

# Web Configuration

# Table of Contents

Chapter 1 Configuration Preparation.....	4
1. 1 Accessing the Switch Through HTTP.....	4
1.1.1 Initially Accessing the Switch.....	4
1.1.2 Upgrading to the Web-Supported Version.....	4
1. 2 Accessing a Switch Through Secure Links.....	5
1.3 Introduction of Web Interface.....	5
1.3.1 Top Control Bar.....	6
1.3.2 Navigation Bar.....	7
1.3.3 Configuration Area.....	7
1.3.4 Bottom Control Bar.....	8
1.3.5 Configuration Area.....	8
Chapter 2 Basic Configuration.....	9
2.1 IP Address Configuration.....	9
2.2 Hostname Configuration.....	10
2. 3 Time Management.....	10
Chapter 3 Configuration of the Physical Interface.....	12
3. 1 Configuring Port Description.....	12
3. 2 Configuring the Attributes of the Port.....	12
3.3 Rate control.....	13
3.4 Storm control.....	13
3.4.1 Broadcast Storm Control.....	14
3.4.2 Multicast Storm Control.....	14
3. 4. 3 Unknown Unicast Storm Control.....	14
3.5 Port security.....	15
3.5.1 IP Binding Configuration.....	15
3.5.2 MAC Binding Configuration.....	15
3. 5. 3 Setting the Static MAC Filtration Mode.....	16
3. 5. 4 Static MAC Filtration Entries.....	16
3. 5. 5 Setting the Dynamic MAC Filtration Mode.....	17
3.6 Port Mirror.....	17
3. 7 Setting the Serial-Interface Server.....	18
3.8 Loopback Detection.....	19
3. 9 DDM Configuration.....	19
Chapter 4 Layer-2 Configuration.....	21
4.1 VLAN Settings.....	21
4.1.1 VLAN List.....	21
4.1.2 VLAN Settings.....	22
4.2 PDP Configuration.....	23
4.2.1 Configuring the Global Attributes of PDP.....	23
4.2.2 Configuring the Attributes of the PDP Port.....	23
4.3 LLDP Configuration.....	23

---

4.3.1 Configuring the Global Attributes of LLDP.....	23
4.3.2 Configuring the Attributes of the LLDP Port.....	24
4.4 Link Aggregation Configuration.....	24
4.5 STP Configuration.....	25
4.5.1 STP Status Information.....	25
4.5.2 Configuring the Attributes of the STP Port.....	26
4.6 IGMP-Snooping Configuration.....	26
4.6.1 IGMP-Snooping Configuration.....	26
4.6.2 IGMP-Snooping VLAN List.....	27
4.6.3 Static Multicast Address.....	28
4.6.4 Multicast List.....	28
4.7 Setting Static ARP.....	29
4.8 Ring Protection Configuration.....	29
4.8.1 EAPS Ring List.....	29
4.8.2 EAPS Ring Configuration.....	30
4.9 EVC Configuration.....	31
4.9.1 Global QinQ Configuration.....	31
4.9.2 Configuring the QinQ Port.....	31
Chapter 5 Layer-3 Configuration.....	32
5.1 Configuring the VLAN Interface.....	32
5.2 Setting the Static Route.....	33
5.3 IGMP Agent.....	34
5.3.1 Enabling the IGMP Agent.....	34
5.3.2 Setting the IGMP Agent.....	34
Chapter 6 Advanced Configuration.....	35
6.1 QoS Configuration.....	35
6.1.1 Configuring QoS Port.....	35
6.1.2 Global QoS Configuration.....	36
6.2 MAC Access Control List.....	36
6.2.1 Setting the Name of the MAC Access Control List.....	36
6.2.2 Setting the Rules of the MAC Access Control List.....	37
6.2.3 Applying the MAC Access Control List.....	37
6.3 IP Access Control List.....	38
6.3.1 Setting the Name of the IP Access Control List.....	38
6.3.2 Setting the Rules of the IP Access Control List.....	38
6.3.3 Applying the IP Access Control List.....	40
Chapter 7 Network Management Configuration.....	41
7.1 SNMP Configuration.....	41
7.1.1 SNMP Community Management.....	41
7.1.2 SNMP Host Management.....	42
7.2 RMON.....	43
7.2.1 RMON Statistic Information Configuration.....	43
7.2.2 RMON History Information Configuration.....	43

---

7.2.3 RMON Alarm Information Configuration.....	44
7.2.4 RMON Event Configuration.....	44
Chapter 8 Diagnosis Tools.....	46
8.1 Ping.....	46
8.1.1 Ping.....	46
Chapter 9 System Management.....	48
9.1 User Management.....	48
9.1.1 User List.....	48
9.1.2 Establishing a New User.....	49
9.2 Log Management.....	49
9.3 Managing the Configuration Files.....	50
9.3.1 Exporting the Configuration Information.....	50
9.3.2 Importing the Configuration Information.....	50
9.4 Software Management.....	51
9.4.1 Backing up the IOS Software.....	51
9.4.2 Upgrading the IOS Software.....	51
9.5 Resuming Initial Configuration.....	52
9.6 Rebooting the Device.....	52

# 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 Initially Accessing the Switch

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

1. Modify the IP address of the network adapter and subnet mask of your computer to **192.168.0.2** and **255.255.255.0** respectively.
2. Open the Web browser and enter **192.168.0.1** in the address bar. It is noted that **192.168.0.1** is the default management address of the switch.
3. If the Internet Explorer browser is used, you can see the dialog box in figure 1. Both the original username and the password are “admin”, which is capital sensitive.

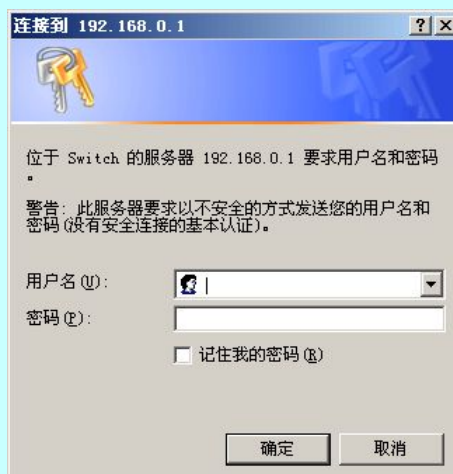


Figure 1: ID checkup of WEB login

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

### 1.1.2 Upgrading to the Web-Supported Version

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

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
  2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to “Switch\_config#”.
  3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
  4. Enter the **ip http server** command in global configuration mode and start the Web service.
  5. Run **username** to set the username and password of the switch. For how to use this command, refer to the “Security Configuration” section in the user manual.
- After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.
6. Enter **write** to store the current configuration to the configuration file.

## 1.2 Accessing a Switch Through Secure Links

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

To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to “Switch\_config#”.
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
4. Enter the **ip http server** command in global configuration mode and start the Web service.
5. Run **username** to set the username and password of the switch. For how to use this command, refer to the “Security Configuration” section in the user manual.
6. Run **ip http ssl-access enable** to enable the secure link access of the switch.
7. Run **no ip http http-access enable** to forbid to access the switch through insecure links.
8. Enter **write** to store the current configuration to the configuration file.
9. Open the WEB browser on the PC that the switch connects, enter **https://192.168.0.1** on the address bar (**192.168.0.1** stands for the management IP address of the switch) and then press the **Enter** key. Then the switch can be accessed through the secure links.

## 1.3 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.

### 1.3.1 Top Control Bar

全部保存 | English | 中文 | 退出 | 关于

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.
English	The interface will turn into the English version.
Chinese	The interface will turn into the Chinese version.
Logout	Exit from the current login state.  After you click "logout", you have to enter the username and the password again if you want to continue the Web function.

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

### 1.3.2 Navigation Bar



Figure 4 Navigation bar

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

**Note:**

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

### 1.3.3 Configuration Area

系统信息	
设备型号	SWITCH
BIOS版本	0.4.1
设备版本	2.1.0C
设备序列号	S39010148
系统MAC地址	FCFA.F72F.8553
系统当前时间	2012-6-7 15:21:53
系统运行时间	0天0时2分25秒
CPU使用率	3%
内存使用率	46%

刷新

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.



### 1.3.4 Bottom Control Bar



Figure 6: Bottom control bar

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

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

---

**Note:**

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

---

### 1.3.5 Configuration Area

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

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

## Chapter 2 Basic Configuration



Figure 1 A list of basic configuration

### 2.1 IP Address Configuration

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

**IP地址配置**

配置Vlan1接口的IP地址。

MAC 地址	00:e0:0f:a5:b3:37
IP地址*	<input type="text" value="90.0.0.2"/>
子网掩码*	<input type="text" value="255.255.0.0"/>
默认网关	<input type="text" value="90.0.0.255"/>

在线帮助

◆配置Vlan1接口的IP地址，用来实现对交换机的访问。

Figure 2 IP address configuration

This page is used to set the IP address of Interface Vlan 1, the management interface of the device. In initial conditions, the MAC address of the device, the IP address, mask and gateway

of the interface will appear on this page. After the content is modified on this page, click “Apply” to finish the modification of the address; click “Reset” to restore the content of the page to the initial unchanged content.

The items with the asterisk symbol “\*” are ones where you must enter values. “Default gateway” is an optional item, which can be null.

Note:

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

## 2.2 Hostname Configuration

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

设备名配置

配置交换机的名字。

设备名\* Switch

应用 重填

在线帮助

◆配置交换机的名字。

Figure 3 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”.

## 2.3 Time Management

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

时间设置	
系统时间	2010-08-16 15:00:55 <input type="button" value="刷新"/>
时区选择	(GMT)格林威治,都柏林,伦敦,里斯本
<input checked="" type="radio"/> 手工设置时间	
设置时间	2010年08月16日15时00分55秒
<input type="radio"/> 网络时间同步	
SNTP服务器一	
SNTP服务器二	
SNTP服务器三	
同步时间间隔	1 分钟
<input type="button" value="应用"/>	

Figure 4 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.

 The 'Port description configuration' page features a table with two columns: '端口' (Port) and '端口描述' (Port Description). The table contains five rows for ports G0/1, G0/2, G0/3, G0/4, and P1. The G0/1 row has the description 'This is a network management port.' Below the table are two buttons: '应用' (Apply) and '重填' (Reset).
 

端口	端口描述
G0/1	This is a network management port.
G0/2	
G0/3	
G0/4	
P1	

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.

端口配置						
端口	状态	速度	双工	流控	介质	
G0/1	使能	自动	全双工	关闭	自动	
G0/2	使能	自动	全双工	关闭	自动	
G0/3	使能	自动	全双工	关闭	自动	
G0/4	使能	自动	全双工	关闭	自动	
G0/5	使能	自动	全双工	关闭	自动	
G0/6	使能	自动	全双工	关闭	自动	
G0/7	使能	自动	全双工	关闭	自动	

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.

端口限速						
端口	接收状态	接收速率	发送状态	发送速率	单位	
G0/1	未启用	(1-16384)	未启用	(1-16384)	64kbps	
G0/2	未启用	(1-16384)	未启用	(1-16384)	64kbps	
G0/3	未启用	(1-16384)	未启用	(1-16384)	64kbps	
G0/4	未启用	(1-16384)	未启用	(1-16384)	64kbps	
G0/5	未启用	(1-16384)	未启用	(1-16384)	64kbps	
G0/6	未启用	(1-16384)	未启用	(1-16384)	64kbps	
G0/7	未启用	(1-16384)	未启用	(1-16384)	64kbps	

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 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.

### 3.4.1 Broadcast Storm Control

广播风暴控制配置			
端口	状态	阈值	
G0/1	未启用	<input type="text"/>	(1-16384)64Kbps
G0/2	未启用	<input type="text"/>	(1-16384)64Kbps
G0/3	未启用	<input type="text"/>	(1-16384)64Kbps
G0/4	未启用	<input type="text"/>	(1-16384)64Kbps

Figure 5 Broadcast storm control

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

### 3.4.2 Multicast Storm Control

多播风暴控制配置			
端口	状态	阈值	
G0/1	未启用	<input type="text"/>	(1-16384)64Kbps
G0/2	未启用	<input type="text"/>	(1-16384)64Kbps
G0/3	未启用	<input type="text"/>	(1-16384)64Kbps
G0/4	未启用	<input type="text"/>	(1-16384)64Kbps

Figure 6 Setting the broadcast storm control

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

### 3.4.3 Unknown Unicast Storm Control

未知单播风暴控制配置			
端口	状态	阈值	
G0/1	未启用	<input type="text"/>	(1-16384)64Kbps
G0/2	未启用	<input type="text"/>	(1-16384)64Kbps
G0/3	未启用	<input type="text"/>	(1-16384)64Kbps
G0/4	未启用	<input type="text"/>	(1-16384)64Kbps

Figure 7 Unknown unicast storm control

通过“状态”一系列的下拉框控制端口是否启用未知单播风暴控制。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.

## 3.5 Port security

### 3.5.1 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 8.

IP端口绑定配置		
第1页/共1页	第一页 上一页 下一页 最后一页	前往 第 <input type="text"/> 页 搜索: <input type="text"/>
		本页28条/共28条
端口名称		详细
F0/1		<a href="#">详细</a>
F0/2		<a href="#">详细</a>
F0/3		<a href="#">详细</a>
F0/4		<a href="#">详细</a>
F0/5		<a href="#">详细</a>
F0/6		<a href="#">详细</a>
F0/7		<a href="#">详细</a>
F0/8		<a href="#">详细</a>
F0/9		<a href="#">详细</a>
F0/10		<a href="#">详细</a>
F0/11		<a href="#">详细</a>
F0/12		<a href="#">详细</a>

Figure 8 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.

IP绑定规则信息			
<a href="#">新建</a>			
第1页/共1页	第一页 上一页 下一页 最后一页	前往 第 <input type="text"/> 页 搜索: <input type="text"/>	本页2条/共2条
序号	地址	操作	
<input type="checkbox"/> 0	192.168.0.3	<a href="#">修改</a>	
<input type="checkbox"/> 1	192.168.0.2	<a href="#">修改</a>	
<input type="checkbox"/> 全选/全不选		<a href="#">删除</a>	<a href="#">返回</a>
<a href="#">在线帮助</a>			

Figure 9 Setting the binding of the source IP address

### 3.5.2 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 10.



MAC端口绑定配置	
第1页/共1页 第一页 上一页 下一页 最后一页 前往 第 <input type="text"/> 页 搜索: <input type="text"/> 本页28条/共28条	
端口名称	详细
F0/1	详细
F0/2	详细
F0/3	详细
F0/4	详细
F0/5	详细
F0/6	详细
F0/7	详细
F0/8	详细
F0/9	详细
F0/10	详细
F0/11	详细
F0/12	详细

Figure 10 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.

MAC绑定规则信息		
<input type="button" value="新建"/>		
第1页/共1页 第一页 上一页 下一页 最后一页 前往 第 <input type="text"/> 页 搜索: <input type="text"/> 本页1条/共1条		
序号	地址	操作
<input type="checkbox"/> 0	2233.4455.6677	修改
<input type="checkbox"/> 全选/全不选		<input type="button" value="删除"/> <input type="button" value="返回"/>

Figure 11 Setting the binding of the source MAC address

### 3.5.3 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 12.

静态MAC过滤模式配置		
端口名称	端口类型	静态MAC过滤模式
G0/1	Access	未使能 <input type="button" value="v"/>
G0/2	Access	未使能 <input type="button" value="v"/>
G0/3	Access	未使能 <input type="button" value="v"/>
G0/4	Access	未使能 <input type="button" value="v"/>
<input type="button" value="应用"/>		<input type="button" value="重填"/>

Figure 12: Setting the static MAC filtration mode

On this page you can set the static MAC filtration mode. By default, the static MAC filtration mode is disabled. The static MAC filtration mode cannot be set on a port which is in Trunk mode.

### 3.5.4 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.

静态MAC过滤配置	
第1页/共1页 第一页 上一页 下一页 最后一页 前往 第 <input type="text"/> 页 搜索: <input type="text"/> 本页4条/共4条	
端口名称	详细
G0/1	<a href="#">详细</a>
G0/2	<a href="#">详细</a>
G0/3	<a href="#">详细</a>
G0/4	<a href="#">详细</a>

Figure 13: 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.

静态MAC过滤规则信息			
<a href="#">新建</a>			
第1页/共1页 第一页 上一页 下一页 最后一页 前往 第 <input type="text"/> 页 搜索: <input type="text"/> 本页1条/共1条			
序号	过滤模式	MAC地址	操作
<input type="checkbox"/> 0	未使能	0001.0002.0003	<a href="#">修改</a>
<input type="checkbox"/> 全选/全不选			
			<a href="#">删除</a> <a href="#">返回</a>

Figure 14: Setting static MAC filtration entries

### 3.5.5 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 15.

动态MAC过滤模式配置			
端口名称	动态MAC过滤模式	最大地址数	
G0/1	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/2	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/3	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/4	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/5	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/6	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/7	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/8	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/9	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)
G0/10	未使能 <input type="button" value="v"/>	<input type="text"/>	(1-4095)

Figure 15: Setting the dynamic MAC filtration mode

On this page you can set the dynamic MAC filtration mode and the allowed maximum number of addresses. The dynamic MAC filtration mode is disabled by default and the maximum number of addresses is 1.

## 3.6 Port Mirror

If you click **Physical port Config -> Port Mirror** in the navigation bar, the **Port Mirror Config** page appears, as shown in figure 16.

被镜像端口	端口镜像模式
<input type="checkbox"/> F0/1	RX
<input checked="" type="checkbox"/> F0/2	RX
<input type="checkbox"/> F0/3	RX
<input checked="" type="checkbox"/> F0/4	TX
<input checked="" type="checkbox"/> F0/5	RX & TX
<input type="checkbox"/> F0/6	RX
<input type="checkbox"/> F0/7	RX

Figure 16 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.

### 3.7 Setting the Serial-Interface Server

If you click **Physical port Config -> Serial-interface server Config**, the **Setting the port of serial-interface server** page appears, as shown in figure 17:

串口服务器端口配置												
第1页/共1页    第一页   上一页   下一页   最后一页   前往 第 <input type="text"/> 页   搜索: <input type="text"/>											本页4条/共4条	
Uart ID	串口会话模式	串口工作模式	Socket端口号	远端服务器IP地址	波特率	数据位	停止位	校验方式	流控方式	超时间隔	触发读取字符数	操作
1	TCP客户端模式	RS232 全双工	5000	10.112.3.8	9600	8	1	关闭校验	关闭流控	100	32	<a href="#">修改</a>
2	NONE	RS485 半双工			9600	8	1	关闭校验	关闭流控	100	32	<a href="#">修改</a>
3	NONE	RS485 半双工			9600	8	1	关闭校验	关闭流控	100	32	<a href="#">修改</a>
4	NONE	RS485 半双工			9600	8	1	关闭校验	关闭流控	100	32	<a href="#">修改</a>

Figure 17: Setting the port of serial interface server

Click **Edit** to modify the attributes of the port of the serial-interface server.



Uart ID	2
串口会话模式	NONE
串口工作模式	RS485 半双工
Socket端口号	
远端服务器IP地址	
波特率	9600
数据位	8
停止位	1
校验方式	关闭校验
流控方式	关闭流控
超时时间	100
触发读取字符数	32

Figure 18: Setting the attributes of the port of serial interface server

Note:  
Only IES212S has the serial-interface server configuration page.

### 3.8 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 19.



端口	状态	环路检测周期
G0/1	不使能	(0-32767)秒
G0/2	不使能	(0-32767)秒
G0/3	不使能	(0-32767)秒
G0/4	不使能	(0-32767)秒
G0/5	不使能	(0-32767)秒
G0/6	不使能	(0-32767)秒
G0/7	不使能	(0-32767)秒
G0/8	不使能	(0-32767)秒
G0/9	不使能	(0-32767)秒
G0/10	不使能	(0-32767)秒

Figure 19: Port loopback detection

Click **Edit** to modify relevant values of port loopback detection.

### 3.9 DDM Configuration

If you click **Physical port Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 20.



Figure 20: DDM configuration

## Chapter 4 Layer-2 Configuration



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 配置			
<a href="#">新建</a>			
第1页/共1页 第一页 上一页 下一页 最后页 前往 第 <input type="text"/> 页 搜索: <input type="text"/>			本页3条/共3条
<input type="checkbox"/>	VLAN ID	VLAN 名称	操作
<input type="checkbox"/>	1	Default	<a href="#">修改</a>
<input type="checkbox"/>	2	VLAN0002	<a href="#">修改</a>
<input type="checkbox"/>	25	VLAN0025	<a href="#">修改</a>
<input type="checkbox"/> 全选/全不选			<a href="#">删除</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.

修改VLAN配置					
VLAN ID		2			
VLAN 名称		VLAN0002			
端口	默认VLAN	模式	是否去标签	是否允许	
FD/1	1 <1-4094>	Trunk	否	是	
FD/2	1 <1-4094>	Access	否	是	
FD/3	1 <1-4094>	Access	否	是	
FD/4	1 <1-4094>	Access	否	是	
FD/5	1 <1-4094>	Access	否	是	
FD/6	1 <1-4094>	Access	否	是	
FD/7	1 <1-4094>	Access	否	是	

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 PDP Configuration

### 4.2.1 Configuring the Global Attributes of PDP

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

Figure 4 Configuring the global attributes of PDP

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

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

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

### 4.2.2 Configuring the Attributes of the PDP Port

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

端口	状态
F0/1	启用PDP协议
F0/2	启用PDP协议
F0/3	未启用PDP协议
F0/4	启用PDP协议
F0/5	启用PDP协议
F0/6	启用PDP协议
F0/7	启用PDP协议
F0/8	启用PDP协议
F0/9	启用PDP协议

Figure 5 PDP port configuration

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

## 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.





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.



端口	接收LLDP报文	发送LLDP报文
F0/1	允许	允许
F0/2	允许	允许
F0/3	允许	允许
F0/4	允许	允许
F0/5	允许	允许

Figure 7 Configuring the LLDP port

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

## 4.4 Link Aggregation Configuration

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



聚合组	模式	配置成员端口	有效成员端口	速率	状态	操作
P1	Static	F0/2,F0/3	F0/2,F0/3	100	down	修改

◆注意:所有聚合端口的物理特性必须相同,例如速率、双工、vlan等

Figure 8 Port aggregation configuration

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



Figure 9: Setting the member port of the aggregation group

An aggregation group is selectable when it is created but is not selectable when it is modified.

When a member port exists on the aggregation group, you can choose the aggregation mode to be **static**, **LACP active** or **LACP passive**.

You can click “>>” and “<<” to delete and add a member port in the aggregation group.

## 4.5 STP Configuration

### 4.5.1 STP Status Information

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

根桥STP配置	
Spanning Tree Priority	0
MAC Address	00E0.0FCC.F4A0
Hello Time	2
Max Age	20
Forward Delay	15

本地STP配置	
协议类型	RSTP
Spanning Tree Priority	32768
MAC Address	FCFA.F72F.8553
Hello Time	2 (1-10)s
Max Age	20 (6-40)s
Forward Delay	15 (4-30)s
BPDU Terminal	不使能

应用      重填

STP端口状态信息					
第1页/共1页 第一页 上一页 下一页 最后一页 前往 第 页 搜索: <input type="text"/>					
本页1条/共1条					
端口	角色	状态	端口开销	优先级_端口号	类型
G0/23	Root	FWD	20000	128.23	P2p

Figure 10 Configuring the global attributes of STP

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

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

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

Note:

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

## 4.5.2 Configuring the Attributes of the STP Port

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

端口信息配置				
端口	协议状态	优先级(0~255)	路径成本(0~200000000)	边缘端口属性
F0/1	使能	128	0	自动检测
F0/4	使能	128	0	自动检测
F0/5	使能	128	0	自动检测
F0/6	使能	128	0	自动检测
F0/7	使能	128	0	自动检测
F0/8	使能	128	0	自动检测
F0/9	使能	128	0	自动检测
F0/10	使能	128	0	自动检测
F0/11	使能	128	0	自动检测
F0/12	使能	128	0	自动检测
F0/13	使能	128	0	自动检测
F0/14	使能	128	0	自动检测
F0/15	使能	128	0	自动检测
F0/16	使能	128	0	自动检测
F0/17	使能	128	0	自动检测
F0/18	使能	128	0	自动检测
F0/19	使能	128	0	自动检测
F0/20	使能	128	0	自动检测
F0/21	使能	128	0	自动检测
F0/22	使能	128	0	自动检测

Figure 11 Configuring the attributes of RSTP

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

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

## 4.6 IGMP-Snooping Configuration

### 4.6.1 IGMP-Snooping Configuration

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

Figure 12 IGMP-snooping configuration

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

#### 4.6.2 IGMP-Snooping VLAN List

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

VLAN ID	IGMP-snooping Vlan状态	Immediate-leave	组播路由器所在端口	操作
<input type="checkbox"/> 1	运行	未使能	G0/1(static);	修改

Figure 13: IGMP-snooping VLAN list

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

Figure 14: Static routing port of IGMP VLAN

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

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

### 4.6.3 Static Multicast Address

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

Figure 15 Multicast List

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

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

### 4.6.4 Multicast List

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

VLAN	群组	类型	端口
1	225.0.0.1	IGMP	F0/23
1	225.0.0.2	IGMP	F0/23
1	225.0.0.4	IGMP	F0/23
25	239.255.255.250	IGMP	G0/1
25	224.1.1.1	IGMP	G0/1
25	224.0.5.37	IGMP	G0/1

Figure 16 Multicast List

On this page the multicast 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.

## 4.7 Setting Static ARP

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

The screenshot shows the 'ARP协议基本配置' (Basic ARP Configuration) page. It features a '新建' (New) button at the top left. Below it is a navigation bar with '第1页/共1页', '第一页', '上一页', '下一页', '最后一页', '前往', '第' (with a dropdown), '页', and a search box. The main area contains a table with the following data:

	IP地址	MAC地址	Alias	操作
<input type="checkbox"/>	10.1.1.1	22:22:22:22:22	True	修改

Below the table is a '全选/全不选' checkbox and a '删除' (Delete) button. At the bottom, there is an '在线帮助' (Online Help) section with a note: '◆Alias: 回答对指定IP地址的ARP请求'.

Figure 17 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.

The screenshot shows the 'ARP协议基本配置' (Basic ARP Configuration) page with the '配置IP地址对应的MAC地址' (Configure MAC address corresponding to IP address) form. The form has three input fields: 'IP地址' (IP address), 'MAC地址\*' (MAC address), and 'Alias' (checkbox). Below the form are '应用' (Apply) and '重填' (Reset) buttons. At the bottom, there is an '在线帮助' (Online Help) section with a note: '◆Alias: 回答对指定IP地址的ARP请求'.

Figure 18 Setting static ARP

## 4.8 Ring Protection Configuration

### 4.8.1 EAPS Ring List

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

The screenshot shows the 'EAPS环网配置' (EAPS Ring Configuration) page. It features a '新建' (New) button at the top left. Below it is a navigation bar with '第1页/共1页', '第一页', '上一页', '下一页', '最后一页', '前往', '第' (with a dropdown), '页', and a search box. The main area contains a table with the following data:

环网ID	节点类型	环网描述	控制VLAN	状态	Hello	Fail	Preforward	主端口/转发/链路状态	次端口/转发/链路状态	操作
<input type="checkbox"/>	0	Master-node	2	RingFail	1	3	3	None/Blocking/Linkdown	None/Blocking/Linkdown	修改

Below the table is a '全选/全不选' checkbox, a '删除' (Delete) button, and a '刷新' (Refresh) button. At the bottom, there is an '在线帮助' (Online Help) section with a note: '◆Alias: 回答对指定IP地址的ARP请求'.

Figure 19 EAPS Ring List

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

Click “New” to create a new EAPS ring.

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

Note:

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

## 4.8.2 EAPS Ring Configuration

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



Figure 20 EAPS ring configuration

Note:

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

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

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

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

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

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

## 4.9 EVC Configuration

### 4.9.1 Global QinQ Configuration

If you click **Layer-2 Config -> EVC Config**, the **Global QinQ configuration** page appears.

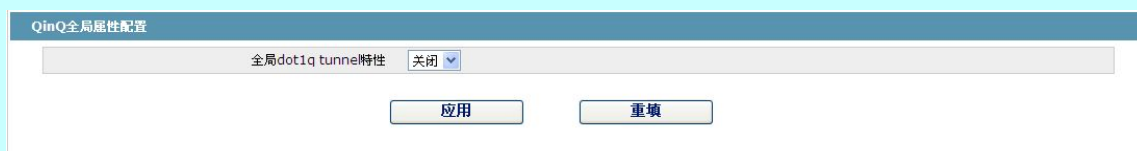


Figure 21: Global EVC configuration

In global EVC configuration mode, you can enable or disable the global dot1q.

### 4.9.2 Configuring the QinQ Port

If you click **Layer-2 Config -> EVC Config -> QinQ port Config**, the **Configuring the QinQ port** page appears.



端口	端口类型	端口PVID	CVLAN翻译表	允许的SVLAN	操作
G0/1	Access	1		1	<a href="#">修改</a>
G0/2	Access	1		1	<a href="#">修改</a>
G0/3	Access	1		1	<a href="#">修改</a>
G0/4	Access	1		1	<a href="#">修改</a>
G0/5	Access	1		1	<a href="#">修改</a>
G0/6	Access	1		1	<a href="#">修改</a>
G0/7	Access	1		1	<a href="#">修改</a>
G0/8	Access	1		1	<a href="#">修改</a>

Figure 22: Configuring the PTP port

The QinQ related configuration of all ports can be displayed and modified on the **Configuring the QinQ port** page.



## 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.

VLAN接口配置				
<input type="button" value="新建"/>				
第1页/共1页 第一页 上一页 下一页 最后一页 前往 第 <input type="text"/> 页 搜索: <input type="text"/>			本页3条/共3条	
<input type="checkbox"/>	VLAN接口名	IP属性	IP地址	操作
<input type="checkbox"/>	1	手动配置	90.0.0.2/16;	<a href="#">修改</a>
<input type="checkbox"/>	4	手动配置	2.2.2.2/8;3.3.3.3/16;4.4.4.4/16;	<a href="#">修改</a>
<input type="checkbox"/>	888	手动配置		<a href="#">修改</a>
<input type="checkbox"/> 全选/全不选				<input type="button" value="删除"/>

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.

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.

Figure 4 Displaying the static route

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

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

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



Figure 5: Setting the static route

## 5.3 IGMP Agent

### 5.3.1 Enabling the IGMP Agent

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



Figure 6: Enabling the IGMP agent

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

### 5.3.2 Setting the IGMP Agent

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



Figure 7: Setting the IGMP agent

## Chapter 6 Advanced Configuration

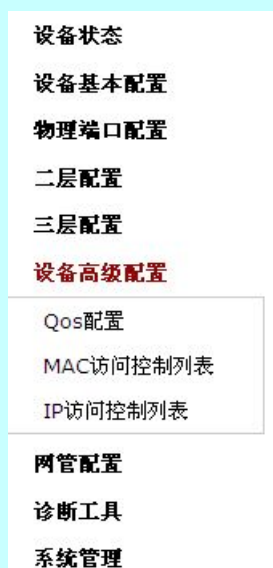


Figure 1 A list of advanced configuration

### 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.

端口优先级配置	
端口	COS值
F0/1	0
F0/2	0
F0/3	0
F0/4	0
F0/5	1
F0/6	3
F0/7	4
F0/8	5
F0/9	6

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 配置**

调度策略: SP

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

**COS值与队列对应表**

COS值	队列
0	队列1
1	队列2
2	队列3
3	队列4
4	队列5
5	队列6
6	队列7
7	队列8

应用      重填

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访问控制列表配置**

新建

第1页/共1页    第一页   上一页   下一页   最后一页   前往 第  页   搜索:     本页1条/共1条

	MAC访问控制列表名	操作
<input type="checkbox"/>	MyACL	修改

全选/全不选      删除

Figure 4: MAC access control list configuration

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



Figure 5: Setting the name of MAC access control list

### 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.



权限	源MAC地址	源MAC掩码	目的MAC地址	目的MAC掩码	操作
<input type="checkbox"/> permit	host	0001.0002.0003	any		<a href="#">修改</a>

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.



端口	出口访问控制列表	入口访问控制列表
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"/>

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.

Figure 9: IP access control list configuration

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

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

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

### 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.

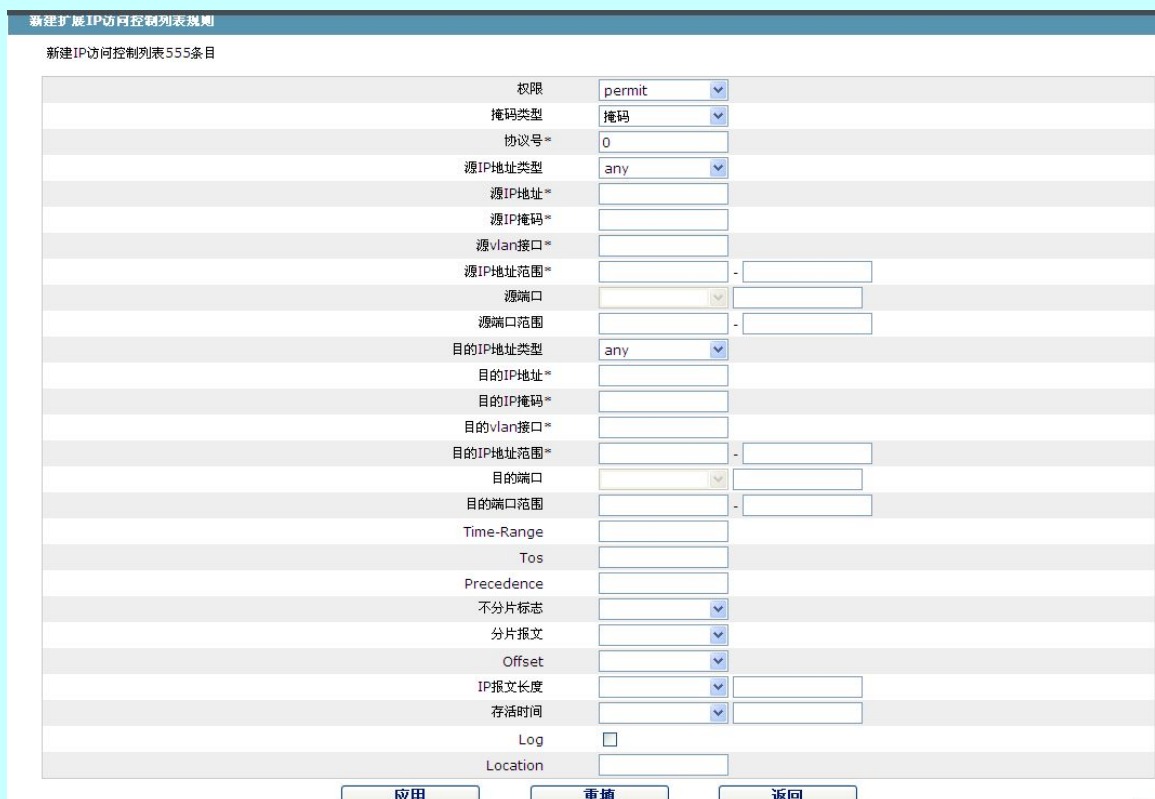


Figure 14: Setting the Rules of the extended IP access control list



### 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.

IP访问控制列表应用		
端口	出口访问控制列表	入口访问控制列表
F0/1	<input type="text" value="MyStandardIPACL"/>	<input type="text"/>
F0/2	<input type="text"/>	<input type="text" value="MyExtendedIPACL"/>
F0/3	<input type="text"/>	<input type="text"/>
F0/4	<input type="text"/>	<input type="text"/>
F0/5	<input type="text"/>	<input type="text"/>
F0/6	<input type="text"/>	<input type="text"/>
F0/7	<input type="text"/>	<input type="text"/>
F0/8	<input type="text"/>	<input type="text"/>
F0/9	<input type="text"/>	<input type="text"/>
F0/10	<input type="text"/>	<input type="text"/>
F0/11	<input type="text"/>	<input type="text"/>
F0/12	<input type="text"/>	<input type="text"/>
F0/13	<input type="text"/>	<input type="text"/>
F0/14	<input type="text"/>	<input type="text"/>
F0/15	<input type="text"/>	<input type="text"/>

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



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' settings page. It features two tabs: 'SNMP Community 管理' (selected) and 'SNMP Host 管理'. The main content area is titled 'SNMP Community 管理' and contains a form with two input fields: 'SNMP共同体名' (SNMP Community Name) and 'SNMP共同体属性' (SNMP Community Attribute), which is currently set to '只读' (Read-Only). Below the form are two buttons: '应用' (Apply) and '返回' (Return).

Figure 4.2 SNMP community management settings

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

### 7.1.2 SNMP Host Management



The screenshot shows the 'SNMP Host Management' page. It has two tabs: 'SNMP Community 管理' and 'SNMP Host 管理' (selected). The main content area is titled 'SNMP Host 管理' and includes a '新建' (New) button. Below the title is a pagination bar showing '第1页/共1页' (Page 1 of 1) and a search box. A table lists the SNMP host configuration:

	SNMP Host IP	SNMP Community String	SNMP Message Type	SNMP Community Version	操作
<input type="checkbox"/>	10.16.1.1	public	Traps	v1	修改

Below the table is a checkbox for '全选/全不选' (Select all/Select none) and a '删除' (Delete) button.

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 Settings' page. It has two tabs: 'SNMP Community 管理' and 'SNMP Host 管理' (selected). The main content area is titled 'SNMP Host 管理' and contains a form with four input fields: 'SNMP Host IP', 'SNMP Community', 'SNMP Message Type' (set to 'Traps' with a note '\* v1版本不支持Informs类型'), and 'SNMP Community Version' (set to 'v1'). Below the form are two buttons: '应用' (Apply) and '返回' (Return).

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.



接口统计信息设置	
应用接口	FE1
索引	1
拥有者	demon

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.



接口历史信息设置	
应用接口	G0/1
索引	
采样数目	50
采样间隔	1800
拥有者	config

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.



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.



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是典型的网络工具，它能够辨别网络功能的某些状态。这些网络功能的状态是日常网络故障诊断的基础，Ping通过向指定主机发送一个数据包，看能否得到其应答来判断对方是否可到达。

PING测试-->	
目的地址*	<input style="width: 100%;" type="text"/>
源IP地址	<input style="width: 100%;" type="text"/> (可选项，可留空。)
PING包大小	<input style="width: 100%;" type="text"/> (60-1514) (可选项，可留空。)

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



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.



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.



用户管理	
用户名	<input type="text"/>
密码	<input type="password"/>
确认密码	<input type="password"/>
用户权限	系统管理员 ▼

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.



日志管理	
启用日志服务器，您可以将日志信息发送到指定的日志服务器上。	
启用日志服务器	<input checked="" type="checkbox"/>
系统日志服务器地址	<input type="text" value="192.168.0.33"/>
系统日志信息等级	(7-debugging) ▼
启用日志缓冲区	<input type="checkbox"/>
系统日志缓冲区大小	<input type="text" value="4096"/> (Bytes)
缓存日志信息等级	(7-debugging) ▼

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



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



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

Figure 7 Backing up IOS

On this page the currently running software version is displayed. If you want to backup IOS, please click “Backing up 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:

IOS 文件的缺省名称为 “Switch.bin”，建议在备份时将其修改为易于识别和查找的名称。

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