DIGITUS®

24 Port L2 Managed Gigabit Ethernet PoE Switch

Web-Manual

DN-95359

About guide 2
Terminology 2
Copyright and statement 2
1. Product's introduction 2
1.1. Front panel 2
1.2. Real panel 3
2. Hardware installation 3
2.1. Open a seal 3
2.2. Switch installation 3
2.2.1. Desktop or Shelf Installation 4
2.2.2. Rack Installation 4
2.3. Plugging in the AC Power Cord 5
2.3.1. Power failure 5
2.4. Console Port Interface 6
3. Getting Started 7
3.1 Using Web-based Management 7
3.1.1 Supported Web Browsers 7
3.1.2 Connecting to the Switch 7
3.1.3 Login Web-based Management 7
3.2 WEB page elements 8
3.3 The structure of Navigation tree 9
3.4 Page button Introduction 9
3.5 Error messages 9
3.6 Entry Field 10
3.7 Status Field 10
4. WEB page introduction 11
4.1. Login dialog Box 11
4.2. Main Page 11
4.3. System Configuration: 12
4.4. Port Configuration 18
4.5. MAC Configuration 23
4.6. VLAN Configuration 26
4.7. SNMP Configuration 28
4.8. ACL Configuration 29
4.9. QoS Configuration 33
4.10. IP Basic Configuration 34
4.11. DHCP Server 36
4.12. (AAA) configuration 38
4.13. Spanning Tree Protocol configuration 42
4.14. IGMP SNOOPING configuration 44
4.15. GMRP configuration 45
4.16. EAPS configuration 47
4.17. RMON configuration 48
4.18. Cluster configuration 51
4.19. ERPS configuration 53
4.20. LLDP Global Configuration 55
4.21. log management 57
4.22. PoE port configuration 58

About guide

This guide provides instructions to install the Switch.

Note: The model you have purchased may appear slightly different from the illustrations shown in the document. Refer to the Product Instruction and Technical Specification sections for detailed information about your switch, its components, network connections, and technical specifications.

Terminology

Note: indicates important information that helps a better use of the device.

Warning: indicates potential property damage or personal injury.

Copyright and statement

Without the express written permission of the company, no unit or individual is allowed to imitate,

Copy, transcribe or translate part or all of the contents of this book without authorization.

The pictures and data shown in this guide are for reference only, subject to change without notice.

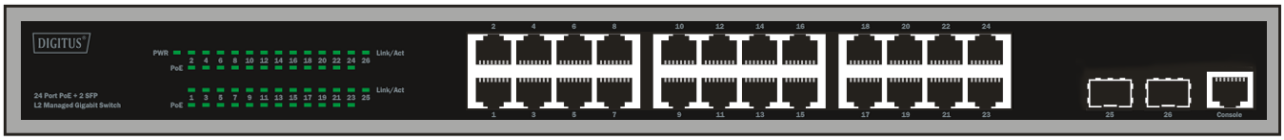
1. Product's introduction

Thanks for purchasing the switch products.

This is a Gigabit Full Managed POE Switch. It provides 24 10/100/1000Mbps Auto-Negotiation RJ45 POE ports and 2 Gigabit SFP Ports. It supports the port's full line speed forwarding to ensure the stable transmission of data. The machine can be used as a small local core switch or a mall and medium-sized LAN switch, and can also be used as an access switch for large LAN. It can be widely used in monitoring, wireless, Internet cafe and other fields.

This product is a Gigabit network management type PoE Switch. Which can satisfy the full speed forwarding of ports. The machine uses 19 "1U the standard chassis can be used on the desktop or on the rack. Excellent performance can help you widely use in wireless, monitoring and other fields.

1.1. Front panel



PWR LED： The Power LED lights up when the Switch is connected to a power source.

Link/Act LED: The Link/Act LED flashes which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port.

PoE LED:

Green: Indicates the PoE powered device (PD) is connected and the port supplies power successfully.

Light off: Indicates no powered device (PD) connected.

1.2. Real panel

Power input: Supports input voltages 100-240VAC, 50/60Hz.

Switch: turn on the switch after inserting the power cord, “I” means to turn on, “O” means closing.

Grounding: use specialized ground lead connect

2. Hardware installation

This chapter provides unpacking and installation information for the switch.

2.1. Open a seal

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged.

- Switch 1pcs
- AC power cord 1pcs
- Console Cable 1pcs
- Rubber feet 4pcs
- Screws 6pcs
- Mounting brackets 2pcs
- User manual 1pcs

If any item is found missing or damaged, please contact the local reseller for replacement.

2.2. Switch installation

For safe switch installation and operation, it is recommended that you:

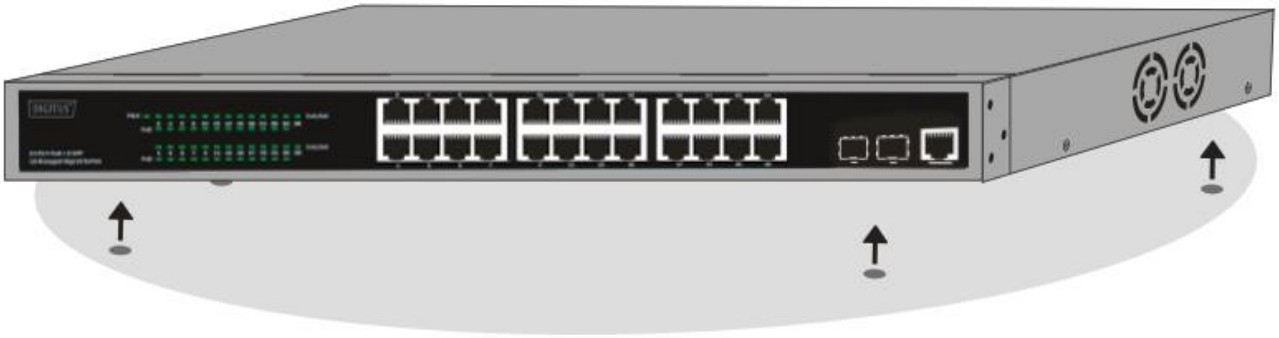
Visually inspect the power cord to see that it is secured fully to the AC power connector.

Make sure that there is proper heat dissipation and adequate ventilation around the switch.

Do not place heavy objects on the switch.

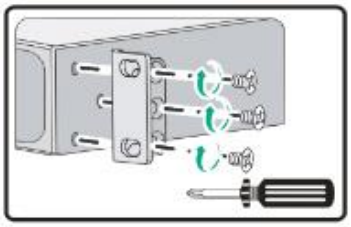
2.2.1. Desktop or Shelf Installation

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.

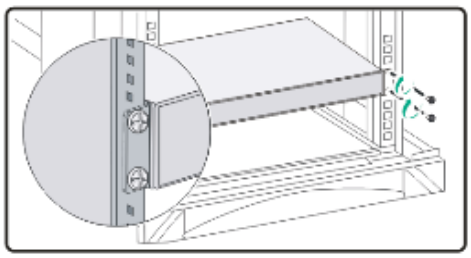


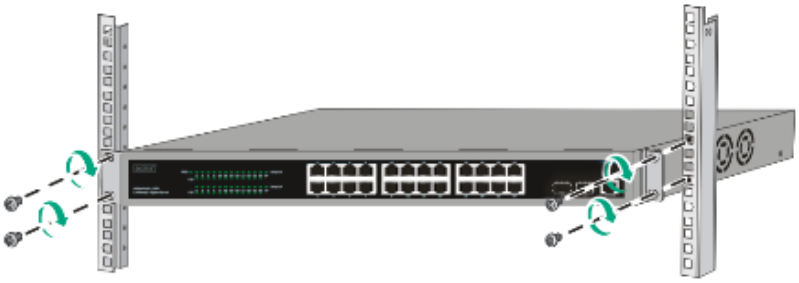
2.2.2. Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (please note that these brackets are not designed for palm size switches).



Then, use the screws provided with the equipment rack to mount the switch in the rack.

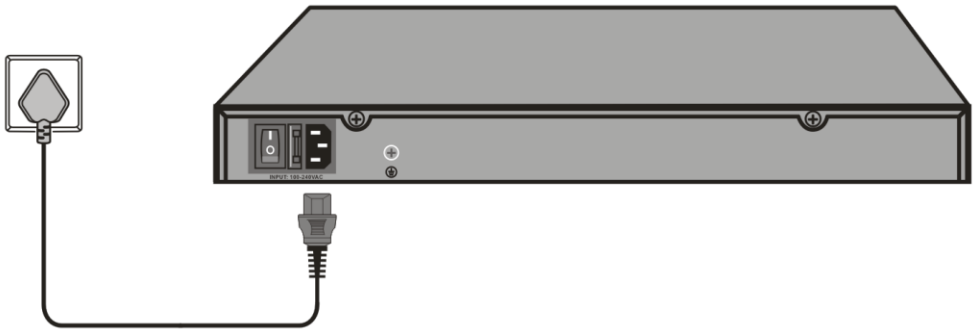




2.3. Plugging in the AC Power Cord

You can connect AC power supply cord to switch back and the other side connect the power outlet. (Power outlet might as well grounding and support over voltage protection)

Warning: Do not turn on the power switch before power cables are connected. Power surge may cause damage to the Switch.



2.3.1. Power failure

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, plug the switch back in.

Please be aware of following safety Instructions when installing:

a) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

b) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

c) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

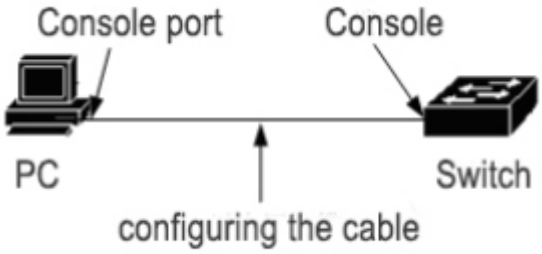
d) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

e) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

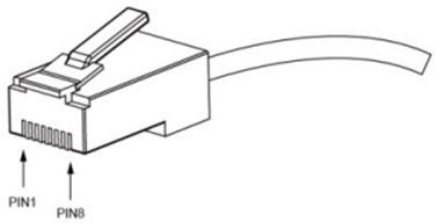
2.4. Console Port Interface

The smart switch has a monitor port (Console port). Rate 9600bps, standard RJ45 plug.

Use a dedicated monitoring cable to lead the port to the PC serial port connection, as follows:



The RJ45 connector used by the Console port is shown in the figure below, and the RJ45 plug corresponds to the RJ45 socket, from left to right numbered from 1 to 8.



This cable is used to connect the console port of the switch to the external monitoring terminal. One end of the RJ45 eight-pin plug, the other end is a 25-hole plug (DB25) and 9-hole plug (DB9), RJ45 head into the switch's console port socket, DB25 and DB9 can be used according to the requirements of the terminal serial port, the cable internal connection schematic as follows:

RJ45<===>DB9

NC1-------8CTS
NC2-------6DSR
TXD3------2RXD
GND4------5GND
GND5------5GND
RXD6------3TXD
NC7-------4DTR
NC8-------7RTS

3. Getting Started

This chapter introduces the management interface of switch.

3.1 Using Web-based Management

After a successful physical installation, you can configure the Switch, monitor the network status, and display statistics using a web browser.

3.1.1 Supported Web Browsers

The embedded Web-based Management currently supports the following web browsers:

- Internet Explorer 6 or higher version
- Netscape 8 or higher version
- Mozilla
- Firefox 1.5/2.0 or higher version

3.1.2 Connecting to the Switch

You will need the following equipment to begin the web configuration of your device:

1. PC with a RJ-45 Ethernet connection
2. Standard Ethernet cable

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

Connected Ethernet cable

3.1.3 Login Web-based Management

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of 192.168.0.1, the PC should have an IP address of **192.168.0.x** (where x is a number between 1 ~ 254), and a subnet mask of **255.255.255.0.** Open the web browser and enter **192.168.0.1** (the factory-default IP address) in the address bar. Then press <Enter>.

Enter the IP address in the web browser

NOTE: The switch's factory default IP address is 192.168.0.1 with a subnet mask of 255.255.255.0

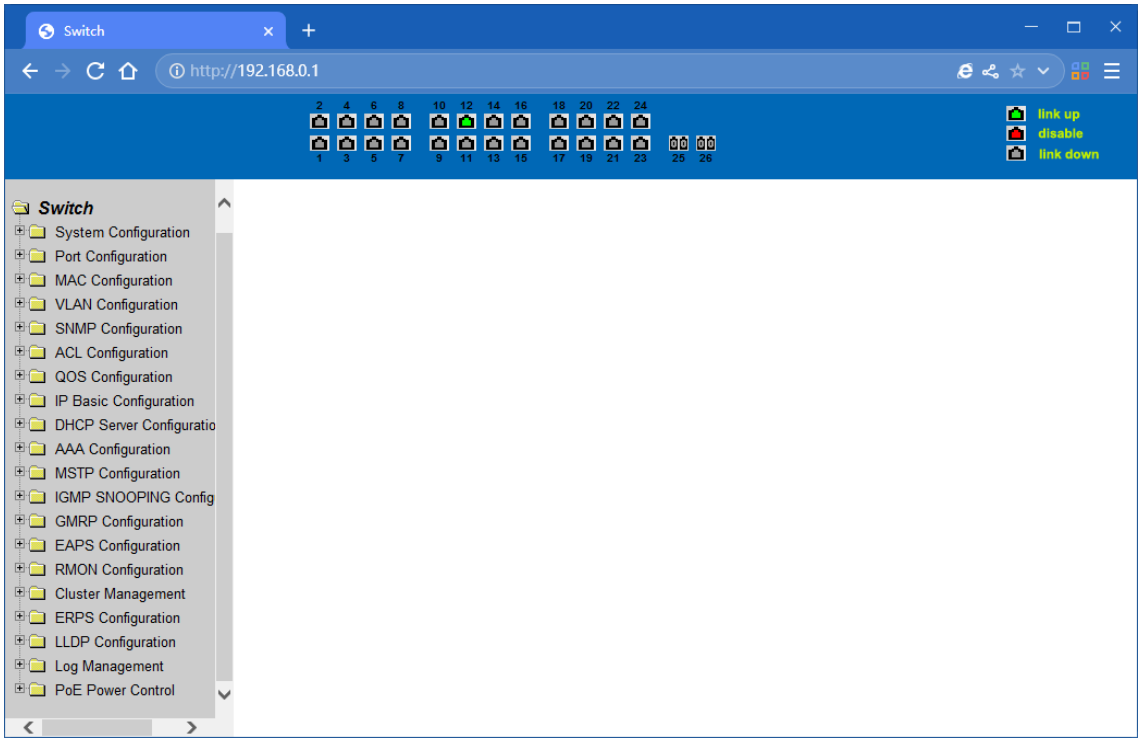
When the following logon dialog box appears, enter the password then click OK.

By default, the username is **admin** and the password is **admin.**

Logon Dialog Box

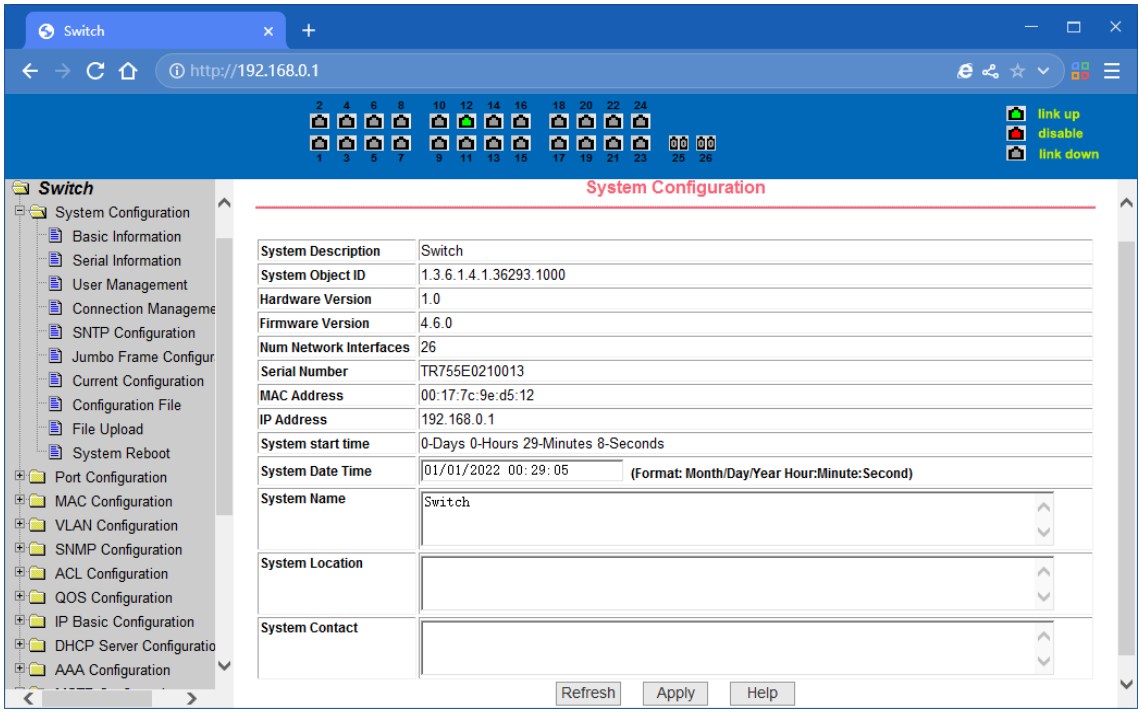
3.2 WEB page elements

WEB page is mainly composed of three parts: title page, navigation tree page and main page



3.3 The structure of Navigation tree

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 is named of the corresponding web page, top of page title abbreviation.



3.4 Page button Introduction

On the pages, here are some commonly used buttons. The role of these buttons is generally the same. The role of these buttons is described below:

button	effect
Refresh	Update all fields on the page
Apply	Numerical value will be updated into the memory. Because the error-checking should be implemented 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

3.5 Error messages

If the switch WEB server error occurred while processing user requests, it will display a dialog box in the corresponding error message.

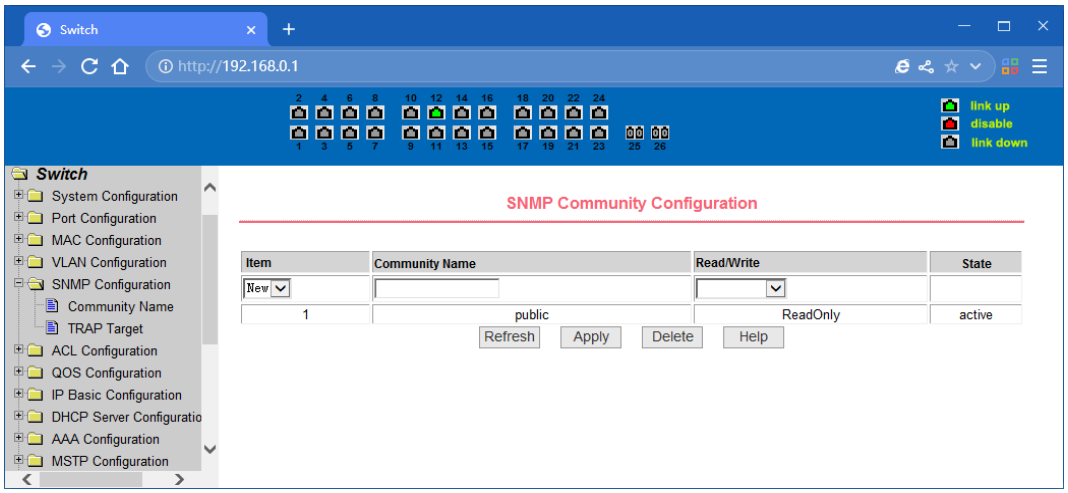
3.6 Entry Field

Some pages of the most left column in the table have an entry field, through the field can access different rows in the table. When you choose a line 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.

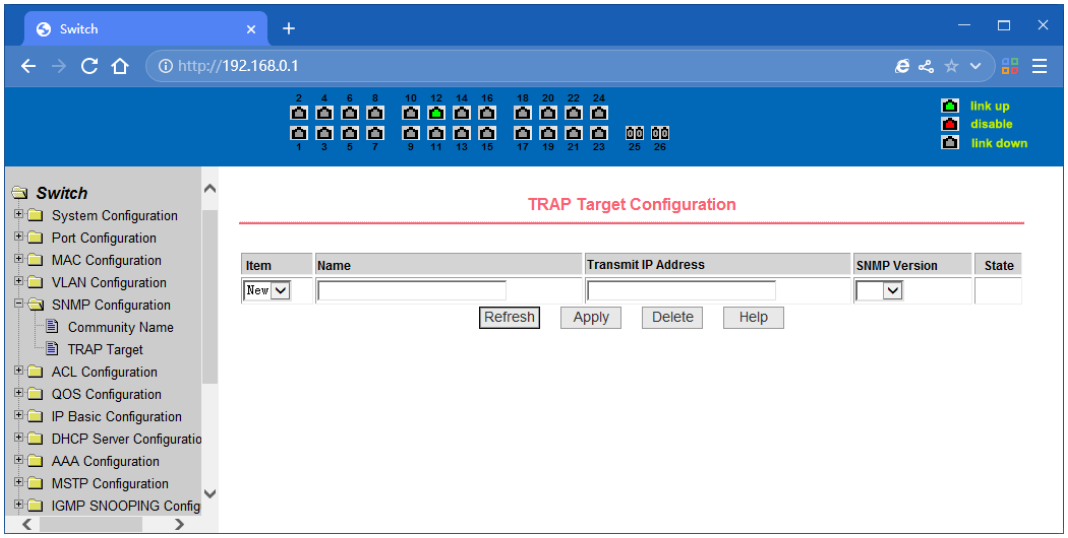
If you want to edit the line already exists, it is necessary select the appropriate line number of the drop-down menu, according to need to edit the line, and then press the apply button, you will see a corresponding change in the table displayed.

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



3.7 Status Field

Some pages of the rightest column in the table there is a state field, 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

4. WEB page introduction

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

4.1. Login dialog Box

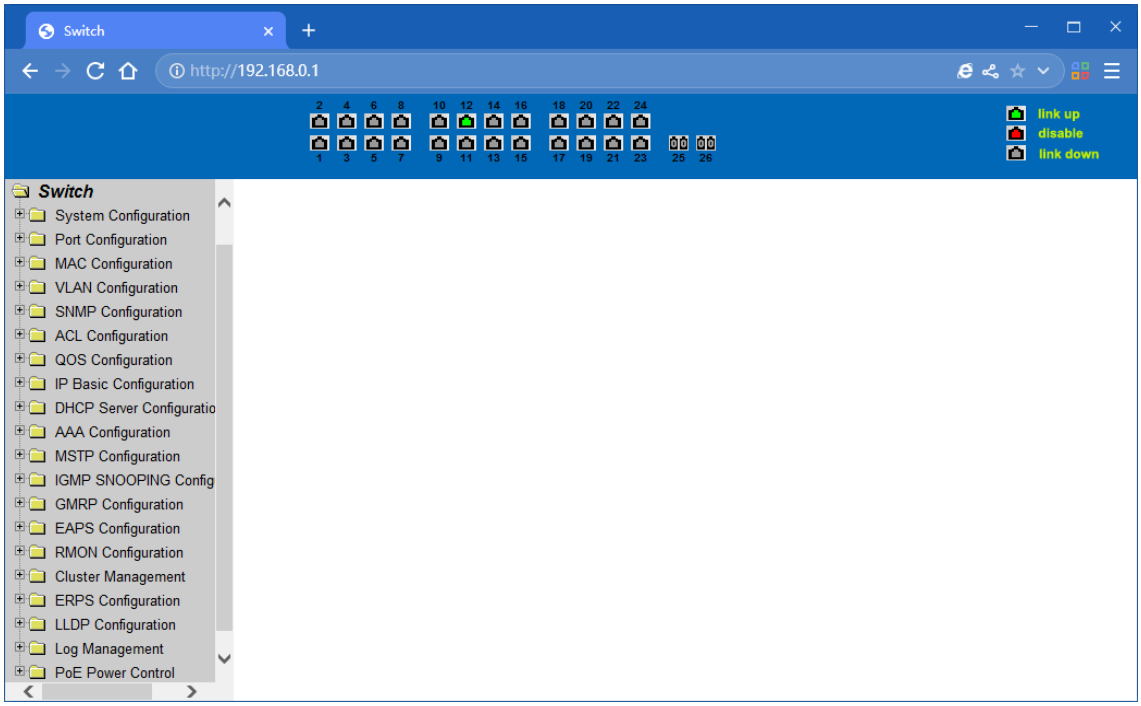
WEB browsing session of the login page

The logon dialog box will be displayed while the user login the web page at the first time. When the user filled out the correct user name and password, then click the Enter button can log on to the switch Web server. Passwords are case-sensitive, the anonymous user password can be maximum set up to 16 characters, while the multi-user name and password can be set up to 11 characters.

The default username is admin, and password is admin.

4.2. Main Page

It shows the WEB main page of Switch. This page will be displayed after the user logs in web pages



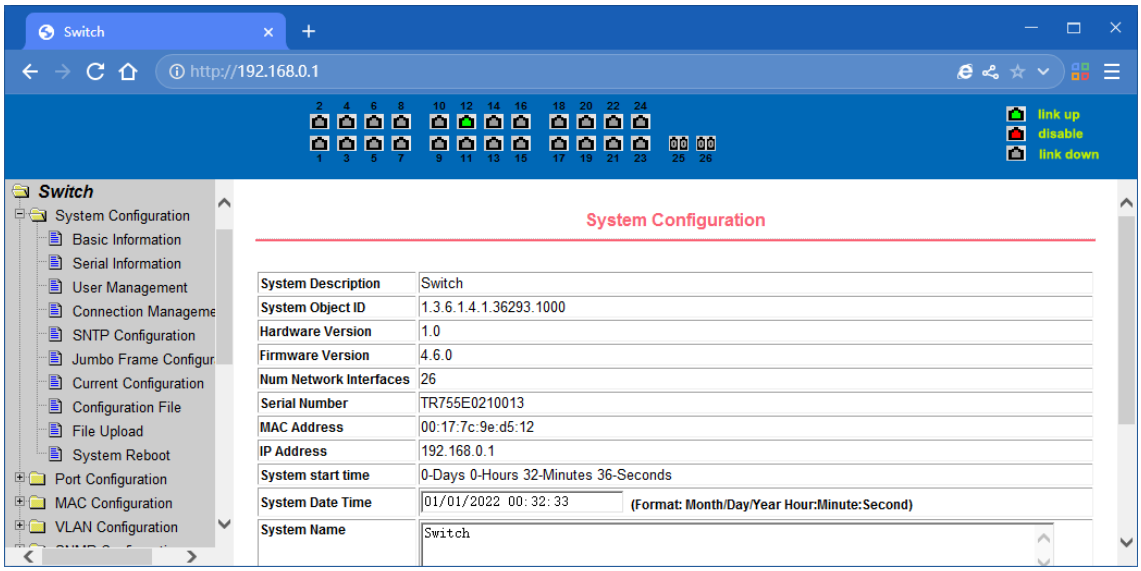
Switch switches main page

4.3. System Configuration:

（1）Basic information page

It is the basic information of configuration page; users can configure the basic information for the switch.

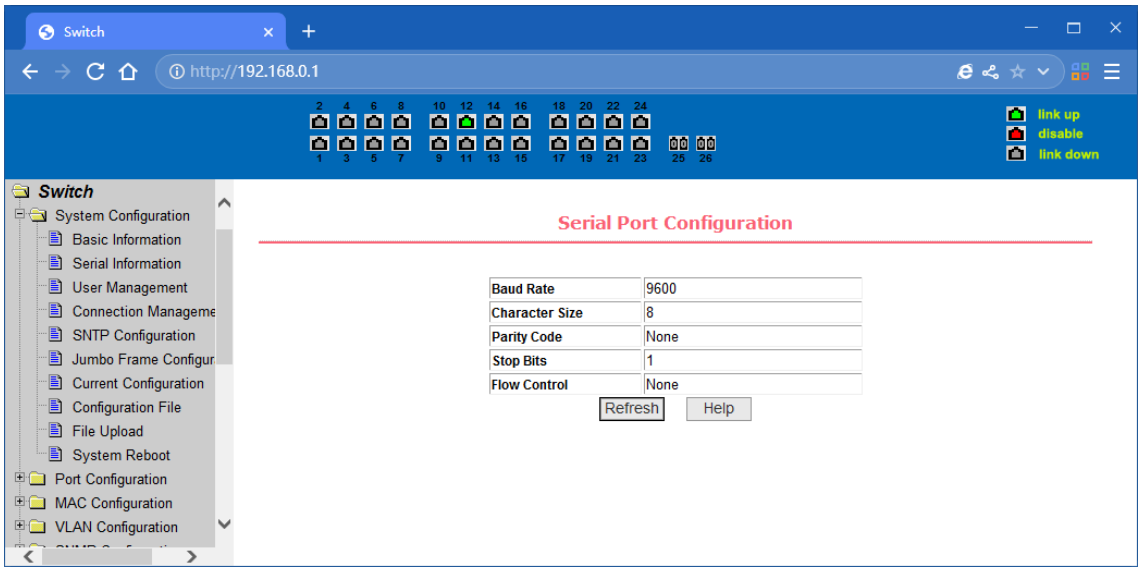
System Description display the description of the relevant parameters of system.
System descriptor ID display system in the network identity management.
The system version number is displayed the current software version number of switches.
The number of switches interface displays the current number of interfaces in the switch.
The system start-up time display switches from start to the present time.
The system name as the switch's system name in the network, the user can modify the system name.
The systematic location as the switch's physical location showing at the network, the user can modify the system locations.
System Contact show the contacts person and details of the current node, the user can modify the system contact.



Basic Information Page

（2）Serial port information page

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

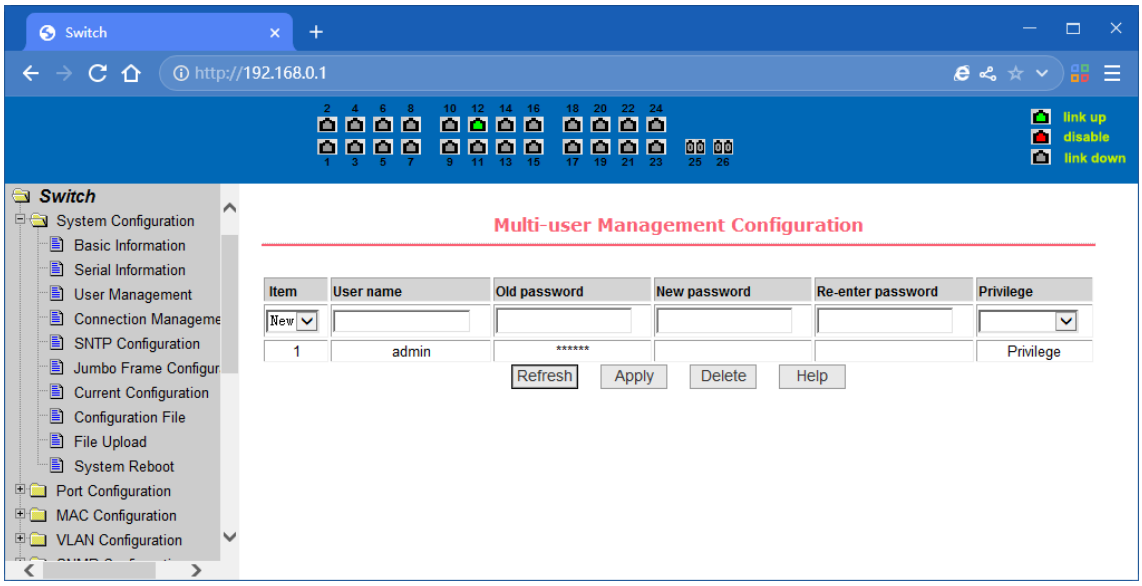


Serial port information page

（3）User management page

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

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

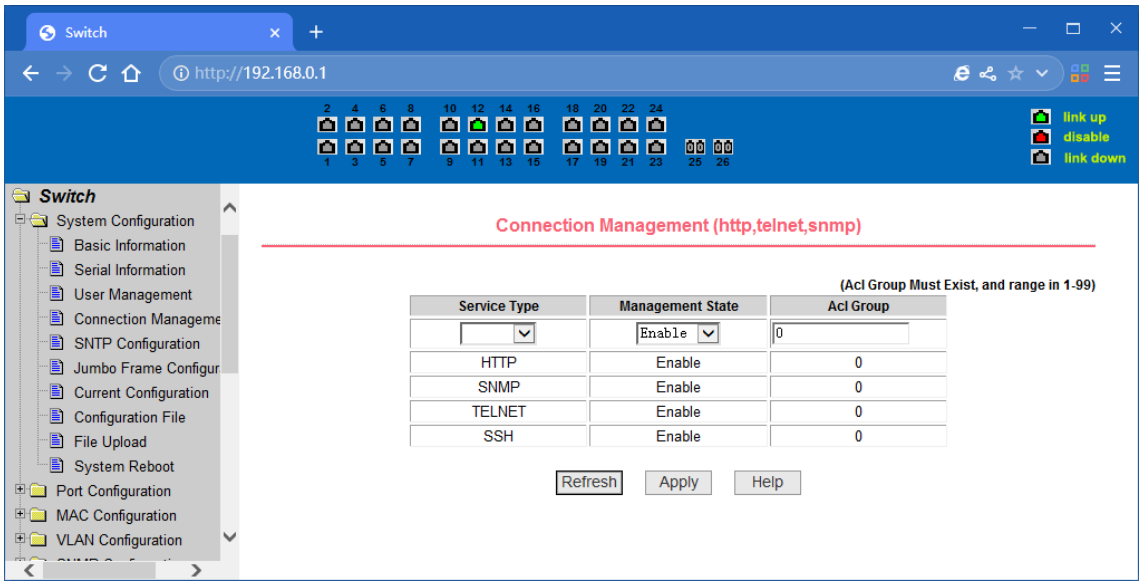


User's management page

（4）Connection Management:

This page is used to configure HTTP, SNMP and Telnet security.

Service Type	Offers HTTP, SNMP and Telnet from the dropdown list
Management State	Offers Enable or Disable for this service type
ACL group	Gives the option to enter a pre-existing ACL group between 1 and 99



Security management page

（5） SNTP Configuration

This page is used to configure and display SNTP protocol.

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.

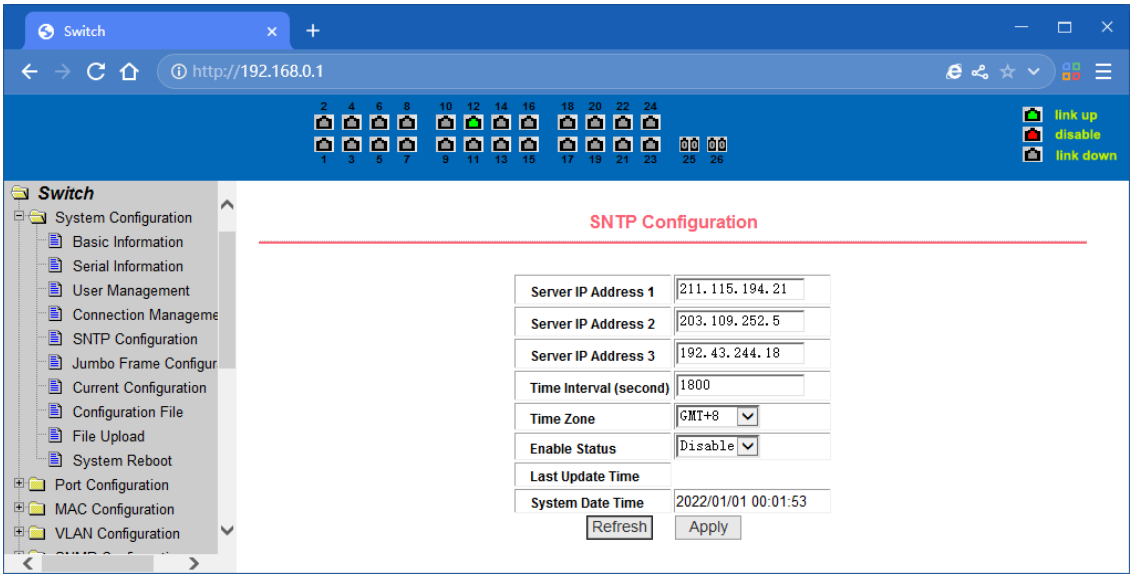
Time Interval: Set the SNTP synchronization time interval in seconds. The default is 1800s.

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.

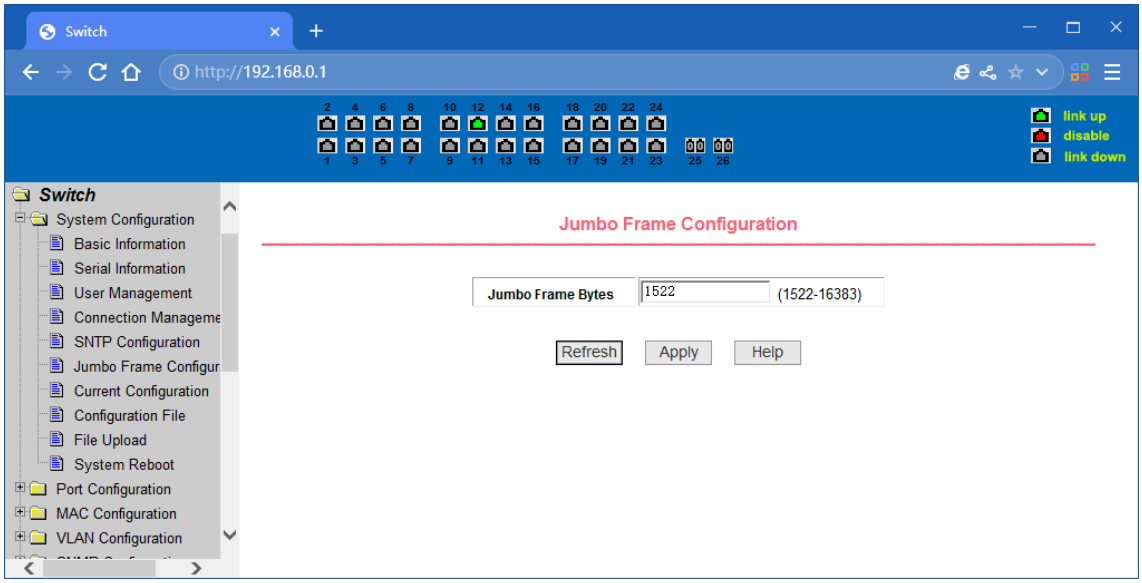


SNTP Configuration page

（6）Jumbo Frame Configuration:

This page is used for configuring jumbo frame.

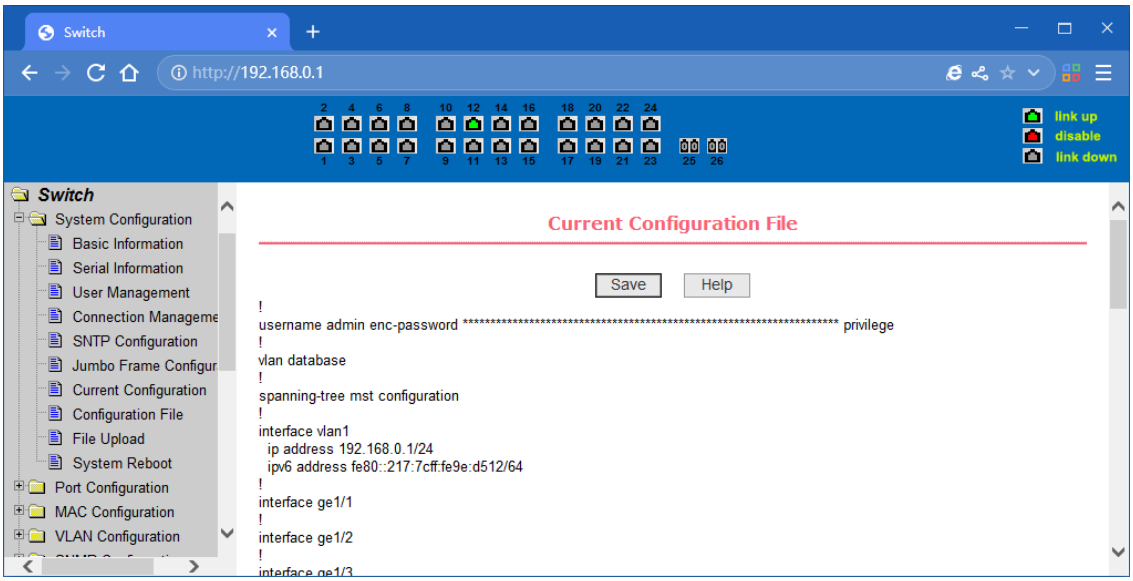
Jumbo Frame Bytes　　Enter the jumbo frame bytes (1522-16383)



Jumbo Frame Configuration page

（7）Configuration page

It is profile configuration page. This page allows users to view the system's initial configuration. The initial configuration is actually the configuration file in the FLASH, when the configuration file does not exist in FLASH, the system starts using the default configuration. Delete key to delete the configuration file in the FLASH. Click the Delete button, will pop up a dialog box, that will Prompts the user sure to delete the configuration file or not, according to the dialog box to determine if it's ok, otherwise click Cancel button. Download button is used to downloaded a configuration file to the PC. Click to download button, will pop up a dialog box, user's select Save and save the configuration file directory path. Download the configuration file names are as switch cfg.



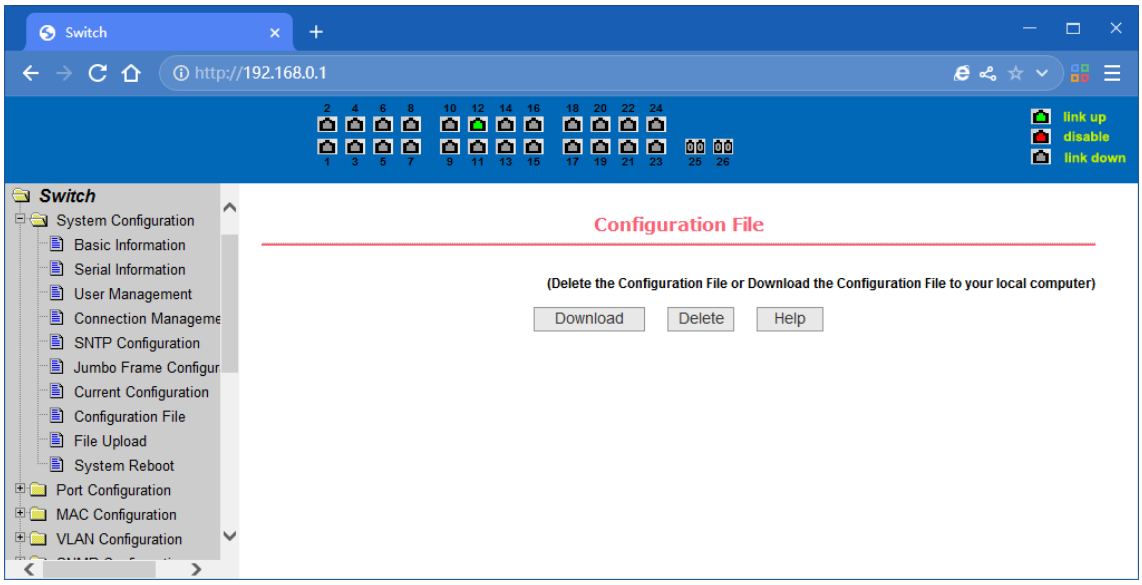
Configuration file page

（8）Configuration File:

This page lets you download and delete the configuration file.

Delete Deletes the configuration file and returns the switch to its default configuration

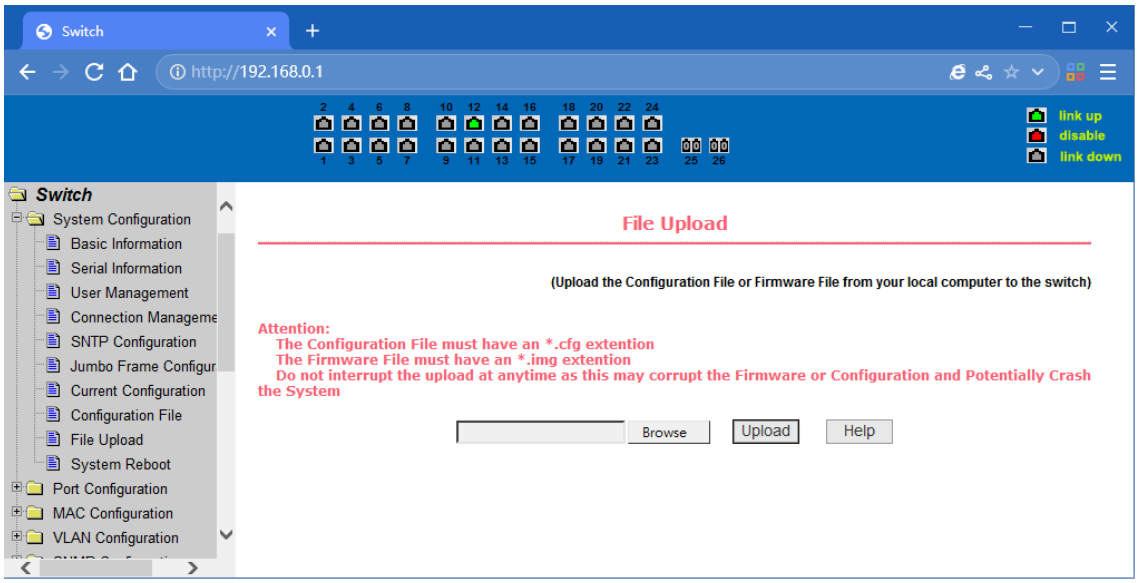
Download Downloads the configuration file to your computer and names it switch.cfg



Configuration File page

（9）File upload page

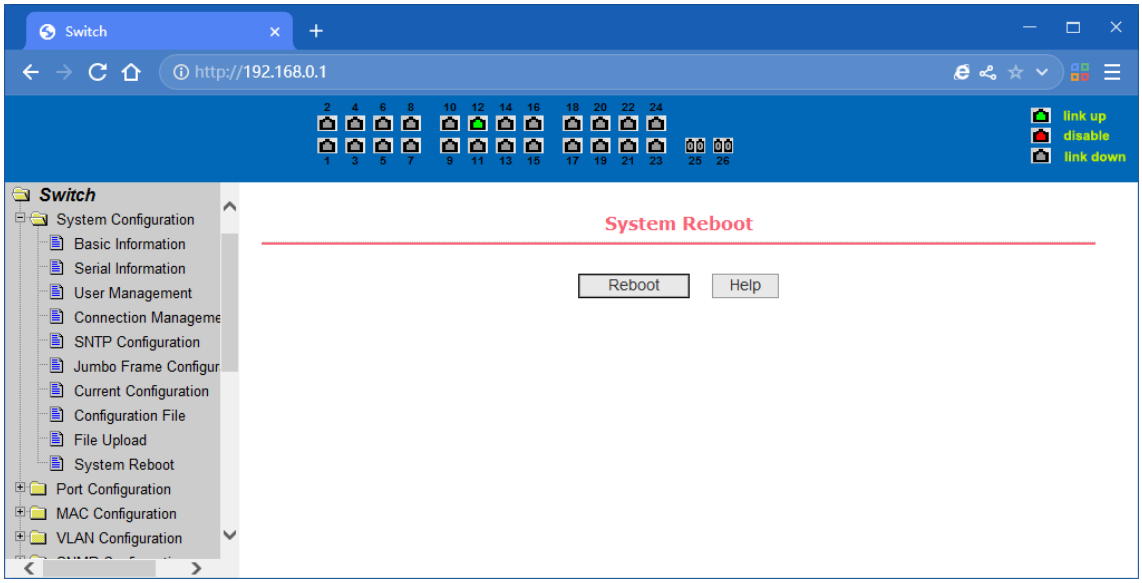
Through this page a user can upload a configuration file and mapping files to the switch. Click the Browse button to select the upload configuration file or image file in the directory path on the PC. Click Upload button upload a configuration file or image file, configuration file extension must be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



File Upload Page

（10）System reset page

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



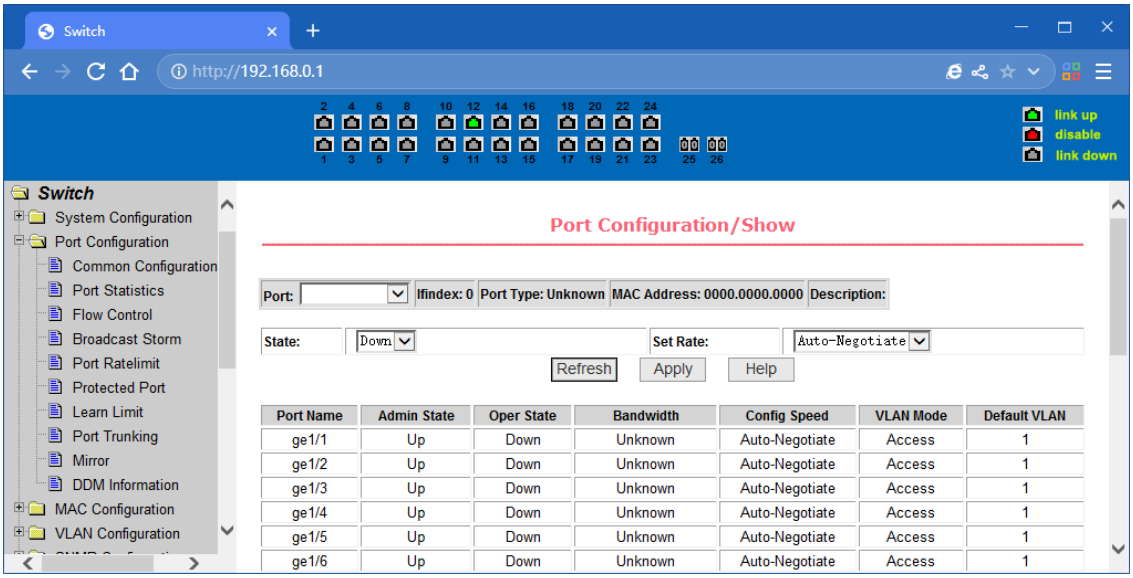
System reset page

4.4. Port Configuration

（1）Port configuration / port -display page

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

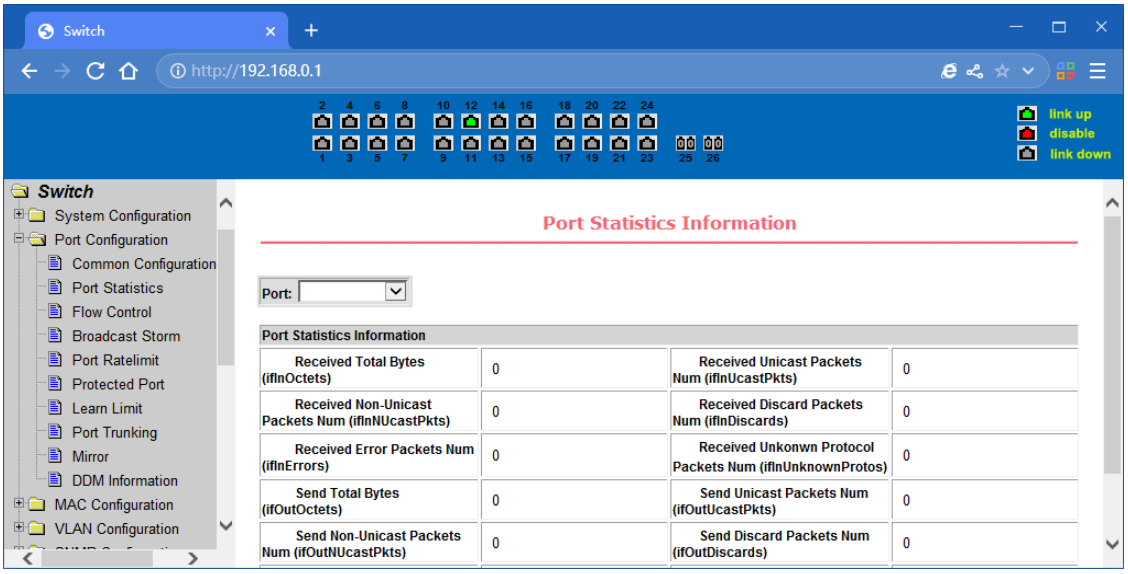
To set a specific port, users need to select the appropriate port name on port drop-down menu. The default port status is up, can select the drop-down menu -down to disable the port. Users can also choose to set the speed of the drop-down menu to set the speed of the port, such as the mandatory half-duplex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



Port configuration and port - display page

（2）Port Statistics Page

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

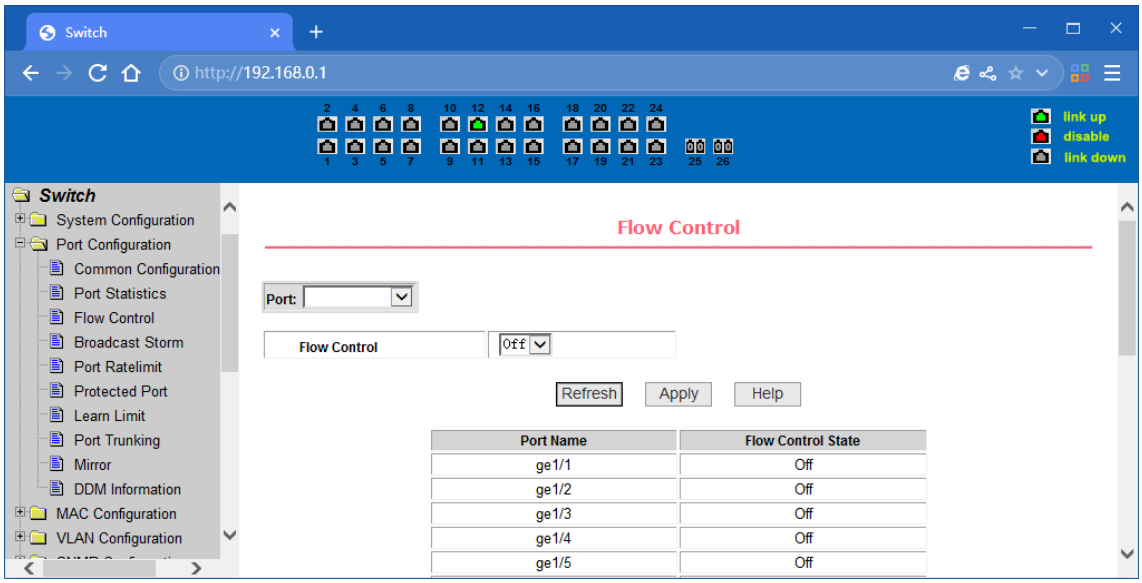


Port Statistics Page

（3）Flow control page

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

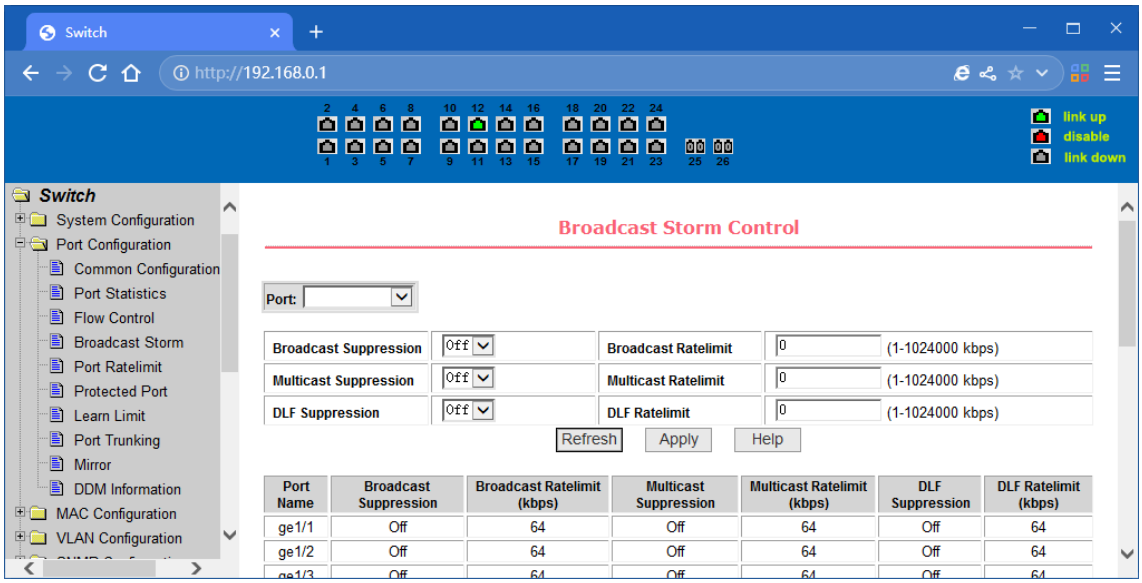
Flow control by sending the side of the drop-down on or off to open or close the sending side of flow control, flow control through the receiving side of the drop-down on or off to open or close the receiver-side flow control, while on and off also shows the port to send side and receiving-side flow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



Flow control page

（4）Broadcast storm control page

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

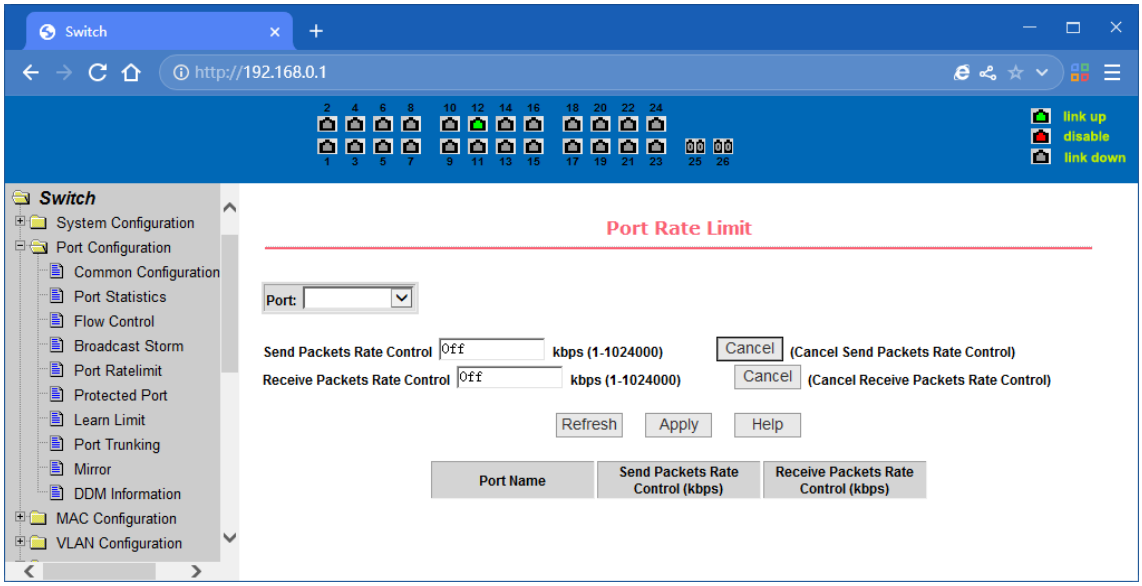


Broadcast Storm Control Page

（5）Port speed limits page

This page is used to configure the port‘s sending and receiving rate

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

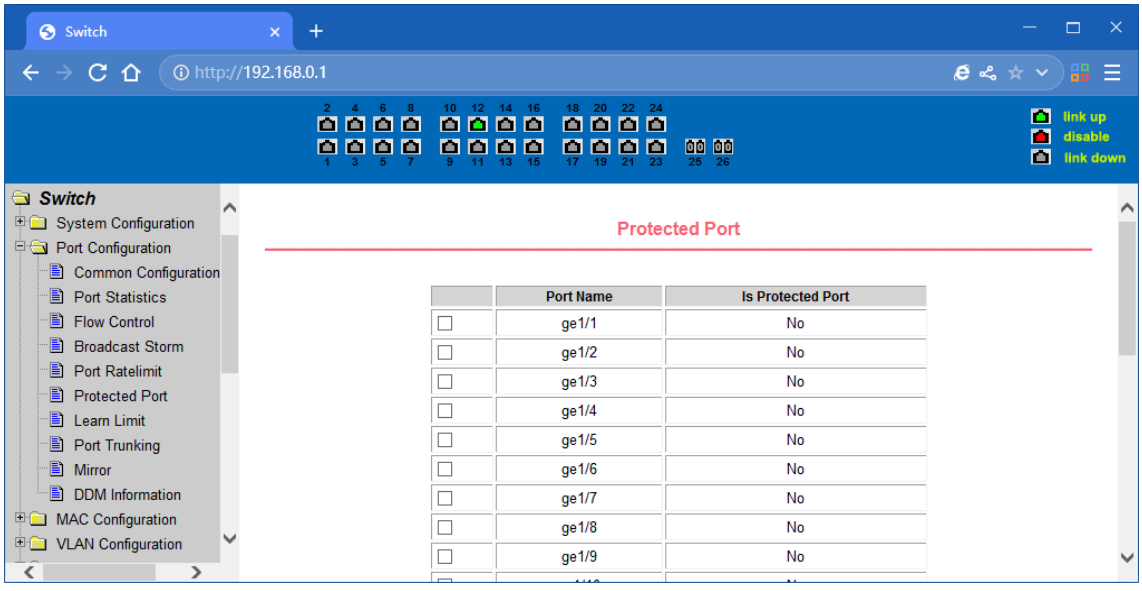


Port speed limit page

（6）Port protection page

This page is used to configure the port for the protection port.

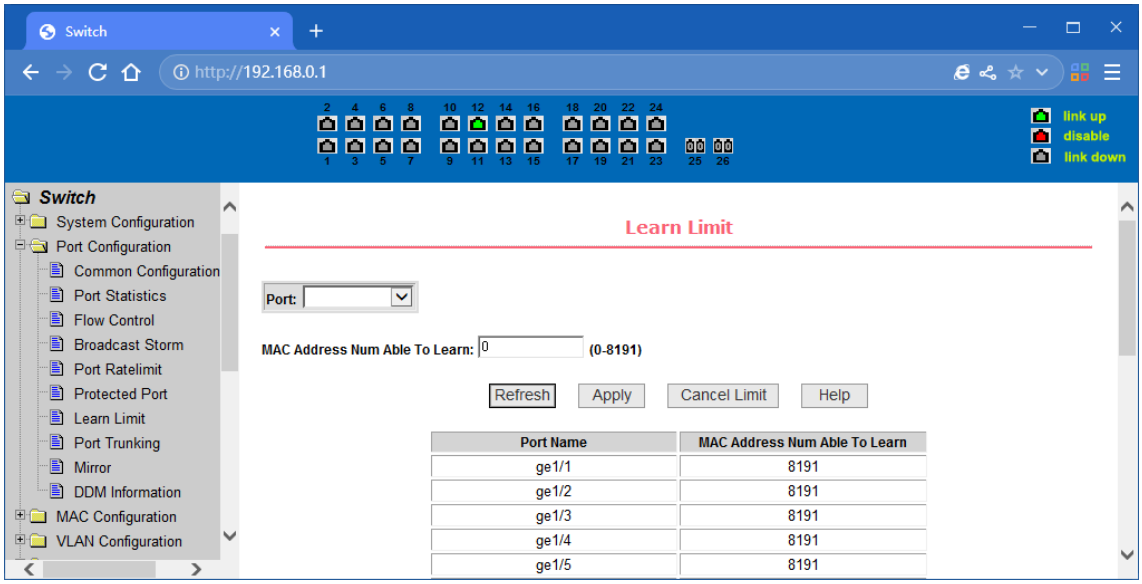
If the port is configured as a protected port, the ports cannot exchange the data with each other, protected port only with non-protected port for data exchange.



Protected port page

（7）Port Learning restrain page

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



Port Learning restrain page

（8）Port Trunking configuration page

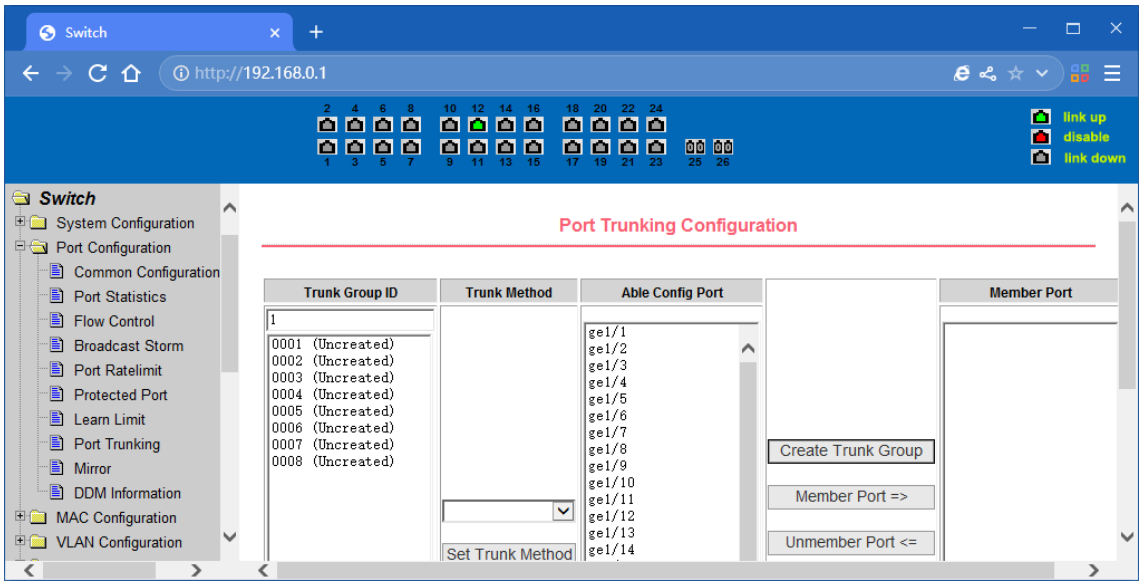
This page allows the user to configure the port trunking. This page consists of four parts: port trunking ID selection, port trunking method selection, configurable ports and group members' port.

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

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

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

Switch supports maximum 3 groups port trunking, can be configured to a maximum of three Trunk Group, Trunk1 and Trunk2 cannot trucking Gigabit ports, and each group can be aggregated up to the same four attributes port. Trunk3 only be aggregated Gigabit ports, and up to 2 Gigabit ports can be aggregated. Port aggregation method is common to all of the Trunk.

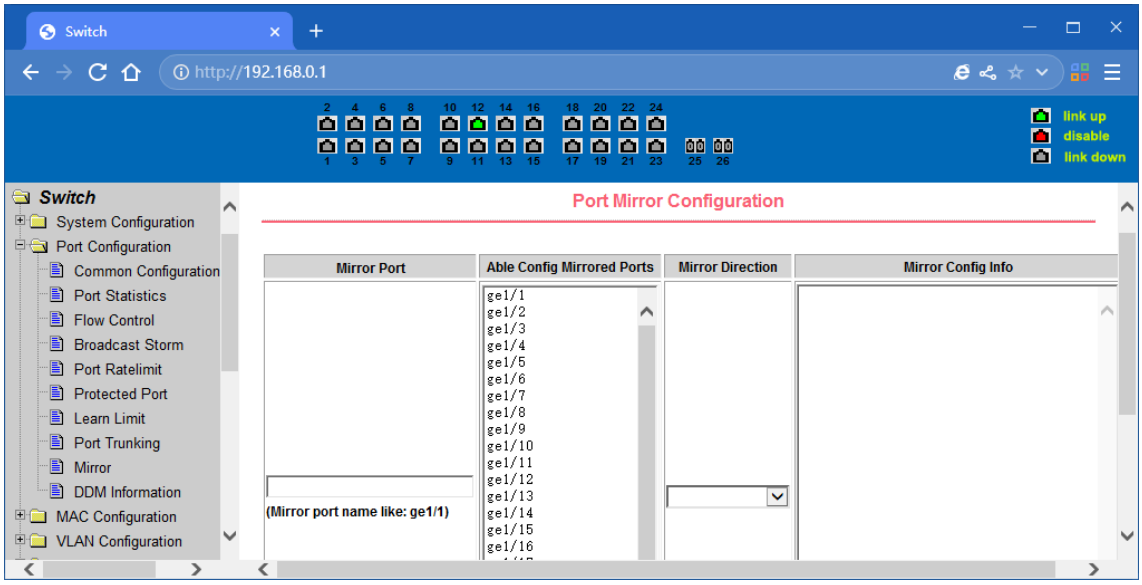


Port Trunking configuration page

（9）Port mirroring configuration page

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

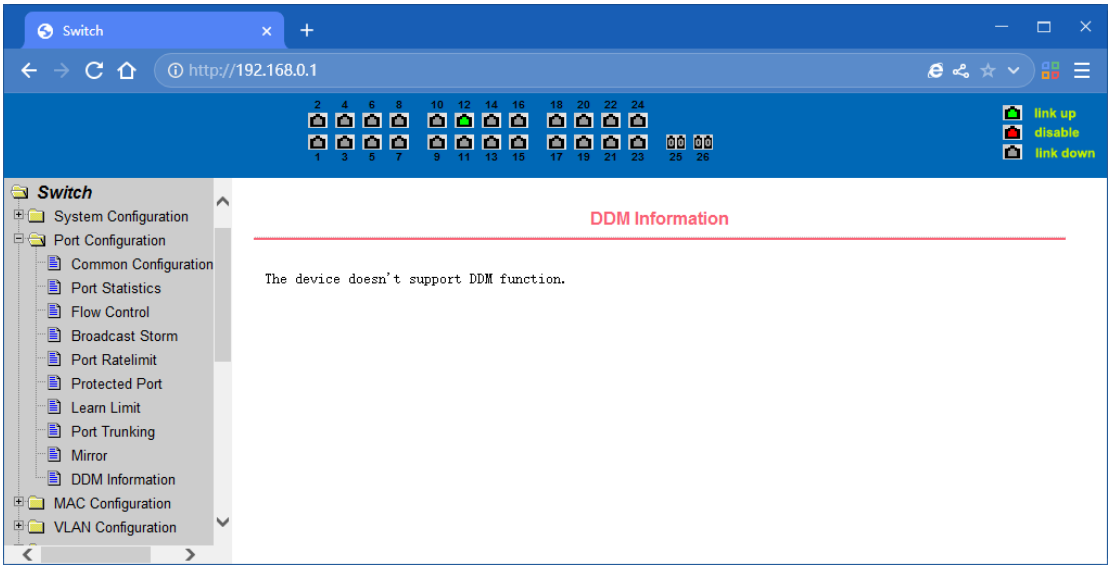
When choose the RECEIVE in direction of monitor, said monitor data packets received, TRANSMIT, said monitor data packets sent, BOTH that monitor all data sent and received packets, NOT_RECEIVE to cancel monitoring received data packets, NOT_TRANSMIT to cancel monitor send data packets, NEITHER cancel monitor data packets received and sent, that is canceling monitor port.



Port mirroring configuration page

(10) DDM Information

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



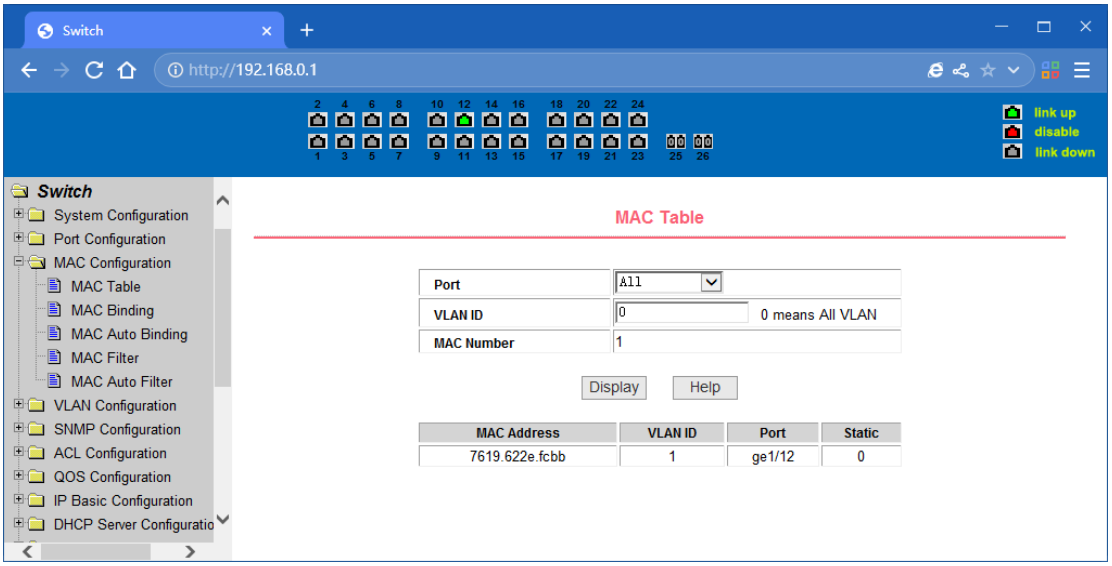
DDM Information page

4.5. MAC Configuration

（1）MAC Table:

This page is used to display the MAC address table.

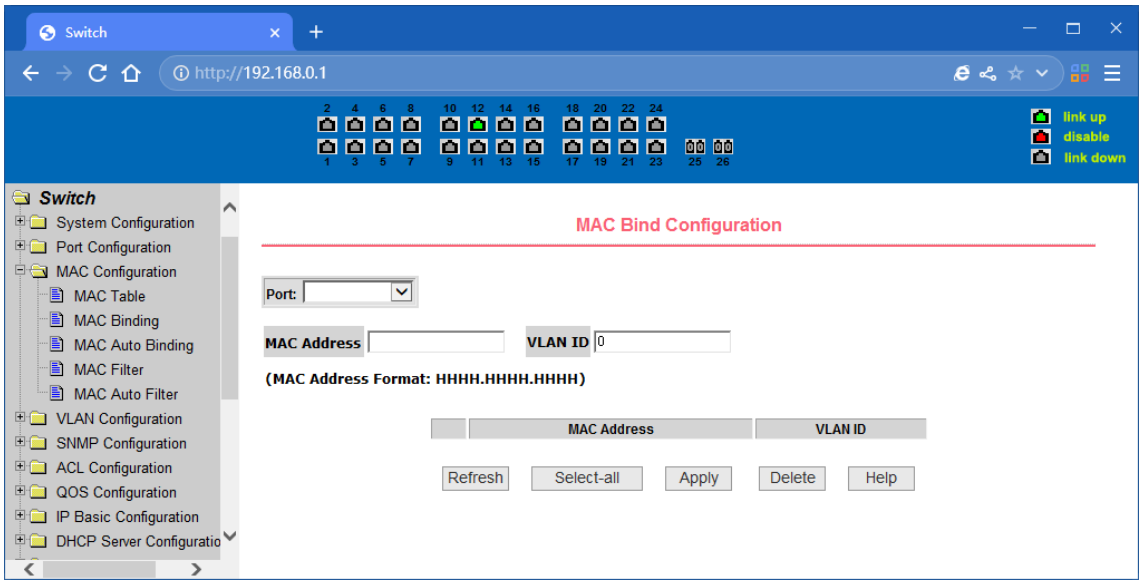
Port	Display the MAC address table of the Selected port. All means display the MAC address table of all ports
VLAN ID	Display the MAC address table of the input VLAN ID. 0 means display the MAC address table of all VLANs
MAC Number	The number of MAC addresses in the displayed MAC address table
MAC Address/VLAN ID/Port/Static	Display the MAC address table information



MAC Table page

（2）MAC binding configuration page

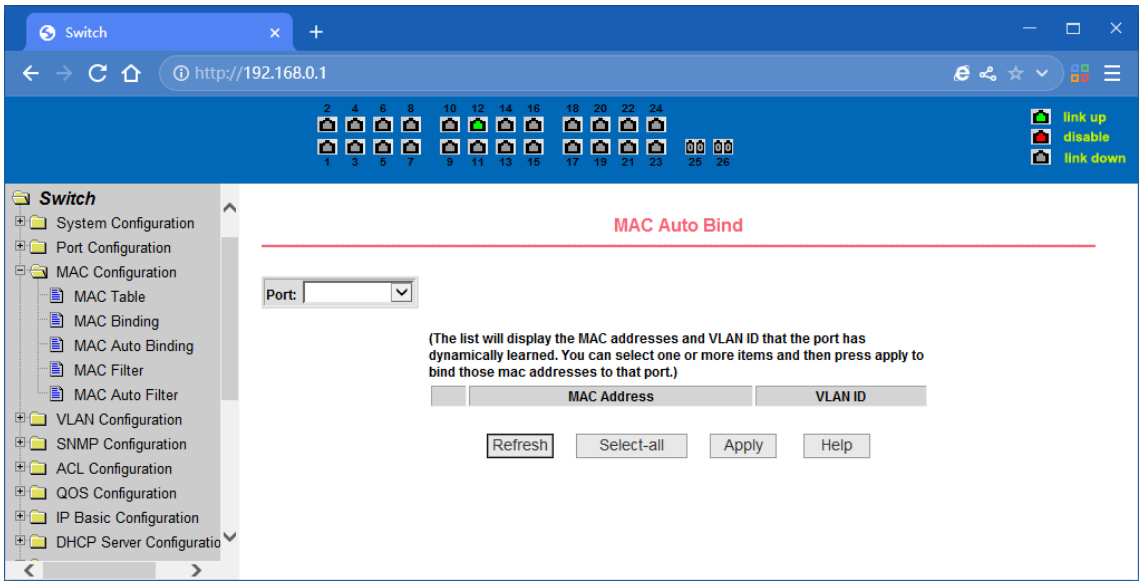
This page is used to achieve the port and MAC address binding.
MAC entries on the page is used to enter the MAC address binding, VLAN ID entry is used to enter the MAC address of VLAN



MAC binding configuration page

（3）MAC binding automatic conversion page

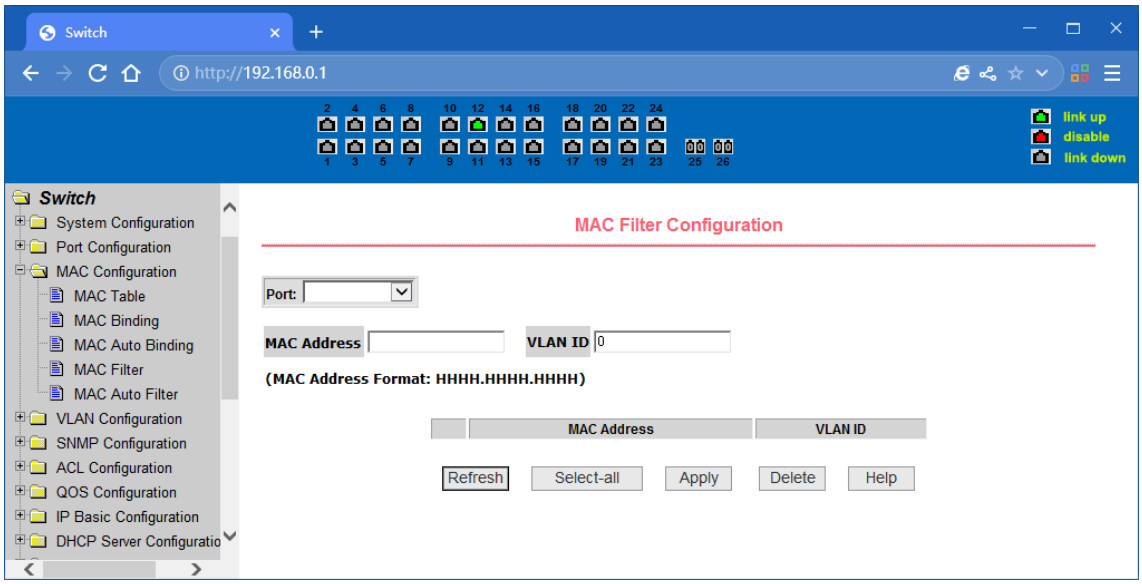
This page is used to achieve the port MAC address auto-binding. Shows the hardware switch on the lay2 the exist port dynamic MAC address and affiliated VLAN. Can choose one of the entry and convert it into static binding.



MAC binding automatic conversion page

（4）MAC filtering configuration page

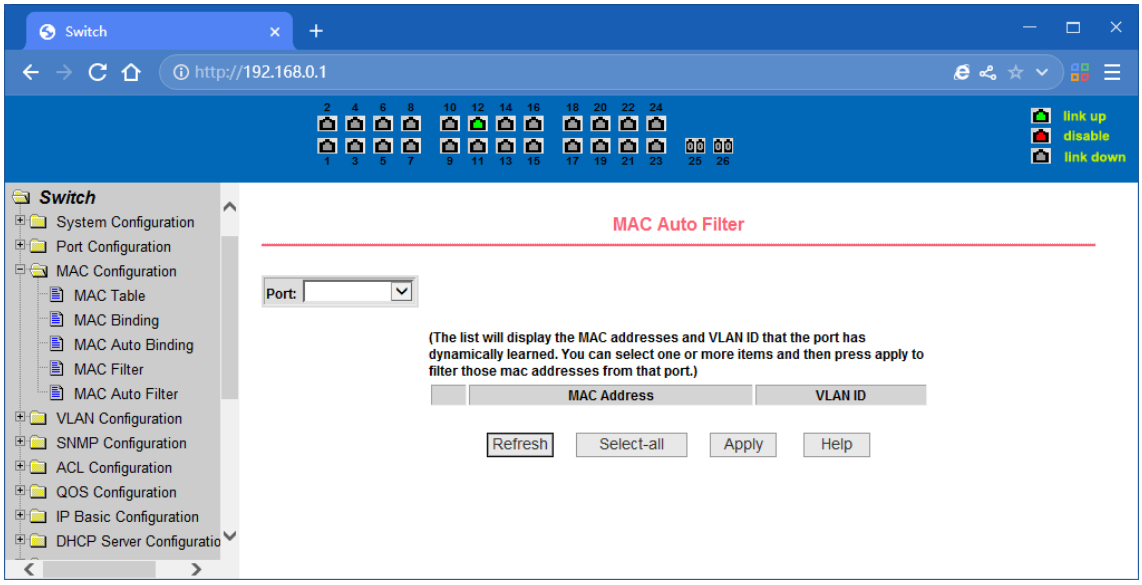
This page is used to configure the ports on the MAC address filtering.
MAC entries on the page is used to enter the MAC address filtering. VLAN ID entry is used to enter the MAC address affiliated VLAN.



MAC filtering configuration page

（5）MAC filtering 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 filtering configuration



MAC filtering automatic conversion page

4.6. VLAN Configuration

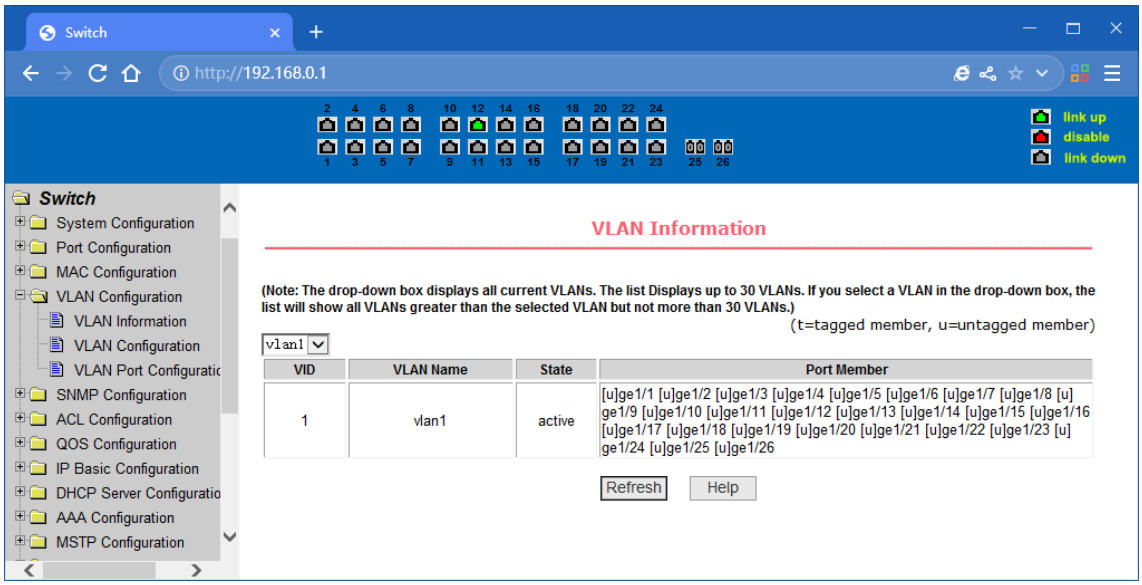
（1）VLAN information page

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

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

T tagged the port is the VLAN tagged member

U untagged the port is the VLAN untagged member



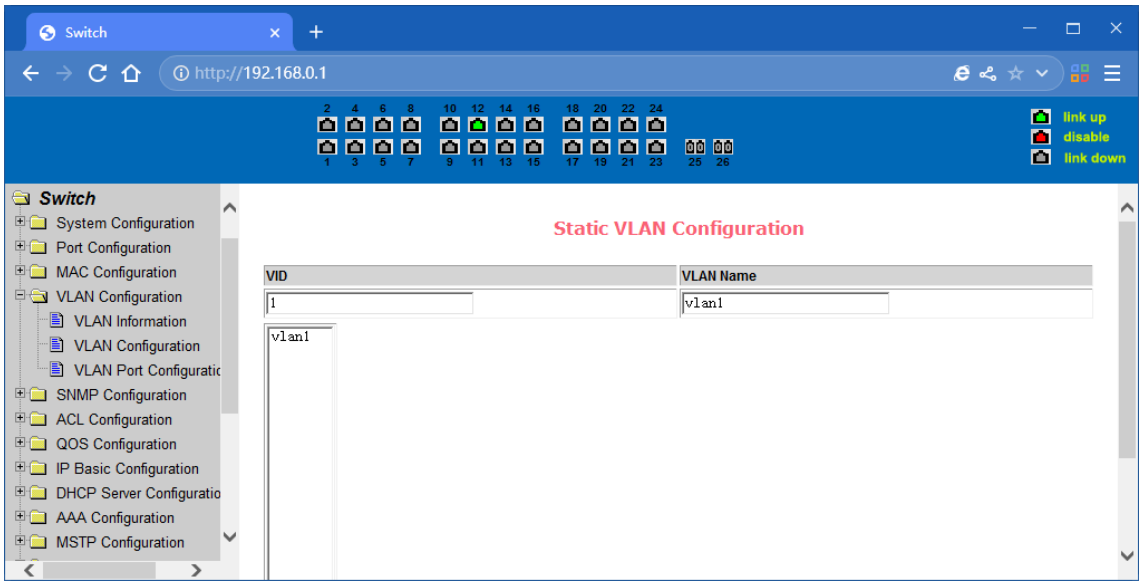
VLAN information page

（2）Static VLAN configuration page

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

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

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



Static VLAN configuration page

（3）VLAN port configuration page

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

Port is defined a designated port that will configure the VLAN

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

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

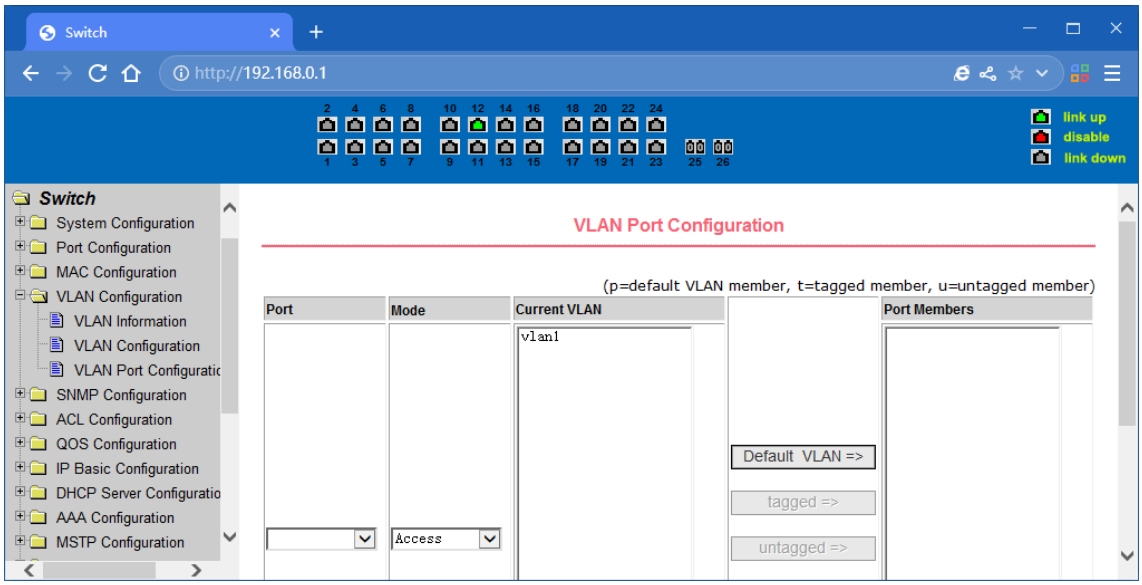
VLAN Port-owned shows the results of VLAN port configuration, [p] indicates that the port VLAN is the default VLAN, [t] that the port is a VLAN tag members, [u] that the port is not tagged VLAN member. When you remove VLAN, the user from the list, select the VLAN, can be multiple-choice.

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

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

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

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



VLAN port configuration page

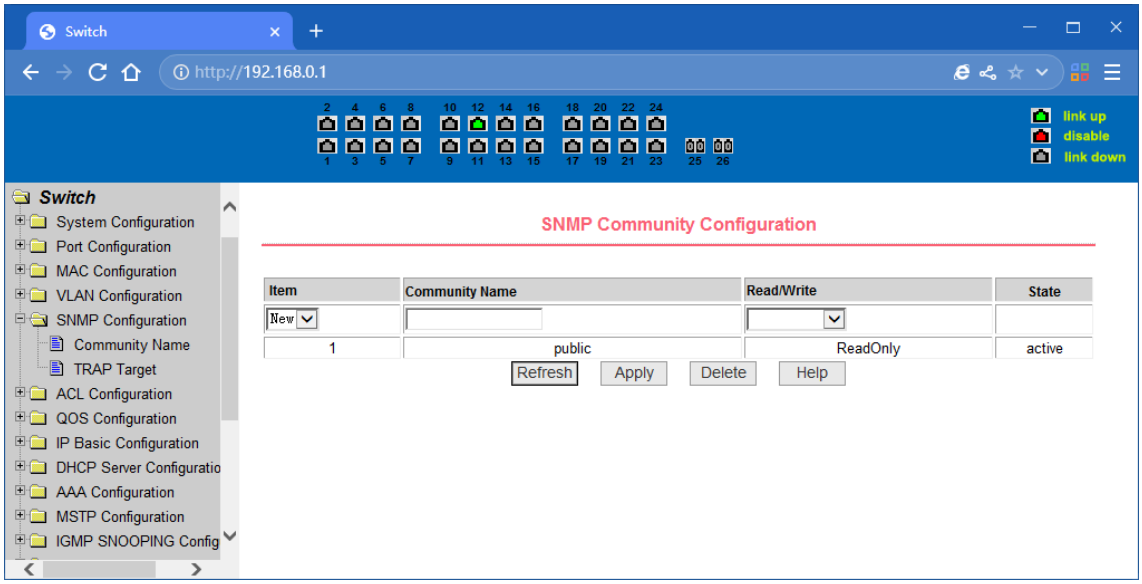
4.7. SNMP Configuration

（1）SNMP share body configuration page

This page allows users to configure the switch common body's name and read and write access, a total of 8 entries can be configured

By default, the switch there is a share name as named public, the common body is read-only access. With this correspondence, the activities of this page are only one entry, shared body names are public, and access is read-only access.

When the switch through SNMP for network management, you need to configure a read-write permissions to the shared body.

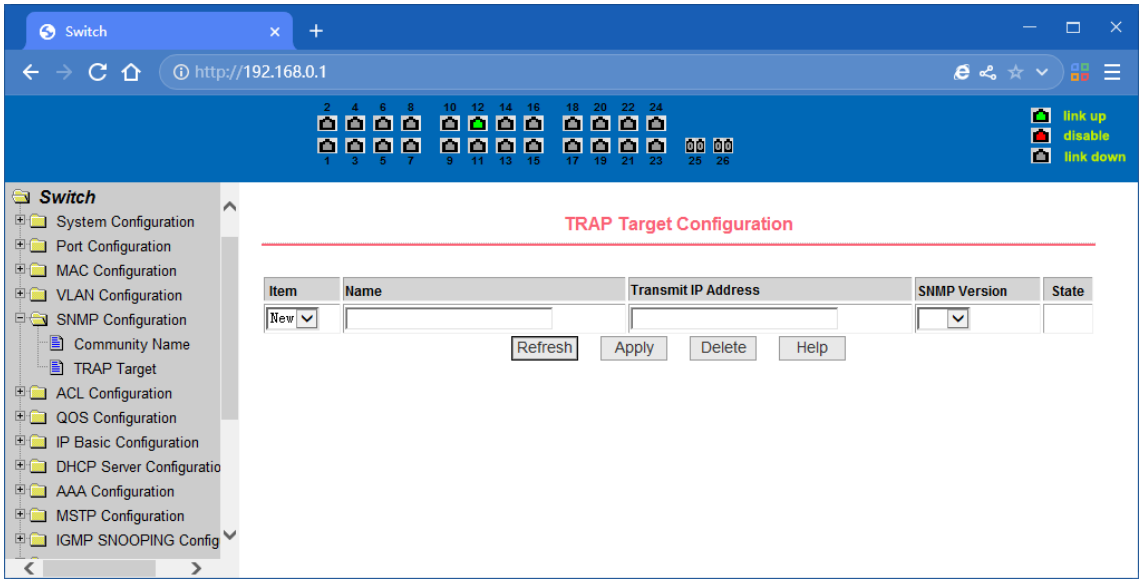


Shared body of SNMP configuration page

（2）TRAP target configuration page

This page allows users to configure the workstation to receive TRAP messages as well as the IP address of TRAP protocol packets of some of the parameters.

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

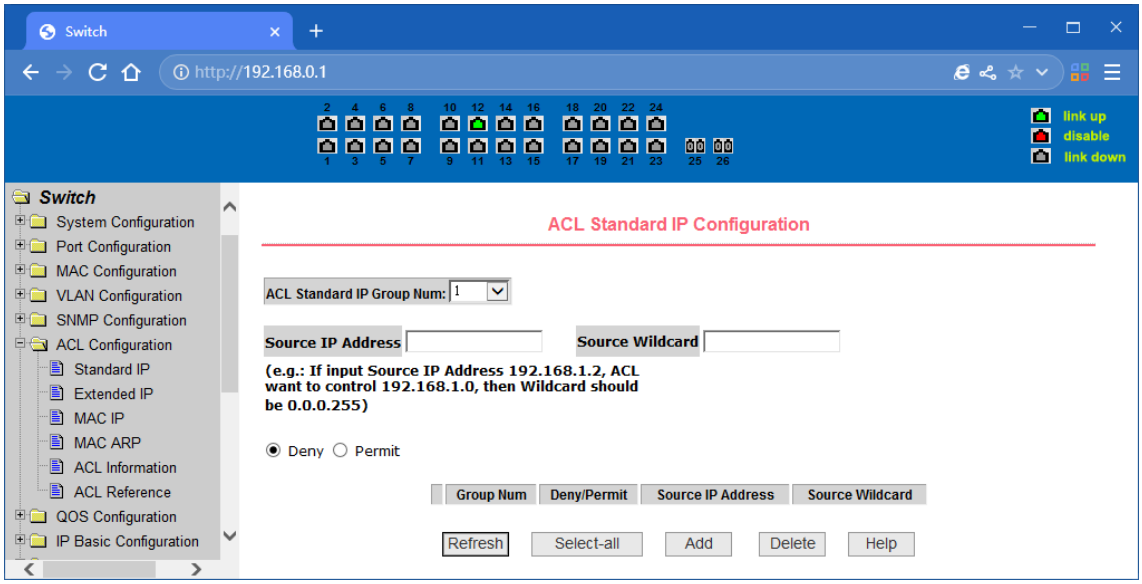


TRAP target configuration page

4.8. ACL Configuration

（1）IP Standard ACL configuration page

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



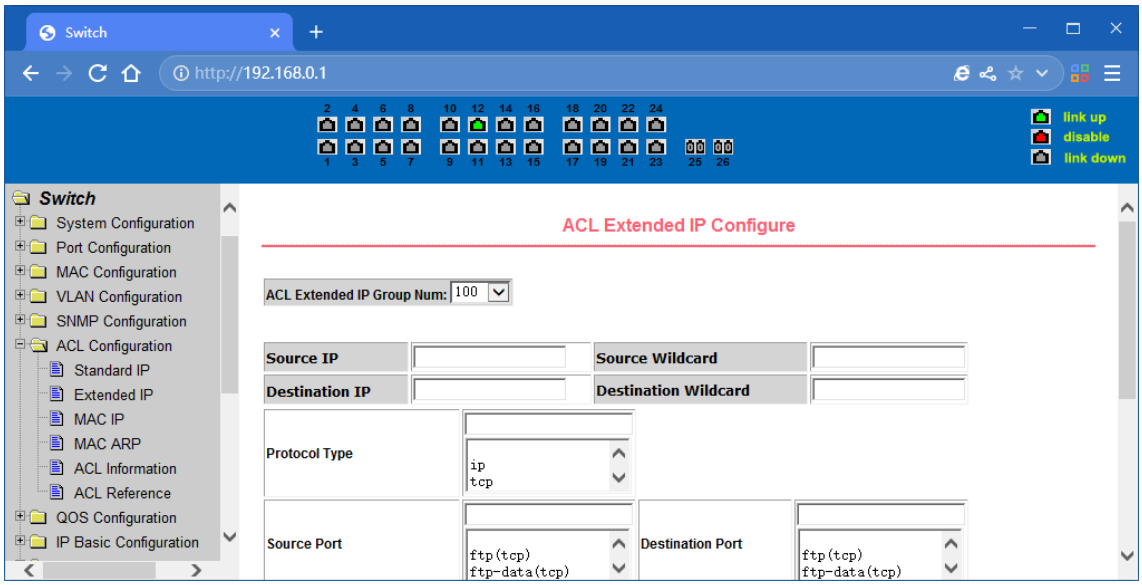
IP standard ACL configuration page

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

When users configure the rules, each rule must have a filter mode: allow or deny.
The user to create a rule in the group, the system will automatically give the rule a rule number, when to delete a rule in the group 1 rules, other rules remain unchanged, and the system will automatically give the rule a rule group sort. If the user wants to delete the entire rule set, you can first select all, then click the delete key.

（2）IP Extended ACL configuration page

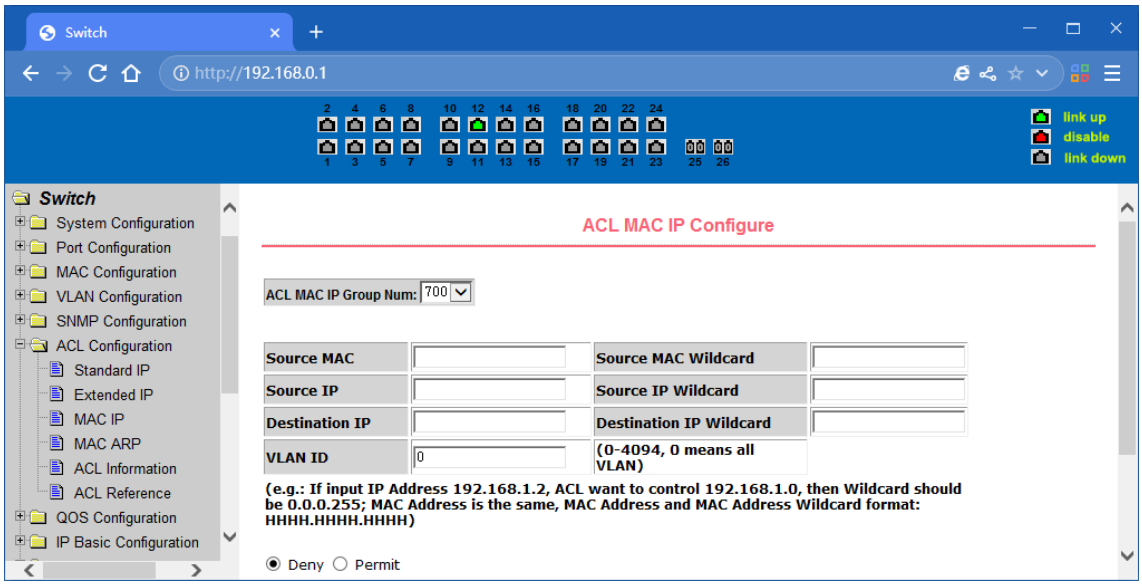
The extended IP group is an extension of the standard IP rules. Control the packet forwarding via source IP, Destination IP, and IP protocol type and service port.



IP Extended ACL configuration page

（3）MAC IP ACL configuration page

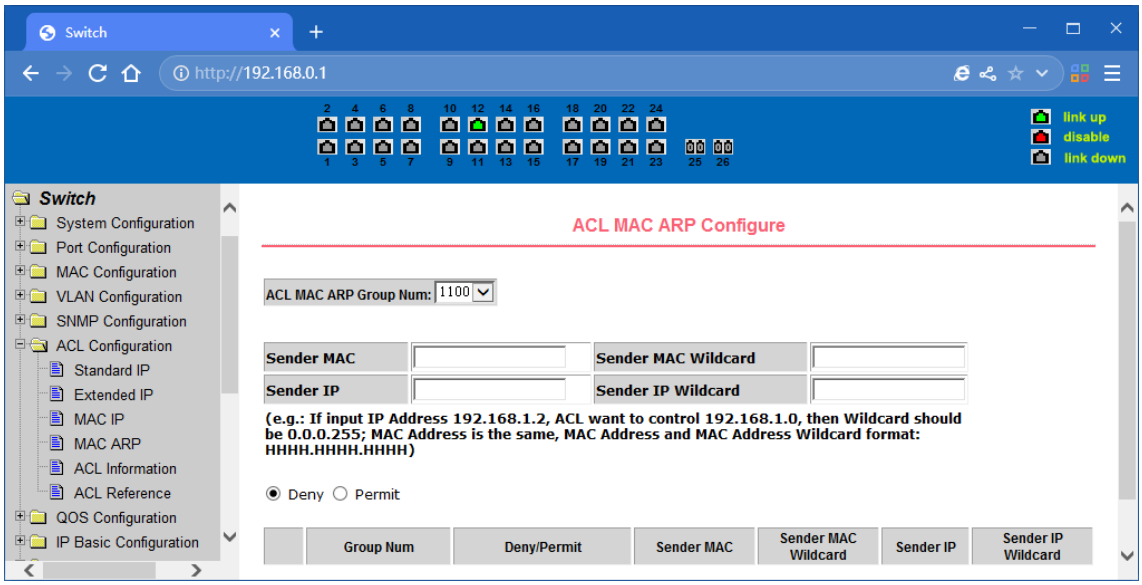
It is the MAC IP ACL configuration page. IP MAC group can be the IP packet source and destination MAC address and source and destination IP address control.



IP Extended ACL configuration page

（4）MAC ARP ACL configuration page

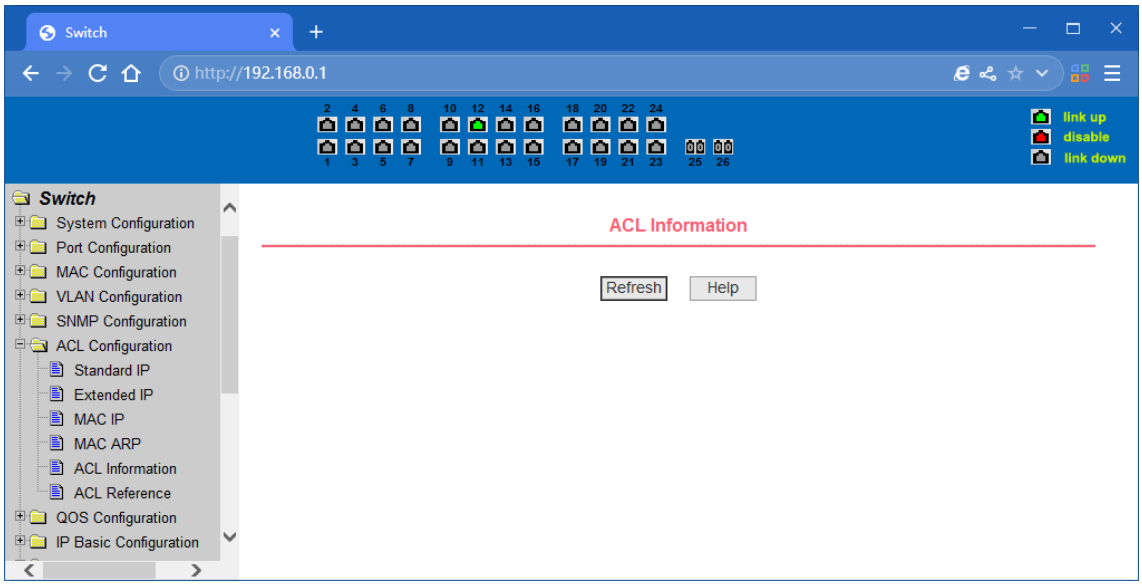
It is the MAC ARP ACL configuration page. ARP group can be the type of the operation of the ARP packet, the sender MAC and the sender IP control.



IP Extended ACL configuration page

（5）ACL information page

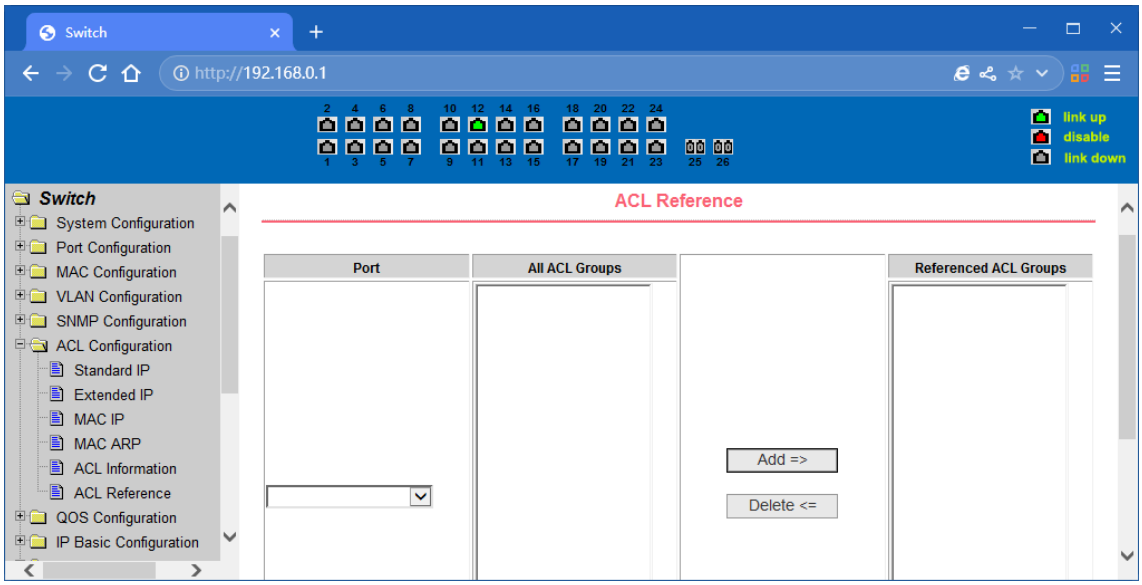
The ACL information page displays the current ACL rules configured in all the information.



ACL information page

（6）ACL configuration information page

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

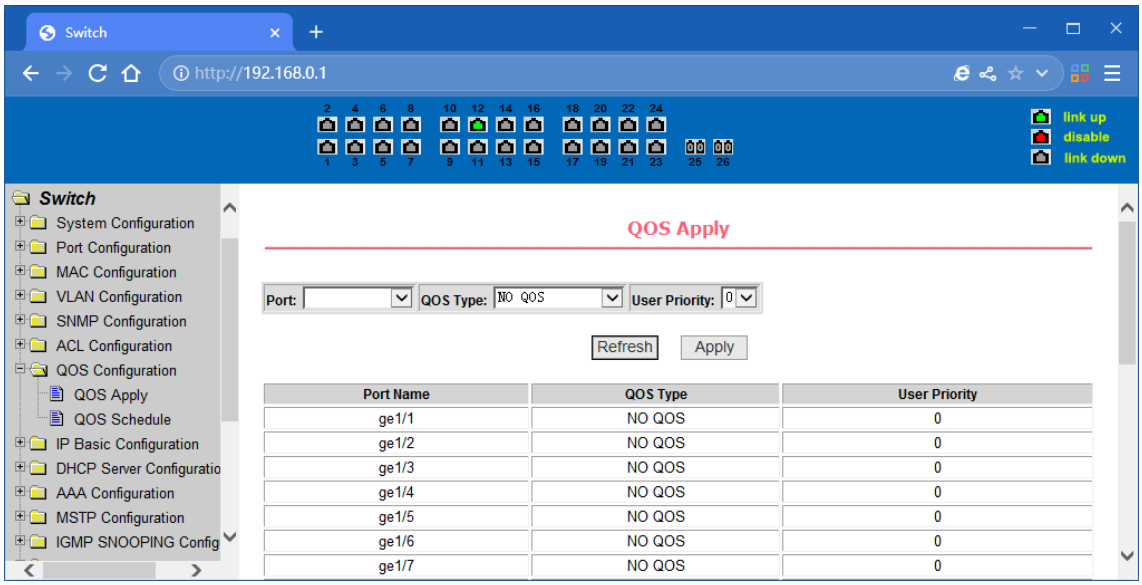


ACL application page for a port

4.9. QoS Configuration

（1）QoS Apply Configuration Page

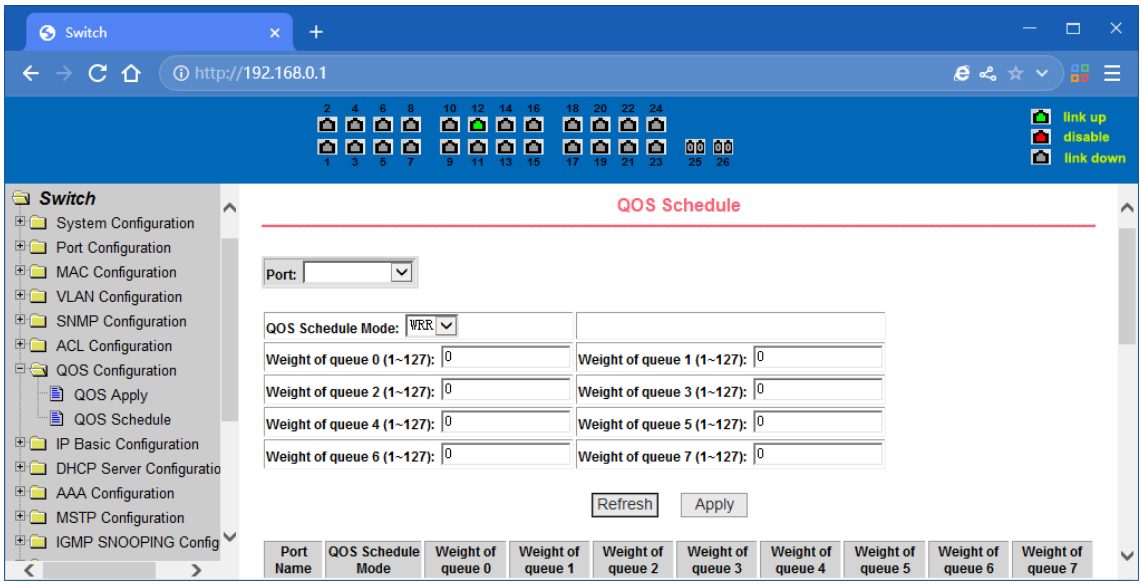
This is a QoS Apply configuration page.



QoS Apply configuration page

（2）QoS Schedule Configuration Page

This is a QoS Schedule configuration page.

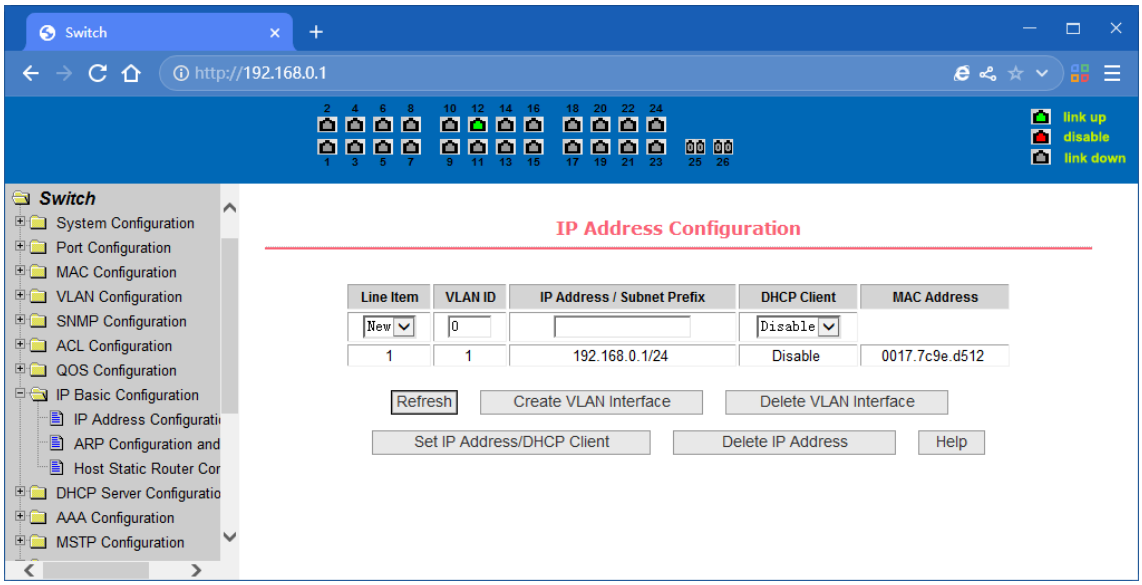


QoS Schedule configuration page

4.10. IP Basic Configuration

（1）VLAN Interface Configuration Page

Users can configure the VLAN interface through this page, delete VLAN interfaces, configure the interface IP address, remove the interface IP address, and view interface information. VLAN already exists can only be set when the interface can only be configured on the interface set interface address.



VLAN interface configuration page

Switch in the default have a VLAN1 interface, the interface cannot be deleted. One can only configure a VLAN interface.

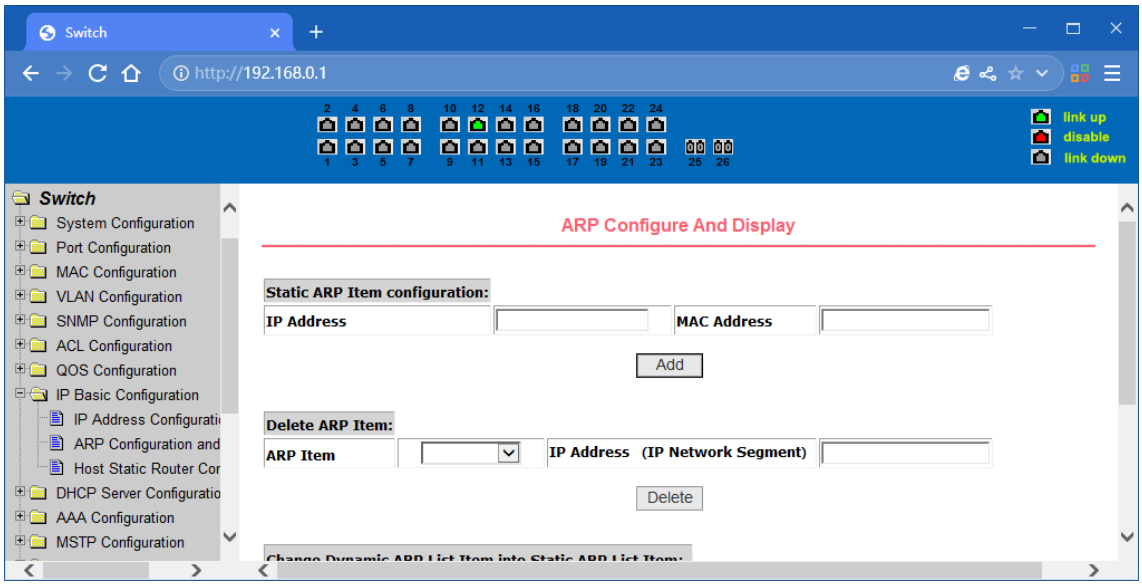
（2）ARP configuration and display page

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

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

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

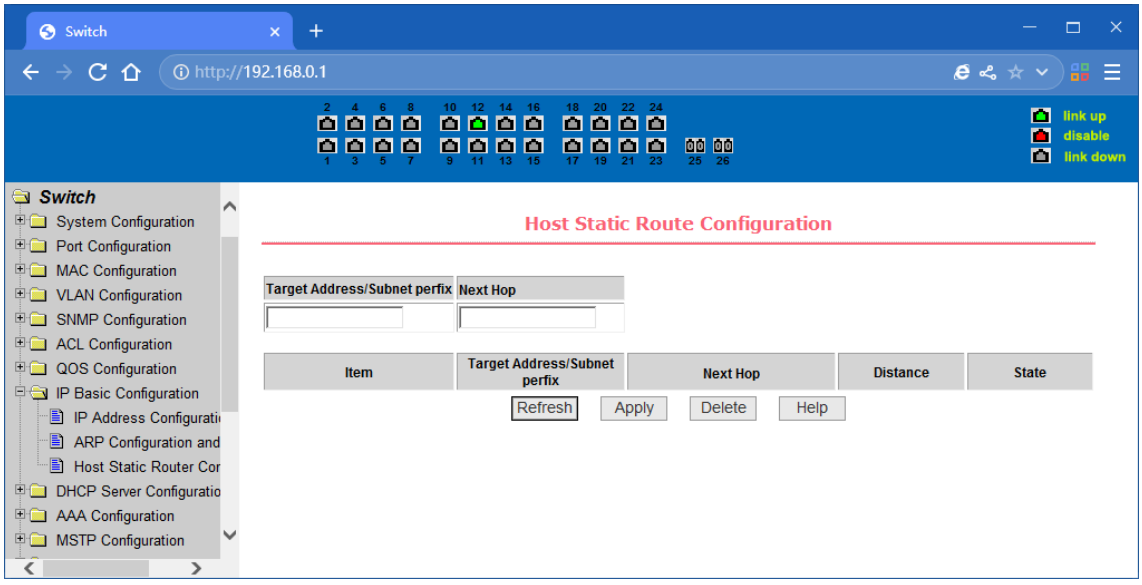
When dynamic ARP table entry was revised to a static ARP table entry, you can choose to a particular network segment or all of the dynamic ARP table entry was revised to a static ARP table entry. For the situation to a network segment is required in the input box, enter the specified network segment.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



ARP configuration and display page

（3）Host Static Routing configuration page

The user can through this page to add, delete static routing switch hosts. By default, the switch is not configured to host a static route, the user can configure the default route through this page, that is the purpose of address / subnet prefix is 0.0.0.0 / 0 routing



Host static route configuration page

4.11. DHCP Server

（1）DHCP Server Global & Interface Configuration

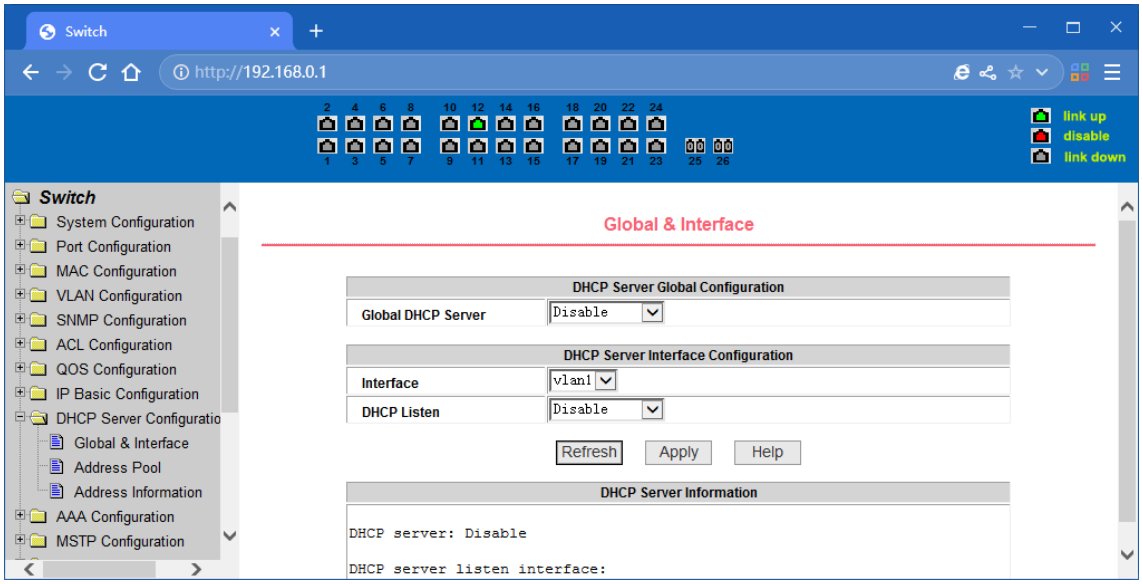
This page is used to configure DHCP server, including global and interface configuration.

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 Configuration

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.

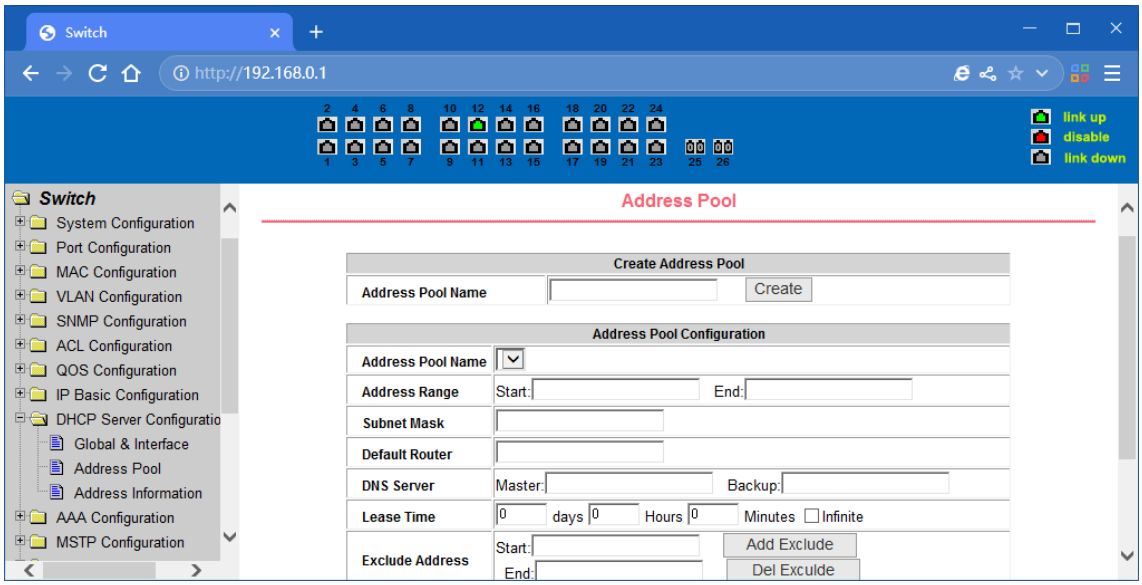
Default Router: Set the default router that this address pool can assign to DHCP clients.

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.

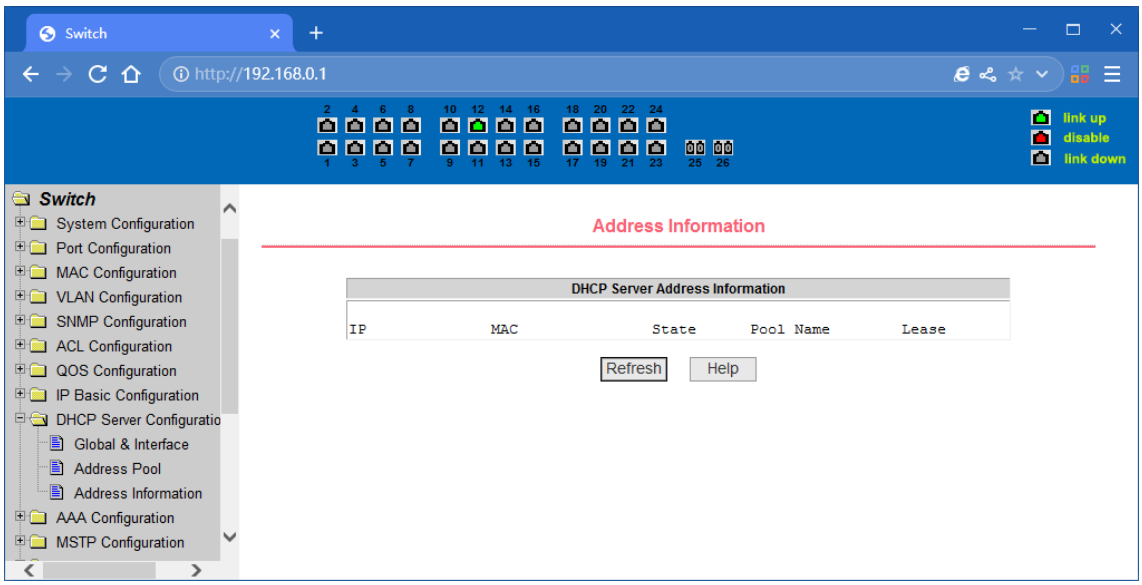
Option 82 Circuit ID: Set the option 82 circuit id applicable to the address pool.



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.



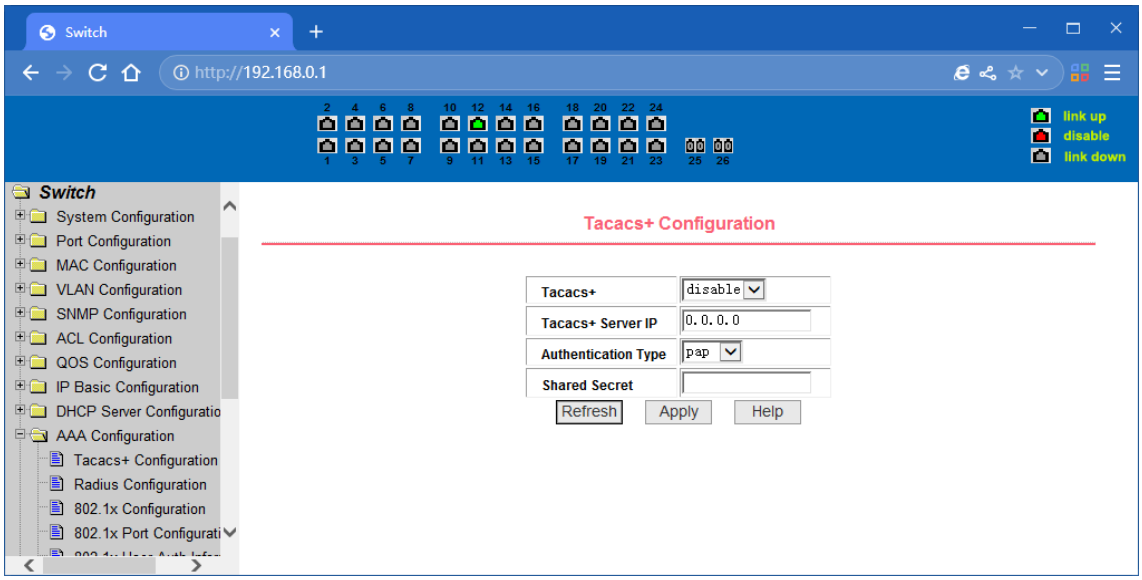
DHCP Server Address information page

4.12. (AAA) configuration

（1）TACACS+ Configuration:

TACACS+ protocol is the latest generation of TACACS. It uses TCP to ensure reliable delivery. The separation of authentication, authorization and accounting is a fundamental component of the design of TACACS+.

TACACS+	gives the option to enable TACACS+
TACACS+ Server IP	Gives the option to specify a TACACS plus server IP address
Authentication Type	The type of authentication supported: PAP (default) and CHAP
Shared Secret	The secret key that is a Shared Secret between TACACS+ client and daemon



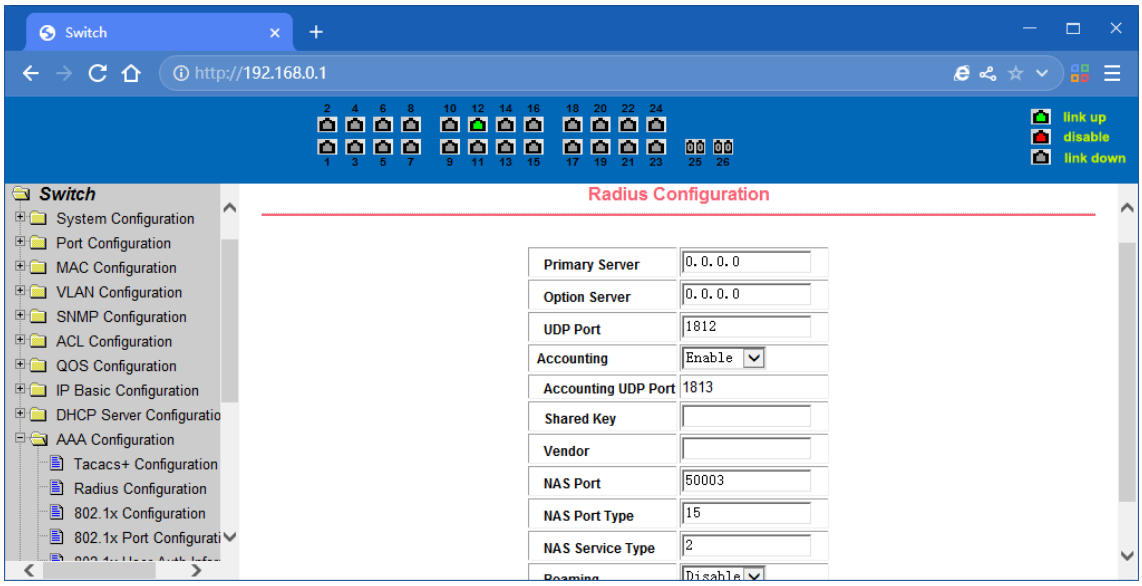
TACACS+ Configuration page

（2）Radius Configuration Page

Users can configure with the Radius-related information via this page, you can set information includes:

1. Be sure to set the Radius server's IP address before do the authentication and accounting in this field,
2. Optional Radius server IP address, if there is spare Radius server can set this field.
3. Authentication UDP port, the default value is 1812, the user generally do not need to modify this field.
4. Whether to activate the , the default is to start, and when you do authentication and accounting in general to start charging.
5. Accounting UDP port, the default value is 1813.
6. Shared secret key is used to setting the shared encryption password between the switch and the Radius server, so be sure to set the authentication and accounting in this field, and with the same settings on the Radius server.

7. Vendor-specific information, the users typically do not need to modify this field.
8. NAS ports, NAS port type, NAS type of service, these three values do not change in general.
9. Whether to on or off the roaming feature of Radius.

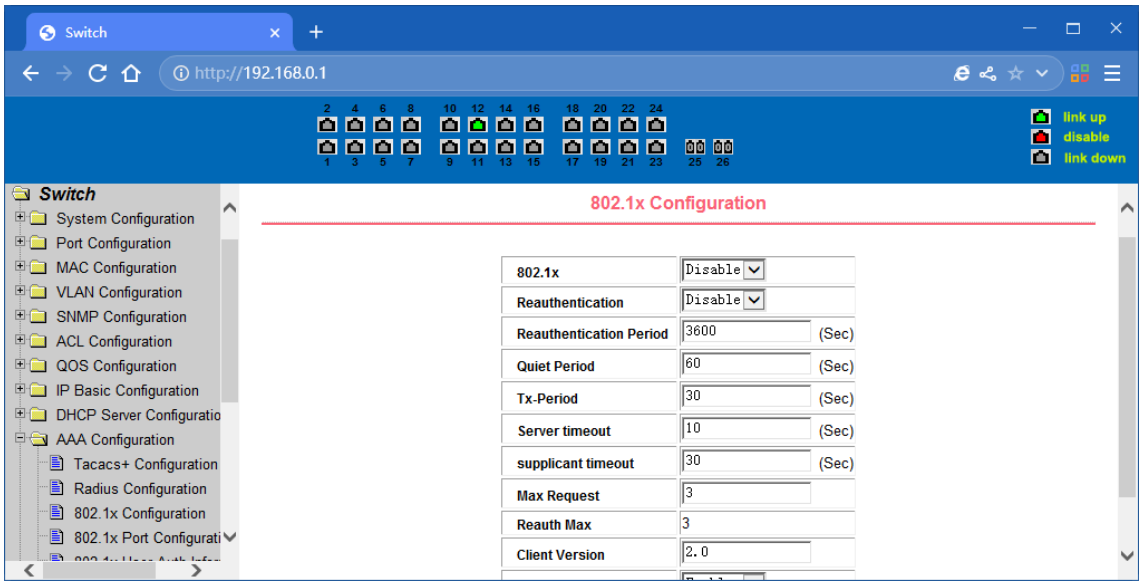


Radius configuration page

（3）802.1x Configuration Page

Users can configure 802.1x related information on this page, including:

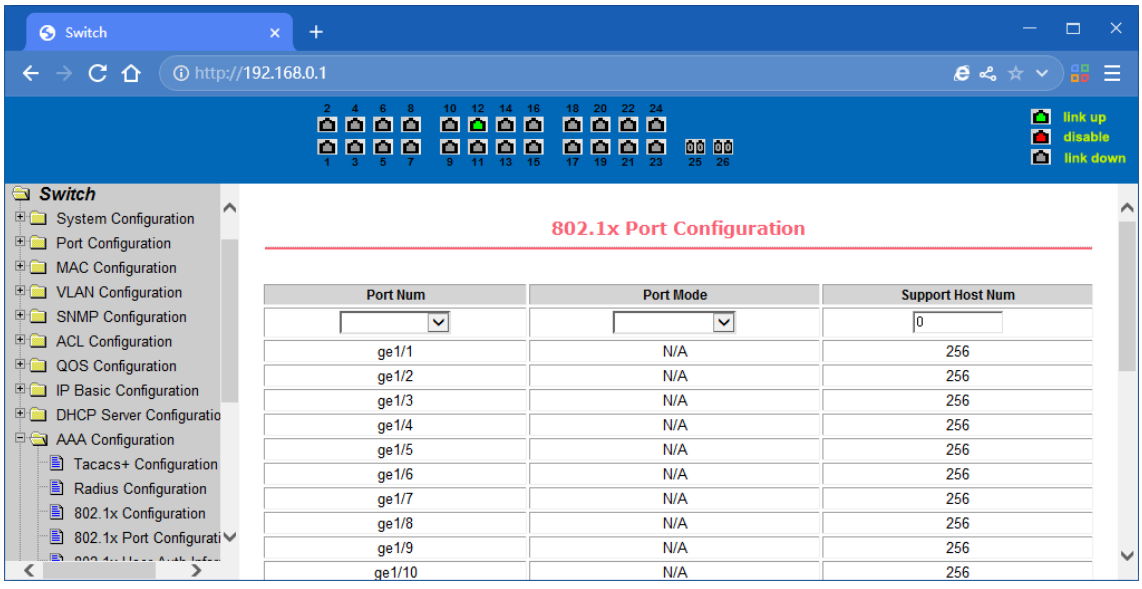
1. Whether to activate the 802.1x protocol, when doing authentication and accounting must be to start 802.1x protocol.
2. Switch is to adopt a common authentication method or the expansion of authentication.
3. Whether to open re-authentication function, the default is not open. When you do authentication and accounting based on the actual circumstances. Open the re-authentication feature will make users more reliable when using the authentication and accounting, but it will slightly increase the network traffic.
4. Setting re-certification time interval, only to re-open the case of authentication to be valid, the default is 3600 seconds, when you do authentication and accounting based on the actual situation to set the value, but the value is not too small.
5. Quiet Period Timer, users typically do not need to modify this field.
6. Tx-Period Timer, users typically do not need to modify this field.
7. Server timeout timer, users typically do not need to modify this field.
8. Supplicant timeout timer, users typically do not need to modify this field.
9. Max Request number, users generally do not need to modify this field.
10. Showing Reauth Max size.
11. Client Version, the client version number.
12. Check Client, whether the certification passed then examine the client's regular flow of packets.



802.1x configuration page

（3）802.1x port configuration page

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

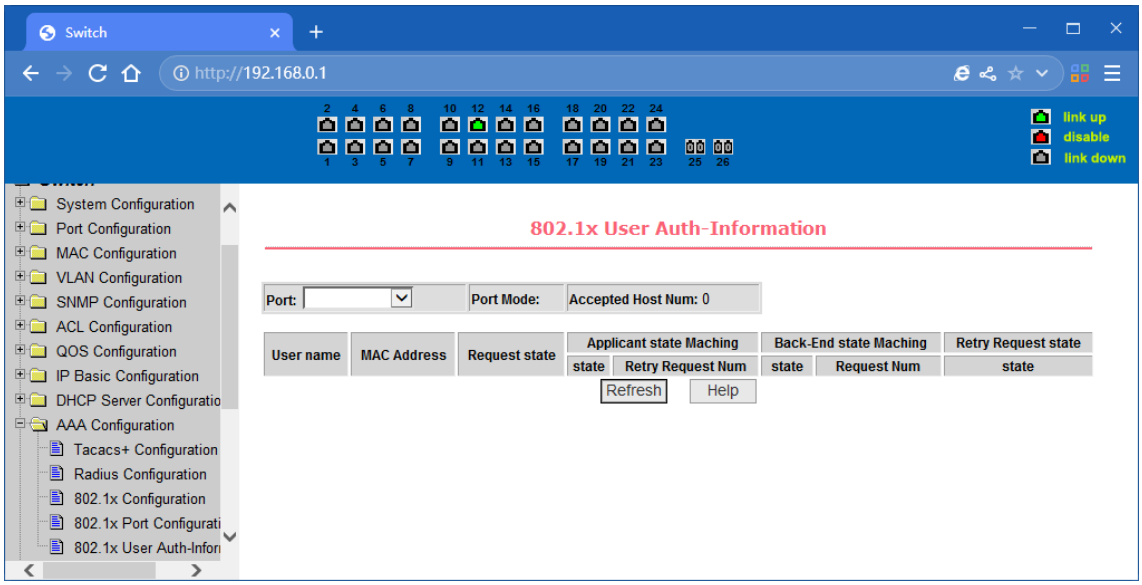


802.1x port configuration page

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

（4）802.1x user authentication information page

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



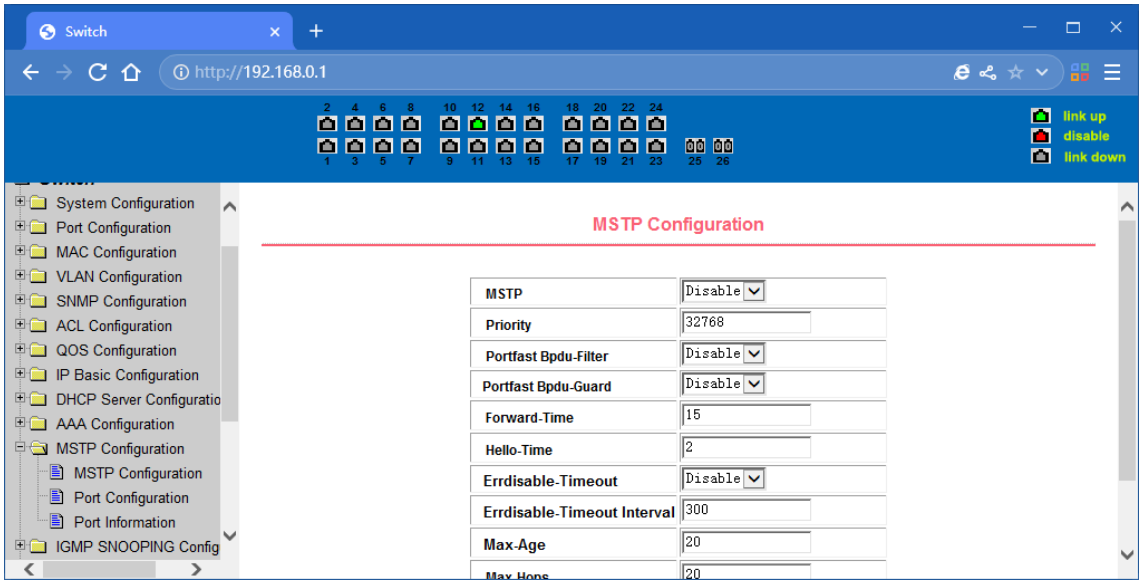
802.1x user authentication information page

4.13. Spanning Tree Protocol configuration

（1）MSTP global configuration page

Through this page, you can configure some MSTP related information, mainly including:

- Whether to enable MSTP.
- Configure the bridge priority. Devices with lower priority are more likely to be the root bridge.
- Enable BPDU filtering function on the port in the portfast bpdu-filter default state.
- Enable BPDU guard function on the port in the portfast bpdu-guard default state.
- Configure the forwarding delay.
- Configure the interval for sending MSTP Hello packets.
- The errdisable mechanism is started. When a port that starts a BPDU guard receives a BPDU, it starts the errordisable timer. errordisable restarts this port after the configured timeout.
- Configure errordisable timeout time.
- Configure the number of seconds the switch waits to receive spanning tree configuration information before triggering a reconfiguration.
- Configure the number of hops specified before a BPDU is dropped in a domain.
- Start or shut down and cisco compatible spanning tree protocol.

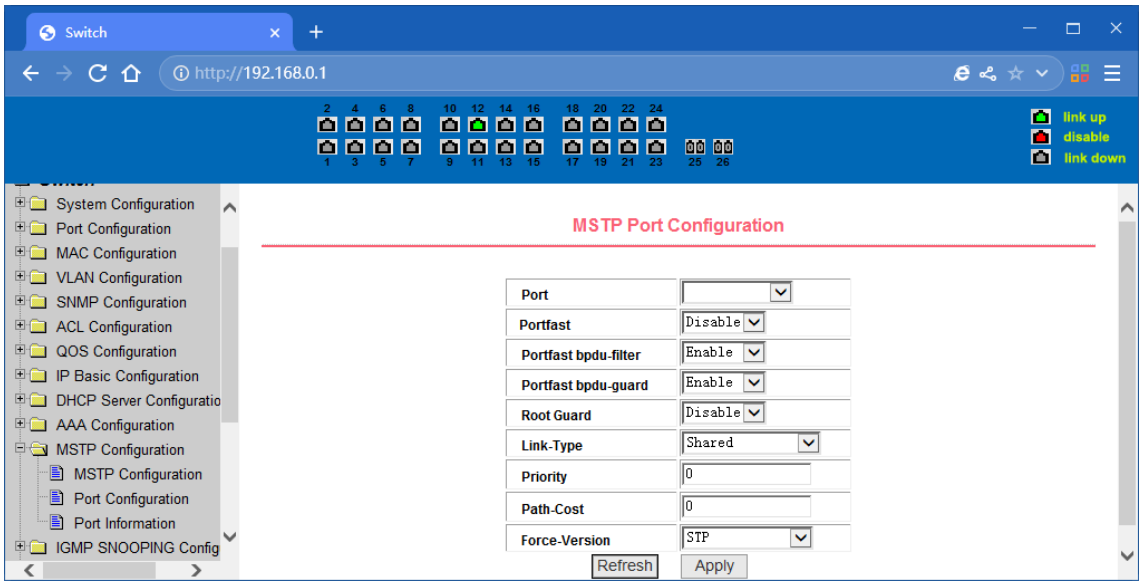


MSTP Global Configuration Page

（2）MSTP port configuration page

Through this page, user can configure some MSTP related information, mainly including:

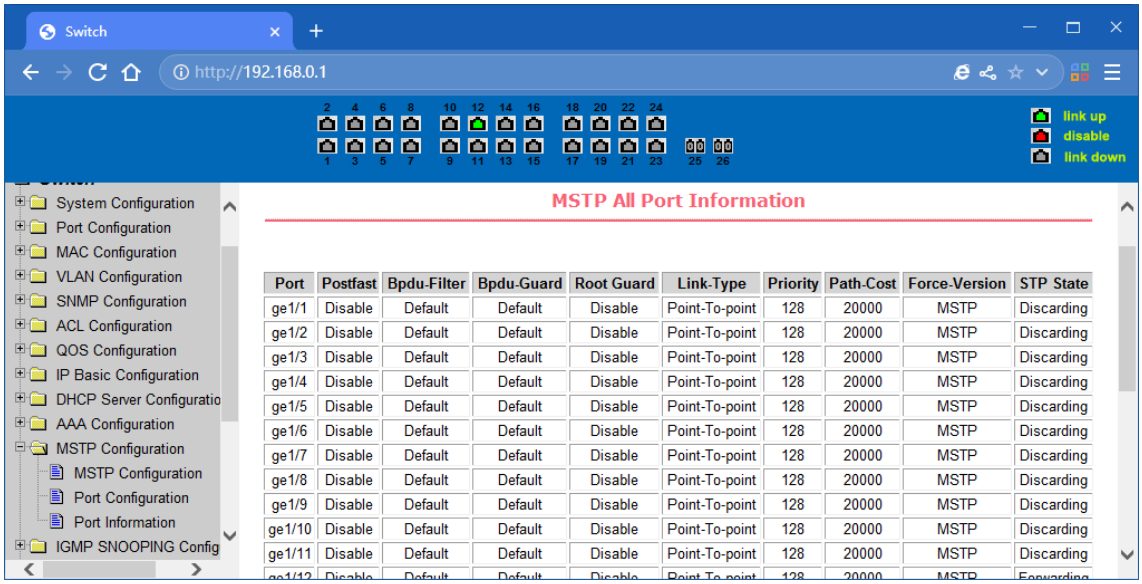
- Select the port to be configured.
- Configure a port as a port fast port to enable the port from the blocking state to the forwarding state, bypassing the listening and learning states.
- Open the BPDU filter on the selected port.
- Enable BPDU guard on the selected port.
- Enable the root guard function, and do not accept BPDU packets with a higher priority than the bridge. Specify the switch as the root switch.
- Configure the connection type. Point-to-point: The type of connection is point-to-point, allowing fast transition of the port status. Shared: Connection type is shared, does not allow rapid conversion of port status, to go through the calculation process of 802.1D to determine the status of the port.
- Configure the cist priority of the interface. Range 0-240, can only be a multiple of 16. The default is 128.
- Configure the cist path cost. Range 1-200000000. The default is 20000000. Lower path costs are more likely to be roots.
- Configure the type of protocol packets to be sent.



MSTP Port Configuration Page

（3） MSTP configuration information page

It is the MSTP configuration information page, through which you can view some MSTP related information



MSTP Configuration Information page

4.14. IGMP SNOOPING configuration

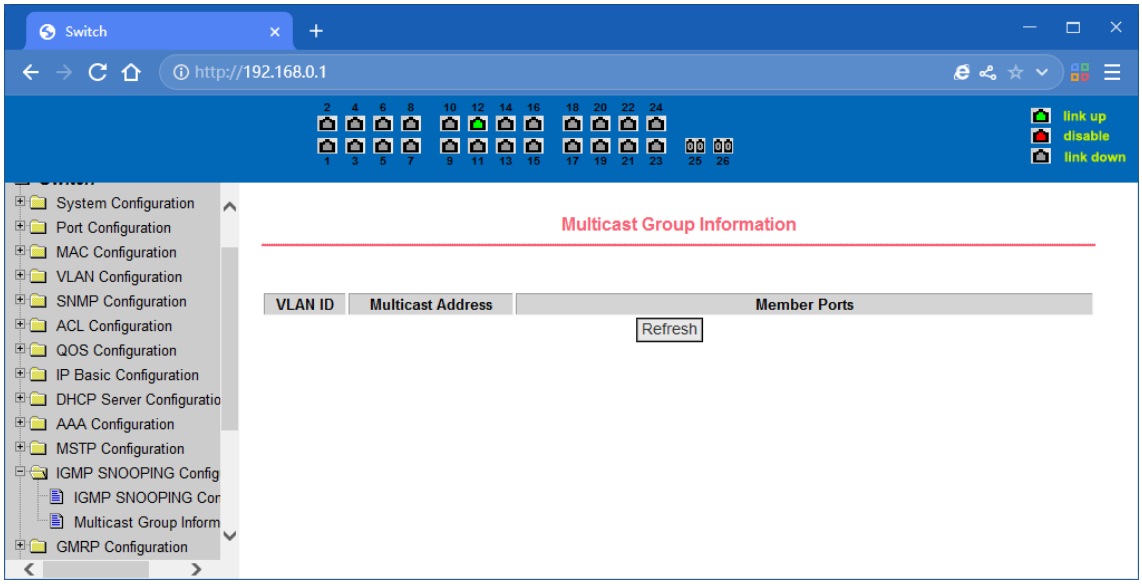
（1）IGMP SNOOPING configuration page

It is the IGMP SNOOPING configuration page, through which you can start IGMP SNOOPING.

GMP SNOOPING configuration page

（2）IGMP SNOOPING information page

It is the IGMP SNOOPING information page, which allows users to view some information about IGMP SNOOPING.



IGMP SNOOPING Information page

4.15. GMRP configuration

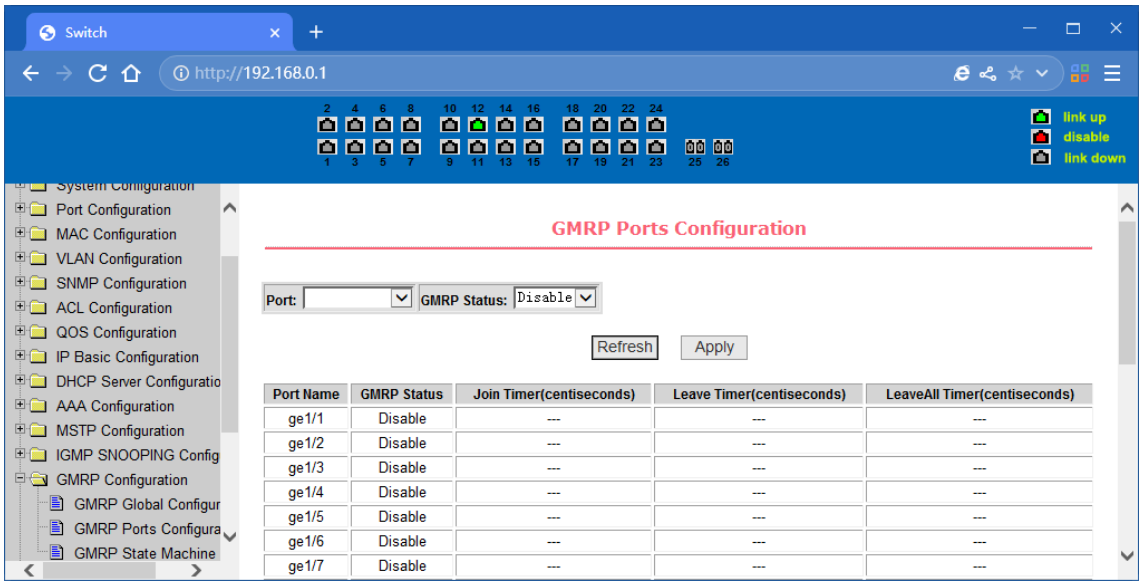
（1）GMRP Global Configuration Page

Users can enable GMRP through this page.

GMRP Global Configuration Page

（2）GMRP port configuration page

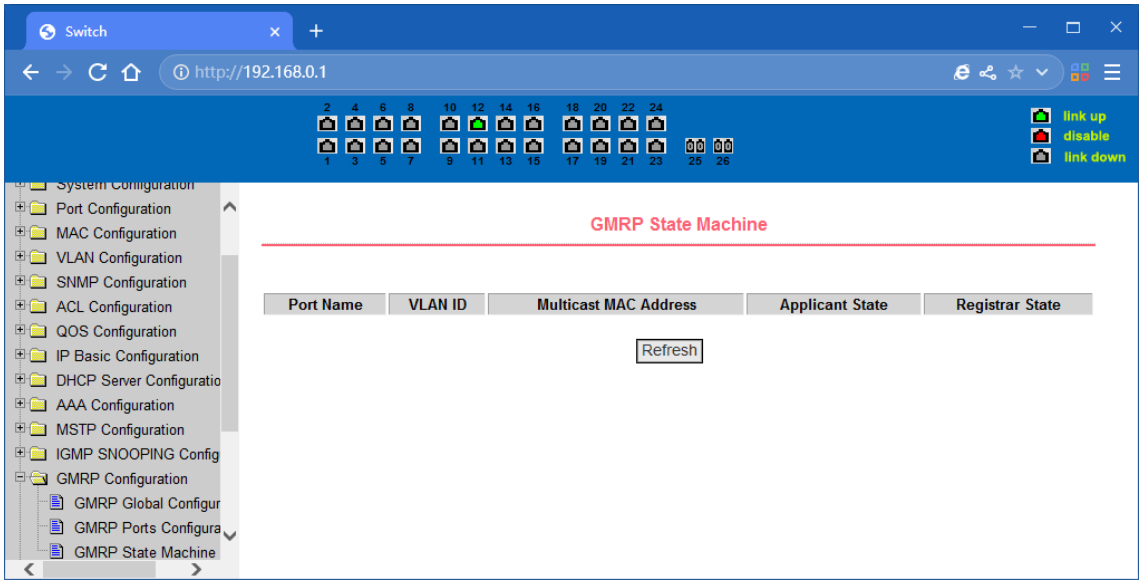
You can use this page to enable the GMRP port and view the port information.



GMRP Port Configuration Page

（3）GMRP state machine page

Users can view the GMRP state machine information through this page.



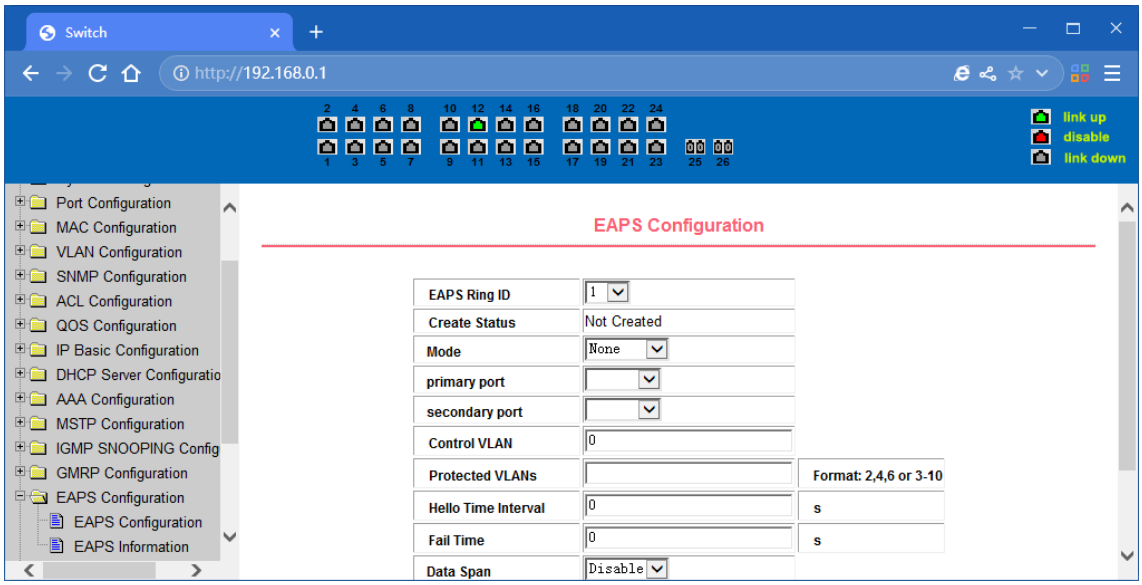
GMRP state machine page

4.16. EAPS configuration

（1）EAPS configuration page

Through this page, you can configure some EAPS related information, including:

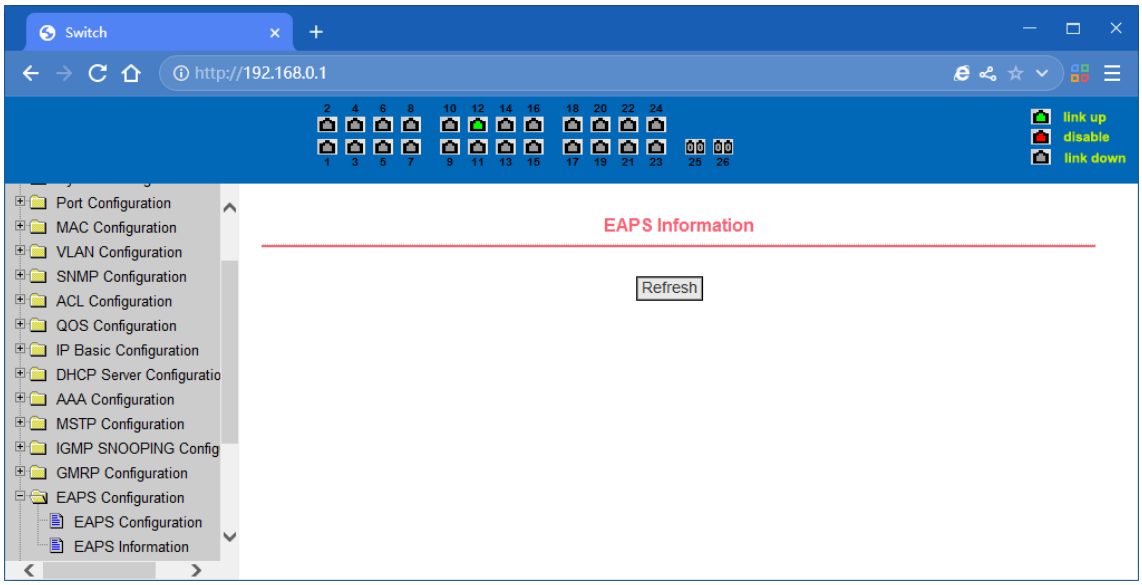
- Select an EAPS ring number.
- Configure the operating node mode of an EAPS Domain.
- Configure Primary Port of EAPS Domain.
- Configure Secondary Port of EAPS Domain.
- Configure a control VLAN for EAPS Domain.
- Add one or more protected VLANs of the EAPS Domain.
- Configure an EAPS Domain to periodically 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

Through this page, users can view some EAPS related information.

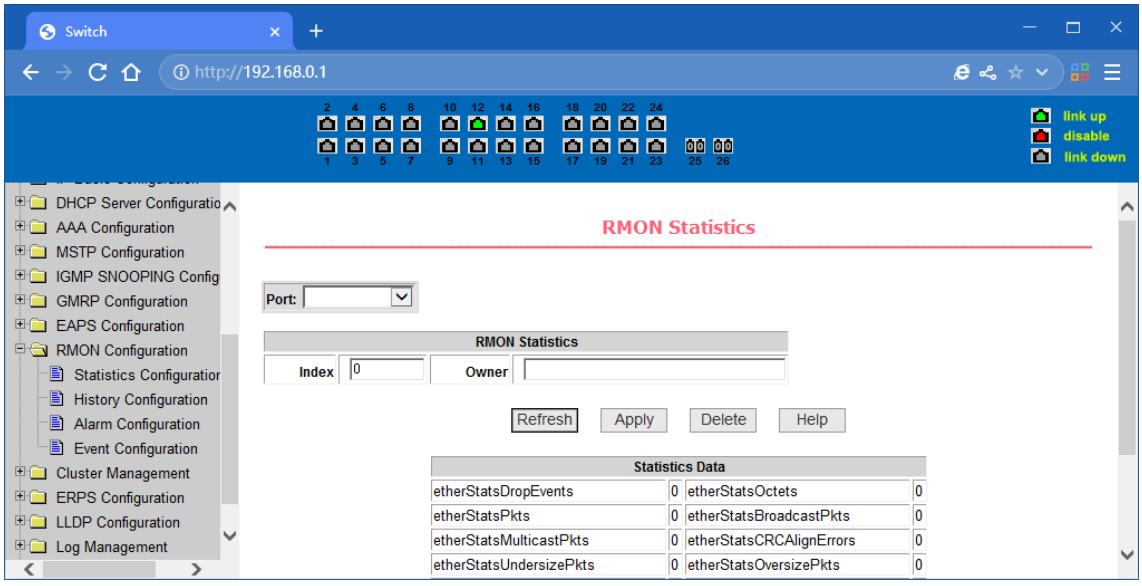


EAPS information page

4.17. RMON configuration

（1）RMON statistics group configuration page

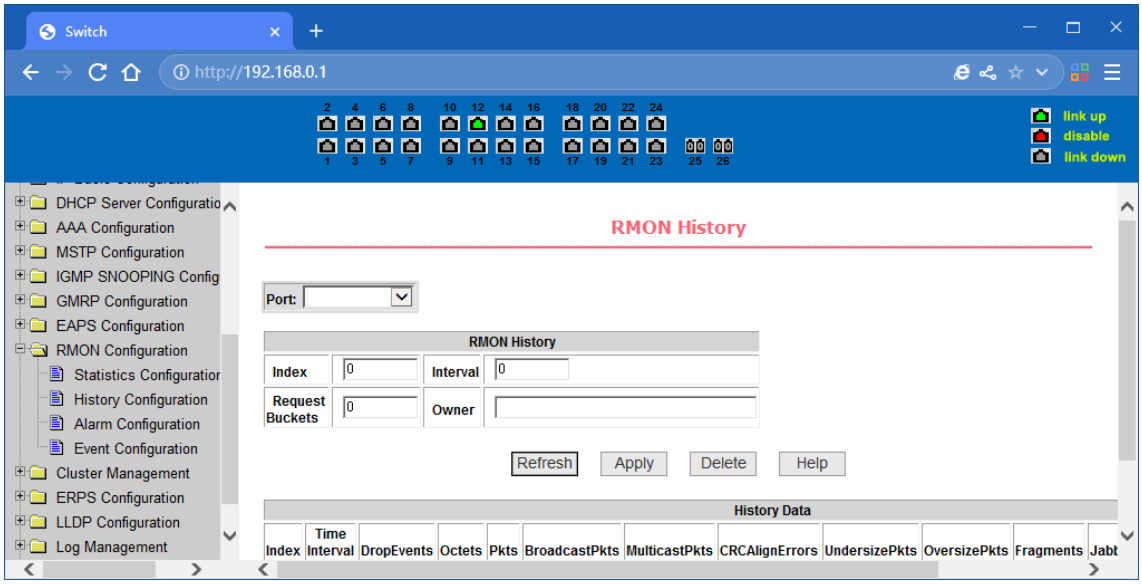
You can use this page to configure the RMON statistics group. Select a port from the drop-down list to view/configure the RMON statistics group configuration for this port. When not configured, the index number is 0, fill in the correct index number (range 1 to 100), the owner is optional, you can configure RMON statistics group for the port. The statistics table shows the port statistics from the successful configuration.



RMON statistics group configuration page

（2）RMON history group configuration page

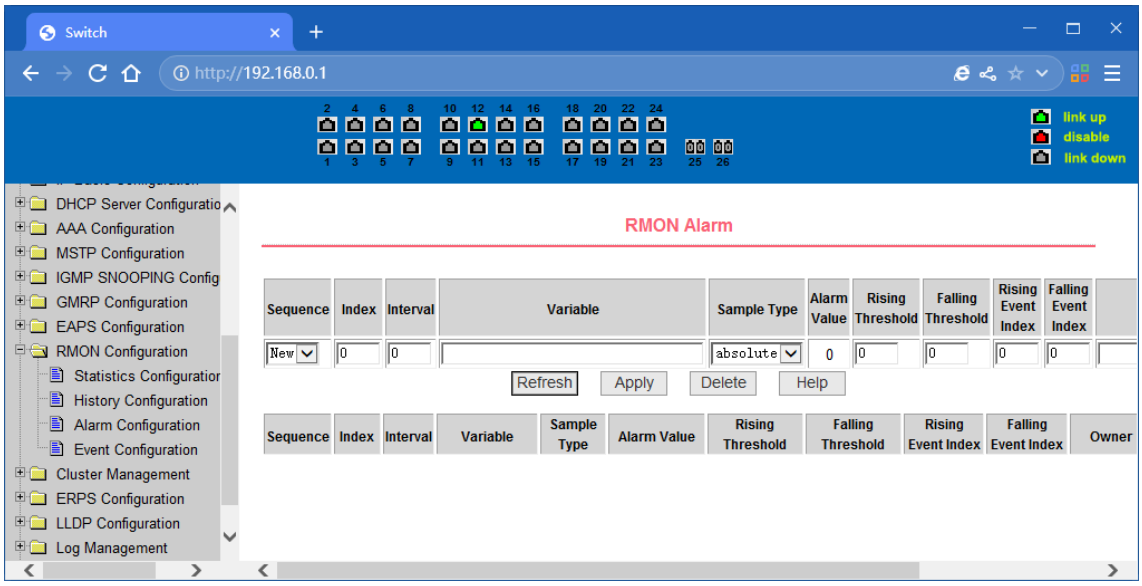
You can configure the RMON history group through this page. Select a port from the drop-down list to view/configure the RMON history group configuration for this port. When not configured, the index number is 0, fill in the correct index number (range is 1 to 100), interval, request Buckets, the owner is optional, you can configure the RMON history group for the port. Interval refers to the time interval in seconds that the data is collected. The range is 1-3600. The bucket is the allocated storage size and it indicates how many records are stored. The range is 1-100. The statistics table shows historical data that has been collected since the configuration was successful.



RMON history group configuration page

（3）RMON alarm group configuration page

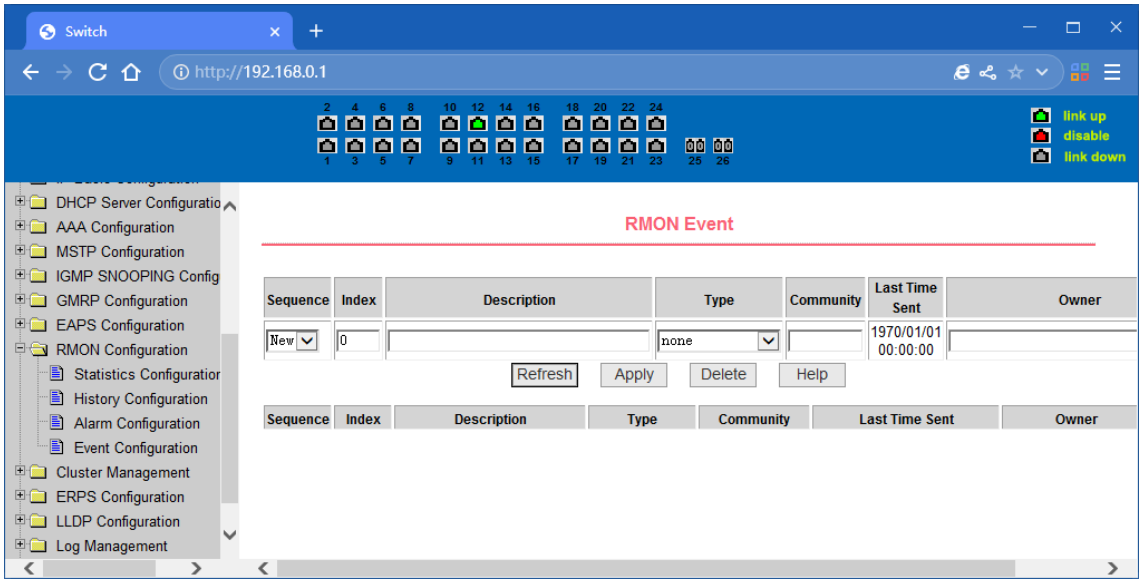
You can use this page to create or modify an RMON alarm group. Select a configured alarm group from the drop-down list to view/configure its information. Select New to create it. The index number range is from 1 to 60, and the interval range is from 1 to 3600. In seconds, the monitoring object must fill in the MIB node. The comparison method can choose absolute (absolute value) or delta (change amount). In addition, the upper and lower limit valves must be filled in. Value, event index, owner is optional. The alarm value is read-only and shows the sampled value when the alarm was last issued. The event index refers to the index number of the RMON event group and must be configured in advance.



RMON alarm group configuration page

（4）RMON event group configuration page

Users can create or modify RMON event groups through this page. Select a configured event group from the drop-down list to view/configure its information. Select New to create it. The index number range is from 1 to 60. The description is a character string. Actions can select none (no operation), log (log), snmp-trap (trap trap) or log-and-trap (log and Trap alarm), Community names do not work in this device, owners are optional. The last send time is read-only, showing the last time the event was sent.



RMON Event Group Configuration Page

4.18. Cluster configuration

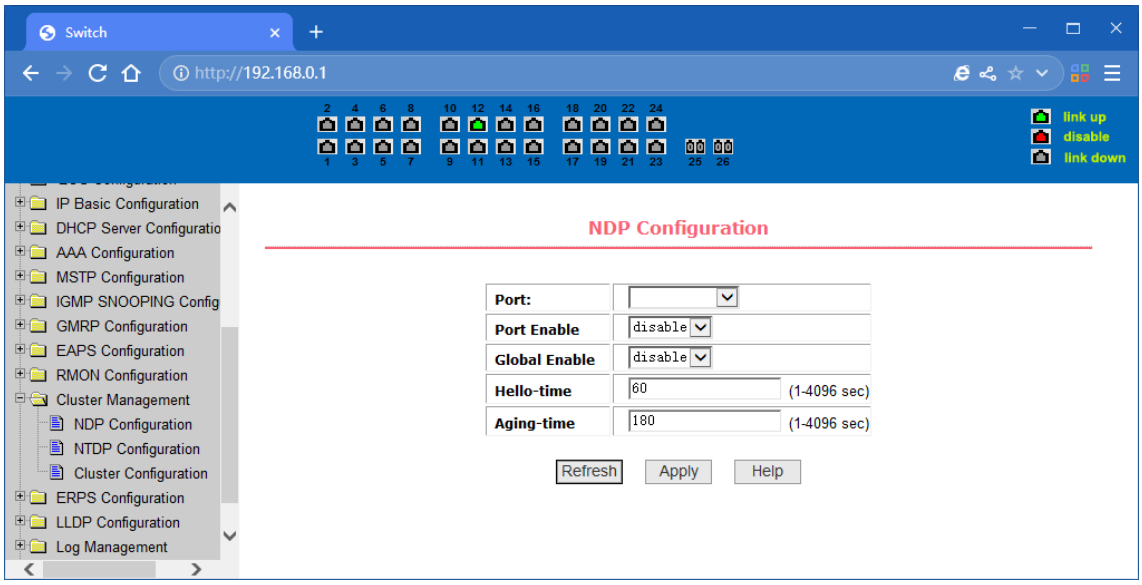
（1） NDP configuration page

You can use this page to configure NDP. The configurable information includes: selecting the port, enabling the NDP function of the port, enabling the global NDP function, the interval for sending NDP packets, and the aging time of the NDP packets on the receiving device.

For port selection, you can select the port as required and enable the port NDP function. For NDP to operate normally, both global and port NDP must be enabled at the same time.

Set the aging time of the NDP packets sent by the local device to the receiving device. The valid time range is 1-4096 seconds. The default value is 180 seconds.

Set the interval for sending NDP packets. The valid time range is 1-4096 seconds and the default is 60 seconds.



NDP configuration page

（2）NTDP configuration page

You can use this page to configure NTDP. The information that can be set includes: selecting the port, enabling the NTDP function of the port, enabling the global NTDP function, the range of the topology collection, the time interval of collecting the regular topology, the delay time of the first port forwarding the packet, and the forwarding of the packet by other ports. delay.

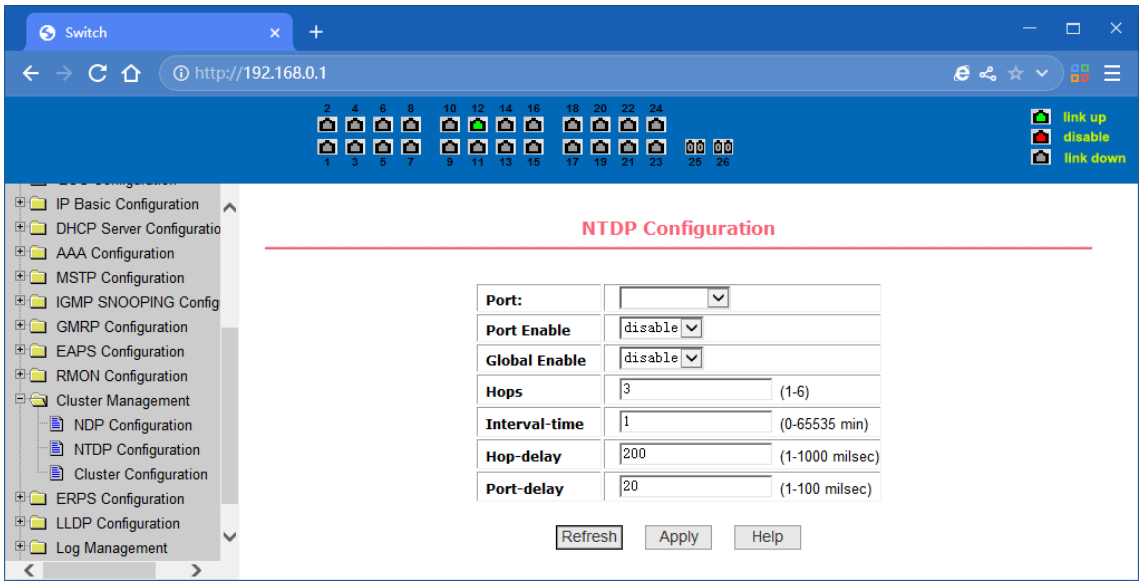
For port selection, you can select the port as required and enable the NTDP function on the port. For NTDP to operate normally, both global and port NTDP must be enabled.

The range of topology collection is configured. The valid range is 1-6. In the default configuration, the maximum number of hops from the most distant device to the topology collection device is 3.

Set the interval for collecting the topology collection. The valid range is 0-65535 minutes. The default configuration is 1 minute.

Set the delay for forwarding packets on the first port. The valid range is 1-1000 milliseconds. The default value is 200 milliseconds.

Sets the delay for forwarding packets on the first port. The valid range is 1 to 100 milliseconds. The default value is 20 milliseconds.



NTDP configuration page

（3）Cluster Configuration Page

Users can configure the cluster and view the cluster member table through this page. The information that can be set includes: enabling the cluster function, configuring the management VLAN, the address pool of the cluster, the interval for sending handshake packets, the effective retention time of the device, the name of the cluster, the way to join the cluster, and deleting the cluster.

To enable the cluster function, you must enable the cluster function before the cluster function can run normally.

Configure a management VLAN. The valid range is 1-4094. The default configuration is vlan1.

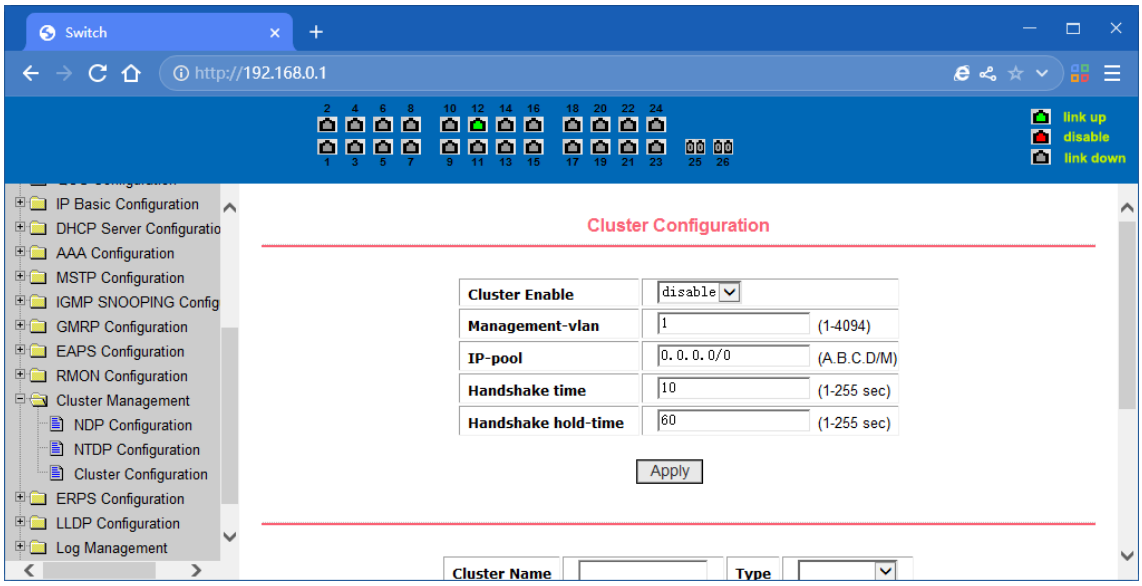
Configure a private IP address range for member devices in the cluster. The valid range of ip addresses is 0.0.0.0 to 255.255.255.255. The valid range of the mask length is 0 to 32.

Set the interval for sending handshake packets. The valid range is 1-255 seconds. The default is 10 seconds.

Configure the device's effective retention time. The valid range is 1-255 seconds and the default is 60 seconds.

To set up a cluster, you need to configure the cluster name and choose to join the cluster. There are manual and automatic joining methods. After establishing a cluster, you can automatically switch to manual, but you cannot manually switch to automatic. Manual mode can change the cluster name.

After a cluster is established, member devices and candidate devices can be viewed in the cluster member table. You can delete member devices or add candidate devices to member devices according to roles.



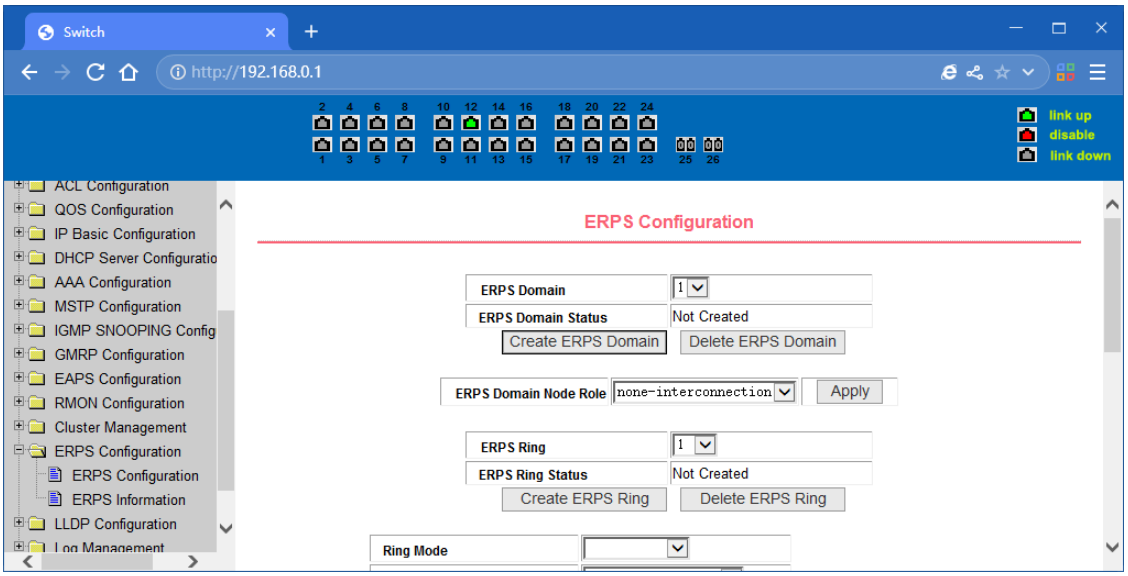
Cluster Configuration Page

4.19. ERPS configuration

（1）ERPS Configuration

This page is use to create, configure or delete ERPS domain and ring.

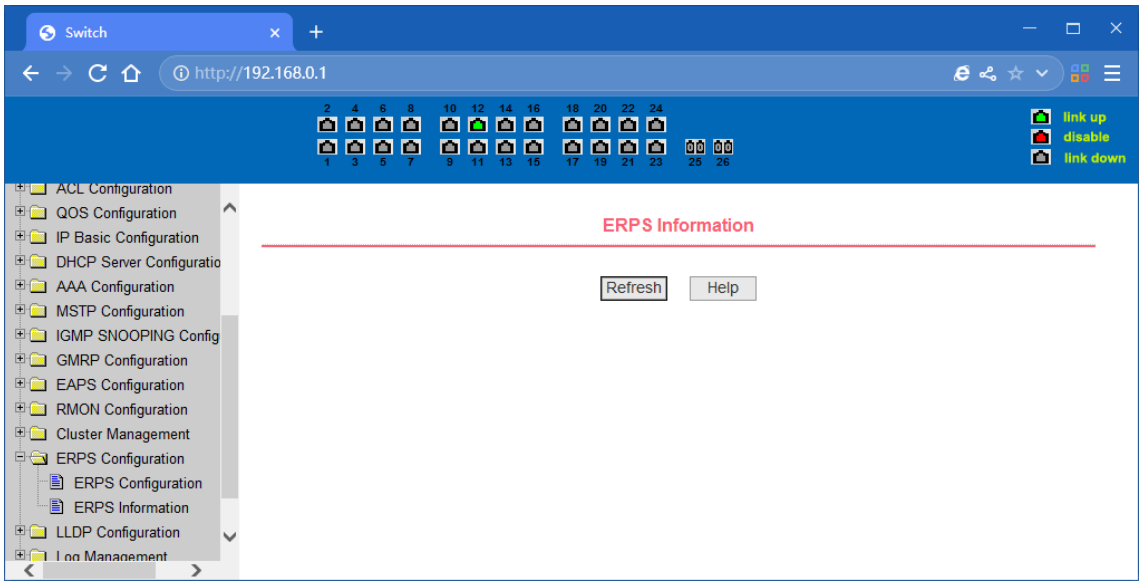
ERPS Domain	create or delete ERPS domain, domain id range is in 1-8
ERPS Domain Status	Created or not created
ERPS Domain Node Role	interconnection or none-interconnection
ERPS Ring	Ring ID range is in 1-32
ERPS Ring Status	Created or Not Created
Ring Mode	major-ring or sub-ring
Node Mode	rpl-owner-node, rpl-neighbor-node, ring-node
Raps VLAN	Configure or delete Raps VLAN<2-4094>
Traffic VLAN	Traffic VLAN<1-4094>
RPL Port	Specifies the RPL port
RL Port	Specifies the RL port
Revertive Behavior	revertive or non-revertive
Hold-off Time	Hold-off time, <0-10000>, unit: ms, the default is 0
Guard Time	Guard Time, <10-2000>, unit: ms, the default is 500
WTR Time	WTR Time, <1-12>, unit: min, the default is 5
WTB Time	WTB Time, <1-10>, unit: sec, the default is 5
Raps-send Time	Raps-send Time, <1-10>, unit: sec, the default is 5
ERPS Ring Enable	Enable or disable ERPS Ring
Forced Switch RPL and RL Port	Specifies Forced switch RPL and RL port
Manual Switch Port	Specifies Manual Switch Port



ERPS predefined configuration page

（2）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.



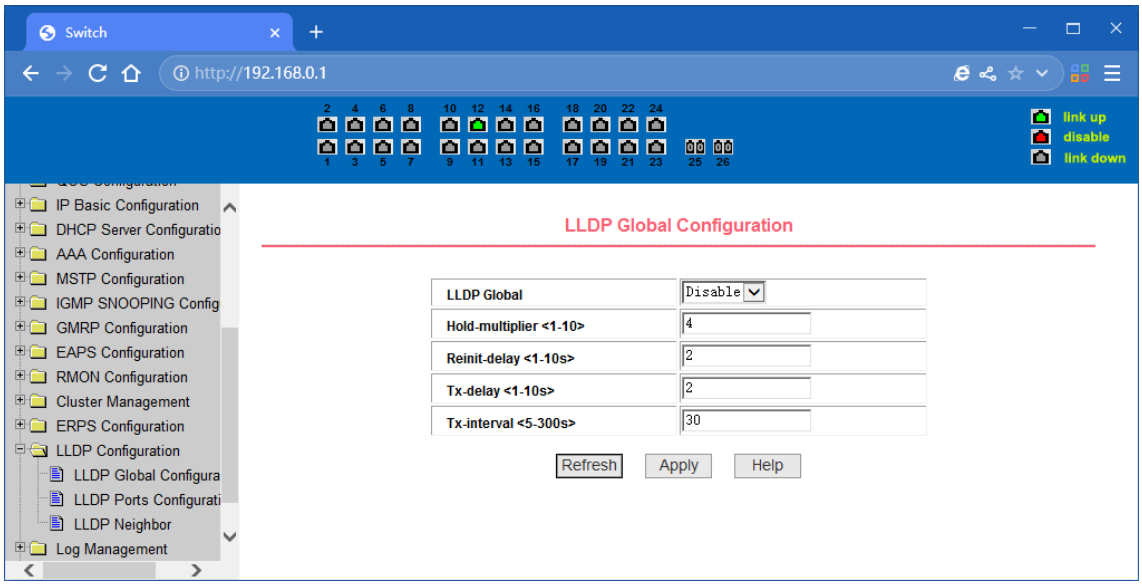
RPS information page

4.20. LLDP Global Configuration

（1）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

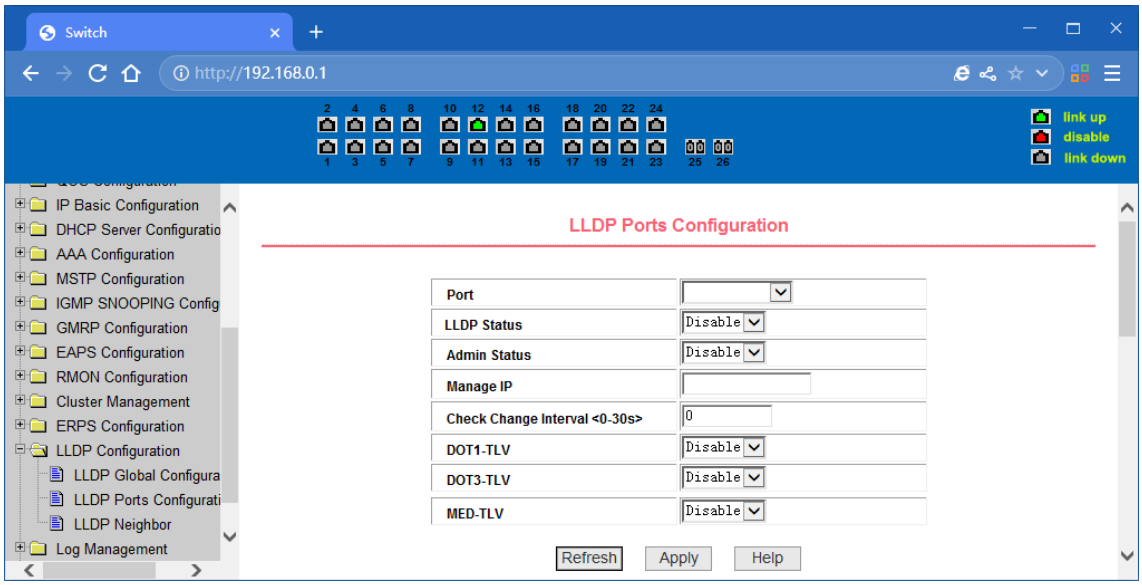


LLDP Global Configuration page

（2）LLDP Ports Configuration

This page is use to configure LLDP ports' parameters.

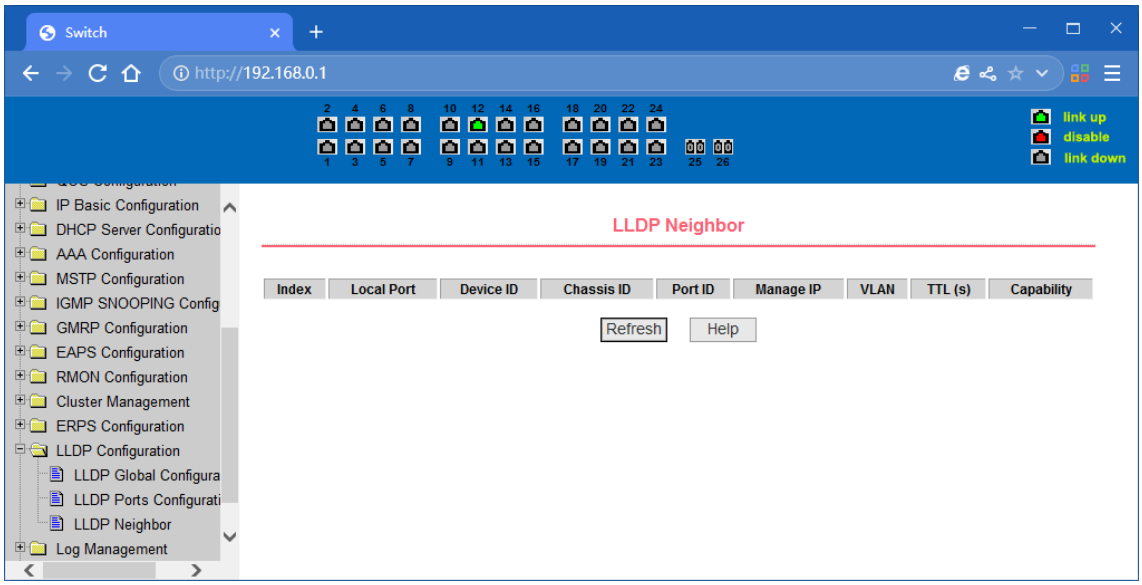
Port	Select the port to be configured
LLDP Status	Enable or disable the LLDP of the configured port, default is enabled
Admin Status	Set the admin status of the configured port, four statuses are disable, Tx, Rx and TxRx, default is TxRx
Manage IP	Set the management IP address of the configured port, use to package 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 Ports Configuration page

（3）LLDP Neighbor

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

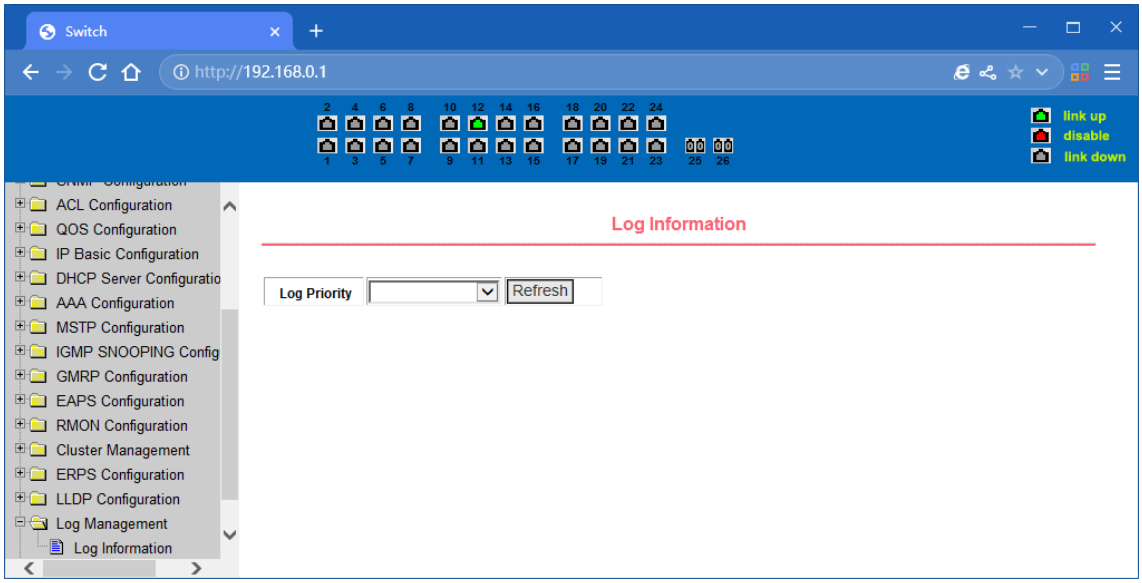


LLDP Neighbor Page

4.21. log management

（1） Log information page

Users can enable and view various log information through this page.



Log Information Page

Critical: output critical level information.

Debugging: Outputs debug level debugging information.

Informational: Output information level debugging information.

Warning: output warning level debugging information.

ALL: output all log information

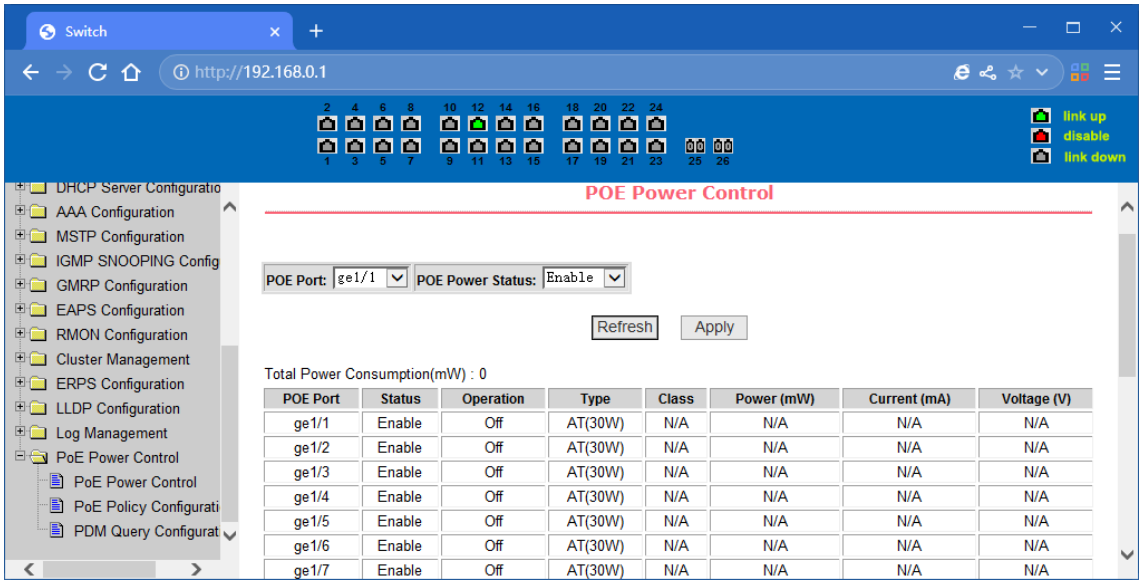
4.22. PoE port configuration

（1）PoE port Configuration Page

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

Information can be seen in the following tables:

Status： Enable means PoE function is available； Disable means PoE function is close. 2，Operation： Displays the PoE ports ON or OFF



PoE port configuration page

This is a Class A product. In home environment, this product may cause radio interference. In this case, the user may be required to take appropriate measures.

Hereby Assmann Electronic GmbH, declares that the Declaration of Conformity is part of the shipping content. If the Declaration of Conformity is missing, you can request it by post under the below mentioned manufacturer address.

www.assmann.com
Assmann Electronic GmbH
Auf dem Schüffel 3
58513 Lüdenscheid
Germany