



**DIGISOL**



**DG-GS1510PL**  
**8 PORT GIGABIT WEB MANAGED POE SWITCH**  
**WITH 2 GIGA SFP PORTS**

**User Manual**

**V1.0**  
**2019-01-18**

As our products undergo continuous development the specifications are subject to change without prior notice

# COPYRIGHT

Copyright 2019 by DIGISOL Systems Ltd. All rights reserved.

Company has an ongoing policy of upgrading its products and it may be possible that information in this document is not up-to-date.

Please check with your local distributors for latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

# Trademark

DIGISOL™ is a trademark of DIGISOL Systems Ltd. All other trademarks are the property of the respective manufacturers.

## INDEX

|  |    |
|--|----|
| Contents :.....                                | i  |
| About guide.....                               | 4  |
| Terminology / Usage.....                       | 4  |
| 1 Products introduction.....                   | 5  |
| Front panel.....                               | 5  |
| Real panel.....                                | 5  |
| 2 Hardware installation.....                   | 6  |
| First step: open a seal.....                   | 6  |
| Second step: switch installation.....          | 6  |
| Desktop or Shelf Installation.....             | 6  |
| Rack Installation.....                         | 7  |
| Third step: Plugging in the AC Power Cord..... | 7  |
| Power failure.....                             | 7  |
| 3 Getting Started.....                         | 8  |
| Management Option.....                         | 8  |
| Using Web-based Management.....                | 8  |
| Supported Web Browsers.....                    | 8  |
| Connecting to the Switch.....                  | 8  |
| Login Web-based Management.....                | 9  |
| 1.WEB page Introduction.....                   | 10 |
| 1. Logon dialog box.....                       | 10 |
| 2. Page button introduction.....               | 11 |
| 3. Entry Field.....                            | 11 |
| 4. Status Field.....                           | 12 |

---

|   |     |
|---|-----|
| 5. Main Page.....   | 13. |
| 1. System Configuration:.....   | 13  |
| 2. Port Configuration.....  | 19  |
| 3. MAC binding.....   | 26  |
| 4. MAC filtering.....   | 27  |
| 5. VLAN Configuration.....  | 29  |
| 6. SNMP Configuration.....  | 32  |
| 7. ACL Configuraion.....  | 33  |
| 8. QoS Configuration.....   | 37  |
| 9. IP Basic Configuration.....  | 38  |
| 10. Certification. Authorization. Accounting (AAA) configuration..... | 40  |
| 11. Spanning Tree Protocol configuration.....                         | 44  |
| 12. IGMP SNOOPING configuration.....                                  | 47  |
| 13. GMRP configuration.....   | 49  |
| 14. EAPS configuration.....   | 51  |
| 15. RMON configuration.....   | 52  |
| 16. Cluster configuration.....  | 54  |
| 17. log management.....   | 57  |
| 18. PoE port configuration.....                                       | 58  |

## 1. Introduction

### 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 / Usage

In this guide, the term "Switch" (first letter capitalized) refers to the Smart Switch, and "switch" (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms "switch", "bridge" and "switching hubs" interchangeably, and both are commonly accepted for Ethernet switches.



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



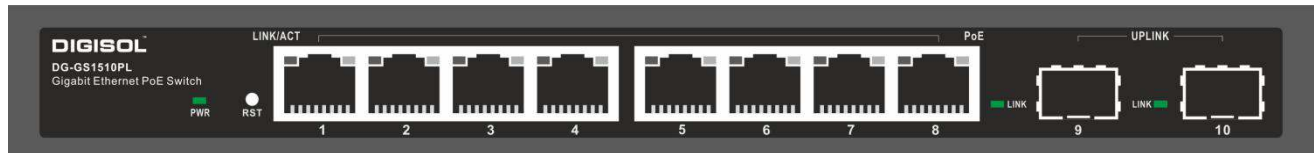
**Warning:** indicates potential property damage or personal injury.

## Products introduction

This is a Gigabit Web Managed POE Switch, It provides 8 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 small and medium-size LAN switch, also can be used as an access switch for large LAN. It can be widely used in monitoring, wireless, Internet cafe and other fields.

### 8 Port 10/100/1000Base-TX with 2 Gigabit SFP and 8 PoE L2+ Managed Switch

#### 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 will flash 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.

**RST:** By pressing the Reset button for 5 seconds the switch will change back to the default configuration and all changes will be lost.



Warning: The SFP ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

#### Real panel



**Grounding:** use specialized ground lead connect

Connect the power adapter output terminal to this port. Supports input voltages +44 ~ +57 VDC

## Hardware installation

This chapter provides unpacking and installation information for the Managed PoE switch.

### First step: 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. If any item is missing or damaged, please contact the local re-seller for replacement.

- Switch 1pcs
- AC power cord 1pcs
- Rubber feet 4pcs
- Screws 6pcs
- Mounting brackets 2pcs
- CD

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

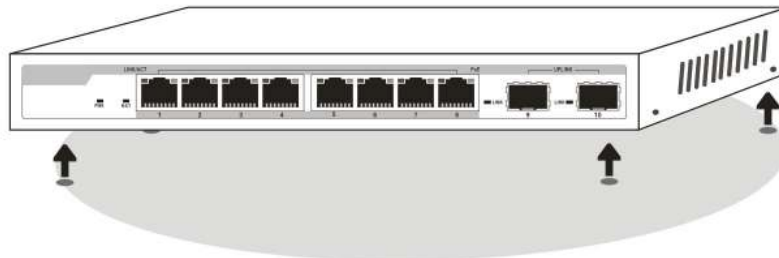
### Second step: switch installation

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

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

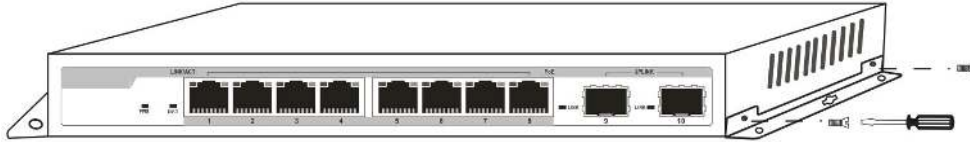
### Desktop or Shelf Installation

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.



## Rack Installation

attach the mounting brackets in 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).



## Third step: Connecting power supply

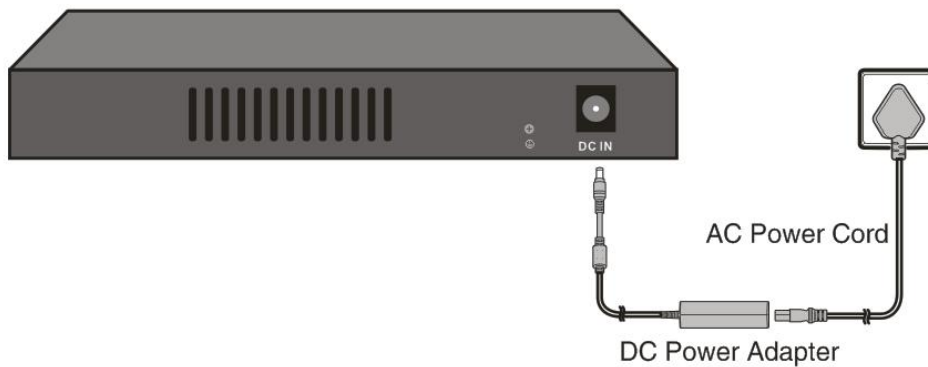
Using the AC power cord to connect to the power adapter, and then plug in output terminal of the adapter into the DC IN socket on the back of the switch. (The AC power outlet should be grounded)



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



Warning: The installation instructions clearly state that the ITE is to be connected only to PoE networks without routing to the outside plant.



## Power failure

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



### 3 Getting Started

This chapter introduces the management interface of Managed PoE switch.

#### Management Option

The Managed PoE switch can be managed through any port on the device by using the Web-based management.

Each switch must be assigned its own IP address, which is used for communication with Web-Based Management or a SNMP network manager. The PC should have an IP address in the same range as the switch.

Please refer to the following installation instructions for the Web-based Management .

#### 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.

#### 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

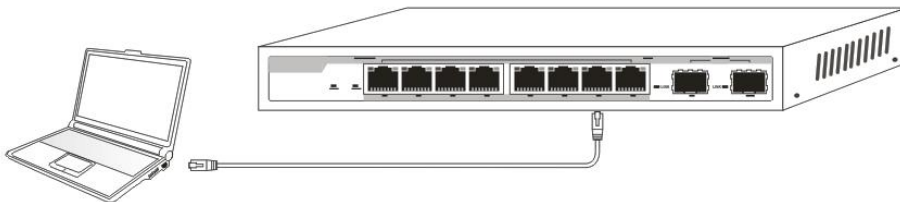
#### Connecting to the Switch

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

A PC with a RJ-45 Ethernet connection

A 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.



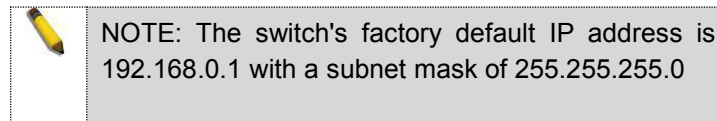
Network connection

## Login Web-based Management

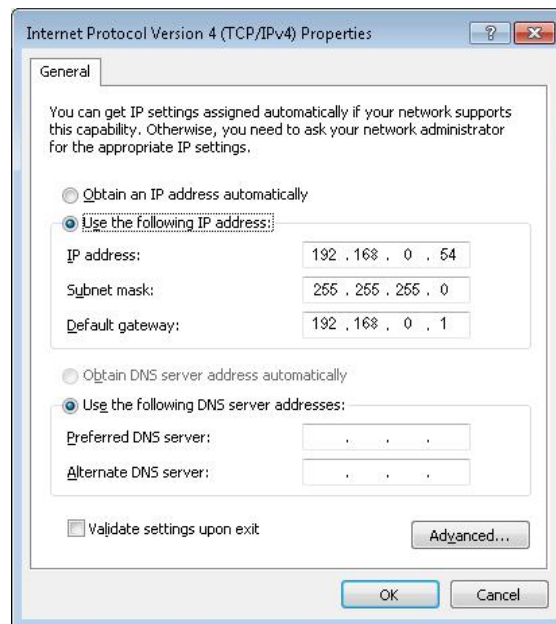
In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of 192.168.0.1, the PC should have an IP address of 192.168.0.x (where x is a number between 1 ~ 254), and a subnet mask 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



To log in to the switch, the IP address of your PC should be set in the same subnet as that of the switch. The IP address is 192.168.0.x ("x" is any number from 2 to 254). Subnet Mask is 255.255.255.0.



## 4. WEB page Introduction

### 1. Logon Dialog Box

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

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



Figure 1 WEB browsing session of the login page

Figure 1 shows the login dialog box, the login dialog box will be displayed while the user enters the web page at the first time.(default IP address is 192.168.0.1/24). When the user fills out the correct user name and password, then clicks the Enter button, can log on to the switch Web server. Passwords are case-sensitive, the anonymous user password can be a maximum of up to 16 characters, while the multi-user name and password can be set up to 11 characters. Switch switch default user name is the anonymous user name admin, default password for the anonymous user's password, the anonymous user's password is empty by default.

## 2. 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:

|         |  |
|---------|--|
| Apply   | On clicking apply the numerical value will be updated in the memory. As the error-checking is implemented by the web server, before the user selects the button there will be no error checking. |
| button  | effect   |
| Delete  | Delete the current record  |
| Help    | Open help pages, view the individual pages of the configuration instructions   |
| Refresh | Update all fields on the page  |

## 3. Entry Field

The extreme left column of the table has an entry field as shown in the Fig2. through this field user can access different rows in the table.

When you choose a line for the field, it will display the corresponding information in the first line where you can also edit the information. This line is also known as activities line. When it is loaded for the first time it shows the field new, activity line is empty.

If you want to add a new line, you 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 existing line it is necessary to select the appropriate line number of the drop down menu, accordingly you need to edit the line and press the apply button, which will display a corresponding change in the table.

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

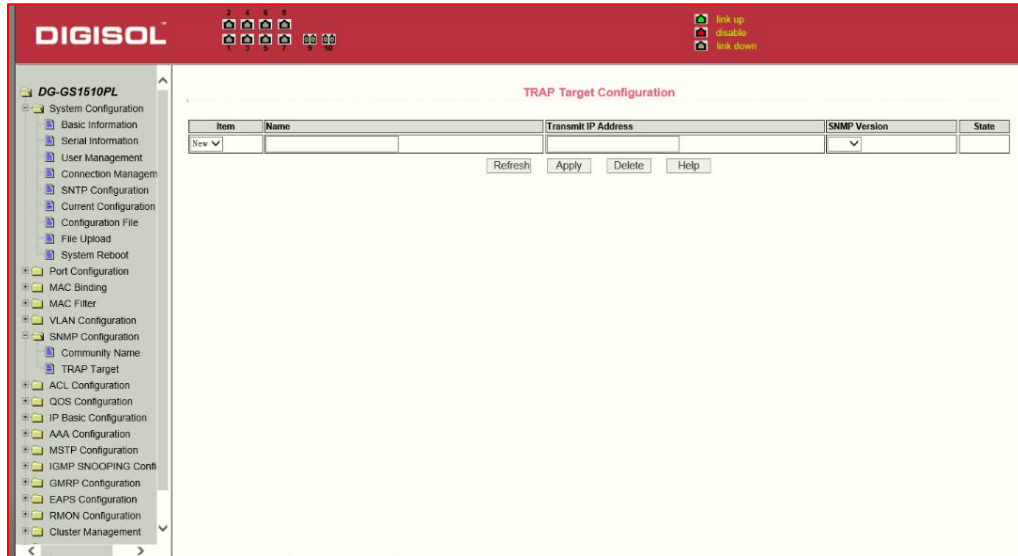


Figure 2: web page of entry field

#### 4. Status Field

As shown in Fig. 3 the state field is in the extreme right corner which displays the line status. Since all row state changes are processed in-house, so the status field is read-only. Once the information is filed it will automatically go to active state and the the status will be active. .

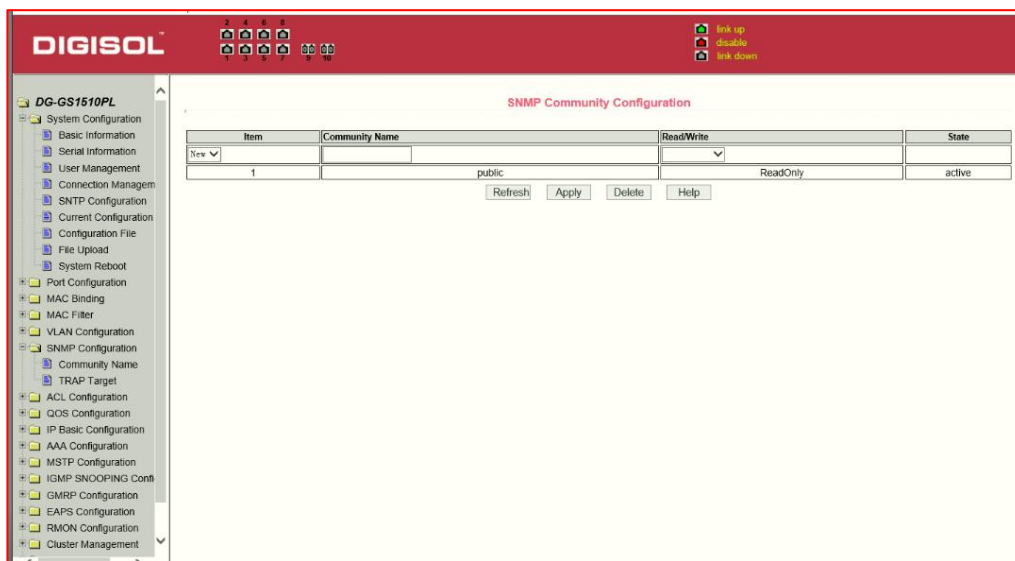


Figure 3: the web page of status field

## 5. Main Page

Figure 4 shows the WEB main page of the Switch. This page will be displayed after the user logs in web pages

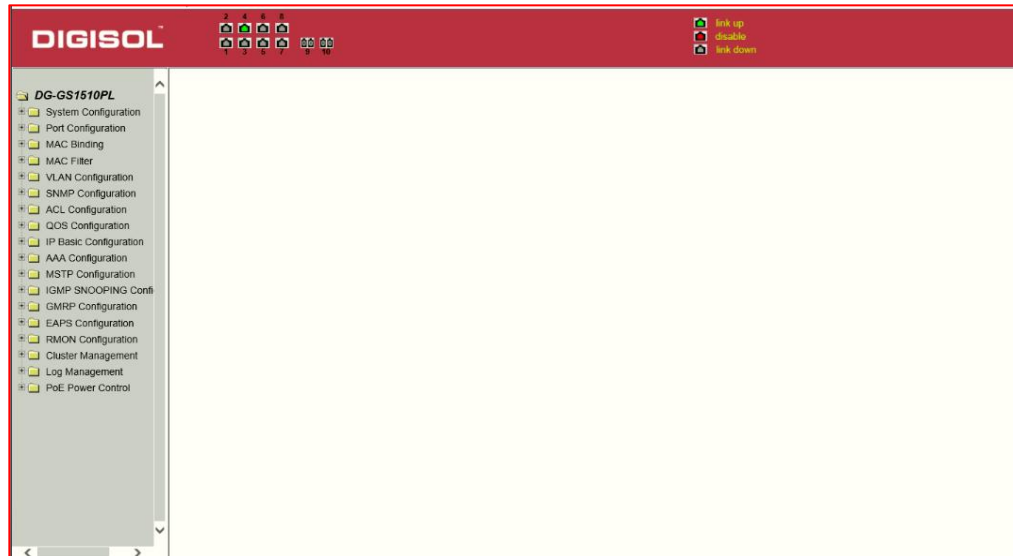


Figure 4: Switch switches main page

### 1. System Configuration:

#### (1) Basic information page

Figure 5 is the basic configuration page, users can configure the basic information for the switch.

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

System descriptor ID displays system in the network identity management.

The system version number displays the current software version number of switches. The system start-up time displays switch's time from switch start to the present time.

The system name is the switch's system name in the network, the user can modify the system name. The system location is the switch's physical location in the network, the user can modify the system location.

System Contact shows the contact person and details of the current node, the user can modify the system contact.

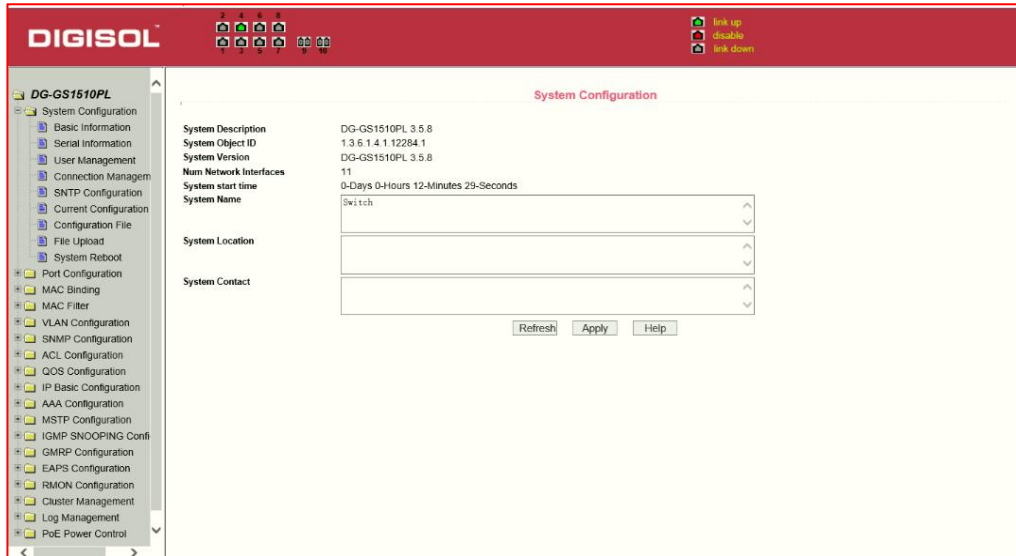


Figure 5 basic information page

## (2) Serial port information page

Figure6 is a serial port configuration page, this page displays serial baud rate and other related information. When the host, through the serial port terminals (such as Windows, Hyper Terminal), connects to switches then COM port configuration must be consistent with this page information. Figure 10 Serial port information page



Figure6 :Serial port information page

### (3) User management page

Figure 7 is a user management page, the user can modify this switch anonymous user's (admin) password. Both Telnet, console 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 apply button, the new password is activated, then if the switch is not enabled multi-user, will display the login dialog box , require the user to re - login the web page, with a new anonymous user password

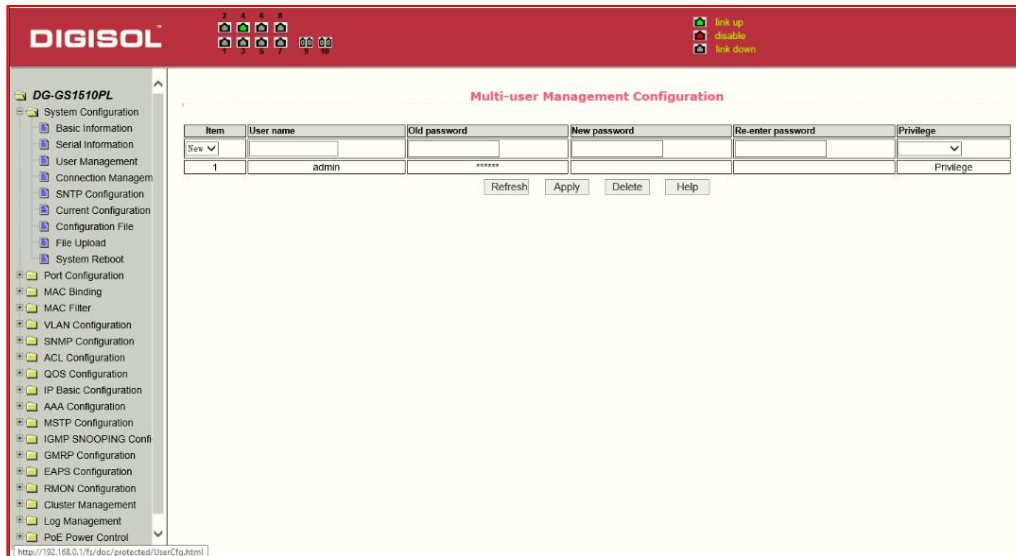


Figure 7 user's management page

### (4) Security Management Page

Figure 8 is **Security** management configuration page. Using this configuration, , the administrator can control network management services like TELNET, WEB and SNMP. You can switch on (enable) or off (disable) this service. Also these services can be mapped with standards IP ACL group ,and the implementation of the source IP address control, control access to the host of these services.

When the Switch default services TELNET, WEB and SNMP are open and no ACL filtering, then all hosts have access to the switch using these three services. If the administrator for security, does not want to provide one or more services, it can be shut down.



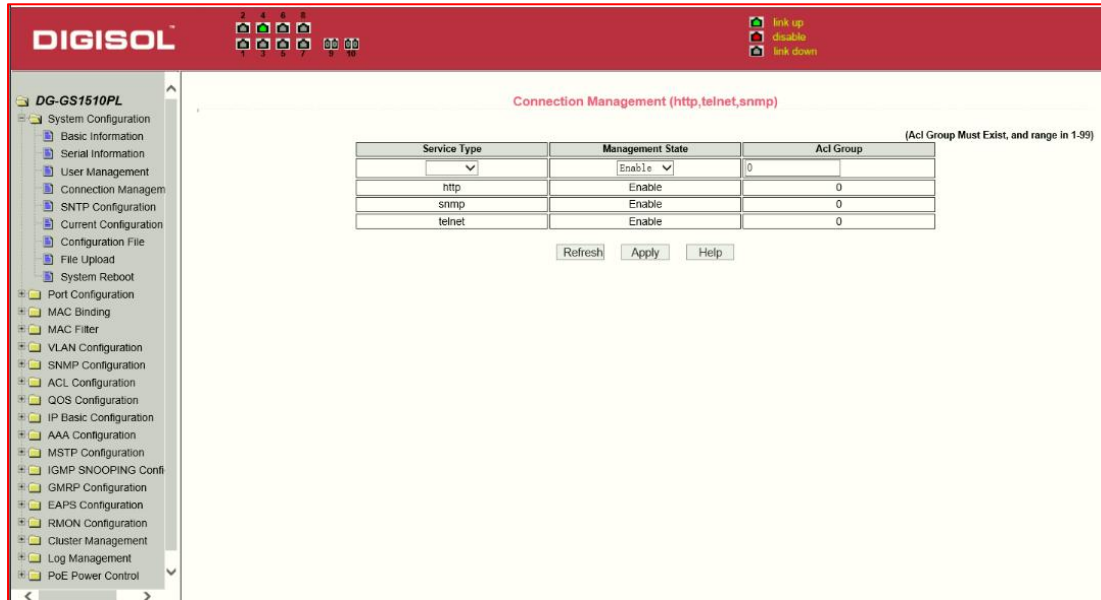


Figure 8: Security management page

### (5) Configure the current page

Figure 9 is the current configuration page. the user can view the current configuration of the switch on this page. Save button is to store the current system configuration in the configuration file. Because the storage operation requires erasing & writing into the FLASH memory, it may take up some time. When the user was configures the switch and restarts it after saving, then configurations are not lost.

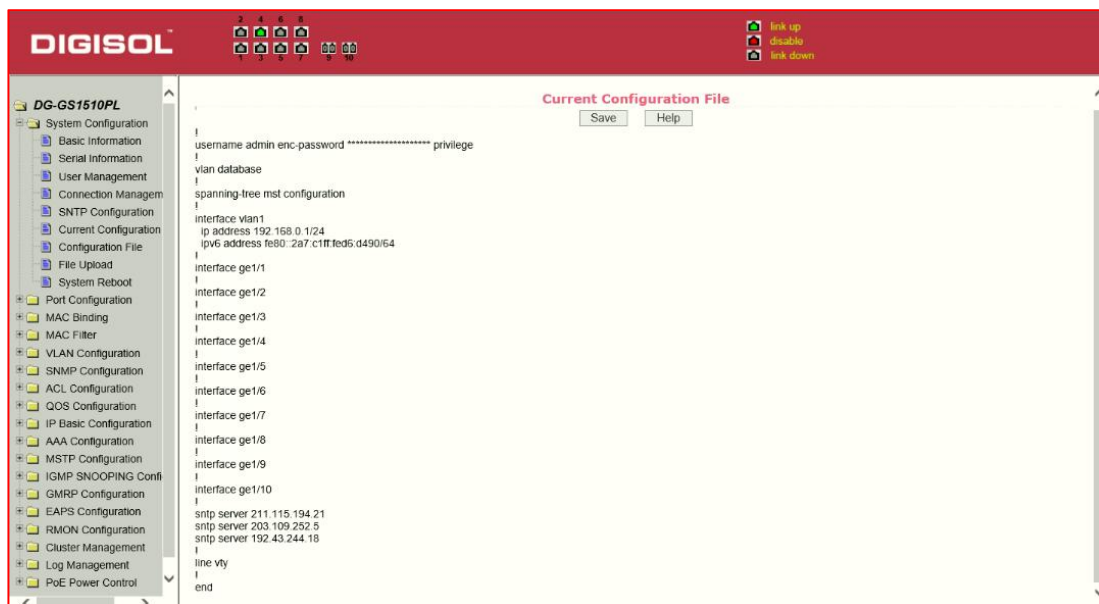


Figure 9: the current configuration page

## (6) Configuration page

Figure 10 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, users select Save and save the configuration file directory path. Download the configuration file names are as switch.cfg.

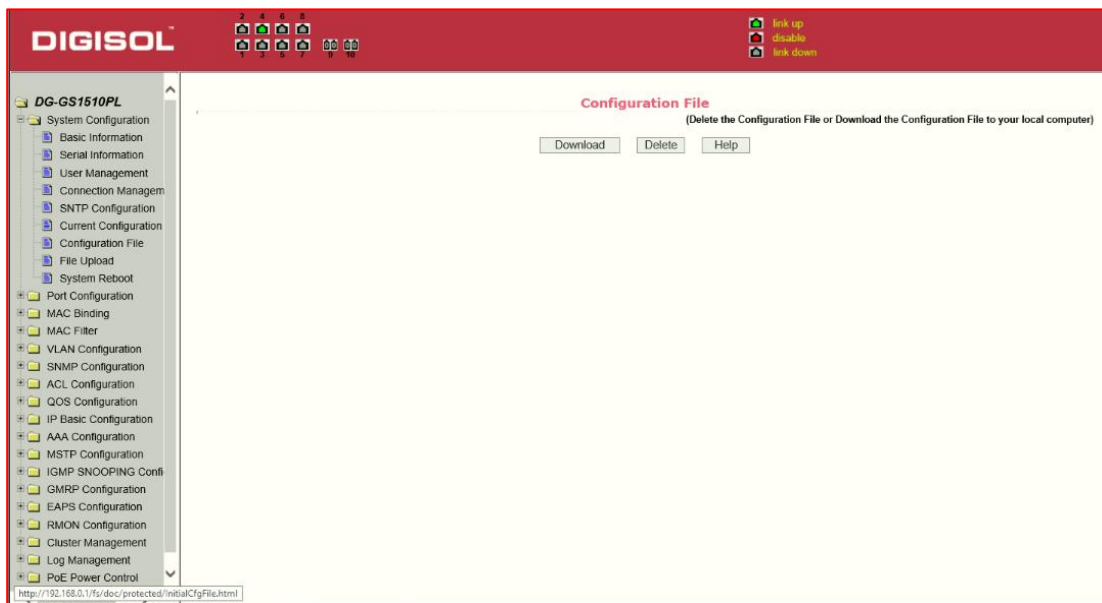


Figure10: Configuration file page

## (7) File upload page

Figure 11 is a file upload page, through this page a user can upload a configuration file and mapping files to the switch. Click the Browse button to select the upload configuration file or image file in the directory path on the PC. Click Upload button to upload a configuration file or image file, configuration file extension must be \*.cfg, image file must be provided by DIGISOL and the file name extension must be \*.img. Before the system automatically returns to the results page, please do not click on other pages, or restart the switch; otherwise, the file transfer will lead to failure causing system crash

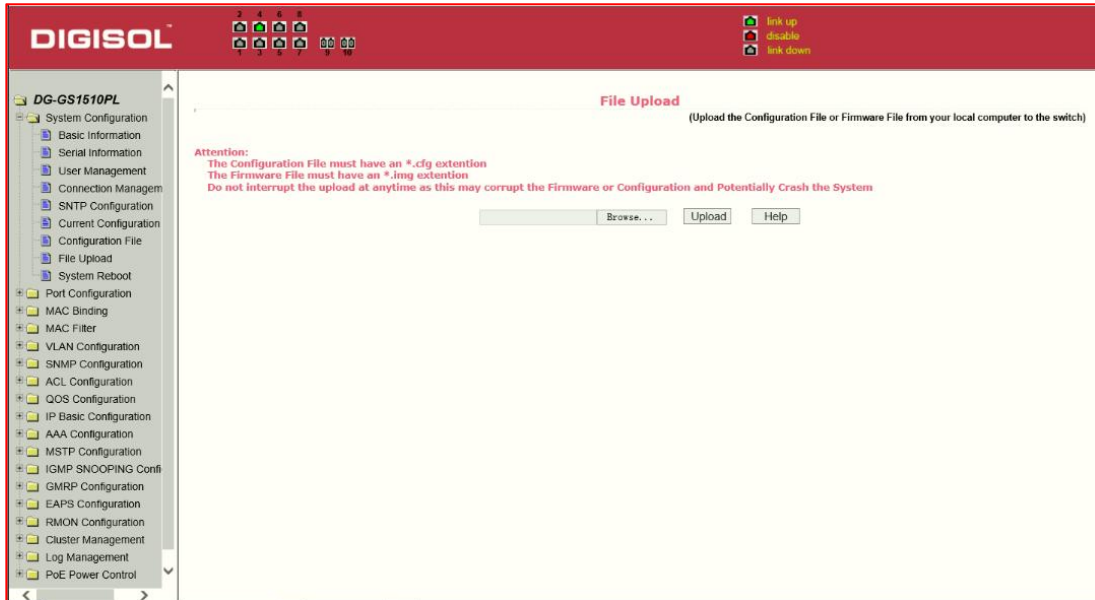


Figure11 File Upload Page

### (8) System reset page

Figure 12. is system reset page. Through this page, users can restart the switch. When you click on Restart button, it will pop up a dialog box that prompts the user to determine whether to restart the switch.

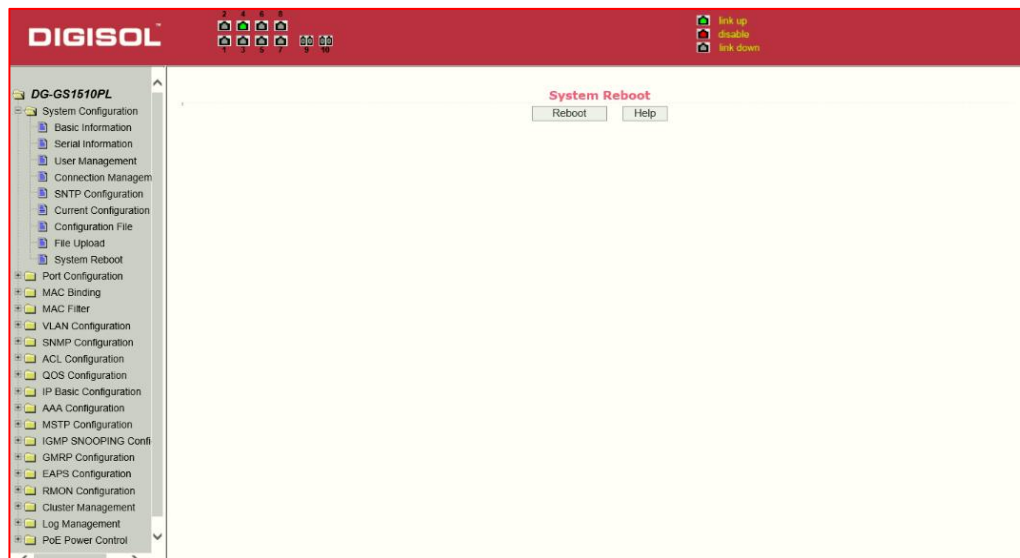


Figure12 System reset page

## 2. Port Configuration

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

Figure 13 is the port configuration page. Users can enable or disable the port, set the port speed, or View basic information of all ports.

To set a specific port, users need to select the appropriate port name from port drop-down menu,. The default port status is up. The drop-down menu can select “down” to disable the port. Users can also choose to set the speed from drop-down menu to set the speed of the port, On this page the user can also view the port’s other basic information

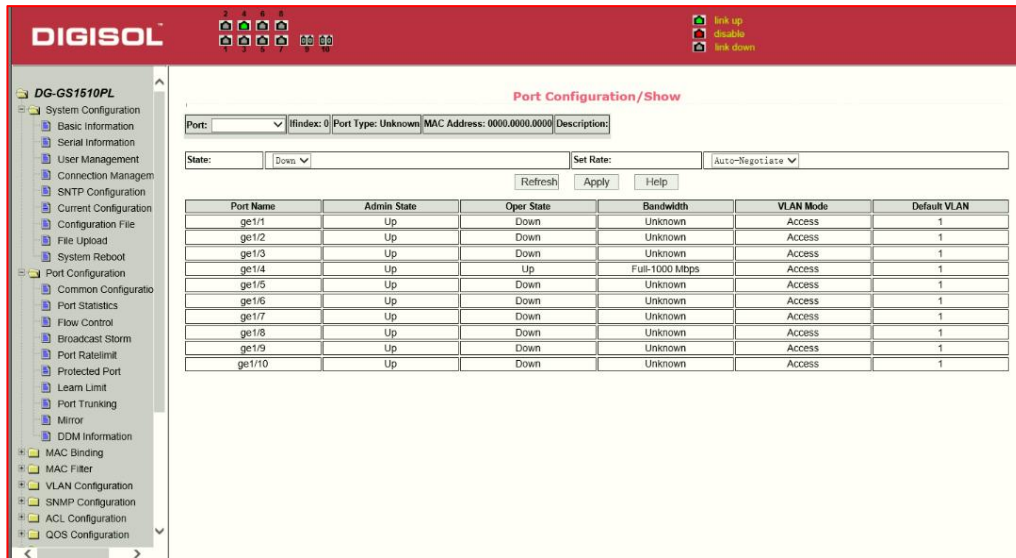


Figure 13: port configuration and port - display page

### (2) Port Statistics Page

Figure 14 is the port statistics information page. To view a particular port, users need to select the appropriate port name in the port drop-down menu. Users can view the statistics information of send and receive packets on this page.

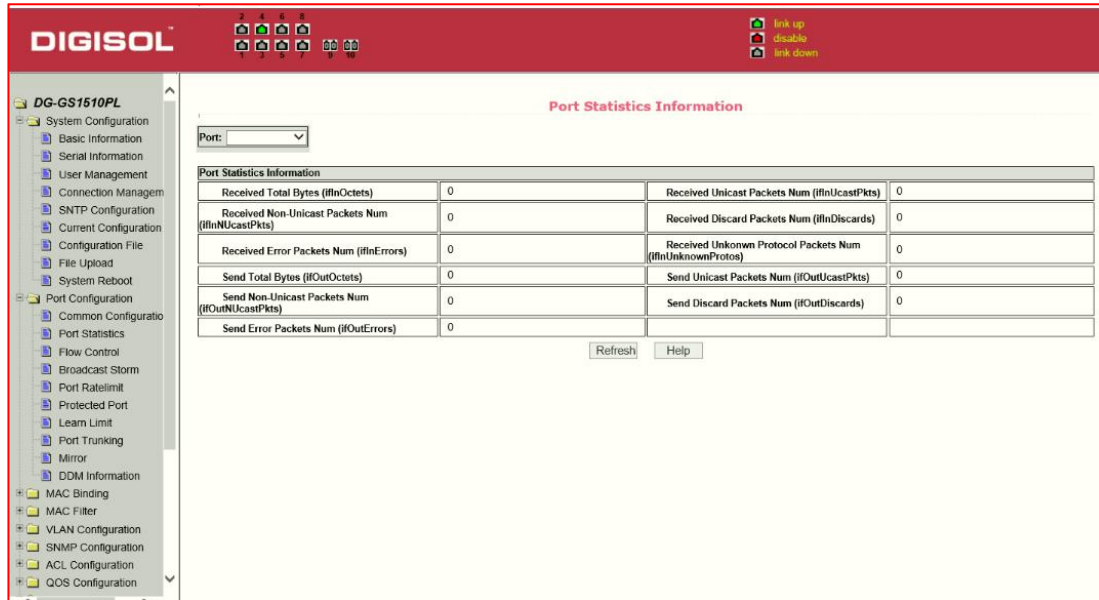


Figure 14 Port Statistics Page

### 3) Flow control page

Figure 15 is the flow control page. Users can enable and disable each port's send and receive flow control through this page.

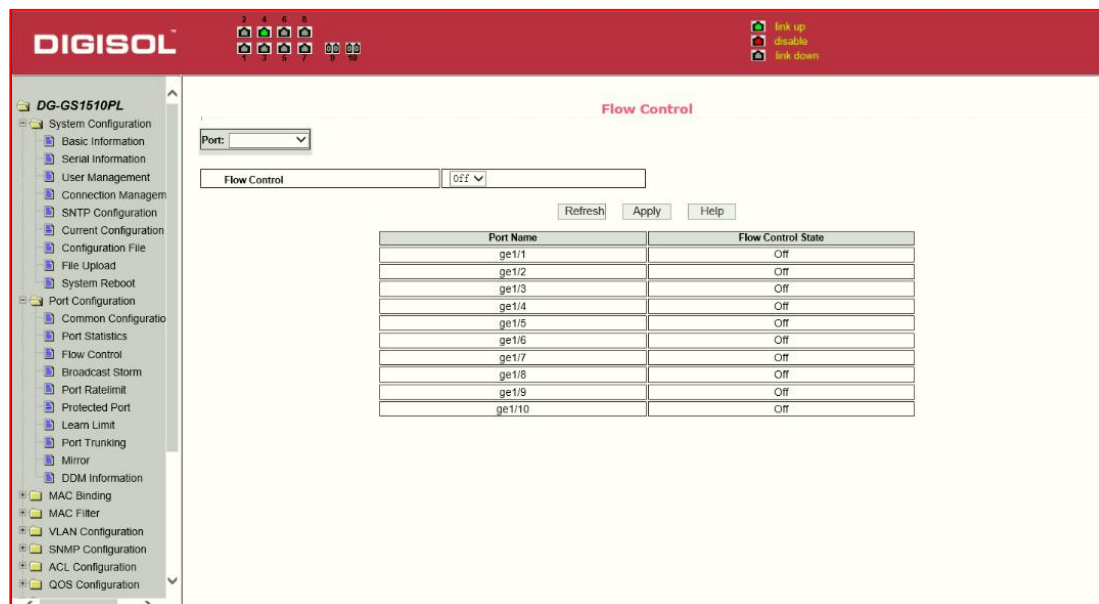


Figure 15 Flow control page

#### 4) Broadcast storm control page

Figure 16 is the Broadcast Storm Control page. This page is used to do the suppression for configure port broadcast packets, multicast packets and DLF packet.

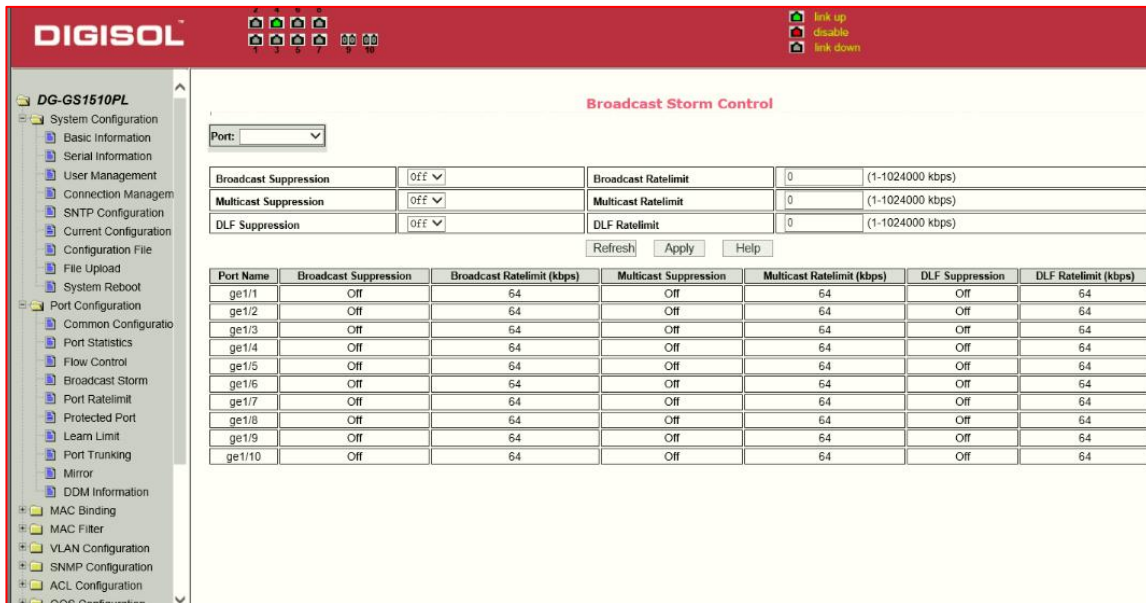


Figure 16 Broadcast Storm control Page

#### (5) Port speed limits page

Figure 17 is the port speed- limit page. This page is used to configure the port’s transmit and receive rate.

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

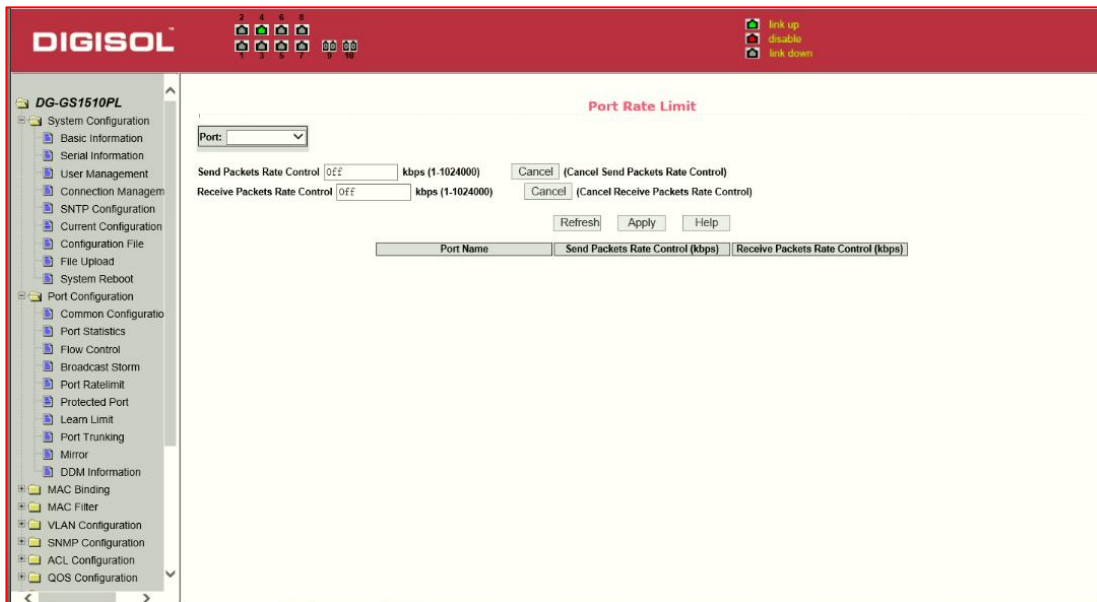


Figure 17 Port speed limit page

## (6) Port protection page

Figure 18 is the Port protection page. This page is used to configure the port for the protection port. If the port is configured as a protected port, the ports cannot exchange data with other Protected port.

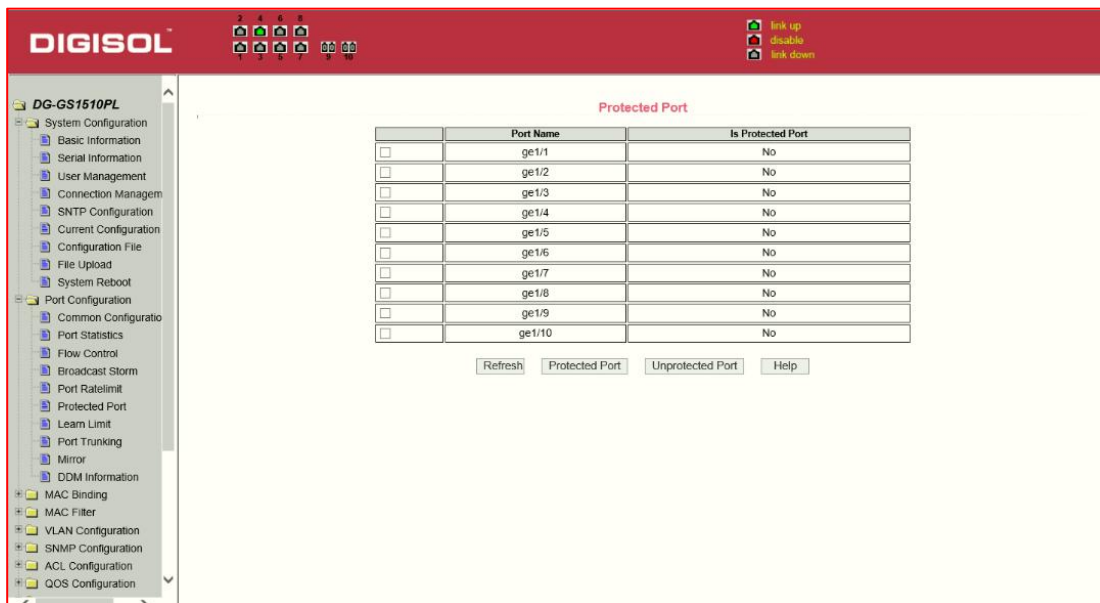


Figure 18 protected port page

### (1) Port Learning restrict page

Figure 19 is the port learning restrict page. This page is used to restrict the number of MAC addresses a port can learn. The range is 0-8191. The default value is 8191, also is the maximum that the port is not configured the restrict learning.

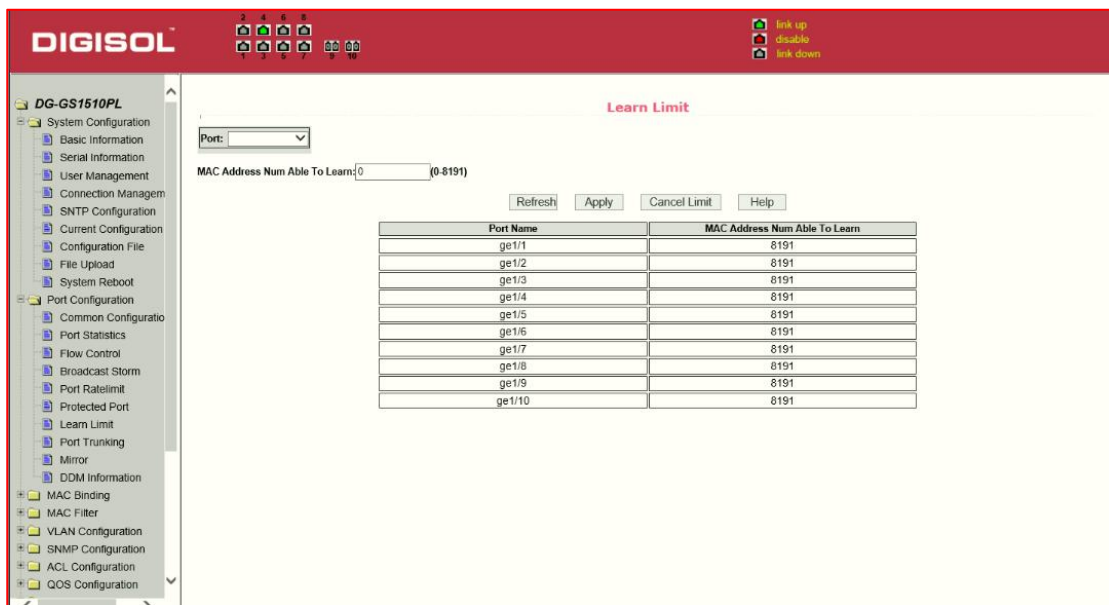


Figure 19 Port Learning restrain page

### 8) Port Trunking configuration page

Figure 20 is the port trunking configuration page,. This page allows the user to configure the port trunking. This page consists of four parts: Port trunking ID selection, Port trunking method selection, Configurable ports and group members port.



To create or modify the port trunking, the user need to select a port trunking ID, port trunking ID from 1 to 3. The user clicks the list box the appropriate port trunking ID, the port trunking of information is 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, if 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 ; You can only delete the Trunk group when it doesn't have any member ports.

Switch supports maximum 3 groups port trunking. Trunk1 and Trunk2 can not used for trunking Gigabit ports, and each group can be aggregated up to the four same attributes port. Trunk3 can only aggregate Gigabit ports, and up to 2 Gigabit ports can be aggregated. Port aggregation method is common to all of the Trunk.

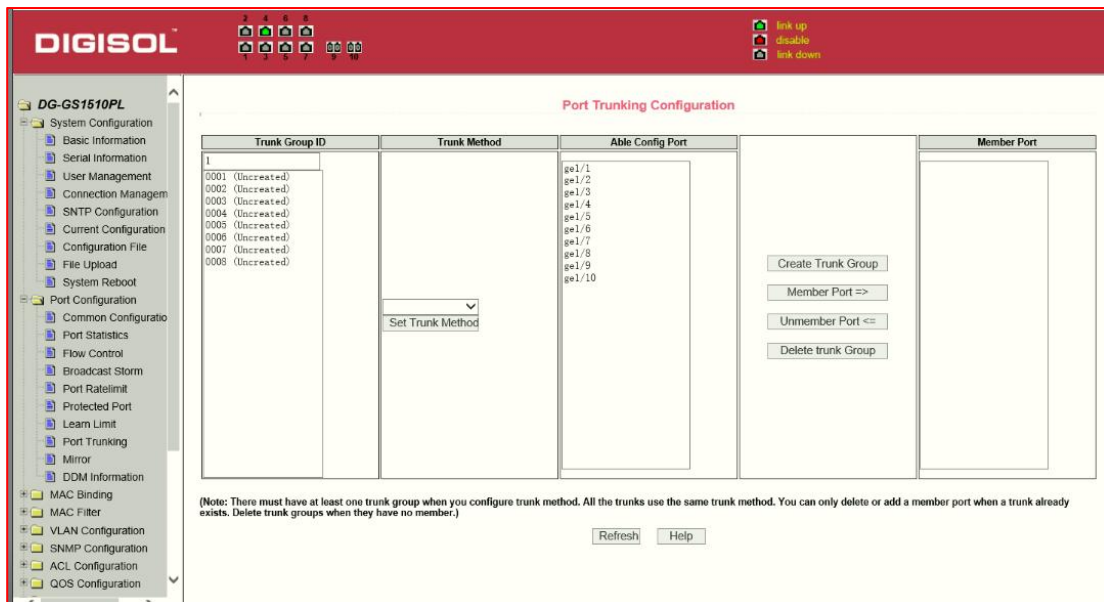


Figure 20 Port Trunking configuration page

### (9) Port mirroring configuration page

Figure 21 is the port mirroring configuration page. This page allows users to configure port mirroring. Port mirroring through the mirror port is used to monitor the data packets of port. Mirroring Port can only choose one, being mirrored output port and being mirrored(monitor port) port can select multiple. This page consists of four components: monitor port, configurable port, monitoring direction and mirror configuration information.

When you start to configure a mirror port ,firstly configured mirroring port from monitor ports, mirror ports can only have one, and then select the mirror port from the configurable port, select the monitor direction, and

press the application key to entry into force, the results is displayed in the mirrored configuration information.

When you choose the RECEIVE direction of monitoring, received data packets will be monitored, TRANSMIT, sent data packets will be monitored.You can use BOTH to monitor all sent and received packets, NOT\_RECEIVE to cancel monitoring received data packets, NOT\_TRANSMIT to cancel monitoring send data packets, while NEITHER cancels monitor data packets received and sent, that is canceling port monitoring.

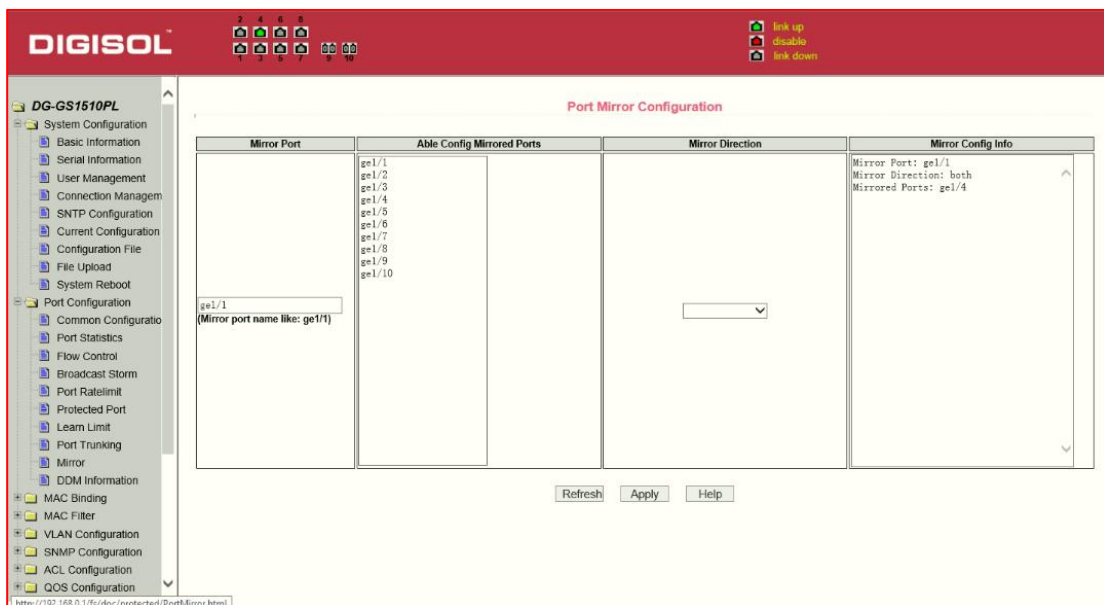


Figure21 Port mirroring configuration page

### 3. MAC binding

#### (1) MAC binding configuration page

Figure 22 is the MAC binding configuration page. This page is used to achieve the port and MAC address binding.

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

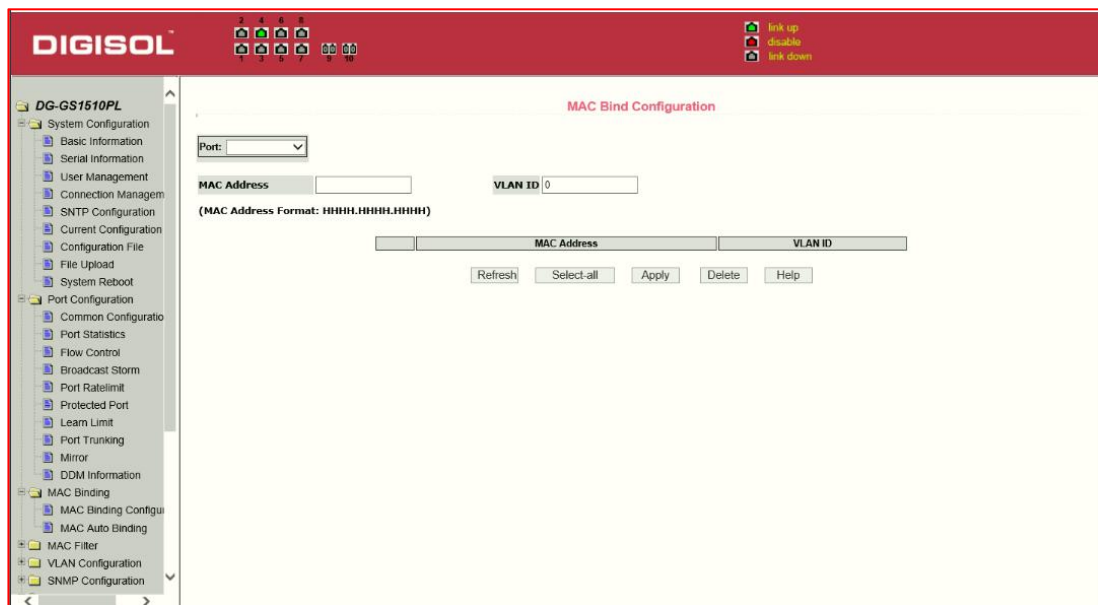


Figure 22 the MAC binding configuration page

#### (2) MAC binding automatic conversion page

Figure 23 is the MAC binding automatic conversion page. This page is used to achieve the port MAC address auto-binding.

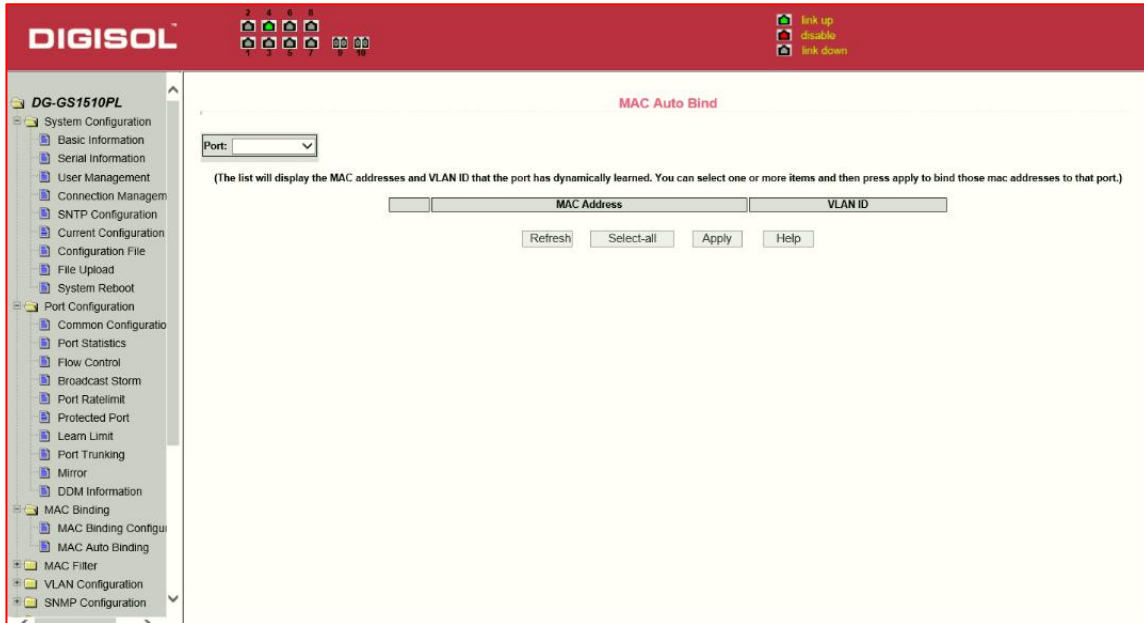


Figure 23 the MAC binding automatic conversion page

## 4. MAC filtering

### (1) MAC filtering configuration page

Figure 24 is the MAC filtering configuration page. This page is used to configure MAC address filtering on the ports.

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

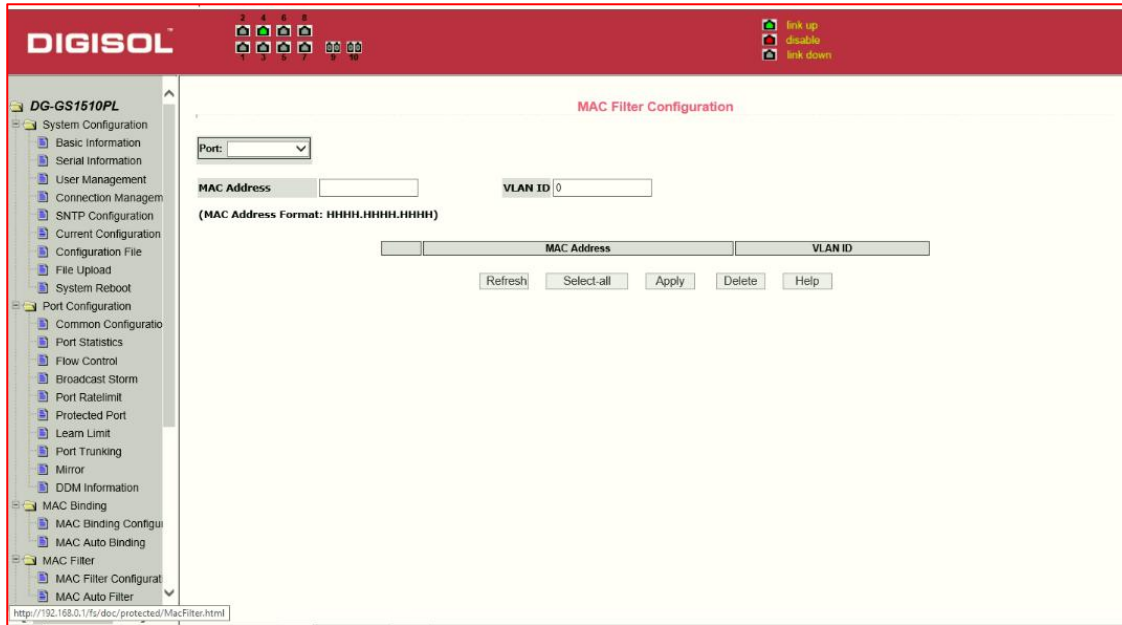


Figure 24 the MAC filtering configuration page

## (2) MAC filtering automatic conversion page

Figure 25 is the MAC filtering automatic conversion page. This page is used to achieve the port MAC address auto-binding.

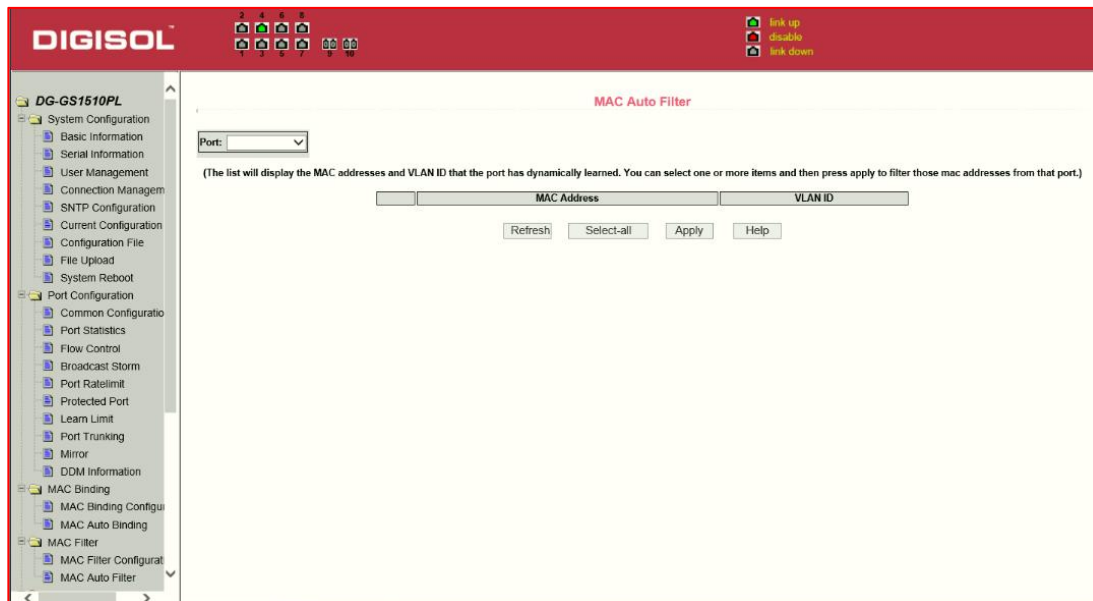


Figure 25 the MAC filtering automatic conversion page

## 5. VLAN Configuration

### (1) VLAN information page

Figure 26 shows the current VLAN information page. This page is read-only page displays the current VLAN configuration information, including the VID, state and port members. Select VLAN from the drop-down VID, shows the port information of the Port VLAN members.

A port may not be a member of VLAN, which can be VLAN-tagged or untagged members . 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

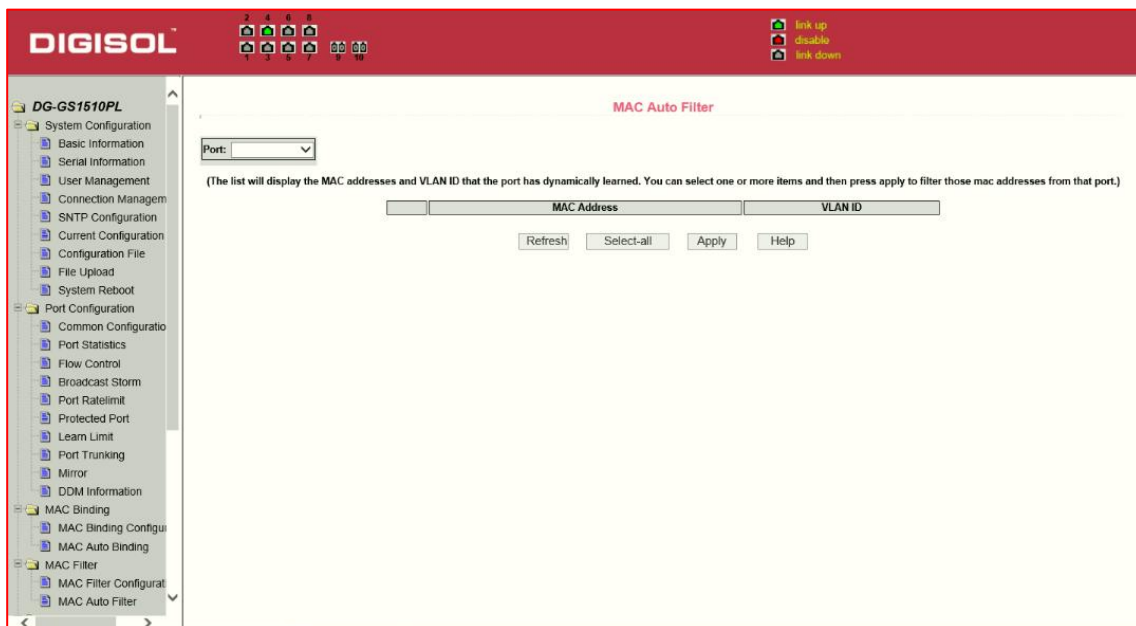


Figure 26: VLAN information page

## (2) Static VLAN configuration page

Figure 27 is the static VLAN configuration page that allows users to create VLAN.

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

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

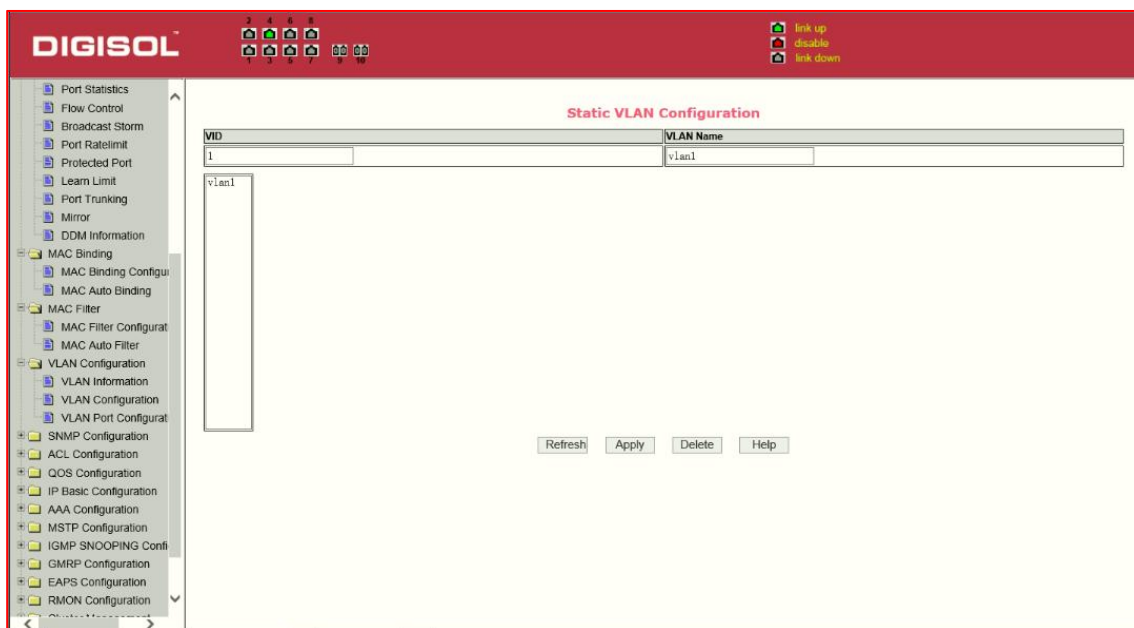


Figure 27: the static VLAN configuration page

### 3) VLAN port configuration page

Figure 28 is a VLAN port configuration page, which is used to configure the VLAN port configuration and display results. This page mainly consists of eight parts: port, mode, all current VLAN, port-owned VLAN, key "default VLAN =>," "tagged =>," "untagged =>" and "non-members" =. "

The port default VLAN is the untagged member of VLAN1, the port's default VLAN is 1.

In VLAN mode HYBRID the port default VLAN is the untagged member of VLAN1, the port's default VLAN is 1. In VLAN mode TRUNK the default is VLAN1.

VLAN Port 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 =>" is used to configure port to new default VLAN.

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

Button "untagged =>" Configured VLAN port is a designated member of the untagged. One or more VLAN from the current all VLAN can be selected.

Button "non-members" is to delete the port from the specified one or more of the VLAN.

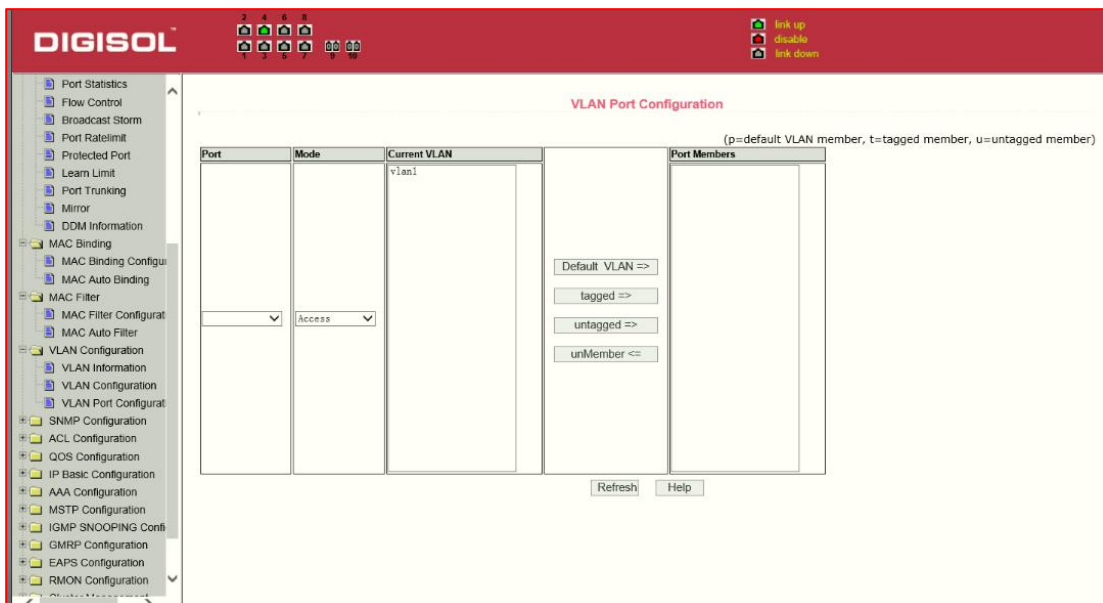


Figure 28 The VLAN port configuration page



## 6. SNMP Configuration

### (1) SNMP share body configuration page

Figure 29 is a shared body of SNMP configuration page that allows users to configure the switch common body name and read and write access, A total of 8 entries can be configured

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

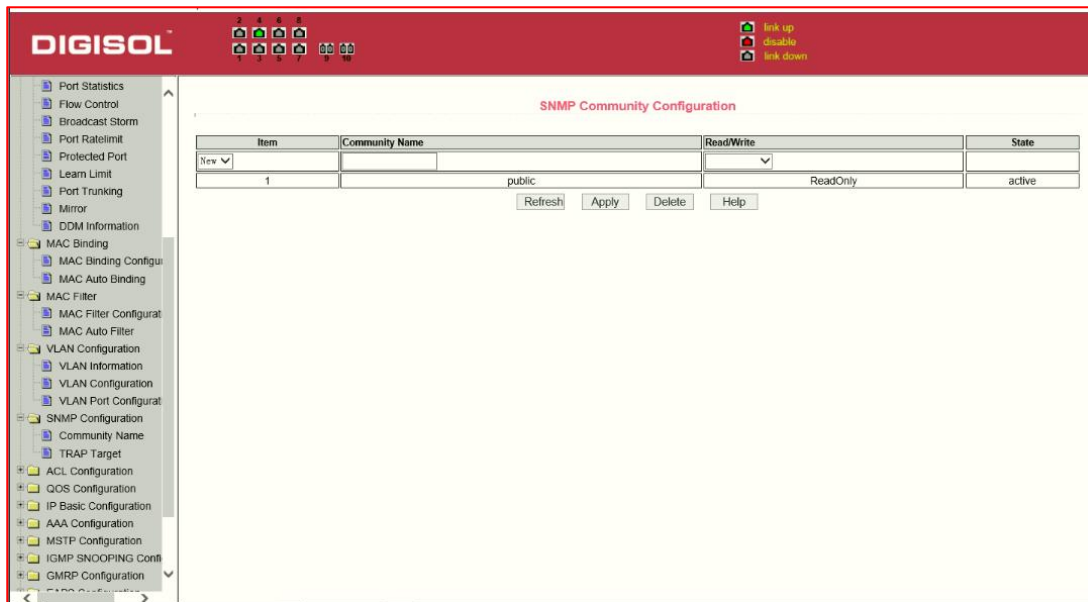


Figure 29 a shared body of SNMP configuration page

### (2) TRAP target configuration page

Figure 30 is the TRAP target configuration page that allows users to configure the workstation to receive TRAP messages as well as the IP address of TRAP protocol packets of some of the parameters.

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

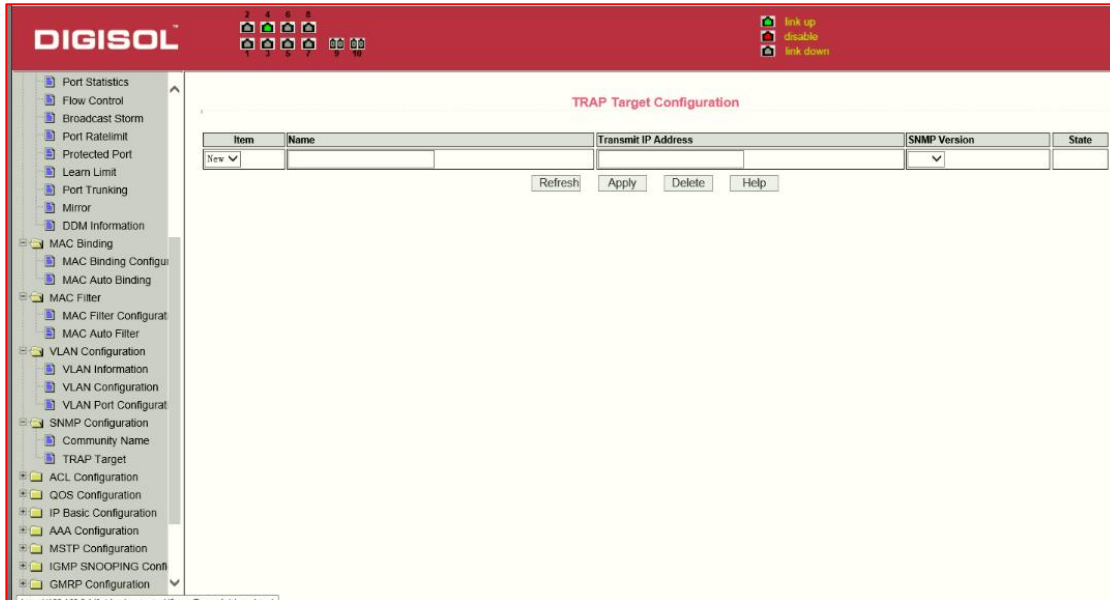


Figure 30 the TRAP target configuration page

## 7. ACL Configuration

### (1) IP Standard ACL configuration page

Figure 31 is the IP standard ACL configuration page. Users build ACL standard IP access list using this page. . User can select a ACL group number, in the group to create one or more rules. A rule can match only the source IP address field (with mask).

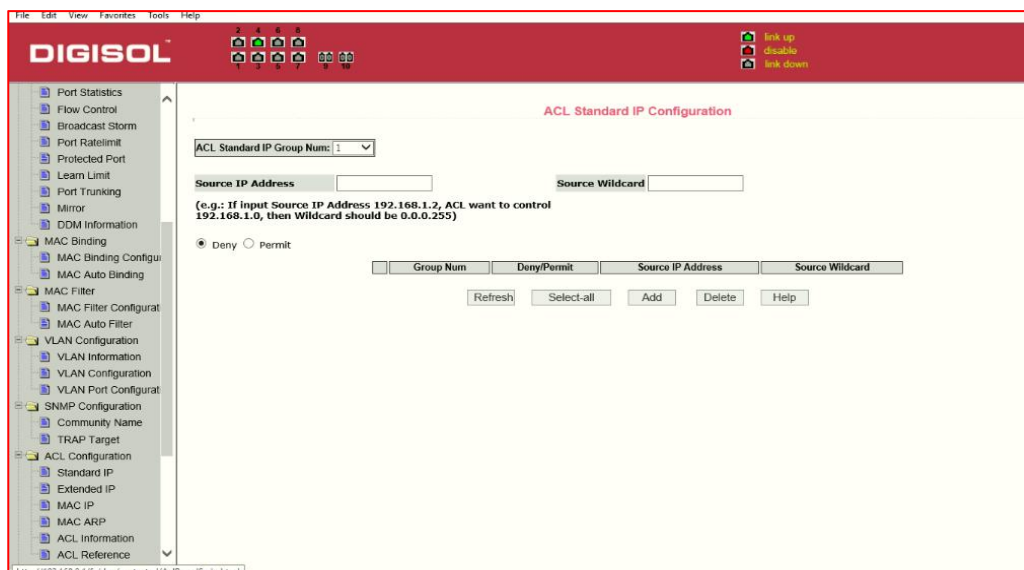


Figure 31 the IP standard ACL configuration page

The addressing method used wild-mask. If the rule were to match the IP address range 192.168.0.0 to 192.168.0.255, then the IP address can be 192.168.0.1, and its mask of 0.0.0.255.

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

The user to create a rule in the group, the system will automatically give a rule number..

## (2) IP Extended ACL configuration page

Figure 32 is the IP extended ACL configuration page. The extended IP group is an extension of the standard IP rules. Control the packet forwarding via source IP, Destination IP, IP protocol type and service port.

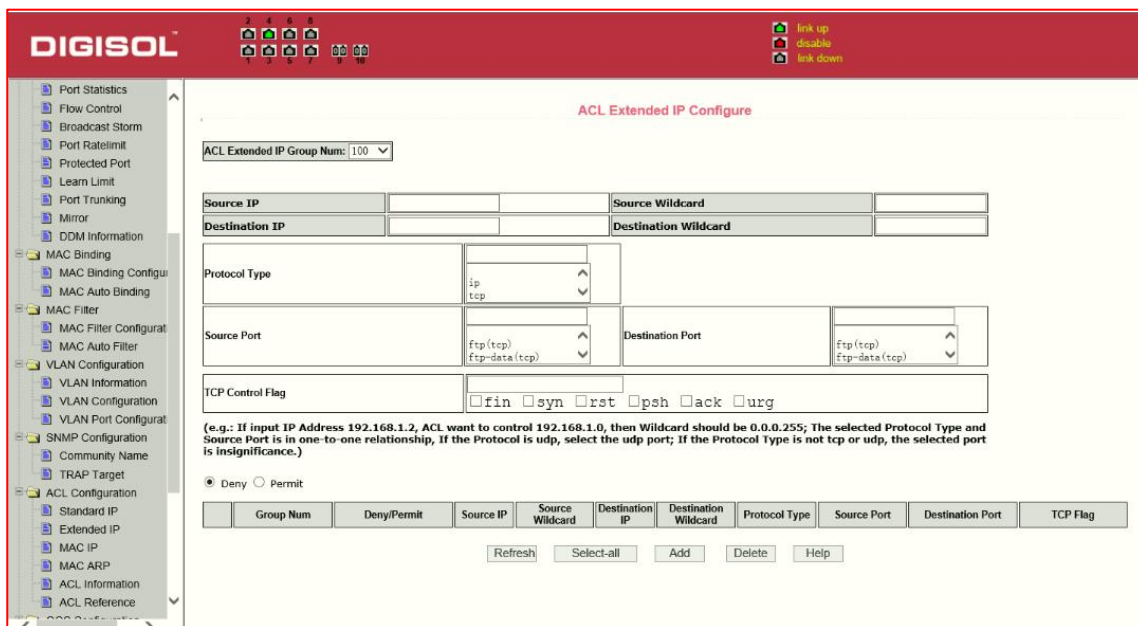


Figure 32: the IP Extended ACL configuration page

### (3) MAC IP ACL configuration page

Figure 33 is the MAC IP ACL configuration page. IP MAC group can be the IP packet source and destination MAC address and source and destination IP address control.

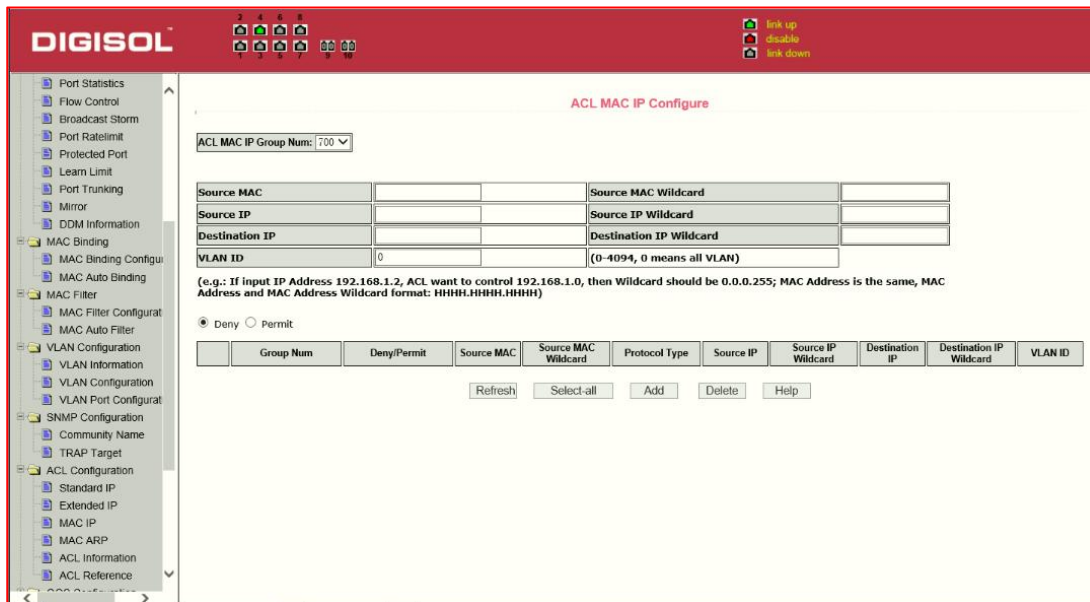


Figure 33 : the MAC IP ACL configuration page.

### (4) MAC ARP ACL configuration page

Figure 34 is the MAC ARP ACL configuration page. ARP group can be the type of the operation of the ARP packet, the sender MAC and the sender IP control.

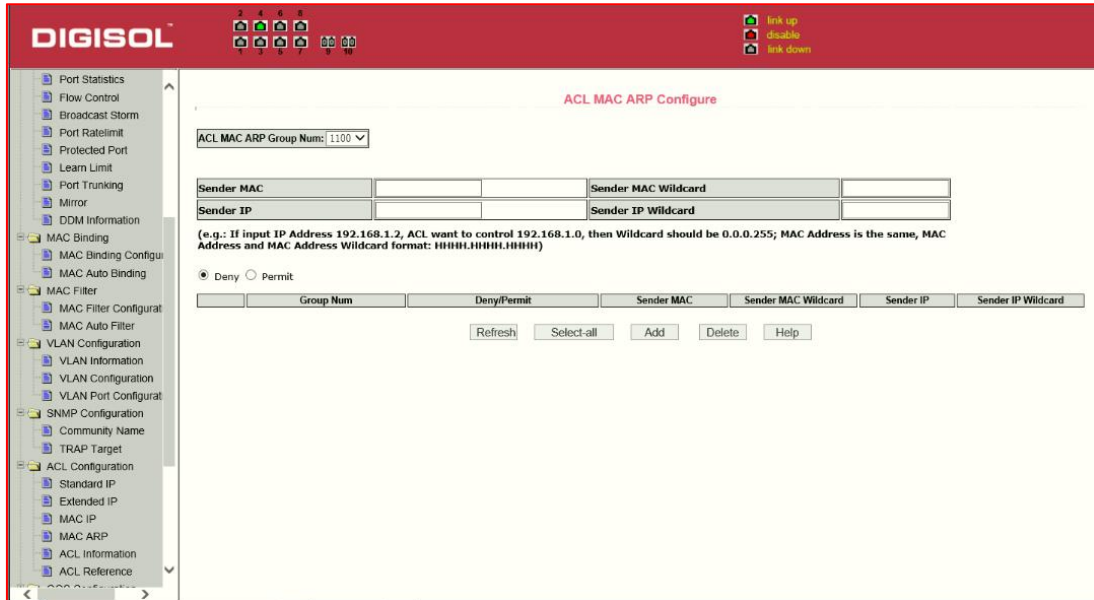


Figure 34 the IP Extended ACL configuration page

### (5) ACL information page

.Figure 35 is the ACL information page, which displays the current ACL rules configured in all the information.

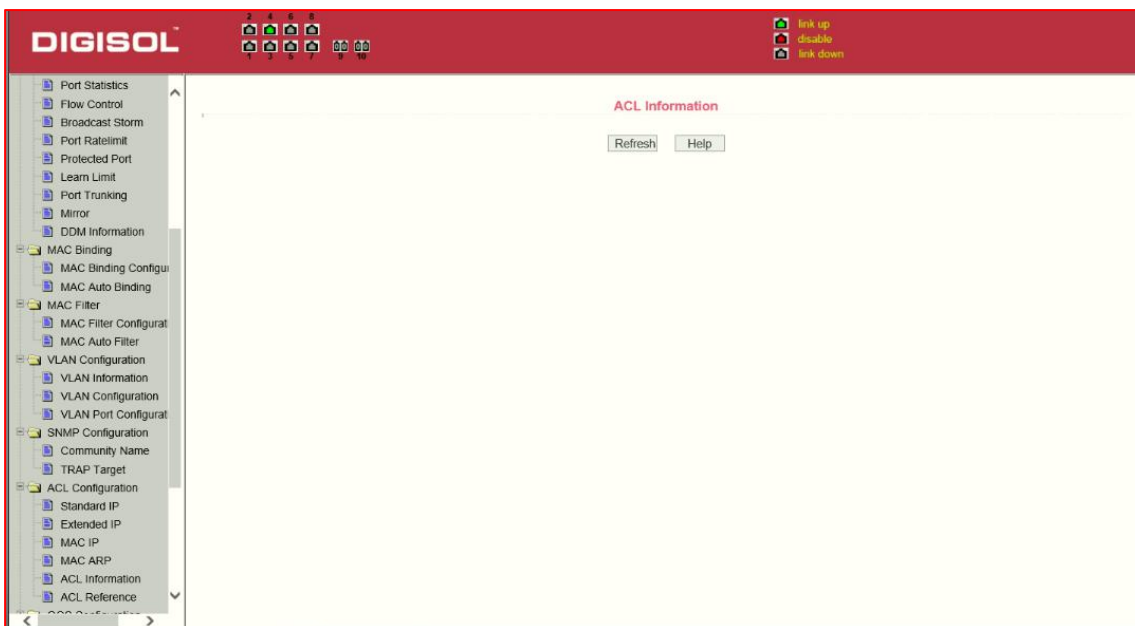


Figure 35 is the ACL information page

## 8. QoS Configuration

### (1) QoS Apply Configuration Page

Figure 36 is a QoS Apply configuration page.



Figure 36 QoS Apply configuration page

### (2) QoS Schedule Configuration Page

Figure 37 is a QoS Schedule configuration page.

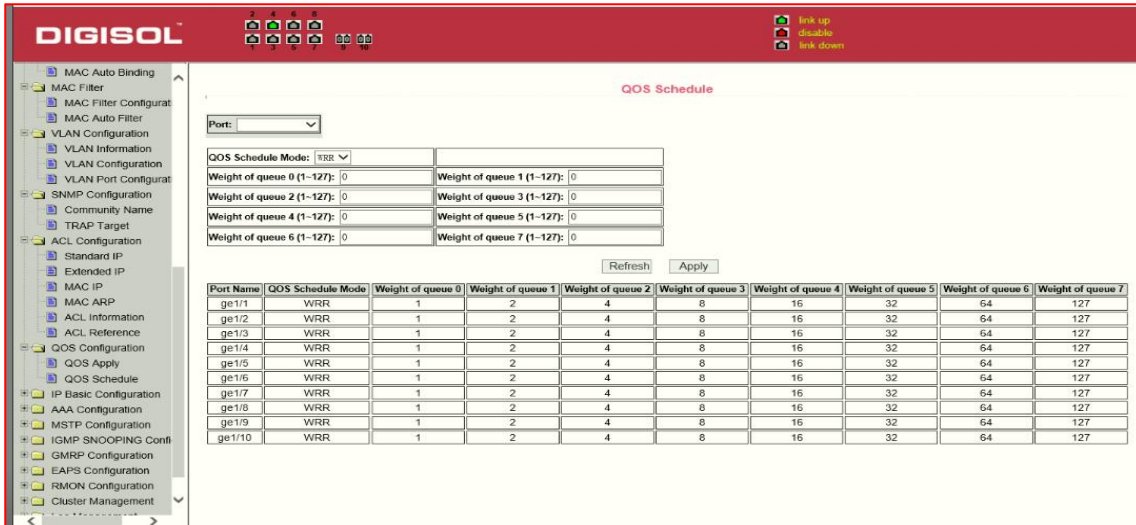


Figure 37 QoS Schedule configuration page

## 9. IP Basic Configuration

### (1) VLAN Interface Configuration Page

Figure 38 is a VLAN interface configuration page. Users can configure the VLAN interface through this page, delete VLAN interfaces, configure the interface IP address, remove the interface IP address, and view interface information.



Figure 38 VLAN interface configuration page

Switch, by default, has a VLAN1 interface, the interface can not be deleted. One can only configure a VLAN interface in this switch.

## (2) ARP configuration and display page

Figure 39 is the ARP configuration and displays all of the information of the ARP table. Users can configure a static ARP entries on this page, delete ARP entries, and revise the dynamic ARP table entry to a static ARP table entry.

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

When a user delete an ARP entry, you can choose to delete an IP-ARP table entry, remove a segment of the ARP table entry, delete all of the ARP table entry, delete all dynamic ARP table entries and delete all of the static ARP table entry.

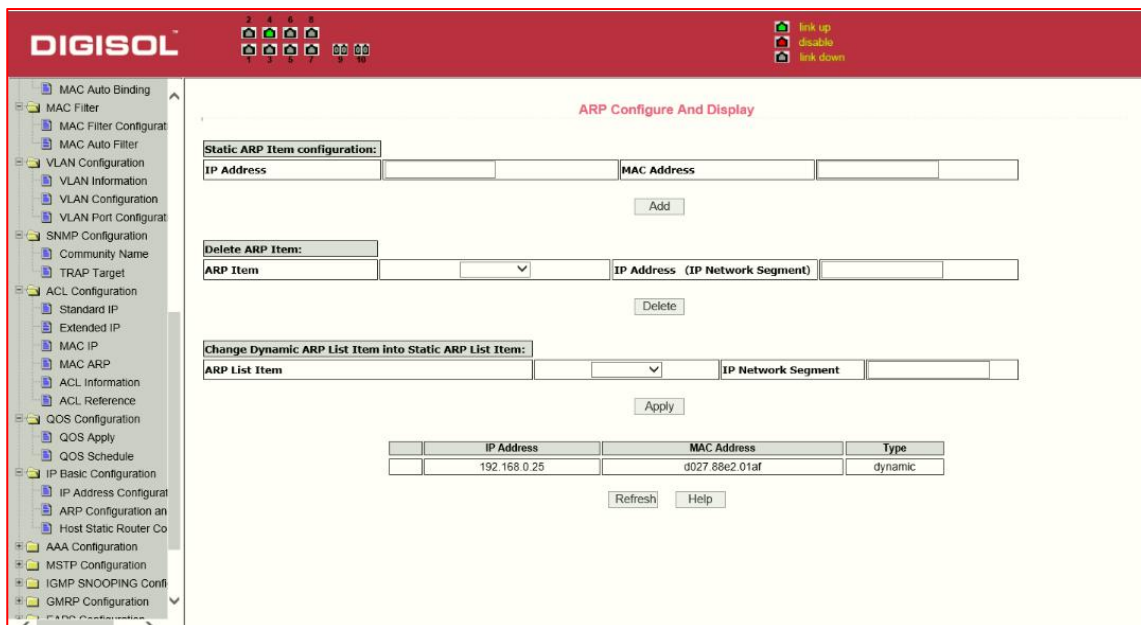


Figure 39 the ARP configuration and display page



### (3) Host Static Routing configuration page

Figure 40 is the static route configuration page, the user can use this page to add, delete static routes.

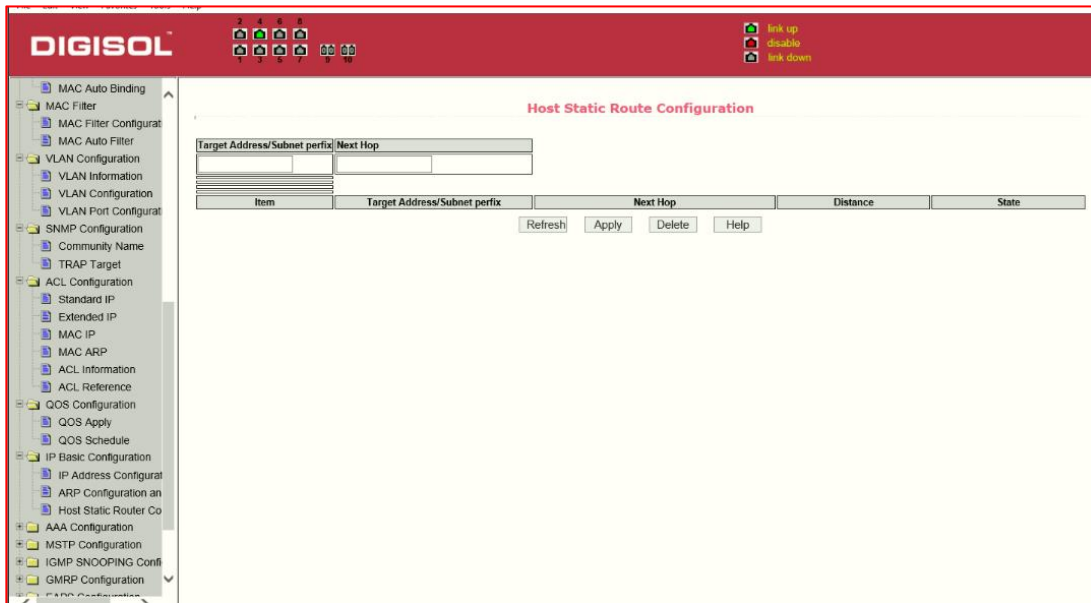


Figure 40 the host static route configuration page

## 10. Certification. Authorization. Accounting (AAA) configuration

### (1) Radius Configuration Page

- Figure 41 is the Radius configuration page, users can configure the Radius-related information, you can set following information:
  - Be sure to set the Radius server's IP address before do the authentication and accounting in this field,
  - Optional Radius server IP address, if there is spare Radius server..
  - Authentication UDP port, the default value is 1812, the user generally do not need to modify this field.
  - Accounting enable when you do authentication and accounting in general to start charging.
  - Accounting UDP port, the default value is 1813.
  - 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.

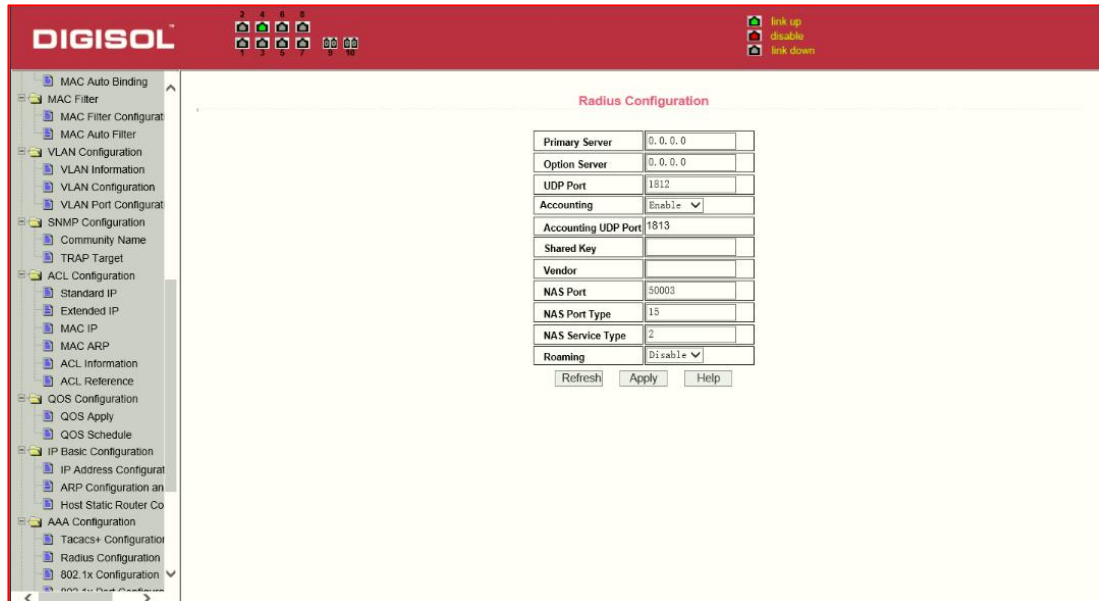


Figure 41 the Radius configuration page

## (2) 802.1x Configuration Page

Figure 42 is the 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. To adopt a common authentication method or the expansion of authentication.
3. Whether to open re-authentication function, the default is not open. 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.
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.

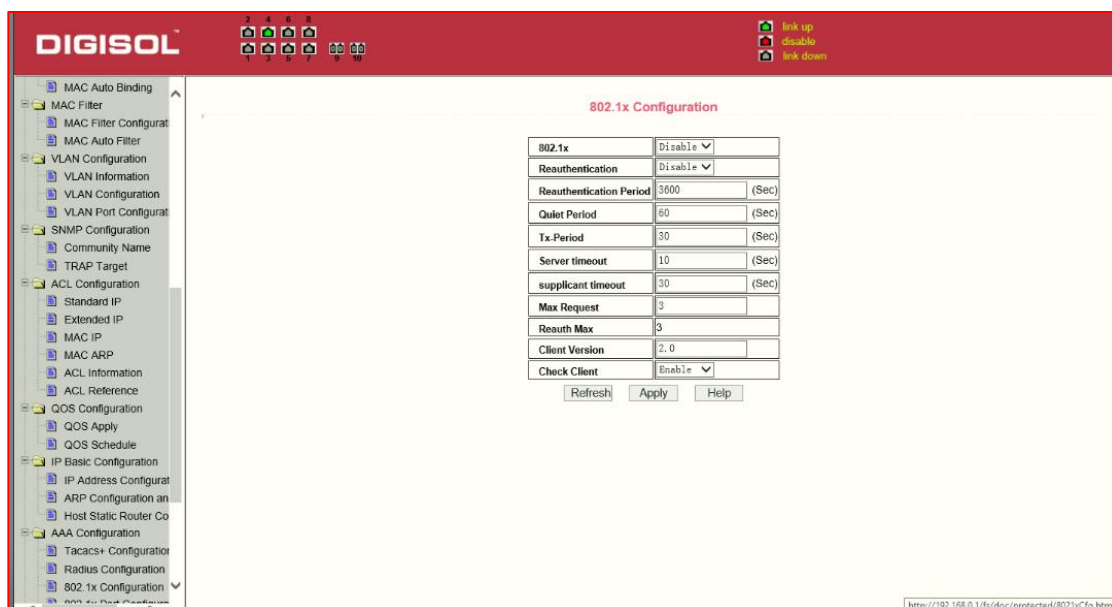


Figure 42 the 802.1x configuration page

### (3) 802.1x port configuration page

Figure 43 is the 802.1x port configuration page. The user through this page can configure the 802.1x port mode. 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

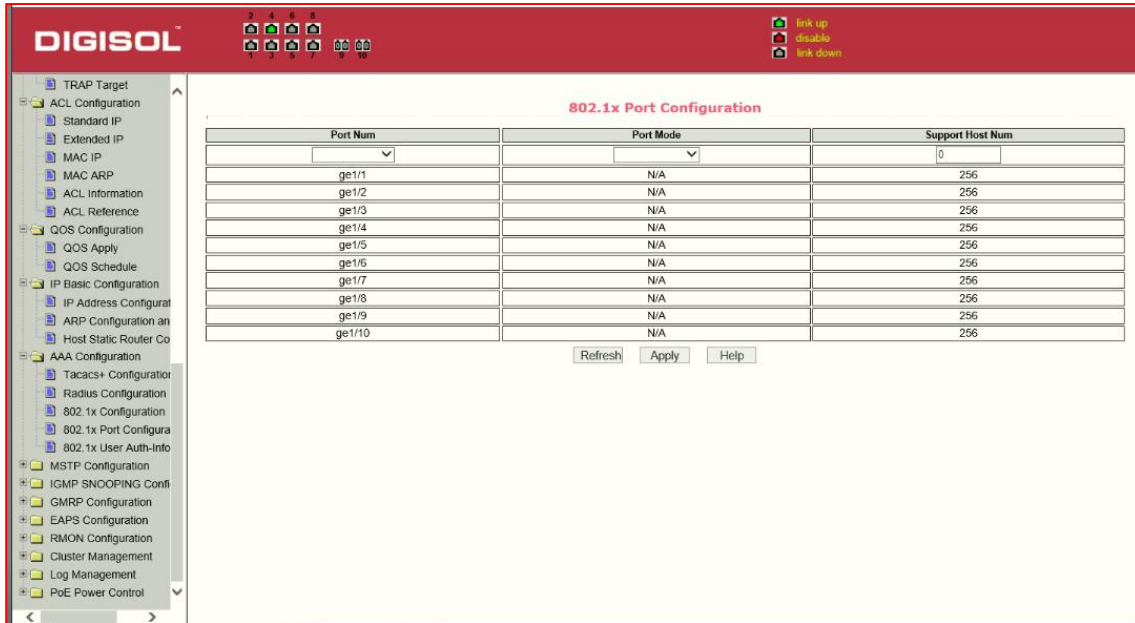


Figure 43 the 802.1x port configuration page

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

#### (4) 802.1x user authentication information page

Figure 44 is a 802.1x user authentication information page, the user can see through this page, all users state information,



Figure 44 802.1x user authentication information page

## 11. Spanning Tree Protocol configuration

### (1) MSTP global configuration page

Figure 45 is the 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 starts a BPDU guard receives a BPDU, it starts the error-disable timer. Error-disable restarts this port after the configured timeout.
- Configure error-disable 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.

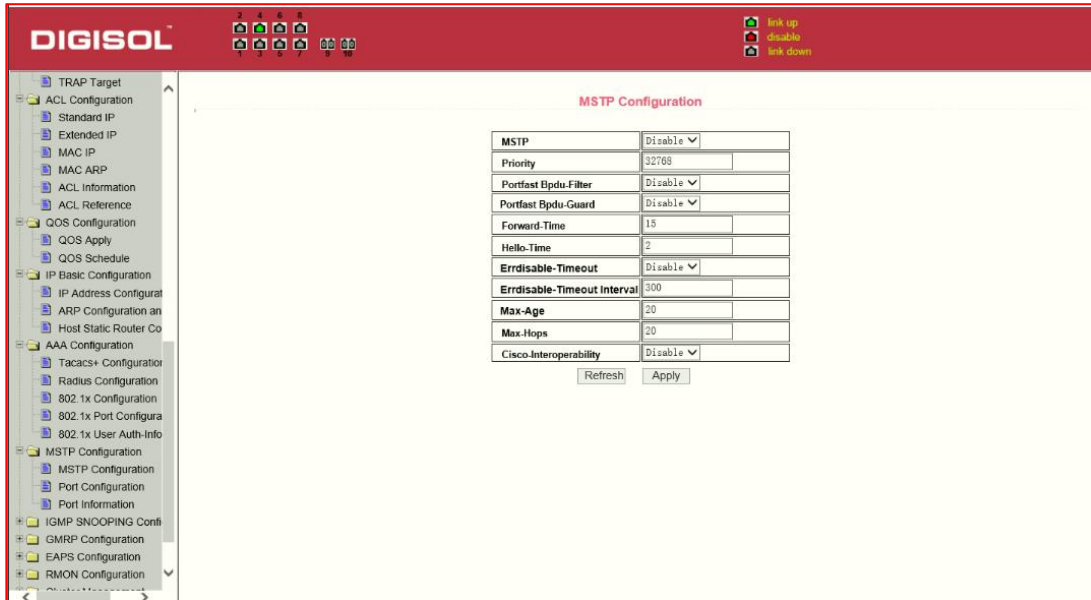


Figure 45 MSTP Global Configuration Page

## (2) MSTP port configuration page

Figure 46 is the MSTP global configuration page. Through this page, you 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 cost 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.

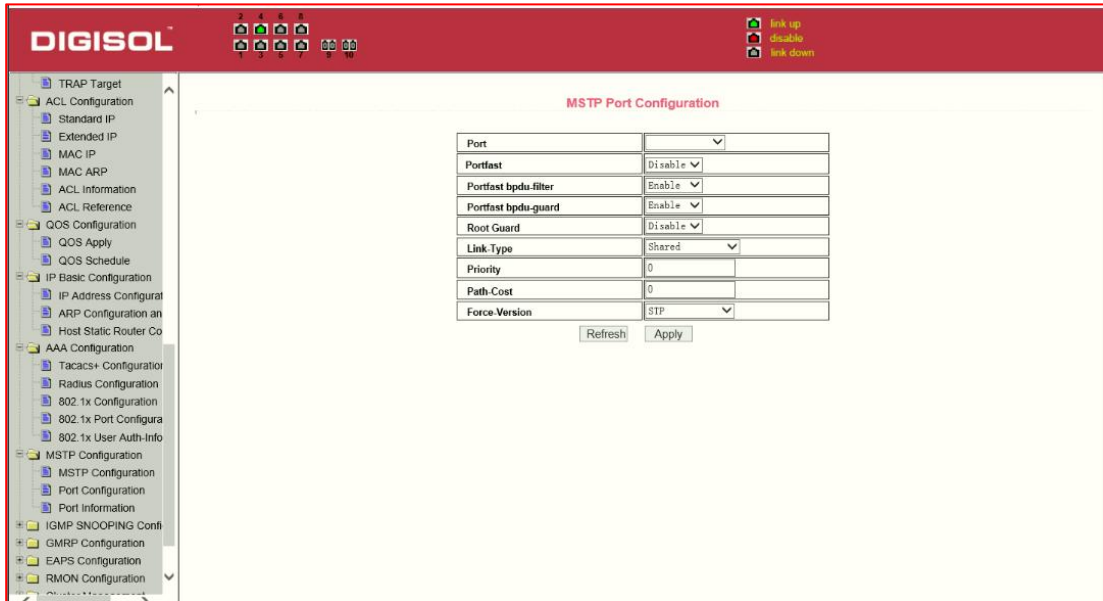


Figure 46 MSTP Port Configuration Page

### (3) MSTP configuration information page

Figure 47 is the MSTP configuration information page, in this page you can view some MSTP related information

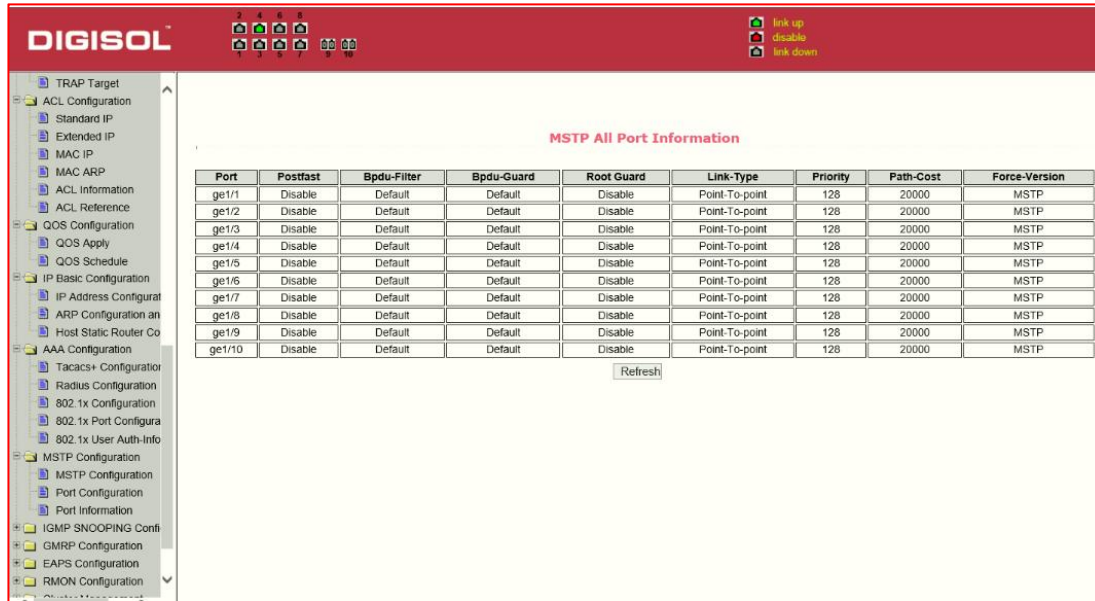


Figure 47 MSTP Configuration Information page

## 12. IGMP SNOOPING configuration

### (1) IGMP SNOOPING configuration page

Figure 48 is the IGMP SNOOPING configuration page, this page you can start IGMP SNOOPING.



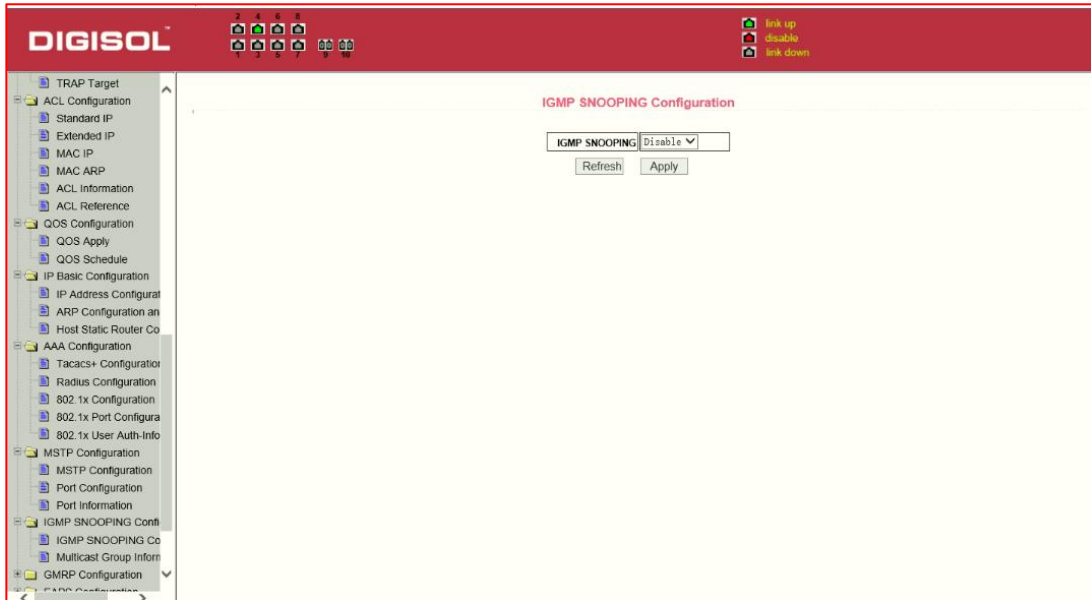


Figure 48 IGMP SNOOPING configuration page

## (2) IGMP SNOOPING information page

Figure 49 is the IGMP SNOOPING information page, which allows users to view some information about IGMP SNOOPING.

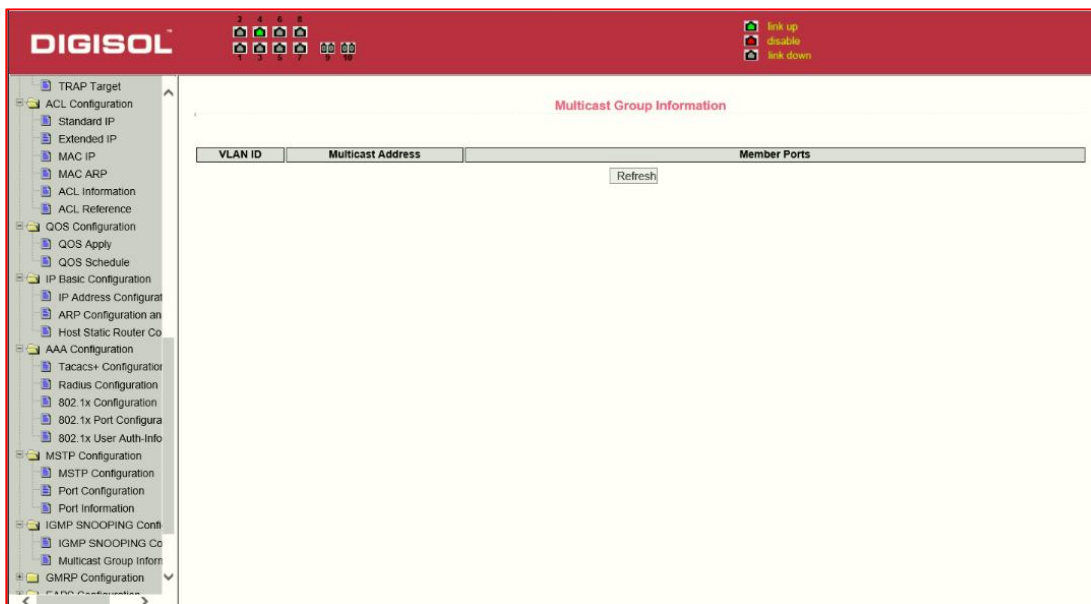


Figure 49 IGMP SNOOPING Information page

### 13. GMRP configuration

#### (1) GMRP Global Configuration Page

Figure 50 shows the GMRP global configuration page. Users can enable GMRP through this page.

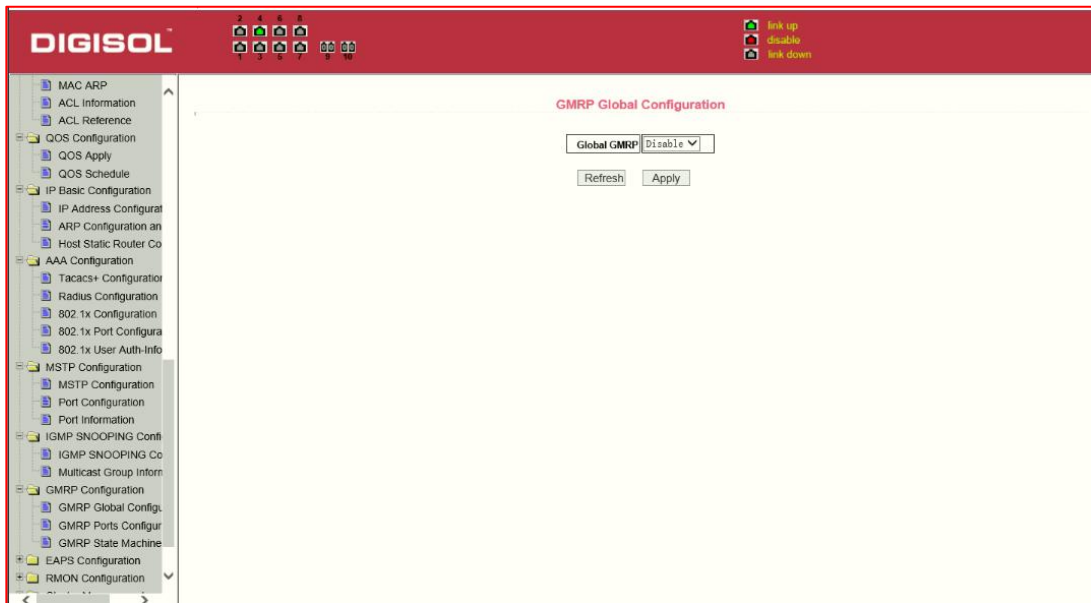


Figure 50 GMRP Global Configuration Page

#### (2) GMRP port configuration page

Figure 51 shows the GMRP port configuration page. You can use this page to enable the GMRP port and view the port information.



## 14. EAPS configuration

### (1) EAPS configuration page

Figure 53 is an 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

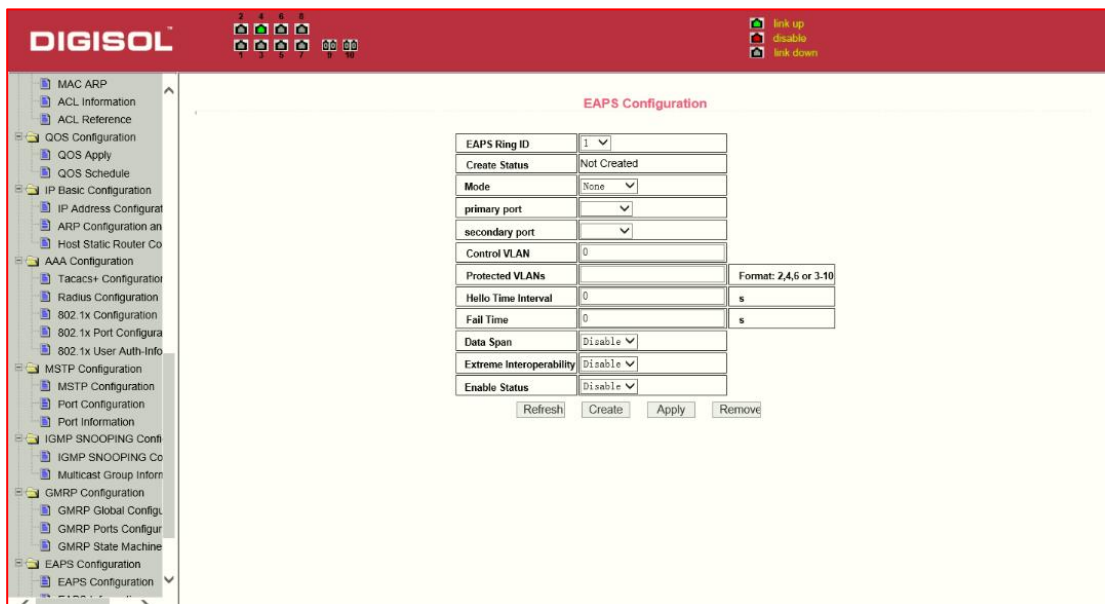


Figure 53 EAPS Configuration Page

## (2) EAPS information page

Figure 54 is an EAPS information page, users can view some EAPS related information.

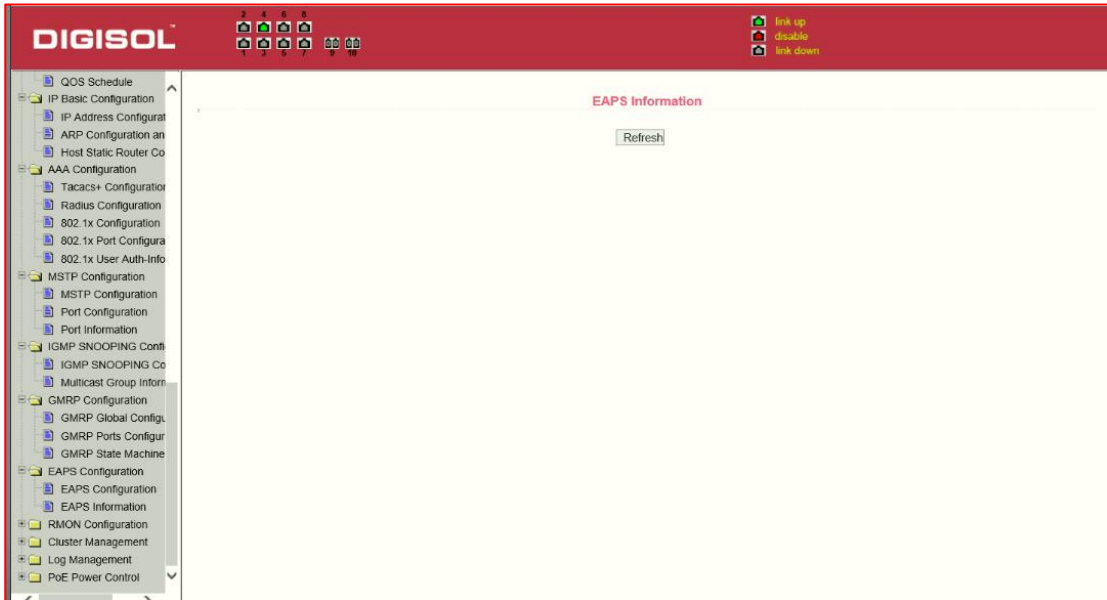


Figure 54 EAPS information page

## 15. RMON configuration

### (1) RMON statistics group configuration page

Figure 55 shows the 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.

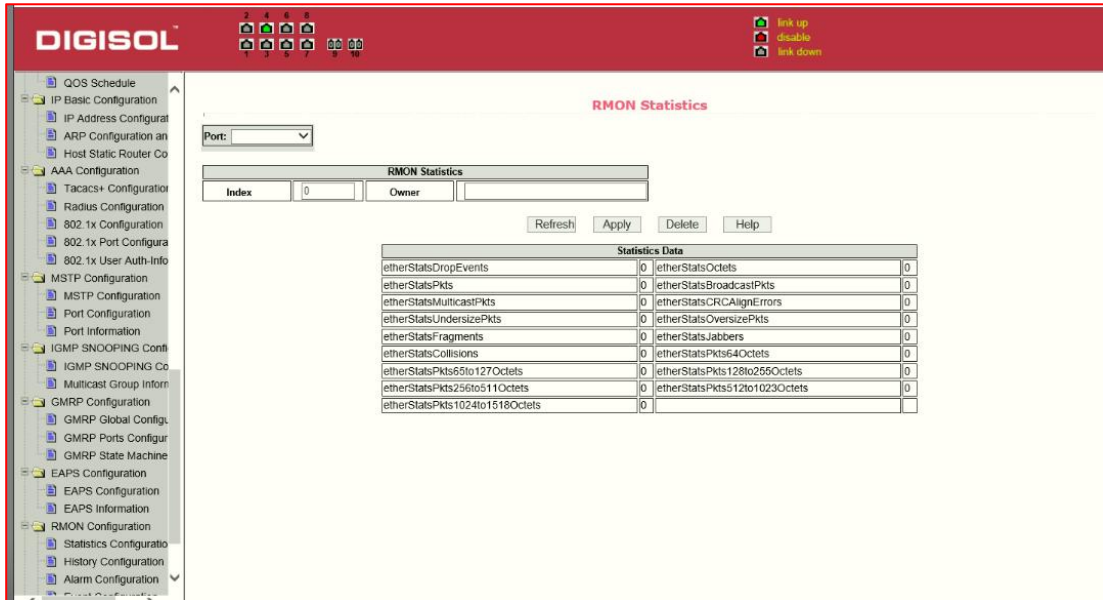


Figure 55 RMON statistics group configuration page

## (2) RMON history group configuration page

Figure 56 shows the 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.

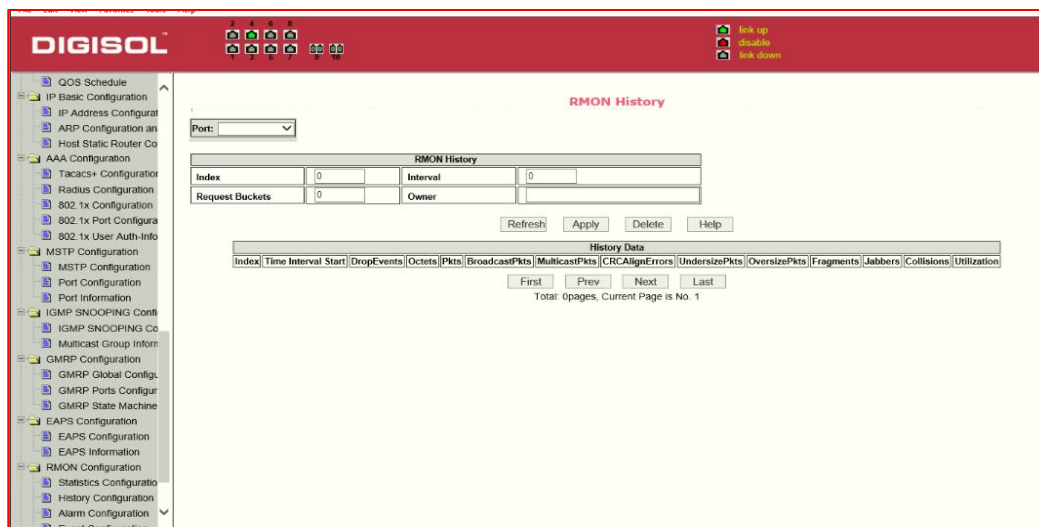


Figure 55: RMON history group configuration page

### (3) RMON alarm group configuration page

Figure 57 shows the RMON alarm group configuration page. You can use this page to create or modify 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. 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.

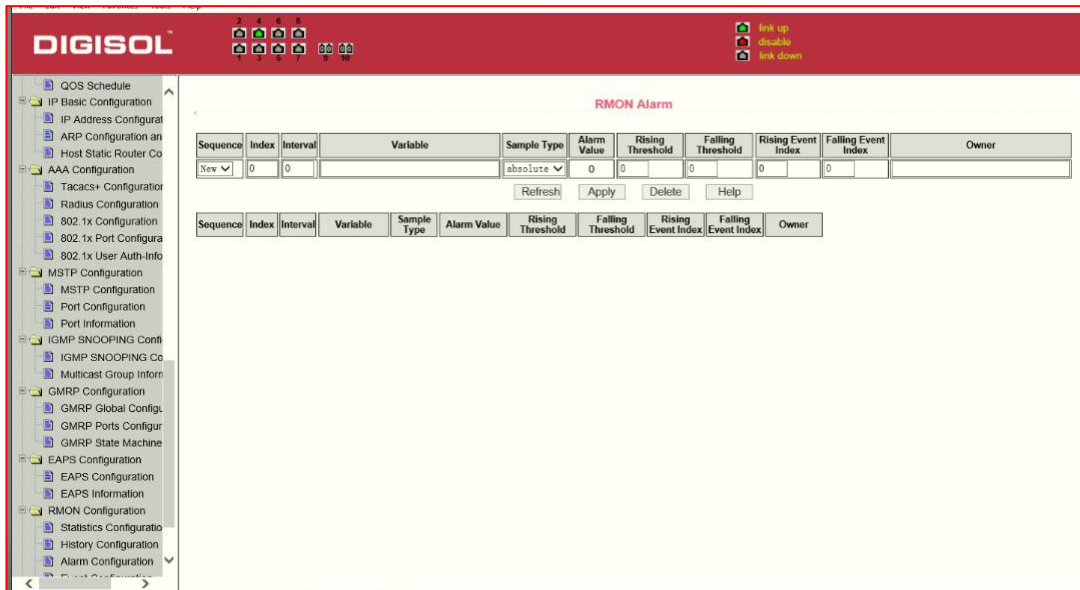


Figure 57: RMON Event Group Configuration Page

## 16. Cluster configuration

### (1) NDP configuration page

Figure 58 shows the 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

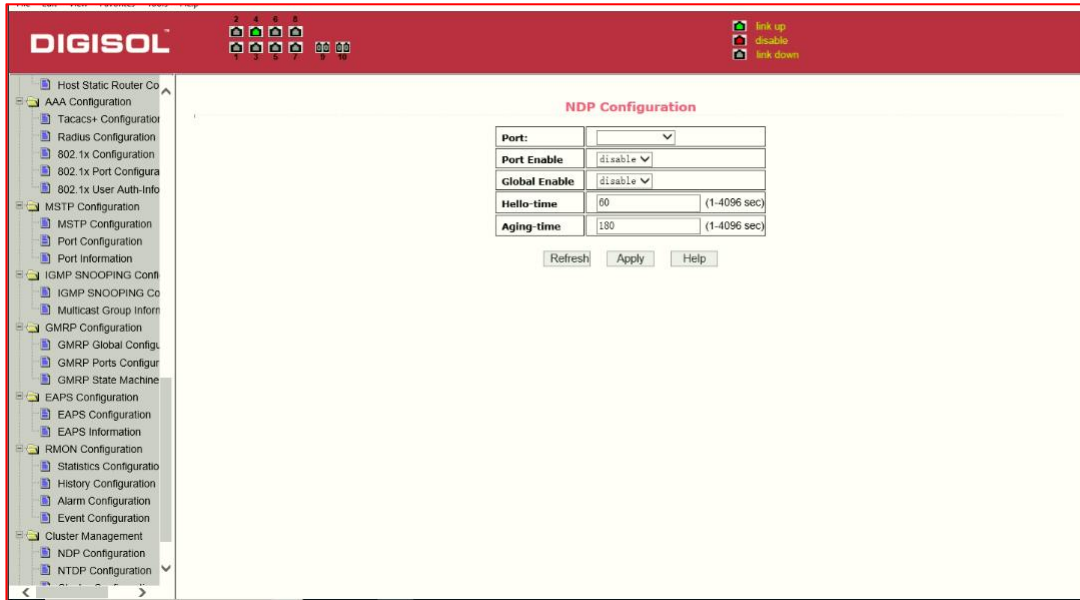


Figure 58 NDP configuration page

## (2) NTDP configuration page

Figure 59 shows the NTDP configuration page. Using 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.



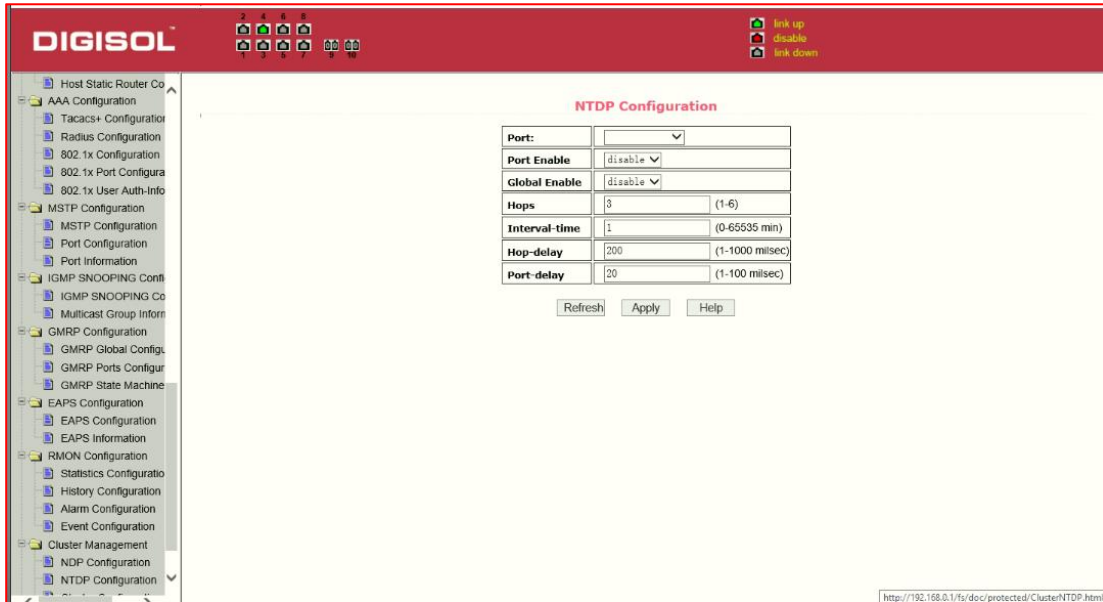


Figure 59 NTDP configuration page

### (3) Cluster Configuration Page

Figure 60 is the 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.

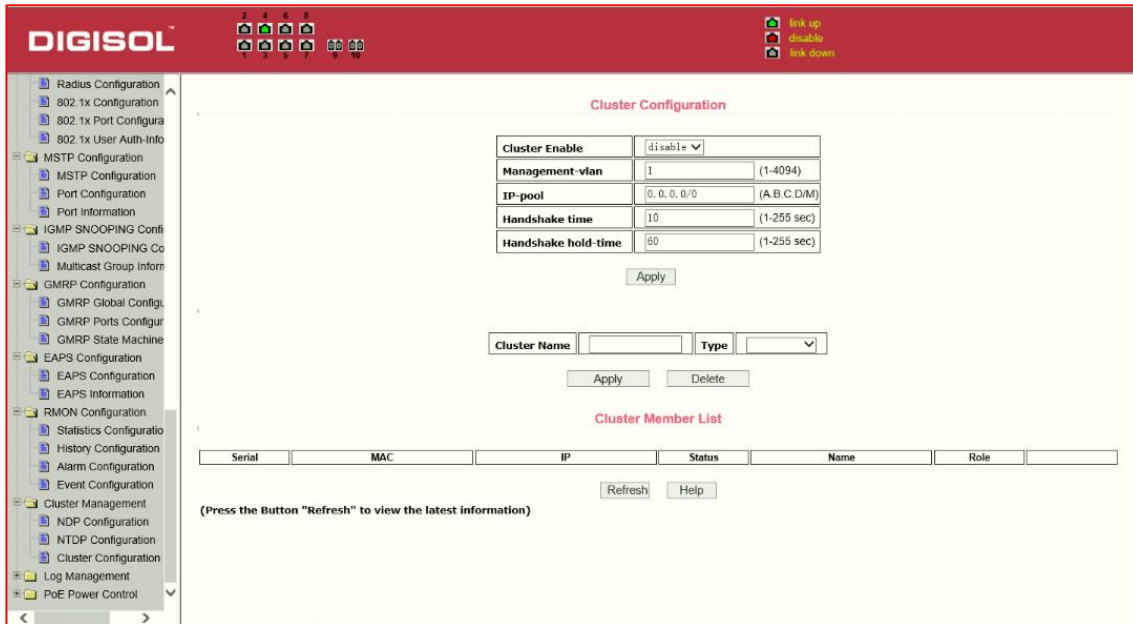


Figure 50 Cluster Configuration Page

## 17. log management

### (1) Log information page

Figure 61 is the Log information page. Users can enable and view various log information through this page.

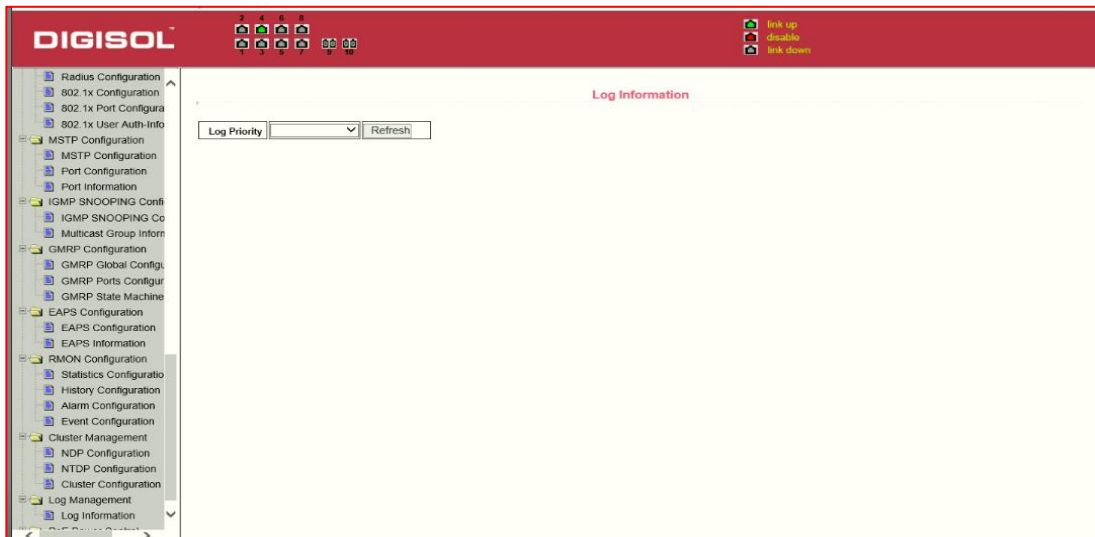


Figure 61 Log Information Page

Critical: output critical level information.

Debugging: Outputs debug level debugging information.

Informational: Output information information level debugging information.

Warning: output warning level debugging information.

ALL: output all log information

### 18. PoE port Configuration Page

Figure 62 is the PoE port configuration / PoE-display page. Users can enable or disable the port's PoE function to the page, or View all ports of PoE information.

Information can be seen in the following tables:

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

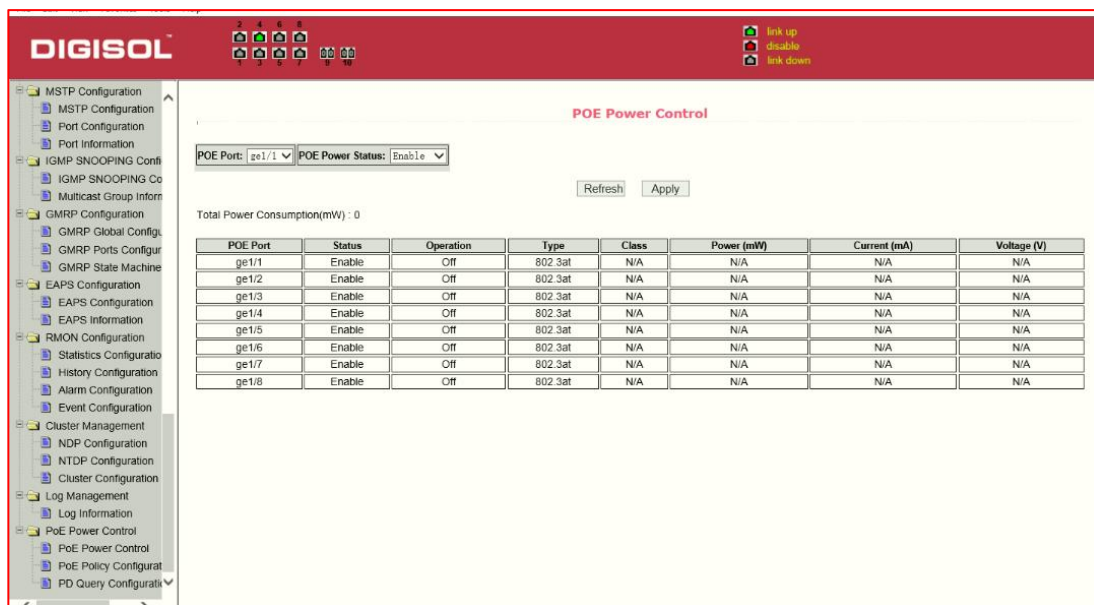


Figure 62 the PoE port configuration page



## Limited Lifetime Warranty

This Product is covered under DIGICARE Limited Lifetime Warranty program backed by DIGICARE Service Center. To avail this Limited Lifetime Warranty offer, customer needs to contact DIGICARE's Technical Assistance Center for the same. You may be asked to provide proof of purchase of product for warranty claim of defective product. Please refer website [www.digisol.com](http://www.digisol.com) for the detailed support terms & conditions and support process.

### Warranty Policy

1. **Hardware Warranty :** Hardware warranty period shall be limited up to Three years. External Power Adapter shall carry One year warranty only against manufacturing defects. Any repair or replacement will be rendered by DIGICARE at its Service Center only.
2. **Software Warranty :** DIGISOL issues this Limited Software Warranty that the software portion of the product ("Software") will substantially confirm to DIGISOL's then current functional specifications for the software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of one year ("Software Warranty period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation.
3. **Governing Law:** This warranty shall be governed by Indian Laws.
4. **Limited Lifetime Warranty** shall subject to the terms & conditions specified in the DIGISOL PRODUCT WARRANTY policy displayed on [www.digisol.com](http://www.digisol.com)
5. To avail and activate warranty for your product.  
Kindly register your product by calling us @18002093444

