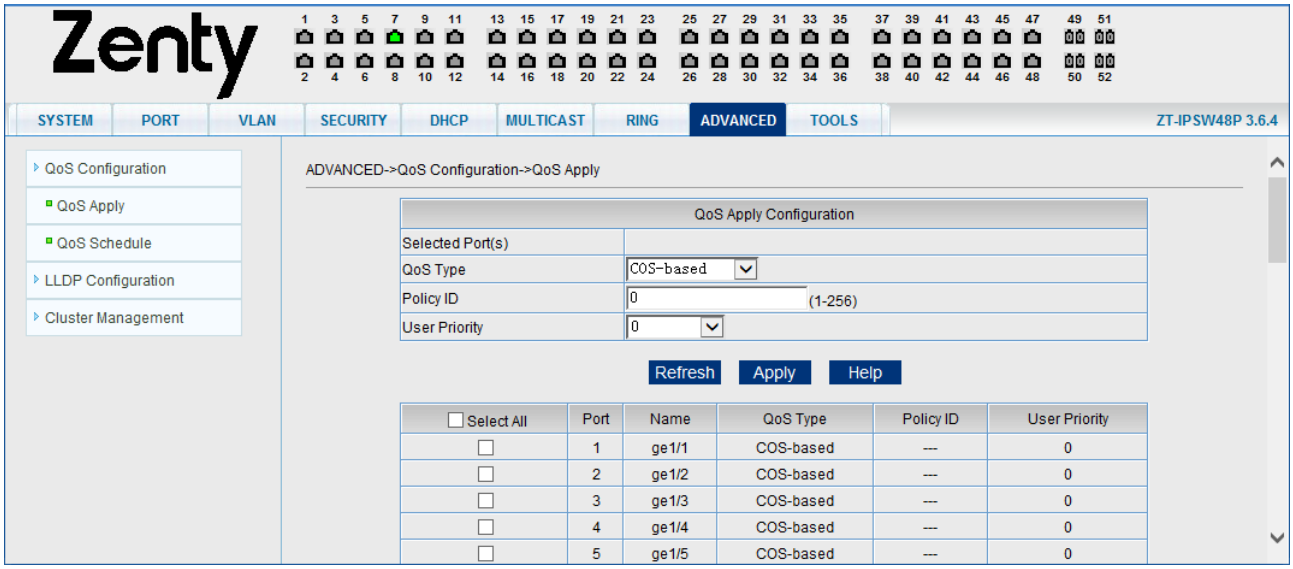


EAPS information page

2.9 Advanced configuration

（1）QoS Apply Configuration Page

This is a QoS Apply configuration page



QoS Apply configuration page

Select Port(s): Select Port(s) from the following list.

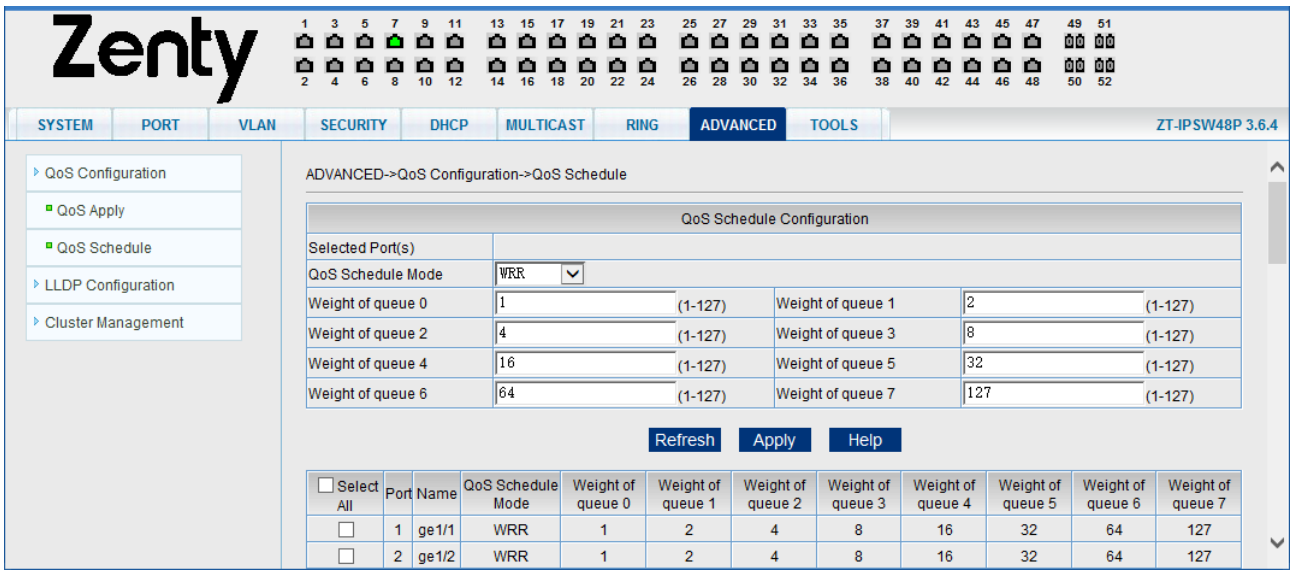
QoS Type: Three QoS types: COS-based, DSCP-based and Apply-policy. The default value is COS-based.

Policy ID: Only valid if the QoS type is Apply-policy. The policy ID must exist before setting.

User Priority: The user proirity is valid only when the incoming packets are not tagged with VLAN. The default value is 0.

（2）QoS Schedule Configuration Page

This is a QoS Schedule configuration page.



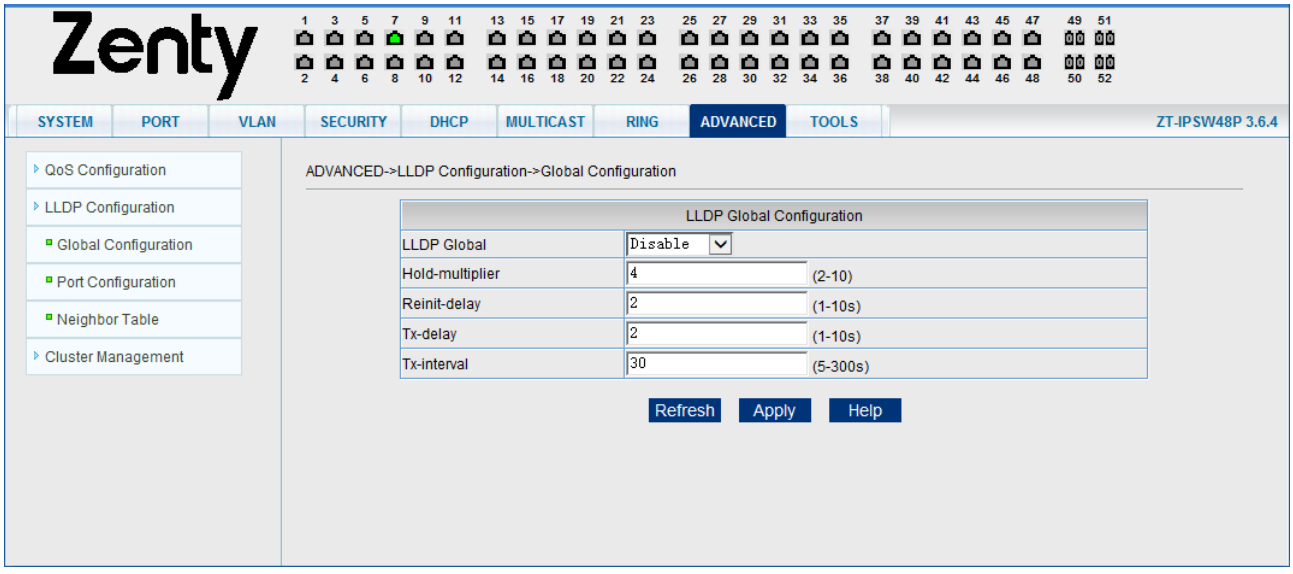
QoS Schedule configuration page

Select Port(s): Select Port(s) from the following list.
QoS Schedule Mode: Four QoS schedule modes: SP, RR, WRR and WDRR. The default value is WRR.
Weight of queue 0: The weight of queue 0 ranges from 1 to 127. The default value is 1.
Weight of queue 1: The weight of queue 1 ranges from 1 to 127. The default value is 2.
Weight of queue 2: The weight of queue 2 ranges from 1 to 127. The default value is 4.
Weight of queue 3: The weight of queue 3 ranges from 1 to 127. The default value is 8.
Weight of queue 4: The weight of queue 4 ranges from 1 to 127. The default value is 16.
Weight of queue 5: The weight of queue 5 ranges from 1 to 127. The default value is 32.
Weight of queue 6: The weight of queue 6 ranges from 1 to 127. The default value is 64.
Weight of queue 7: The weight of queue 7 ranges from 1 to 127. The default value is 127.

(3) LLDP Global Configuration

This page is use to configure LLDP global parameters.

LLDP Global	Enable or disable the global LLDP, default is disabled
Hold-multiplier	Set the hold-multiplier, default is 4
Reinit-delay	Set the Reinit-delay, default is 2 seconds
Tx-delay	Set the tx-delay, default is 2 seconds
Tx-interval	Set the tx-interval, default is 30 seconds

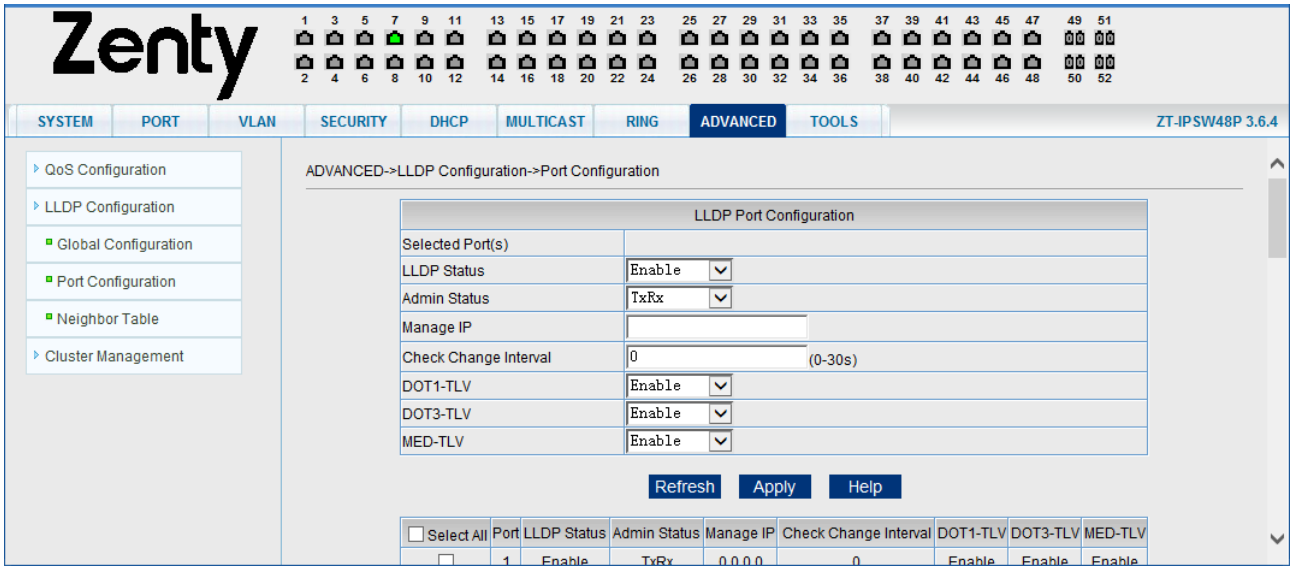


LLDP Global Configuration page

(4) LLDP Port Configuration

This page is use to configure LLDP ports' parameters.

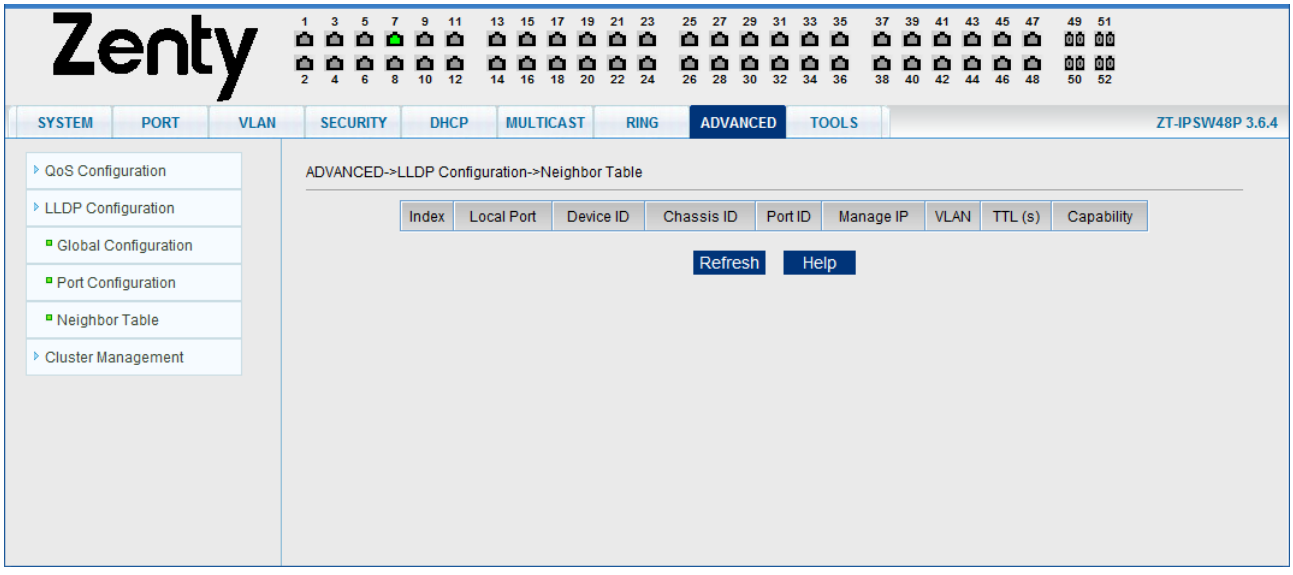
Select Port(s)	Select Port(s) from the following list.
LLDP Status	Enable or disable the LLDP of the configured port, default is enabled
Admin Status	Set the admin status of the configured port, four status are disable, Tx, Rx and TxRx, default is TxRx
Manage IP	Set the management IP address of the configured port, use to packege the management TLV
Check Change Interval	Set the interval for querying local changed configuration, default is 0, means no query
DOT1-TLV	Wether the LLDP packets sent from the configured port include the DOT1-TLV, default is inclusion
DOT3-TLV	Wether the LLDP packets sent from the configured port include the DOT3-TLV, default is inclusion
MED-TLV	Wether the LLDP packets sent from the configured port include the MED-TLV, default is inclusion



LLDP Port Configuration page

(5) LLDP Neighbor Table

This page is use to display all the LLDP neighbor information.



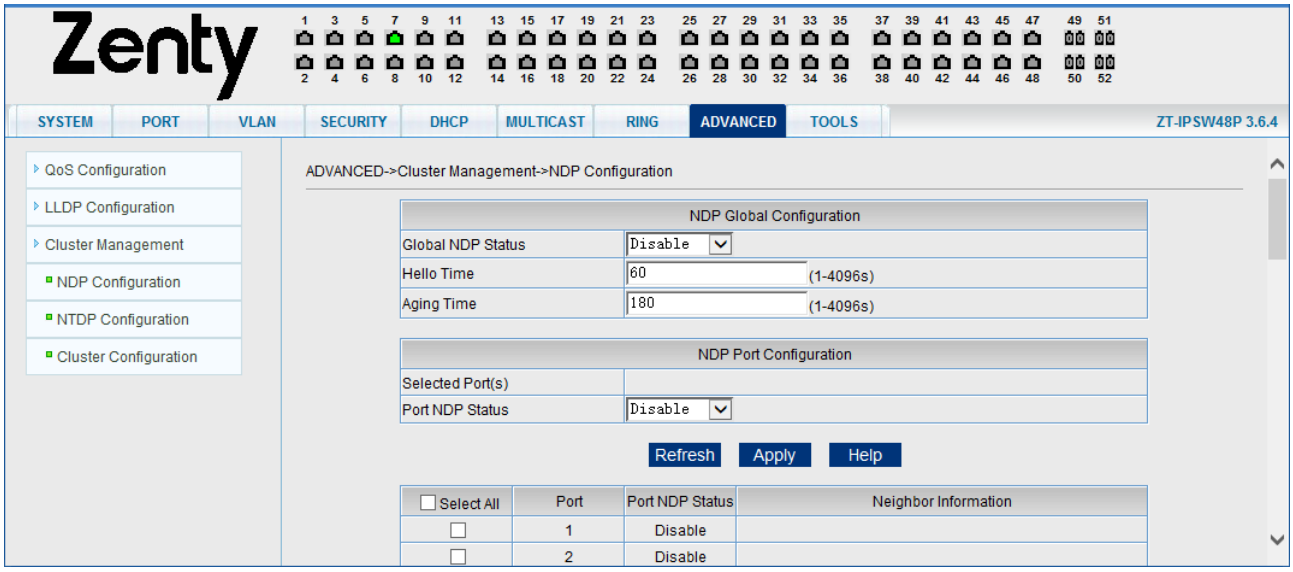
Neighbor Table page

(6) NDP Configuration

This page is use to configure the NDP function.

Global NDP Status	Enable or disable the Global NDP status.
Hello Time	Set NDP hello timer in seconds, default value is 60 seconds.

Aging Time	Set NDP aging timer in seconds, default value is 180 seconds.
Select Port(s)	Select Port(s) from the following list.
Port NDP Status	Enable or disable the NDP status of the selected ports.

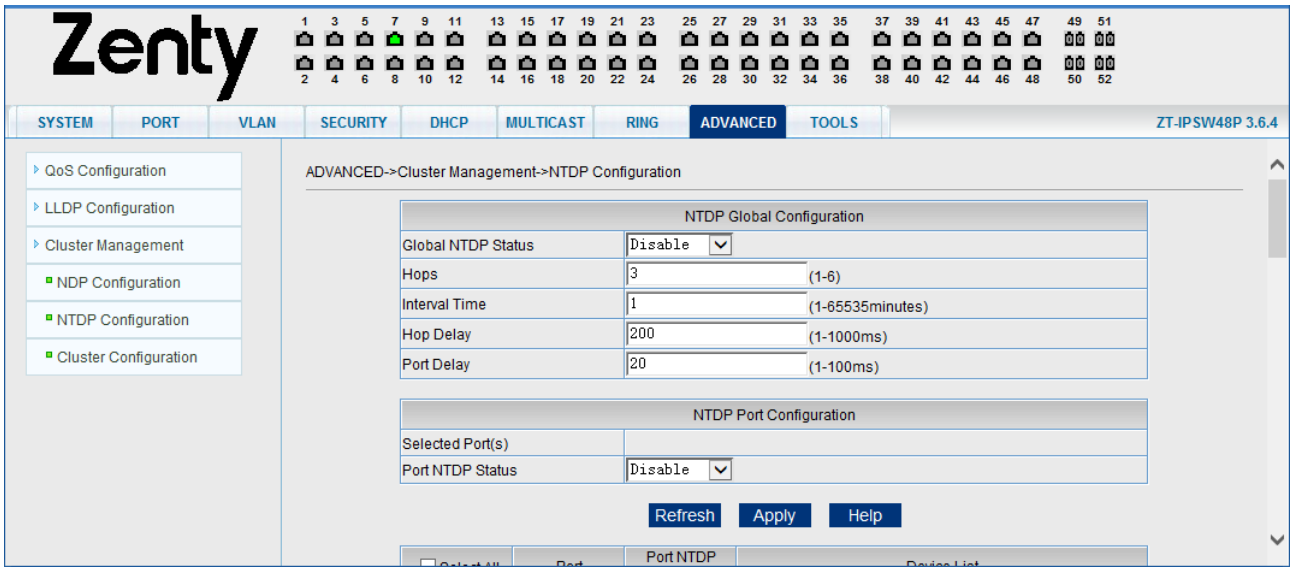


NDP Global Configuration page

(7) NTDP Configuration

This page is use to configure the NTDP function.

Global NTDP Status	Enable or disable the Global NTDP status.
Hops	Set NTDP collect hops, default value is 3.
Interval Time	Set NDTP auto collect timer interval in minutes, default value is 1 minute.
Hop Delay	Set NTDP request transmit first delay time, default value is 200ms.
Port Delay	Set NTDP request transmit to next port delay time, default value is 20ms.
Select Port(s)	Select Port(s) from the following list.
Port NTDP Status	Enable or disable the NTDP status of the selected ports.



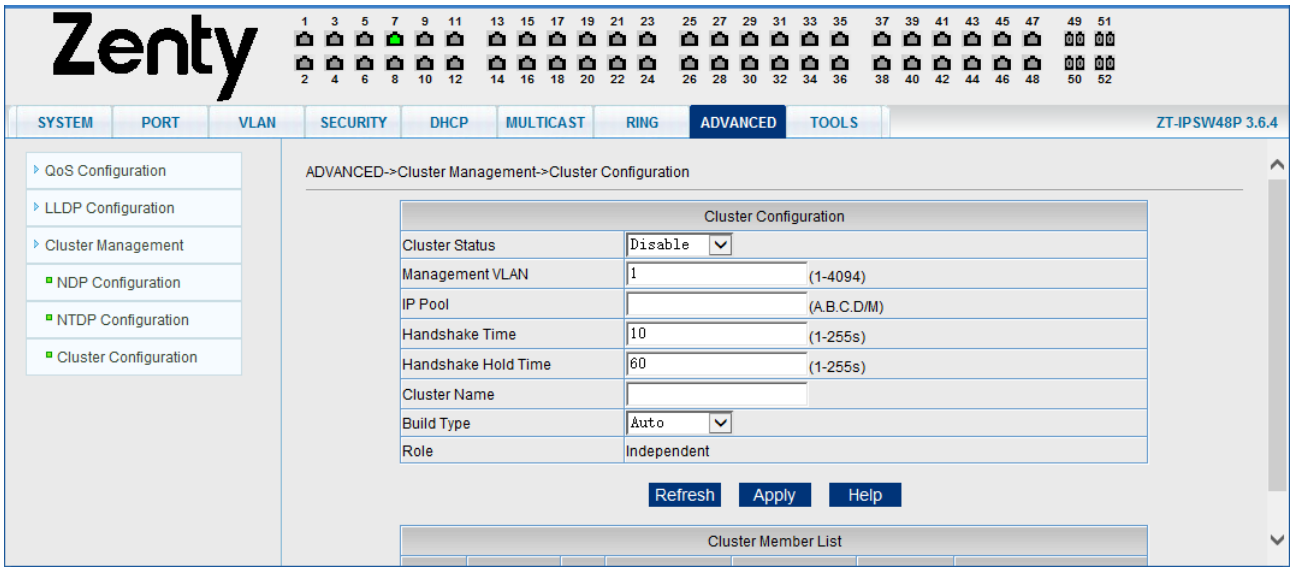
NTDP Configuration page

(8) Cluster Configuration

This page is use to configure the cluster function and display the cluster member list.

Cluster Status	Enable or disable the cluster status.
Management VLAN	set management VLAN ID, default value is VLAN 1.
IP Pool	Set IP pool, format is A.B.C.D/M.
Handshake Time	Set cluster handshake time in seconds, default value is 10 seconds.

Handshake Hold Time	Set cluster handshake hold time in seconds, default value is 60 seconds.
Cluster Name	Set cluster name, only administrator needs to set cluster name.
Build Type	The build type to create a cluster set, auto build or manual.
Role	Display the cluster role of this switch, for example administrator or member.
Cluster Member List	Display the cluster administrator device, member devices and candidators.

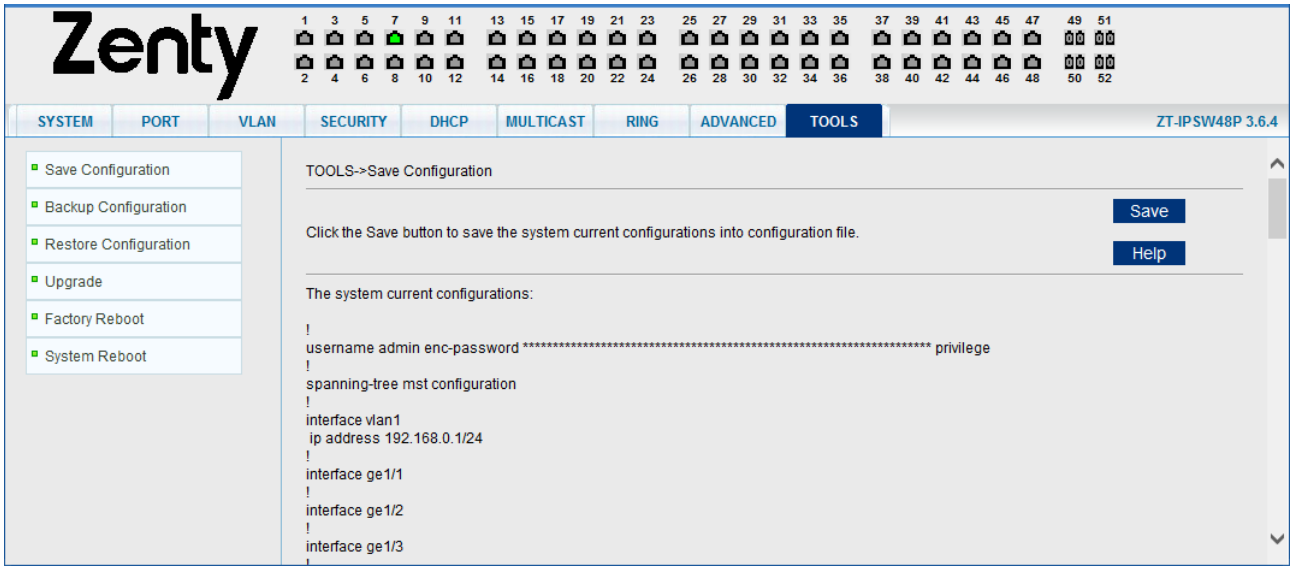


Cluster Configuration page

3.0 System tools

（1）Save the configuration page

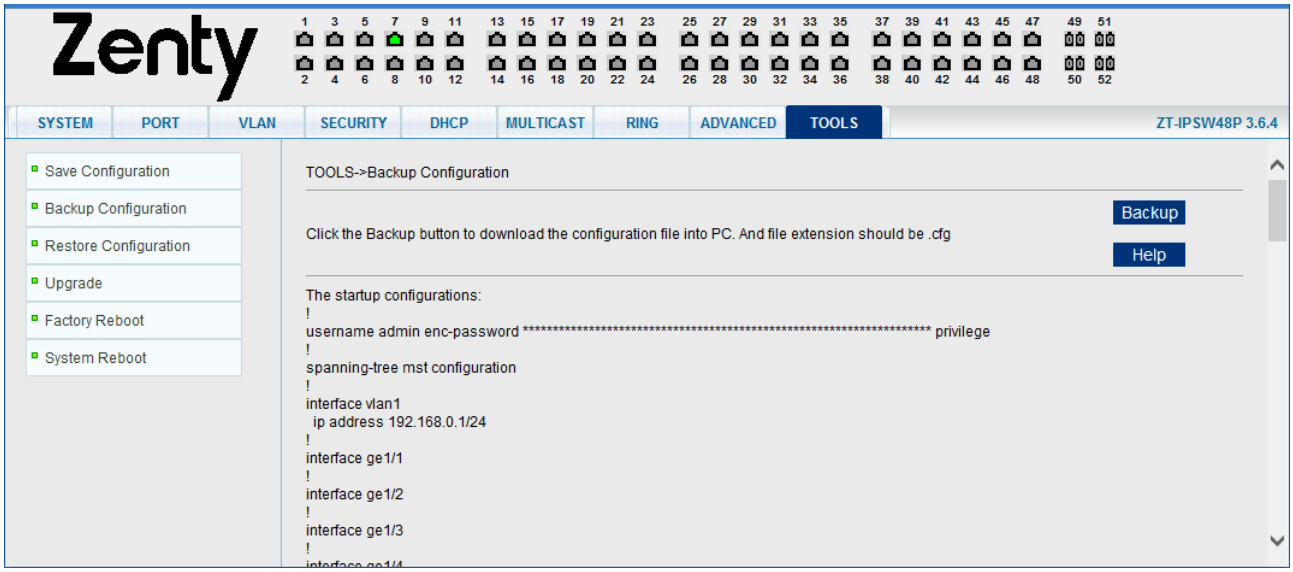
This is the save configuration page. Through this page, the user can view the current configuration of the switch. The Save button stores the current configuration of the system into the configuration file. Because the storage operation needs to erase the FLASH chip, which takes a certain amount of time. When the user is configured on the page and wants to restart the switch after the configuration is not lost, must exit the page in the current configuration page, click the Save button.



Save the configuration page

（2）Back up the configuration file page

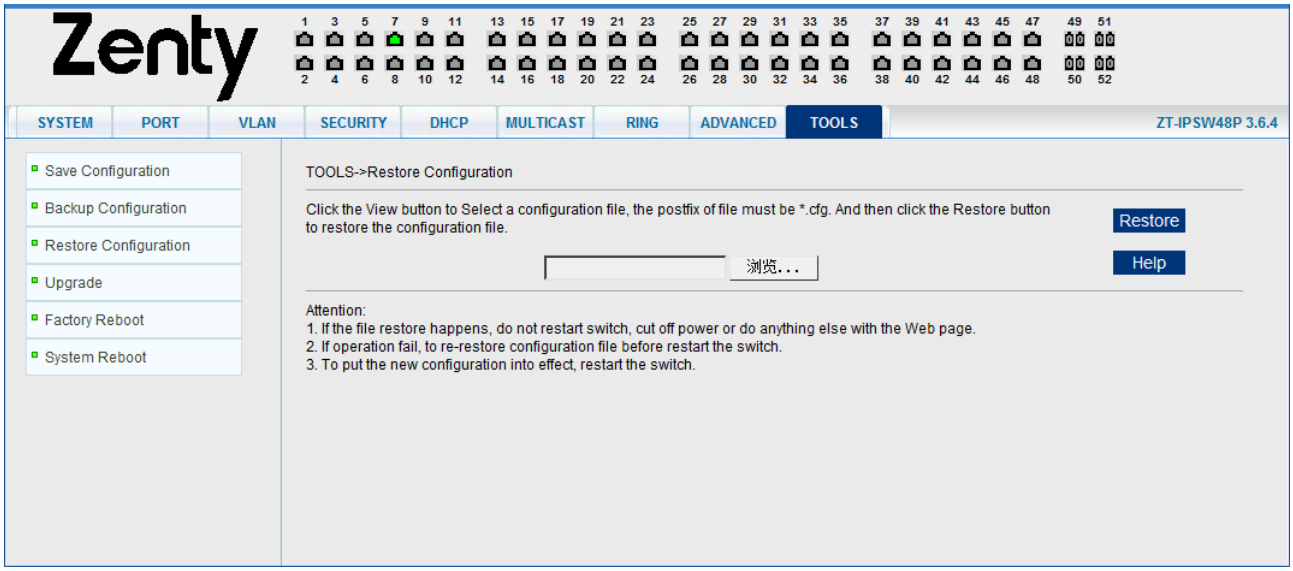
This shows the backup profile page. This page allows the user to view the initial configuration of the system. The initial configuration is actually in the FLASH in the configuration file, when the FLASH does not exist in the configuration file, the system starts using the default configuration. Click the backup button, will pop up a dialog box, the user chooses to save directory path and save the configuration file. The file name of the downloaded configuration file defaults to switch. cfg



Back up the configuration file page

（3） Restore the configuration file page

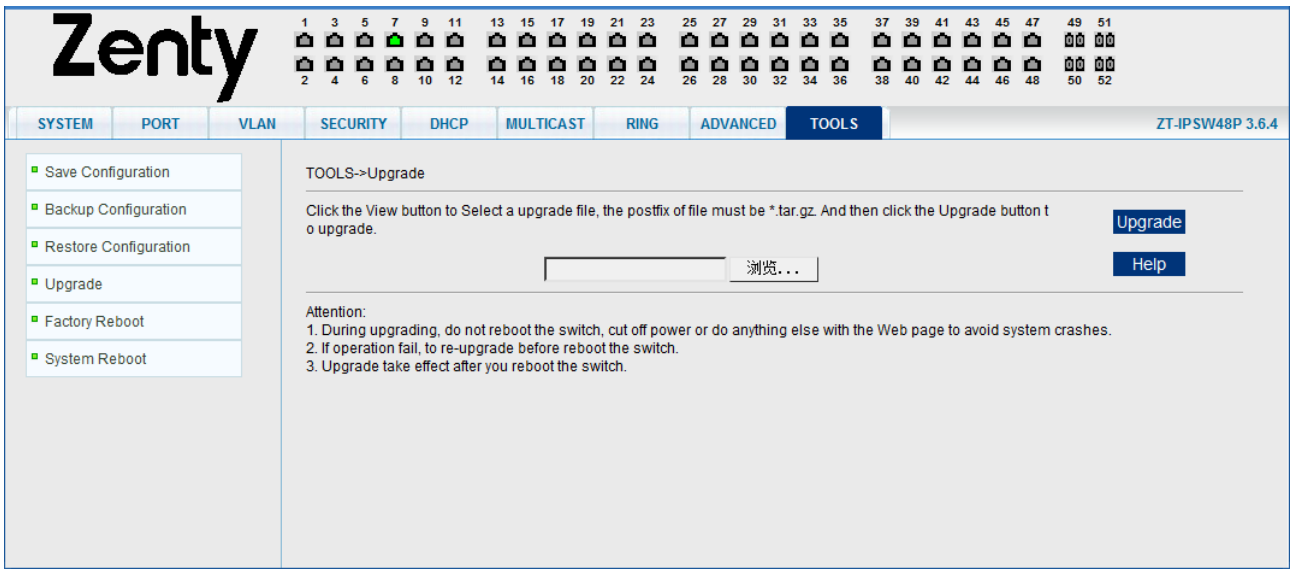
This is the recovery profile page, through which users can upload configuration files to the switch. Click the Browse button to select the directory path of the uploaded profile on the PC. Click the upload button to upload the configuration file. The suffix of the configuration file must be * .cfg. Do not click on other pages or reboot the switch before the transfer results page returns. Otherwise, the file transfer will cause the system to crash.



Restore the configuration file page

（4）Software upgrade page

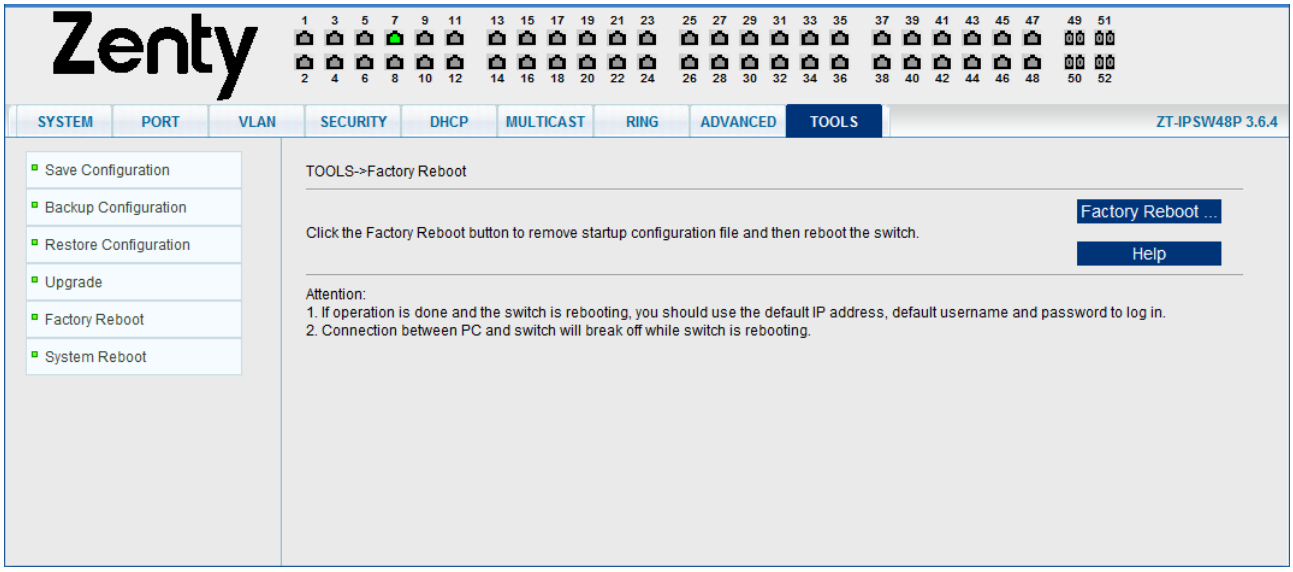
This is the software upgrade page, through which users can upload image files to the switch. Click the Browse button to select the directory path of the uploaded image file on the PC. Click the Upload button to upload the image file, which must be provided by the manufacturer and the file name suffix must be * .img. Do not click on other pages or reboot the switch before the transfer results page returns. Otherwise, the file transfer will cause the system to crash.



Software upgrade page

（5）Restore the factory configuration page

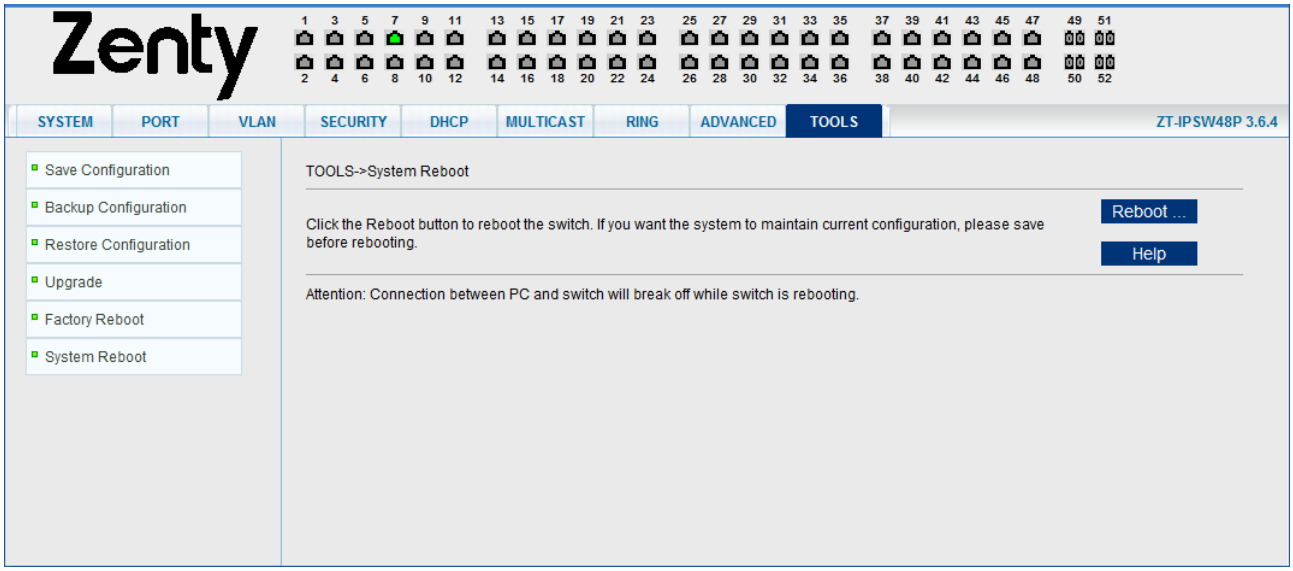
This is the Restore Factory Configuration page. This page allows the user to delete the configuration file in the FLASH to restore to the factory configuration. Click the Restore Factory Configuration button to bring up a dialog box that prompts the user if it is OK. After the factory configuration is restored, the switch will automatically restart to make the factory configuration take effect. Please use the factory default IP address and password the next time when log in.



Restore factory configuration page

（6）System Reboot

This is the system reboot page, through which the user restarts the switch. When click the restart button, a dialog box will pop up prompting if the user is sure to restart the switch or not. If sure, press the OK key. Otherwise, press the Cancel key. The Web page will no longer be opened when it is restarted.



System Reboot page

 Copyright © Zenty AV



WWW.ZENTY.COM
9807 EMILY LANE
STAFFORD, TX 77477

(844) 200-1945
SUPPORT@ZENTY.COM
SALES@ZENTY.COM