

Web Management Guide

(GTL-2091)



V1.0

Digital Data Communications GmbH, Germany.

<http://www.level1.com>

Table of Contents

Chapter 1 HTTP Switch Configuration.....	5
1.1 HTTP Configuration.....	5
1.1.1 Choosing the Prompt Language.....	5
1.1.2 Setting the HTTP Port.....	5
1.1.3 Enabling the HTTP Service.....	5
1.1.4 Setting the HTTP Access Mode.....	5
1.1.5 Setting the Maximum Number of VLAN Entries on Web Page.....	6
1.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page.....	6
1.2 HTTPS Configuration.....	6
1.2.1 Setting the HTTP Access Mode.....	6
1.2.2 It is used to set the HTTPS port.....	6
Chapter 2 Configuration Preparation.....	7
2.1 Accessing the Switch Through HTTP.....	7
2.1.1 Initially Accessing the Switch.....	7
2.1.2 Upgrading to the Web-Supported Version.....	8
2.2 Accessing a Switch Through Secure Links.....	8
2.3 Introduction of Web Interface.....	9
2.3.1 Top Control Bar.....	9
2.3.2 Navigation Bar.....	10
2.3.3 Configuration Area.....	10
2.3.4 Bottom Control Bar.....	11
2.3.5 Configuration Area.....	11
Chapter 3 Basic Configuration.....	12
3.1 Host name Configuration.....	12
3.2 Time Management.....	13
Chapter 4 Configuration of the Physical Interface.....	14
4.1 Configuring Port Description.....	14
4.2 Configuring the Attributes of the Port.....	15
4.3 Rate control.....	1
4.4 Port mirroring.....	1
4.5 Loopback Detection.....	2
4.6 Port security.....	2
4.6.1 IP Binding Configuration.....	2
4.6.2 MAC Binding Configuration.....	3
4.6.3 Setting the Static MAC Filtration Mode.....	3
4.6.4 Static MAC Filtration Entries.....	3
4.6.5 Setting the Dynamic MAC Filtration Mode.....	4
4.7 Storm control.....	4
4.7.1 Broadcast Storm Control.....	4
4.7.2 Multicast Storm Control.....	4
4.7.3 Unknown Unicast Storm Control.....	5
Chapter 5 Layer-2 Configuration.....	6
5.1 VLAN Settings.....	6
5.1.1 VLAN List.....	6
5.1.2 VLAN Settings.....	7
5.2 PDP Configuration.....	7
5.2.1 Configuring the Global Attributes of PDP.....	7
5.2.2 Configuring the Attributes of the PDP Port.....	8

5.3 LLDP Configuration	8
5.3.1 Configuring the Global Attributes of LLDP	8
5.3.2 Configuring the Attributes of the LLDP Port.....	9
5.4 Link Aggregation Configuration.....	9
5.5 STP Configuration	10
5.5.1 STP Status Information	10
5.5.2 Configuring the Attributes of the STP Port.....	11
5.6 IGMP-Snooping Configuration.....	11
5.6.1 IGMP-Snooping Configuration.....	11
5.6.2 IGMP-Snooping VLAN List	12
5.6.3 Static Multicast Address	13
5.6.4 Multicast List.....	13
5.7 Setting Static ARP	14
5.8 Ring Protection Configuration.....	15
5.8.1 EAPS Ring List.....	15
5.8.2 EAPS Ring Configuration	15
5.9 DDM Configuration	16
Chapter 6 Layer-3 Configuration.....	17
6.1 VLAN Interface and IP Address Configuring.....	17
6.2 Setting the Static Route	18
6.3 IGMP Agent	19
6.3.1 Enabling the IGMP Agent	19
6.3.2 Setting the IGMP Agent	20
Chapter 7 Advanced Configuration.....	21
7.1 QoS Configuration	21
7.1.1 Configuring QoS Port	21
7.1.2 Global QoS Configuration.....	22
7.2 MAC Access Control List	23
7.2.1 Setting the Name of the MAC Access Control List	23
7.2.2 Setting the Rules of the MAC Access Control List.....	23
7.2.3 Applying the MAC Access Control List	24
7.3 IP Access Control List.....	24
7.3.1 Setting the Name of the IP Access Control List.....	24
7.3.2 Setting the Rules of the IP Access Control List	25
7.3.3 Applying the IP Access Control List	26
Chapter 8 Network Management Configuration.....	27
8.1 SNMP Configuration	27
8.1.1 SNMP Community Management	27
8.1.2 SNMP Host Management.....	28
8.2 RMON.....	29
8.2.1 RMON Statistic Information Configuration.....	29
8.2.2 RMON History Information Configuration	29
8.2.3 RMON Alarm Information Configuration	30
8.2.4 RMON Event Configuration	31
Chapter 9 Diagnosis Tools.....	33
9.1 Ping.....	33
Chapter 10 System Management	34
10.1 User Management	34
10.1.1 User List	34
10.1.2 Establishing a New User	35
10.2 Log Management.....	35
10.3 Managing the Configuration Files.....	36

10.3.1 Exporting the Configuration Information	36
10.3.2 Importing the Configuration Information	36
10.4 Software Management.....	37
10.4.1 Backing up the IOS Software	37
10.5 Resuming Initial Configuration.....	38
10.6 Rebooting the Device	38

Chapter 1 HTTP Switch Configuration

1.1 HTTP Configuration

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

1.1.1 Choosing the Prompt Language

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

Command	Purpose
<code>ip http language {chinese english}</code>	Sets the prompt language of Web configuration to Chinese or English .

1.1.2 Setting the HTTP Port

Generally, the HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support 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 switches. 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
<code>ip http port { portNumber }</code>	Sets the HTTP port.

1.1.3 Enabling the HTTP Service

Switches support to control the HTTP access. Only when the HTTP service is enabled can HTTP exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops.

Command	Purpose
<code>ip http server</code>	Enables the HTTP service.
<code>ip http {timeout}</code>	Configures the timeout time of HTTP abnormal packets.

1.1.4 Setting 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
<code>ip http http-access enable</code>	Sets the HTTP access mode.

1.1.5 Setting the Maximum Number of VLAN Entries on Web Page

A switch 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 { <i>max-vlan</i> }	Sets the maximum number of VLAN entries displayed in a web page.

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

A switch 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 { <i>igmp-groups</i> }	Sets the maximum number of multicast entries displayed in a web page.

1.2 HTTPS Configuration

In order to improve the security of communications, switches support 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 Setting 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 It is used to set 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.

Parameter	Remarks
ip http secure-port { <i>portNumber</i> }	Sets the HTTPS port.

Chapter 2 Configuration Preparation

2.1 Accessing the Switch Through HTTP

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

- HTML of version 4.0
- HTTP of version 1.1
- JavaScript™ of version 1.5

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

2.1.1 Initially Accessing the Switch

When the switch 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 192.168.1.2 and 255.255.255.0 respectively.
2. Open the Web browser and enter 192.168.1.1 in the address bar. It is noted that 192.168.1.1 is the default management address of the switch.
3. If the Internet Explorer browser is used, you can see the dialog box in figure 1. Both the original username and the password are "admin"



Figure 1: ID checkup of WEB login

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

2.1.2 Upgrading to the Web-Supported Version

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

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Console_config#".
3. If the management address of the switch 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. Run **username** to set the username and password of the switch. 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 switch.

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

2.2 Accessing a Switch Through Secure Links

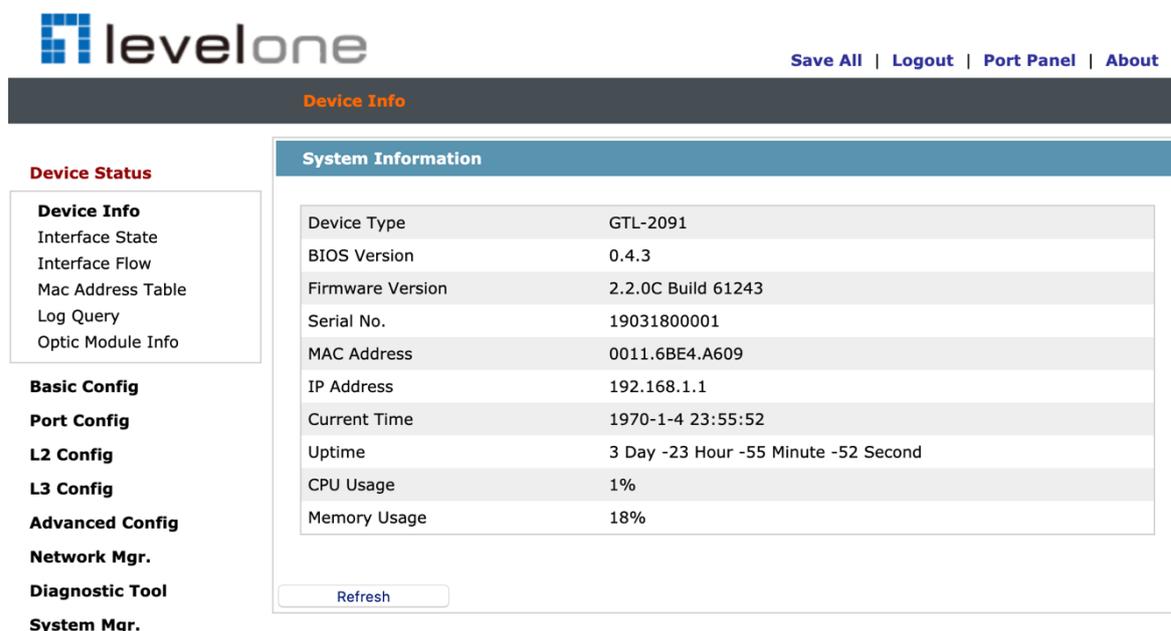
The data between the WEB browser and the switch will not be encrypted if you access a switch through common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to access the switch.

To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Console_config#".
3. If the management address of the switch 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. Run **username** to set the username and password of the switch. 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 switch.
7. Run **no ip http http-access enable** to forbid to access the switch 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 switch connects, enter <https://192.168.1.1> on the address bar (**192.168.1.1** stands for the management IP address of the switch) and then press the **Enter** key. Then the switch can be accessed through the secure links.

2.3 Introduction of Web Interface

The Web homepage appears after login, as shown in figure 2:



The screenshot shows the LevelOne web interface. At the top right, there are links for [Save All](#), [Logout](#), [Port Panel](#), and [About](#). Below this is a dark grey bar with the text "Device Info" in orange. On the left side, there is a "Device Status" menu with the following items: **Device Info**, Interface State, Interface Flow, Mac Address Table, Log Query, and Optic Module Info. Below this menu are sections for **Basic Config**, **Port Config**, **L2 Config**, **L3 Config**, **Advanced Config**, **Network Mgr.**, **Diagnostic Tool**, and **System Mgr.**. The main content area is titled "System Information" and contains a table with the following data:

Device Type	GTL-2091
BIOS Version	0.4.3
Firmware Version	2.2.0C Build 61243
Serial No.	19031800001
MAC Address	0011.6BE4.A609
IP Address	192.168.1.1
Current Time	1970-1-4 23:55:52
Uptime	3 Day -23 Hour -55 Minute -52 Second
CPU Usage	1%
Memory Usage	18%

At the bottom of the "System Information" section, there is a "Refresh" button.

Figure 2: Web homepage

The whole 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](#) | [Logout](#) | [Port Panel](#) | [About](#)

Figure 3: 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. If you 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



Figure 4 Navigation bar

The contents in the navigation bar 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 sub-item. 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 Configuration Area

System Information	
Device Type	GTL-2091
BIOS Version	0.4.3
Firmware Version	2.2.0C Build 61243
Serial No.	19031800001
MAC Address	0011.6BE4.A609
IP Address	192.168.1.1
Current Time	1970-1-4 23:55:52
Uptime	3 Day -23 Hour -55 Minute -52 Second
CPU Usage	1%
Memory Usage	18%

Refresh

Figure 5 Configuration Area

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 in the navigation bar.

2.3.4 Bottom Control Bar



Figure 6: Bottom control bar

If you click the **About** button on the top control bar, the bottom control bar appears. The main function of the bottom control bar is to realize the automatic refreshing of the configuration display area. For example, if you click “Interface Flow” in the navigation bar and then click “Refresh”, the flow of the interface can be continuously monitored.

After you click “Refresh”, the countdown of the next-time refresh will appear on the left side. You can modify the countdown settings by clicking the dropdown list.

Note:

The smaller the countdown value is set, that is, the higher the frequency is, the higher the CPU usage is.

2.3.5 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

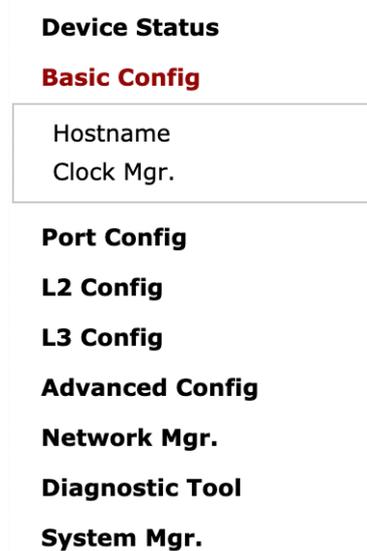


Figure 1 A list of basic configuration

3.1 Host name Configuration

If you click **Basic Config -> Hostname Config** in the navigation bar, the **Hostname Configuration** page appears, as shown in figure 3.

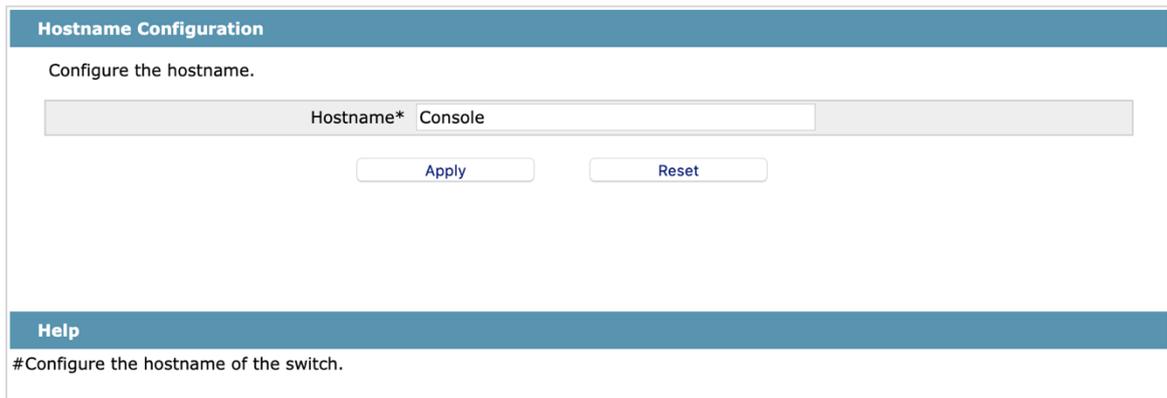


Figure 2 Hostname configuration

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 Time Management

If you click **Basic Config** -> **Clock Mar**, the **Time Setting** page appears.

The screenshot displays the 'Time Setting' configuration page. At the top, the 'System Time' is shown as '1970-01-06 22:29:45' with a 'Refresh' button. Below this, there is a 'Select Time-Zone' dropdown menu currently set to '(GMT)Greenwich Mean Time,Dublin,London,Lisbon'. Two radio buttons are present: 'Set Time Manually' (which is selected) and 'Network Time Synchronization'. Under 'Set Time Manually', there are input fields for 'Set Time' with values: Year: 1970, Month: 01, Day: 06, Hour: 22, Minute(s): 45, and Second. Under 'Network Time Synchronization', there are three input fields labeled 'NTP Server One', 'NTP Server Two', and 'NTP Server Three'. An 'Apply' button is located at the bottom of the configuration section. A 'Help' section at the bottom provides instructions for each option.

Time Setting

System Time: 1970-01-06 22:29:45 Refresh

Select Time-Zone: (GMT)Greenwich Mean Time,Dublin,London,Lisbon

Set Time Manually

Set Time: 1970 Year 01 Month 06 Day 22 Hour 29 Minute(s) 45 Second

Network Time Synchronization

NTP Server One

NTP Server Two

NTP Server Three

Apply

Help

#There are two ways to update the system time, one is to use ntp and the other is to manually set the time.

#Set Time Manually: Select the 'Set Time Manually' option, select the local time zone, enter the current time, and click 'Apply' to save the configuration.

#Network Time Synchronization: Select the 'Network Time Synchronization' option, add no more than three IP addresses of the NTP server.

#Refresh: Click to get the current time of the switch.

Figure 3 Clock management

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

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 Configuration of the Physical Interface

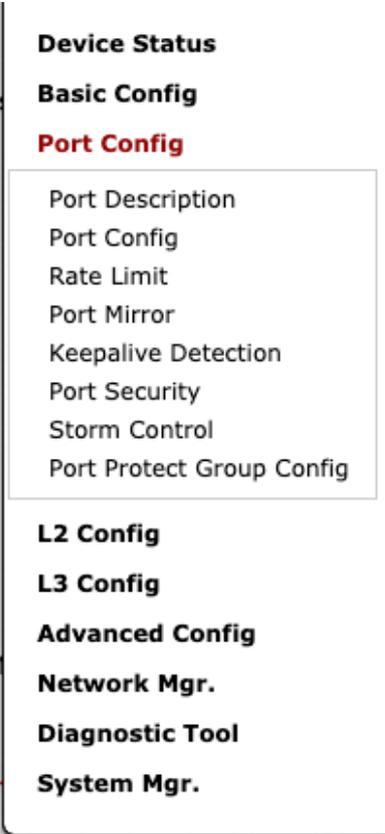
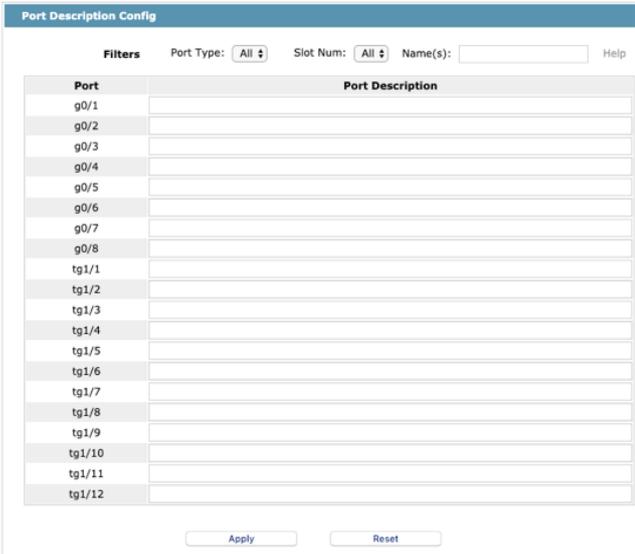


Figure 1: Physical port configuration list

4.1 Configuring Port Description

If you click **Port config -> Port Description** in the navigation bar, the **Port description Configuration** page appears, as shown in figure 2.



The screenshot shows the 'Port Description Config' page. At the top, there are filters for 'Port Type' (set to 'All'), 'Slot Num' (set to 'All'), and 'Name(s)'. Below the filters is a table with two columns: 'Port' and 'Port Description'. The 'Port' column lists various ports: g0/1 through g0/8, tg1/1 through tg1/12. The 'Port Description' column is empty for all rows. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

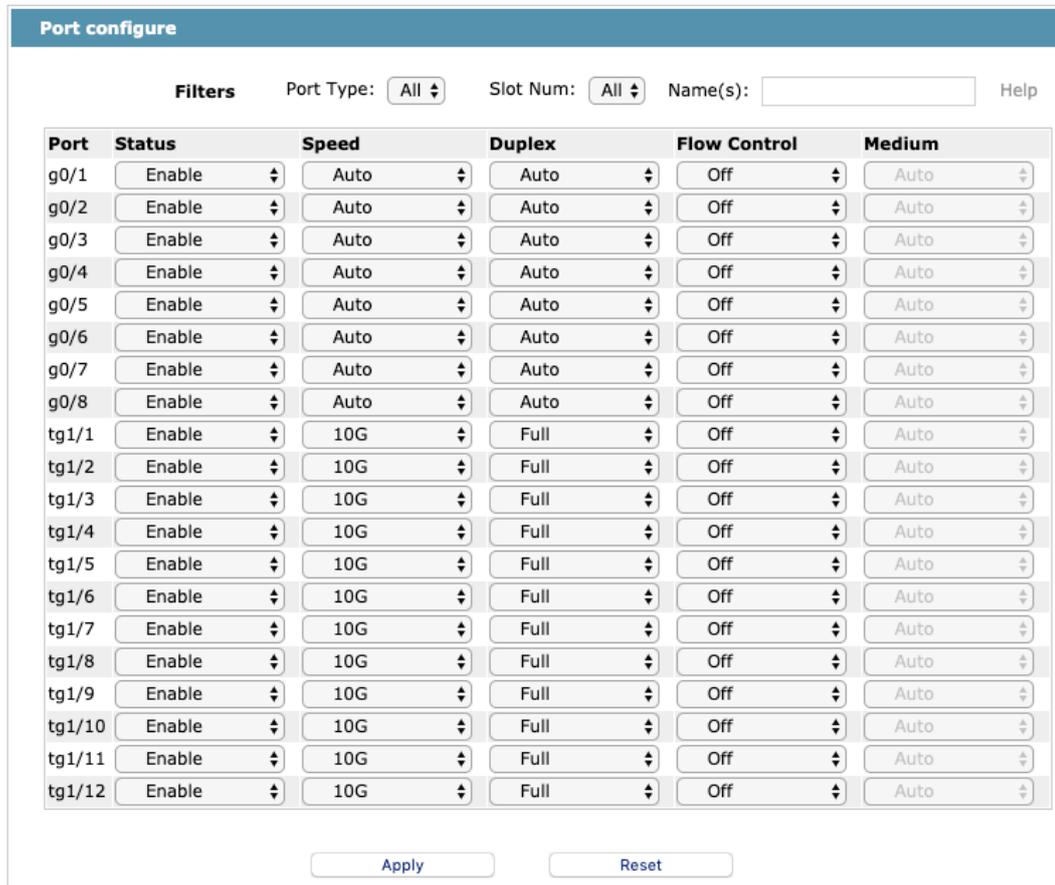
Port	Port Description
g0/1	
g0/2	
g0/3	
g0/4	
g0/5	
g0/6	
g0/7	
g0/8	
tg1/1	
tg1/2	
tg1/3	
tg1/4	
tg1/5	
tg1/6	
tg1/7	
tg1/8	
tg1/9	
tg1/10	
tg1/11	
tg1/12	

Figure 2: Port description configuration

You can modify the port description on this page and enter up to 120 characters. The description of the VLAN port cannot be set at present.

4.2 Configuring the Attributes of the Port

If you click **Port Config -> Port Configure** in the navigation bar, the **Port Attribute Configuration** page appears, as shown in figure 3.



The screenshot shows the 'Port configure' interface. At the top, there are filter options: 'Filters', 'Port Type: All', 'Slot Num: All', and a 'Name(s):' input field. Below this is a table with columns for Port, Status, Speed, Duplex, Flow Control, and Medium. The table lists ports from g0/1 to tg1/12. Each cell in the table contains a dropdown menu with the current value. Below the table are 'Apply' and 'Reset' buttons.

Port	Status	Speed	Duplex	Flow Control	Medium
g0/1	Enable	Auto	Auto	Off	Auto
g0/2	Enable	Auto	Auto	Off	Auto
g0/3	Enable	Auto	Auto	Off	Auto
g0/4	Enable	Auto	Auto	Off	Auto
g0/5	Enable	Auto	Auto	Off	Auto
g0/6	Enable	Auto	Auto	Off	Auto
g0/7	Enable	Auto	Auto	Off	Auto
g0/8	Enable	Auto	Auto	Off	Auto
tg1/1	Enable	10G	Full	Off	Auto
tg1/2	Enable	10G	Full	Off	Auto
tg1/3	Enable	10G	Full	Off	Auto
tg1/4	Enable	10G	Full	Off	Auto
tg1/5	Enable	10G	Full	Off	Auto
tg1/6	Enable	10G	Full	Off	Auto
tg1/7	Enable	10G	Full	Off	Auto
tg1/8	Enable	10G	Full	Off	Auto
tg1/9	Enable	10G	Full	Off	Auto
tg1/10	Enable	10G	Full	Off	Auto
tg1/11	Enable	10G	Full	Off	Auto
tg1/12	Enable	10G	Full	Off	Auto

Figure 3 Configuring the port attributes

On this page you can modify the on/off status, rate, duplex mode, flow control status and medium type of a port.

Note:

1. The Web page does not support the speed and duplex mode of the fast-Ethernet port.
2. After the speed or duplex mode of a port is modified, the link state of the port may be switched over and the network communication may be impaired.

4.3 Rate control

If you click **Physical port Config -> Port rate-limit Config** in the navigation bar, the **Port rate limit** page appears, as shown in figure 4.

Port	Receive Status	Receive Speed Unit	Receive Speed	Send Status	Send Speed Unit	Send Speed
g0/1	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/2	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/3	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/4	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/5	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/6	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/7	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
g0/8	Disable	64kbps	(1-16384)	Disable	64kbps	(1-16384)
tg1/1	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/2	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/3	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/4	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/5	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/6	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/7	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/8	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/9	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/10	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/11	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)
tg1/12	Disable	64kbps	(1-156250)	Disable	64kbps	(1-156250)

Figure 4: Port's rate limit

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited.

4.4 Port mirroring

If you click **Physical port Config -> Port Mirror** in the navigation bar, the **Port Mirror Config** page appears, as shown in figure 4-5.

Figure 4-5 Port mirror configuration

4.6.2 MAC Binding Configuration

If you click **Physical port Config -> Port Security -> MAC bind** in the navigation bar, the **Configure the MAC-Binding Info** page appears, as shown in figure 4-10.

Interface Name	Detail
G0/1	Detail

Figure 4-9 MAC binding configuration

Click “Detail” and then you can conduct the binding of the source MAC address for each physical port. In this way, the MAC address that is allowed to visit the port will be limited.

	Serial number	Address	Operate
<input type="checkbox"/>	1	1234.1234.1234	Edit
<input type="checkbox"/>	2	1234.1234.1235	Edit

Figure 4-10 Setting the binding of the source MAC address

4.6.3 Setting the Static MAC Filtration Mode

If you click **Physical port Config -> Port Security -> Static MAC filtration mode** in the navigation bar, the **Configure the static MAC filtration mode** page appears, as shown in figure 4-11.

Interface Name	Port Mode	Static MAC Filtration Mode
G0/1	Access	Disable

Figure 4-11: Setting the static MAC filtration mode

On this page you can set the static MAC filtration mode. By default, the static MAC filter is disabled. Also, the static MAC filter mode cannot be set on ports in trunk mode.

4.6.4 Static MAC Filtration Entries

If you click **Physical port Config -> Port security -> Static MAC filtration entries** in the navigation bar, the **Setting the static MAC filtration entries** page appears.

Interface Name	Detail
G0/1	Detail

Figure 4-12: Static MAC filtration entry list

If you click “Detail”, you can conduct the binding of the source MAC address for each physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.

	Serial number	Filtration Mode	MAC Address	Operate
<input type="checkbox"/>	1	Disable	0001.0002.0003	Edit

Figure 4-13: Setting static MAC filtration entries

4.6.5 Setting the Dynamic MAC Filtration Mode

If you click **Physical port Config -> Port Security -> Dynamic MAC filtration mode** in the navigation bar, the **Configure the dynamic MAC filtration mode** page appears, as shown in figure 4-14.

Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
G0/1	Disable	1 (1-4095)

Figure 4-14: Setting the dynamic MAC filtration mode

You can set the dynamic MAC filtration mode and the allowable maximum number of addresses on this page. By default, the dynamic MAC filtration mode is disabled and the maximum number of addresses is 1.

4.7 Storm control

In the navigation bar, click **Physical port Config -> Storm control**. The system then enters the page, on which the broadcast/multicast/unknown unicast storm control can be set.

4.7.1 Broadcast Storm Control

Broadcast-storm control configuration			
Filters	Port Type:	Slot Num:	Name(s):
	All	All	Help
Port	Status	Threshold	
g0/1	Disable	(1-163840) 100PPS	
g0/2	Enable	(1-163840) 100PPS	
g0/3	Disable	(1-163840) 100PPS	

Figure 5 Broadcast storm control

Through the dropdown boxes in the **Status** column, you can decide whether to enable broadcast storm control on a port. In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.7.2 Multicast Storm Control

Broadcast-storm control configuration			
Filters	Port Type:	Slot Num:	Name(s):
	All	All	Help
Port	Status	Threshold	
g0/1	Disable	(1-163840) 100PPS	
g0/2	Disable	(1-163840) 100PPS	
g0/3	Disable	(1-163840) 100PPS	
g0/4	Disable	(1-163840) 100PPS	
g0/5	Disable	(1-163840) 100PPS	
g0/6	Disable	(1-163840) 100PPS	
g0/7	Disable	(1-163840) 100PPS	
g0/8	Disable	(1-163840) 100PPS	
tg1/1	Disable	(1-1638400) 100PPS	
tg1/2	Disable	(1-1638400) 100PPS	
tg1/3	Disable	(1-1638400) 100PPS	
tg1/4	Disable	(1-1638400) 100PPS	
tg1/5	Disable	(1-1638400) 100PPS	
tg1/6	Disable	(1-1638400) 100PPS	
tg1/7	Disable	(1-1638400) 100PPS	
tg1/8	Disable	(1-1638400) 100PPS	
tg1/9	Disable	(1-1638400) 100PPS	
tg1/10	Disable	(1-1638400) 100PPS	
tg1/11	Disable	(1-1638400) 100PPS	
tg1/12	Disable	(1-1638400) 100PPS	

Figure 6 Setting the broadcast storm control

Through the dropdown boxes in the **Status** column, you can decide whether to enable multicast storm control on a port. In the **Threshold** column you can enter the threshold of the multicast packets. The legal threshold range for each port is given behind the threshold.

4.7.3 Unknown Unicast Storm Control

Broadcast-storm control configuration

Filters Port Type: Slot Num: Name(s): Help

Port	Status	Threshold	
g0/1	<input type="button" value="Enable"/>	<input type="text"/>	(1-163840) 100PPS
g0/2	<input checked="" type="button" value="Disable"/>	<input type="text"/>	(1-163840) 100PPS
g0/3	<input type="button" value="Enable"/>	<input type="text"/>	(1-163840) 100PPS
g0/4	<input type="button" value="Disable"/>	<input type="text"/>	(1-163840) 100PPS
g0/5	<input type="button" value="Disable"/>	<input type="text"/>	(1-163840) 100PPS
g0/6	<input type="button" value="Disable"/>	<input type="text"/>	(1-163840) 100PPS
g0/7	<input type="button" value="Disable"/>	<input type="text"/>	(1-163840) 100PPS
g0/8	<input type="button" value="Disable"/>	<input type="text"/>	(1-163840) 100PPS
tg1/1	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/2	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/3	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/4	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/5	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/6	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/7	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/8	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/9	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/10	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/11	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS
tg1/12	<input type="button" value="Disable"/>	<input type="text"/>	(1-1638400) 100PPS

Figure 7 Unknown unicast storm control

In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

Chapter 5 Layer-2 Configuration

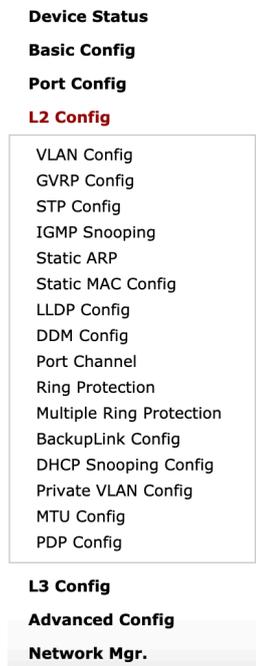


Figure 1: Layer-2 configuration list

5.1 VLAN Settings

5.1.1 VLAN List

If you click **Layer-2 Config -> VLAN Config** in the navigation bar, the **VLAN Config** page appears, as shown in figure 2.

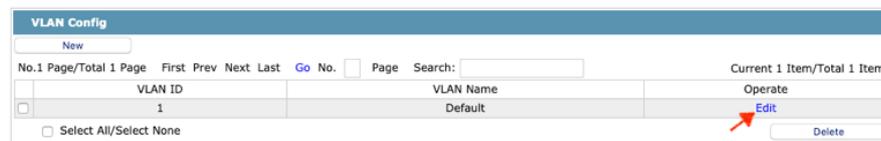


Figure 2 VLAN configuration

The VLAN list will display VLAN items that exist in the current device according to the ascending order. In case of lots of items, you can look for the to-be-configured VLAN through the buttons like “Prev”, “Next” and “Search”.

You can click “New” to create a new VLAN.

You can also click “Edit” at the end of a VLAN item to modify the VLAN name and the port’s attributes in the VLAN.

If you select the checkbox before a VLAN and then click “Delete”, the selected VLAN will be deleted.

Note:

By default, a VLAN list can display up to 100 VLAN items. If you want to configure more VLANs through Web, please log on to the switch through the Console port or Telnet, enter the global configuration mode and then run the **"ip http web max-vlan"** command to modify the maximum number of VLANs that will be displayed.

5.1.2 VLAN Settings

If you click "New" or "Edit" in the VLAN list, the VLAN configuration page appears, on which new VLANs can be created or the attributes of an existent VLAN can be modified.

Port	Default VLAN	Mode	Untag or not	Allow or not
g0/1	1 <1-4094>	Access	Yes	Yes
g0/2	1 <1-4094>	Access	Yes	Yes
g0/3	1 <1-4094>	Access	Yes	Yes
g0/4	1 <1-4094>	Access	Yes	Yes
g0/5	1 <1-4094>	Access	Yes	Yes
g0/6	1 <1-4094>	Access	Yes	Yes
g0/7	1 <1-4094>	Access	Yes	Yes
g0/8	1 <1-4094>	Access	Yes	Yes
tg1/1	1 <1-4094>	Access	Yes	Yes
tg1/2	1 <1-4094>	Access	Yes	Yes
tg1/3	1 <1-4094>	Access	Yes	Yes
tg1/4	1 <1-4094>	Access	Yes	Yes
tg1/5	1 <1-4094>	Access	Yes	Yes
tg1/6	1 <1-4094>	Access	Yes	Yes
tg1/7	1 <1-4094>	Access	Yes	Yes
tg1/8	1 <1-4094>	Access	Yes	Yes
tg1/9	1 <1-4094>	Access	Yes	Yes
tg1/10	1 <1-4094>	Access	Yes	Yes
tg1/11	1 <1-4094>	Access	Yes	Yes
tg1/12	1 <1-4094>	Access	Yes	Yes

Figure 3 Revising VLAN configuration

If you want to create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be null.

Through the port list, you can set for each port the default VLAN, the VLAN mode (Trunk or Access), whether to allow the entrance of current VLAN packets and whether to execute the untagging of the current VLAN when the port works as the egress port.

Note:

When a port in Trunk mode serves as an egress port, it will untag the default VLAN by default.

5.2 PDP Configuration

5.2.1 Configuring the Global Attributes of PDP

If you click **Layer-2 Config -> PDP Config** in the navigation bar, the **Global PDP Config** page appears, as shown in figure 4.

Basic Config of PDP Protocol	
Protocol State	Close the PDP protocol ▾
HoldTime Settings	180 (10-255)s
Setting the packet transmission cycle	60 (5-254)s
Protocol Version	Version2 ▾

Help

#HoldTime:If the other PDP packets are not received, the switch will save the holdtime before clearing the received packets.Its default value is 180s.
#Cycle of Sending Packets:Its default value is 60s.

Figure 4 Configuring the global attributes of PDP

You can choose to enable PDP or disable it. When you choose to disable PDP, you cannot configure PDP.

The “HoldTime” parameter means the time to be saved before the router discards the received information if other PDP packets are not received.

The protocol version cannot be read currently through the command line “show run”, so the protocol version is not handled on the Web.

5.2.2 Configuring the Attributes of the PDP Port

If you click **Layer-2 Config -> PDP Config-> PDP port Config** in the navigation bar, the **Setting the attributes of the PDP port** page appears, as shown in figure 5.

Port	Status
G0/1	Enable PDP ▾

Figure 5 PDP port configuration

After the PDP port is configured, you can enable or disable PDP on this port.

5.3 LLDP Configuration

5.3.1 Configuring the Global Attributes of LLDP

If you click **Layer-2 Config -> LLDP Config** in the navigation bar, the **Global LLDP Config** page appears, as shown in figure 6.

Basic Config of LLDP Protocol	
Protocol State	Close the LLDP protocol ▾
HoldTime Settings	120 (0-65535)s
Reinit Settings	2 (2-5)s
Setting the packet transmission cycle	30 (5-65534)s

Help

◆HoldTime : Means the TTL(Time to live) of sending LLDP packets. Its default value is 120s.
◆Reinit : Means the delay of continuously sending LLDP packets. Its default value is 2s.

Figure 6 Configuring the global attributes of LLDP

You can choose to enable LLDP or disable it. When you choose to disable LLDP, you cannot configure LLDP.

The “HoldTime” parameter means the ttl value of the packet that is transmitted by LLDP, whose default value is 120s.

The “Reinit” parameter means the delay of successive packet transmission of LLDP, whose default value is 2s.

5.3.2 Configuring the Attributes of the LLDP Port

If you click **Layer-2 Config -> LLDP Config-> LLDP port Config** in the navigation bar, the **Setting the attributes of the LLDP port** page appears, as shown in figure 7.

Port	Receive LLDP Packet	Send LLDP Packet
G0/1	Disable ▾	Disable ▾
G0/2	Disable ▾	Disable ▾
G0/3	Disable ▾	Disable ▾
G0/4	Disable ▾	Disable ▾

Figure 7 Configuring the LLDP port

After the LLDP port is configured, you can enable or disable LLDP on this port.

5.4 Link Aggregation Configuration

If you click **Advanced Config -> Link aggregation Config** in the navigation bar, the **Link aggregation Config** page appears, as shown in figure 8.

The screenshot shows the 'Port Channel Global Loading Balance' configuration page. The main section is 'Port Aggregation Config'. It features a 'New' button at the top left. Below it, there are navigation and search options: 'No.0 Page/Total 0 Page', 'First', 'Prev', 'Next', 'Last', 'Go No.', 'Page', and 'Search:'. On the right, it shows 'Current 0 Item/Total 0 Item'. The main content area contains a table with the following columns: 'Aggregation Group', 'Mode', 'Configure port members', 'Valid port members', 'Speed', 'State', and 'Operate'. Below the table, there is a checkbox for 'Select All/Select None' and a 'Delete' button. At the bottom, there is a 'Help' section with a note: '#Note: The physical attributes of all the aggregated ports shall be the same, including Speed, Duplex mode and Vlan'.

Figure 8 Port aggregation configuration

If you click **New**, an aggregation group can be created. Up to 32 aggregation groups can be configured through Web and up to 8 physical ports in each group can be aggregated. If you click **Cancel**, you can delete a selected aggregation group; if you click **Modify**, you can modify the member port and the aggregation mode.

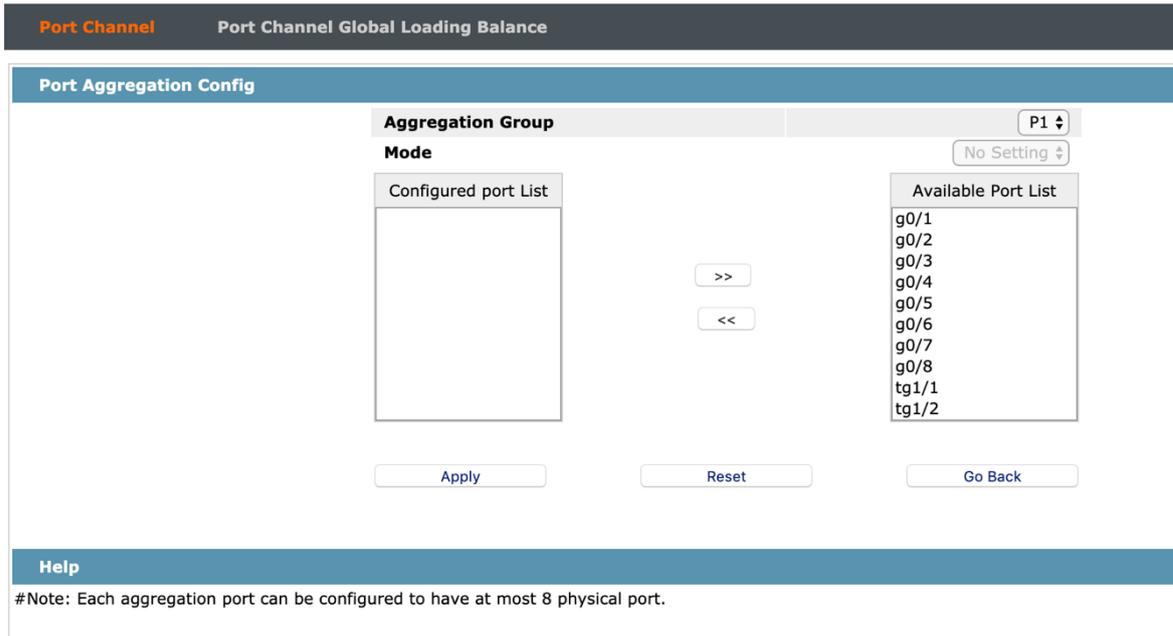


Figure 9: Setting the member port of the aggregation group

An aggregation group is selectable when it is created but is not selectable when it is modified. When a member port exists on the aggregation group, you can choose the aggregation mode to be **static**, **LACP active** or **LACP passive**. You can click “>>” and “<<” to delete and add a member port in the aggregation group.

5.5 STP Configuration

5.5.1 STP Status Information

If you click **Layer-2 Config -> STP Config** in the navigation bar, the **STP Config** page appears, as shown in figure 10.

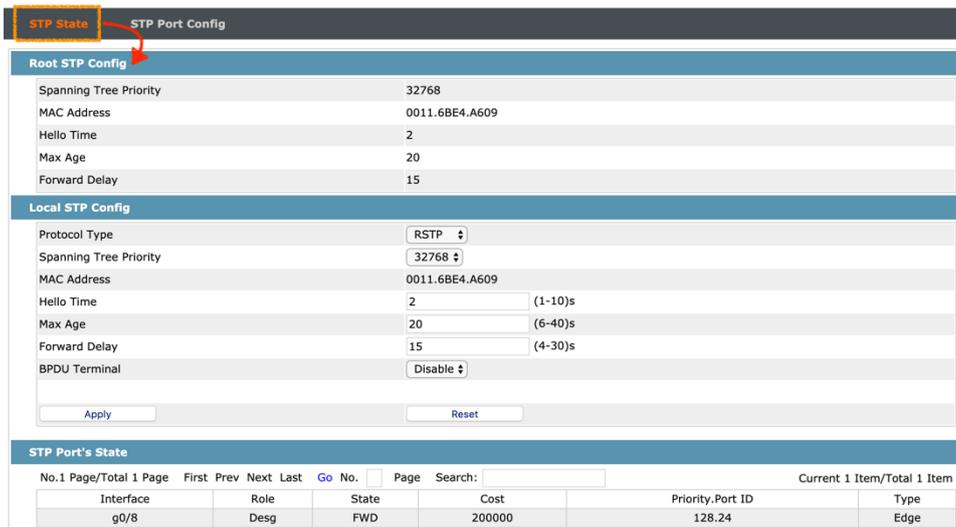


Figure 10 Configuring the global attributes of STP

The root STP configuration information and the STP port's status are only-read.

On the local STP configuration page, you can modify the running STP mode by clicking the Protocol type dropdown box. The STP modes include STP, RSTP and disabled STP.

The priority and the time need be configured for different modes.

Note:

The change of the STP mode may lead to the interruption of the network.

5.5.2 Configuring the Attributes of the STP Port

If you click the "Configure RSTP Port" option, the "Configure RSTP Port" page appears.

Port	Protocol Status	Priority(0~240)	Path-Cost(0~200000000)	Edge Port	RSTP Ring
g0/1	Enable	128	0	Disable	Disable
g0/2	Enable	128	0	Disable	Disable
g0/3	Enable	128	0	Disable	Disable
g0/4	Enable	128	0	Disable	Disable
g0/5	Enable	128	0	Disable	Disable
g0/6	Enable	128	0	Disable	Disable
g0/7	Enable	128	0	Disable	Disable
g0/8	Enable	128	0	Disable	Disable
tg1/1	Enable	128	0	Disable	Disable
tg1/2	Enable	128	0	Disable	Disable

Figure 11 Configuring the attributes of RSTP

The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to "Disable" and the STP mode is also changed, the port will not run the protocol in the new mode.

The default value of the path cost of the port is 0, meaning the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

5.6 IGMP-Snooping Configuration

5.6.1 IGMP-Snooping Configuration

If you click **Layer-2 Config** -> **IGMP snooping**, the IGMP-Snooping configuration page appears.

Port	Protocol Status	Priority(0~240)	Path-Cost(0~200000000)	Edge Port	RSTP Ring
g0/1	Enable	128	0	Disable	Disable
g0/2	Enable	128	0	Disable	Disable
g0/3	Enable	128	0	Disable	Disable
g0/4	Enable	128	0	Disable	Disable
g0/5	Enable	128	0	Disable	Disable
g0/6	Enable	128	0	Disable	Disable
g0/7	Enable	128	0	Disable	Disable
g0/8	Enable	128	0	Disable	Disable
tg1/1	Enable	128	0	Disable	Disable
tg1/2	Enable	128	0	Disable	Disable

Figure 12 IGMP-snooping configuration

On this page you can set whether to make a switch to forward unknown multicasts, whether to enable IGMP snooping, and whether to configure the switch as the querier of IGMP.

5.6.2 IGMP-Snooping VLAN List

If you click **Layer-2 Config -> IGMP snooping vlan list**, the **IGMP-Snooping VLAN list** page appears.

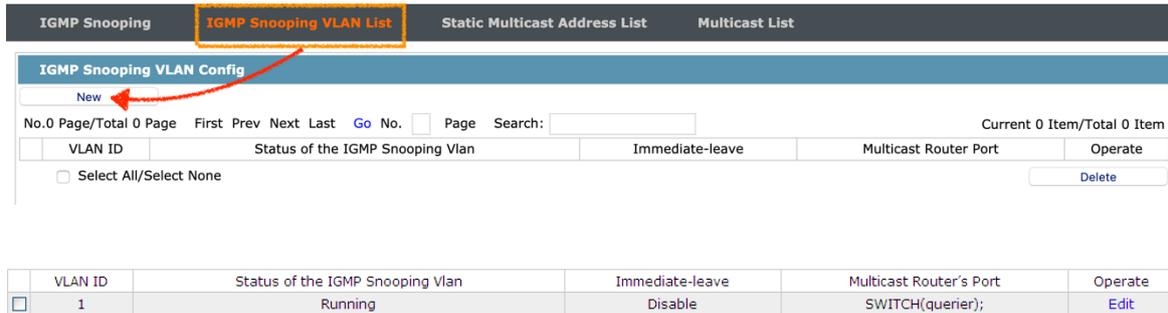


Figure 13: IGMP-snooping VLAN list

If you click **New**, IGMP-snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP snooping VLAN. If you click **Cancel**, a selected IGMP-Snooping VLAN can be deleted; if you click **Edit**, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.

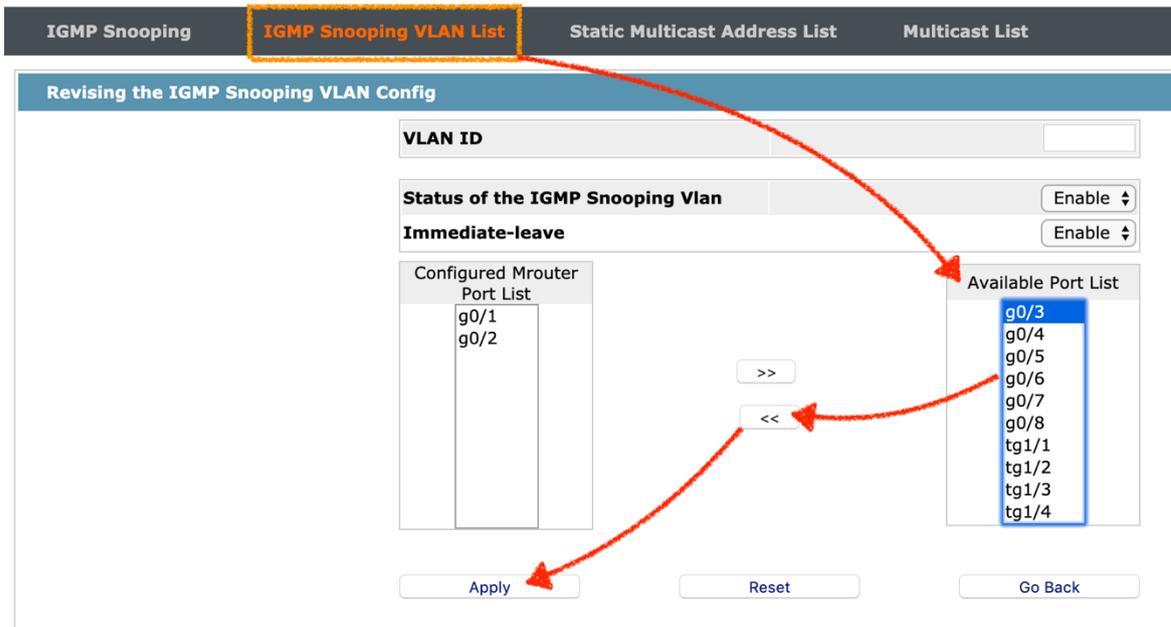


Figure 14: Static routing port of IGMP VLAN

When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click “>>” and “<<” to delete and add a routing port.

5.6.3 Static Multicast Address

If you click **Static multicast address**, the **Setting the static multicast address** page appears.

Figure 15 Multicast List

On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

Click “Refresh” to refresh the contents in the list.

5.6.4 Multicast List

Click the **Multicast List Info** option on the top of the page and the **Multicast List Info** page appears.

Figure 16 Multicast List

On this page the multicat groups, which are existent in the current network and are in the statistics of IGMP snooping, as well as port sets which members in each group belong to are displayed.

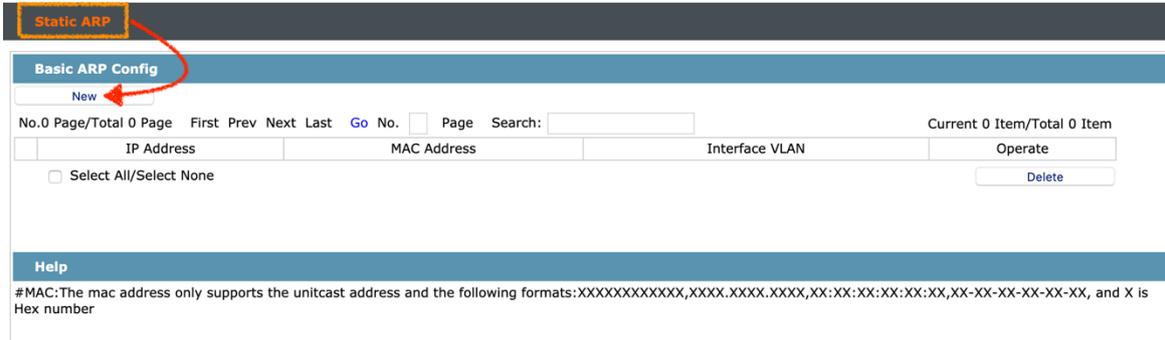
Click “Refresh” to refresh the contents in the list.

Note:

By default, a multicast list can display up to 15 VLAN items. You can modify the number of multicast items by running **ip http web igmp-groups** after you log on to the device through the Console port or Telnet.

5.7 Setting Static ARP

If you click **Layer-2 Config -> Static ARP Config**, the static ARP configuration page appears.



You can click **New** to add an ARP entry. If the **Alias** column is selected, it means to answer the ARP request of the designated IP address.

If you click **Edit**, you can modify the current ARP entry.

If you click **Cancel**, you can cancel the chosen ARP entry.

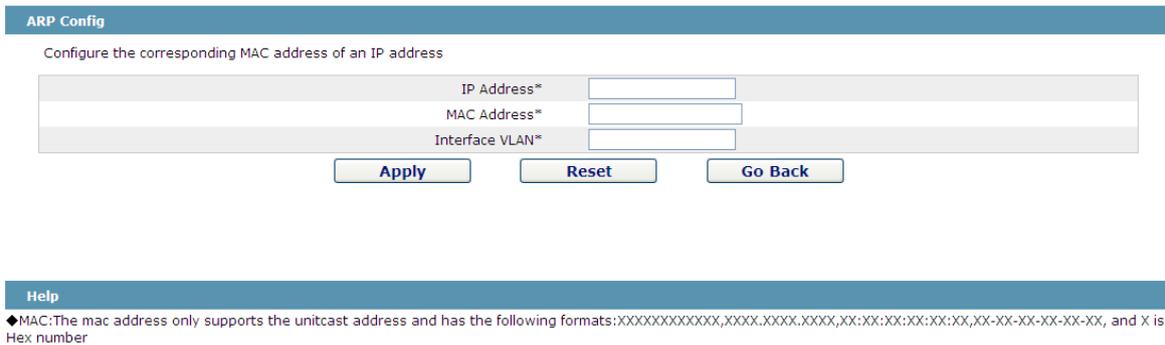


Figure 17 Setting static ARP

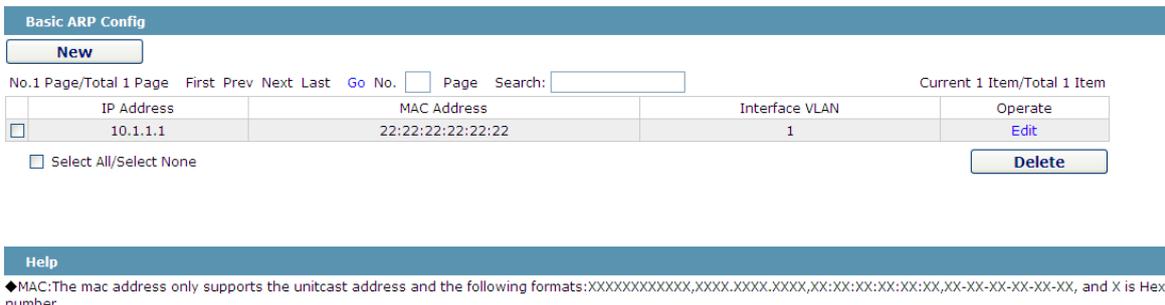


Figure 18 Displaying static ARP

5.8 Ring Protection Configuration

5.8.1 EAPS Ring List

If you click **Layer-2 Config -> Ring protection Config**, the **EAPS ring list** page appears.

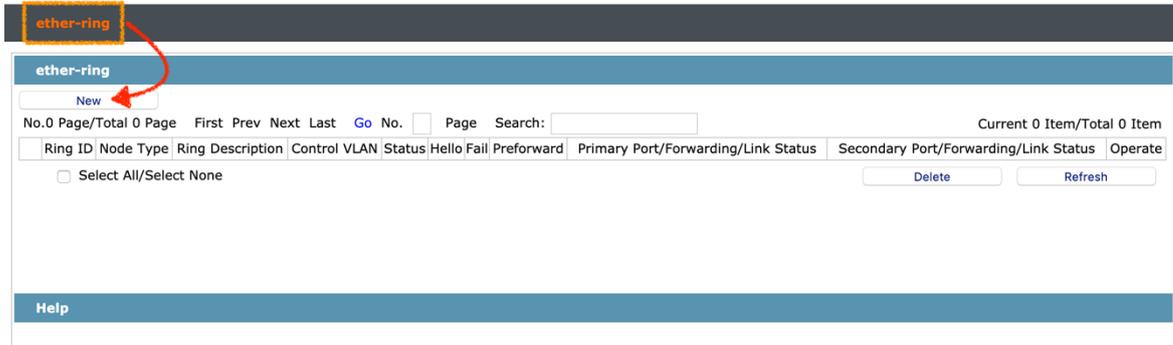


Figure 19 EAPS Ring List

In the list shows the currently configured EAPS ring, including the status of the ring, the forwarding status of the port and the status of the link.

Click “New” to create a new EAPS ring.

Click the “Operate” option to configure the “Time” parameter of the ring.

Note:

1. The system can support 8 EAPS rings.
2. After a ring is configured, its port, node type and control Vlan cannot be modified. If the port of the ring, the node type or the control Vlan need be adjusted, please delete the ring and then establish a new one.

5.8.2 EAPS Ring Configuration

If you click “New” on the EAPS ring list, or “Operate” on the right side of a ring item, the “Configure EAPS” page appears.

Figure 20 EAPS ring configuration

Note:

If you want to modify a ring, on this page the node type, the control VLAN, the primary port and the secondary port cannot be modified.

In the dropdown box on the right of "Ring ID", select an ID as a ring ID. The ring IDs of all devices on the same ring must be the same.

The dropdown box on the right of "Node Type" is used to select the type of the node. Please note that only one master node can be configured on a ring.

Enter a value between 1 and 4094 in the text box on the right of "Control VLAN" as the control VLAN ID. When a ring is established, the control VLAN will be automatically established too. Please note that if the designated control VLAN is 1 and the VLAN of the control device is also 1 the control device cannot access the control VLAN. Additionally, please do not enter a control VLAN ID that is same as that of another ring.

In the text boxes of "Primary Port" and "Secondary Port", select a port as the ring port respectively. If "Node Type" is selected as "Transit-Node", the two ports will be automatically set to transit ports.

Click "Apply" to finish EAPS ring configuration, click "Reset" to resume the initial values of the configuration, or click "Return" to go back to the EAPS list page.

5.9 DDM Configuration

If you click **L2 Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 5-21.

DDM Config

DDM Enable

Apply Reset

Help

Figure 23: DDM configuration

Chapter 6 Layer-3 Configuration

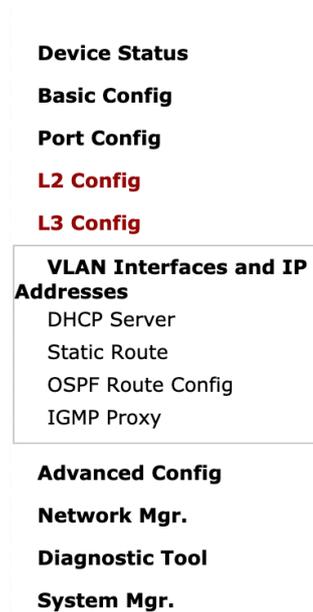


Figure 1: Layer-3 configuration list

Note:

Only layer-3 switches have the layer-3 configuration.

6.1 VLAN Interface and IP Address Configuring

If you click **Layer-3 Config -> VLAN interface and IP addresses**, the **Configuring the VLAN interface** page appears.

The screenshot shows the 'VLAN Interface Config' page. At the top, there is a 'New' button. Below it is a table with columns: Name of the VLAN Interface, IP Attribute, IP Address, and Operate. The table contains one row with the value '1' under 'Name of the VLAN Interface', 'Manual Config' under 'IP Attribute', and '192.168.1.1/24;' under 'IP Address'. The 'Operate' column has an 'Edit' link. There are also 'First', 'Prev', 'Next', 'Last', 'Go', 'Page', and 'Search' controls. A red arrow points from the 'VLAN Interfaces and IP Addresses' menu item to the 'New' button.

Name of the VLAN Interface	IP Attribute	IP Address	Operate
1	Manual Config	192.168.1.1/24;	Edit

Figure 2: Configuring the VLAN interface

Click **New** to add a new VLAN interface. Click **Cancel** to delete a VLAN interface. Click **Modify** to modify the settings of a corresponding VLAN interface.

When you click **New**, the name of the corresponding VLAN interface can be modified; but if you click **Modify**, the name of the corresponding VLAN interface cannot be modified.

Note:

On the Web page, you can only set the IP address of Interface Vlan1; if the L3 switch is used and more Vlan interfaces need be created, please make configuration after a successful login through the console port or Telnet.

VLAN Interface Config

IP Attribute

VLAN Interface Name*	<input type="text"/>
IP Attribute*	Manual Config ▼

Primary IP Address

IP Address*	<input type="text"/>
MASK address*	<input type="text"/>

Secondary IP Address 1

IP Address*	<input type="text"/>
MASK address*	<input type="text"/>

Secondary IP Address 2

IP Address*	<input type="text"/>
MASK address*	<input type="text"/>

Apply
Reset
Go Back

Help

The primary IP must be configured for the VLAN interface before the secondary IP is configured

Figure 3: VLAN interface configuration

Note:

Before the accessory IP of a VLAN interface is set, you have to set the main IP.

6.2 Setting the Static Route

If you click **Layer-3 Config -> Static route Config**, the **Static route configuration** page appears.



Figure 4 Displaying the static route

Click **Create** to add a static route.

If you click **Edit**, you can modify the current static route.

If you click **Cancel**, you can cancel the chosen static route.

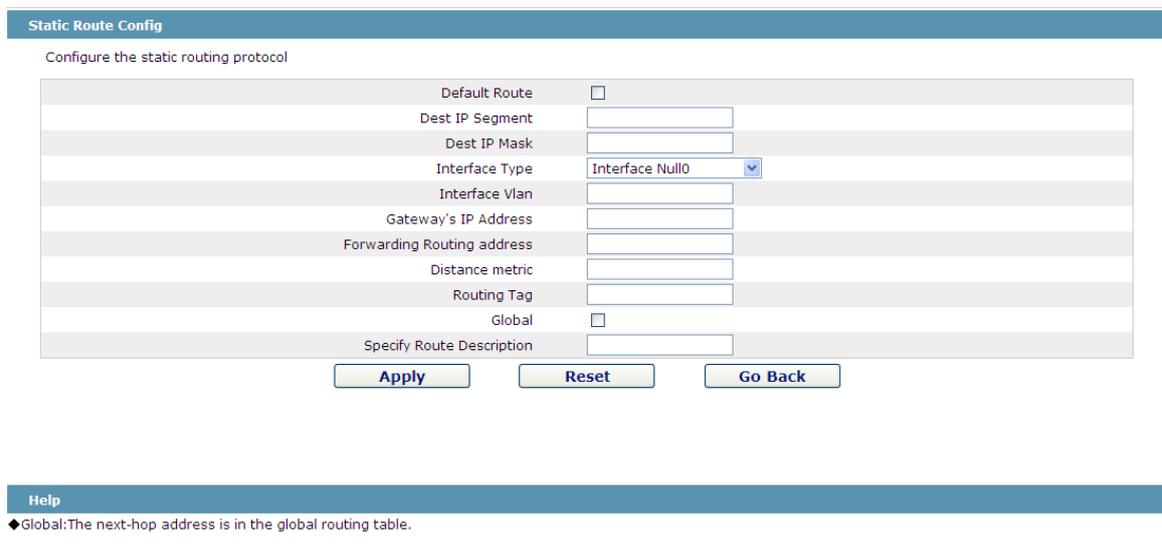


Figure 5: Setting the static route

6.3 IGMP Agent

6.3.1 Enabling the IGMP Agent

If you click **Layer-3 Config -> IGMP agent**, the **IGMP agent** page appears.



Figure 6: Enabling the IGMP agent

On this page you can enable or disable the IGMP agent. It is noted that the IGMP agent can be enabled or disabled on a switch only after the IP IGMP-snooping function is enabled on the switch.

6.3.2 Setting the IGMP Agent

If you click **Layer-3 Config -> IGMP agent -> IGMP agent Config**, the **IGMP agent configuration** page appears. Click **New** to create a new IGMP agent.



New IGMP Proxy	
Agent VLAN*	1
Client VLAN*	1
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Go Back"/>	

Figure 7: Setting the IGMP agent

Chapter 7 Advanced Configuration



Figure 1 A list of advanced configuration

7.1 QoS Configuration

7.1.1 Configuring QoS Port

If you click **Advanced Config -> QoS -> Configure QoS Port**, the **Port Priority Config** page appears.

Port	COS value
G0/1	0
G0/2	0
G0/3	0
G0/4	0
G0/5	
G0/6	
G0/7	
G0/8	
G0/9	
G0/10	
G0/11	

Figure 2 Configuring the QoS Port

You can set the CoS value by clicking the dropdown box on the right of each port and selecting a value. The default CoS value of a port is 0, meaning the lowest priority. If the CoS value is 7, it means that the priority is the highest.

7.1.2 Global QoS Configuration

If you click **Advanced Config -> QoS Config -> Global QoS Config**, the **Port's QoS parameter configuration** page appears.

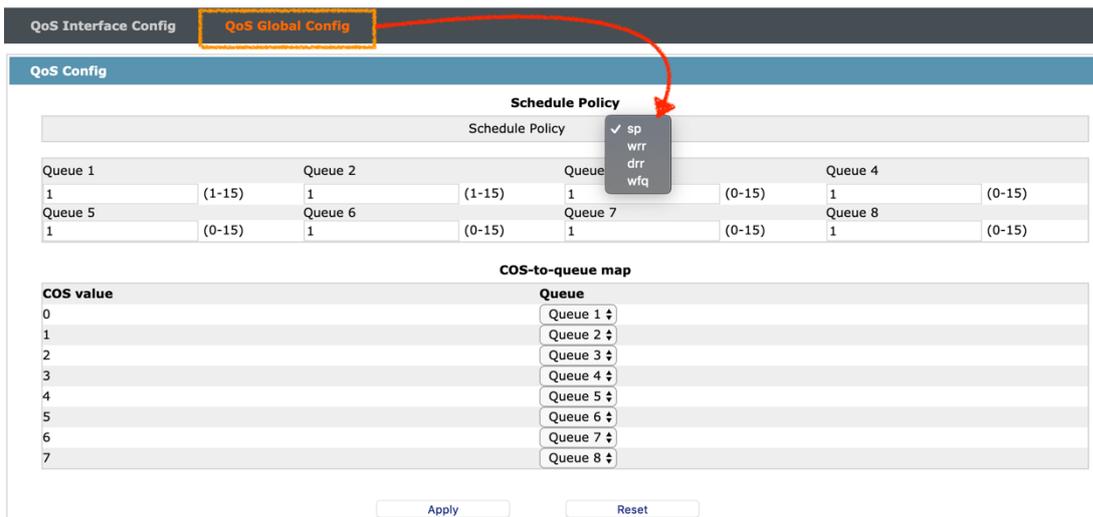
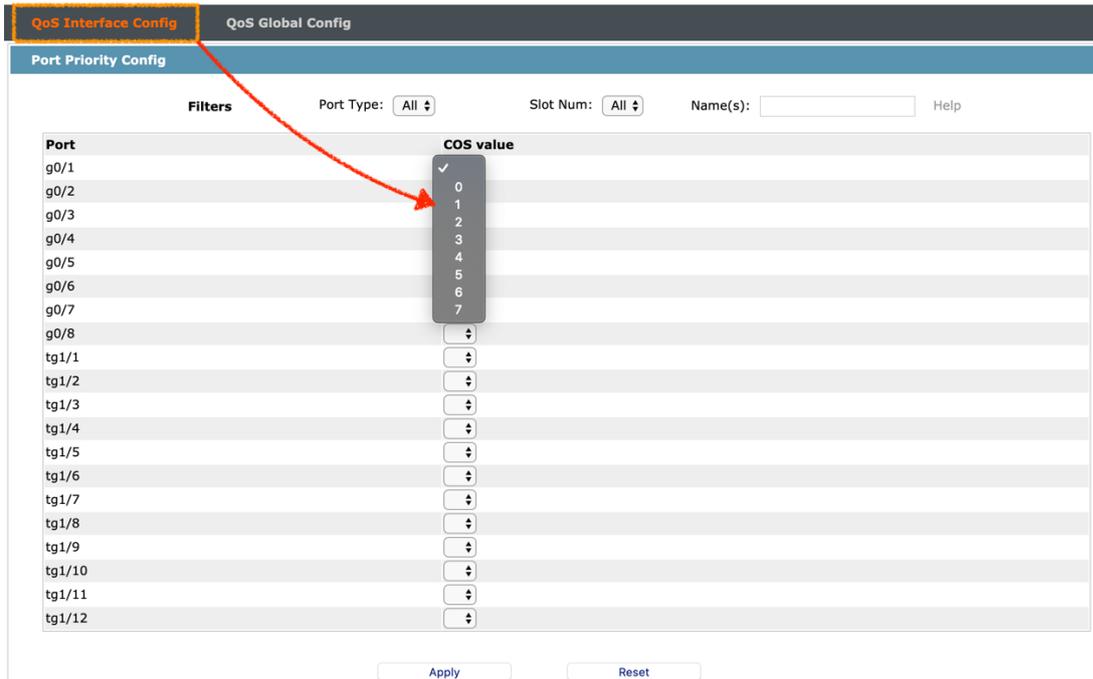


Figure 3 Configuring global QoS attributes

In WRR schedule mode, you can set the weights of the QoS queues. There are 4 queues, among which queue 1 has the lowest priority and queue 4 has the highest priority.

7.2 MAC Access Control List

7.2.1 Setting the Name of the MAC Access Control List

If you click **Advanced Config** -> **MAC access control list** -> **MAC access control list Config**, the MAC ACL configuration page appears.

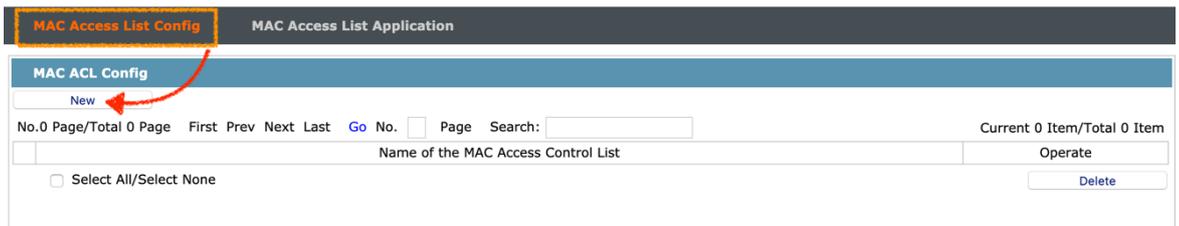


Figure 4: MAC access control list configuration

Click **New** to add a name of the MAC access control list. Click **Cancel** to delete a MAC access control list.

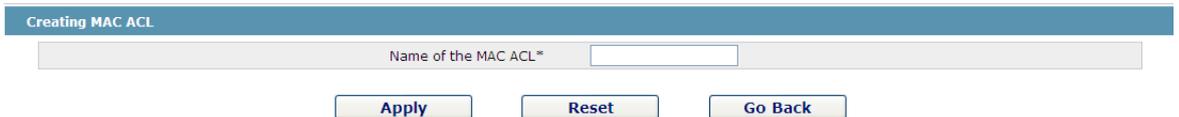


Figure 5: Setting the name of MAC access control list

7.2.2 Setting the Rules of the MAC Access Control List

If you click **Modify**, the corresponding MAC access control list appears and you can set the corresponding rules for the MAC access control list.

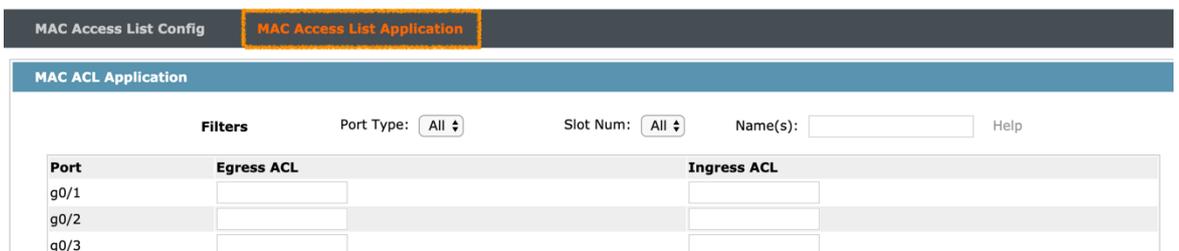


Figure 6: Specific MAC access control list configuration

Click **New** to add a rule of the MAC access control list. Click **Cancel** to delete a rule of the MAC access control list.

New MAC ACL Regulation

NewMAC ACLmyaclItem

Authority	permit
Src MAC Type*	host
Src MAC*	000100020003
Src MAC Mask*	
Dst MAC Type*	any
Dst MAC*	
Dst MAC Mask*	

[Apply](#) [Reset](#) [Go Back](#)

Help

◆MAC: the valid mac address can be one of the following formats: XXXXXXXXXXXX, XXXX.XXXX.XXXX, XX:XX:XX:XX:XX:XX, and XX-XX-XX-XX-XX-XX, among which X is a Hex number

Figure 7: Setting the Rules of the MAC Access Control List

7.2.3 Applying the MAC Access Control List

If you click **Advanced Config -> MAC access control list -> Applying the MAC access control list**, the **Applying the MAC access control list** page appears.

Port	Egress ACL	Ingress ACL
G0/1	<input type="text"/>	<input type="text"/>
G0/2	<input type="text"/>	<input type="text"/>
G0/3	<input type="text"/>	<input type="text"/>
G0/4	<input type="text"/>	<input type="text"/>
G0/5	<input type="text"/>	<input type="text"/>
G0/6	<input type="text"/>	<input type="text"/>
G0/7	<input type="text"/>	<input type="text"/>

Figure 8: Applying the MAC access control list

7.3 IP Access Control List

7.3.1 Setting the Name of the IP Access Control List

If you click **Advanced Config -> IP access control list -> IP access control list Config**, the IP ACL configuration page appears.

IP ACL Config

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 2 Item/Total 2 Item

	Name of the IP ACL	Attribute of the IP ACL	Operate
<input type="checkbox"/>	acla	extended	Edit
<input type="checkbox"/>	myacl	standard	Edit

Select All/Select None [Delete](#)

Figure 9: IP access control list configuration

Click **New** to add a name of the IP access control list. Click **Cancel** to delete an IP access control list.

Figure 10: Creating a name of the IP access control list

If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

7.3.2 Setting the Rules of the IP Access Control List

➤ Standard IP access control list

Authority	Src IP	Src IP Mask	Record the log	Operate
permit	1.1.1.1	255.255.255.0	log	Edit

Figure 11: Standard IP access control list

Click **New** to add a rule of the IP access control list. Click **Cancel** to delete a rule of the IP access control list. If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

Figure 12: Setting the Rules of the standard IP access control list

➤ Extended IP access control list

Authority	Mask Type	Protocol Number	Src Address	Src Port	Dst Address	Dst Port	Time-Range	Tos	Precedence	Do not fragment the flag	Fragmented Packet	Offset	Length of the IP packet	Time-to-live Value	Record the log	Operate
permit	Mask	0	1.1.1.1/255.255.255.0	any		10									log	Edit

Figure 13: Extended IP access control list

Click **New** to add a rule of the IP access control list. Click **Cancel** to delete a rule of the IP access control list. If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

Authority	permit
Mask Type	Mask
Protocol Number*	0
Src IP Type	Specify IP
Src IP*	1.1.1.1
Src IP Mask*	255.255.255.0
Src Interface Vlan*	
Src IP Range*	
Src Port	
Src Port Range	
Dst IP Type	any
Dst IP*	
Dst IP Mask*	
Dst Interface Vlan*	
Dst IP Range*	
Dst Port	
Dst Port Range	
Time-Range	10
Tos	
Precedence	
Do not fragment	
Fragmented Packet	
Offset	
Length of the IP Packet	
Time-to-live Value	
Log	<input checked="" type="checkbox"/>
Location	1

Figure 14: Setting the Rules of the extended IP access control list

7.3.3 Applying the IP Access Control List

If you click **Advanced Config -> IP access control list -> Applying the IP access control list**, the **Applying the IP access control list** page appears.

Port	Egress ACL	Ingress ACL
G0/1	myacl	
G0/2		acla
G0/3		
G0/4		
G0/5		
G0/6		
G0/7		
G0/8		

Figure 15: Applying the IP access control list

Chapter 8 Network Management Configuration



Figure 1: Network management configuration list

8.1 SNMP Configuration

If you click **Network management Config -> SNMP management** in the navigation bar, the **SNMP management** page appears, as shown in figure 2.

8.1.1 SNMP Community Management

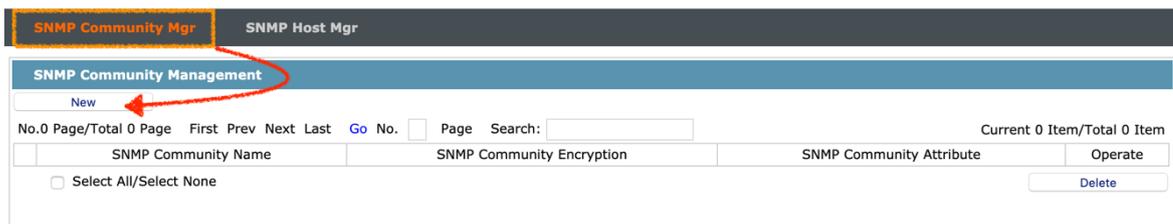


Figure 2 SNMP community management

On the SNMP community management page, you can know the related configuration information about SNMP community.

You can create, modify or cancel the SNMP community information, and if you click **New** or **Edit**, you can switch to the configuration page of SNMP community.

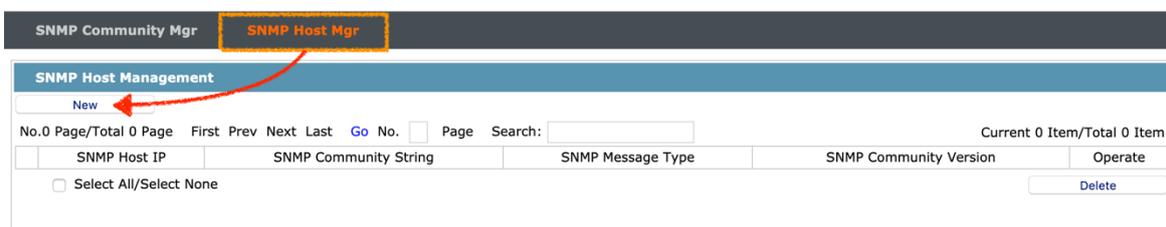


The screenshot shows the 'SNMP Community Management' page. It features a form with two input fields: 'SNMP Community Name' with the value 'public' and a note 'Input less than 20 characters', and 'SNMP Community Attribute' with a dropdown menu set to 'Read Only'. Below the form are two buttons: 'Apply' and 'Go Back'.

Figure 4.2 SNMP community management settings

On the SNMP community management page you can enter the SNMP community name, select the attributes of SNMP community, which include Read only and Read-Write.

8.1.2 SNMP Host Management



The screenshot shows the 'SNMP Host Management' page. At the top, there are two tabs: 'SNMP Community Mgr' and 'SNMP Host Mgr', with the latter highlighted. Below the tabs is a 'New' button. A table header is visible with columns: 'SNMP Host IP', 'SNMP Community String', 'SNMP Message Type', 'SNMP Community Version', and 'Operate'. Below the table is a 'Delete' button and a 'Select All/Select None' checkbox. Navigation controls include 'No. 0 Page/Total 0 Page', 'First', 'Prev', 'Next', 'Last', 'Go No.', 'Page', 'Search:', and 'Current 0 Item/Total 0 Item'.

Figure 4 SNMP host management

On the SNMP community host page, you can know the related configuration information about SNMP host.

You can create, modify or cancel the SNMP host information, and if you click **New** or **Edit**, you can switch to the configuration page of SNMP host.



The screenshot shows the 'SNMP Host Management' configuration page. It features a form with four input fields: 'SNMP Host IP', 'SNMP Community', 'SNMP Message Type' (set to 'Traps' with a note '* Informs is not supported in version v1'), and 'SNMP Community Version' (set to 'v1'). Below the form are two buttons: 'Apply' and 'Go Back'.

Figure 5 SNMP host management settings

On the SNMP host configuration page, you can enter **SNMP Host IP**, **SNMP Community**, **SNMP Message Type** and **SNMP Community Version**. **SNMP Message Type** includes **Traps** and **Informs**, and as to version 1, **SNMP Message Type** does not support **Informs**.

8.2 RMON

8.2.1 RMON Statistic Information Configuration

If you click **Network Management Config -> RMON -> RMON Statistics -> New**, the **RMON Statistics** page appears.

Figure 6 Configuring the RMON statistic information

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

At present, the monitor statistic information can be obtained through the command line “show rmon statistics”, but the Web does not support this function.

8.2.2 RMON History Information Configuration

If you click **Network Management Config -> RMON -> RMON history -> New**, the **RMON history** page appears.

RMON Statistics **RMON History** RMON Alarm RMON Event

RMON History

New

No.0 Page/Total 0 Page First Prev Next Last Go No. Page Search: Current 0 Item/Total 0 Item

Index	Sampling Number	Sampling Interval	Interface	Owner	Operate
<input type="checkbox"/> Select All/Select None					

Delete

Help

#Sampling Number means how many history items must be saved recently.

Interface History config

Interface	G0/1	
Index		(1-65535)
Sampling Number	50	(1-65535)
Sampling Interval	1800	(1-3600)
Owner	config	Enter less than 31 characters*

Apply Go Back

Help

◆Sampling Number means how many history items must be saved recently

Figure 7 Configuring the RMON history information

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

The sampling number means the items that need be reserved, whose default value is 50.

The sampling interval means the time between two data collection, whose default value is 1800s.

At present, the monitor statistic information can be obtained through the command line "show rmon history", but the Web does not support this function.

8.2.3 RMON Alarm Information Configuration

If you click **Network Management Config -> RMON -> RMON Alarm -> New**, the **RMON Alarm** page appears.

RMON Statistics RMON History **RMON Alarm** RMON Event

RMON Alarm

New

No.0 Page/Total 0 Page First Prev Next Last Go No. Page Search: Current 0 Item/Total 0 Item

Index	OID	Interface	Sampling Interval	Alarm type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Operate
<input type="checkbox"/> Select All/Select None										

Delete

Help

#OID is the OID of the monitored MIB node.

#The relevant event will be triggered when the rising threshold or falling threshold is exceeded.

RMON Alarm config

Index	<input type="text" value="1"/>	(1-65535)
MIB Node	<input type="text" value="IfnOctets"/>	
OID	<input type="text" value="1.3.6.1.2.1.2.1.10"/>	
Interface	<input type="text" value="G0/1"/>	
Alarm type	<input type="text" value="absolute"/>	
Sampling Interval	<input type="text" value="5"/>	(1-2147483647)
Rising Threshold	<input type="text" value="5"/>	(-2147483648 - 2147483647)
Rising Event Index	<input type="text" value="2"/>	(1-65535)
Falling Threshold	<input type="text" value="6"/>	(-2147483648 - 2147483647)
Falling Event Index	<input type="text" value="3"/>	(1-65535)
Owner	<input type="text" value="default"/>	Enter less than 31 characters*

Help

◆The owner can be empty
*◆The string you totally entered is limited in 255 characters

Figure 8 Configuring the RMON alarm information

The index is used to identify a specific alarm information; if the index is same to the previously applied index, it will replace the previous one.

The MIB node corresponds to OID.

If the alarm type is **absolute**, the value of the MIB object will be directly monitored; if the alarm type is **delta**, the change of the value of the MIB object in two sampling will be monitored.

When the monitored MIB object reaches or exceeds the rising threshold, the event corresponding to the index of the rising event will be triggered.

When the monitored MIB object reaches or exceeds the falling threshold, the event corresponding to the index of the falling event will be triggered.

8.2.4 RMON Event Configuration

If you click **Network Management Config -> RMON -> RMON Event -> New**, the **RMON event** page appears.

RMON Statistics
RMON History
RMON Alarm
RMON Event

RMON Event

No.0 Page/Total 0 Page First Prev Next Last Go No. Page Search: Current 0 Item/Total 0 Item

Index	Enable log	Community	Description	Owner	Operate
<input type="checkbox"/> Select All/Select None					

Help

#If the log is enabled◆◆the items will be added to the log table at the trigger of the event.

RMON Event Config

Index	<input type="text" value="1-65535"/>	(1-65535)
Owner	<input type="text"/>	
Description	<input type="text"/>	
Enable log	<input type="checkbox"/>	
Enable trap	<input type="checkbox"/>	
Community	<input type="text"/>	

Apply **Go Back**

Help

- ◆ If the log is enabled, the items will be added to the log table at the trigger of the event.
- ◆ If the trap is enabled, the trap will be generated with the event community name.
- *◆ The string you totally entered is less than 255 characters

Figure 9 RMON event configuration

The index corresponds to the rising event index and the falling event index that have already been configured on the **RMON alarm config** page.

The owner is used to describe the descriptive information of an event.

"Enable log" means to add an item of information in the log table when the event is triggered.

"Enable trap" means a trap will be generated if the event is triggered.

Chapter 9 Diagnosis Tools



Figure 1: Diagnosis tool list

9.1 Ping

If you click **Diagnosis Tools -> Ping**, the **Ping** page appears.

Ping

Ping is a typical network tool, which is used to identify the states of some network functions. The states of network functions are the basis of regular network diagnosis. Ping is used to check whether the peer is reachable. If Ping transmits a packet to the host and receives a response from the peer, the peer is reachable.

PING test-->	
Destination address*	<input type="text"/>
Source IP address	<input type="text"/> (An option which can be null)
Size of the PING packet	<input type="text"/> (36-20000) (An option which can be null)

Help

- ◆The ping program can test whether a destination can be reached, or it can test the packet loss to reach a destination.
- ◆Destination address: Enter the to-be-tested destination address.
- ◆Source IP: Source IP.
- ◆Packet's size: Designate the size of a packet when the packet is used to ping a destination. It is optional and cannot be configured.

Figure 2 Ping

Ping is used to test whether the switch 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.

"Size of the PING packet" is used to set the length of the Ping packet which is transmitted by the device.

Chapter 10 System Management

Device Status
Basic Config
Port Config
L2 Config
L3 Config
Advanced Config
Network Mgr.
Diagnostic Tool
System Mgr.

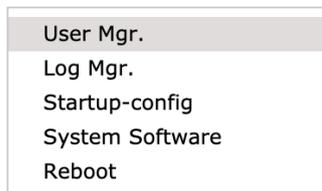


Figure 1 Navigation list of system management

10.1 User Management

10.1.1 User List

If you click **System Manage -> User Manage**, the **User Management** page appears.

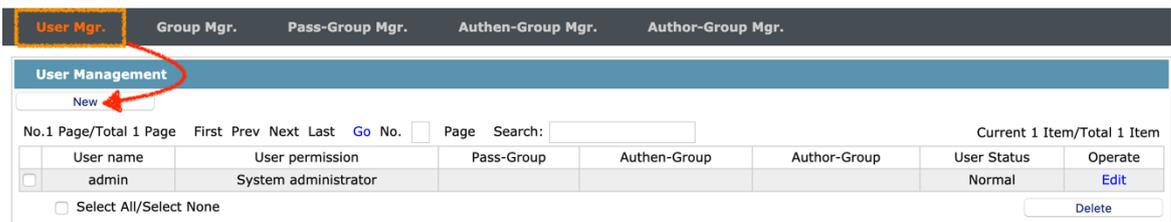


Figure 2 User list

You can click “New” to create a new user.

To modify the permission or the login password, click “Edit” on the right of the user list.

Note:

1. Please make sure that at least one system administrator exists in the system, so that you can manage the devices through Web.
2. The limited user can only browse the status of the device.

10.1.2 Establishing a New User

If you click “New” on the **User Management** page, the **Creating User** page appears.

User Management	
User name	<input type="text"/>
Password	<input type="password"/>
Confirming password	<input type="password"/>
Pass-Group	<input type="text"/>
Authen-Group	<input type="text"/>
Author-Group	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Go Back"/>	

Figure 3 Creating new users

In the “User name” text box, enter a name, which contains letters, numbers and symbols except “?”, “\”, “&”, “#” and the "Space" symbol. \ " & #和空格以外的字符。

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

In the “User permission” dropdown box set the user’s permission. The “System administrator” user can browse the status of the device and conduct relevant settings, while the limited user can only browse the status of the device.

10.2 Log Management

If you click **System Manage -> Log Manage**, the **Log Management** page appears.

Log Management	
System logs will be sent to the server when it is enabled	
Enable the log server	<input checked="" type="checkbox"/>
Address of the log server	<input type="text" value="192.168.1.77"/>
Level of system logs	<input type="text" value="(7-debugging)"/>
Enable the log buffer	<input type="checkbox"/>
Size of the log buffer	<input type="text" value="4096"/> (Bytes)
Level of cache logs	<input type="text" value="(7-debugging)"/>
<input type="button" value="Apply"/>	

Figure 4 Log management

If “Enabling 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 system log server” textbox and select the log’s grade in the “Grade of the system log information” dropdown box.

If “Enabling the log buffer” is selected, the device will record the log information to the memory. By logging on to the device through the Console port or Telnet, you can run the command “show log” to browse the logs which are saved on the device. The log information which is saved in the memory will be lost after rebooting. Please enter the size of the buffer area in the “Size of the system log buffer” textbox and select the grade of the cached log in the “Grade of the cache log information” dropdown box.

10.3 Managing the Configuration Files

If you click **System Manage -> Configuration file**, the **Configuration file** page appears.

10.3.1 Exporting the Configuration Information



Figure 5 Exporting the configuration file

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.

10.3.2 Importing the Configuration Information



Figure 6 Importing the configuration files

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.

10.4 Software Management

If you click **System Manage -> Software Upgrade**, the software management page appears.

10.4.1 Backing up the IOS Software

Figure 7 Backing up IOS

On this page the currently running software version is displayed. If you want to backup IOS, please click “Backuping IOS”; then on the browser the file download dialog box appears; click “Save” to store the IOS file to the disk of the PC, mobile storage device or other network location. Upgrading the IOS Software

Note:

1. Please make sure that your upgraded IOS matches the device type, because the matchable IOS will not lead to the normal startup of the device.
2. The upgrade of IOS probably takes one to two minutes; when the “updating” button is clicked, the IOS files will be uploaded to the device.
3. If errors occur during upgrade, please do not restart the device or cut off the power of the device, or the device cannot be started. Please try the upgrade again.
4. After the upgrade please save the configuration and then restart the device to run the new IOS.

Figure 8 Upgrading the IOS software

The upgraded IOS is always used to solve the already known problems or to perfect a specific function. If you device run normally, do not upgrade your IOS software frequently.

If IOS need be upgraded, please first enter the complete path of the new IOS files in the textbox on the right of “Upgrading IOS”, or click the “Browsing” button and select the new IOS files on your computer, and then click “Updating”.

10.5 Resuming Initial Configuration

If you click **System Manage -> Resume Config**, the **Resuming the original configuration** page appears.

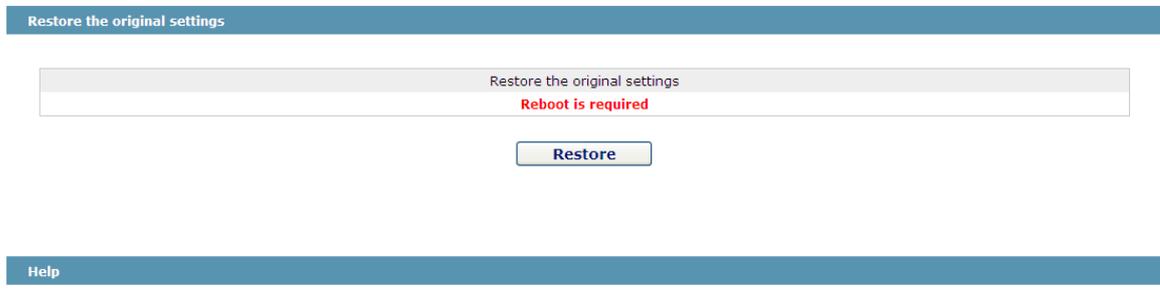


Figure 9 Resuming the original configuration

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 192.168.1.1/255.255.255.0, and the username and password are both “admin”.

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

10.6 Rebooting the Device

If you click **System Manage -> Reboot Device**, the **Rebooting** page appears.

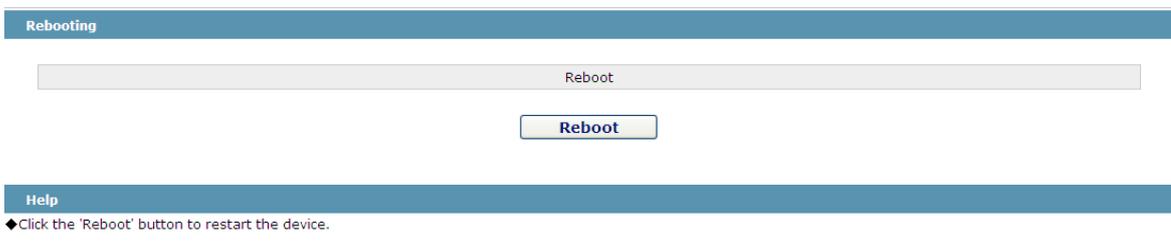


Figure 10 Rebooting the device

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.