

---

## Web Configuration

# Table of Contents

Chapter 1 Configuration Preparation .....	4
1.1 Accessing the Switch Through HTTP .....	4
1.1.1 Upgrading to the Web-Supported Version .....	4
1.1.2 Initially Accessing the Switch .....	5
1.2 Introduction of Web Interface .....	5
1.2.1 Top Control Bar .....	6
1.2.2 Navigation Bar .....	7
1.2.3 Configuration Area .....	8
1.2.4 Bottom Control Bar .....	8
1.2.5 Configuration Area .....	8
Chapter 2 Basic Configuration .....	10
2.1 Hostname Configuration .....	10
2.2 Time Management .....	11
Chapter 3 Configuration of the Physical Interface .....	12
3.1 Configuring Port Description .....	12
3.2 Configuring the Attributes of the Port .....	13
3.3 Rate control .....	13
3.4 Port mirroring .....	13
3.5 Loopback Detection .....	14
3.6 Port security .....	14
3.6.1 IP Binding Configuration .....	14
3.6.2 MAC Binding Configuration .....	15
3.6.3 Setting the Static MAC Filtration Mode .....	15
3.6.4 Static MAC Filtration Entries .....	15
3.6.5 Setting the Dynamic MAC Filtration Mode .....	16
3.7 Storm control .....	16
3.7.1 Broadcast Storm Control .....	16
3.7.2 Multicast Storm Control .....	17
3.7.3 Unknown Unicast Storm Control .....	18
Chapter 4 Layer-2 Configuration .....	19
4.1 VLAN Settings .....	19
4.1.1 VLAN List .....	19
4.1.2 VLAN Settings .....	20
4.2 GVRP Configuration .....	21
4.2.1 GVRP Config .....	21
4.2.2 GVRP Interface configuration .....	21
4.3 LLDP Configuration .....	21
4.3.1 Configuring the Global Attributes of LLDP .....	21
4.3.2 Configuring the Attributes of the LLDP Port .....	22
4.4 STP Configuration .....	22
4.4.1 STP Status Information .....	22
4.4.2 Configuring the Attributes of the STP Port .....	23

4.5 IGMP-Snooping Configuration .....	23
4.5.1 IGMP-Snooping Configuration .....	23
4.5.2 IGMP-Snooping VLAN List .....	24
4.5.3 Static Multicast Address .....	24
4.5.4 Multicast List .....	25
4.6 Setting Static ARP .....	25
4.7 Setting Static MAC .....	26
4.8 DDM Configuration .....	27
4.9 Link Aggregation Configuration .....	27
4.10 Ring Protection Configuration .....	28
4.10.1 EAPS Ring List .....	28
4.10.2 EAPS Ring Configuration .....	29
4.10.3 Configuration instance .....	30
4.11 Multiple Ring Protection .....	31
4.11.1 MEAPS Ring List .....	31
4.11.2 MEAPS Ring Configuration .....	31
4.11.3 Configuration instance .....	32
4.12 Backuplink Configuration .....	35
4.12.1 Backuplink protocol global configuration .....	35
4.12.2 Backuplink Protocol Interface Configuration .....	35
4.13 DHCP Snooping Configuration .....	36
4.13.1 DHCP Snooping configuration .....	36
4.13.2 DHCP Snooping VLAN Configuration .....	37
4.13.3 DHCP Snooping Interface Configuration .....	38
4.13.4 DHCP Snooping Binding List Manual Configuration .....	38
4.14 MTU Configuration .....	39
4.15 PDP Configuration .....	39
4.15.1 Configuring the Global Attributes of PDP .....	39
4.15.2 Configuring the Attributes of the PDP Port .....	40
4.16 POE Management .....	40
4.16.1 POE Global Configuration .....	40
4.16.2 POE Global Realtime Info .....	41
4.16.3 POE Interface List .....	41
4.16.4 POE Port Policy Power .....	42
4.16.5 POE Interface Power List .....	42
4.16.6 POE Port Other Info .....	42
Chapter 5 Layer-3 Configuration .....	44
5.1 Configuring the VLAN Interface .....	44
5.2 Setting the Static Route .....	45
5.3 OSPF Route Configuration .....	46
5.3.1 OSPF Process .....	46
5.3.2 OSPF Route Entries .....	47
5.4 IGMP Agent .....	47
5.4.1 Enabling the IGMP Agent .....	47
5.4.2 Setting the IGMP Agent .....	48
Chapter 6 Advanced Configuration .....	49

---

6.1 QoS Configuration .....	49
6.1.1 Configuring QoS Port .....	49
6.1.2 Global QoS Configuration .....	50
6.2 MAC Access Control List .....	50
6.2.1 Setting the Name of the MAC Access Control List .....	50
6.2.2 Setting the Rules of the MAC Access Control List .....	51
6.2.3 Applying the MAC Access Control List .....	51
6.3 IP Access Control List .....	52
6.3.1 Setting the Name of the IP Access Control List .....	52
6.3.2 Setting the Rules of the IP Access Control List .....	52
6.3.3 Applying the IP Access Control List .....	54
Chapter 7 Network Management Configuration .....	55
7.1 SNMP Configuration .....	55
7.1.1 SNMP Community Management .....	55
7.1.2 SNMP Host Management .....	56
7.2 RMON .....	56
7.2.1 RMON Statistic Information Configuration .....	56
7.2.2 RMON History Information Configuration .....	57
7.2.3 RMON Alarm Information Configuration .....	58
7.2.4 RMON Event Configuration .....	58
Chapter 8 Diagnosis Tools .....	60
8.1 Ping .....	60
8.1.1 Ping .....	60
Chapter 9 System Management .....	62
9.1 User Management .....	62
9.1.1 User List .....	62
9.1.2 Establishing a New User .....	63
9.2 Log Management .....	63
9.3 Managing the Configuration Files .....	64
9.3.1 Exporting the Configuration Information .....	64
9.3.2 Importing the Configuration Information .....	65
9.4 Software Management .....	65
9.4.1 Backing up the IOS Software .....	65
9.4.2 Upgrading the IOS Software .....	66
9.5 Resuming Initial Configuration .....	66
9.6 Rebooting the Device .....	67

# Chapter 1 Configuration Preparation

## 1.1 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.

### 1.1.1 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#".

```
Switch>ena
Switch# 1 1 00:01:29 User admin enter privilege mode from console 0, level = 15

Switch#
Switch#
Switch#
Switch#
Switch#conf
Switch_config#
```

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

```
Switch_config#
Switch_config#int vlan 1
Switch_config_v1#ip add 192.168.0.1 255.255.255.0
Switch_config_v1#
```

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

```
Switch_config#ip http server
Switch_config#
Switch_config#
```

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.

```
Switch_config#aaa authentication login default local
Switch_config#aaa authentication enable default none
Switch_config#username admin password admin
Switch_config#
Switch_config#
Switch_config#
```

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

```
Switch_config#write
Saving current configuration...
OK!
Switch_config# 1 1 00:07:52 /startup-config is wrote, TID:87113610

Switch_config#
Switch_config#
```

### 1.1.2 Initially Accessing the Switch

1. Modify the IP address of the network adapter and subnet mask of your computer to **192.168.0.1** 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.

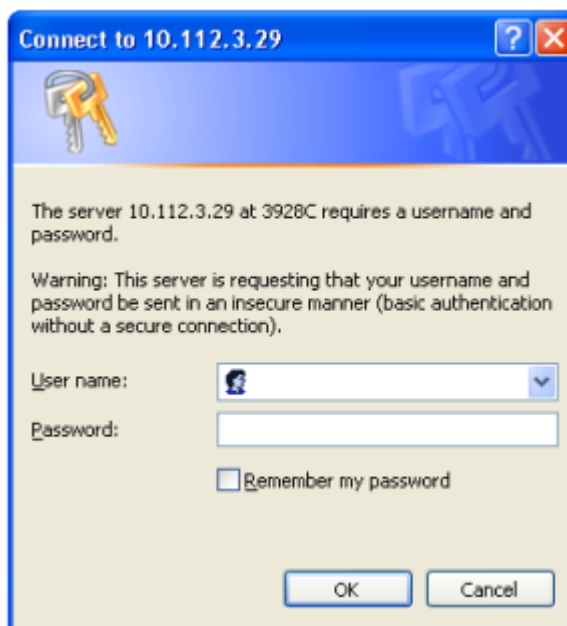


Figure 1: ID checkup of WEB login

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

## 1.2 Introduction of Web Interface

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

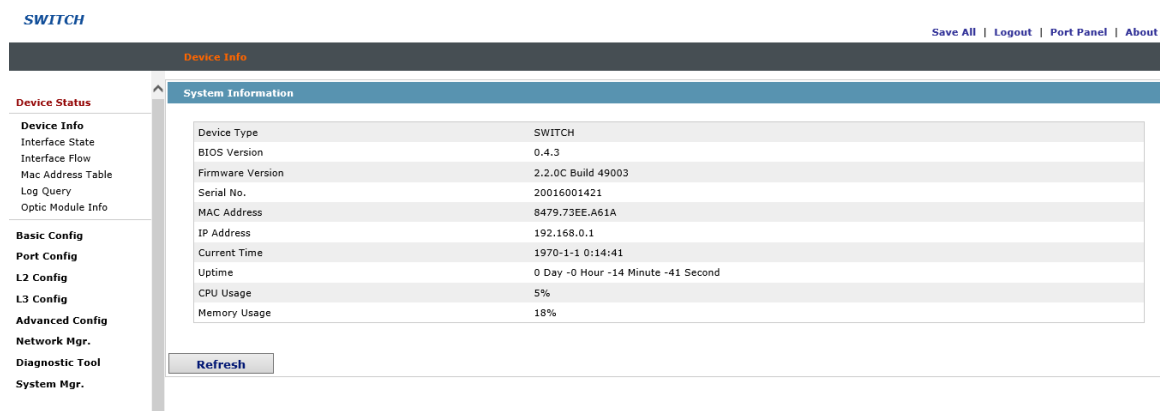


Figure 2: Web homepage

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

### 1.2.1 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 <b>write</b> 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.
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	After you click "port panel", You can see the port panel information above the page.
About	After you click "about", You can see the Copyright and refresh time.

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.

## 1.2.2 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.

---



## 1.2.3 Configuration Area

System Information	
Device Type	SWITCH
BIOS Version	0.4.3
Firmware Version	2.2.0C Build 49003
Serial No.	20016001421
MAC Address	8479.73EE.A61A
IP Address	192.168.0.1
Current Time	1970-1-1 0:2:5
Uptime	0 Day -0 Hour -2 Minute -5 Second
CPU Usage	7%
Memory Usage	18%

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.

## 1.2.4 Bottom Control Bar

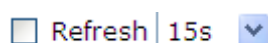


Figure 6: Bottom control bar

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.

## 1.2.5 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 2 Basic Configuration

### Device Status

### Basic Config

#### Hostname

Clock Mgr.

### Port Config

### L2 Config

### L3 Config

### Advanced Config

### Network Mgr.

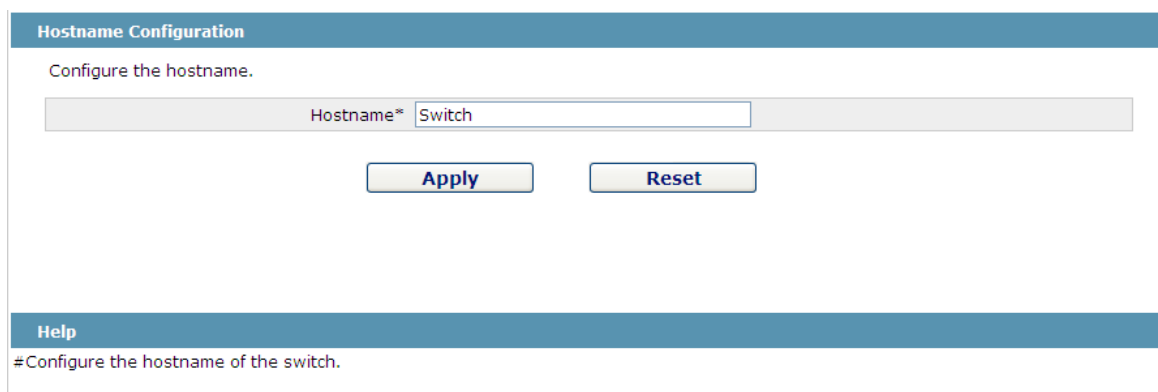
### Diagnostic Tool

### System Mgr.

Figure 1 A list of basic configuration

### 2.1 Hostname Configuration

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



Hostname Configuration

Configure the hostname.

Hostname\*

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".

## 2.2 Time Management

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

**Time Setting**

System Time

Select Time-Zone

☒ Set Time Manually

Set Time  Year  Month  Day  Hour  Minute(s)  Second

☐ Network Time Synchronization

SNTP Server One

SNTP Server Two

SNTP Server Three

Synchronization Interval  Minute(s)

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 3 Configuration of the Physical Interface



Figure 1: Physical port configuration list

### 3.1 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	
G0/2	
G0/3	
G0/4	

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.

## 3.2 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
G0/2	Up	Auto	Auto	Off	Auto
G0/3	Up	Auto	Auto	Off	Auto
G0/4	Up	Auto	Auto	Off	Auto
G0/5	Up	Auto	Auto	Off	Auto
G0/6	Up	Auto	Auto	Off	Auto
G0/7	Up	Auto	Auto	Off	Auto
G0/8	Up	Auto	Auto	Off	Auto
G0/9	Up	Auto	Auto	Off	Auto
G0/10	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:

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.

## 3.3 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)
G0/2	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/3	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/4	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/5	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/6	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/7	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/8	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/9	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/10	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.

## 3.4 Port mirroring

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

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. |

## 3.5 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 6.

Port	Status	Keepalive Period
G0/1	Enable	3333 (0-32767)Seconds

Figure 6: Port loopback detection

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

## 3.6 Port security

### 3.6.1 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 7.

Interface Name	Detail
G0/1	<a href="#">Detail</a>

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	<a href="#">Edit</a>
<input type="checkbox"/>	2	192.168.0.3	<a href="#">Edit</a>

Figure 8 Setting the binding of the source IP address

### 3.6.2 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 9.

Interface Name	Detail
G0/1	<a href="#">Detail</a>

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	<a href="#">Edit</a>
<input type="checkbox"/>	2	1234.1234.1235	<a href="#">Edit</a>

Figure 10 Setting the binding of the source MAC address

### 3.6.3 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 11.

Interface Name	Port Mode	Static MAC Filtration Mode
G0/1	Access	<a href="#">Disable</a>

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.

### 3.6.4 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	<a href="#">Detail</a>

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	<a href="#">Edit</a>

Figure 13: Setting static MAC filtration entries



### 3.6.5 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 14.

Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
G0/1	Disable <input type="button" value="v"/>	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.

## 3.7 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.

### 3.7.1 Broadcast Storm Control

Port	Status	Threshold
G0/1	Disable <input type="button" value="v"/>	<input type="text"/> (1-1638400) 100PPS
G0/2	Disable <input type="button" value="v"/>	<input type="text"/> (1-1638400) 100PPS
G0/3	Disable <input type="button" value="v"/>	<input type="text"/> (1-1638400) 100PPS
G0/4	Disable <input type="button" value="v"/>	<input type="text"/> (1-1638400) 100PPS
G0/5	Disable <input type="button" value="v"/>	<input type="text"/> (1-1638400) 100PPS
G0/6	Disable <input type="button" value="v"/>	<input type="text"/> (1-1638400) 100PPS
G0/7	Disable <input type="button" value="v"/>	<input type="text"/> (1-1638400) 100PPS

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.

### 3.7.2 Multicast Storm Control

G0/38	Disable ▾		(1-1638400) 100PPS
G0/39	Disable ▾		(1-1638400) 100PPS
G0/40	Disable ▾		(1-1638400) 100PPS
G0/41	Disable ▾		(1-1638400) 100PPS
G0/42	Disable ▾		(1-1638400) 100PPS
G0/43	Disable ▾		(1-1638400) 100PPS
G0/44	Disable ▾		(1-1638400) 100PPS
G0/45	Disable ▾		(1-1638400) 100PPS
G0/46	Disable ▾		(1-1638400) 100PPS
G0/47	Disable ▾		(1-1638400) 100PPS
G0/48	Disable ▾		(1-1638400) 100PPS
T1/1	Disable ▾		(1-1638400) 100PPS
T1/2	Disable ▾		(1-1638400) 100PPS
T1/3	Disable ▾		(1-1638400) 100PPS
T1/4	Disable ▾		(1-1638400) 100PPS
T1/5	Disable ▾		(1-1638400) 100PPS
T1/6	Disable ▾		(1-1638400) 100PPS
T1/7	Disable ▾		(1-1638400) 100PPS
T1/8	Disable ▾		(1-1638400) 100PPS



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.

## 3.7.3 Unknown Unicast Storm Control

G0/39	Disable ▾		(1-1638400) 100PPS
G0/40	Disable ▾		(1-1638400) 100PPS
G0/41	Disable ▾		(1-1638400) 100PPS
G0/42	Disable ▾		(1-1638400) 100PPS
G0/43	Disable ▾		(1-1638400) 100PPS
G0/44	Disable ▾		(1-1638400) 100PPS
G0/45	Disable ▾		(1-1638400) 100PPS
G0/46	Disable ▾		(1-1638400) 100PPS
G0/47	Disable ▾		(1-1638400) 100PPS
G0/48	Disable ▾		(1-1638400) 100PPS
T1/1	Disable ▾		(1-1638400) 100PPS
T1/2	Disable ▾		(1-1638400) 100PPS
T1/3	Disable ▾		(1-1638400) 100PPS
T1/4	Disable ▾		(1-1638400) 100PPS
T1/5	Disable ▾		(1-1638400) 100PPS
T1/6	Disable ▾		(1-1638400) 100PPS
T1/7	Disable ▾		(1-1638400) 100PPS
T1/8	Disable ▾		(1-1638400) 100PPS

Apply

Reset

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.

## Chapter 4 Layer-2 Configuration

**Device Status****Basic Config****Port Config****L2 Config****VLAN Config**

GVRP Config

STP Config

IGMP Snooping

Static ARP

Static MAC Config

LLDP Config

DDM Config

Port Channel

Ring Protection

Multiple Ring Protection

BackupLink Config

DHCP Snooping Config

Private VLAN Config

MTU Config

PDP Config

**L3 Config****Advanced Config****Network Mgr.****Diagnostic Tool****System Mgr.**

Figure 1: Layer-2 configuration list

### 4.1 VLAN Settings

#### 4.1.1 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	<a href="#">Edit</a>

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.

---

## 4.1.2 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

2

VLAN Name

VLAN0002

Port	Default VLAN	Mode	Untag or not	Allow or not
G0/1	1 <1-4094>	Access	No	Yes
G0/2	1 <1-4094>	Access	No	Yes
G0/3	1 <1-4094>	Access	No	Yes
G0/4	1 <1-4094>	Access	No	Yes
G0/5	1 <1-4094>	Access	No	Yes
G0/6	1 <1-4094>	Access	No	Yes
G0/7	1 <1-4094>	Access	No	Yes
G0/8	1 <1-4094>	Access	No	Yes
G0/9	1 <1-4094>	Access	No	Yes
G0/10	1 <1-4094>	Access	No	Yes
G0/11	1 <1-4094>	Access	No	Yes
G0/12	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.

---

## 4.2 GVRP Configuration

### 4.2.1 GVRP Config

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

GVRP Global Config

GVRP Global Config Disable ▾

Set Dynamic Vlan to Take Effect Only On Registration Ports Disable ▾

Apply Reset

Figure 4 GVRP configuration

Users can configure to turn on or off the global GVRP protocol, and can set whether the dynamic VLAN is valid only on the registered port.

### 4.2.2 GVRP Interface configuration

If you click **Layer-2 Config -> GVRP Config-> GVRP Interface Configuration** in the navigation bar, the GVRP Port configuration page appears, as shown in figure 5.

GVRP Interface Config

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

Port	GVRP Status
g0/1	<span>Enable ▾</span>
g0/2	<span>Enable ▾</span>
g0/3	<span>Enable ▾</span>
g0/4	<span>Enable ▾</span>
g0/5	<span>Enable ▾</span>
g0/6	<span>Enable ▾</span>

Figure 5 GVRP Interface Configuration

GVRP port configuration can start or close operation of GVRP protocol on ports.

## 4.3 LLDP Configuration

### 4.3.1 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

Apply Reset

**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.

### 4.3.2 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.

## 4.4 STP Configuration

### 4.4.1 STP Status Information

If you click **Layer-2 Config -> STP Config** in the navigation bar, the **STP Config** page appears, as shown in figure 8.

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 ▾
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

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 8 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.

## 4.4.2 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 9 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.

## 4.5 IGMP-Snooping Configuration

### 4.5.1 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 10 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.

### 4.5.2 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);	<a href="#">Edit</a>

Figure 11 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

2

Status of the IGMP Snooping Vlan

Enable

Immediate-leave

Disable

Configured Mrouter Port List

G0/1  
G0/12

Available Port List

G0/10  
G0/11  
G0/13  
G0/14  
G0/15  
G0/16  
G0/17  
G0/18  
G0/19  
G0/20

>>

<<

Apply

Reset

Go Back

Figure 12 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.

### 4.5.3 Static Multicast Address

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

Static Multicast Address Config

VLAN ID

Multicast IP Address

Assignment Port

Apply

Static Multicast List Info

No.0 Page/Total 0 Page

First Prev Next Last

Go No.

Page

Search:

Current 0 Item/Total 0 Item

	VLAN ID	Group	Port
<input type="checkbox"/>	Select All/Select None		

Delete

Refresh

Help

Figure 13 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.

#### 4.5.4 Multicast List

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

Multicast List Info

No.0 Page/Total 0 Page

First Prev Next Last

Go No.

Page

Search:

Current 0 Item/Total 0 Item

	VLAN ID	Group	Type	Port
<div>Refresh</div>				

Figure 14 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.

## 4.6 Setting Static ARP

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

**Basic ARP Config**

[New](#)

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

	IP Address	MAC Address	Interface VLAN	Operate
<input type="checkbox"/>	10.1.1.1	22:22:22:22:22:22	1	<a href="#">Edit</a>

☐ Select All/Select None [Delete](#)

**Help**

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

Figure 15 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"/>

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

**Help**

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

Figure 16 Setting static ARP

## 4.7 Setting Static MAC

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

**Static MAC Address List Info**

[New](#)

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

	Index	Static MAC Address	VLAN ID	Port	Operate
<input type="checkbox"/>					<a href="#">Delete</a>

☐ Select All/Select None

**Help**

Click New to configure a static MAC address and VLAN for the specified port. Unicast MAC addresses can configure only one port. Multicast MAC addresses can configure multiple ports.

Click Modify to modify the configured static MAC address.

Click delete can delete the selected static MAC address table entry.

**Static MAC Address Config**

Static MAC Address

VLAN ID

Configured Port List

Available Port List

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 20 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.

## 4.10 Ring Protection Configuration

### 4.10.1 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 21 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.

## 4.10.2 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	<input type="text"/>
Control VLAN	<input type="text"/>
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 22 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.

## 4.10.3 Configuration instance

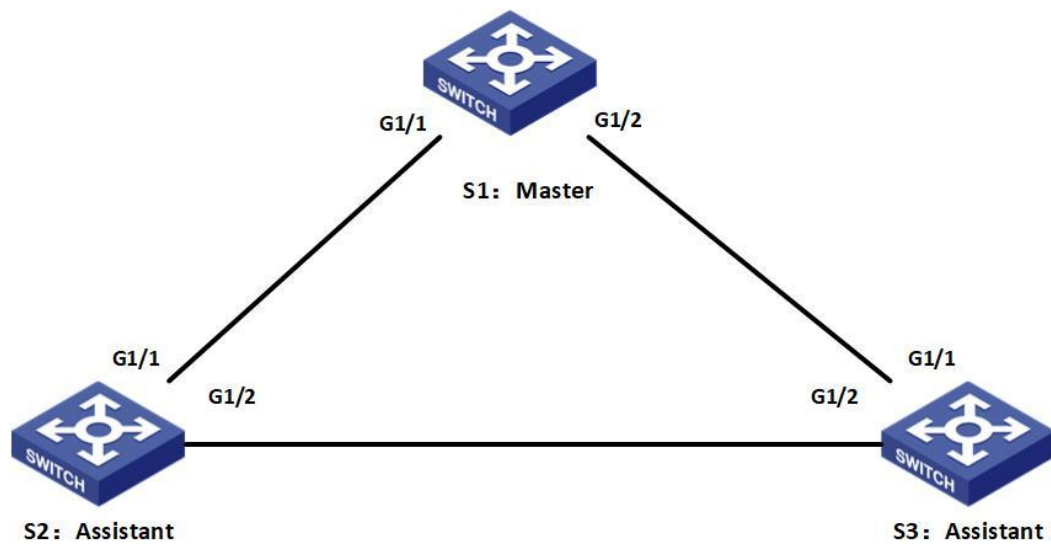


Figure 23 EAPS ring configuration

## SW1 Configuration

ether-ring	
Ring ID	0
Node Type	Master Node
Ring Description	
Control VLAN	9
Hello Time	1 (1-10)s
Fail Time	3 (3-30)s
Preforward Time	3 (3-30)s
Primary Port	g0/1
Secondary Port	g0/2

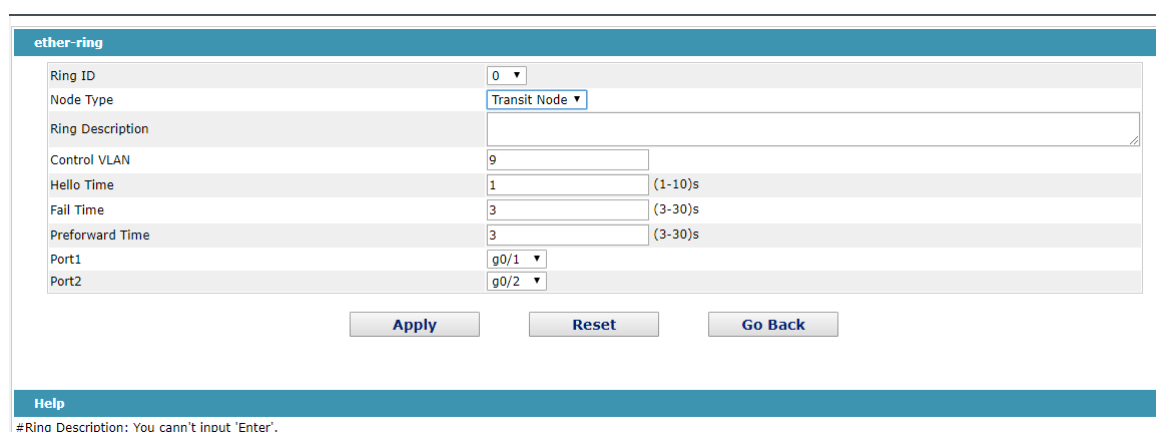
[Apply](#) [Reset](#) [Go Back](#)

**Help**

#Ring Description: You can't input 'Enter'.

Figure 24 EAPS ring configuration

## SW2&amp;SW3 Configuration



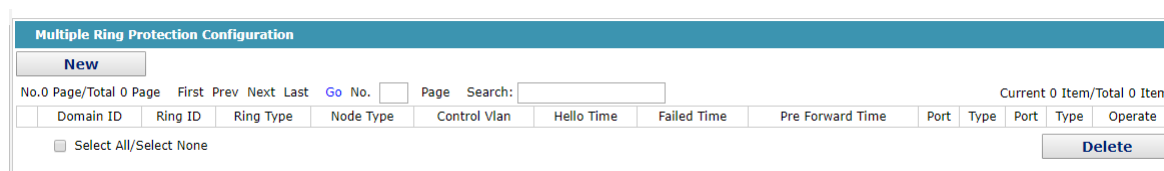
The image shows the 'ether-ring' configuration page. It contains several input fields: 'Ring ID' (0), 'Node Type' (Transit Node), 'Ring Description' (empty), 'Control VLAN' (9), 'Hello Time' (1), 'Fail Time' (3), 'Preforward Time' (3), 'Port1' (g0/1), and 'Port2' (g0/2). Each time field has a range in parentheses: (1-10)s, (3-30)s, and (3-30)s. At the bottom are 'Apply', 'Reset', and 'Go Back' buttons. A 'Help' section at the very bottom states: '#Ring Description: You can't input 'Enter'.'

Figure 25 EAPS ring configuration

## 4.11 Multiple Ring Protection

### 4.11.1 MEAPS Ring List

If you click **Layer-2 Config -> Multiple Ring Protection**, the **Multiple Ring Protection** page appears.



The image shows the 'Multiple Ring Protection Configuration' page. It has a 'New' button and a table with columns: No.0, Page/Total 0, Page, First, Prev, Next, Last, Go, No., Page, Search:, and Current 0 Item/Total 0 Item. Below the table is a 'Select All/Select None' checkbox and a 'Delete' button. The table itself is empty.

Figure 26 MEAPS Ring List

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

Click "New" to create a new MEAPS ring.

Note:

- 1, the number of MEAPS domains supported by the system is 4 (0-3).
- 2, the number of rings supported within a domain is 8 (0-7).
- 3, Once a MEAPS is configured, its domain name ID, ring ID, ring type, node type, and control Vlan will not be modified. If you need to adjust, please delete the ring net and rebuild it.

### 4.11.2 MEAPS Ring Configuration

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



NewMEAPS Global Config	
Domain ID*	<input type="text"/>
Ring ID*	<input type="text"/>
Ring Type*	Major Ring ▼
Node Type*	Master Node ▼
Control Vlan*	<input type="text"/>
Hello Time	<input type="text"/>
Failed Time	<input type="text"/>
Pre-Forward Time	<input type="text"/>
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 27 MEAPS Ring configuration

**Note:**

If the existing MEAPS ring network is configured, the domain name ID, ring ID, ring type, node type, and control Vlan in the page are not modifiable.

Only the master node and the transport node can be configured in the main ring.

The main nodes, transmission nodes, edge nodes and auxiliary edge nodes can be configured in the sub ring.

The primary node and the transport node can only exist in one ring, while the edge node and the auxiliary edge node can exist in multiple rings at the same time.

In the drop-down boxes to the right of Main Port and Secondary Port, choose one port for each ring port, or choose None.

## 4.11.3 Configuration instance

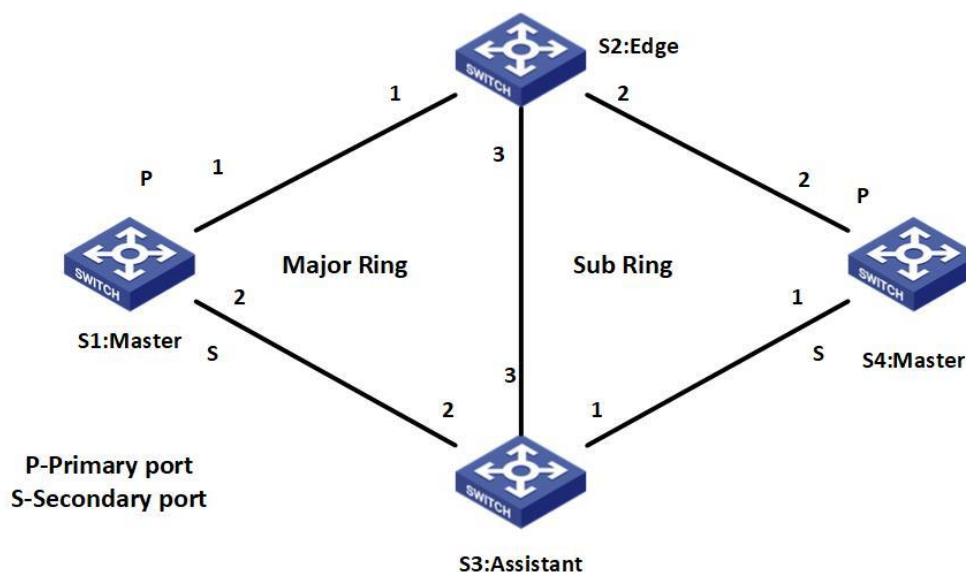


Figure 28 MEAPS Ring configuration

S1, S2, S3 constitute the main ring, S2, S3, S4 constitute the sub-ring; the main ring S1 as the main node, S1 g1/2 port as the logical breakpoint; the sub-ring S4 as the main node, S4 g1/2 port as the logical breakpoint

### SW1 Configuration

NewMEAPS Global Config		
Domain ID*	<input type="text" value="0"/>	
Ring ID*	<input type="text" value="1"/>	
Ring Type*	Major Ring ▼	
Node Type*	Master Node ▼	
Control Vlan*	<input type="text" value="9"/>	
Hello Time	<input type="text" value="1"/>	
Failed Time	<input type="text" value="3"/>	
Pre-Forward Time	<input type="text" value="3"/>	
Primary-Port	g0/1 ▼	
Secondary-Port	g0/2 ▼	

**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 29 MEAPS Ring configuration

### SW2&SW3 Major Ring Configuration

NewMEAPS Global Config		
Domain ID*	<input type="text" value="0"/>	
Ring ID*	<input type="text" value="1"/>	
Ring Type*	Major Ring ▼	
Node Type*	Transit Node ▼	
Control Vlan*	<input type="text" value="9"/>	
Hello Time	<input type="text" value="1"/>	
Failed Time	<input type="text" value="3"/>	
Pre-Forward Time	<input type="text" value="3"/>	
Transit-Port	g0/1 ▼	
Transit-Port	g0/2 ▼	

**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 30 MEAPS Ring configuration

### SW2 sub-ring Configuration

NewMEAPS Global Config		
Domain ID*	<input type="text" value="0"/>	
Ring ID*	<input type="text" value="2"/>	
Ring Type*	<input type="text" value="Sub Ring"/>	
Node Type*	<input type="text" value="Edge Node"/>	
Control Vlan*	<input type="text" value="9"/>	
Hello Time	<input type="text" value="1"/>	
Failed Time	<input type="text" value="3"/>	
Pre-Forward Time	<input type="text" value="3"/>	
Common-Port	<input type="text" value="g0/3"/>	
Edge-Port	<input type="text" value="g0/2"/>	

**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 31 MEAPS Ring configuration

## SW3 sub-ring Configuration

NewMEAPS Global Config		
Domain ID*	<input type="text" value="0"/>	
Ring ID*	<input type="text" value="2"/>	
Ring Type*	<input type="text" value="Sub Ring"/>	
Node Type*	<input type="text" value="Assistant Node"/>	
Control Vlan*	<input type="text" value="9"/>	
Hello Time	<input type="text" value="1"/>	
Failed Time	<input type="text" value="3"/>	
Pre-Forward Time	<input type="text" value="3"/>	
Common-Port	<input type="text" value="g0/3"/>	
Edge-Port	<input type="text" value="g0/2"/>	

**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 32 MEAPS Ring configuration

## SW4 sub-ring Configuration

NewMEAPS Global Config		
Domain ID*	<input type="text" value="0"/>	
Ring ID*	<input type="text" value="2"/>	
Ring Type*	<input type="text" value="Sub Ring"/>	
Node Type*	<input type="text" value="Master Node"/>	
Control Vlan*	<input type="text" value="9"/>	
Hello Time	<input type="text" value="1"/>	
Failed Time	<input type="text" value="3"/>	
Pre-Forward Time	<input type="text" value="3"/>	
Primary-Port	<input type="text" value="g0/1"/>	
Secondary-Port	<input type="text" value="g0/2"/>	

**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 33 MEAPS Ring configuration

## 4.12 Backuplink Configuration

### 4.12.1 Backuplink protocol global configuration

If you click **Layer-2 Config -> Backuplink configuration**, the **Backuplink protocol global configuration** page appears.

Figure 34 Backuplink protocol global configuration

The current link backup group is listed in the page, including its preemption mode and preemption delay.

Click new to create a new link backup group.

Click the "Modify" option on the right side of the entry to configure the preemption mode and preemption delay parameters for the link backup group.

Figure 35 Backuplink protocol global configuration

Note:

- 1, the number of link backup groups supported by the system is 8.
- 2, the preemptive mode of the link backup group determines the strategy of selecting the forwarding message by the main port and the backup port.

### 4.12.2 Backuplink Protocol Interface Configuration

If you click **Layer-2 Config -> Backuplink configuration**, the **Backuplink protocol Interface configuration** page appears.

BackupLink Protocol Interface Config					
No.1	Page/Total 1 Page	First	Prev	Next	Last
Go	No.		Page	Search:	
					Current 56 Item/Total 56 Item
Interface Name	Group ID	Interface Attribute	MMU Attribute	Shareload VLAN	Operate
g0/1					Edit
g0/2					Edit
g0/3					Edit
g0/4					Edit
g0/5					Edit
g0/6					Edit
g0/7					Edit
g0/8					Edit
g0/9					Edit
g0/10					Edit
g0/11					Edit
g0/12					Edit
g0/13					Edit
g0/14					Edit
g0/15					Edit
g0/16					Edit
g0/17					Edit
g0/18					Edit
g0/19					Edit
g0/20					Edit
g0/21					Edit

Figure 36 Backuplink protocol Interface configuration

The page lists the member ports currently added to the backup link group, as well as the port attributes of the member ports, MMU attributes and load balancing vlan. The MMU sender can trigger the receiver to update the MAC address table quickly by sending MMU messages to the receiver.

Click the "edit" option on the right side of the item to configure the link backup protocol for the port.

BackupLink Protocol Interface Config	
Interface Name	g0/1
Group ID	<input type="text"/>
Interface Attribute	<input type="text"/>
MMU Attribute	<input type="text"/>
Shareload VLAN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Go Back"/>	
<b>Help</b> #Share Load VLAN can be Only Configured On The Backup Port	

Figure 37 Backuplink protocol Interface configuration

For a link backup group with a primary port configured, no other port can be configured as the primary port for the link backup group. Similarly, for a link backup group with a backup port configured, no other port can be configured as a backup port for the link backup group.

## 4.13 DHCP Snooping Configuration

### 4.13.1 DHCP Snooping configuration

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

BackupLink Protocol Interface Config	
Interface Name	g0/1
Group ID	<input type="text"/>
Interface Attribute	<input type="text"/>
MMU Attribute	<input type="text"/>
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 38 DHCP Snooping configuration

The global DHCP Snooping protocol is opened, and the switch listens to all DHCP packets to form the corresponding binding relationship. If the client gets the address through the switch before configuring the command, the switch cannot add the corresponding binding relationship.

When the switch configuration saves and restarts, the original configuration of the interface binding relationship will be lost, at this time, there is no binding relationship on the interface, the switch refuses to forward all IP packets after starting the IP source address monitoring function. After configuring the TFTP server with the interface binding relationship backup, the binding relationship will be backed up to the server through the TFTP protocol. After the switch restarts, the binding table will be automatically downloaded to the TFTP server to ensure the normal operation of the network.

The name of the file that is saved on the TFTP server when the backup interface binding relation is configured. In this way, different switches can backup their interface binding relation tables to the same TFTP server.

The binding table of the MAC address and IP address of the interface is dynamic and needs to be checked after a certain time interval to see if the binding is updated, and if there is an update (add or delete the binding entry), it is backed up again. The default interval is 30 minutes.

#### 4.13.2 DHCP Snooping VLAN Configuration

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

DHCP Snooping VLAN Config	
Enable DHCP Snooping VLAN	<input type="text"/>
Enable Dynamic ARP Inspection VLAN	<input type="text"/>
Enable Verify Source VLAN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 39 DHCP Snooping vlan configuration

Starting the DHCP Snooping function on the VLAN validates the DHCP packets received by all untrusted physical ports belonging to the entire VLAN. DHCP response packets received by untrusted physical ports in the VLAN will be discarded to prevent users from forging or misallocating addresses to DHCP servers; for untrusted port DHCP request packets, if the MAC address sent by the message does not match the hardware address field in the message, it is considered to be intentionally forged by the user. In the DHCP DOS (denial of service) attack message, the switch will also be discarded.

ARP dynamic monitoring is performed on all physical ports belonging to a VLAN. If the source MAC and source IP addresses of ARP packets received by the interface do not meet the MAC and IP address binding relationships configured on the interface, the packet is rejected. The binding relationship configured on the interface can be dynamically bound by DHCP or manually configured. If no MAC and IP address bindings are configured on the physical interface, the switch refuses to forward all ARP packets.

A VLAN that starts IP source address monitoring is rejected if the source MAC and source IP addresses of IP packets received by all physical ports of the VLAN do not meet the MAC and IP address binding relationships configured on the interface. The binding relationship configured on the interface can be dynamically bound by DHCP or manually configured. If no MAC and IP address bindings are configured on this physical interface, the switch refuses to forward all IP packets received by the interface.

### 4.13.3 DHCP Snooping Interface Configuration

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

Port	DHCP Trust Port	ARP Inspection Trust Port	IP Source Trust Port
g0/1	Distrust	Distrust	Distrust
g0/2	Distrust	Distrust	Distrust
g0/3	Distrust	Distrust	Distrust
g0/4	Distrust	Distrust	Distrust
g0/5	Distrust	Distrust	Distrust
g0/6	Distrust	Distrust	Distrust
g0/7	Distrust	Distrust	Distrust

Figure 40 DHCP Snooping interface configuration

The configuration interface is the DHCP trust interface, and the DHCP message received by the interface is not checked.

For ARP monitoring the trust interface, the ARP monitoring function is not started. The interface is default to a non trusted interface.

For the IP source address trust interface, the source address checking function is not started.

### 4.13.4 DHCP Snooping Binding List Manual Configuration

If you click **Layer-2 Config -> DHCP Snooping configuration -> DHCP Snooping Binding List Manual configuration**, the **DHCP Snooping Binding List Manual configuration** page appears.

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

MAC Address	IP Address	Interface Name	VLAN
-------------	------------	----------------	------

☐ Select All/Select None Delete

**Help**  
#Manual binding list is prior to the dynamic binding list, and the mac address is the only index of the binding item.

Figure 41 DHCP Snooping binding list manual configuration

For hosts that do not use DHCP to get addresses, you can manually configure the addition of binding entries on the switch interface to enable the host to access the

network normally. Using the no command of this command, you can delete binding entries.

Manually configured binding entries have higher priority than dynamically configured binding entries. If the MAC address of the configured entry is the same as the MAC address of the dynamically configured entry, the manually configured update dynamically configured entry. The interface binding entry is uniquely indexed by the MAC address.

Click new, users can create DHCP Snooping manually configure interface binding entries.

Figure 42 DHCP Snooping binding list manual configuration

## 4.14 MTU Configuration

If you click **Layer-2 Config -> MTU Configuration**, the **MTU Configuration** page appears.

Figure 43 MTU configuration

The user can set the maximum transmission unit MTU size within the specified range.

## 4.15 PDP Configuration

### 4.15.1 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 44 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.

#### 4.15.2 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 45 PDP port configuration

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

## 4.16 POE Management

### 4.16.1 POE Global Configuration

**Poe enabled devices can be configured.**

If you click **Port Config -> POE Mgr** in the navigation bar, the POE management configuration page appears, as shown in the following figure.

POE Global Configure		
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	Stop	
Power Supply Standard	Max Power Supply	
<input type="button" value="Apply"/> <input type="button" value="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

Figure 46 POE configuration

On this page, you can configure the POE power supply management mode, lower priority upgrade preemption threshold, enable/disable POE MIB inform.

#### 4.16.2 POE Global Realtime Info

If you click **Port Config -> POE Mgr->POE Global Realtime Info** in the navigation bar, the POE management configuration page appears, as shown in the following figure.

POE Global Realtime Info		
POE Chip	PD69100	
POE Port Number	16	
PSE Total Power	300000	
PSE Uage Threshold	100%	
PSE Alarm Power	100	
PSE Consumed Power	0	
PSE Temperature	38	
<div>Refresh</div>		

Figure 47 POE configuration

On this page, you can check POE port number, PSE power and PSE temperature.

#### 4.16.3 POE Interface List

If you click **Port Config -> POE Mgr->POE Interface List** in the navigation bar, the POE management configuration page appears, as shown in the following figure.

POE Interface List					
<div> <b>Filters</b> Port Type: <input type="button" value="All"/> Slot Num: <input type="button" value="All"/> Name(s): <input type="text"/> <input type="button" value="Help"/> </div>					
Port	Port Max Power	Port Priority	Force Connection	POE Interface Description	
g0/1	30000 mw	Low Priority	Disable		
g0/2	30000 mw	Low Priority	Disable		
g0/3	30000 mw	Low Priority	Disable		
g0/4	30000 mw	Low Priority	Disable		
g0/5	30000 mw	Low Priority	Disable		
g0/6	30000 mw	Low Priority	Disable		
g0/7	30000 mw	Low Priority	Disable		

Figure 48 POE configuration

On this page, you can configure the Port Priority, Port Max Power, Force Connection and POE Interface Description.

#### 4.16.4 POE Port Policy Power

If you click **Port Config -> POE Mgr->POE Port Policy Power** in the navigation bar, the POE Port Policy Power configuration page appears, as shown in the following figure.

**POE Port Policy Power**

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

Port	POE Function	Time Range
g0/1	<input type="button" value="Disable"/>	POETIME
g0/2	<input type="button" value="Disable"/>	
g0/3	<input type="button" value="Enable"/>	
g0/4	<input type="button" value="Enable"/>	
g0/5	<input type="button" value="Enable"/>	
g0/6	<input type="button" value="Enable"/>	
g0/7	<input type="button" value="Enable"/>	

Figure 49 POE configuration

On this page, you can enable/disable POE Function and Time Range.

#### 4.16.5 POE Interface Power List

If you click **Port Config -> POE Mgr-> POE Port Policy Power** in the navigation bar, the POE Port Policy Power configuration page appears, as shown in the following figure.

**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	30000mw	-	-	-
g0/2	0mw	30000mw	-	-	-
g0/3	0mw	30000mw	-	-	-
g0/4	0mw	30000mw	-	-	-
g0/5	0mw	30000mw	-	-	-
g0/6	0mw	30000mw	-	-	-

Figure 50 POE configuration

On this page, you can check Current Power, Setting Max Power, Average Power, Peak Power and Bottom Power.

#### 4.16.6 POE Port Other Info

If you click **Port Config -> POE Mgr-> POE Port Other Info** in the navigation bar, the PPOE Port Other Info configuration page appears, as shown in the following figure.

**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	Searching	Signal	0	0mA
g0/2	Searching	Signal	0	0mA
g0/3	Searching	Signal	0	0mA
g0/4	Searching	Signal	0	0mA
g0/5	Searching	Signal	0	0mA
g0/6	Searching	Signal	0	0mA
g0/7	Searching	Signal	0	0mA

Figure 51 POE configuration

On this page, you can check POE Port Detection Status, POE Port Power Supply, POE IEEE Class, and POE Port Current.

## Chapter 5 Layer-3 Configuration



Figure 1 Layer-3 configuration list

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

### 5.1 Configuring the VLAN Interface

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

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"/>	Name of the VLAN Interface	IP Attribute	IP Address	Operate	
<input type="checkbox"/>	1	Manual Config	192.168.0.1/24;	<a href="#">Edit</a>	
<input type="checkbox"/> Select All/Select None					<a href="#">Delete</a>

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\*

**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.

## 5.2 Setting the Static Route

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

**Static Routing Protocol Config**

**New**

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

Default Route	Dest IP Segment	Dest IP Mask	Interface Type	VLAN Interface	Gateway's IP Address	Forwarding Routing Address	Distance metric	Routing Tag	Global	Specify the route description	Operate
<input type="checkbox"/> Select All/Select None											<b>Delete</b>

**Help**

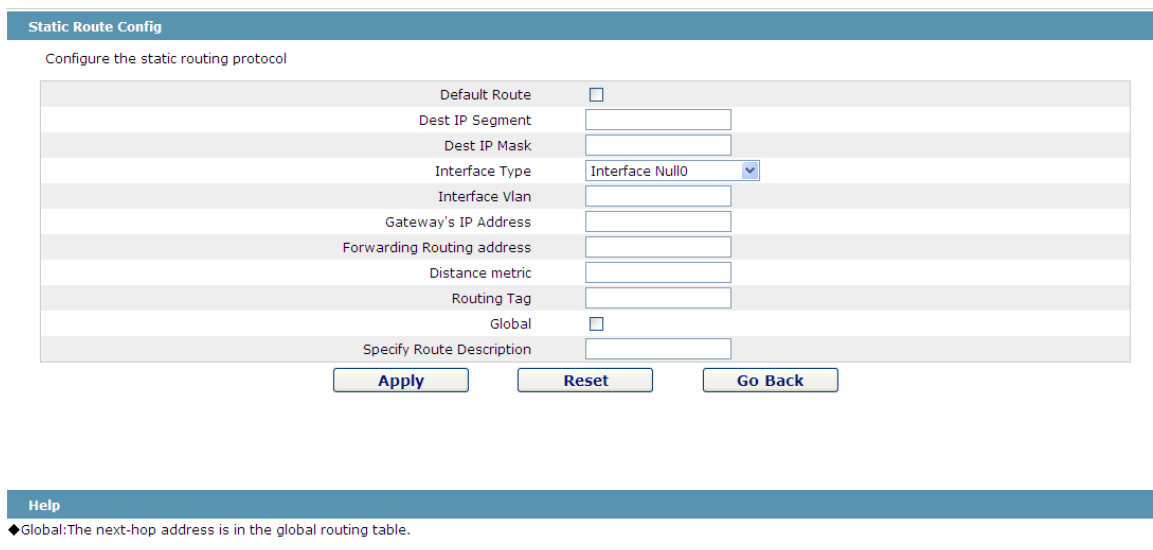
◆ Global: The next-hop address is in the global routing table.

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.



**Static Route Config**

Configure the static routing protocol

Default Route	<input type="checkbox"/>
Dest IP Segment	<input type="text"/>
Dest IP Mask	<input type="text"/>
Interface Type	Interface Null0
Interface Vlan	<input type="text"/>
Gateway's IP Address	<input type="text"/>
Forwarding Routing address	<input type="text"/>
Distance metric	<input type="text"/>
Routing Tag	<input type="text"/>
Global	<input type="checkbox"/>
Specify Route Description	<input type="text"/>

**Apply** **Reset** **Go Back**

**Help**

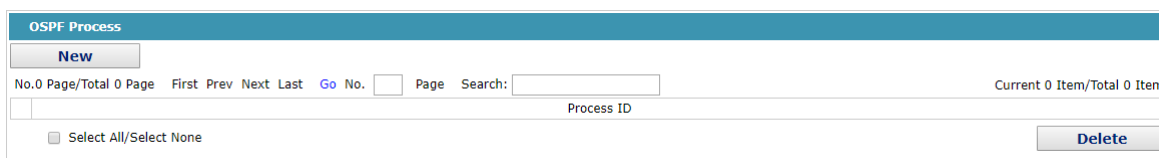
◆ Global: The next-hop address is in the global routing table.

Figure 5 Setting the static route

## 5.3 OSPF Route Configuration

### 5.3.1 OSPF Process

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



**OSPF Process**

**New**

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


No.	Process ID
<input type="checkbox"/>	

☐ Select All/Select None **Delete**

Figure 6 Displaying the ospf route

Before configuring the OSPF routing entry, you must first create the OSPF process, otherwise it will not be configured. In the OSPF process page, you can create the OSPF process or delete the OSPF process.

Click new to enter the OSPF process page.



**Creating the OSPF Process**

OSPF Process

**Apply** **Go Back**

Figure 7 Displaying the ospf route

## 5.3.2 OSPF Route Entries

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

Figure 8 Displaying the ospf route

Enter the OSPF process number that has been created and click on the application to enter the specified OSPF process routing entry page.

Figure 9 Displaying the ospf route

Click on the new build to create the OSPF routing entry for the specified process.

Figure 10 Displaying the ospf route

Area supports integer and IP address forms.

## 5.4 IGMP Agent

### 5.4.1 Enabling the IGMP Agent

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

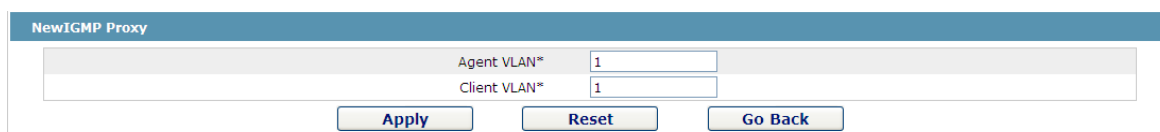


Figure 11 Enabling the IGMP agent

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.

#### 5.4.2 Setting the IGMP Agent

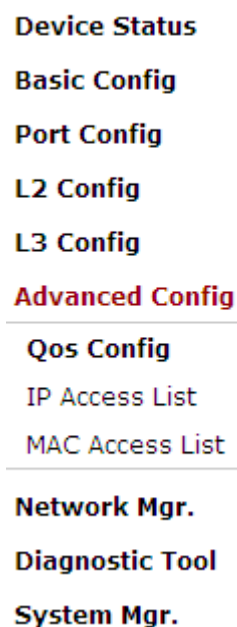
If you click **Layer-3 Config -> IGMP agent -> IGMP agent Config**, the **IGMP agent configuration** page appears. Click **New** to create a new IGMP agent.



NewIGMP Proxy	
Agent VLAN*	1
Client VLAN*	1
<div>Apply    Reset    Go Back</div>	

Figure 12 Setting the IGMP agent

## Chapter 6 Advanced Configuration



Device Status  
Basic Config  
Port Config  
L2 Config  
L3 Config  
**Advanced Config**  
Qos Config  
IP Access List  
MAC Access List  
Network Mgr.  
Diagnostic Tool  
System Mgr.

Figure 1 A list of advanced configuration

### 6.1 QoS Configuration

#### 6.1.1 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	0
G0/7	1
G0/8	2
G0/9	3
G0/10	4
G0/11	5
	6
	7

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.

### 6.1.2 Global QoS Configuration

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

**QoS Config**

**Schedule Policy**

Schedule Policy: sp

Queue 1	Queue 2	Queue 3	Queue 4
1 (1-15)	1 (1-15)	1 (0-15)	1 (0-15)
Queue 5	Queue 6	Queue 7	Queue 8
1 (0-15)	1 (0-15)	1 (0-15)	1 (0-15)

**COS-to-queue map**

COS value	Queue
0	Queue 1
1	Queue 2
2	Queue 3
3	Queue 4
4	Queue 5
5	Queue 6
6	Queue 7
7	Queue 8

**Help**

- ◆ If you want to configure the cos value of the interface, please goto QoS Interface Configuration.
- ◆ 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.

## 6.2 MAC Access Control List

### 6.2.1 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.

**MAC ACL Config**

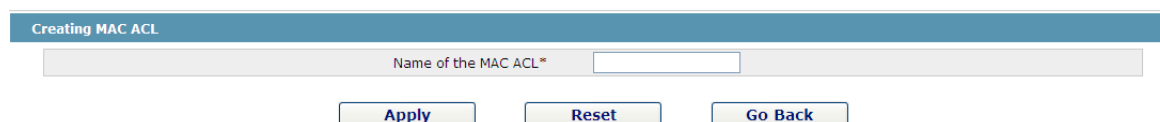
No. 0 Page/Total 0 Page First Prev Next Last Go No.  Page Search:

Current 0 Item/Total 0 Item

Name of the MAC Access Control List	Operate
<input type="checkbox"/> Select All/Select None	<input type="button" value="Delete"/>

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.

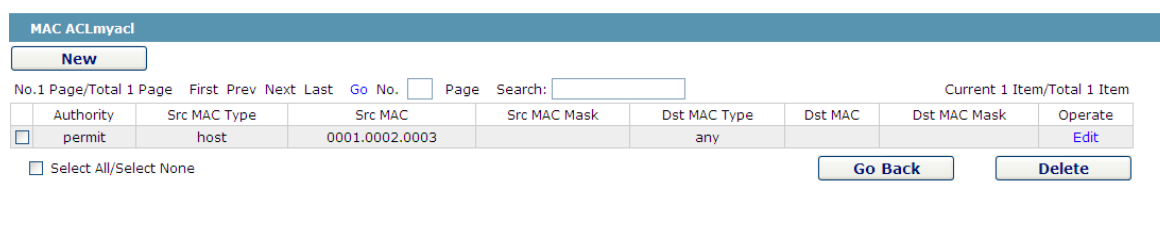


The 'Creating MAC ACL' form features a title bar with the text 'Creating MAC ACL'. Below the title bar is a text input field labeled 'Name of the MAC ACL \*'. At the bottom of the form are three buttons: 'Apply', 'Reset', and 'Go Back'.

Figure 5 Setting the name of MAC access control list

## 6.2.2 Setting the Rules of the MAC Access Control List

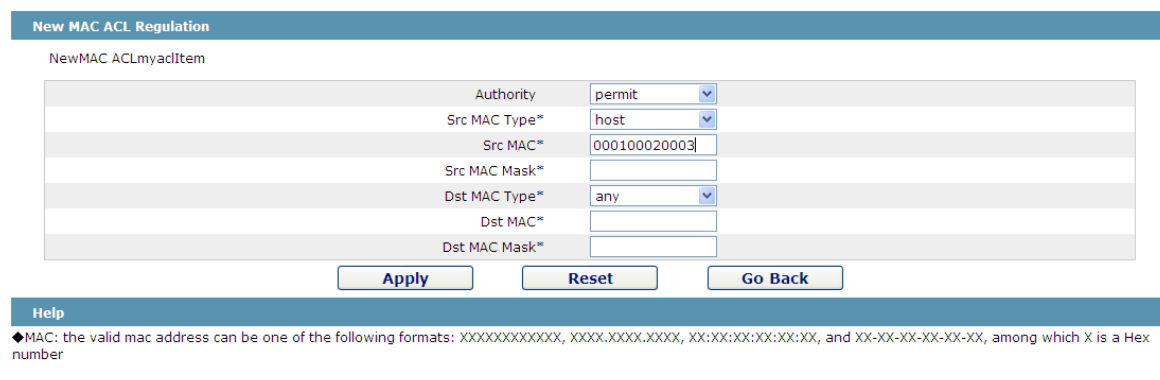
If you click Modify, the corresponding MAC access control list appears and you can set the corresponding rules for the MAC access control list.



The 'MAC ACLmyacl' configuration page includes a 'New' button at the top left. Below it is a table with columns: No.1, Page/Total 1 Page, First, Prev, Next, Last, Go No., Page, Search:, and Current 1 Item/Total 1 Item. The table contains one row with the following data: Authority: permit, Src MAC Type: host, Src MAC: 0001.0002.0003, Src MAC Mask: (empty), Dst MAC Type: any, Dst MAC: (empty), Dst MAC Mask: (empty), and Operate: Edit. Below the table is a checkbox labeled 'Select All/Select None' and two buttons: 'Go Back' and 'Delete'.

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.



The 'New MAC ACL Regulation' form has a title bar with the text 'New MAC ACL Regulation'. Below the title bar is a section labeled 'NewMAC ACLmyaclItem' containing a table with the following fields: Authority (dropdown menu with 'permit' selected), Src MAC Type\* (dropdown menu with 'host' selected), Src MAC\* (text input field with '000100020003'), Src MAC Mask\* (text input field), Dst MAC Type\* (dropdown menu with 'any' selected), Dst MAC\* (text input field), and Dst MAC Mask\* (text input field). At the bottom of the form are three buttons: 'Apply', 'Reset', and 'Go Back'. Below the form is a 'Help' section with a diamond icon and the text: '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

## 6.2.3 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

## 6.3 IP Access Control List

### 6.3.1 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.

The screenshot shows the 'IP ACL Config' page. At the top, there is a 'New' button. Below it, a navigation bar shows 'No.1 Page/Total 1 Page' and 'First Prev Next Last' links. A search bar is present with the text 'Go No. [ ] Page Search: [ ]'. On the right, it says 'Current 2 Item/Total 2 Item'. The main table has three columns: 'Name of the IP ACL', 'Attribute of the IP ACL', and 'Operate'. It contains two rows: one with 'acla' and 'extended', and another with 'myacl' and 'standard'. Each row has an 'Edit' link in the 'Operate' column. At the bottom left, there is a checkbox labeled 'Select All/Select None'. At the bottom right, there is a 'Delete' button.

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.

The screenshot shows the 'Creating the IP ACL' form. It has a text field labeled 'Name of the IP ACL\*' and a dropdown menu labeled 'Attribute' with 'standard' selected. At the bottom, there are three buttons: 'Apply', 'Reset', and 'Go Back'.

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.

### 6.3.2 Setting the Rules of the IP Access Control List

Standard IP access control list

**IP Standard ACLmyacl**

[New](#)

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

No.	Authority	Src IP	Src IP Mask	Record the log	Operate
<input type="checkbox"/>	permit	1.1.1.1	255.255.255.0	log	<a href="#">Edit</a>

☐ Select All/Select None

[Go Back](#) [Delete](#)

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.

**NewStandard IP ACL Regulation**

NewIP Access Control ListmyaclItem

Authority	permit
Src IP Type	Specify IP
Src IP*	1.1.1.1
Src IP Mask	255.255.255.0
Src IP Range*	<input type="text"/> - <input type="text"/>
Log	<input checked="" type="checkbox"/>

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

Figure 12 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.  Page Search:  Current 1 Item/Total 1 Item

No.	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	<a href="#">Edit</a>

☐ Select All/Select None

[Go Back](#) [Delete](#)

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	

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

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

### 6.3.3 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 7 Network Management Configuration

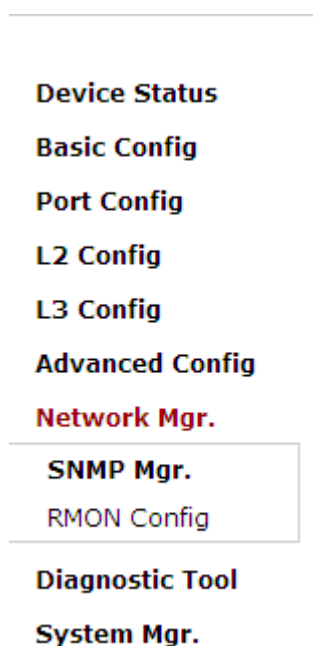


Figure 1 Network management configuration list

### 7.1 SNMP Configuration

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

#### 7.1.1 SNMP Community Management

 The screenshot shows the 'SNMP Community Mgr' tab selected. Below it is the 'SNMP Community Management' section with a 'New' button. A table lists the community configuration. The table has columns for 'SNMP Community Name', 'SNMP Community Encryption', 'SNMP Community Attribute', and 'Operate'. The first row shows 'public' as the name, 'False' as encryption, 'RO' as the attribute, and an 'Edit' link as the operate action. There are also pagination controls at the top and bottom of the table.
 

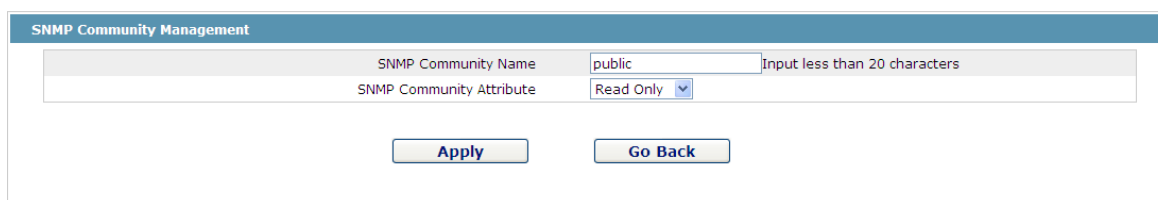
SNMP Community Name	SNMP Community Encryption	SNMP Community Attribute	Operate
public	False	RO	<a href="#">Edit</a>

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.



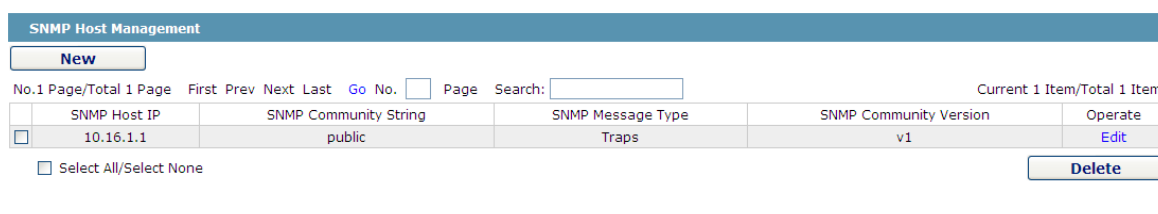


The screenshot shows the 'SNMP Community Management' web interface. It features a header bar with the title. Below it, there are two input fields: 'SNMP Community Name' with the value 'public' and a note 'Input less than 20 characters', and 'SNMP Community Attribute' with a dropdown menu set to 'Read 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.

## 7.1.2 SNMP Host Management



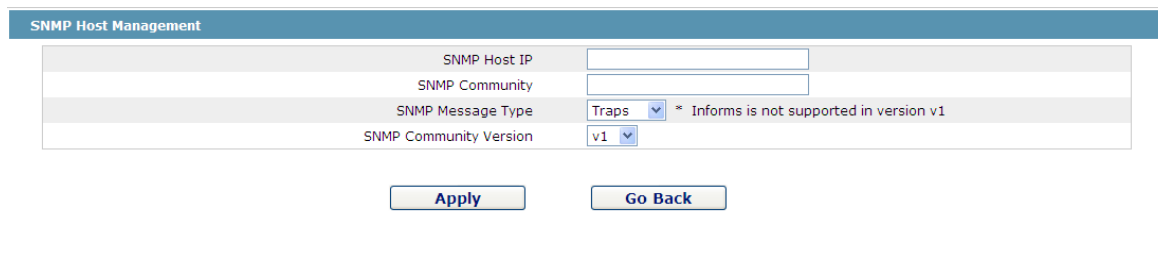
The screenshot shows the 'SNMP Host Management' web interface. It includes a 'New' button, a table with one row of data, and a 'Delete' button. The table has columns for 'SNMP Host IP', 'SNMP Community String', 'SNMP Message Type', 'SNMP Community Version', and 'Operate'. The data row shows '10.16.1.1', 'public', 'Traps', 'v1', and 'Edit'. There are also pagination controls and a search bar at the top.

SNMP Host IP	SNMP Community String	SNMP Message Type	SNMP Community Version	Operate
10.16.1.1	public	Traps	v1	Edit

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 form. It includes fields for 'SNMP Host IP', 'SNMP Community', 'SNMP Message Type' (set to 'Traps'), and 'SNMP Community Version' (set to 'v1'). There is a note '\* Informs is not supported in version 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.

## 7.2 RMON

### 7.2.1 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	
<div> <input type="button" value="Apply"/> <input type="button" value="Go Back"/> </div>		

**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.

## 7.2.2 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*
<div> <input type="button" value="Apply"/> <input type="button" value="Go Back"/> </div>		

**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.

### 7.2.3 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.

### 7.2.4 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" value="(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 8 Diagnosis Tools



Figure 1 Diagnosis tool list

### 8.1 Ping

#### 8.1.1 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)

PING

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

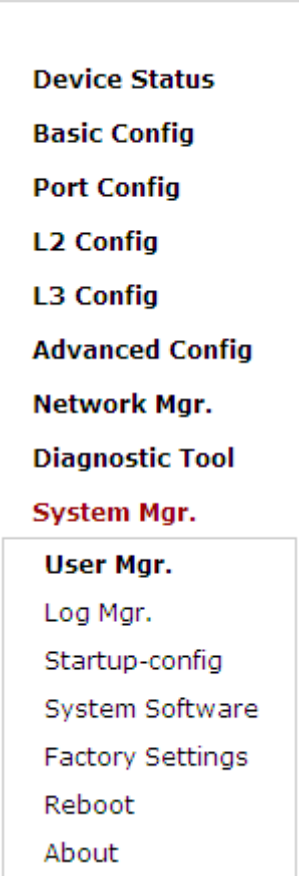
Ping is used to test whether the switch connects other devices.

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 9 System Management



A vertical list of system management options. The first seven items are in a standard black font, while 'System Mgr.' is highlighted in red. Below this list is a light blue rectangular box containing a sub-menu.

- Device Status
- Basic Config
- Port Config
- L2 Config
- L3 Config
- Advanced Config
- Network Mgr.
- D diagnostic Tool
- System Mgr.**

### User Mgr.

- Log Mgr.
- Startup-config
- System Software
- Factory Settings
- Reboot
- About

Figure 1 Navigation list of system management

## 9.1 User Management

### 9.1.1 User List

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

**User Management**

[New](#)

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	<a href="#">Edit</a>

☐ Select All/Select None   [Delete](#)

**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.

### 9.1.2 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"/>

[Apply](#)   [Reset](#)   [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。

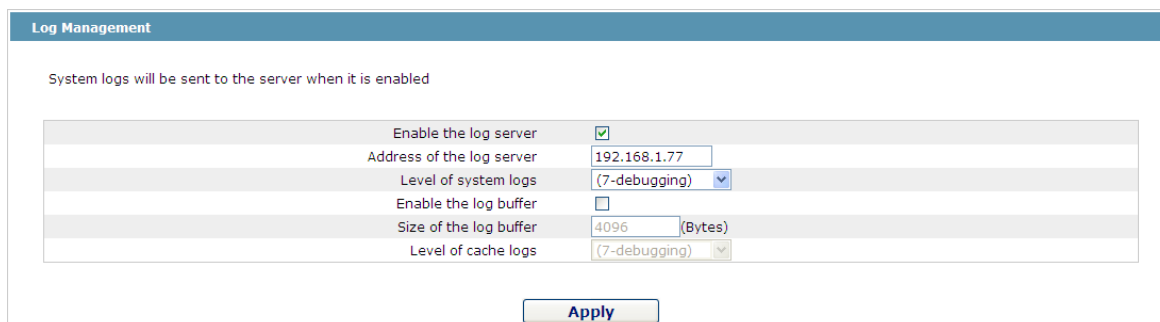
In the “Password” textbox enter a login password, and in the “Confirming password” textbox enter this login password again.

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.

## 9.2 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)

**Apply**

Figure 4 Log management

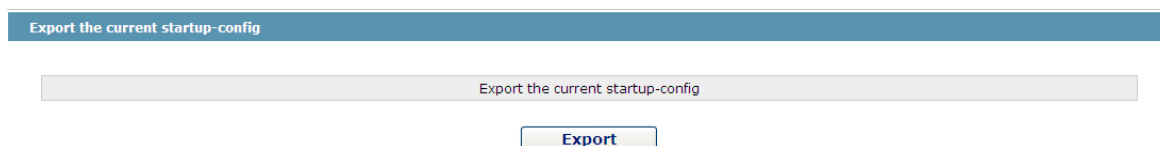
If “Enabling the log server” is selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the “Address of the system log server” textbox and select the log's grade in the “Grade of the system log information” dropdown box.

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.

## 9.3 Managing the Configuration Files

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

### 9.3.1 Exporting the Configuration Information



**Export the current startup-config**

Export the current startup-config

**Export**

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.

### 9.3.2 Importing the Configuration Information

Import startup-config file

Import startup-config file  浏览...

Reboot is required after importing startup-config!

Import

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.

## 9.4 Software Management

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

### 9.4.1 Backing up the IOS Software

Backup system

Current software version: switch.bin, 2.1.1A Build 13295, 2013-6-5 17:37:3 by SYS

File name on the server

Backup system

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.

Note:

The default name of the IOS file is "Switch. bin" and it is recommended to change it to a name that is easy to identify and find when backing up.

## 9.4.2 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 8 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”.

## 9.5 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 192.168.0.1/255.255.255.0, and the username and password are both “admin”.

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

## 9.6 Rebooting the Device

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

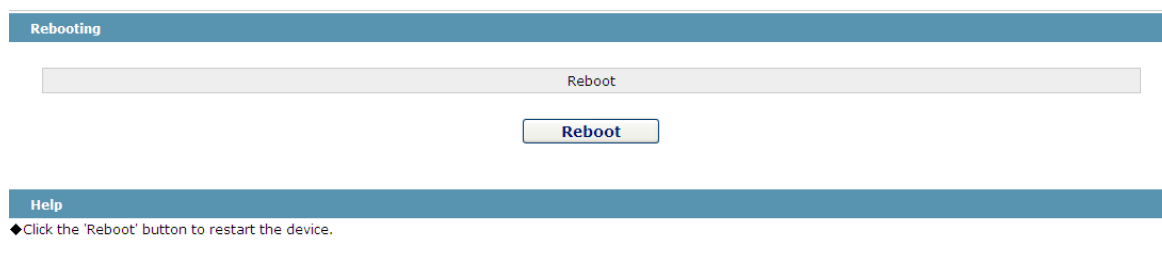


Figure 10 Rebooting the device

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.