
Web Configuration

Table of Contents

Chapter 1 HTTP Switch Configuration.....	1
1.1 HTTP Configuration.....	1
1.1.1 Choosing the Prompt Language	1
1.1.2 Setting the HTTP Port	1
1.1.3 Enabling the HTTP Service.....	1
1.1.4 Setting the HTTP Access Mode	1
1.1.5 Setting the Maximum Number of VLAN Entries on Web Page	2
1.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page.....	2
1.2 HTTPS Configuration	2
1.2.1 Setting the HTTP Access Mode	2
1.2.2 It is used to set the HTTPS port.....	2
Chapter 2 Configuration Preparation.....	错误！未定义书签。
2.1 Accessing the Switch Through HTTP	3
2.1.1 Initially Accessing the Switch	3
2.1.2 Upgrading to the Web-Supported Version.....	4
2.2 Accessing a Switch through Secure Links.....	4
2.3 Introduction of Web Interface	5
2.3.1 Top Control Bar	5
2.3.2 Navigation Bar.....	5
2.3.3 Configuration Information Area	6
2.3.4 Configuration Area	6
Chapter 3 Basic Configuration.....	7
3.1 Hostname Configuration.....	7
3.2 Time Management.....	7
Chapter 4 Configuration of the Physical Interface	9
4.1 Configuring Port Description	9
4.2 Configuring the Attributes of the Port	9
4.3 Rate control	10
4.4 Port mirroring.....	10
4.5 Loopback Detection.....	11
4.6 Port security	11
4.6.1 IP Binding Configuration.....	11
4.6.2 MAC Binding Configuration.....	11
4.6.3 Setting the Static MAC Filtration Mode	12
4.6.4 Static MAC Filtration Entries	12
4.6.5 Setting the Dynamic MAC Filtration Mode	12
4.7 Storm control	12
4.7.1 Broadcast Storm Control.....	13
4.7.2 Multicast Storm Control.....	13
4.7.3 Unknown Unicast Storm Control.....	13
4.8 Port Protect Group Configuration	13
4.8.1 Port Protect Group List.....	13

4.8.2 Port Protect Group Interface Configuration	14
4.9 POE Management	14
4.9.1 POE Global Configuration	14
4.9.2 POE Global Real-time Information	14
4.9.3 POE Port List	15
4.9.4 POE Ports' Policy Power-up	15
4.9.5 POE Ports' Power Real-time Information	16
4.9.6 POE Ports' Other Real-time Information	16
Chapter 5 Layer-2 Configuration	18
5.1 VLAN Settings	18
5.1.1 VLAN List	18
5.1.2 VLAN Settings	19
5.2 GVRP Configuration	20
5.2.1 GVRP Global Attribute Configuration	20
5.2.2 Global Interface Attribute Configuration	20
5.3 STP Configuration	20
5.3.1 STP Status Information	20
5.3.2 Configuring the Attributes of the STP Port	21
5.4 IGMP-Snooping Configuration	22
5.4.1 IGMP-Snooping Configuration	22
5.4.2 IGMP-Snooping VLAN List	22
5.4.3 Static Multicast Address	23
5.4.4 Multicast List	24
5.5 Setting Static ARP	24
5.6 Static MAC Address Configuration	25
5.7 LLDP Configuration	26
5.7.1 Configuring the Global Attributes of LLDP	26
5.7.2 LLDP Port Attribute Configuration	26
5.8 DDM Configuration	26
5.9 Port Aggregation Configuration	27
5.9.1 Port Aggregation Configuration	27
5.9.2 Port Channel Group Loading Balance Configuration	28
5.10 Ring Protection Configuration	28
5.10.1 EAPS Ring List	28
5.10.2 EAPS Ring Configuration	29
5.11 MEAPS Configuration	29
5.11.1 MEAPS Ring Network List	29
5.10.2 EAPS Ring Network Configuration	30
5.11.2 New MEAPS Global Configuration	错误！未定义书签。
5.12 Backup Link Protocol Configuration	31
5.12.1 Backup Link Protocol Global Configuration	31
5.12.2 Backup Link Protocol Interface Configuration	31
5.13 MTU Configuration	32
5.14 PDP Configuration	32
5.14.1 Configuring the Global Attributes of PDP	32
5.14.2 PDP Interface Attribute Configuration	33

Chapter 6 Layer-3 Configuration	34
6.1 Configuring the VLAN Interface.....	34
6.2 Static Routing Configuration.....	35
Chapter 7 Advanced Configuration	37
7.1 QoS Configuration.....	37
7.1.1 Configuring QoS Port.....	37
7.1.2 Global QoS Configuration	38
7.2 IP Access Control List.....	38
7.2.1 Setting the Name of the IP Access Control List.....	38
7.2.2 Setting the Rules of the IP Access Control List.....	39
7.2.3 Applying the IP Access Control List.....	40
7.3 MAC Access Control List.....	41
7.3.1 Setting the Name of the MAC Access Control List.....	41
7.3.2 Setting the Rules of the MAC Access Control List	41
7.3.3 Applying the MAC Access Control List.....	42
Chapter 8 Network Management Configuration	43
8.1 SNMP Configuration.....	43
8.1.1 SNMP Community Management.....	43
8.1.2 SNMP Host Management.....	44
8.2 RMON	44
8.2.1 RMON Statistic Information Configuration	44
8.2.2 RMON History Information Configuration.....	45
8.2.3 RMON Alarm Information Configuration.....	46
8.2.4 RMON Event Configuration.....	46
Chapter 9 Diagnosis Tools	48
9.1 Ping	48
9.1.1 Ping.....	48
Chapter 10 System Management.....	50
10.1 User Management.....	50
10.1.1 User List.....	50
10.1.2 Establishing a New User	51
10.1.3 User Group Management.....	51
10.1.4 Password Group Management	52
10.1.5 Authentication Group Configuration	53
10.1.6 Author-Group Management.....	53
10.2 Log Management	54
10.3 Managing the Configuration Files.....	54
10.3.1 Exporting the Configuration Information.....	54
10.3.2 Importing the Configuration Information.....	55
10.4 Software Management	55
10.4.1 Backing up the IOS Software	55
10.4.2 Upgrading the IOS Software	56
10.5 Rebooting the Device	56

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
[no] ip http language { english }	Sets the prompt language of Web configuration to 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
ip http port { <i>portNumber</i> }	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
ip http server	Enables the HTTP service.

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
---------	---------

ip http http-access enable	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 Accessing the Switch

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 192.168.0.2 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 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", which is capital sensitive.



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 "Switch_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 "Switch_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://192.168.0.1** on the address bar (**192.168.0.1** 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 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](#) | [English](#) | [Chinese](#) | [Logout](#) | [Port Panel](#) | [About](#)

Figure 2: 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.
Port Panel	Displays the simple port panel.
About	Displays vendor information and sets automatic refresh.

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

Device Status

Runtime Info

- Interface State
- Interface Flow
- Mac Address Table
- Log Query
- Optical Module Info

Basic Info

- Port Info
- L2 Config
- L3 Config
- Advanced Config
- Network Mgr.
- Dagnostic Tool
- System Mgr.

Figure 3 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 Information Area

System Information	
Device Type	SWITCH
BIOS Version	0.4.1
Device Version	2.2.0C Build 36608
Series No.	E20005050101
Mac Address	8479.733A.2000
IP Address	192.168.0.1
Current Time	1970-1-1 0:14:31
UP Time	0 Day- 0 Hour- 14 Minute- 31 Second
CUP Usage	2%
Memory Usage	26%

[Refresh](#)

Figure 4 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 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 Hostname Configuration

If you click **Basic Config** -> **Hostname Config** in the navigation bar, the **Hostname Configuration** page appears, as shown in figure 2.

Hostname Configuration

Configure the hostname.

Hostname*

Apply **Reset**

Help

#Configure the hostname of the switch.

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 **System Manage** -> **Time Manage**, the **Time Setting** page appears.

Time Setting

System Time: 2000-12-06 01:48:35

Select Time-Zone	(GMT)Greenwich Mean Time,Dublin,London,Lisbon
<input checked="" type="radio"/> Set Time Manually	
Set Time	2020 Year 12 Month 06 Day 01 Hour 48 Minute(s) 35 Second
<input type="radio"/> Network Time Synchronization	
SNTP Server One	
SNTP Server Two	
SNTP Server Three	

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.

Chapter 4 Configuration of the Physical Interface



Figure 1: Physical port configuration list

4.1 Configuring Port Description

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

Port	Port Description
G0/1	

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 **Physical port config -> Port attribute Config** in the navigation bar, the **Port Attribute Configuration** page appears, as shown in figure 3.

Port	Status	Speed	Duplex	Flow Control	Medium
G0/1	Up	Auto	Auto	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:

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	(1-15625)	Disable	64kbps	(1-15625)

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. The receiving and sending rates can be configured either by percentage or by specific units of the switch.

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.

Mirror Port		G0/1	
Filters		Port Type: All	Slot Num: All Name(s): <input type="text"/> Help
Mirrored Port		Mirror Mode	
<input type="checkbox"/> G0/1		RX	
<input checked="" type="checkbox"/> G0/2		TX	

Figure 5 Port mirror configuration

Click the dropdown list on the right side of "Mirror Port" and select a port to be the destination port of mirror.

Click a checkbox and select a source port of mirror, that is, a mirrored port.

RX The received packets will be mirrored to the destination port.

TX The transmitted packets will be mirrored to a destination port.

RX & TX The received and transmitted packets will be mirrored simultaneously.

4.5 Loopback Detection

If you click **Physical port Config -> Port loopback detection** in the navigation bar, the **Setting the port loopback detection** page appears, as shown in figure 4-6.

Port	Status	Keepalive Period
G0/1	Enable <input type="button" value="v"/>	3333 (0-32767)Seconds

Figure 6: Port loopback detection

You can set the loopback detection cycle on the **Loopback Detection** page.

4.6 Port security

4.6.1 IP Binding Configuration

If you click **Physical port Config -> Port Security -> IP bind** in the navigation bar, the **Configure the IP-Binding Info** page appears, as shown in figure 4-7.

Interface Name	Detail
G0/1	Detail

Figure 7 IP binding configuration

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

	Serial number	Address	Operate
<input type="checkbox"/>	1	192.168.0.2	Edit
<input type="checkbox"/>	2	192.168.0.3	Edit

Figure 8 Setting the binding of the source IP address

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 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 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 <input type="button" value="v"/>

Figure 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 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 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 <input type="button" value="v"/>	<input type="text" value="1"/> (1-4095)

Figure 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

Port	Status	Threshold
F0/1	Disable	(1-1638) 64Kbps

Figure 15 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

Port	Status	Threshold
F0/1	Disable	(1-1638) 64Kbps

Figure 16 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

Port	Status	Threshold
F0/1	Disable	(1-1638) 64Kbps

Figure 17 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.

4.8 Port Protect Group Configuration

Click "Port Config" -> "Port Protect Group Config" in the navigation bar, and enter the configuration page of Port Protect Group List and Port Protect Group Interface Config.

4.8.1 Port Protect Group List

Click "Port Config" -> "Port Protect Group Config" -> "Port Protect Group List" in the navigation bar, and enter the configuration page of "Port Protect Group List".

Port Protect Group List	
<input type="button" value="New"/>	
No.1 Page/Total 1 Page First Prev Next Last Go No. <input type="text"/> Page Search: <input type="text"/> Current 1 Item/Total 1 Item	
<input type="checkbox"/>	Port Protect Group 1
<input type="checkbox"/> Select All/Select None <input type="button" value="Delete"/>	
Help	
#Port Protect Group 0 is Default Port Protect Group, and it can not be deleted.	

Click “New” to create a new port protect group, as shown in the above figure.

Tick one port protect group and delete it. The port protect group is 0 by default, which cannot be deleted.

4.8.2 Port Protect Group Interface Configuration

Click "Port Config" -> “Port Protect Group Config” -> “Port Protect Group Interface Config” in the navigation bar, and enter the configuration page of “Port Protect Group Interface Config”.

Port	Port Protect Group
g0/1	<input type="text"/>

The port protect group must be a created group. If one port has configured the default protect group, other ports can only be configured with the default protect group.

4.9 POE Management

4.9.1 POE Global Configuration

Click “physical port configuration” and “POE management” in turn to enter POE global configuration page.

Power Management Mode	Auto	
Low Disable Threshold	18000	(100-30000) mw
Low No Connect Threshold	18000	(100-30000) mw
Duration of POE LED	30	(1-300) s
POE MIB Notification Function	Start	
Threshold of Available Power	100	(1-100)
Power Counter	0	(0-100) s
POE Chip Automatic Protection	Start	
Power Supply Standard	Max Power Supply	

Apply **Reset**

Help

#Low Disable Threshold means that the lower priority port will be disabled when consumed power

#Low No Connect Threshold means that the lower priority port will not be connected when consumed power

On this page, POE can be configured as power management mode, low disable threshold, and enable/ disable POE MIB notification function and other global POE properties.

4.9.2 POE Global Real-time Information

Click “physical port configuration”, “POE management” and “POE global real-time information” in turn on the navigation bar to enter POE global real-time information page.

POE Global Realtime Info

POE Chip	PD69000
POE Port Number	8
PSE Total Power	300000
PSE Usage Threshold	100%
PSE Alarm Power	100
PSE Consumed Power	0
PSE Temperature	0

Check POE port quantity, POE power, POE temperature and other information as above on this page.

4.9.3 POE Port List

Click “physical port configuration”, “POE management” and “POE port list” on navigation bar in turn to enter POE port list page.

POE Interface List

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

Port	Port Max Power	Port Priority	Force Connection	POE Interface Description
g0/1	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>
g0/2	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>
g0/3	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>
g0/4	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>
g0/5	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>
g0/6	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>
g0/7	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>
g0/8	<input type="text" value="30000"/> mw	<input type="button" value="Low Priority"/>	<input type="button" value="Disable"/>	<input type="text"/>

Help

#The port that cannot be configured with POE will not be displayed

#When the Power Management Mode is auto, both the Port Max Power and the Port Priority cannot be configured. If it need to be configured, you can switch to the POE Mgr and change the Power Management Mode to Preemptive

Each of POE port's maximum power, priority and mandatory power-up could be configured at this page; illustrative information could also be added on the port at this page.

4.9.4 POE Ports' Policy Power-up

Click “physical port configuration”, “POE management” and “POE ports' policy power-up” in turn on navigation bar to enter POE ports' policy power-up management page.

POE Port Policy Power

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

Port	POE Function	Time Range
g0/1	Enable	<input type="text"/>
g0/2	Enable	<input type="text"/>
g0/3	Enable	<input type="text"/>
g0/4	Enable	<input type="text"/>
g0/5	Enable	<input type="text"/>
g0/6	Enable	<input type="text"/>
g0/7	Enable	<input type="text"/>
g0/8	Enable	<input type="text"/>

Help

#The port that cannot be configured with POE will not be displayed

#Time Range can be configured by Advanced Config->Time Range Config

Two controlling methods of ports' power-up can be configured at this page. One is to open and shut down POE function directly; the other is configure Time Range to set the POE operating time of the port.

4.9.5 POE Ports' Power Real-time Information

Click "physical port configuration", "POE management" and "POE ports power real-time information" in turn on navigation bar to enter POE ports' power real-time information.

POE Interface Power List

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

Port	Current Power	Setting Max Power	Average Power	Peak Power	Bottom Power
g0/1	0mw	0mw	-	-	-
g0/2	0mw	0mw	-	-	-
g0/3	0mw	0mw	-	-	-
g0/4	0mw	0mw	-	-	-
g0/5	0mw	0mw	-	-	-
g0/6	0mw	0mw	-	-	-
g0/7	0mw	0mw	-	-	-
g0/8	0mw	0mw	-	-	-

PSE Total Power 0

Help

#The port that cannot be configured with POE will not be displayed

#When the Power Counter is 0, the Average Power, the Peak Power and the Bottom Power will not be shown

At this page, you could check POE ports' current power, set real time information like the maximum power, average power, peak power, valley power and etc.

4.9.6 POE Ports' Other Real-time Information

Click "physical port configuration", "POE management" and "POE port other real-time information" in turn on navigation bar to enter POE ports' other real-time information page.

POE Port Other Info

Filters Port Type: Slot Num: Name(s): [Help](#)

Port	POE Port Detection Status	POE Port Power Supply	POE IEEE Class	POE Port Current
g0/1	Fault	Signal	0	0mA
g0/2	Fault	Signal	0	0mA
g0/3	Fault	Signal	0	0mA
g0/4	Fault	Signal	0	0mA
g0/5	Fault	Signal	0	0mA
g0/6	Fault	Signal	0	0mA
g0/7	Fault	Signal	0	0mA
g0/8	Fault	Signal	0	0mA

Help
=The port that cannot be configured with POE will not be displayed

POE port detection status, POE port power-up status could be checked at this page.

Chapter 5 Layer-2 Configuration

Device Status
Basic Config
Port Config
L2 Config
VLAN Config
GVRP Config
STP Config
IGMP Snooping
Static ARP Config
Static MAC Config
LLD Config
DDM Config
Port Aggregation
Ring protection
Multiple Ring protection
Backup Link Config
MTU Config
PDP Config
L3 Config
Advanced Config
Network Config
Diagnostic Tool
System Mgr.

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.

	VLAN ID	VLAN Name	Operate
<input type="checkbox"/>	1	Default	Edit

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.

Revising VLAN Config

	VLAN ID	<input type="text" value="2"/>
	VLAN Name	<input type="text" value="VLAN0002"/>

Port	Default VLAN	Mode	Untag or not	Allow or not
G0/1	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/2	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/3	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/4	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/5	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/6	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/7	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/8	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/9	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/10	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/11	<input type="text" value="1"/> <1-4094>	Access	No	Yes
G0/12	<input type="text" value="1"/> <1-4094>	Access	No	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 GVRP Configuration

5.2.1 GVRP Global Attribute Configuration

If you click **Layer-2 Config -> GVRP Config -> GVRP Global Config** in the navigation bar, the **GVRP Global Config** page appears, as shown the following Figure.

GVRP Global Config	
GVRP Global Config	Disable ▾
Set Dynamic Vlan to Take Effect Only On Registration Ports	Disable ▾
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 4 GVRP Global Configuration

You can enable or disable the global GVRP protocol and sets whether the dynamic vlan is only effective on the registration interface.

5.2.2 Global Interface Attribute Configuration

If you click **Layer-2 Config -> GVRP Config -> GVRP Interface Config** in the navigation bar, the **GVRP Interface Config** page appears, as shown the following Figure.

Port	GVRP Status
G0/1	Enable ▾

Figure 5 Global Interface Attribute Configuration

To enable or disable GVRP protocol on the GVRP interface configuration.

5.3 STP Configuration

5.3.1 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.

Root STP Config	
Spanning Tree Priority	4096
MAC Address	00E0.0F8E.7025
Hello Time	2
Max Age	20
Forward Delay	15

Local STP Config	
Protocol Type	RSTP
Spanning Tree Priority	32768
MAC Address	FCFA.F72E.09A1
Hello Time	2 (1-10)s
Max Age	20 (6-40)s
Forward Delay	15 (4-30)s
BPDU Terminal	Disable

STP Port's State						
No.1 Page/Total 1 Page	First	Prev	Next	Last	Go No. <input type="text"/>	Page Search: <input type="text"/>
						Current 1 Item/Total 1 Item
Interface	Role	State	Cost	Priority	Port ID	Type
G0/1	Root	FWD	20000		128.1	P2p

Figure 6 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.

5.3.2 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 Property
G0/1	Enable	128	0	Auto
G0/2	Enable	128	0	Auto
G0/3	Enable	128	0	Auto
G0/4	Enable	128	0	Auto
G0/5	Enable	128	0	Auto
G0/6	Enable	128	0	Auto
G0/7	Enable	128	0	Auto
G0/8	Enable	128	0	Auto

Figure 7 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.

5.4 IGMP-Snooping Configuration

5.4.1 IGMP-Snooping Configuration

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

IGMP Snooping Config	
Multicast Filtration Mode	Transfer Unknown
IGMP Snooping	Enable
Enable Auto Query	Enable

[Apply](#)

Figure 8 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.

5.4.2 IGMP-Snooping VLAN List

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

	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router's Port	Operate
<input type="checkbox"/>	1	Running	Disable	SWITCH(querier);	Edit

Figure 9: 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.

VLAN ID		<input type="text" value="2"/>
Status of the IGMP Snooping Vlan		Enable ▾
Immediate-leave		Disable ▾
Configured Mrouter Port List		Available Port List
G0/1 G0/12	>> <<	G0/10 ▲ G0/11 G0/13 G0/14 G0/15 G0/16 ▤ G0/17 G0/18 G0/19 G0/20 ▼
<input type="button" value="Apply"/>		<input type="button" value="Reset"/>
		<input type="button" value="Go Back"/>

Figure 10: 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.

5.4.3 Static Multicast Address

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

Static Multicast Address Config			
VLAN ID	<input type="text"/>		
Multicast IP Address	<input type="text"/>		
Assignment Port	<input type="text"/>		
<input type="button" value="Apply"/>			
Static Multicast List Info			
No.0 Page/Total 0 Page	First Prev Next Last	Go No. <input type="text"/> Page	Search: <input type="text"/>
		Current 0 Item/Total 0 Item	
	VLAN ID	Group	Port
<input type="checkbox"/> Select All/Select None			
		<input type="button" value="Delete"/>	<input type="button" value="Refresh"/>
Help			

Figure 11 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.

5.4.4 Multicast List

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

Figure 12 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.

5.5 Setting Static ARP

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

◆MAC: The mac address only supports the unicast address and the following formats:XXXXXXXXXXXX,XXXX.XXXX.XXXX,XX:XX:XX:XX:XX:XX,XX-XX-XX-XX-XX-XX, and X is Hex number

Figure 13 Displaying static ARP

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.

ARP Config

Configure the corresponding MAC address of an IP address

IP Address*	<input type="text"/>
MAC Address*	<input type="text"/>
Interface VLAN*	<input type="text"/>

Help

◆MAC: The mac address only supports the unicast address and has the following formats:XXXXXXXXXXXX,XXXX.XXXX.XXXX,XX:XX:XX:XX:XX:XX,XX-XX-XX-XX-XX-XX, and X is Hex number

Figure 14 Setting static ARP

5.6 Static MAC Address Configuration

If you click **Layer-2 Config -> Static MAC Config -> Static MAC List**, the **Static MAC Address List Info** page appears.

Static MAC Address List Info

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

	Index	Static MAC Address	VLAN ID	Port	Operate
<input type="checkbox"/>	1	1022.3344.5566	1	G0/8	Edit

Select All/Select None

Figure 15 Setting Static MAC Address List Info

Click **New** to designate static MAC address and VLAN. The unicast MAC address can only configure one interface. Multiple MAC addresses can configure multiple interfaces.

Click **Edit** to modify the static MAC address.

Click **Delete** to delete the selected MAC address table.

Static MAC Address Config

Static MAC Address	<input type="text"/>
VLAN ID	<input type="text"/>

Configured Port List	<input type="button" value=" >> "/> & <input type="button" value=" << "/> &	Available Port List
<input type="text"/>		G0/1 G0/2 G0/3 G0/4 G0/5 G0/6 G0/7 G0/8 G0/9 G0/10

Help

◆Only one port can be configured for a unicast MAC address, while multiple MAC addresses can be configured for a multicast MAC address

◆MAC format: XXXX.XXXX.XXXX

Figure 16 Static MAC Address Config

5.7 LLDP Configuration

5.7.1 Configuring the Global Attributes of LLDP

If you click **Layer-2 Config -> LLDP Config -> LLDP Global Config** in the navigation bar, the **Basic Config of LLDP Protocol** page appears, as shown in the following Figure.

Basic Config of LLDP Protocol		
Protocol State	<input type="text" value="Open the LLDP protocol"/>	▼
HoldTime Settings	<input type="text" value="120"/>	(0-65535)s
Reinit Settings	<input type="text" value="2"/>	(2-5)s
Setting the packet transmission cycle	<input type="text" value="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.

Figure17 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. Its default value is 120s.

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

5.7.2 LLDP Port Attribute Configuration

If you click **Layer-2 Config -> LLDP Config -> LLDP Interface Config** in the navigation bar, the **LLDP Port Config** page appears.

Port	Receive LLDP Packet	Send LLDP Packet
G0/1	<input type="text" value="Enable"/>	<input type="text" value="Enable"/>

Figure 18 Configuring the LLDP port

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

5.8 DDM Configuration

If you click **L2 Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 19.

DDM Config

DDM Enable ▼

Apply
Reset

Help

Figure 19: DDM configuration

5.9 Port Aggregation Configuration

5.9.1 Port Aggregation Configuration

If you click **Layer-2 Config -> Port Channel-> Port Channel**, the **Port Aggregation Config** page appears.

Port Aggregation Config

New

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

	Aggregation Group	Mode	Configure port members	Valid port members	Speed	State	Operate
<input type="checkbox"/>	P1	Static	G0/6,G0/9			down	Edit

Select All/Select None
 Delete

Help

◆Note: The physical attributes of all the aggregated ports shall be the same, including Speed, Duplex mode and Vlan

Figure 20 Port Aggregation Information

Click **New** to create an aggregation group. It can configure 32 aggregation groups in maximum and each group is with 8 physical ports into aggregation. Click **Delete** to delete the selected aggregation group. Click **Reset** to modify the setting.

Port Aggregation Config

New

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

Aggregation Group

P1 ▼

Mode

Static ▼

Configured port List

GigaEthernet0/6
GigaEthernet0/9

Available Port List

GigaEthernet0/2
GigaEthernet0/3
GigaEthernet0/5
GigaEthernet0/7
GigaEthernet0/8
GigaEthernet0/10
GigaEthernet0/11
GigaEthernet0/12
GigaEthernet0/13
GigaEthernet0/14

>>
<<

Apply
Reset
Go Back

Help

◆Note: Each aggregation port can be configured to have at most 8 physical port.

Figure 21 Port Aggregation Configuration

If you create an aggregation group, it is optional; if you modify the aggregation group, it is not optional.

When the aggregation port has a member port, the user can select the aggregation mode: static, LACP Active and LACP Passive.

You can click “>>” and “<<” to delete and add an aggregation member port.

5.9.2 Port Channel Group Loading Balance Configuration

Some models support link aggregation load balancing configuration and others not, but they can be configured in the global configuration mode.

3928 supports the aggregation group based load balancing configuration:

Port Channel	Loading Balance Mode
p1	DST MAC

The Aggregation Group Based Load Balancing Configuration

You can use different aggregation groups to set different aggregation modes.

5.10 Ring Protection Configuration

5.10.1 EAPS Ring List

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

Ring ID	Node Type	Ring Description	Control VLAN	Status	Hello	Fail	Preforward	Primary Port/Forwarding/Link Status	Secondary Port/Forwarding/Link Status	
<input type="checkbox"/> Select All/Select None <input type="button" value="Delete"/> <input type="button" value="Refresh"/>										

Figure 22 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.

5.10.2 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.

ether-ring	
Ring ID	0
Node Type	Master Node
Ring Description	
Control VLAN	
Hello Time	1 (1-10)s
Fail Time	3 (3-30)s
Preforward Time	3 (3-30)s
Primary Port	None
Secondary Port	None

Figure 23 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.

5.11 MEAPS Configuration

5.11.1 MEAPS Ring Network List

Click “L2 Config” -> “Multiple Ring Protection” in the navigation bar, and enter the multiple ring protection configuration page.

Multiple Ring Protection Configuration													
<input type="button" value="New"/>													
No.1 Page/Total 1 Page First Prev Next Last Go No. <input type="text"/> Page Search: <input type="text"/>											Current 1 Item/Total 1 Item		
Domain ID	Ring ID	Ring Type	Node Type	Control Vlan	Hello Time	Failed Time	Pre Forward Time	Port	Type	Port	Type	Operate	
<input type="checkbox"/>	3	3	Major Ring	Master Node	3	3	3	3	None	Primary-Port	None	Secondary-Port	Edit
<input type="checkbox"/> Select All/Select None												<input type="button" value="Delete"/>	

Figure 24 MEAPS Network List

The list displays the currently configured MEAPS ring, including the domain ID, the ring ID, the ring type, the node type, control VLAN, Hello Time, Fail Time, Pre Forward Time and the primary and secondary port on the ring.

Click “New” to create MEAPS ring network.

Click “Modify” right of the entry to configure the time parameter, and the primary and secondary port of the ring network.

Note that:

1. MEAPS domain numbers the system supported is 4 (0-3).
2. The ring numbers supported in the domain is 8 (0-7).
3. Once one MEAPS has configured, its ID, ring ID, ring type, node type and control Vlan cannot be configured. If these parameters need to be configured, please delete the net ring and re-create it.

5.11.2 EAPS Ring Network Configuration

Click “New” in the EAPS ring list or “Modify” right of the ring entry, and enter EAPS ring network configuration page.

NewMEAPS Global Config

Domain ID*	<input type="text" value="3"/>
Ring ID*	<input type="text" value="3"/>
Ring Type*	Major Ring ▾
Node Type*	Master Node ▾
Control Vlan*	<input type="text" value="3"/>
Hello Time	<input type="text" value="3"/>
Failed Time	<input type="text" value="3"/>
Pre-Forward Time	<input type="text" value="3"/> X
Primary-Port	None ▾
Secondary-Port	None ▾

Help
 #Your web management may be interrupted as the control VLAN is modified to be the vlan interface that the web browser connects
 #Only the master or transit node can be configured in the major ring
 #The master node, transit node, edge node or assistant node can be configured in the sub ring
 #The master or transit node can be configured in one ring, while the edge node or assistant edge node can be configured in several rings

Figure 25 MEAPS Configuration

Note that:

Once one MEAPS has configured, its ID, ring ID, ring type, node type and control Vlan cannot be configured.

The primary ring can only configure the master node and the transit node.

The secondary ring can configure the primary node, the transit node, the edge node

The primary node and the transit node can only exist in one ring, and the edge node and the assistant edge node can exist in many rings simultaneously.

In the text boxes of “Primary Port” and “Secondary Port”, select a port as the ring port respectively or select “None”.

5.12 Backup Link Protocol Configuration

5.12.1 Backup Link Protocol Global Configuration

If you click **Layer-2 Config ->Backup Link Config ->Backup Link Protocol Global Config** on the navigation bar, the **Backup Link Protocol Global Config** page appears.

BackupLink Protocol Global Config

[New](#)

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

	Group ID	Preemption Mode	Preemption Delay	Operate
<input type="checkbox"/>	2	No Preemption		Edit

Select All/Select None [Delete](#)

Figure 26 Backup Link Protocol Global Configuration

On the page, the current configured backup link groups are shown, including Preemption Mode and Preemption Delay.

Click **New** to create a new link backup group.

Click **Edit** on the right to configure Preemption Mode and Preemption Delay.

BackupLink Protocol Global Config

Group ID

Preemption Mode

Preemption Delay

[Apply](#) [Reset](#)

Figure 27 Backup Link Protocol Global Configuration

Note:

1. The system supports 8 link backup groups.
2. The Preemption mode determines the policy the primary port and the backup port forward packets.

5.12.2 Backup Link Protocol Interface Configuration

If you click **Layer-2 Config -> Backup Link Protocol Config -> Backup Link Protocol Interface Config** on the navigation bar, the **Backup Link Protocol Global Config** page appears.

BackupLink Protocol Interface Config

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 25 Item/Total 25 Item

Interface Name	Group ID	Interface Attribute	MMU Attribute	Shareload VLAN	Operate
G0/1	2	Active Port			Edit
G0/2					Edit
G0/3					Edit
G0/4					Edit

Figure 28 Backup Link Protocol Interface Configuration

This page shows the backup link group's member ports, Interface Attribute, MMU Attribute, Shareload Vlan, etc.

Click **Edit** on the right to configure the Backup Link Protocol.

BackupLink Protocol Interface Config	
Interface Name	G0/1
Group ID	<input type="text" value="2"/>
Interface Attribute	Active Port <input type="button" value="v"/>
MMU Attribute	<input type="button" value="v"/>
Shareload VLAN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Go Back"/>	

Help

◆Share Load VLAN can be Only Configured On The Backup Port

Figure 29 Backup Link Protocol Interface Configuration

The backup link group which has configured the primary port cannot take other ports as its primary port. Likewise, the backup link group which has configured the backup port cannot take other ports as its backup port.

5.13 MTU Configuration

If you click **Layer-2 Config -> MTU Config** on the navigation bar, the **MTU Config** page appears.

MTU Config	
MTU	<input type="text" value="1500"/> (1500-13312)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Help

◆Configure the size of the system mtu, whose default value is 1500

Figure 30 MTU Configuration

You can set the size of the maximum transmission unit (MTU).

5.14 PDP Configuration

5.14.1 Configuring the Global Attributes of PDP

If you click **Layer-2 Config -> PDP Config -> PDP Global Config** in the navigation bar, the **Basic Config of PDP Protocol** page appears.

Basic Config of PDP Protocol	
Protocol State	Open the PDP protocol <input type="button" value="v"/>
HoldTime Settings	<input type="text" value="180"/> (10-255)s
Setting the packet transmission cycle	<input type="text" value="60"/> (5-254)s
Protocol Version	Version2 <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

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 31 Basic Config of PDP Protocol

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

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

5.14.2 PDP Interface Attribute Configuration

If you click **Layer-2 Config -> PDP Config-> PDP Interface Config** in the navigation bar, the **Protocol Port Config** page appears.

Port	Status
G0/1	Enable PDP <input type="button" value="v"/>

Figure 32 PDP Interface Attribute Configuration

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

Chapter 6 Layer-3 Configuration



Figure 1: Layer-3 configuration list

6.1 Configuring the VLAN Interface

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

	Name of the VLAN Interface	IP Attribute	IP Address	
<input type="checkbox"/>	1	Manual Config	192.168.1.79/24;	<input type="checkbox"/>

Select All/Select None

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.

VLAN Interface Config

IP Attribute

VLAN Interface Name*

IP Attribute* Manual Config

Primary IP Address

IP Address*

MASK address*

Secondary IP Address 1

IP Address*

MASK address*

Secondary IP Address 2

IP Address*

MASK address*

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 Static Routing Configuration

If you click **Layer-3 Config -> Static Routing**, the **Configuring the static routing table** page appears.

Static Routing Config

Operate

No. 1 Page/Total 1 Page First Pre Next Last No. Page Search: Current 1 Term/Total 1 Term

	Default	Destination IP segment	Destination IP mask	Port type	VLAN Port	Gateway IP	Forwarding address	AD	Route tag	Global	Description	Operate
<input type="checkbox"/>	false	192.168.1.0	255.255.255.0	gateway		192.168.1.1				false		edit

Select All/ Selete None

Help

◆Global : The next address is in the global routing table

Figure 4: configure Static Routing

Click **New** to add a new static routing table.

Click **Modify** to modify the settings of a corresponding static routing table.

Click **Cancel** to delete a static routing table.

Static Routing Config

Static Routing Protocol

Default	<input type="checkbox"/>
Destination IP segment	<input type="text"/>
Destination IP mask	<input type="text"/>
Port type	Null0 Port ▾
VLAN Port	<input type="text"/>
Gateway IP	<input type="text"/>
Forwarding address	<input type="text"/>
AD	<input type="text"/>
Route tag	<input type="text"/>
Global	<input type="checkbox"/>
Description	<input type="text"/>

Help

- ◆ Global: The next address is in the global routing table

Figure 5: Static Routing configuration

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	0
G0/8	1
G0/9	2
G0/10	3
G0/11	4

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.

The screenshot shows the 'QoS Config' page. At the top, there is a 'Schedule Policy' dropdown menu set to 'sp'. Below this, there are eight queues arranged in a 2x4 grid. Each queue has a 'Queue ID' field (all set to 1) and a 'Bandwidth' field (all set to 0-15). Below the queues is a 'COS-to-queue map' table with 'COS value' on the left (0-7) and 'Queue' on the right (Queue 1-8). Each row in the map has a dropdown menu. At the bottom of the configuration area are 'Apply' and 'Reset' buttons. Below the configuration area is a 'Help' section with two bullet points: 'If you want to configure the cos value of the interface, please goto QoS Interface Configuration.' and 'if the bandwidth of queue has been set to 0, the queue after this also must be set to 0'.

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 IP Access Control List

7.2.1 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.

The screenshot shows the 'IP ACL Config' page. At the top left is a 'New' button. Below it is a navigation bar with 'No.1 Page/Total 1 Page', 'First Prev Next Last', 'Go No. [] Page', and 'Search: []'. On the right, it says 'Current 2 Item/Total 2 Item'. The main area is a table with three columns: 'Name of the IP ACL', 'Attribute of the IP ACL', and 'Operate'. There are two rows: one for 'acla' with attribute 'extended' and one for 'myacl' with attribute 'standard'. Each row has an 'Edit' link. At the bottom left is a 'Select All/Select None' checkbox, and at the bottom right is a 'Delete' button.

Figure 4: 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 5: 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.

7.2.2 Setting the Rules of the IP Access Control List

➤ Standard IP access control list

No.	Authority	Src IP	Src IP Mask	Record the log	Operate
1	permit	1.1.1.1	255.255.255.0	log	Edit

Figure 6: 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 7: Setting the Rules of the standard IP access control list

➤ Extended IP access control list

Extended IP ACLacla																
New																
No.1 Page/Total 1 Page First Prev Next Last Go No. <input type="text"/> Page Search: <input type="text"/>															Current 1 Item/Total 1 Item	
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
<input type="checkbox"/>	permit	Mask	0	1.1.1.1/255.255.255.0		any	10								log	Edit
<input type="checkbox"/> Select All/Select None											Go Back		Delete			

Figure 8: 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*	<input type="text"/> - <input type="text"/>
Src Port	<input type="text"/>
Src Port Range	<input type="text"/> - <input type="text"/>
Dst IP Type	any
Dst IP*	
Dst IP Mask*	
Dst Interface Vlan*	
Dst IP Range*	<input type="text"/> - <input type="text"/>
Dst Port	<input type="text"/>
Dst Port Range	<input type="text"/> - <input type="text"/>
Time-Range	10
Tos	
Precedence	
Do not fragment	<input type="checkbox"/>
Fragmented Packet	<input type="checkbox"/>
Offset	<input type="text"/>
Length of the IP Packet	<input type="text"/>
Time-to-live Value	<input type="text"/>
Log	<input checked="" type="checkbox"/>
Location	1

Figure 9: Setting the Rules of the extended IP access control list

7.2.3 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 10: Applying the IP access control list

7.3 MAC Access Control List

7.3.1 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 11: 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 12: Setting the name of MAC access control list

7.3.2 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 13: 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 ACLmyadItem

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 14: Setting the Rules of the MAC Access Control List

7.3.3 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 style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
G0/2	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
G0/3	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
G0/4	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
G0/5	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
G0/6	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
G0/7	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>

Figure 15: Applying the MAC 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

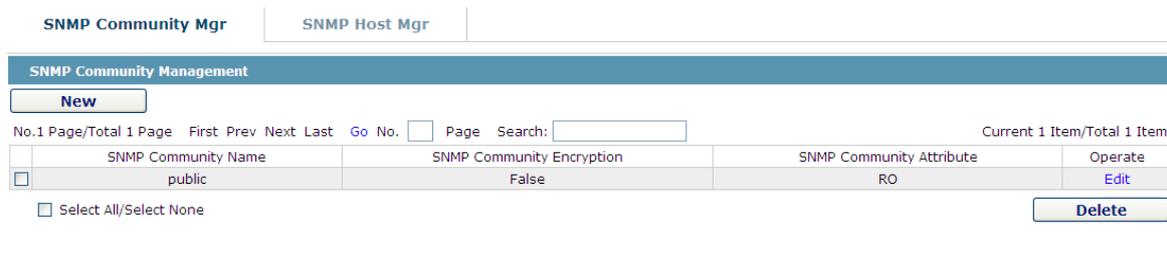
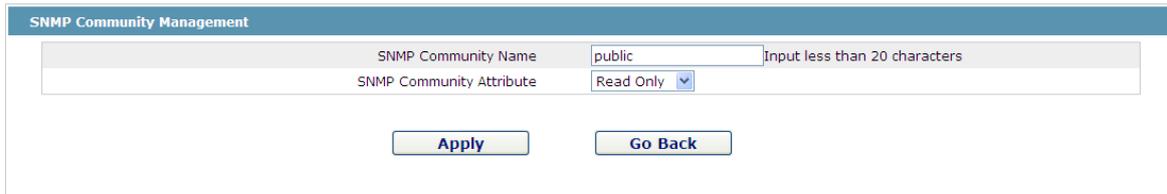


Figure 2 SNMP community management

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.

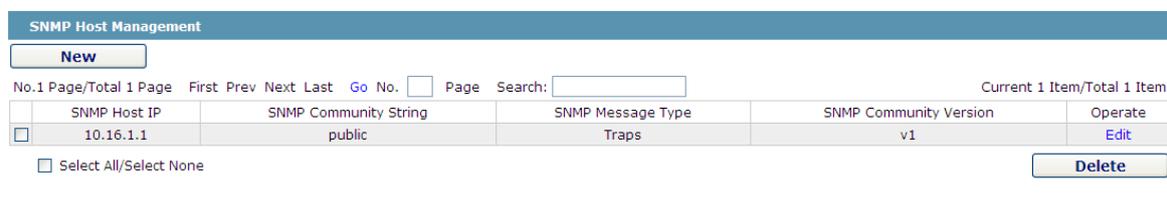


The screenshot shows the 'SNMP Community Management' configuration page. It features a header bar with the title. Below it, there are two input fields: 'SNMP Community Name' with the value 'public' and a note 'Input less than 20 characters', and 'SNMP Community Attribute' with a dropdown menu set to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

Figure 3 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

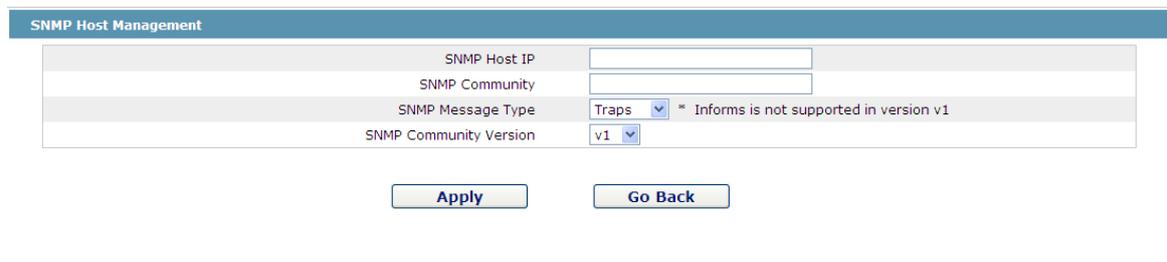


The screenshot shows the 'SNMP Host Management' page. It has a 'New' button at the top left. Below it, there is a table with the following columns: 'SNMP Host IP', 'SNMP Community String', 'SNMP Message Type', 'SNMP Community Version', and 'Operate'. The table contains one row with the following data: '10.16.1.1', 'public', 'Traps', 'v1', and 'Edit'. There are also navigation controls like 'No. 1 Page/Total 1 Page', 'First', 'Prev', 'Next', 'Last', 'Go No.', 'Page', 'Search:', and 'Current 1 Item/Total 1 Item'. At the bottom left, there is a checkbox for 'Select All/Select None' and a 'Delete' button at the bottom right.

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 header bar with the title. Below it, there are four input fields: 'SNMP Host IP', 'SNMP Community', 'SNMP Message Type' with a dropdown menu set to 'Traps' and a note '* Informs is not supported in version v1', and 'SNMP Community Version' with a dropdown menu set to 'v1'. At the bottom, there 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.

Interface Statistics Config		
Interface	G0/1	
Index	1	(1-65535)
Owner	demon	
<input type="button" value="Apply"/> <input type="button" value="Go Back"/>		
Help		
◆ It must be configured in interface mode, which is used to enable the interface statistics		
*◆ The string you totally entered is less than or equal to 255 characters		

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.

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*
<input type="button" value="Apply"/> <input type="button" value="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 Alarm config		
Index	1	(1-65535)
MIB Node	IfinOctets	
OID	1.3.6.1.2.1.2.2.1.10	
Interface	G0/1	
Alarm type	absolute	
Sampling Interval	5	(1-2147483647)
Rising Threshold	5	(-2147483648 - 2147483647)
Rising Event Index	2	(1-65535)
Falling Threshold	6	(-2147483648 - 2147483647)
Falling Event Index	3	(1-65535)
Owner	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 Event Config	
Index	<input type="text"/> (1-65535)
Owner	<input type="text"/>
Description	<input type="text"/>
Enable log	<input type="checkbox"/>
Enable trap	<input type="checkbox"/>
Community	<input type="text"/>

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

9.1.1 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



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.

User Management

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

	User name	User permission	Pass-Group	Authen-Group	Author-Group	User Status	Operate
<input type="checkbox"/>	admin	System administrator				Normal	Edit

Select All/Select None

Help

- ◆Note: When only one Admin user exists, You cannot delete the current administrator user. Otherwise, you cannot log on to the switch and configure it.
- ◆Users can be divided into the Admin user and the limited user according to the permission. The Admin user can use all functions of the switch, including browsing, configuring and remote login, while the limited user only has the permission to browse the switch's running state through the WEB page.
- ◆Click the 'New' button to create a new user.

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.

The screenshot shows a web form titled 'User Management' with a sub-header 'User Management'. The form contains the following fields: 'User name', 'Password', 'Confirming password', 'Pass-Group', 'Authen-Group', and 'Author-Group'. Each field has a corresponding text input box. Below the form are three buttons: 'Apply', 'Reset', and '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. \ “ & # and characters other than spaces.

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.

10.1.3 User Group Management

If you click **New** on the **User Mgr.** page, the **User Group Management** page appears.

The screenshot shows a web page titled 'User Group Mgr.'. At the top left is a 'New' button. Below it is a table with the following structure:

Serial Number	Group Name	Pass-Group Rule	Authen-Group Rule	Author-Group Rule	Operate	Detail
1	group				Edit	Detail

Below the table is a checkbox labeled 'Select All/Select None' and a 'Delete' button.

Figure 4 User group list

Click **New** to create a new user group.

Click **Delete** to delete the user group.

User Group Config

User Group Name*	<input type="text"/>
Pass-Group Name	<input type="text"/>
Authen-Group Name	<input type="text"/>
Author-Group Name	<input type="text"/>

Help

- ◆The user group mustn't exist.
- ◆Rule must exist.

Figure 5 User group configuration

The User Group Name must be different with the existing group names. The user group cannot be created until the Pass-Group name, Authen-Group Name and Author-Group Name are specified. Configuring the Pass-Group name, Authen-Group Name and Author-Group Name in another 3 pages.

10.1.4 Password Group Management

Click **Pass-Group Mgr.** and the **Pass-Group Mgr.** page appears.

Pass-Group Mgr.

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

Serial Number	Pass-Group Name	Same as the username	Min Length	Validity	Number	Lower-letter	Upper-letter	Special-character	Operate
<input type="checkbox"/>	1	password1	Can be same		Must	Must	Must	Must	Edit

Select All/Select None

Figure 6 Password Group Management

Click **New** to create a new password rule.

Click **Delete** to delete the password rule.

Pass-Group Config

Pass-Group Name*	<input type="text"/>
Same as Username	Can <input type="button" value="v"/>
Contain Number	Must <input type="button" value="v"/>
Contain Lower-letter	Must <input type="button" value="v"/>
Contain Upper-letter	Must <input type="button" value="v"/>
Contain Special-character	Must <input type="button" value="v"/>
Min Length	<input type="text"/> (1-127)
Validity	0 <input type="text"/> d 0 <input type="text"/> h 0 <input type="text"/> m 0 <input type="text"/> s

In the Pass-Group Configuration, the password can be set whether to be same as Username, Contain Number, Contain Lower-letter, Contain Upper-letter, Contain Special-character, Min Length and validity.

The rule can be applied to the user management. The password is valid only when it conforms to the rule.

10.1.5 Authentication Group Configuration

Click **Authen-Group Mgr.** on the navigation bar, and **Authen-Group Mgr.** appears.



Figure 7 Pass Group Configuration

Click **New** to create a new authorization rule.

Click **Delete** to delete the authorization rule.



Help

- ◆ Configure the Authen-Group
- ◆ 'Max Try Times' and 'Duration for all tries' must be entered at the same time

The **Max try times** and **Duration of all tries** can be configured or not. But they must be adjusted simultaneously.

10.1.6 Authorization Group Management

If you click **Author-Group Mgr.** and the **Author-Group Mgr.** page appears.

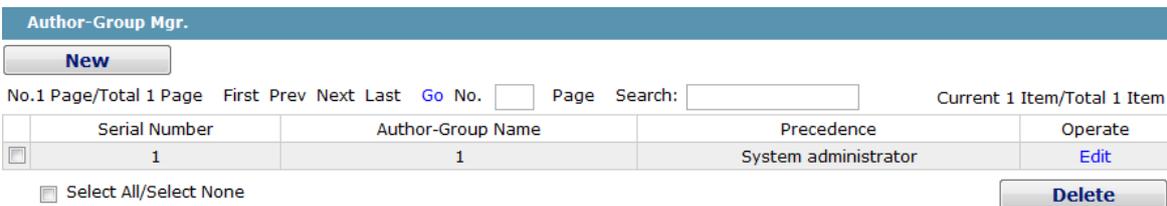


Figure 8 Author Group Management

Click **New** to create a new authorization rule.

Click **Delete** to delete the new authorization rule.

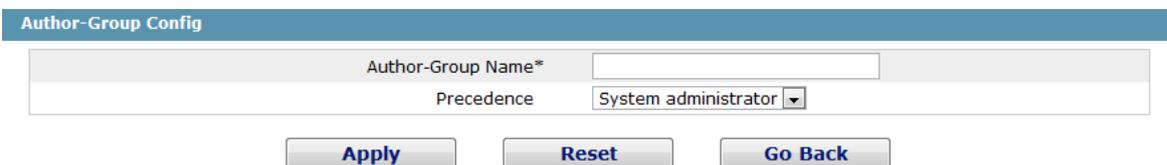


Figure 9 Author Group Configuration

The authorization rule determines the user's access: Administrator or Limited user. The **Administrator** has full access to the configuration and the **Limited user** only has access to check the configuration.

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	192.168.1.77
Level of system logs	(7-debugging)
Enable the log buffer	<input type="checkbox"/>
Size of the log buffer	4096 (Bytes)
Level of cache logs	(7-debugging)
<input type="button" value="Apply"/>	

Figure 10 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

Export the current startup-config

Figure 11 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

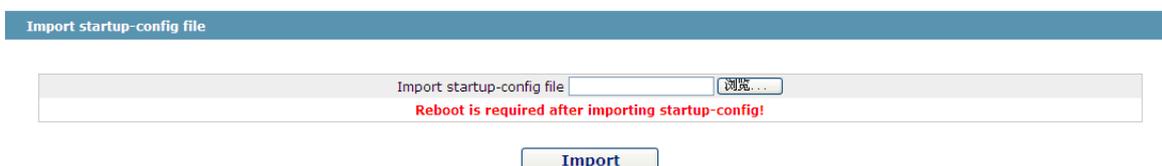


Figure 12 Importing the configuration files

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 13 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.

Note:

The default name of IOS document is “Switch.bin”. It is suggested to modify it as a name which is detectable and searchable when its backup is created.

10.4.2 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 14 Upgrading the IOS software

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

If IOS needs to 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 Rebooting the Device

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

Figure 15 Rebooting the device

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