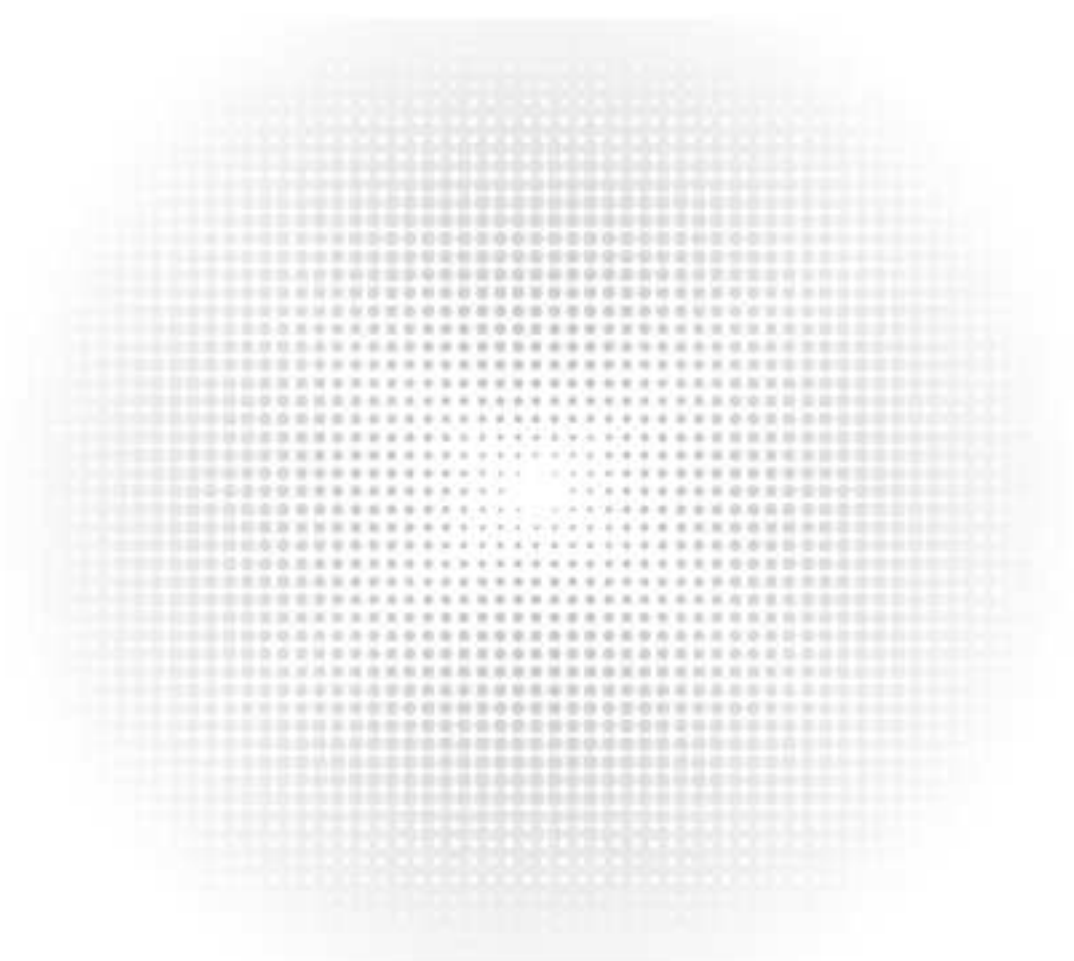


S3150-8T2F Switch Web-based Configuration Guide

Models: S3150-8T2F



Contents

Chapter 1 Configuration Preparation	1
1.1 HTTP Configuration	1
1.1.1 Choosing the Empty Language	1
1.1.2 Setting the HTTP Port	1
1.1.3 Enabling the HTTP service	1
1.1.4 Setting the HTTP Access Mode	1
1.1.5 Setting the maximum number of VLAN entries displayed on a web page	2
1.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page	2
1.2 HTTPS Configuration	2
1.2.1 Setting the HTTP Access Mode	2
1.2.2 Setting the HTTPS Port	2
Chapter 2 Accessing the Switch through HTTP	4
2.1 Accessing the Switch through HTTP	4
2.1.1 Initially Accessing the Switch	4
2.1.2 Upgrading to the Web-Supported Version	4
2.2 Accessing a Switch through Secure Links	5
2.3 Introduction of Web Interface	6
2.3.1 Top Control Bar	6
2.3.2 Navigation Bar	7
2.3.3 Configuration Area	7
2.3.4 Configuration Area	8
Chapter 3 Basic Configuration	9
3.1 Hostname Configuration	9
3.2 Time Management	9
Chapter 4 Configuration of the Physical Interface	11
4.1 Configuring Port Description	11

4.2 Configuring the Attributes of the Port.....	11
4.3 Rate Limit.....	12
4.4 Port Mirror.....	12
4.5 Loopback Detection.....	12
4.6 Port security.....	13
4.6.1 P Binding Configuration.....	13
4.6.2 MAC Binding Configuration.....	13
4.6.3 Setting the Static MAC Filtering Mode.....	13
4.6.4 Static MAC Filtering Entries.....	13
4.6.5 Setting the Dynamic MAC Filtering Mode.....	14
4.7 Storm Control.....	14
4.7.1 Broadcast storm control.....	14
4.7.2 Multicast Storm Control.....	14
4.7.3 Unknown Unicast Storm Control.....	15
4.8 Port Protect Group Configuration.....	15
4.8.1 Port Protect Group List.....	15
4.8.2 Port Protect Group Interface Configuration.....	15
Chapter 5 Layer 2 Configuration.....	16
5.1 VLAN Configuration.....	16
5.1.1 VLAN List.....	16
5.1.2 VLAN Configuration.....	17
5.2 GVRP Configuration.....	17
5.2.1 GVRP Global Attribute Configuration.....	17
5.2.2 GVRP Port Attribute Configuration.....	18
5.3 STP Configuration.....	18
5.3.1 STP Status Information.....	18
5.3.2 Configuring the Attributes of the STP Port.....	18
5.4 IGMP Snooping Configuration.....	19

5.4	GMP Snooping Configuration.....	19
5.4.1	GMP Snooping VLAN List.....	19
5.4.2	GMP Snooping VLAN List.....	19
5.4.3	Static Multicast Address.....	20
5.4.4	Port List.....	20
5.5	Setting Static ARP.....	21
5.6	Static MAC Configuration.....	21
5.7	IGMP Configuration.....	22
5.7.1	Configuring the Global Attributes of IGMP.....	22
5.7.2	Configuring the Attributes of the IGMP Port.....	23
5.8	DDM Configuration.....	23
5.9	Link Aggregation Configuration.....	23
5.9.1	Port Aggregation Configuration.....	23
5.9.2	Configuring Access Mode of Port Aggregation Group.....	24
5.10	FAPS Ring Protection Configuration.....	24
5.10.1	FAPS Ring List.....	24
5.10.2	FAPS Ring Configuration.....	25
5.11	MFAPS Configuration.....	25
5.11.1	MFAPS Ring Configuration.....	25
5.11.2	MFAPS Ring Configuration.....	26
5.12	Backup Link Protocol Configuration.....	27
5.12.1	Backup Link Protocol Global Configuration.....	27
5.12.2	Backup Link Protocol Interface Configuration.....	27
5.13	MTU Configuration.....	28
5.14	PDP Configuration.....	28
5.14.1	Configuring the Global Attributes of PDP.....	28
5.14.2	Configuring the Attributes of the PDP Port.....	29
Chapter 6	Layer 3 Configuration.....	30
6.1	Vlan interface configuration.....	30

6.2 Setting the Static Route.....	31
Chapter 7 Advanced Configuration.....	32
7.1 Qos Configuration.....	32
7.1.1 Configuring QoS Entry.....	32
7.1.2 Global Qos Configuration.....	32
7.2 IP Access Control List.....	33
7.2.1 Setting the Name of the IP Access Control List.....	33
7.2.2 Setting the Rules of the IP Access Control List.....	33
7.2.3 Applying the IP Access Control List.....	34
7.3 MAC Access Control List.....	34
7.3.1 Setting the Name of the IP Access Control List.....	34
7.3.2 Setting the Rules of the MAC Access Control List.....	35
7.3.3 Applying the MAC Access Control List.....	35
Chapter 8 Network Management Configuration.....	37
8.1 SNMP Configuration.....	37
8.1.1 SNMP Community Management.....	37
8.1.2 SNMP Host Management.....	38
8.2 RMON.....	38
8.2.1 RMON Statistic Information Configuration.....	38
8.2.2 RMON History Information Configuration.....	39
8.2.3 RMON Alarm Information Configuration.....	39
8.2.4 RMON Event Configuration.....	40
Chapter 9 Diagnosis Tools.....	41
9.1 Ping.....	41
9.1.1 Ping.....	41
Chapter 10 System Management.....	42
10.1 User Management.....	42

10.1.1 User List.....	43
10.1.2 Creating a New User.....	43
10.1.3 User Group Management.....	43
10.1.4 Password Rule Management.....	44
10.1.5 Authentication Rule Management.....	45
10.1.6 Authorization Rule Management.....	45
10.2 Log Management.....	46
10.3 Managing the Configuration Files.....	46
10.3.1 Exporting the Configuration Information.....	46
10.3.2 Importing the Configuration Information.....	47
10.4 Software Management.....	47
10.4.1 Upgrade System Software.....	47
10.4.2 Update System Software.....	48
10.4.3 Rebooting the Device.....	48

Chapter 1 Configuration Preparation

1.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and Ssh/PP but also through Web browser. The switches support the HTTP configuration, the abnormal configuration and configuration are shown.

1.1.1 Choosing the Prompt Language

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

Command	Purpose
<code>(n) ip http language {english}</code>	Set the prompt language of Web configuration to English.

1.1.2 Setting the HTTP Port

Generally, the HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support users to change the service port and after the service port is changed you have to use the IP address and the changed port to access switches. For example, if you set the IP address and the service port to 192.168.1.1 and 1234 respectively, the HTTP access address should be changed to `https://192.168.1.1:1234`. You'd better not use either common or reserved ports (such as ftp 20, telnet 23, dns 53, snmp 161) so that no collision should ever happen. Because the ports used by a lot of protocols are hard to remember, you'd better use port IDs following port 1024.

Command	Purpose
<code>snmp port {portNumber}</code>	Setting the HTTP Port

1.1.3 Enabling the HTTP Service

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

Command	Purpose
<code>snmp server</code>	Enabling the HTTP service

1.1.4 Setting the HTTP Access Mode

You can access a switch through two access modes: HTTP access and HTTPS access, and you can use the following command to set the access mode to HTTP.

Command	Purpose
<code>http http access mode</code>	Setting the HTTP Access Mode

1.1.5 Setting the maximum number of VLAN entries displayed on a web page

A switch supports at most 4094 VLANs and in most cases Web only displays parts of VLANs, that is, those VLANs users want to view. You can use the following command to set the maximum number of VLANs. The default maximum number of VLANs is 100.

Command	Purpose
<code>http maxvlan web {maxvlan}</code>	Set the maximum number of VLAN entries displayed on a web page.

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

A switch supports at most 100 multicast entries. You can run the following commands to set the maximum number of multicast entries and Web then shows those multicast entries. The default maximum number of multicast entries is 15.

Command	Purpose
<code>http web group group {group group}</code>	Set the maximum number of multicast entries displayed on a web page.

1.2 HTTPS Configuration

In order to increase the security of communications, switch support not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security improved HTTP channel and it is added to the SSL layer under HTTP.

1.2.1 Setting the HTTP Access Mode

You can run the following command to set the access mode to HTTPS.

Command	Purpose
<code>http https access mode</code>	Setting the HTTPS access mode

1.2.2 Setting the HTTPS Port

As the HTTP port, HTTPS has its default service port, port 443, and you also can run the following command to change its service port. It is recommended to use those ports following port 1024 so as to avoid collision with other protocols' ports following port 1024 so as to avoid collision with other protocols' ports.

Command	Purpose
<code>http secure port /portNumber</code>	Set the HTTPS port.

Chapter 2 Accessing the Switch through HTTP

2.1 Accessing the Switch through HTTP

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

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

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

2.1.1 Initially Accessing the Switch

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

1. Modify the IP address of the network adapter and subnet mask of your computer to 192.168.0.2 and 255.0.0.0 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 as below. Both the original username and the password are 'admin' (which is capital sensitive).



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

2.1.2 Upgrading to the Web-Supported Version

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

1. Connect the network port of the switch with the access cable, or refer to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DCS prompt of command 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 command `http server` to enable Web services.
5. Enter the 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 the command `write`, to save the current configuration to the configuration file.

2.2 Accessing a Switch through Secure Links

The data between the Web browser and the switch is not being 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 network port of the switch with the access cable, or refer to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DCS prompt of command 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 command `http server` to enable Web services.
5. Enter the 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 secure` command to enable the secure link access of the switch.
7. Run the `ip http https` command to access the switch through the secure links.
8. Enter the command `write`, to save 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) IP address of the switch; and then press the Enter key. Then the switch can be accessed through the secure links.

2.3 Introduction of Web Interface

The whole Web browser page consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

2.3.1 Top Control Bar

	
Save all	Writes the current settings in the configuration file of the device. It is equivalent to the execution of the <code>write</code> command. The configurations 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.
Interface panel	Displays the figure of interface panel.
About	Displays the manufacturer information and sets auto refresh.

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

2.3.2 Navigation Bar

Device Status
Device Info
Interface State
Interface Flow
Mac Address Table
Log Query
Optic Module Info
Basic Config
Port Config
L2 Config
L3 Config
Advanced Config
Network Mgr.
Diagnostic Tool
System Mgr.

The contents shown in the 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 subitem. For example, to browse the flux of the current port, you have to click 'Interface State' and then 'Interface Flow'.

Notes

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 users permissions, only 'Interface State' will appear.

2.3.3 Configuration Area

System Information	
Device Type	SWITCH
BIOS Version	0.4.5
Firmware Version	3.8.11 Build 37543
Serial No.	E20005050102
MAC Address	9479.733A.2013
IP Address	192.168.1.202
Current Time	1979-1-1 0:5:36
Uptime	0 Day -0 Hour -3 Minute -36 Second
CPU Usage	3%
Memory Usage	28%
Refresh	

The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

2.3.4 Configuration Area

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

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration on 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 reverting the modification of the sheet. The content of the sheet will be reverted.
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 web configuration page.

Chapter 3 Basic Configuration



3.1 Hostname Configuration

When you click **Basic Config** > **Hostname** in the navigation bar, the **Hostname Configuration** page appears, as shown in the following figure.



The hostname will be displayed in this login dialog box.

The default name of the device is "Switch". You can enter the new hostname in the text box shown in figure 3 and then click 'Apply'.

3.2 Time Management

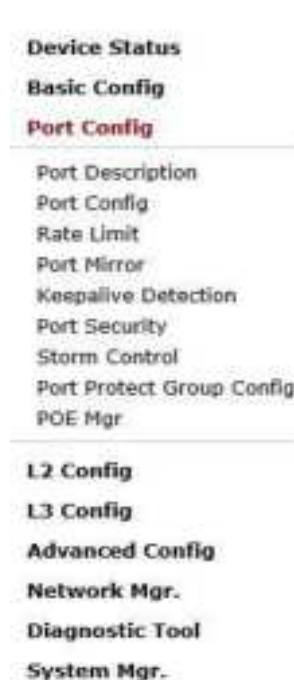
When you click **System Mgr.** > **Time Setting**, the **Time Setting** page appears.



To refresh the clock of the distributed 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 NTP servers for the device and set the interval of time synchronization.

Chapter 4 Configuration of the Physical Interface



4.1 Configuring Port Description.

If you click Port Config > Port Description in the navigation bar, the Port Description Configuration page appears, as shown in the following figure:

Port	Port Description
g0/1	

You can modify the port description on this page and enter up to 20 characters. The description of the VLAN port cannot be set at present.

4.2 Configuring the Attributes of the Port

If you click Port Config > Port Config > Port Attribute Config in the navigation bar, the Port Attribute Configuration page appears, as shown in the following figure:

Port	Status	Speed	Duplex	Flow Control	Medium
g0/1	Enable	Auto	Auto	Off	Auto

You can change the status, speed, duplex mode and flow control of a port on this page.

Notes

1. 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 interrupted.

4.3 Rate Limit

When you click **Port Config > Rate Limit** in the navigation bar, the **Port rate limit** page appears, as shown in Figure 4.

Port	Receive Status	Receive Speed Unit	Receive Speed	Send Status	Send Speed Unit	Send Speed
g0/1	Enable ▾	64kps ▾	(0-10000)	Enable ▾	64kps ▾	(0-10000)

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limit. The reception speed and transmission speed are configured by a percentage or by the designated unit of the system.

4.4 Port Mirror

When you click **Port Config > Port Mirror** in the navigation bar, the **Port Mirror Config** page appears, as shown in the following figure.

Mirror Port		g0/1 ▾	
Filters	Port Type: All ▾	Slot Num: All ▾	Name(s): Help
Mirrored Port	Mirror Mode		
g0/1	RX ▾		

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

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

- ☐ RX The received packets will be mirrored to the destination port.
- ☐ TX The transmitted packets will be mirrored to a destination port.
- ☐ RX & TX The received and transmitted packets will be mirrored simultaneously.

4.5 Keepalive Detection

When you click **Port Config > Keepalive Detection** in the navigation bar, the **Setting the port keepalive detection** page appears, as shown in Figure 6.

Port	Status	Keepalive Period
g0/1	Enable ☒	(0-32767)Seconds

You can set the keepalive detection cycle on the **Keepalive Detection** page.

4.6 Port security

4.6.1 IP Binding Configuration

When you click **Port Config > Port Security > IP Bind** in the navigation bar, the **Configure the IP Binding Info** page appears, as shown in Figure 7.

Interface Name		Detail
g0/0/1		Detail

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

	Serial number	Address	Operate
☐	1	192.168.0.2	Edit
☐	2	192.168.0.3	Edit

4.6.2 MAC Binding Configuration

When you click **Port Config > Port Security > MAC Bind** in the navigation bar, the **Configure the MAC Binding Info** page appears, as shown in Figure 8.

Interface Name		Detail
g0/0/1		Detail

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

	Serial number	Address	Operate
☐	1	1234-1234-1234	Edit
☐	2	1234-1234-1235	Edit

4.6.3 Setting the Static MAC Filtration Mode

When you click **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.

Interface Name	Port Mode	Static MAC Filtration Mode
g0/0/1	Access	Select

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

4.6.4 Static MAC Filtration Entries

When you click **Port Config > Port Security > Static MAC Filtration Entries** in the navigation bar, the **Setting the static MAC filtration entries** page appears.

Interface Name	Detail
g0/1	Detail

If you click "Detail", you can conduct the binding of the source MAC address for the physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forced to vibrate.

Serial number	Filtration Mode	MAC Address	Operation
1	Disable	0001.0003.0003	Edit

4.6.5 Setting the Dynamic MAC Filtration Mode

If you click 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.

Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
g0/1	Enable	1 (1-2048)

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

4.7 Storm Control

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

4.7.1 Broadcast storm control

Port	Status	Threshold
g0/1	Enable	(1-65535) 64Kbps

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

4.7.2 Multicast Storm Control

Port	Status	Threshold
g0/1	Enable	(1-65535) 64Kbps

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

4.7.3 Unknown Unicast Storm Control

Port	Status	Threshold
g0/1	Enable v	(1-65535) 64Kbps

Through the "Status" dropdown box, you can decide whether to enable the unknown unicast storm control on a port. In the "Threshold" column, you can enter the threshold of the broadcast packets. The legal threshold is no greater than permitted behind the threshold.

4.8 Port Protect Group Configuration

If you click **Port Config** > **Port Protect Group Config** > **Port Protect Group List** in the navigation bar, the Port Protect Group List page appears.

4.8.1 Port Protect Group List

If you click **Port Config** > **Port Protect Group Config** > **Port Protect Group List** in the navigation bar, the Port Protect Group List page appears.

If you click **New**, a new port protect group will be created, as shown in the following figure.

If you tick a Port Protect Group, you can delete it. The port protect group 0 is by default which cannot be deleted.

4.8.2 Port Protect Group Interface Configuration

If you click **Port Config** > **Port Protect Group Config** > **Port Protect Group Interface Config** in the navigation bar, the Port Protect Group Config page appears.

Port	Port Protect Group
g0/1	
g0/2	

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

Chapter 5 Layer-2 Configuration



5.1 VLAN Configuration

5.1.1 VLAN List

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

	VLAN ID	VLAN Name	Operate
☐	1	Default	Edit
☐	2	2	Edit

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 click 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 click **Edit** at the end of a VLAN item to modify the VLAN name and the config 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 30 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 maxvlan`

command to modify the maximum number of VLANs that will be displayed.

5.1.2 VLAN Configuration

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

Port	Default VLAN	Mode	Untag or not	Allow or not
g0/1	1 <3-4094>	Access	No	Yes
g0/2	1 <3-4094>	Access	No	Yes
g0/3	1 <3-4094>	Access	No	Yes
g0/4	1 <3-4094>	Access	No	Yes
g0/5	1 <3-4094>	Access	No	Yes
g0/6	1 <3-4094>	Access	No	Yes
g0/7	1 <3-4094>	Access	No	Yes

If you want to create a new VLAN, enter a VLAN ID and a VLAN name in the VLAN name column.

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 this current VLAN when the port works as the egress port.

Notes

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

5.2 GVRP Configuration

5.2.1 GVRP Global Attribute Configuration

Click **Config > GVRP Config > GVRP Global Config** in the navigation bar and enter GVRP global attribute configuration page.

You can enable or disable the global GVRP control, and set dynamic vlan to take effect or not only in the registered ports.

5.2.2 GVRP Port Attribute Configuration

Click **Config > GVRP Config > GVRP Interface Config** in the navigation bar and enter GVRP interface attribute configuration page.

Port	GVRP Status
g0/1	Enable v

GVRP interface configuration can enable or disable GVRP protocol of the port.

5.3 STP Configuration

5.3.1 STP Status Information

Click **Advanced Config > STP Config** in the navigation bar, the STP Config page appears, as shown in figure 10.

Root STP Config	
Spanning Tree Priority	4096
MAC Address	00E0.0F8E.7025
Hello Time	2
Max Age	20
Forward Delay	15
Local STP Config	
Protocol Type	RSTP v
Spanning Tree Priority	32768 v
MAC Address	8479.733A.2033
Hello Time	2 (1-10)s
Max Age	20 (6-40)s
Forward Delay	15 (4-30)s
BPDU Terminal	Disable v
Apply Reset	

The root STP configuration information and the STP ports status are only read.

Click the dropdown box on the right side of "Protocol" to change the currently running STP mode. The supported modes include STP, RSTP and Disabled STP.

The priority and the time need to be configured for different mode.

Notes

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

5.3.2 Configuring the Attributes of the STP Port

Click the "Configure RSTP Port" option, this "Configure RSTP Port" page appears.

Port	Port Name	Priority (0-255)	Path Cost (0-65535)	Edge Port	RSTP Ring
2/21	Eth21	128	0	Disable	Disable

The configuration of this attribute of the port is irrelevant of the global STP mode. For example, if the priority value is set to 'Disable' and the RSTP mode is enabled, the port will not run this attribute in the network.

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

5.4 IGMP Snooping Configuration

5.4.1 IGMP Snooping Configuration

Click **2 Config > IGMP Snooping** in the navigation bar and enter the **IGMP Snooping Configuration** page.



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

5.4.2 IGMP Snooping VLAN List

In the navigation bar, click **2 Config > IGMP Snooping > IGMP Snooping VLAN List** in the navigation bar and enter IGMP Snooping VLAN page.



If you click **New**, IGMP snooping VLAN configuration can be done. Through Web up to 6 original 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.

Configuring the IGMP Snooping VLAN Config

VLAN ID:

Status of the IGMP Snooping Vlan: Enable

Immediate-leave: Enable

Configured Member Port List:

1 2 3 4 5 6 7 8 9 10

Available Port List:

g0/1
g0/2
g0/3
g0/4
g0/5
g0/6
g0/7
g0/8
g0/9
g0/10

Apply Reset Go Back

When create new IGMP Snooping Vlan, VLAN ID can be modified; when modify IGMP Snooping Vlan, VLAN ID cannot be modified.

You can add or delete the mirroring port by buttons "+" or "-" on it.

5.4.3 Static Multicast Address

Click **Config > IGMP Snooping > Static Multicast Address** in the navigation bar, and enter the static multicast address configuration page.

Static Multicast Address Config

VLAN ID:

Multicast IP Address:

Assignment Port: g0/1

Apply

Static Multicast List Info

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

VLAN ID	Group	Port
☐ Select All/Select none		

Delete Refresh

This page displays the static multicast group in current network according to IGMP Snooping statistics and the port where each member belongs to. Click "Refresh" to refresh the contents in this list.

5.4.4 Multicast List

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

Multicast List Info

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

VLAN ID	Group	Type	Port
1	239.255.255.250	IGMP	g0/9
1	225.0.0.83	IGMP	g0/9

Refresh

On this page the multicast groups, which are existent in the current network and are in the statistics of IGMP Snooping, are

will display network members in each group belong to and assigned.

Click 'Refresh' to refresh the contents in this list.

Notes

By default, a multitenant list can display up to 15 VLAN items. You can modify the number of multitenant items by clicking on the page with group groups after you log on to the device through the Console port in the net.

5.5 Setting Static ARP

Click **Config > Static ARP** in the navigation bar, and enter the basic ARP configuration page.

Click 'New' to add ARP entry. The VLAN interface needs to be assigned when configuring the ARP entry.

Click 'Modify' to modify the current ARP entry.

Click 'Delete' to delete the selected ARP entry.

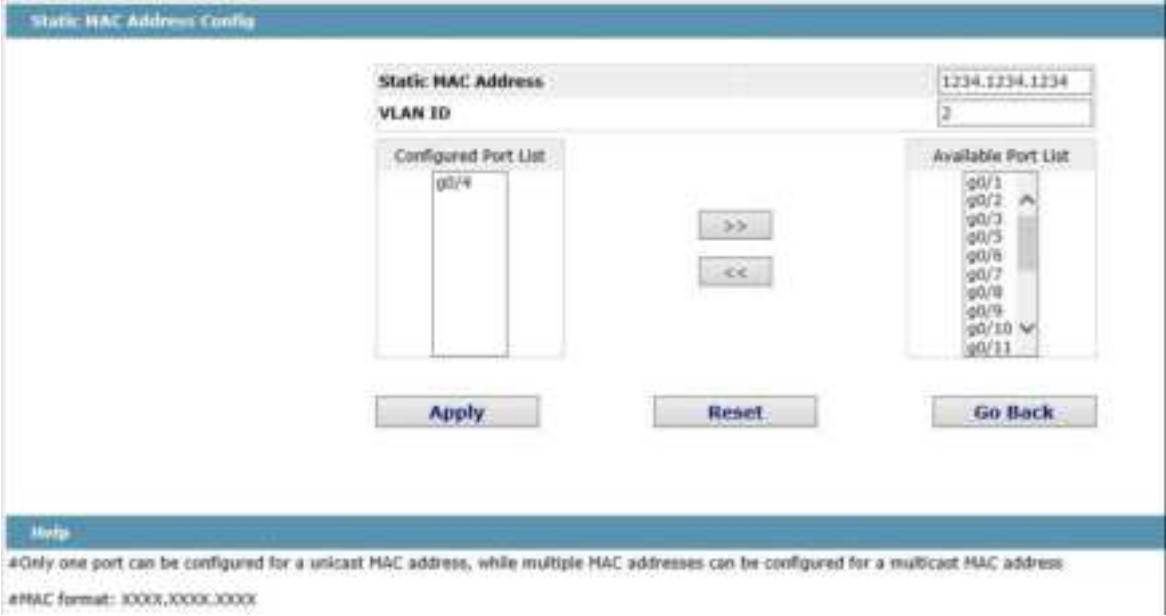
5.6 Static MAC Configuration

Click **Config > Static MAC Config** in the navigation bar, and enter static MAC address configuration page.

Click 'New' to configure static MAC address and VLAN for the assigned port. The unicast MAC address can only be configured with one port and the multicast MAC address can be configured with multiple ports.

Click 'Modify' to modify the configured static MAC address.

Click 'Delete' to delete the static MAC address entry.



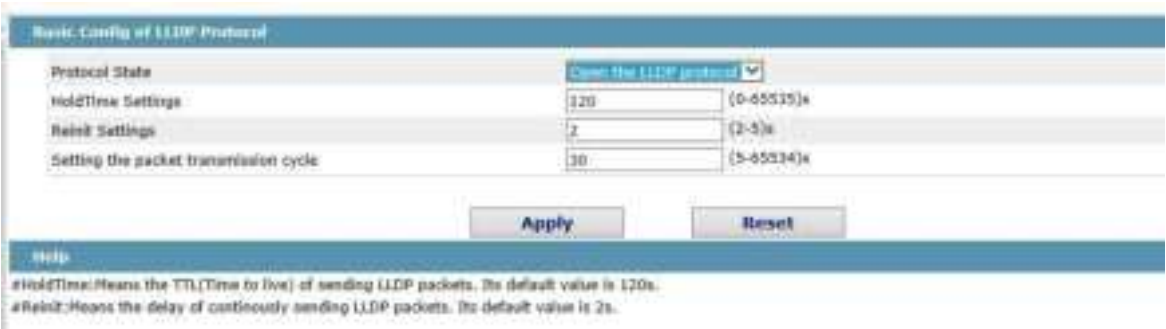
The 'Static MAC Address Config' window contains the following elements:

- Static MAC Address:** A text field containing '1234.1234.1234'.
- VLAN ID:** A text field containing '2'.
- Configured Port List:** A list box containing 'g0/4'.
- Available Port List:** A list box containing ports g0/1 through g0/11.
- Navigation Buttons:** '>>' and '<<' buttons between the port lists.
- Action Buttons:** 'Apply', 'Reset', and 'Go Back' buttons at the bottom.
- Help Section:**
 - Only one port can be configured for a unicast MAC address, while multiple MAC addresses can be configured for a multicast MAC address.
 - MAC format: XXXX.XXXX.XXXX

5.7 LLDP Configuration

5.7.1 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 15.



The 'Basic Config of LLDP Protocol' window contains the following elements:

- Protocol State:** A dropdown menu set to 'Open the LLDP protocol'.
- HoldTime Settings:** A text field with '120' and a unit '(0-65535)s'.
- Reinit Settings:** A text field with '2' and a unit '(2-5)s'.
- Setting the packet transmission cycle:** A text field with '30' and a unit '(5-65534)s'.
- Action Buttons:** 'Apply' and 'Reset' buttons.
- Help Section:**
 - 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.

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

The 'HoldTime' parameter means the delay value of the packet that is transmitted by LLDP, whose default value is 120s.

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

5.7.2 Configuring the Attributes of the LLDP Port

Click **Link Layer 2 Config** > **LLDP Config** > **LLDP Port Config** in the navigation bar, the **Setting the attributes of the LLDP port** page appears, as shown in Figure 7.

Port	Receive LLDP Packet	Send LLDP Packet
g0/1	Enable ▾	Enable ▾

LLDP interface configuration can enable or disable the port transmitting LLDP packets.

5.8 DDM Configuration

Click **Link 2 Config** > **DDM Config** in the navigation bar, and enter DDM configuration page.



5.9 Link Aggregation Configuration

5.9.1 Port Aggregation Configuration

Click **Link Advanced Config** > **Link Aggregation Config** in the navigation bar, the **Link aggregation Config** page appears, as shown in Figure 22.



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 new 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 port, you can choose the aggregation mode to be Static LACP Active or LACP Passive.

You can click **add** and **del** to delete and add a member port in the aggregation group.

5.9.2 Configuring Load Balance of Port Aggregation Group

Some models support aggregation group-level load balance mode configuration and some models do not have configuration in the global configuration mode.



You can select link aggregation load balance mode and click 'Apply' to apply it.

5.10 EAPS Ring Protection Configuration

5.10.1 EAPS Ring List

Click **Link Layer 2 Configuration > Ring Protection > EAPS Config**, the EAPS Ring Config page appears.



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' button to configure the 'Time' parameter of the ring.

Notes:

1. The system can support 6 EAPS rings.
2. After a ring is configured, its port, node type and control VLAN cannot be modified. If the port of the ring, the node type or the control VLAN need be adjusted, please delete the ring and then establish a new one.

5.10.2 FAPS Ring Configuration

You click "New" on the FAPS ring list, or "Open" on the right side of a ring item, the "Configure FAPS" page appears.

Notes:

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 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", then two ports or two automatically set to transit ports.

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

5.11 MEAPS Configuration

5.11.1 MEAPS Ring Configuration

You click Layer 2 Config > Multiple Ring Protection > Multiple Ring Protection on the navigation bar, the Multiple Ring Protection Configuration page appears.

Multiple Ring Protection Configuration												
New												
Res./Page/Total 4 Page	First	Prev	Next	Last	Go To:		Page	Search:				
Domain ID	Ring ID	Ring Type	Node Type	Control Vlan	Hello Time	Failed Time	Pre-Forward Time	Port	Type	Port	Type	Operate
1	2	Major Ring	Master Node	2	3	6	6	None	Primary Port	None	Secondary Port	Edit
☐ Select All/Select None												Delete

The list shows the current configured MFAPS ring, including Domain ID, Ring ID, Ring type, Node type, Control Vlan, Hello Time, Failed Time, Pre-Forward Time, primary port and secondary port.

Click New to create a MFAPS ring.

Click Edit on the right and configure the time parameter and the primary and secondary port of the ring.

Notes:

1. The system supports 4 MFAPS (0-3).
2. One domain supports 8 rings (0-7).
3. Once one MFAPS is configured, its Domain ID, ring ID, ring type, node type and control Vlan cannot be modified. If adjustment is needed, please delete the Ethernet ring and recreate it.

5.11.2 MFAPS Ring Configuration

you click New on the Multiple Ring Protection page or click Edit on the right, the New MFAPS Global Config page appears.

New MFAPS Global Config	
Domain ID*	
Ring ID*	
Ring Type*	Major Ring ▾
Node Type*	Master Node ▾
Control Vlan*	
Hello Time	
Failed Time	
Pre-forward Time	
Primary Port	None ▾
Secondary Port	None ▾
Apply Reset Go Back	
Notes	
*Your web management may be interrupted as the control VLAN is modified to be the vlan interface that the web browser connects. *Only the master or transit node can be configured in the major ring. *The master node, transit node, edge node or assistant node can be configured in the sub ring. *The master or transit node can be configured in one ring, while the edge node or assistant edge node can be configured in several rings.	

Notes:

In an existed MFAPS ring, its domain ID, ring ID, ring type, node type and control Vlan cannot be modified.

The primary ring can only be configured with the main node and the Transit node.

The secondary ring can be configured with the main node, the transit node, the edge node and the assistant edge node.

The primary node and the transit node can only be existed in one ring.

The edge node and the assistant edge node can be existed in multiple rings simultaneously.

On the right drop box of 'Primary Port' and 'Secondary Port', select one port respectively as the ring port or select None.

5.12 Backup Link Protocol Configuration

5.12.1 Backup Link Protocol Global Configuration

System Link Layer 2 Config > Backup Link Config > Backup Link Protocol Global

Configure the navigation bar, the Backup Link Protocol Global Config page appears.



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

Click New to create a new link backup group.

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



Notes

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

5.12.2 Backup Link Protocol Interface Configuration

System Link Layer 2 Config > Backup Link Protocol Config > Backup Link Protocol Interface Config on the navigation bar.

the Backup Link Protected Global Config page appears.

Backup Link Protected Interface Config						
No. 1 Page/Total 1 Page	First Prev Next Last	Go No.	Page	Search:	Current 18 Item/Total 18 Item	
Interface Name	Group ID	Interface Attribute	MMU Attribute	Shared VLAN	Operate	
g0/1					Edit	
g0/2					Edit	
g0/3					Edit	
g0/4					Edit	
g0/5					Edit	
g0/6					Edit	
g0/7					Edit	
g0/8					Edit	

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

Click Edit on the right to configure the Backup Link Protected.

Backup Link Protected Interface Config

Interface Name

g0/3

Group ID

Interface Attribute

MMU Attribute

Shared VLAN

Apply

Reset

Go Back

Help

Shared Used VLAN can be Only Configured On The Backup Port

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

5.13 MTU Configuration

From Link Layer 2 Config > MTU Config in the navigation bar, the MTU Config page appears.

MTU Config

mtu: (1500-9216)

Apply

Reset

Help

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

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

5.14 PDP Configuration

5.14.1 Configuring the Global Attributes of PDP

From Link Layer 2 Config > PDP Config in the navigation bar, the Global PDP Config page appears, as shown in Figure 4.



Basic Config of PDP Protocol

Protocol State	[Close the PDP protocol ▼]	
HoldTime Settings	180	(30-255)s
Setting the packet transmission cycle	60	(5-254)s
Protocol Version	[version2 ▼]	

Notes:

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

#Cycle of Sending Packets: Its default value is 60s.

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

The "Hold Time" parameter means the time to be saved before the meter discards the received information if other PDP packets are not received.

5.14.2 Configuring the Attributes of the PDP Port

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



Port	Status
g0/1	[Enable PDP ▼]

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

Chapter 6 Layer-3 Configuration



6.1 Vlan interface configuration

Click **L3 Config > VLAN Interfaces and IP Addresses**, and enter the VLAN interface configuration page.



Click **New** to add a new VLAN interface. Click **Delete** 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.



Notes:

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

6.2 Setting the Static Route

When you click Layer3 Config > Static Route Config, the Static route configuration page appears.

Static Route Config

New

No.	Default Route	Dest IP Segment	Dest IP Mask	Interface Type	VLAN Interface	Gateway's IP Address	Forwarding Address	Distance metric	Routing Tag	Specify the route description	Operate
1	☐	192.168.0.0	255.255.0.0	gateway		192.168.1.3			0	None	Edit

☐ Select All/Select None [Delete](#)

Help

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

Click Create to add a static route.

When you click Edit, you can modify the current static route.

When you click Cancel, you can cancel the current static route.

Static Route Config

Configure the static routing protocol

Default Route ☐

Dest IP Segment

Dest IP Mask

Interface Type

Interface Vlan

Gateway's IP Address

Forwarding Address

Distance metric

Routing Tag

Specify Route Description

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

Help

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

Chapter 7 Advanced Configuration

Device Status

Basic Config

Port Config

L2 Config

L3 Config

Advanced Config

Qos Config

IP Access List

MAC Access List

Network Mgr.

Diagnostic Tool

System Mgr.

7.1 Qos Configuration

7.1.1 Configuring QoS Port

Click link **Advanced Config** > **Qos** > **Configure Qos Port**, the **Port Priority Config** page appears.

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

7.1.2 Global Qos Configuration

Click link **Advanced Config** > **Qos** > **Configure Qos Port**, the **Port Priority Config** page appears.

In WRR mode, you can set the weight ratio of the queue. There are 4 queues in total, among which queue 1 has the lowest priority and queue 4 the highest priority.

7.2 IP Access Control List

7.2.1 Setting the Name of the IP Access Control List

If you click **Advanced Config** > **IP Access Control List** > **IP Access Control List Config**, the IP ACL configuration page appears.



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



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

7.2.2 Setting the Rules of the IP Access Control List

➤ Standard IP access control list



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.



➤ Extended IP access control list

Extended IP ACL (Advanced ACL)

New

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

Action	Rule Type	Rule Number	Src Address	Src Port	Dest Address	Dest Port	Time Range	Precedence	Do not fragment the flag	Fragmented packet	Offset	Length of the IP packet	Time-to-live value	Record the log	Operate
permit	Basic	0	192.168.1.1/255.0.0.0			any									edit

☐ Select All/Select None

Go Back Delete

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

Advanced IP ACL Configuration

ACL Name: Basic ACL

Action	permit
Rule Type	Basic
Rule Number	0
Src IP Type	any
Src IP Mask	
Src Interface Mask	
Src Port Range	
Dest Port Range	
Time Range	
Precedence	
Do not fragment	
Fragmented packet	
Offset	
Length of the IP packet	
Time-to-live value	

Apply Reset Go Back

7.2.3 Applying the IP Access Control List

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

Port	Egress ACL	Degress ACL
00/1	inward	
00/2		out
00/3		
00/4		
00/5		
00/6		
00/7		
00/8		

7.3 MAC Access Control List

7.3.1 Setting the Name of the IP Access Control List

If you click **Advanced Config** > **MAC Access Control List** > **MAC Access Control List Config**, the **MAC ACL configuration** page appears.

MAC ACL Config

New

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

Current 1 Item/Total 1 Item

No.	Name of the MAC Access Control List	Operate
1	MyACL	Edit

☐ Select All/Select None

Delete

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

Creating MAC ACL

Name of the MAC ACL*

Apply Reset Go Back

7.3.2 Setting the Rules of the MAC Access Control List

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

MAC ACL Rule Config

New

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

Current 1 Item/Total 1 Item

No.	Authority	Src MAC Type	Src MAC	Src MAC Mask	Dst MAC Type	Dst MAC	Dst MAC Mask	Operate
1	permit	host	0001.0002.0003		any			Edit

☐ Select All/Select None

Go Back Delete

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

MAC ACL Rule Config

New MAC ACL Rule Config

Authority: permit

Src MAC Type: any

Src MAC:

Src MAC Mask:

Dst MAC Type: any

Dst MAC:

Dst MAC Mask:

Apply Reset Go Back

Note: The valid mac address can be one of the following formats: 0000.0000.0000, 0000.0000.0000, 00:00:00:00:00:00, and 00:00:00:00:00:00, among which 0 is a hex number

7.3.3 Applying the MAC Access Control List

If you click **Advanced Config** > **MAC Access Control List** > **Applying This MAC Access Control List**, the Applying the MAC access control list page appears.

Port	Egress ACL	Egress ACL
00/1		
00/2		
00/3		
00/4		
00/5		
00/6		
00/7		

Chapter 8 Network Management Configuration

Device Status

Basic Config

Port Config

L2 Config

L3 Config

Advanced Config

Network Mgr.

SNMP Mgr.

RMON Config

Diagnostic Tool

System Mgr.

8.1 SNMP Configuration

If you click Network Management Config > SNMP Management in the navigation bar, the SNMP management page appears, as shown in Figure 7.

8.1.1 SNMP Community Management



The screenshot shows the 'SNMP Community Management' page with a table of existing communities. The table has columns for 'No.', 'Page/Total', 'SNMP Community Name', 'SNMP Community Description', 'SNMP Community Attribute', and 'Operate'. One entry is visible with the name 'public@snacFree' and attribute 'RO'. A 'Delete' button is at the bottom right.

No.	Page/Total	SNMP Community Name	SNMP Community Description	SNMP Community Attribute	Operate
1	1/1	public@snacFree	False	RO	edit

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

You can create, modify or delete 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 configuration form for a new SNMP community. It includes input fields for 'SNMP Community Name' (with a hint 'Input less than 20 characters') and 'SNMP Community Attribute' (a dropdown menu currently set to 'Read Only'). There are 'Apply' and 'Go Back' buttons at the bottom.

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

8.1.2 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 Inform, and as its version is 1, SNMP Message Type does not support Inform.

8.2 RMON

8.2.1 RMON Statistic Information Configuration

If you click Network Management Config > Rmon > Rmon Statistics RMON Statistics page appears.

Now, the RMON Statistics page appears.



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

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

At present, the use for statistic information can be obtained through the command line 'show rmon statistics', but the

Web does not support this function.

8.2.2 RMON History Information Configuration

Typically, click **Network Management Config** > **RMON** > **RMON History** > **new**, the RMON history page appears.

Interface History Config

Interface	gig1/0/1	
Index		(1-40000)
Sampling Number	20	(1-40000)
Sampling Interval	1000	(1-10000)
Owner	config	Enter less than 31 characters*

Apply Go Back

Note

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

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 configuration 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 1000s.

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

8.2.3 RMON Alarm Information Configuration

Typically, click **Network Management Config** > **Rmon** > **Rmon Alarm** > **new**, the RMON Alarm page appears.

RMON Alarm Config

Index		(1-40000)
RMON Mode	RMON2	
OID	1.3.6.1.2.1.1.3.1.10	
Interface	gig1/0/1	
Alarm type	absolute	
Sampling Interval		(1-2147483647)
Rising Threshold		(1-2147483648 - 2147483647)
Rising Event Index		(1-45530)
Falling Threshold		(1-2147483648 - 2147483647)
Falling Event Index		(1-45530)
Owner		Enter less than 31 characters*

Apply Go Back

Note

*The owner can be empty

*The string was totally entered is limited to 255 characters

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 ones.

The MID number always sends to CID.

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

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

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

8.2.4 RMON Event Configuration

You click **Network Management Config > RMON > RMON Event** RMON event page appears. Now, the RMON event page appears.

RMON Event Config

Index	01-000000
Owner	
Description	
Enable log	☐
Enable trap	☐
Community	

Apply **Go Back**

Help

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

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 owner of the information of an event.

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

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

Chapter 9 Diagnosis Tools



9.1 Ping

9.1.1 Ping

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

 A screenshot of the 'SNMP Event Config' page. The 'Ping' section is expanded, showing a table with columns for 'Index', 'Owner', 'Description', 'Enable log', 'Enable trap', and 'Community'. The 'Index' column has a value of '(1-65535)'. The 'Enable log' and 'Enable trap' checkboxes are unchecked. Below the table are 'Apply' and 'Go Back' buttons. At the bottom, there is a 'Note' section with the following text:

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

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

To 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 to your entered address, the device can promptly return a test result to you. But, the device will take a little more time to return the test result.

'Source IP address' is used to set the source IP address which is carried in the Ping packet.

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

Chapter 10 System Management



10.1 User Management

10.1.1 User List

When you click **System Mgr.** > **User Mgr.**, 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.

3. The limited user can only browse the status of the device.

10.1.2 Establishing a New User

If you click "New" on the User Management page, the Creating User page appears.

User Management

User name:

Password:

Confirming password:

Role-Group:

Authen-Group:

Author-Group:

Help

Click the 'Apply' button to add a user or modify the password and the permission.

Users can be divided into the Admin user and the limited user according to the permission. The Admin user can use all functions of the switch, including browsing, configuring and remote login, while the limited user only has the permission to browse the switch's running state through the WEB page.

In the "User name" text box, enter a name, which contains letters, numbers and

symbols except '?', '\', '%', '*' and the 'Space' symbol.

In the "Password" text box enter a login password, and in the "Confirming password"

Text box enter this login password again.

10.1.3 User Group Management

Click the Tab page of user group management and enter user group management page.

User Group Man.

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

No.	Serial Number	Group Name	Role-Group Rule	Authen-Group Rule	Author-Group Rule	Operate	Detail
1		all		a		Add	Delete

☐ Select All/Select None

Click "create new" to create a new user group.

Click "delete" to delete the user group.



User Group Config

User Group Name*
 Pass-Group Name
 Authen-Group Name
 Author-Group Name

Hint

*The user group name's exist.
 *Rule must exist.

The new user group name must be not used before. The password rule name, authentication rule name and authorization rule name must have been created, or you cannot create a new user group. Configure the password rule, authentication rule and authorization rule in other 3 tabs pages.

10.1.4 Password Rule Management

Click password rule management Tab page to enter password rule management page.



Password Rule

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

Serial Number	Pass-Group Name	Same as the username	Min Length	Validity	Number	Lower-letter	Upper-letter	Special-character	Operate
1	11111	Can be same			Must	Must	Must	Must	Edit

☐ Select All/Select None

Click "create new" to create new password rule.

Click "delete" to delete password rule.



Password Config

Pass-Group Name*
 Same as Username
 Contain Number
 Contain Lower-letter
 Contain upper-letter
 Contain Special-character
 Min length
 validity

Hint

1. Config Pass-Group

Set some password rules including whether the password can be the same with the user name, whether the password must contain numbers, lower case, uppercase, special characters, the minimum length and the period of validity.

When the rule is created and applied to the user management, this user password will never invalid if this user password is not complied with the password rule, vice versa.

10.1.5 Authentication Rule Management

Click the Tab page of authentication rule management to enter authentication management page.



Click 'create new' to create the new authentication rule.

Click 'delete' to delete the authentication rule.



You can configure the maximum number of attempts and periods or you don't, but you must configure them simultaneously or neither.

10.1.6 Authorization Rule Management

Click the Tab page of authorization rule and enter the authorization rule management page.



Click 'create new' to create new authorization rule.

Click 'delete' to delete the authorization rule.

The authorization rule determines your permission of the administrator or the limited user. If you are the administrator, you have the administrator right. If you are the limited user, you can only check the web.

10.2 Log Management

If you click **System Mgmt > Log Mgt**, 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" text box 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 know the logs which are saved on the device. The log information on chip 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" text box and select the grade of the cached log in the "Grade of the cache log information" dropdown box.

10.3 Managing the Configuration Files

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

10.3.1 Exporting the Configuration Information

The current configuration file can be exported, saved in the disk of PC or in the on-chip storage device as the backup file.

To export the configuration file, please click the "Export" button and then select the "Save" option in the pop-up download dialog box.

The default name of the configuration file is 'Startup-config', but you are suggested to set it to an easily memorable name.

10.3.2 Importing the Configuration Information



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.

Notes

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 an error occurs during the process of importation, please try it again or click the "Save All" button to make the device re-establish the configuration file with the current configuration, avoiding the importing file and the abnormality of the device.
3. After the configuration file is imported, if you want to use the imported configuration file immediately, please click "Save All", but reboot the device directly.

10.4 Software Management

Click System Mgmt. > Software Update in the navigation bar and enter the device software management page.

10.4.1 Backup System Software



The current running software version is displayed on the page. If you need to backup the system, please click "Backup

system software', then select 'save' in the pop-up file download dialog box and save the system profile to your computer disk, transfer to a data device or other positions in the network.

Notes

Default name of the system profile is 'Switch.bin'. You are suggested to change the default name to a name that easy to identify.

10.4.2 Update System Software

Notes

1. Please ensure you update system profile match with the device type. Otherwise, the system cannot operate normally.
2. The system profile update may need 1 to 2 minutes. After clicking and confirming the 'update' button, the profile will be uploaded to the device. Please be patient.
3. Please do not restart or interrupt the device if errors occur in the update process or the device cannot start up. Please try update again later.
4. Please save the configuration and restart the device after updating, so that the new system can operate.



The update software is usually used for solving the existing problems or improving certain functions. You don't need to update the system software regularly. If your device operates normally.

If your system needs to be upgraded, please enter the full path of the new system profile into the text box right of 'update system software' or click 'browse' button to select new system profile and click 'update'.

10.4.3 Rebooting the Device

If you click System > Reboot, this Rebooting page appears.



If the device needs to be restarted, please first make sure that the modification configuration of the device has already been saved, and then click the 'Reboot' button.