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
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#".
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
4. Enter the ip http server command in global configuration mode and start the Web service.
5. Run username to set the username and password of the switch. For how to use this command, refer to the “Security Configuration” section in the user manual.

After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.
6. Enter `write` to store the current configuration to the configuration file.

```
switch_config# write
Saving current configuration...
OK!
```

```
switch_config# 1 1 00:07:52 /startup-config is wrote, TID:87113610
```

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](image)

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:
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**

Write the current settings to the configuration file of the device. It is equivalent to the execution of the `write` command.

The configuration that is made through Web will not be promptly written to the configuration file after validation. If you click “Save All”, the unsaved configuration will be lost after rebooting.

**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

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 needs to be configured, please click the group name and then the sub-item. For example, to browse the flux of the current port, you need 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

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](image)

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:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refresh the content shown in the current configuration area.</td>
</tr>
<tr>
<td>Apply</td>
<td>Apply the modified configuration to the device.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Reset</td>
<td>Means discarding the modification of the sheet. The content of the sheet will be reset.</td>
</tr>
</tbody>
</table>
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

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.

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”.

Figure 2  Hostname configuration
2.2 Time Management

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

![Time Setting](image)

**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

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/1</td>
<td></td>
</tr>
<tr>
<td>G0/2</td>
<td></td>
</tr>
<tr>
<td>G0/3</td>
<td></td>
</tr>
<tr>
<td>G0/4</td>
<td></td>
</tr>
</tbody>
</table>

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.

![Figure 3](image-url) 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.

![Figure 4](image-url) 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.
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.

![Figure 6: Port loopback detection](image)

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.

![Figure 7: IP binding configuration](image)

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.

![Figure 8: Setting the binding of the source IP address](image)
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.

![Figure 9  MAC binding configuration](image)

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.

![Figure 10  Setting the binding of the source MAC address](image)

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.

![Figure 11: Setting the static MAC filtration mode](image)

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 filtraion entries** in the navigation bar, the **Setting the static MAC filtration entries** page appears.

![Figure 12: Static MAC filtration entry list](image)

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.

![Figure 13: Setting static MAC filtration entries](image)
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.

![Figure 14: Setting the dynamic MAC filtration mode](image)

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

![Figure 15: Broadcast storm control](image)

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>60/38</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/39</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/40</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/41</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/42</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/43</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/44</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/45</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/46</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/47</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>60/48</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/1</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/2</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/3</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/4</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/5</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/6</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/7</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/8</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/39</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/40</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/41</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/42</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/43</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/44</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/45</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/46</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/47</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>G0/48</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/1</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/2</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/3</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/4</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/5</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/6</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/7</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
<tr>
<td>T1/8</td>
<td>Disable</td>
<td>(1-1638400) 100PPS</td>
</tr>
</tbody>
</table>

**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

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.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>Operate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default</td>
<td>Edit</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Default VLAN</th>
<th>Mode</th>
<th>Untag or not</th>
<th>Allow or not</th>
</tr>
</thead>
<tbody>
<tr>
<td>GO/1</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/2</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/3</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/4</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/5</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/6</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/7</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/8</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/9</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/10</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/11</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GO/12</td>
<td>1 &lt;1-4094&gt;</td>
<td>Access</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 configuration](image)

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 Configuration](image)

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](image)

- **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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Receive LLDP Packet</th>
<th>Send LLDP Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/1</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>G0/2</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>G0/3</td>
<td>Disable</td>
<td>Disable</td>
</tr>
<tr>
<td>G0/4</td>
<td>Disable</td>
<td>Disable</td>
</tr>
</tbody>
</table>

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.

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol Status</th>
<th>Priority(0~240)</th>
<th>Path Cost(0~200000000)</th>
<th>Edge Port Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/1</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>G0/2</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>G0/3</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>G0/4</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>G0/5</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>G0/6</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>G0/7</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
<tr>
<td>G0/8</td>
<td>Enable</td>
<td>128</td>
<td>0</td>
<td>Auto</td>
</tr>
</tbody>
</table>

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.

Figure 10 IGMP-snooping configuration
Web 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.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Status of the IGMP Snooping Vlan</th>
<th>Immediate-leave</th>
<th>Multicast Router’s Port</th>
<th>Operate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Running</td>
<td>Disable</td>
<td>SWITCH (querier)</td>
<td>Edit</td>
</tr>
</tbody>
</table>

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.

![Figure 12 Static routing port of IGMP VLAN](image)

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.
### 4.5.4 Multicast List

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

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Group</th>
<th>Current 0 Item/Total 0 Item</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
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.

### 4.7 Setting Static MAC

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

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.
4.8 DDM Configuration

If you click **L2 Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 18.

![Figure 18 DDM configuration](image)

4.9 Link Aggregation Configuration

If you click **Advanced Config -> Link aggregation Config** in the navigation bar, the **Link aggregation Config** page appears, as shown in figure 19.

![Figure 19 Port aggregation configuration](image)
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.

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.

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.

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

Figure 24 EAPS ring configuration

SW2&SW3 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 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.
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
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

![SW1 Configuration](image1)

**Figure 29** MEAPS Ring configuration

SW2 & SW3 Major Ring Configuration

![SW2 & SW3 Major Ring Configuration](image2)

**Figure 30** MEAPS Ring configuration

SW2 sub-ring Configuration
Figure 31  MEAPS Ring configuration

SW3 sub-ring Configuration

Figure 32  MEAPS Ring configuration

SW4 sub-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.

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.

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.
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.

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.
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.

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.

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.

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.

![DHCP Snooping binding list manual configuration](image)

4.14 MTU Configuration

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

![MTU configuration](image)

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.
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.

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.
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.

![Figure 47: POE configuration](image)

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.

![Figure 48: POE configuration](image)
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 configuration](image)

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](image)

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.
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

Device Status
Basic Config
Port Config
L2 Config
L3 Config

- VLAN Interfaces and IP Addresses
  - Static Route
  - OSPF Route Config
  - IGMP Proxy

Advanced Config
Network Mgr.
Diagnostic Tool
System Mgr.

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.

<table>
<thead>
<tr>
<th>No.</th>
<th>Page/Total</th>
<th>Name of the VLAN Interface</th>
<th>IP Attribute</th>
<th>IP Address</th>
<th>Operate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Manual Config</td>
<td>192.108.0.1/24;</td>
<td></td>
<td>Edit</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>IP Attribute</th>
<th>VLAN Interface Name**</th>
<th>IP Attribute**</th>
<th>Manual Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary IP Address</td>
<td>IP Address*</td>
<td>MASK address*</td>
<td></td>
</tr>
<tr>
<td>Secondary IP Address 1</td>
<td>IP Address**</td>
<td>MASK address**</td>
<td></td>
</tr>
<tr>
<td>Secondary IP Address 2</td>
<td>IP Address**</td>
<td>MASK address**</td>
<td></td>
</tr>
</tbody>
</table>

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

![Figure 3 VLAN interface configuration](image)

**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.

![Figure 4 Displaying the static route](image)

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](image)

**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](image)

**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](image)

**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](image)

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](image)

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

![Figure 10 Displaying the ospf route](image)

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.

![Enabling the IGMP Proxy](image)

**Help**

Before enabling or disabling IGMP Proxy, you must enable IGMP Snooping, which is configured if you click 'L2 Config -> IGMP Snooping'.

-47-
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.
Chapter 6  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.

<table>
<thead>
<tr>
<th>Port</th>
<th>COS value</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/1</td>
<td>0</td>
</tr>
<tr>
<td>G0/2</td>
<td>0</td>
</tr>
<tr>
<td>G0/3</td>
<td>0</td>
</tr>
<tr>
<td>G0/4</td>
<td>0</td>
</tr>
<tr>
<td>G0/5</td>
<td>0</td>
</tr>
<tr>
<td>G0/6</td>
<td>0</td>
</tr>
<tr>
<td>G0/7</td>
<td>0</td>
</tr>
<tr>
<td>G0/8</td>
<td>0</td>
</tr>
<tr>
<td>G0/9</td>
<td>0</td>
</tr>
<tr>
<td>G0/10</td>
<td>0</td>
</tr>
<tr>
<td>G0/11</td>
<td>0</td>
</tr>
</tbody>
</table>
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.

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

Figure 5 Setting the name of MAC access control list

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.

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.

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.
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.

![IP access control list configuration](image)

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

![Creating a name of the IP access control list](image)

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
Figure 11 Standard IP access control list

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

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

Extended IP access control list

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.
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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Egress ACL</th>
<th>Ingress ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0/1</td>
<td>mrtg</td>
<td></td>
</tr>
<tr>
<td>0/0/2</td>
<td>mrtg</td>
<td></td>
</tr>
<tr>
<td>0/0/3</td>
<td>mrtg</td>
<td></td>
</tr>
<tr>
<td>0/0/4</td>
<td>mrtg</td>
<td></td>
</tr>
<tr>
<td>0/0/5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/0/6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/0/7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/0/8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 7  Network Management Configuration

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

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.
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

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.

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.
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 the same as 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.

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 the same as 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.

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.
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

8.1 Ping

8.1.1 Ping

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

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

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.
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.

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.
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

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

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

On this page the currently running software version is displayed. If you want to backup IOS, please click “Backping 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](image)

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

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

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](image)

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 -&gt; Reboot Device, the Rebooting page appears.

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.