Web Configuration

Table of Contents

Chapter 1 Configuration Preparation....1
1.1 HTTP Configuration....1
1.1.1 Choosing the Prompt Language....1
1.1.2 Configuring the HTTP Port....1
1.1.3 Enabling the HTTP service....1
1.1.4 Configuring the HTTP Access Mode....1
1.1.5 Configuring the maximum number of VLAN entries displayed on a web page....2
1.1.6 Configuring the Maximum Number of Multicast Entries Displayed on a Web Page....2
1.2 HTTPS Configuration....2
1.2.1 Configuring the HTTP Access Mode....2
1.2.2 Configuring the HTTPS Port....2
Chapter 2 Accessing the OLT....4
2.1 Accessing the OLT through HTTP....4
2.1.1 Initially Accessing the OLT....4
2.1.2 Upgrading to the Web-Supported Version....5
2.2 Accessing an OLT through Secure Links....5
2.3 Introduction of Web Interface....6
2.3.1 Top Control Bar....6
2.3.2 Navigation Bar....7
2.3.3 System Information....7
2.3.4 Configuration Area....8
Chapter 3 Basic Configuration....9
3.1 Hostname....9
3.2 Clock Mgr....10
Chapter 4 GPON Interface Config....11
4.1 GPON Global Config....11
4.2 ONU Bind Relationship Config....11
4.3 ONU Discover Mode....12
Chapter 5 ONU Config Profile....14
5.1 ONU T-Cont Config....14
5.2 ONU Rate Limit Config....15
5.3 ONU Virtual Port Config....16
5.4 T-Cont Virtual Port Bind Config....16
5.5 ONU VLAN Config....17
5.6 ONU Flow Mapping Config....18
Chapter 6 ONU Interface Config....19
6.1 T-Cont Virtual Port Bind....19
6.2 Flow Mapping....19
6.3 VLAN Config....20
6.4 Virtual Port GEM Port Bind....20
Chapter 7 Advanced Config....21

7.1 Port Description..... 22
7.2 Port Config..... 22
7.3 Rate Limit..... 23
7.4 Port Mirror..... 24
7.5 VLAN Config..... 25
7.5.1 VLAN Config..... 25
7.5.2 VLAN Batch Config..... 27
7.5.3 Interface VLAN Attribute Config..... 27
7.6 VLAN Interface..... 28
7.7 LLDP Config..... 29
7.8 STP Config..... 29
7.8.1 STP State..... 29
7.8.2 STP Port Config..... 30
7.9 Static MAC Config..... 30
7.10 Port Security..... 31
7.10.1 IP Bind..... 31
7.10.2 MAC Bind..... 32
7.10.3 Static MAC Filtration Mode..... 33
7.10.4 Static MAC Filtration Entry..... 34
7.10.5 Dynamic MAC Filtration Mode..... 35
7.11 Storm Control..... 35
7.11.1 Broadcast Storm Control..... 36
7.11.2 Multicast Storm Control..... 37
7.11.3 Unknown Unicast Storm Control..... 38
7.12 IP Access List..... 38
7.12.1 IP Access List Config..... 38
7.12.2 IP Access List Application..... 40
7.13 MAC Access List..... 41
7.13.1 MAC Access List Config..... 41
7.13.2 MAC Access List Application..... 42
7.14 Port Channel..... 43
7.14.1 Port Channel..... 43
7.14.2 Port Channel Group Loading Balance..... 44
7.15 Ring Protection..... 44
7.16 DDM Config..... 45
7.17 MTU Config..... 46
Chapter 8 L3 Config..... 47
8.1 Static Route..... 47
Chapter 9 Remote Monitor..... 49
9.1 SNMP Mgr..... 49
9.1.1 SNMP Community Mgr..... 49
9.1.2 SNMP Host Mgr..... 50
9.2 RMON..... 50
9.2.1 RMON Statistics..... 50
9.2.2 RMON History..... 51
9.2.3 RMON Alarm..... 52

9.2.4 RMON Event..... 52
Chapter 10 System Mgr..... 54
10.1 User Mgr..... 54
10.1.1 User Mgr..... 54
10.1.2 Group Mgr..... 55
10.1.3 Pass-Group Mgr..... 56
10.1.4 Authen-Group Mgr..... 57
10.1.5 Author-Group Mgr..... 57
10.2 Log Mgr..... 58
10.3 Diagnostic..... 58
10.4 Startup-config..... 59
10.4.1 Export the current startup-config..... 59
10.4.2 Import startup-config file..... 60
10.5 IOS Software..... 60
10.5.1 Backup IOS..... 60
10.5.2 Update IOS..... 61
10.6 Factory Settings..... 61
10.7 Reboot..... 62
10.8 About..... 62

Chapter 1 Configuration Preparation

1.1 HTTP Configuration

OLT configuration can be conducted not only through command lines and SNMP but also through Web browser. The OLT supports the HTTP configuration, the abnormal packet timeout configuration, and so on.

1.1.1 Choosing the Prompt Language

Up to now, the OLT supports two languages, that is, English and Chinese, and the two languages can be switched over through the following command.

Command	Purpose
ip http language {**chinese** | **english**}	Sets the prompt language of Web configuration to (Chinese|English).

1.1.2 Configuring the HTTP Port

Generally, the HTTP port is port 80 by default, and users can access an OLT by entering the IP address directly; however, the OLT also supports users to change the service port and after the service port is changed you have to use the IP address and the changed port to access OLT. For example, if you set the IP address and the service port to 192.168.1.3 and 1234 respectively, the HTTP access address should be changed to http:// 192.168.1.3:1234. You'd better not use other common protocols' ports so that access collision should not happen. Because the ports used by a lot of protocols are hard to remember, you'd better use port IDs following port 1024.

Command	Purpose
ip http port { *portNumber* }	Sets the HTTP Port

1.1.3 Enabling the HTTP service

The OLT supports to control the HTTP access. Only when the HTTP service is enabled can HTTP exchange happen between the OLT and PC and, when the HTTP service is disabled, HTTP exchange stops.

Command	Purpose
ip http server	Enables the HTTP service

1.1.4 Configuring the HTTP Access Mode

You can access a switch through two access modes: HTTP access and HTTPS access, and you can use the following command to set the access mode to HTTP.

Command	Purpose

ip http http-access enable	Sets the HTTP Access Mode

1.1.5 Configuring the maximum number of VLAN entries displayed on a web page

An OLT supports at most 4094 VLANs and in most cases Web only displays parts of VLANs, that is, those VLANs users want to see. You can use the following command to set the maximum number of VLANs. The default maximum number of VLANs is 100.

Command	Purpose
ip http web max-vlan { *max-vlan* }	Sets the maximum number of VLAN entries displayed in a web page.

1.1.6 Configuring the Maximum Number of Multicast Entries Displayed on a Web Page

An OLT supports at most 100 multicast entries. You can run the following command to set the maximum number of multicast entries and Web then shows these multicast entries. The default maximum number of multicast entries is 15.

Command	Purpose
ip http web igmp-groups { *igmp-groups* }	Sets the maximum number of multicast entries displayed in a web page.

1.2 HTTPS Configuration

In order to improve the security of communications, the OLT supports not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

1.2.1 Configuring the HTTP Access Mode

You can run the following command to set the access mode to HTTPS.

Command	Purpose
ip http ssl-access enable	Sets the HTTPS access mode

1.2.2 Configuring the HTTPS Port

As the HTTP port, HTTPS has its default service port, port 443, and you also can run the following command to change its service port. It is recommended to use those ports following port 1024 so as to avoid collision with other protocols' ports.

Parameters	Purpose
ip http secure-port {*portNumber*}	Sets the HTTPS port.

Chapter 2 Accessing the OLT

2.1 Accessing the OLT through HTTP

When accessing the OLT through Web, please make sure that the applied browser complies with the following requirements:

- HTML of version 4.0
- HTTP of version 1.1
- JavaScriptTM of version 1.5

What's more, please ensure that the main program file, running on an OLT, supports Web access and your computer has already connected the network in which the OLT is located.

2.1.1 Initially Accessing the OLT

When the OLT is initially used, you can use the Web access without any extra settings:

1. Modify the IP address of the network adapter and subnet mask of your computer to 192.168.0.2 and 255.255.255.0 respectively.

2. Open the Web browser and enter 192.168.0.1 in the address bar. It is noted that 192.168.0.1 is the default management address of the OLT.

3. If the Internet Explorer browser is used, you can see the dialog box as below. Both the original username and the password are “admin”, which is capital sensitive.

4. After successful authentication, the systematic information about the OLT will appear on the IE browser.

2.1.2 Upgrading to the Web-Supported Version

If your OLT is upgraded to the Web-supported version during its operation and the OLT has already stored its configuration files, the Web visit cannot be directly applied on the OLT. Perform the following steps one by one to enable the Web visit on the OLT:

1. Connect the console port of the OLT with the accessory cable, or telnet to the management address of the OLT through the computer.

2. Enter the global configuration mode of the OLT through the command line, the prompt of which is similar to “Switch_config#”.

3. If the management address of the OLT is not configured, please create the VLAN interface and configure the IP address.

4. Enter the **ip http server**” command in global configuration mode and start the Web service.

5. Enter the **username** to set the user name and password of the OLT. For how to use this command, refer to the “Security Configuration” section in the user manual.

After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the OLT.

6. Enter **write** to store the current configuration to the configuration file.

2.2 Accessing an OLT through Secure Links

The data between the WEB browser and the OLT will not be encrypted if you access an OLT through common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to access the OLT.

To do this, you should follow the following steps:

1. Connect the console port of the OLT with the accessory cable, or telnet to the management address of the OLT through the computer.

2. Enter the global configuration mode of the OLT through the command line, the DOS prompt of which is similar to “Switch_config#”.

3. If the management address of the OLT is not configured, please create the VLAN interface and configure the IP address.

4. Enter the “**ip http server**” command in global configuration mode and start the Web service.

5. Enter the “**username**” to set the user name and password of the OLT for how to use this command, refer to the “Security Configuration” section in the user manual.

6. Run “**ip http ssl-access enable**” to enable the secure link access of the OLT.

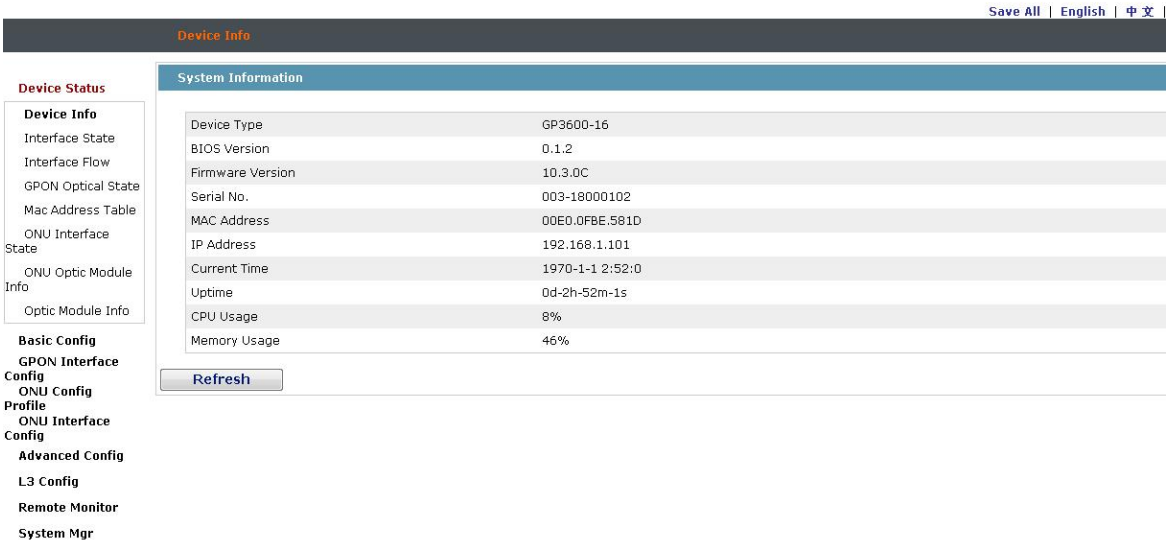
7. Run “**no ip http http-access enable”** to access the OLT through insecure links.

8. Enter “**write**” to store the current configuration to the configuration file.

9. Open the WEB browser on the PC that the OLT connects, enter https://192.168.0.1 on the address bar (192.168.0.1 stands for the management IP address of the OLT) IP address of the OLT) and then press the Enter key. Then the OLT can be accessed through the secure links.

2.3 Introduction of Web Interface

The whole Web homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.



2.3.1 Top Control Bar

Save All	Write the current settings to the configuration file of the device. It is equivalent to the execution of the "**write**" command. The configuration that is made through Web will not be promptly written to the configuration file after validation. On the left navigation bar, click "Save All", the unsaved configuration will be lost after rebooting.
English	The interface will turn into the English version.
Chinese	The interface will turn into the Chinese version.
Logout	Exit from the current login state. After you click "logout", you have to enter the username and the password again if you want to continue the Web function.

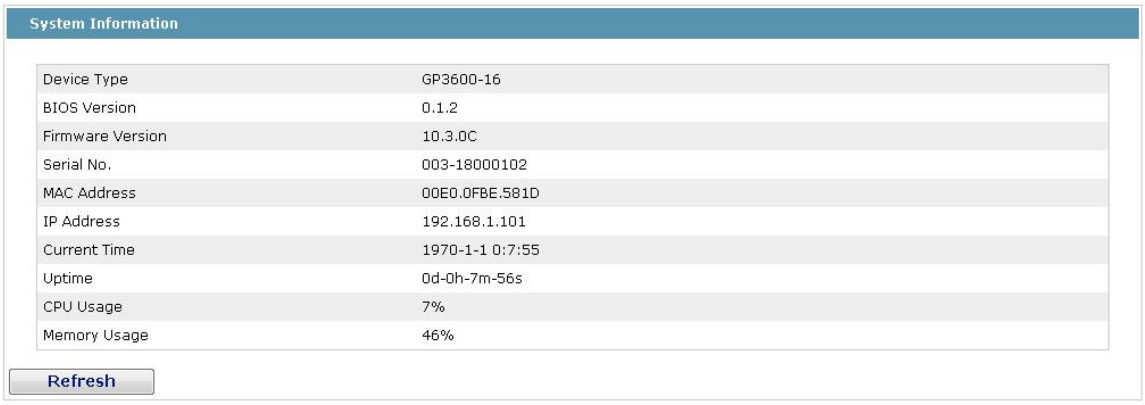
After you configure the device, the result of the previous step will appear on the left side of the top control bar. If error occurs, please check your configuration and retry it later.

2.3.2 Navigation Bar

The contents shown . The contents are shown in a form of list and are classified according to types. By default, the list is located at “Runtime Info”. If a certain item need be configured, please click the group name and then the subitem. For example, to browse the flux of the current port, you have to click “Interface State" and then “Interface Flow”.

Note:
The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web with limited user’s permissions, only “Interface State” will appear.

2.3.3 System Information



The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items .

2.3.4 Configuration Area

The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to the device. The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click “Save All” on the top control bar.
Reset	Means discarding the modification of the sheet. The content of the sheet will be reset.
New	Creates a list item. For example, you can create a VLAN item or a new user.
Delete	Deletes an item in the list.
Back	Go back to the previous-level configuration page.

Chapter 3 Basic Configuration

Figure 3-1: Basic Config

3.1 Hostname

On the left navigation bar, click “Basic Config” -> “Hostname”, and the Hostname Configuration page appears.

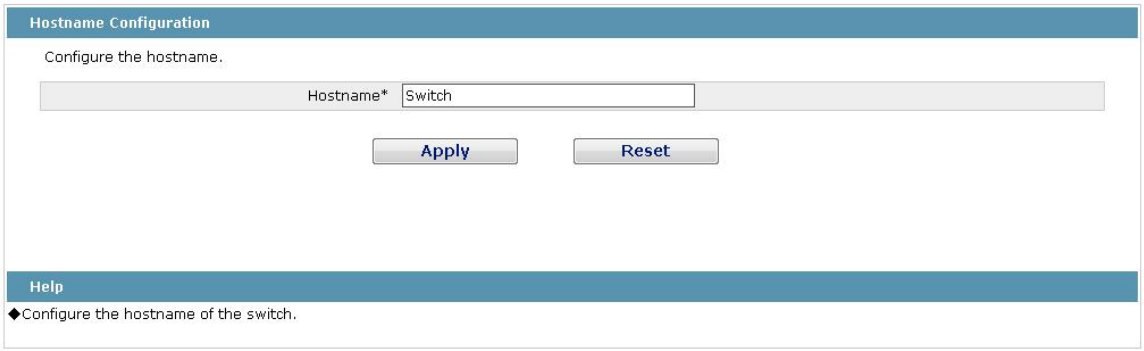


Figure 3-2: Hostname Configuration

The hostname will be displayed in the login dialog box.

The default name of the device is “Switch”. You can enter the new hostname in the text box shown in figure 3 and then click “Apply”.

3.2 Clock Mgr

On the left navigation bar, click “Basic Config” -> “Clock Mgr”, and the following page appears.

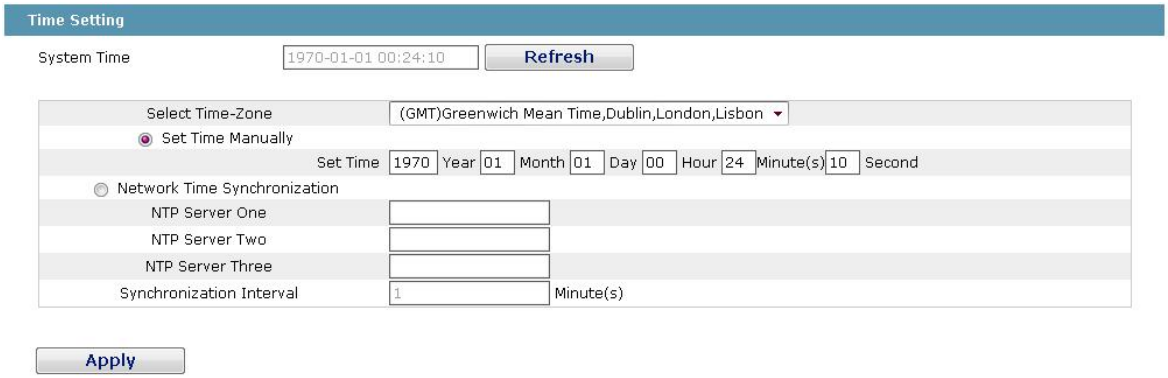


Figure 3-3 Time Setting

To refresh the clock of the displayed device, click “Reset”.

In the “Select Time-Zone” dropdown box select the time zone where the device is located. When you select “Set Time Manually”, you can set the time of the device manually. When you select “Network Time Synchronization”, you can designate 3 SNTP servers for the device and set the interval of time synchronization.

Chapter 4 GPON Interface Config

Figure 4-1: GPON Interface Configuration

4.1 GPON Global Config

On the left navigation bar, click “GPON Interface Config” -> “GPON Global Config”, and the following interface appears.

Figure 4-2: Device Name Configuration

On this page, you can configure ONU authentication method to serial number, password and authentication. You can broadcast GEM Port and the value ranges from 385 to 4094. Click “Apply” and the operation will take effect on the OLT. Click “Reset” to return to the default setting.

4.2 ONU Bind Relationship Config

On the left navigation bar, click “GPON Interface Config” -> “ONU Bind Relationship Config” and the following page appears.

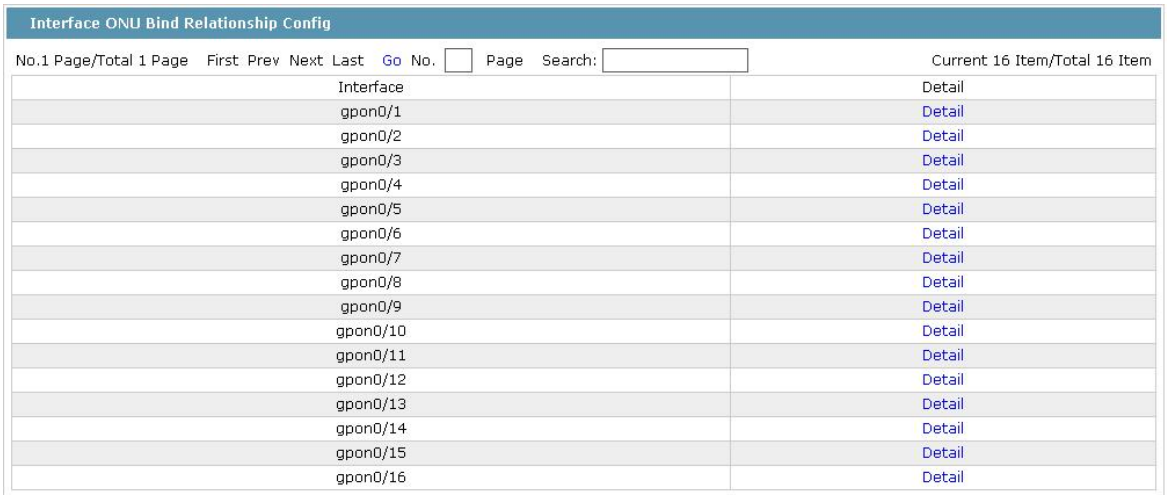


Figure 4-3: Interface ONU Bind Relationship Configuration

Click “Detail” to show the concrete ONU binding relationship of the concrete interface. Select an ONU and click “Delete” to remove the binding or click “Go Back” to return to the default setting. Click “New” on the top left of the interface to create a new “Interface ONU Bind Relationship Config” and the corresponding interface will pop up:

Figure 4-4: Interface ONU Bind Relationship List GPON 0/1

You can “Reset” the binding relationship and fill in the password and ONU ID. Click “Apply” to apply the configuration; click “Reset” to reset the information; click “Go Back” after you complete the configuration.

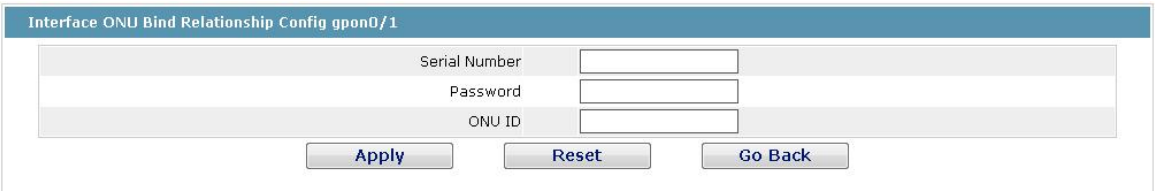


Figure4-5: Interface ONU Bind Relationship Config GPON0/1

4.3 ONU Discover Mode

On the left navigation bar, click “GPON Interface Config” -> “ONU Discover Mode”, and the following page appears.

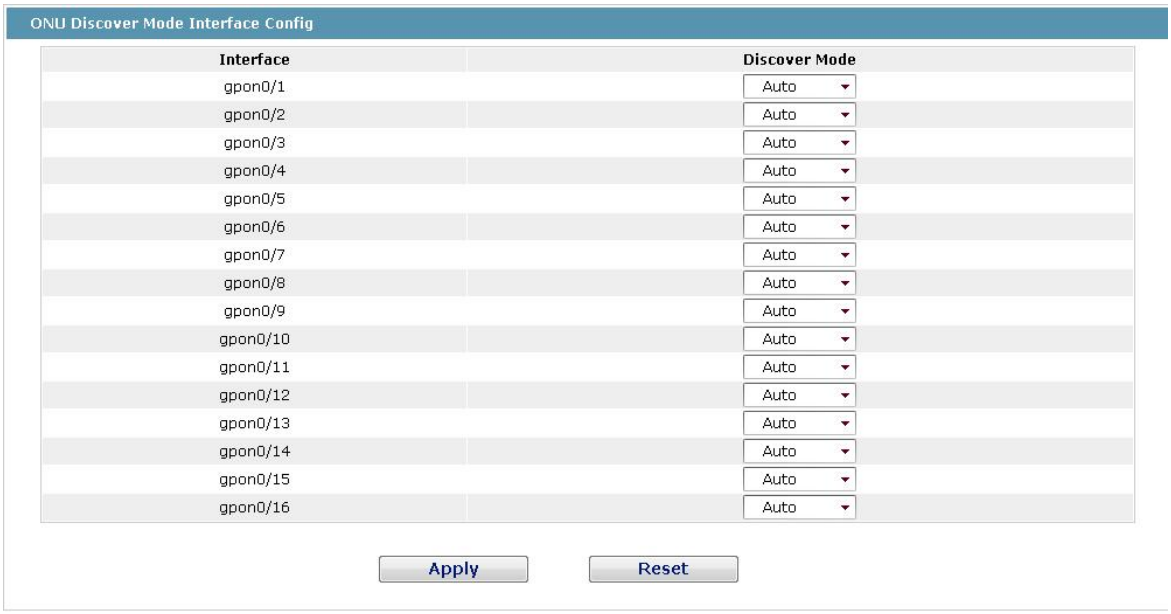


Figure 4-6: ONU Discover Mode Interface Config

You can designate the discover mode for each PON port: Auto or Disable. Click “Apply” to save the configuration.

Chapter 5 ONU Config Profile

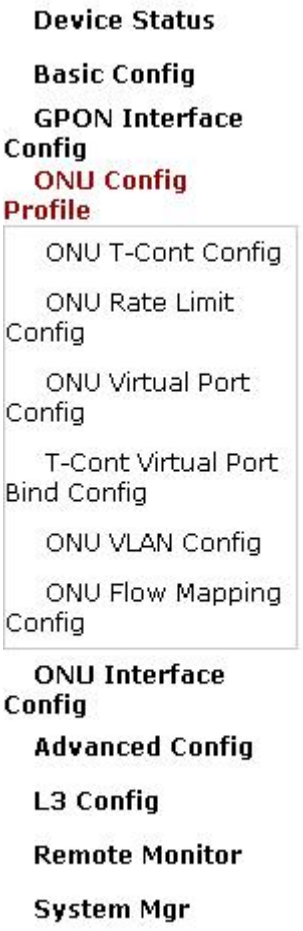


Figure 5-1: ONU Configuration Profile

5.1 ONU T-Cont Config

On the left navigation bar, click “ONU Config Profile” -> “ONU T-Cont Config”, and the following page appears.

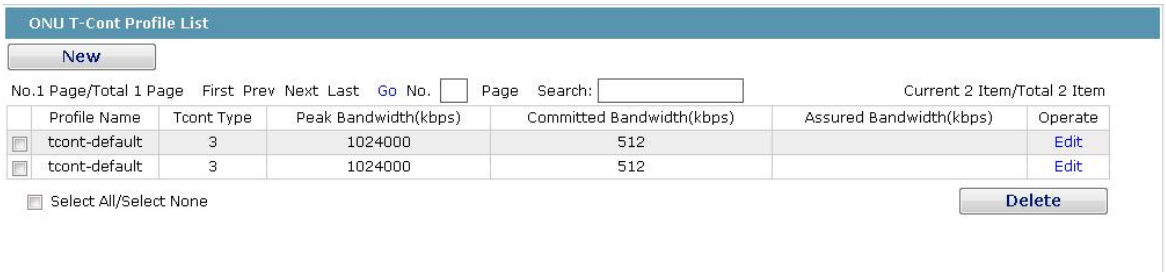


Figure 5-2 ONU T-Cont Profile List

On ONU T-Cont Profile List, select a to-be-deleted item, click “Delete” to delete the corresponding ONU profile. The default profile cannot be deleted.

Click “New” or “Edit” to edit the profile on the following page. On the page, you can edit Profile Name or select Tcont type (1-5), peak bandwidth, committed bandwidth and assured bandwidth (one or multiple). After completing the configuration, click “Apply” to save the configuration.

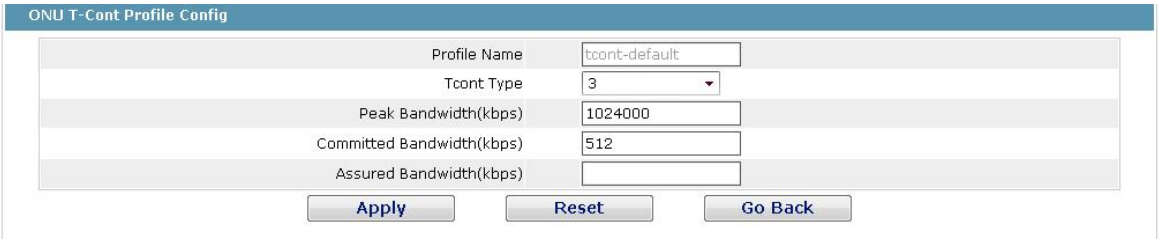


Figure 5-3: ONU T-Cont Profile Config

5.2 ONU Rate Limit Config

On the left navigation bar, click “ONU Config Profile” -> “ONU Rate Limit Config”, and the following page appears.

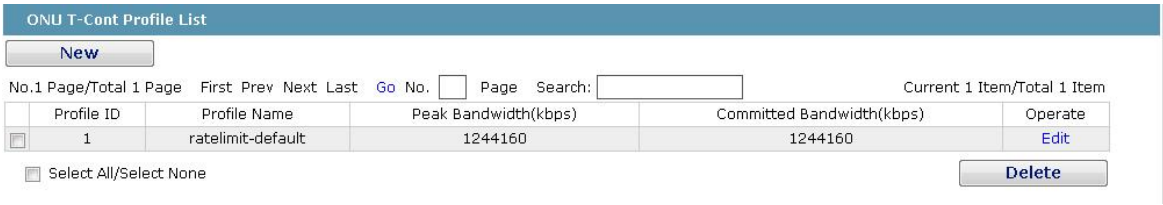


Figure 5-4: ONU T-Cont Profile List

On ONU T-Cont Profile List, select a to-be-deleted item, click “Delete” to delete the corresponding ONU profile. The default profile cannot be deleted.

Click “New” or “Edit” to edit the profile on the following page. On the page, you can edit Profile Name or set Peak Bandwidth and Committed Bandwidth. After the configuration is finished, click “Apply” to save the configuration.

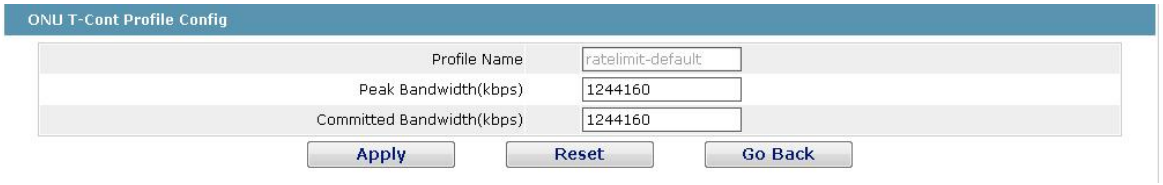


Figure 5-5: ONU T-Cont Profile Config

5.3 ONU Virtual Port Config

On the left navigation bar, click “ONU Config Profile” -> “ONU Rate Virtual Port Config”, and the following page appears.

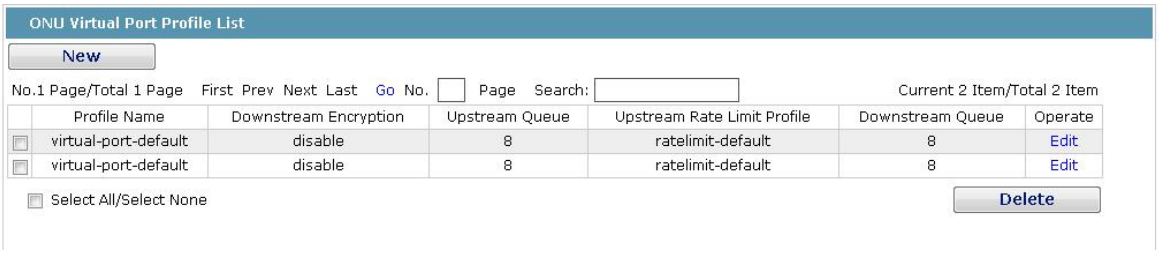


Figure 5-6: ONU Virtual Port Profile List

On ONU Virtual Profile List, select a to-be-deleted item, click “Delete” to delete the corresponding ONU profile. The default profile cannot be deleted.

Click “New” or “Edit” to edit the profile on the following page. On the page, you can edit Profile Name, Downstream Encryption, Upstream Queue, Upstream Rate Limit Profile and Downstream Queue. After the configuration is finished, click “Apply” to save the configuration.

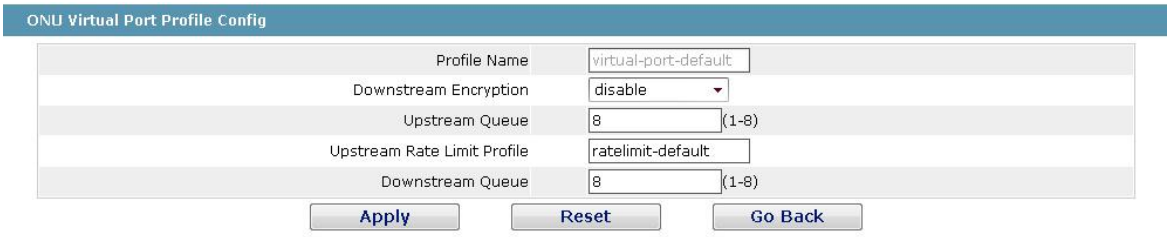


Figure 5-7: ONU Virtual Port Profile Config

5.4 T-Cont Virtual Port Bind Config

On the left navigation bar, click “ONU Config Profile” -> “T-Cont Virtual Port Bind Config”, and the following page appears.

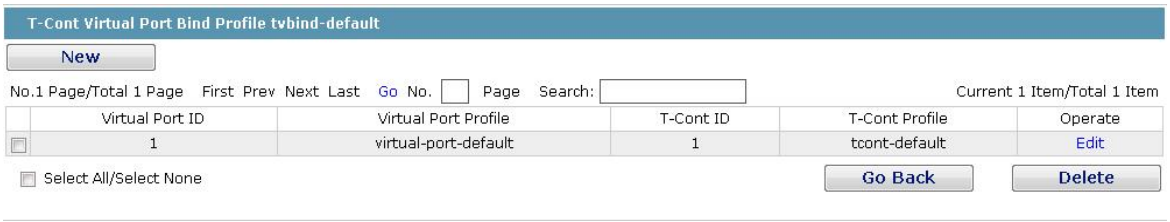


Figure 5-8: ONU T-Cont Virtual Port Bind Profile tvbind-default

On ONU Virtual Profile List, select a to-be-deleted item, click “Delete” to delete the corresponding ONU profile. The default profile cannot be deleted.

Click “New” or “Edit” to edit the profile on the following page. On the page, you can edit Virtual Port ID, Virtual Port Profile, T-Cont ID and T-Cont Profile. After the configuration is finished, click “Apply” to save the configuration.

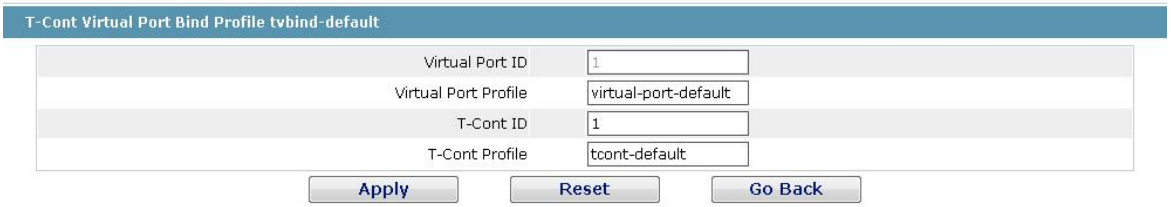


Figure 5-9: ONU T-Cont Virtual Port Bind Profile tvbind-default

5.5 ONU VLAN Config

On the left navigation bar, click “ONU Config Profile” -> “ONU VLAN Config”, and the following page appears.

Figure 5-10: ONU VLAN Profile List

On ONU VLAN Profile List, select a to-be-deleted item, click “Delete” to delete the corresponding ONU profile.

Click “New” or “Edit” to edit the profile on the following page. On the page, you can edit Profile Name, VLAN Mode, Port PVID, VLAN Trunk Allowed, IPoE VLAN, PPPoE VLAN and ARP VLAN.

After the configuration is finished, click “Apply” to save the configuration.

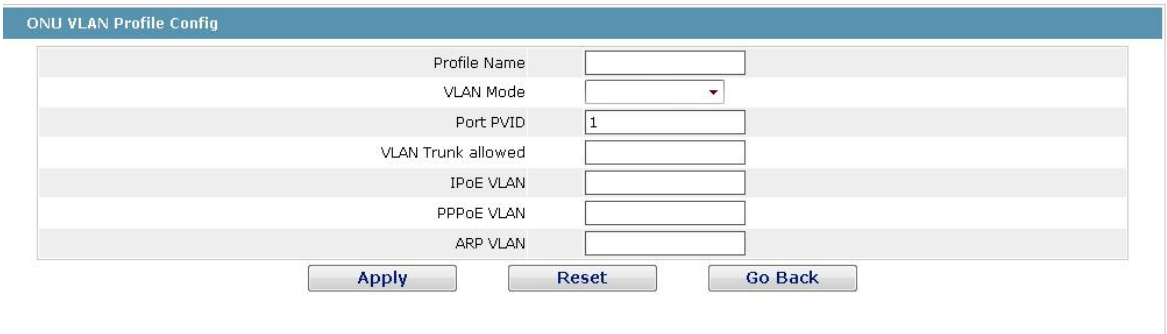


Figure 11: ONU VLAN Profile Config

5.6 ONU Flow Mapping Config

On the left navigation bar, click “ONU Config Profile” -> “ONU Flow Mapping Configuration”, and the following page appears.

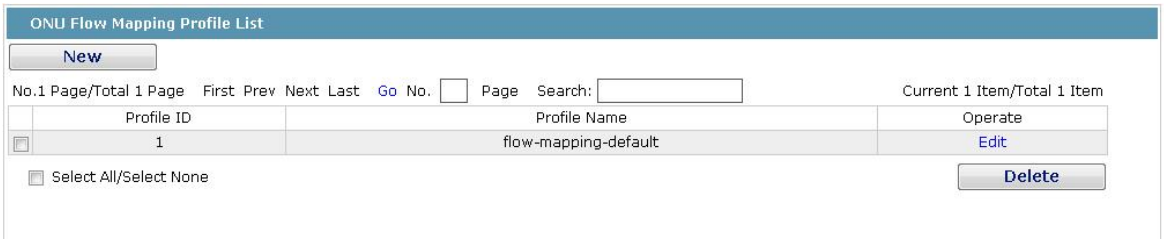


Figure 12: ONU Flow Mapping Profile List

On ONU Flow Mapping Profile List, select a to-be-deleted item, click “Delete” to delete the corresponding ONU profile. The default profile cannot be deleted.

Click “New” or “Edit” to edit the profile on the following page. On the page, you can edit Entry ID, UNI Port Bitmap, VLAN ID, Class of Service and Virtual Port.

After the configuration is finished, click “Apply” to save the configuration.

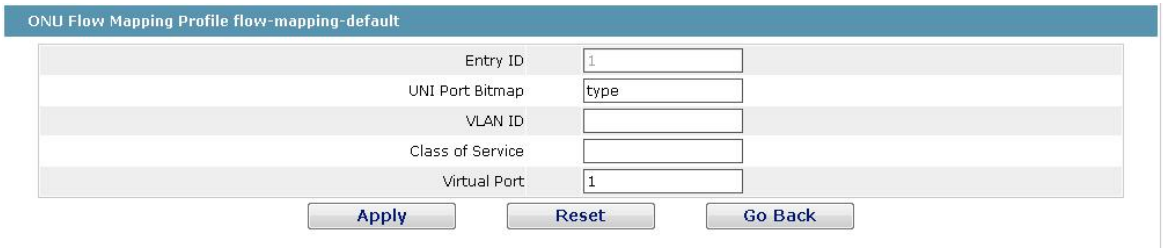


Figure 13: ONU Flow Mapping Profile flow-mapping-default

Chapter 6 ONU Interface Config

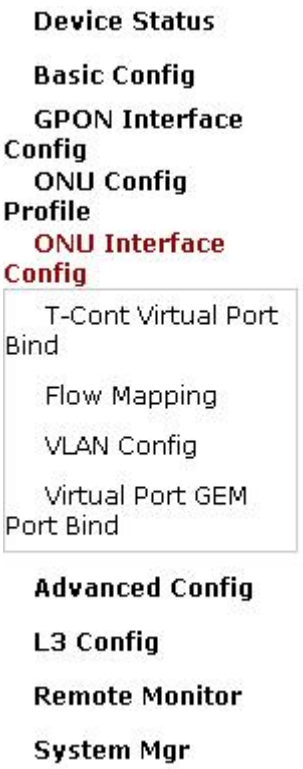


Figure 6-1: ONU Interface Configuration

6.1 T-Cont Virtual Port Bind

On the left navigation bar, click “ONU Interface Config” -> “T-Cont Virtual Port Bind”, and the following page appears.

Figure 6-2: T-Cont Virtual Port Bind

On the page of T-Cont Virtual Port Bind Interface Config, click “Apply” to save the setting or click “Reset” to return to the default setting.

6.2 Flow Mapping

On the left navigation bar, click “ONU Interface Config” -> “Flow Mapping”, and the following page appears.

Figure 6-3: Flow Mapping Interface Configuration

On the page of Flow Mapping Interface Config, click “Apply” to save the setting or click “Reset” to return to the default setting.

6.3 VLAN Config

On the left navigation bar, click “ONU Interface Config” -> “VLAN Config”, and the following page appears.

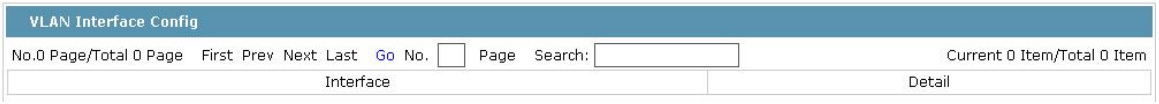


Figure 4: VLAN Interface Configuration

6.4 Virtual Port GEM Port Bind

On the left navigation bar, click “ONU Interface Config” -> “Virtual Port GEM Port Bind”, and the following page appears.

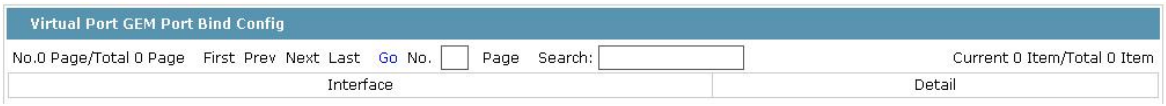


Figure 5: Virtual Port GEM Port Bind Config

Chapter 7 Advanced Config

Figure7-1: Advanced Configuration

7.1 Port Description

On the left navigation bar, click “Advanced Config” -> “Port Description” and the following page appears.

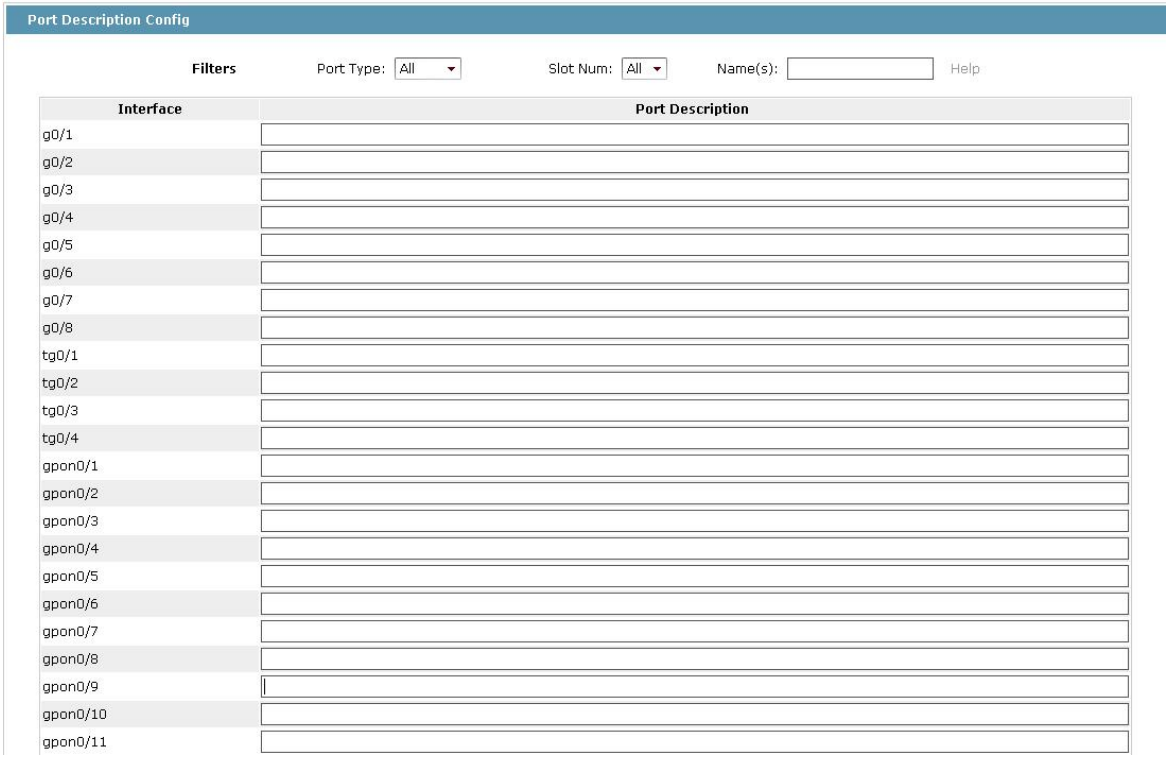


Figure 7-2: Port Description Configuration

On the above page, you can fill in the port description information with at most 120 characters. It does not support configuration of VLAN interface description information at present.

7.2 Port Config

On the left navigation bar, click “Advanced Config” -> “Port Config” and the following page appears.

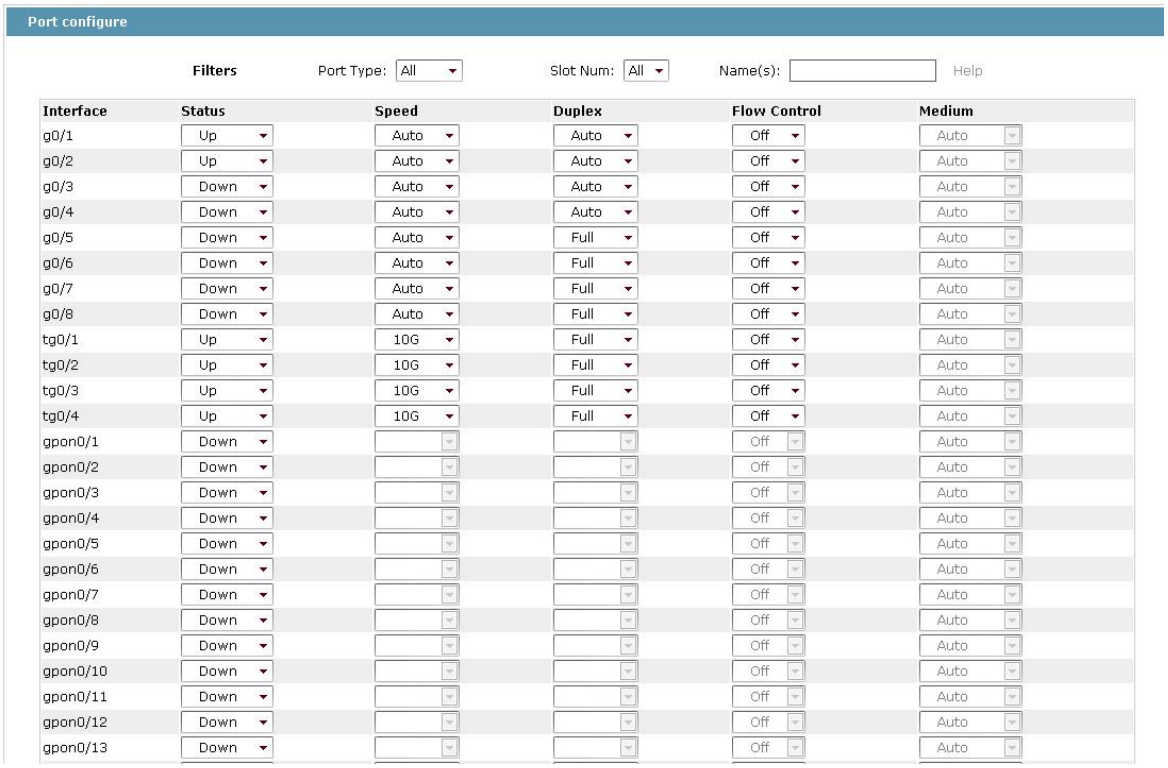


Figure 7-3: Port Configure

On the above page, you can modify the status, speed, duplex and flow control of the interface.

Note:

If the interface rate or the duplex mode is modified, the interface link status may be switched, affecting the network communication.

7.3 Rate Limit

On the left navigation bar, click “Advanced Config” -> “Rate Limit” and the following page appears.

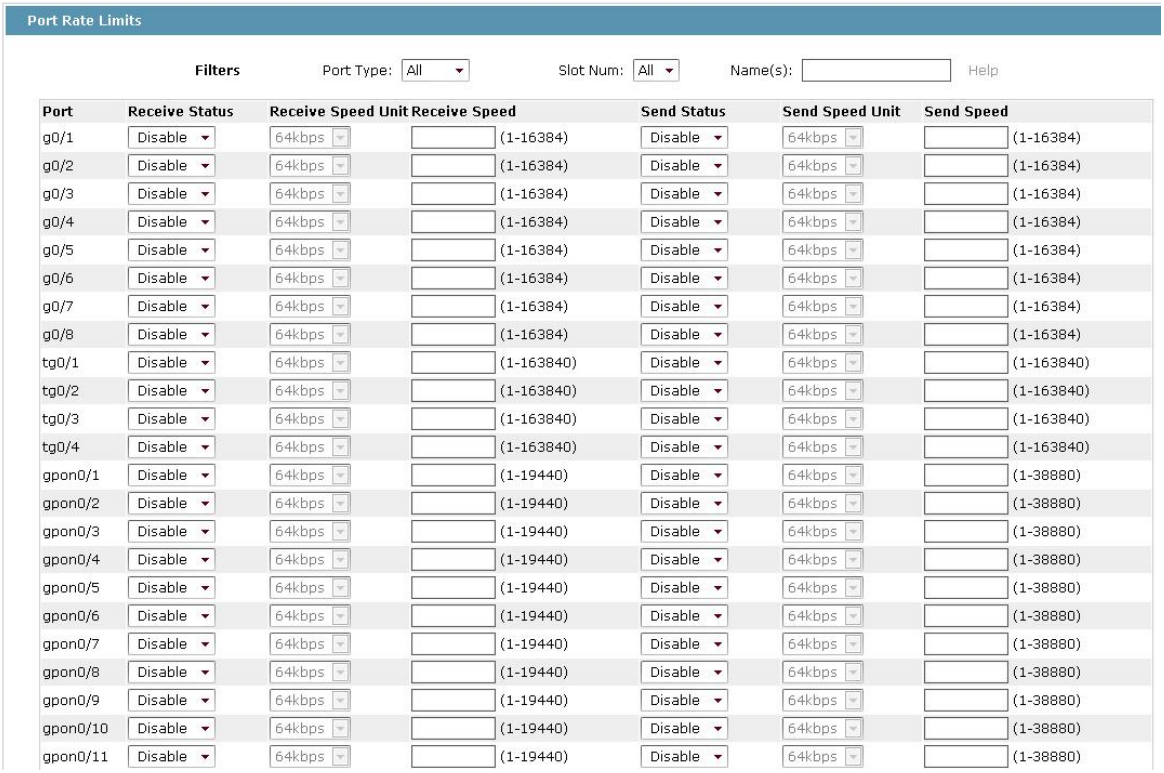


Figure 4: Port Rate Limits

On the above page, you can modify the Receive Status, Receive Speed, Send Status and Send Speed. The rate limit is invalid for PON ports.

7.4 Port Mirror

On the left navigation bar, click “Advanced Config” -> “Port Mirror” and the following page appears.

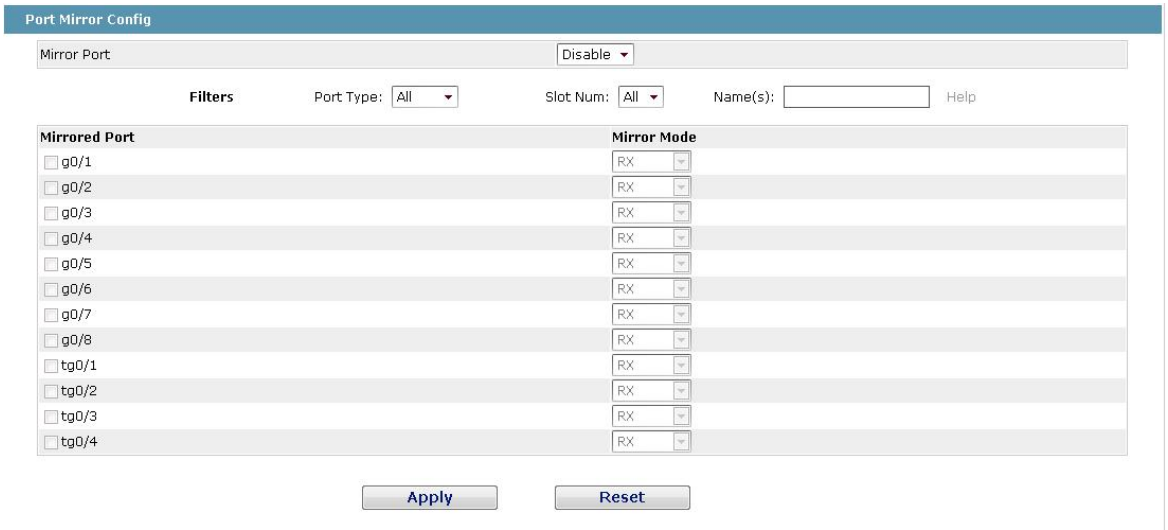


Figure 5: Port Mirror Config

On the right dropdown box of the “Port Mirror Config”, select a Mirrored Port as the destination port.

Click the check box to select the source port of port mirror.

RX	RX means that the received packet will be mirrored to the destination port.
TX	TX means that the forwarded packet will be mirrored to the destination port.
RX & TX	The received port and the forwarded packet will be mirrored simultaneously.

7.5 VLAN Config

7.5.1 VLAN Config

On the left navigation bar, click “Advanced Config” -> “VLAN Config” -> “VLAN Config” and the following page appears.

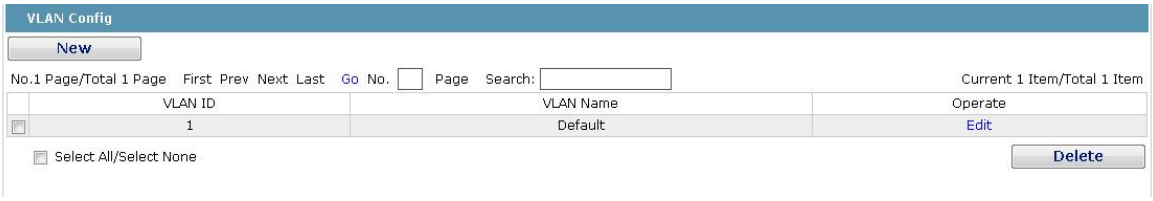


Figure 6: VLAN Config

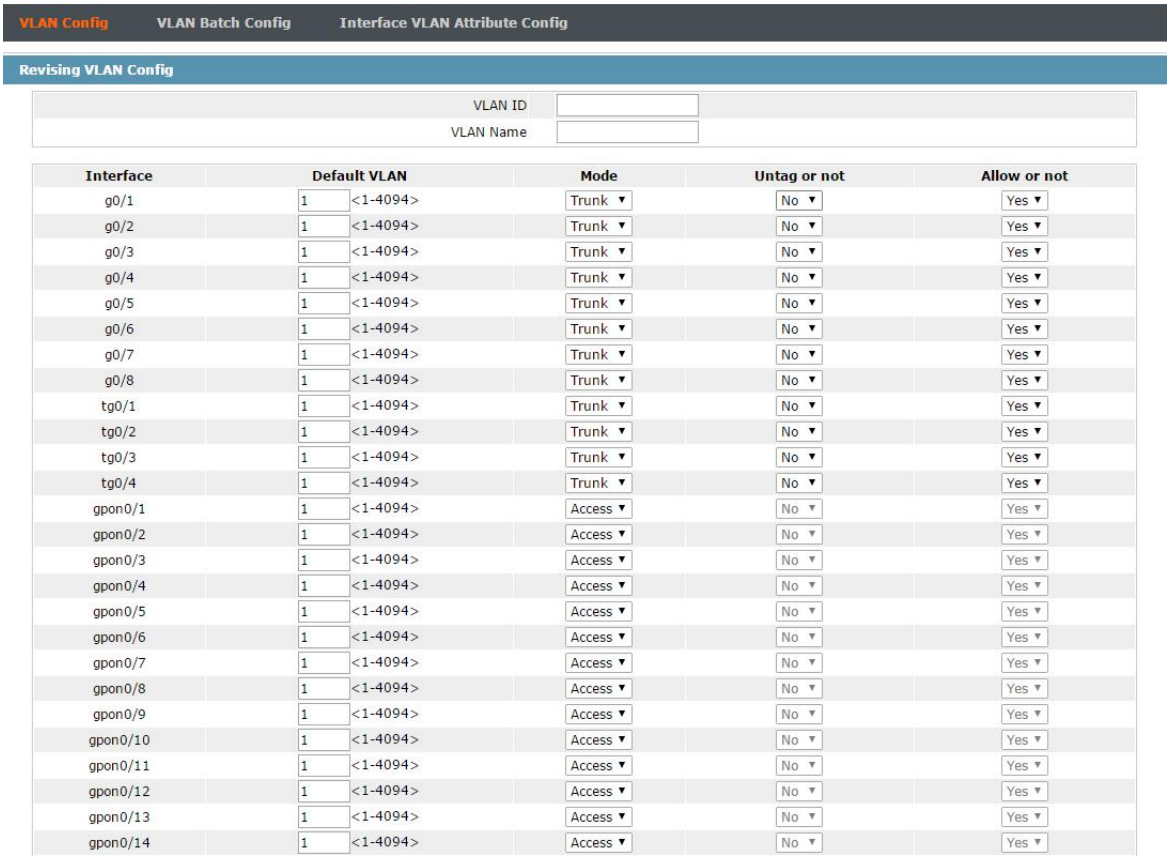
On the above page, the VLAN items are listed out in ascending sequence.

Click “Pre” below “New” to check the VLAN items before the current page; click “Next” to check the VLAN items after the current page. Or you can find out an item by input its VLAN ID or its VLAN Name in the box beside “Search”.

Note:
On the page of “VLAN Config” at most 100 entries can be displayed. If changing the number of displayed entries, enter the global configuration mode by Console port or Telnet to OLT, and run command “ip http web max-vlan”.

Tick an item and click “Delete” to delete it.

Click “New” on the top left of the interface, and the following page appears. On this page, you can add a new VLAN. If creating a new VLAN, fill in the VLAN ID. The VLAN name can be empty.



Or you can click “Edit” on the right of the interface of “VLAN Config”, and the following page appears. On this page, you can modify the attribute of a VLAN.

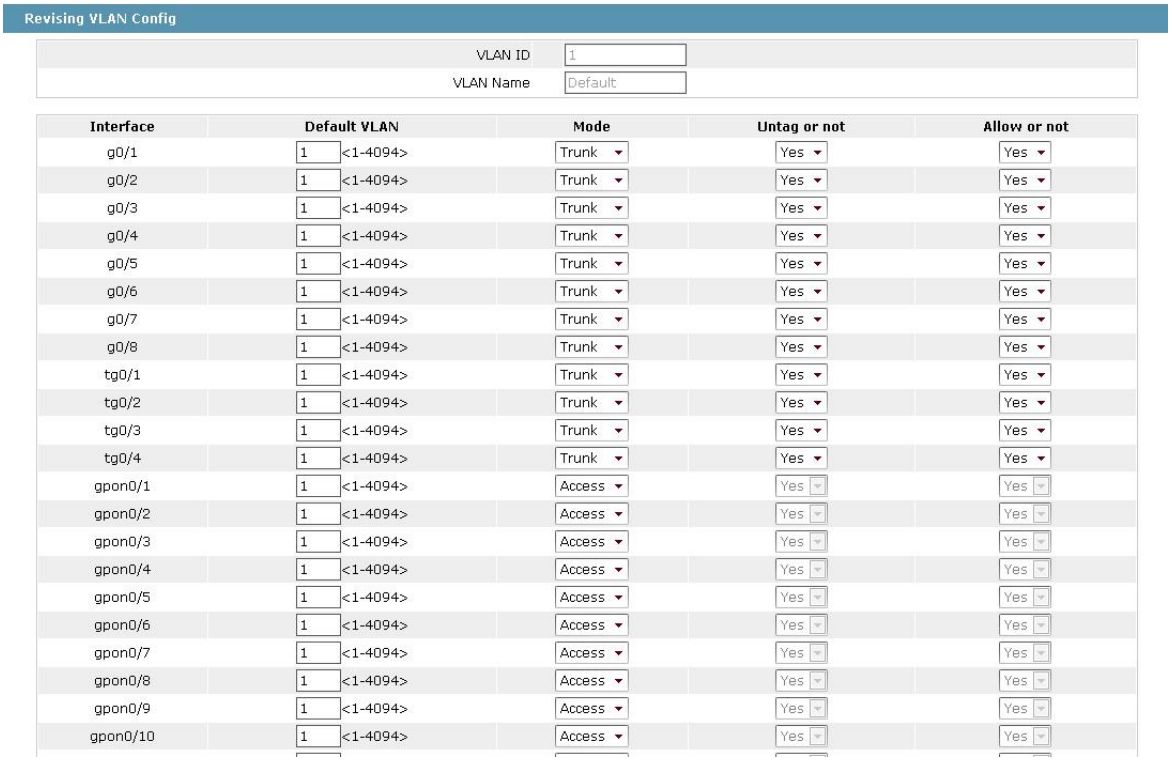
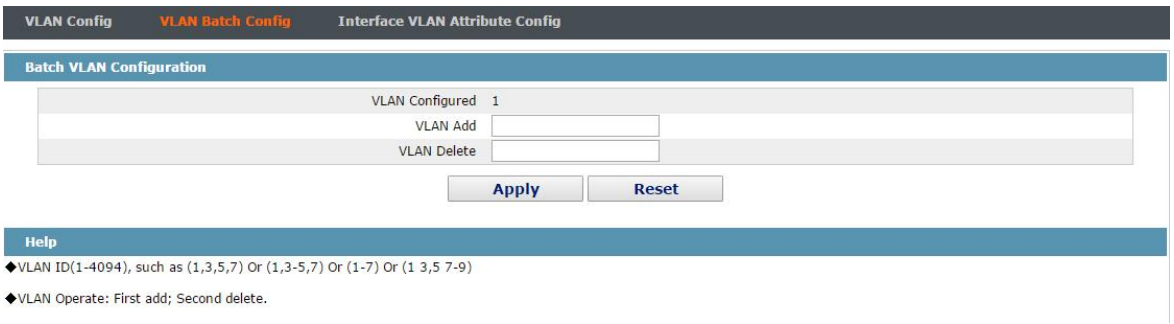


Figure 7-7: Revising VLAN Configuration

7.5.2 VLAN Batch Config

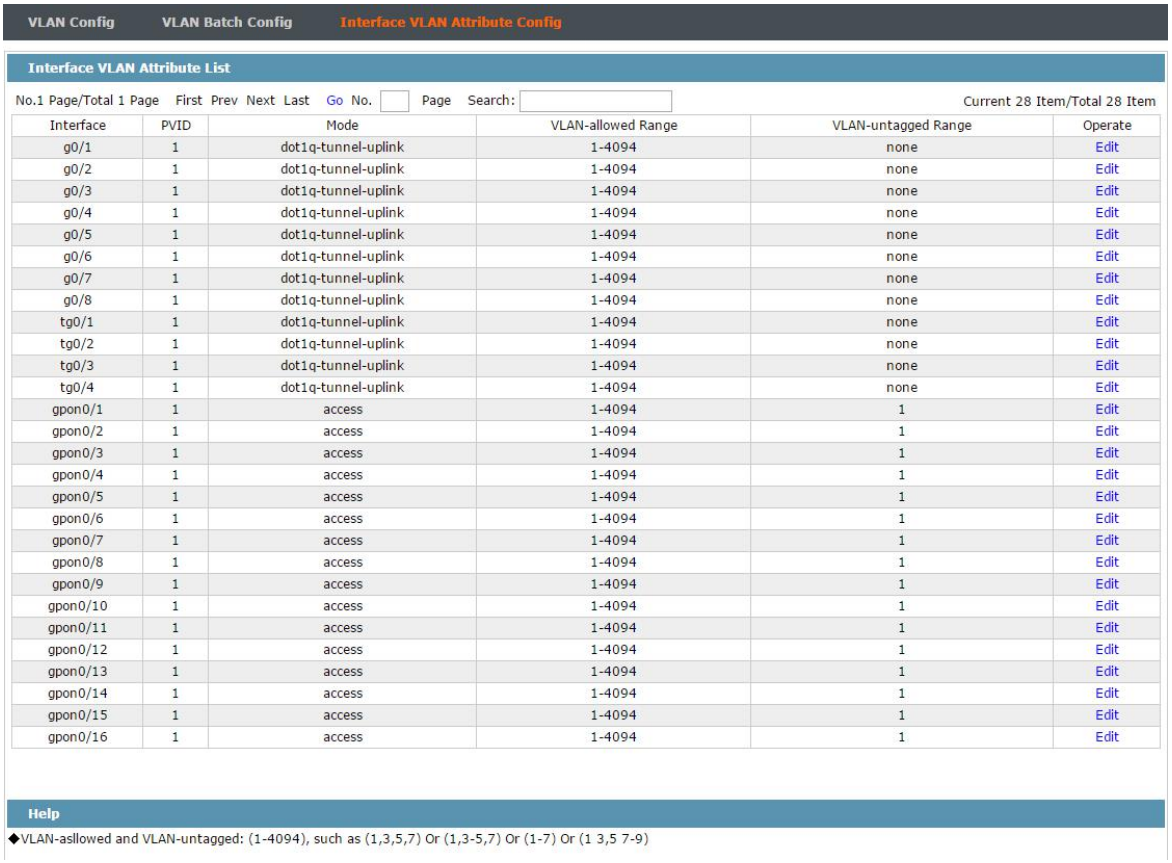
On the left navigation bar, click “Advanced Config” -> “VLAN Config” -> “VLAN Batch Config” and the following page appears.



On the page, you can batch add or delete VLANs.

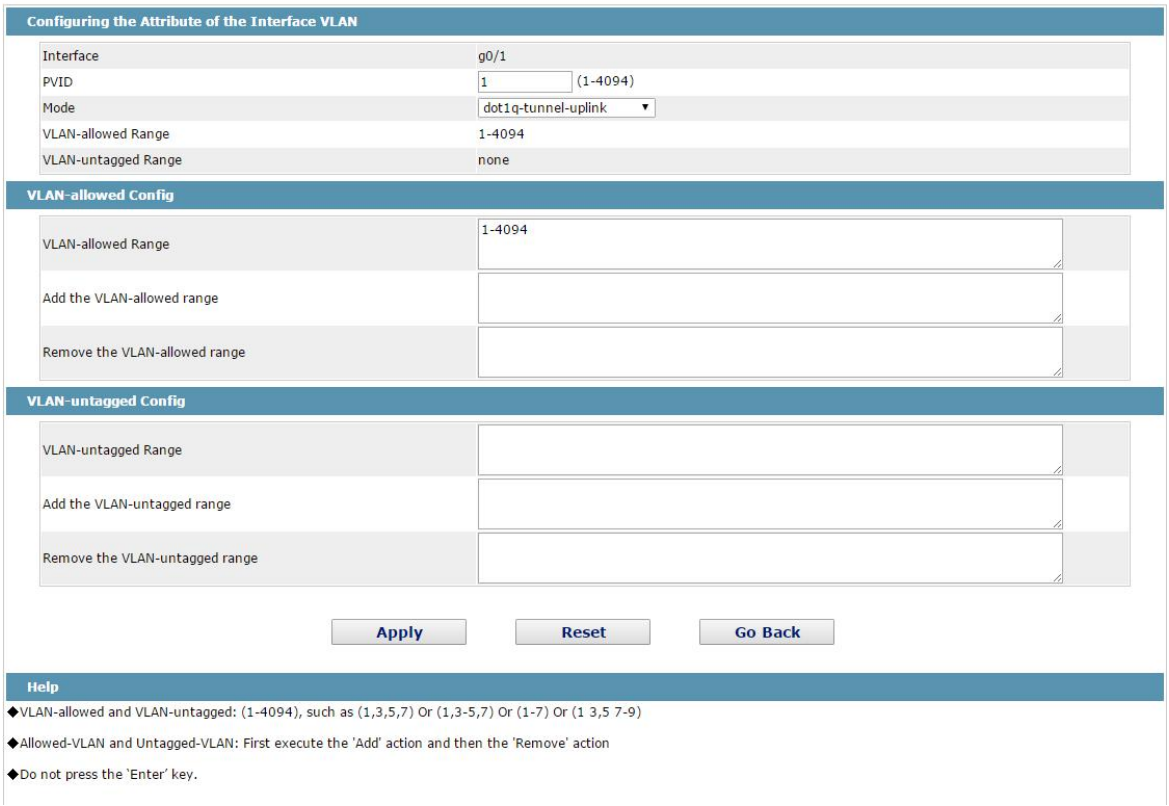
7.5.3 Interface VLAN Attribute Config

On the left navigation bar, click “Advanced Config” -> “VLAN Config” -> “Interface VLAN Attribute Config” and the following page appears.



On this page, you can see “Interface VLAN Attribute List”.

Click “Edit” on the right of an item, and you can modify the port’s PVID, Mode, VLAN-allowed Range, VLAN-untagged Range, VLAN-allowed Config and VLAN-untagged Config.



On this page, you can configure the attribute of the interface VLAN, such as Mode (Trunk or Access), VLAN allowed range and VLAN-untagged range.

Note:

In case the interface in Trunk mode works as the egress, only the default VLAN will be untagged by default.

7.6 VLAN Interface

On the left navigation bar, click “Advanced Config” -> “VLAN Config” and the following page appears.

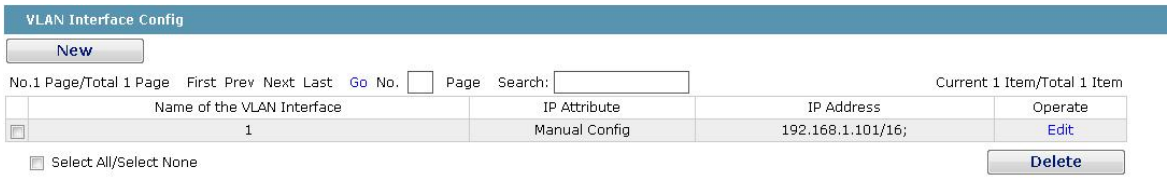


Figure 7-9: VLAN Interface Config

Click “New” to add a new VLAN interface configuration. Click “Delete” to delete the VLAN interface. Click “Edit” to edit the VLAN interface configuration.

Click “New” to modify the VLAN Interface Name; click “Reset” to change the information of “VLAN Interface Config”. The VLAN interface name cannot be modified.

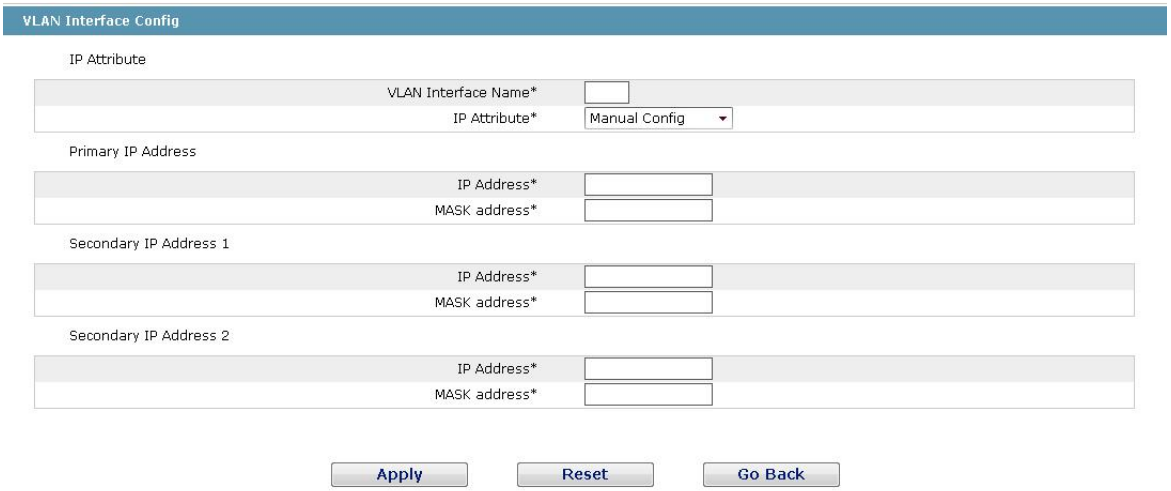


Figure 7-10: VLAN Interface Configuration Page

Note:
Before configuring VLAN interface auxiliary IP, the master IP must be configured first.

7.7 LLDP Config

On the left navigation bar, click “Advanced Config” -> “LLDP Config” and the following page appears.

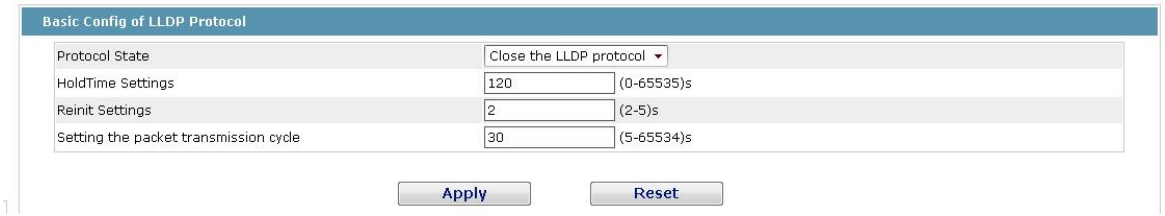


Figure 7-11: Basic Config of LLDP Protocol

Enter LLDP global configuration by default. On the page, you can configure Protocol State, HoldTime Settings, Reint Settings and Setting the packet transmission cycle.

7.8 STP Config

7.8.1 STP State

On the left navigation bar, click “Advanced Config” -> “STP Config” and the following page appears. It includes three parts: Root STP Config, Local STP Config, and STP Port’s State.

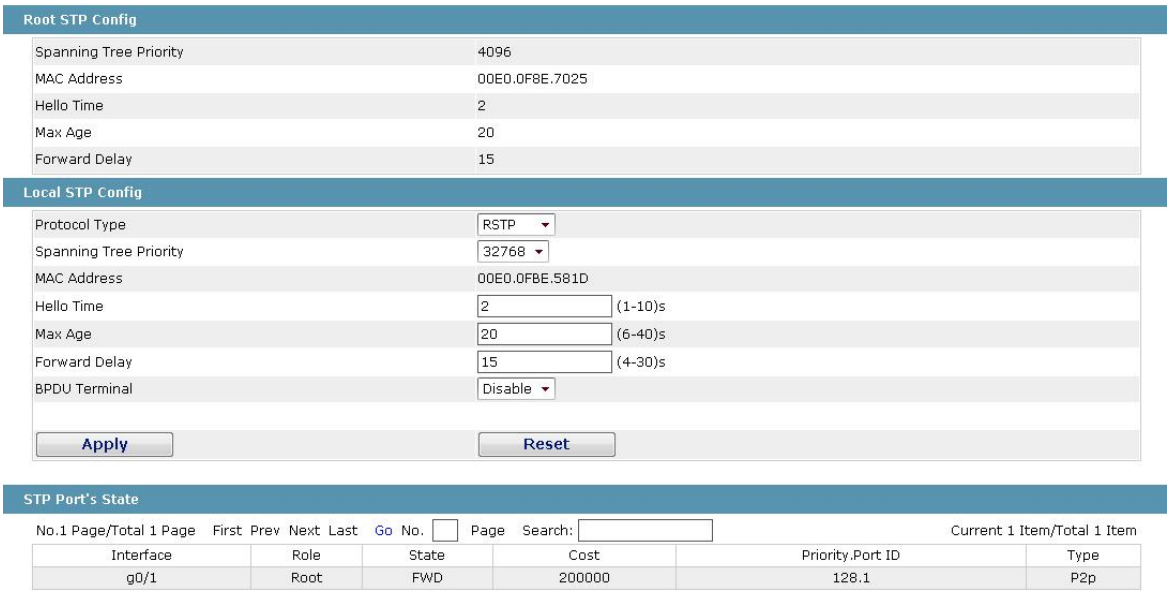


Figure 7-12: STP Global Attribute Configuration

Among the above three parts, Root STP Config and STP Port's State are read only.

In local STP configuration, select the Protocol Type in the dropdown box on the right. It supported mode includes SSTP, RSTP and disable STP.

The priority and time parameter be configured vary with the mode.

Note:
Changing STP mode may cause network interruption.

7.8.2 STP Port Config

Click "STP Port's State" to enter the corresponding configuration interface.

There is irrelevant between the port state configuration and global STP mode. For instance, if the port state is configured to "disable" and then changes to STP mode, the port will not work.

The path cost of the port is 0 by default, which means the path cost will be calculated according to the port rate. If the path cost needs to be changes, enter a value beyond 0.

7.9 Static MAC Config

On the left navigation bar, click "Advanced Config" -> "Static MAC Config" and the following page appears.

Figure 7-13: Static MAC Address List Info

On the page, you can check the static MAC address configuration information. Click “Delete” to delete an item. Click “New” and “Edit” to configure static MAC address.

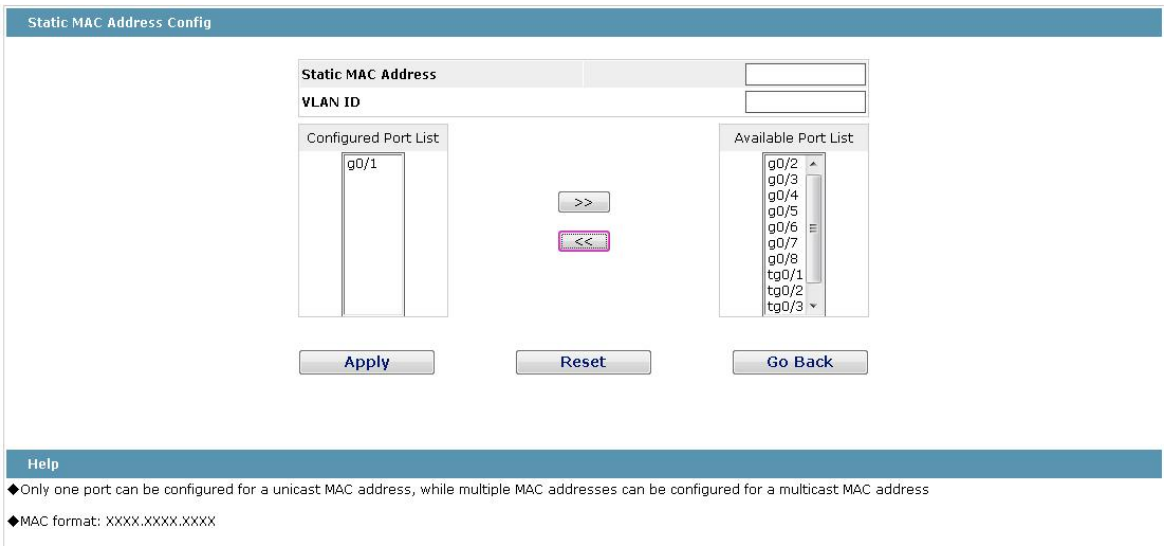


Figure 7-14: Static MAC Address Config

On the above page, you can configure MAC address, VLAN ID and available port list. Click “Apply” to save the setting.

7.10 Port Security

7.10.1 IP Bind

On the left navigation bar, click “Advanced Config” -> “Port Security” and the following page appears.

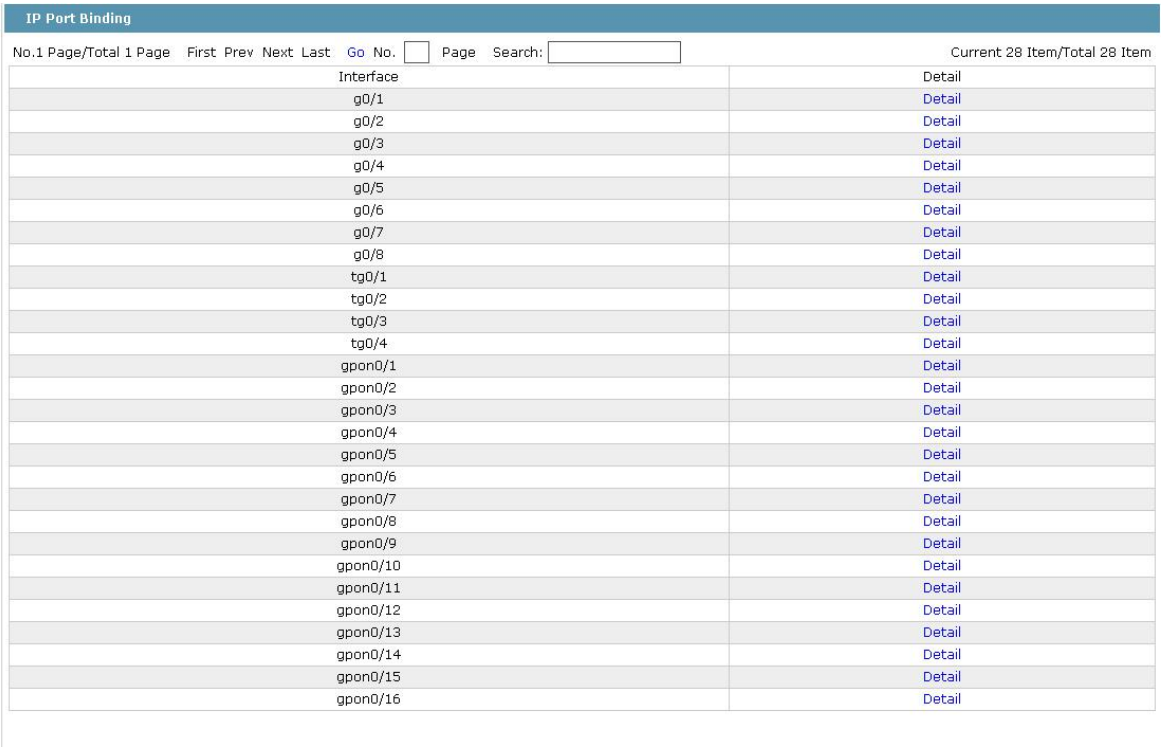


Figure 15: IP Port Binding

Click “Detail” to bind the source IP address for each physical port, which limits the port available IP address.

Figure 16: IP-Bind Rule Info

7.10.2 MAC Bind

On the left navigation bar, click “Advanced Config” -> “Port Security” and the following page appears. Click MAC Binding on the page, and the following page pops up:

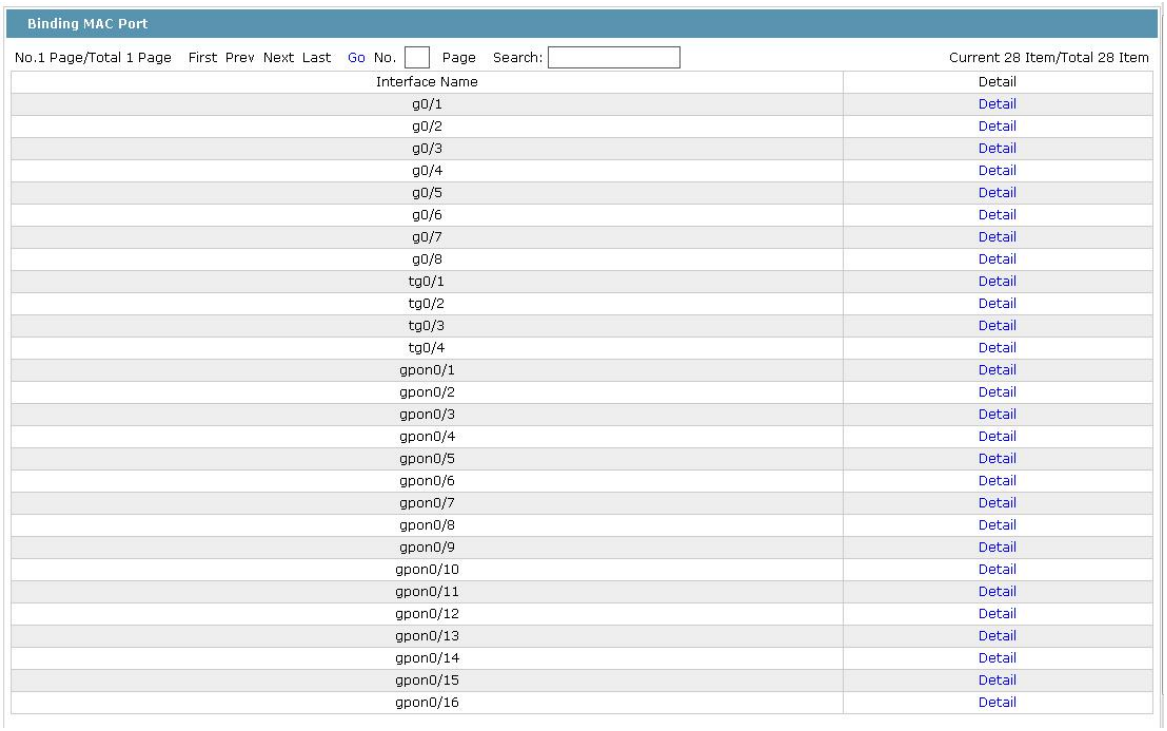


Figure 7-17: Binding MAC Port

Click “Detail” to bind source MAC address for each physical port, so that set limitation on the available MAC address of the port.

Figure 7-18 MAC Bind Rule Info

7.10.3 Static MAC Filtration Mode

On the left navigation bar, click “Advanced Config” -> “Port Security” -> “Static MAC Filter Mode” and the following page appears.

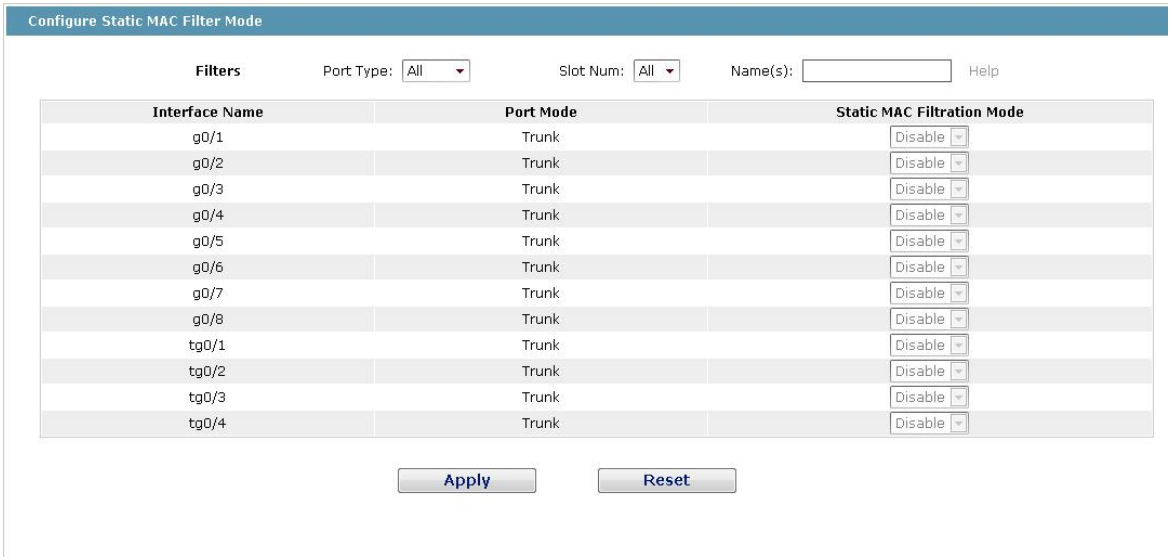


Figure 7-19 Configure Static MAC Filter Mode

On the above page, you can configure static MAC filter mode. By default, the static MAC filter mode is not enabled. The static MAC filter mode cannot be configured on the port in the trunk mode.

7.10.4 Static MAC Filtration Entry

On the left navigation bar, click “Advanced Config” -> “Port Security” -> “Static MAC Filter Item” and the following page appears.

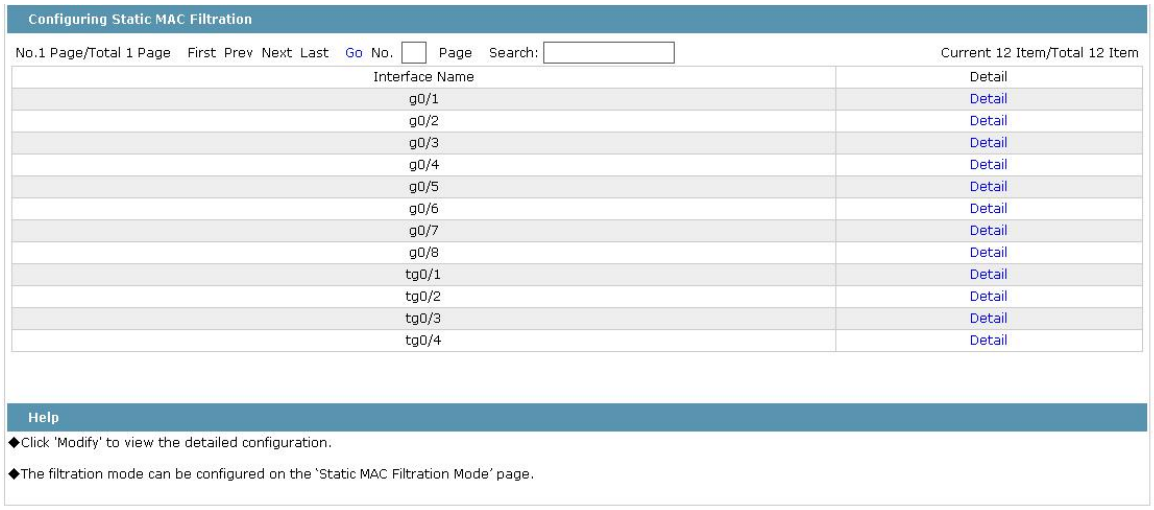


Figure 7-20 Configuring Static MAC Filtration

Click “Detail” to bind the source IP address for each physical port. Enable or disable MAC address of the port according to the static MAC filter mode.

Figure 7-21: Static MAC Filtration Rule Info

7.10.5 Dynamic MAC Filtration Mode

On the left navigation bar, click “Advanced Config” -> “Port Security” -> “Dynamic MAC Filter Mode” and the following page appears.

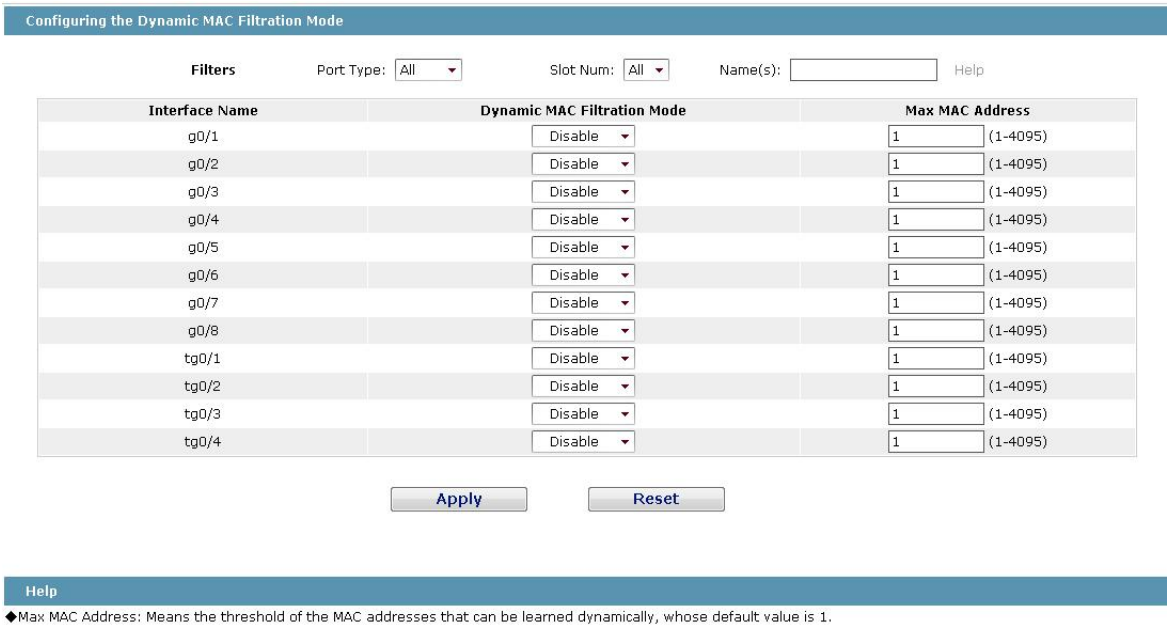


Figure 7-22: Configuring the Dynamic MAC Filtration Mode

On the page, you can configure the Dynamic MAC Filtration Mode and Max MAC Address. By default, MAC filtration mode is disabled and the max address number is 1.

7.11 Storm Control

On the left navigation bar, click “Advanced Config” -> “Storm Control” and the following page appears. On the page, you can configure “Broadcast Storm Control”, “Multicast Storm Control” and “Unknown Unicast Storm Control”.

7.11.1 Broadcast Storm Control

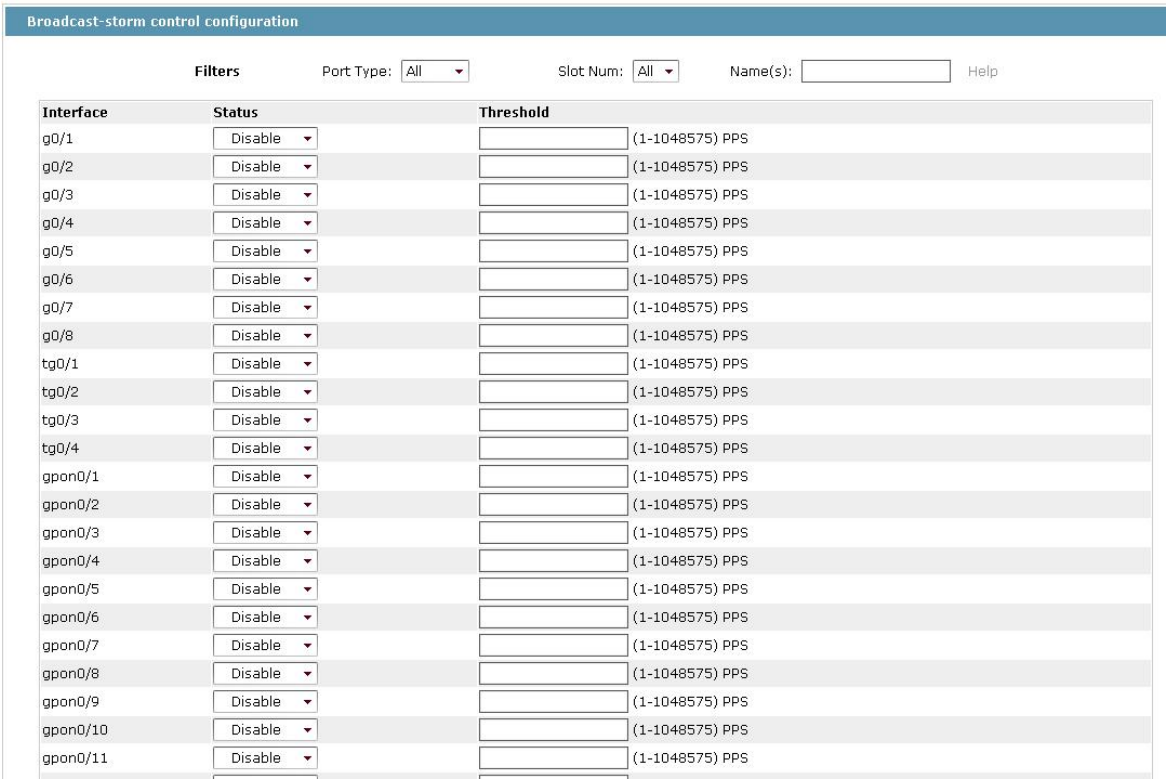


Figure 7-23: Broadcast Strom Control Configuration

“Enable” or “Disable” the broadcast storm control in the dropdown box below “Status”. Input the threshold of the port dealing processing the broadcast packet in the column “Threshold”. Each port shows its legal range of the threshold.

7.11.2 Multicast Storm Control

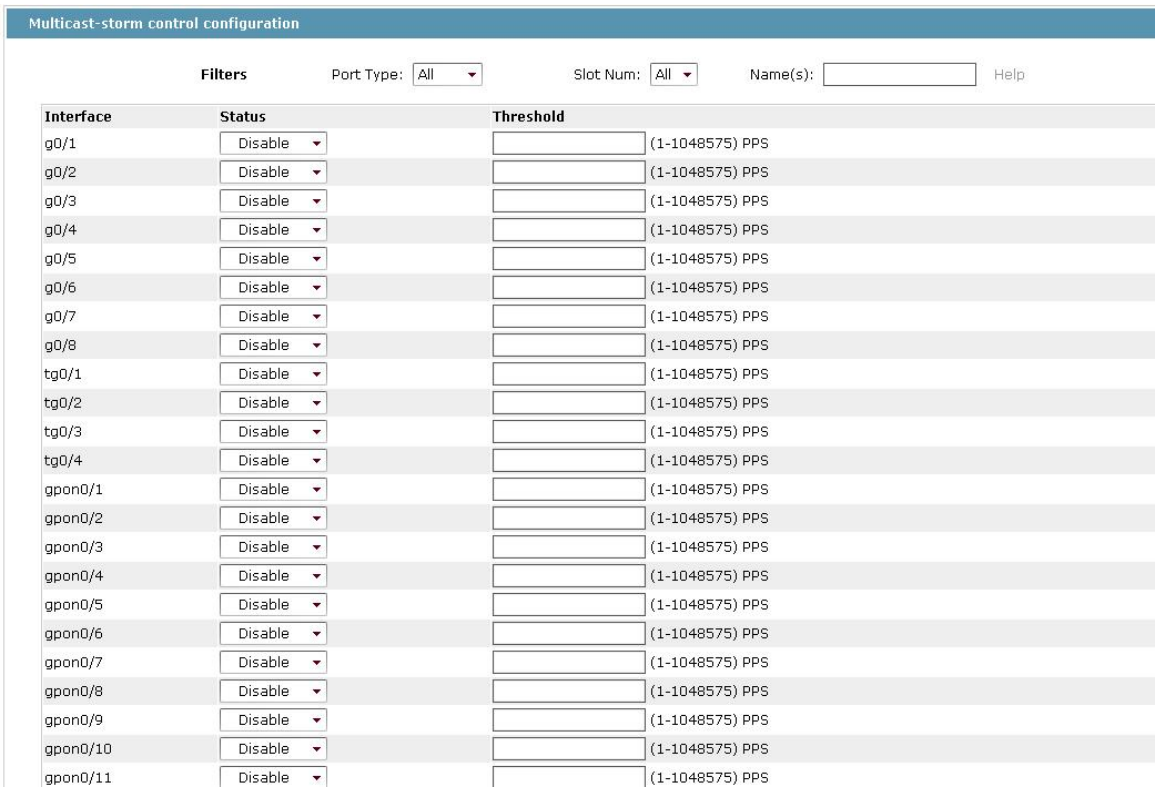


Figure 7-24: Multicast-storm Control Configuration

"Enable" or "Disable" the multicast storm control in the dropdown box below "Status". Input the threshold of the port processing the broadcast packet in the column "Threshold". Each port shows its legal range of the threshold.

7.11.3 Unknown Unicast Storm Control

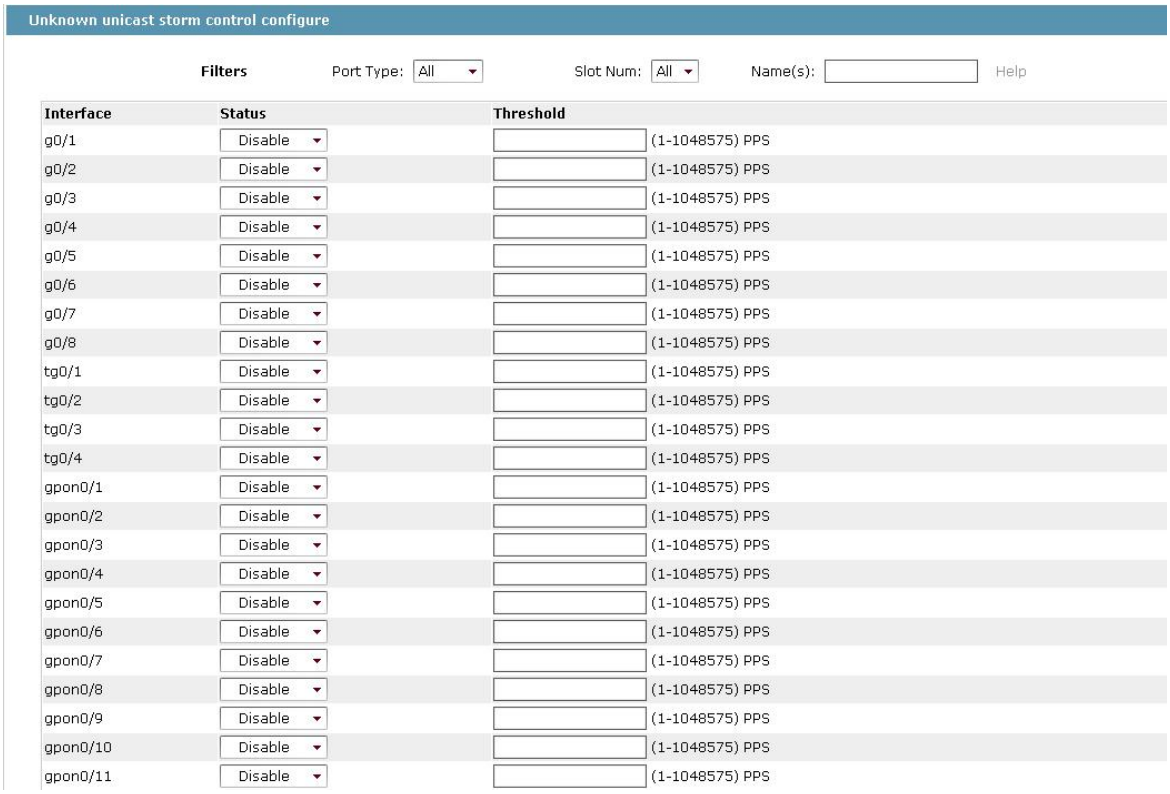


Figure 7-25 Unknown Unicast Storm Control Configuration

"Enable" or "Disable" the unknown unicast storm control in the dropdown box below "Status". Input the threshold of the port processing the broadcast packet in the column "Threshold". Each port shows its legal range of the threshold.

7.12 IP Access List

7.12.1 IP Access List Config

On the left navigation bar, click "Advanced Config" -> "IP Access List" -> "IP Access List Config" and the following page appears.

Figure 7-26 IP ACL Config

Click "New" on the top left of the interface to add an IP ACL List. Click "Delete" to delete the selected IP ACL List.

If you click "New" on the top left of the interface, the following page will appear:

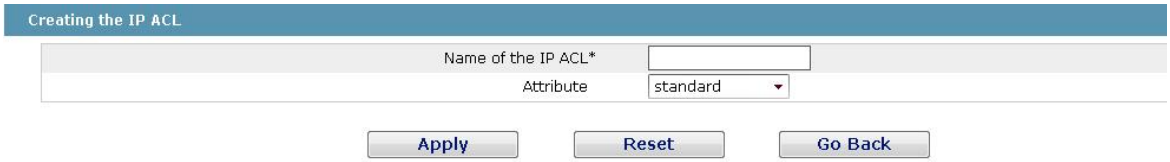
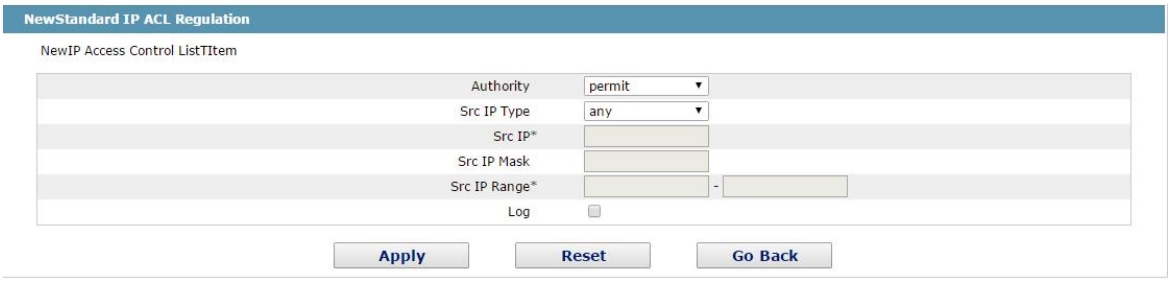


Figure 7-27: Creating the IP ACL

(1) NewStandard IP ACL Regulation

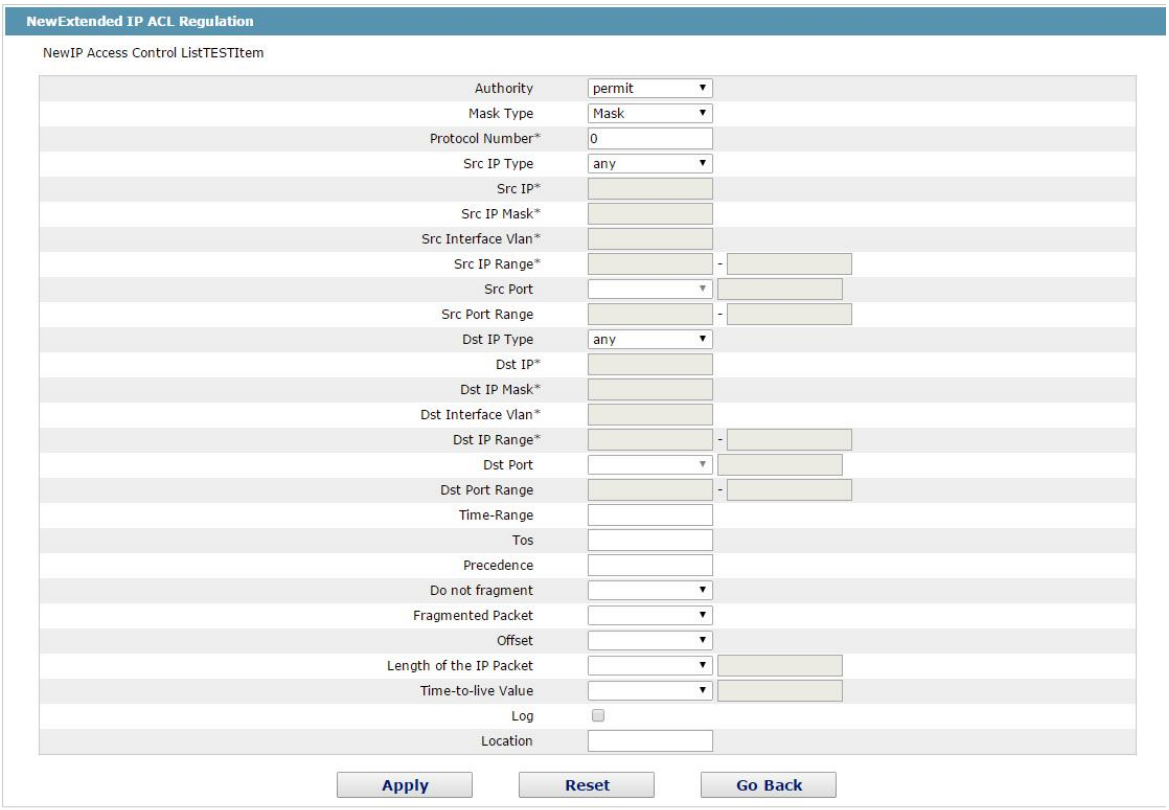
If you select “standard” in the right dropdown box of the **Attribute**, the following page will pop up:



On the above page, you can add a NewStandard ACL Regulation. Click “Reset” to change the regulation.

(2) NewStandard IP ACL Regulation

If you select “extended” in the right dropdown box of the **Attribute**, the following page will pop up:



7.12.2 IP Access List Application

On the left navigation bar, click “Advanced Config”-> “IP Access List” -> “IP Access List Application” -> “IP Access List Application”, and the following page appears.

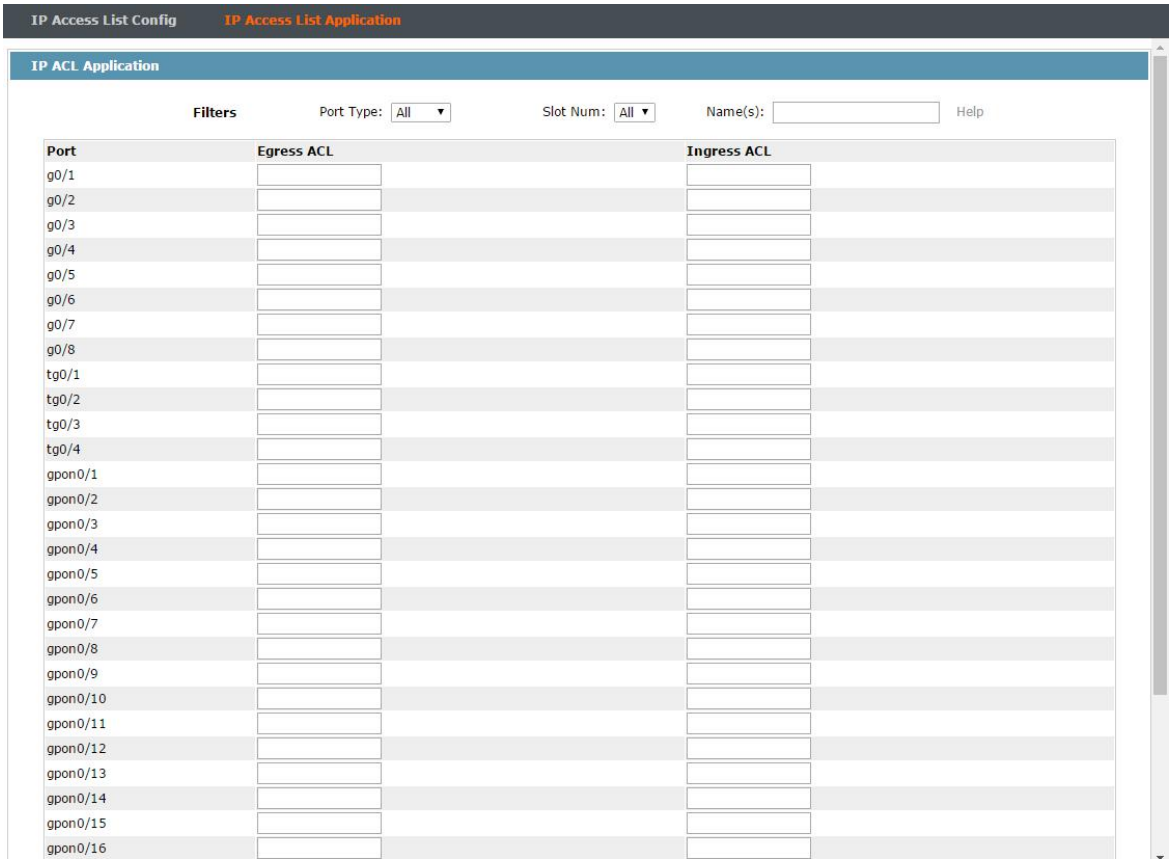


Figure 7-28: IP ACL Application

7.13 MAC Access List

7.13.1 MAC Access List Config

On the left navigation bar, click “Advanced Config” -> “MAC Access List” -> “MAC Access List Config”, and the following page appears.

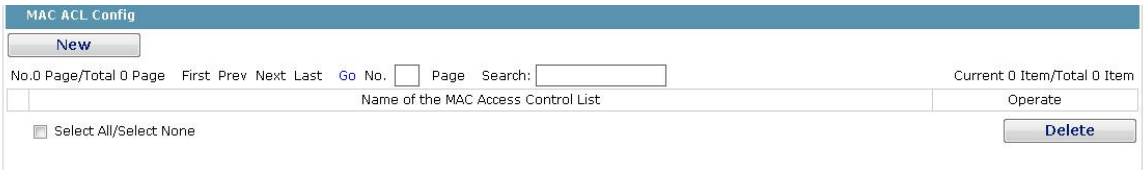


Figure 7-29: MAC ACL Config

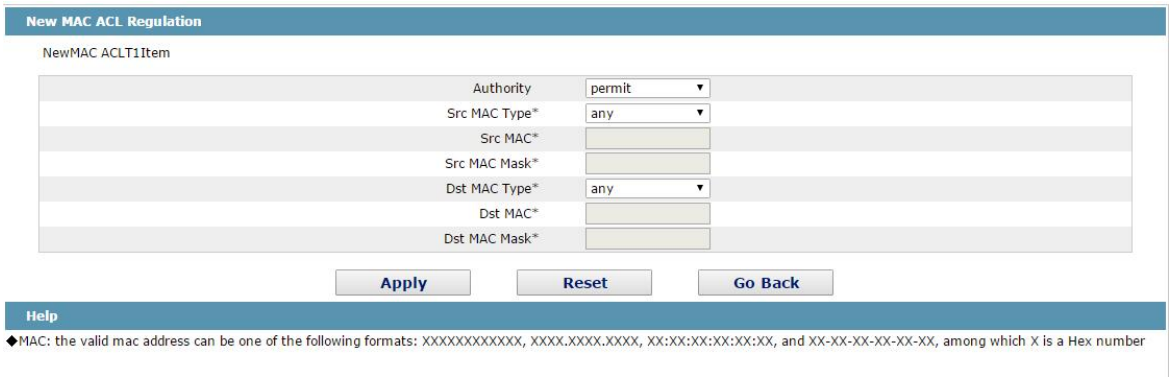
Click “New” On the above page and the following page appears. You can add a new MAC access control list on the following page.

You can also tick an item on the page of “MAC ACL Config” and click “Delete” to delete the ACL.

Figure 30: Creating MAC ACL

New MAC ACL Regulation

Select an ACL On the page of “MAC ACL Config, click “Edit” and then click “New” on the pop-up interface. The following page pops up thereafter. On the page, you can configure the “New MAC ACL Regulation”.



7.13.2 MAC Access List Application

On the left navigation bar, click “Advanced Config” -> “MAC Access List” -> “MAC Access Application”, and the following page appears.

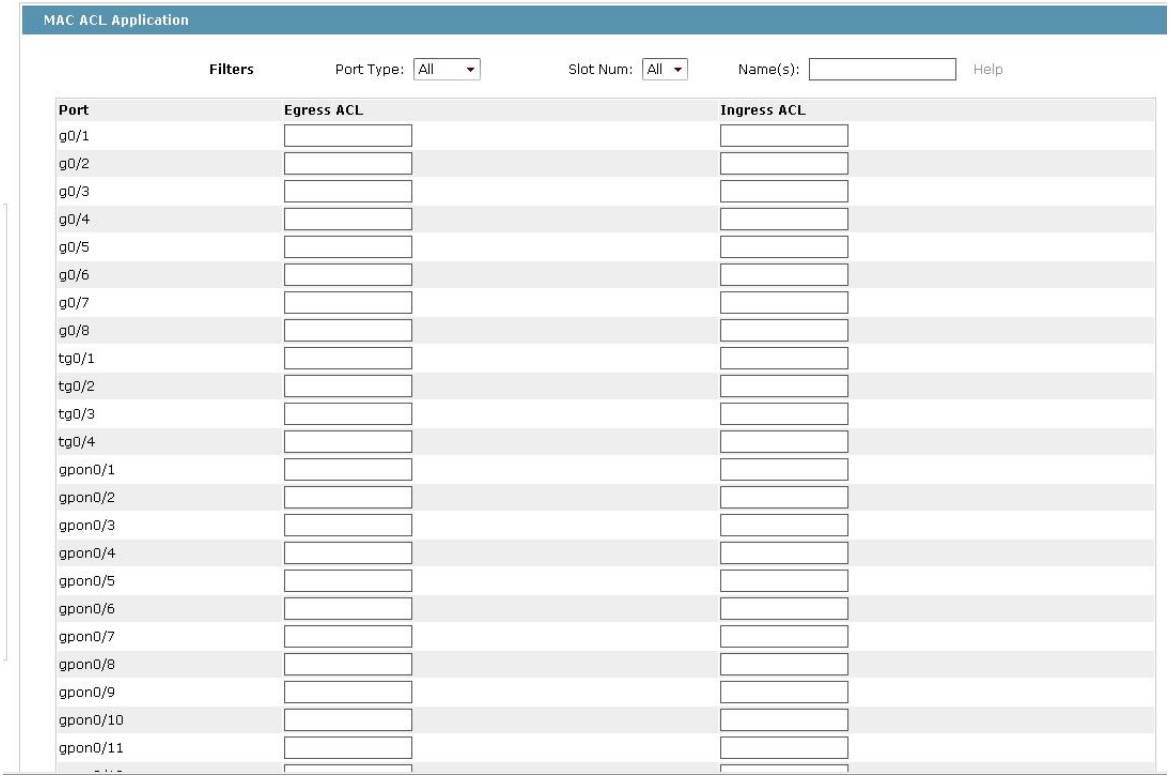


Figure 7-31: MAC ACL Application

7.14 Port Channel

7.14.1 Port Channel

On the left navigation bar, click “Advanced Config” -> “Port Channel” and the following page appears.

Figure 32: Port Aggregation Config

Click “New” on the page and the following page pops up. On the following page, you can configure at most 8 aggregation groups. Each group can configure at most 8 aggregation ports. Select the mode of the aggregation port in the dropdown box behind Mode.

Tick an item on the page of “Port Aggregation Config” and Click “Delete” to delete the aggregation group.

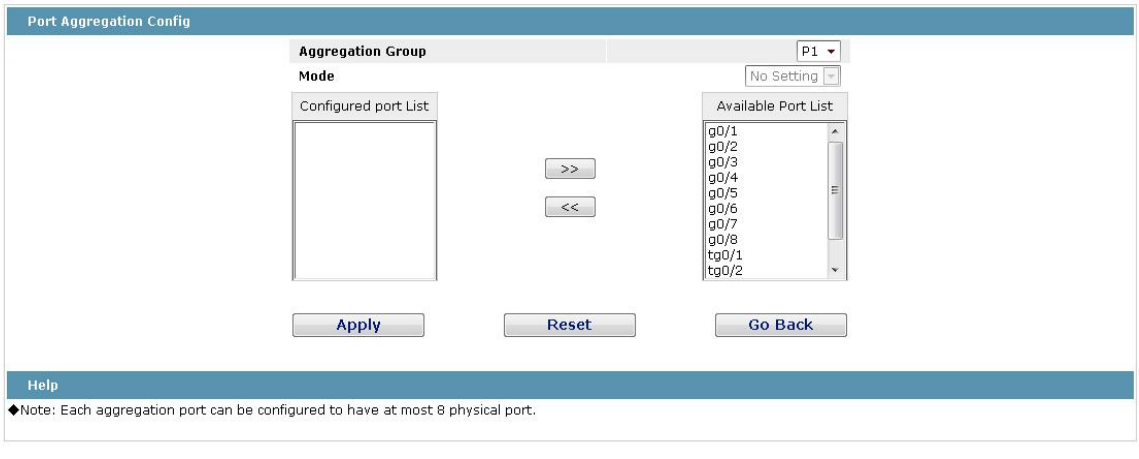


Figure 7-33: Port Aggregation Config

When creating a new aggregation group, it is optional; when modifying the aggregation group, it is not optional.

When the aggregation port exists the member port, you can select the aggregation mode: Static, LACP Active and LACP Passive.

You can delete and add the aggregation member port by “>>” and “<<”.

7.14.2 Port Channel Group Loading Balance

Some devices support load balance based on the aggregation group and some not, but can be configured in the global configuration mode.

GP3616 supports load balance mode based on the aggregation group.

On the left navigation bar, click “Advanced Config” -> “Port Channel” -> “Port Channel Group Loading Balance” and the following page appears.

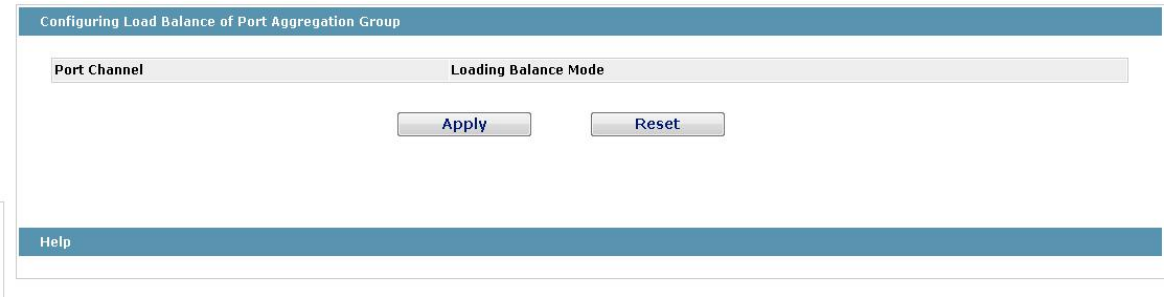


Figure 7-34: Configuring Load Balance of Port Aggregation Group

You can configure different aggregation mode for different aggregation groups.

7.15 Ring Protection

On the left navigation bar, click “Advanced Config” -> “Ring Protection” -> “EAPS Config” and the following page appears.

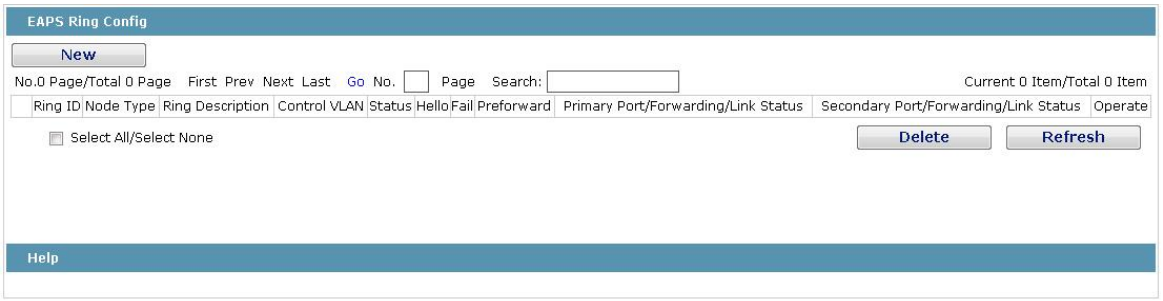


Figure 35: EAPS Ring Config

Select an item and click “Delete” to delete it or click “Refresh” to refresh it. Click “New” on the top left of the interface, and the following page pops up. On the following page, you can configure Node Type, Ring Description, Control VLAN, Hello Time, Fail Time, Preforward Time, Primary Port and Secondary Port.

In “Ring Description”, you cannot enter the “Enter” key.

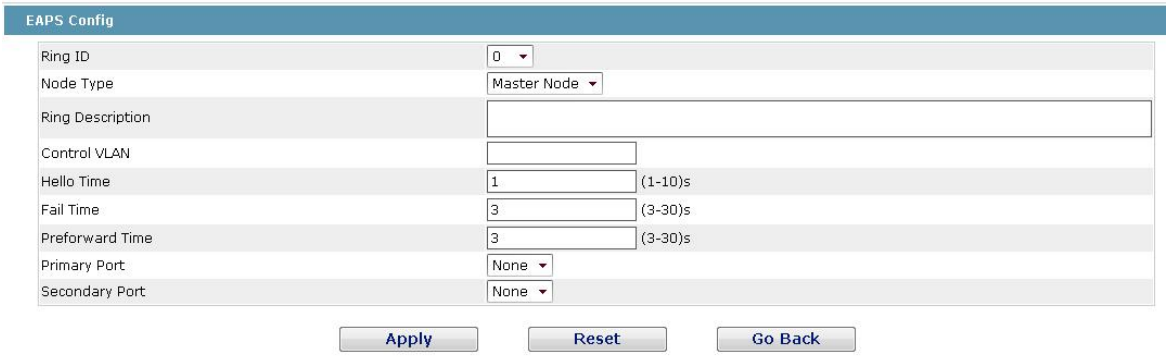


Figure 7-36: EAPS Config

7.16 DDM Config

On the left navigation bar, click “Advanced Config” -> “DDM Config” and the following page appears.

Figure 7-37: MTU Config

You can enable or disable DDM On the page.

7.17 MTU Config

On the left navigation bar, click “Advanced Config” -> “MTU Config” and the following page appears.

Figure 7-38: MTU Config

You can set the size of MTU within a designated range.

Chapter 8 L3 Config

Figure 8-1: L3 Config

8.1 Static Route

On the left navigation bar, click “Advanced Config” -> “Static Route” and the following page appears.

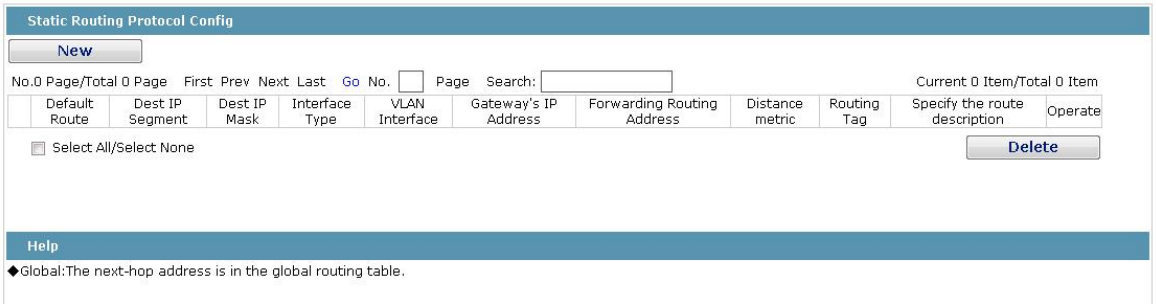


Figure 8-2: Static Routing Protocol Config

Click “New” to add a static route entry, as shown in the following interface.

Tick an item and click “Edit” to modify the static routing entry.

Tick an item and click “Delete” to delete the static routing entry.

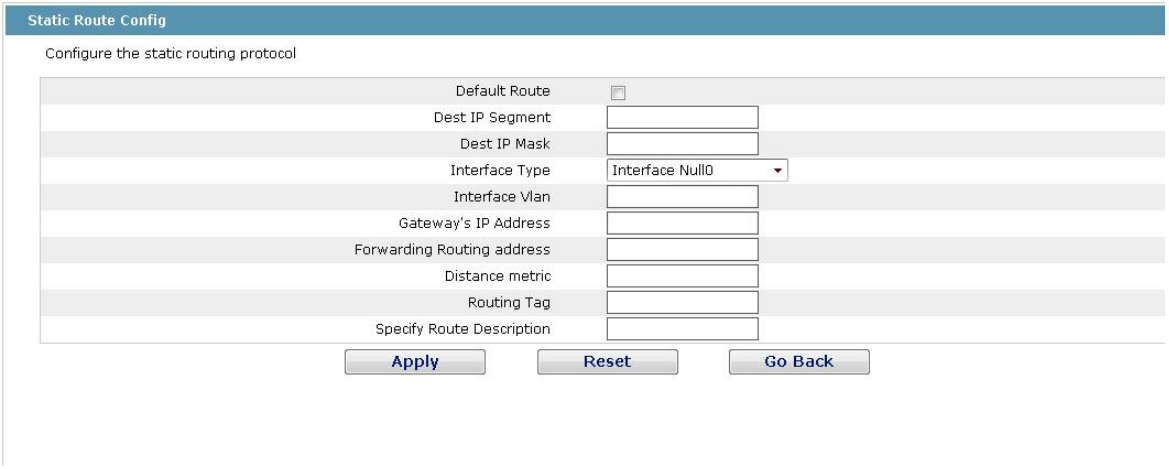


Figure 8-3: Static Route Config

Chapter 9 Remote Monitor

Figure 9-1: Remote Monitor

9.1 SNMP Mgr

9.1.1 SNMP Community Mgr

On the left navigation bar, click “Remote Monitor” -> “SNMP Mgr” -> “SNMP Community Mgr” and the following page appears.

Figure 9-2: SNMP Community Management

You can learn SNMP Community information on the above page. You can also click “New” to create a new SNMP Community.

Tick an item and click “Delete” On the page of “SNMP Community Management” to delete the item.

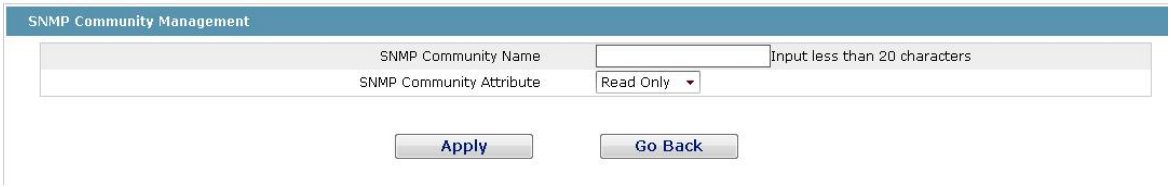


Figure 9-3: SNMP Community Management

On the above page, you can enter the name of SNMP Community Management. You can select “SNMP Community Attribute”: Read Only and Read Write.

9.1.2 SNMP Host Mgr

On the left navigation bar, click “Remote Monitor” -> “SNMP Mgr” -> “SNMP Host Mgr” and the following page appears.

Figure 9-4: SNMP Host Management

Through the interface of SNMP Host Management, you can learn the relevant configuration information of SNMP Host.

On the page, you can create, modify and delete SNMP Host information.

Figure 9-5: SNMP Host Management

On the page of “SNMP Host Management”, you can configure “SNMP Host IP”, “SNMP Community”, SNMP Message Type and SNMP Community Version. SNMP Message Type includes Traps and Informs. For v1 (SNMP Community Version) does not support Informs type.

9.2 RMON

9.2.1 RMON Statistics

On the left navigation bar, click “Remote Monitor” -> “RMON Config” -> “RMON Statistics” and the following page appears.

Figure 9-6: RMON Statistics

On the above page, you can create, edit or delete a RMON information. Click “New” on the top left of the interface or tick an item and click “Edit” in the end of the item line, the following page appears. Here you can designate the Index and Interface.

Figure 9-7: Interface Statistics Config

9.2.2 RMON History

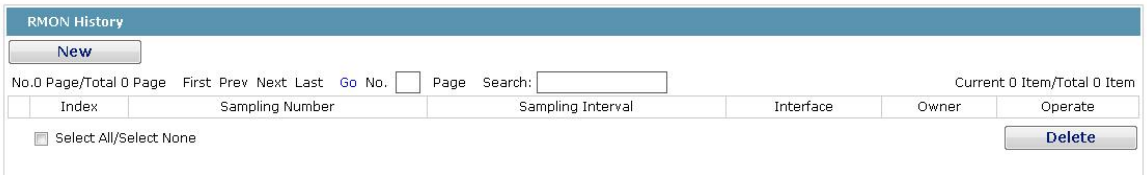


Figure 9-8: RMON History

On the above page, you can create, edit or delete RMON information. Click “New” on the top left of the interface, or tick an item and click “Edit” in the end of the item line, then the following page appears. Here you can configure Index, Sampling Number, Sampling interval, and Owner.

Figure 9-9: Interface History Config

9.2.3 RMON Alarm

Figure 9-10: RMON Alarm

On the above page, you can create, edit or delete RMON information. Click “New” on the top left of the interface, or tick an item and click “Edit” in the end of the item line, then the following page appears. Here you can configure Interface, Alarm Type, Sampling Interval, Rising Threshold, Rising Event Index, Failing Threshold, Failing Event Index and Owner.

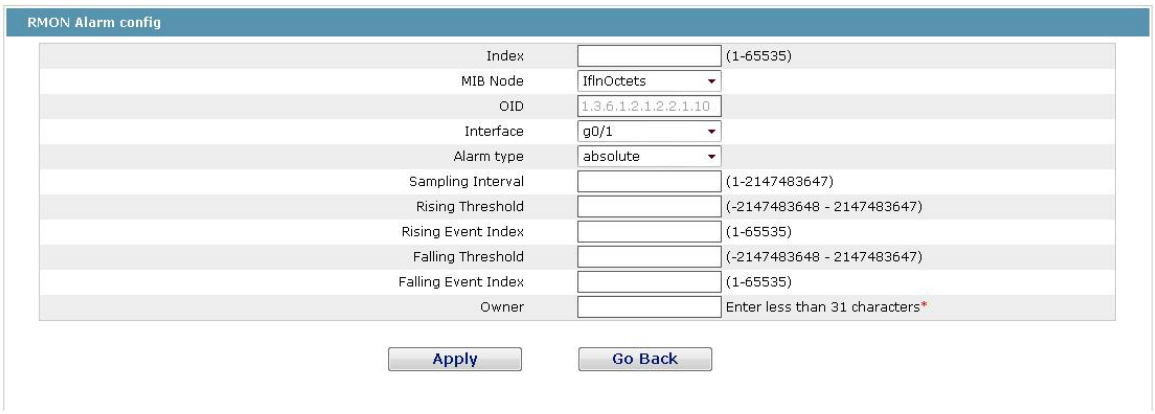


Figure 9-11: RMON Alarm Config

9.2.4 RMON Event

Figure 9-12: RMON Event

On the above page, you can create, edit or delete RMON information. Click “New” on the top left of the interface, or tick an item and click “Edit” in the end of the item line, then the following page appears. Here you can configure Index, Owner, Description, Enable log, Enable trap, and Community.

Figure 9-13: RMON Event Config

Chapter 10 System Mgr

Figure 10-1 System Management

10.1 User Mgr

10.1.1 User Mgr

On the left navigation bar, click “System Mgr” -> “User Mgr” -> “User Mgr” and the following page appears.

Figure10-2: User Management

Click “New” on the top left of the above interface to create a new user.

Tick an item and click “Edit” at the end of the item line, and then you can modify the user authority and log-in password on the pop-up interface.

Note:
1. Please ensure that there is one user with the permission of “system administrator”, so that the device can be managed through Web.

2. The user with “limited authority” can only check device status, but not modify the configuration.

Creating New User

Click “New” on the above page of “User Management” and the following page appears:

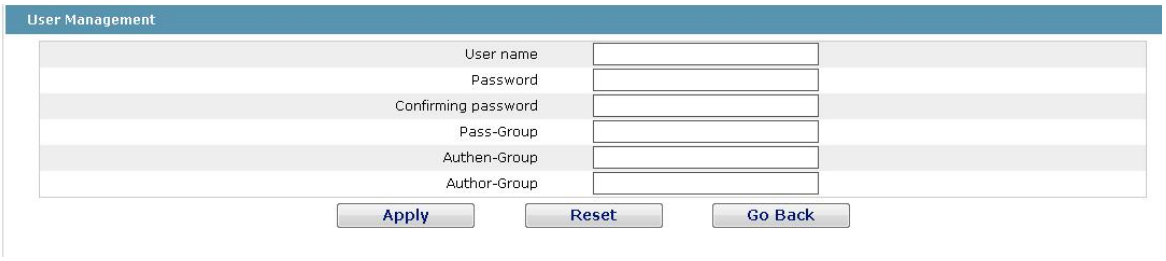


Figure10-3: Creating New User

In the “User name” text box, enter a name, which contains letters, numbers and symbols except “?”, “\”, “&”, “#” and the "Space" symbol.

In the “Password” textbox enter a login password, and in the “Confirming password” textbox enter this login password again.

10.1.2 Group Mgr

On the left navigation bar, click “System Mgr” -> “User Mgr” -> “User Group Mgr” and the following page appears.

Figure 10-4: User Group Management

Click “New” on the top left of the interface to create a new user group.

Click “Delete” to delete the user group.

Figure 10-5: User Group Config

The user group name cannot be created before. The Pass-Group Name, Authen-Group Name and Author-Group Name must be created before, otherwise, the new created user group cannot be succeeded. Set Pass-Group Name, Authen-Group Name, and Author-Group Name on the relevant tab pages.

10.1.3 Pass-Group Mgr

On the left navigation bar, click “System Mgr” -> “User Mgr” -> “Pass- Group Mgr” and the following page appears.

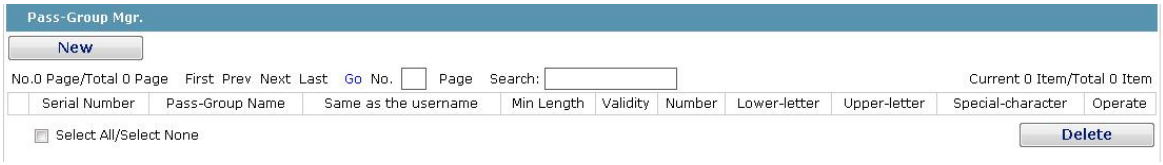


Figure 10-6: Password Group Management

Click “New” to create a new Pass-Group Name.

Click “Delete” to delete the selected Pass-Group Name.

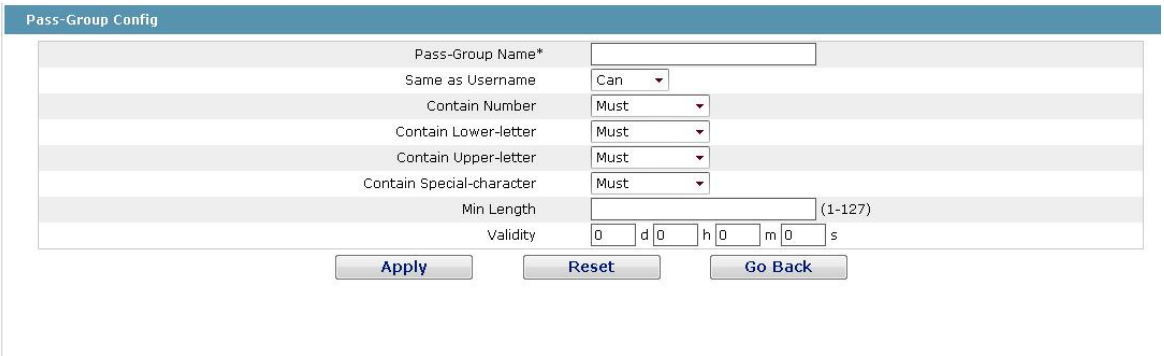


Figure 10-7 Pass Group Configuration

Set some password rules including whether the password can be the same with the user name, whether the password must contain numbers, lowercase, uppercase, special characters, the minimum length and the period of validity.

When the rule is created and applied to the user management, the user password will show invalid if the set password is not complied with the password rule, vice versa.

10.1.4 Authen-Group Mgr

On the left navigation bar, click “System Mgr” -> “User Mgr” -> “Authen-Group Mgr” and the following page appears.

Figure 10-8: Authorization Group Management

Click “New” to create a new authen-group name.

Click “Delete” to delete the authen-group name.

Figure 10-9: Authentication Group Configuration

On the above page, the Max try times and Duration for all tries must be configured simultaneously. Otherwise, the configuration cannot take effect.

10.1.5 Author-Group Mgr

On the left navigation bar, click “System Mgr” -> “User Mgr” -> “Author-Group Mgr” and the following page appears.

Figure 10-10: Authorization Group Management

Click “New” to create a new author-group name.

Click “Delete” to delete the author-group name.

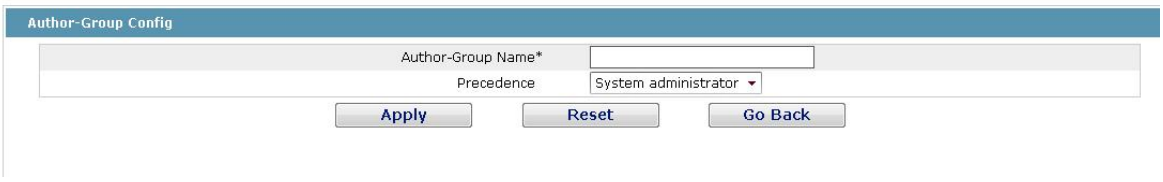


Figure 10-11: Authorization Group Configuration

The authorization rule determines your permission of the administrator or the limited user. If you are the administrator, you have the administrator right. If you are the limited user, you can only but check the web.

10.2 Log Mgr

On the left navigation bar, click “System Mgr” -> “Log Mgr” -> “Log Mgr” and the following page appears.

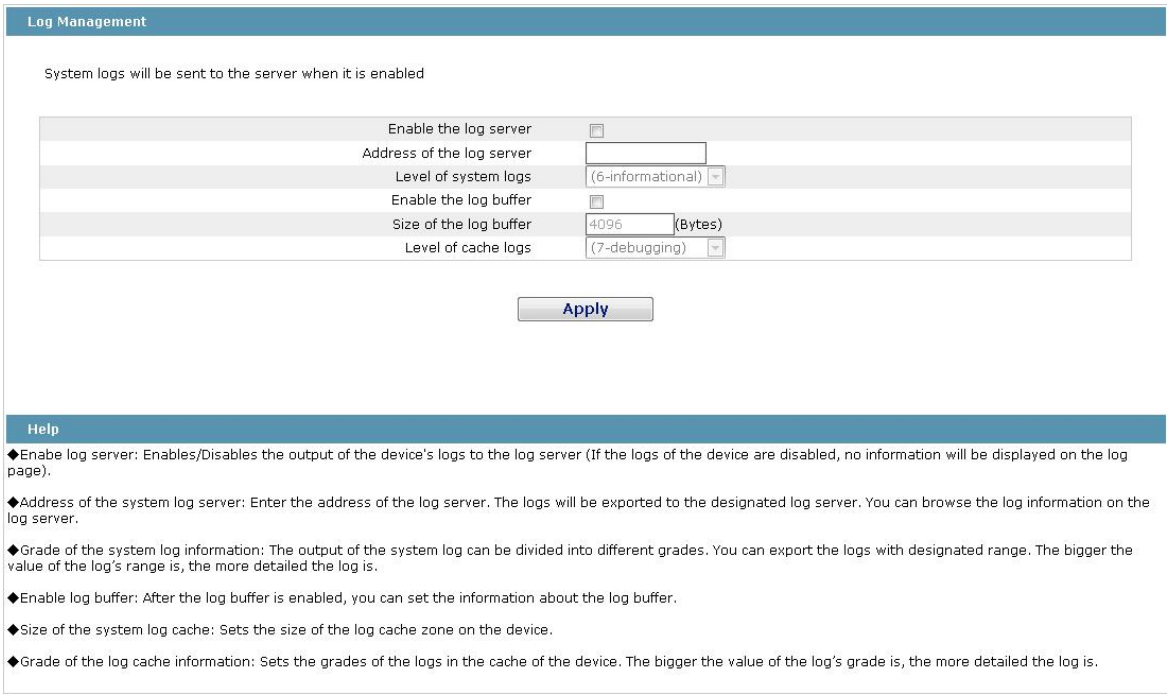


Figure 10-12: Log Management

If “Enable the log server” is selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the “Address of the log server” textbox and select the log's level in the “Level of the cache logs” dropdown box. “7-debugging” is the lowest level for log information.

If “Enable the log buffer” is selected, the device will record the log information into the memory. Log in the device by the Console port or Telnet, and run the command “show log” to check the log the device recorded. The log information in the memory will be lost after rebooting the device. Input the Size of the log buffer and select the Level of cache logs.

10.3 Diagnostic

On the left navigation bar, click “System Mgr” -> “Diagnostic” and the following page appears.

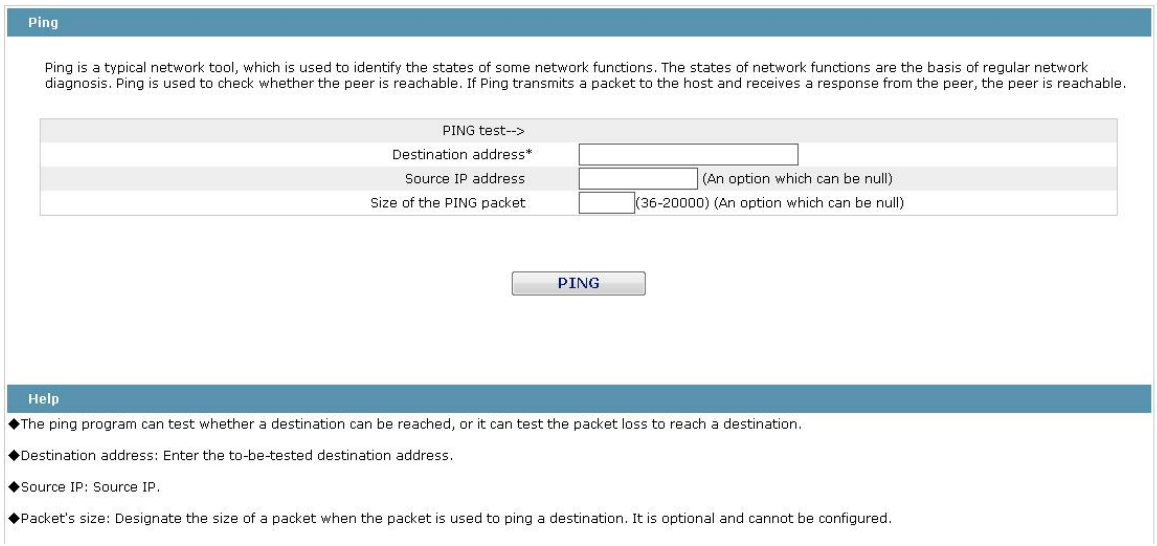


Figure 10-13: Ping

Ping is used to test whether the OLT connects other devices.

If a Ping test need be conducted, please enter an IP address in the “Destination address” textbox, such as the IP address of your PC, and then click the “PING” button. If the switch connects your entered address, the device can promptly return a test result to you; if not, the device will take a little more time to return the test result.

“Source IP address” is used to set the source IP address which is carried in the Ping packet.

10.4 Startup-config

10.4.1 Export the current startup-config

On the left navigation bar, click “System Mgr” -> “Starpup-config” and the following page appears.

Figure 10-14; Export the current startup-config

The current configuration file can be exported, saved in the disk of PC or in the mobile storage device as the backup file.

To export the configuration file, please click the “Export” button and then select the “Save” option in the pop-up download dialog box.

The default name of the configuration file is “startup-config”, but you are suggested to set it to an easily memorable name.

10.4.2 Import startup-config file

Figure 10-15: Import Startup-Config File

You can import the configuration files from PC to the device and replace the configuration file that is currently being used. For example, by importing the backup configuration files, you can resume the device to its configuration of a previous moment.

Note:
1. Please make sure that the imported configuration file has the legal format for the configuration file with illegal format cannot lead to the normal startup of the device.
2. If error occurs during the process of importation, please try it later again, or click the “Save All” button to make the device re-establish the configuration file with the current configuration, avoiding the incomplete file and the abnormality of the device.
3. After the configuration file is imported, if you want to use the imported configuration file immediately, do **not** click “Save All”, but reboot the device directly.

10.5 IOS Software

10.5.1 Backup IOS

On the left navigation bar, click “System Mgr” -> “IOS Software” and the following page appears.

Figure 10-16: Backup IOS

The current running software version is displayed in the page. If you need to backup the system, please click “backup system software”, then select “save” in the pop-up file download dialog box and save the system profile to your computer disk, transferable data device or other positions in the network.

Note:

Default name of the system profile is “Switch.bin”. You are suggested to change the default name to a name that easy to identify.

10.5.2 Update IOS

Note:
1. Please ensure your update system profile match with the device type. Otherwise, the system cannot operate normally.
2. The system profile update may need 1 to 2 minutes. After clicking and confirming the “update” button, the profile will be upload to the device. Please be patient.
3. Please do not restart or interrupt the device if errors occur in the update process, or the device cannot start up. Please try update again later.
4. Please save the configuration and restart the device after updating, so that the new system can operate.

Figure 10-17: Update IOS

The update software is usually used for solving the existing problems or improving certain functions. You don’t need to update the system software regularly, if your device operates normally.

If your system needs to be update, please enter the full path of the new system profile into the text box right of “update system software” or click “browse” button to select new system profiles and click “update”.

10.6 Factory Settings

On the left navigation bar, click “System Mgr” -> “Factory Setting” and the following page appears.

Figure 10-10: Restore to the original settings

Note:
1. If you click the “Resume” button, the current configuration will be replaced by the original configuration, which will take effect after rebooting.

2. Before rebooting the device still works under the current configuration, and if you click “Save All” at the moment, the current configuration will replace the original configuration. The original configuration, therefore, cannot take effect after rebooting.
3. After the rebooting is done and the original configuration takes effect, the Web access of the device will be automatically started. The address of Vlan 1 is 192.168.0.1/255.255.255.0, and the username and password are both “admin”.

To resume the original configuration, click “Resume” and then reboot the device.

10.7 Reboot

On the left navigation bar, click “System Mgr” -> “Reboot” and the following page appears.

Figure 10-19: Rebooting

If the device need be rebooted, please first make sure that the modified configuration of the device has already been saved, and then click the “Reboot” button.

10.8 About

On the left navigation bar, click “System Mgr” -> “ About” and the following page appears.

Figure 10-12: About