

# S3410-10TF-P Switch Web Configuration Guide

Model: S3410-10TF-P



# Contents

1. Web-Based Configuration	1
1.1 Overview	1
1.2 Application	1
1.2.1 Web-based Management	1
1.3 Web Management System	3
1.3.1 Favorites	5
1.3.2 Network	
1.3.3 Security	
1.3.4 Advanced	25
1.3.5 System	31

# 1. Web-Based Configuration

# 1.1 Overview

A user accesses the Web-based management system of a switch by using a browser (for example, IE browser) to manage the switch. Web-based management involves two parts: Web server and Web client. A Web server is integrated onto a device to receive and process requests sent from a client (for example, read a Web file or execute a command request) and returns the processing result to the client. Generally, a Web client refers to a Web browser, for example, IE browser.

Currently, this file is applicable to only switches.

# 1.2 Application

Application	Description
Web-based Management	After finishing relevant configuration, a user can access the Web-based management system through a browser

#### 1.2.1 Web-based Management

#### Scenario

As shown in the following figure, a user can access an access switch or aggregation switch through a browser on a PC to manage and configure the device.

#### Figure 1-1



#### NOTE:

A user can access the Web-based management system of the switch in the red rectangle if this switch can be pinged from the PC.

#### **Function Deployment**

## **\U** Configuration Environment Requirements

**Requirements for Client** 

- An administrator logs in to the Web-based management system by using the Web browser on a client to manage the switch. Generally, a client refers to a PC. It may also be other mobile terminal devices, for example, a laptop.
- Browser: IE7.0, IE8.0, IE9.0, IE10.0, IE11.0, Google chrome, Firefox, and some IE kernel-based browsers (for example, 360 security browser) are all supported. Exceptions such as messy code and format error may occur when other browsers are used.
- Resolution: It is recommended that the resolution be set to 1024\*768, 1280\*1024, or 1920\*1080. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

#### Requirements for server

- The Web service must be enabled for the switch.
- Login authentication information for Web-based management must be configured for the switch.
- A management IP address must be configured for the switch.

## NOTE:

For the detailed configuration of the switch on the command line interface (CLI), see Configuring Web Server.

## NOTE:

Web configuration and CLI configuration can be performed synchronously. It is recommended that the write command be executed after CLI configuration is completed. If any Web page is opened, please refresh this page to synchronize Web configuration and CLI configuration.

# Login L

You can type http://X.X.X.X (management IP address) in the address bar of a browser and press Enter to access the login page, as shown in the following figure.

#### Figure 1-2 Login Page

WELCOME TO FS SWITCH		
Username		
Please enter the username	Exything & Cruit 1	
Password	Gis	
Plase enter the password →		
LOGIN		

After typing the username and password, click Login. The following table lists the default username and password.

Default Username/Password Permission Description	Default Username/Password	Permission Description
--	---------------------------	------------------------

#### admin / admin

# Super administrator who possesses all permissions

#### NOTE:

The default username and password are not displayed by running the show running-config command.

After passing authentication, the home page of the Web-based management platform is displayed, as shown in the following figure.

# Figure 1-3 Home Page

	Device De	tails					~	Device Usage	0 /
etwork > scurity > tvanced >	 Model: \$341		Up Port Cour	Model: \$2410-10TF-P Device MAC: 649d,990 nt Device SN: 61PL91W0	00.0401 Runnie	urrent 2022-03-24 16:56:13 ng Time: 0 d 06 h 08Min n: 53410_FSOS 11.4(1)87454		CPU Usage Memory Usage	6.10% 49.8%
rstem >	Device Por	rt						Selected 🛛 AG Port 🗖 Up 🖷 Shute	down 🖸 VSL Po
	RE FS		4 SAV6 7AV8	9 10 11 11 11 11 11 11 11 11 11 11 11 11	S24510-3079-JP Police 12 RESET				
	Port Role: 🕚	Trunk Port 💿 Ro	outed Port					💼 Copper 📰 Fiber 📰 40Gb	40Gb(Splite
	Port Infor	mation O							
	Port Infor		Output Rate :	Status(Port real speed) :	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count	
			Output Rate ÷	Status(Port real speed) = Connected(1000M)	InOctets/OutOctets 44392388/5171881	UnderSize/OverSize	CRC/FCS Error 0/0	Collision Count 0	
	Port	Input Rate :							
	Port Gi0/1	Input Rate a	0.1K	Connected(1000M)	44392388/5171881	0/0	0/0	0	
	Port Gi0/1 Gi0/2	Input Rate ÷ 2.2K 0K	0.1К ОК	Connected(1000M) Not Connected	44392388/5171881 0/0	0/0 0/0	0/0	0	
	Port Gi0/1 Gi0/2 Gi0/3	Input Rate = 2.2K OK OK	0.1К ОК ОК	Connected(1000M) Not Connected Not Connected	44392388/5171881 0/0 0/0	0/0 0/0 0/0	0/0 0/0 0/0	0 0 0	
	Port Gi0/1 Gi0/2 Gi0/3 Gi0/4	Input Rate = 2.2К ОК ОК	0.1К ОК ОК	Connected(1000M) Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0	0/0 0/0 0/0	0/0 0/0 0/0 0/0	0 0 0	
	Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5	Input Rate = 2.2К ОК ОК ОК	0.1К ОК ОК ОК	Connected(1000M) Not Connected Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0	0 0 0 0	
	Port G10/1 G10/2 G10/3 G10/4 G10/5 G10/6	Input Rate : 2.2к ок ок ок ок ок	0.1K OK OK OK OK	Connected(1000M) Not Connected Not Connected Not Connected Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0		
	Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7	Input Rate : 2.2К ОК ОК ОК ОК ОК	0.1K OK OK OK OK	Connected(1000M) Not Connected Not Connected Not Connected Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0		

#### NOTE:

For details about the Web page, see Web Management System.

# 1.3 Web Management System

#### **Basic Concepts**

# ك Various Icons and Buttons on the GUI

lcon/Button	Note
	Edit button. You can click this icon to edit the currently selected item
Batch Delete	Delete button
	Status icon
	Port available for selection. After you click or select this port, this port becomes a selected port
	Port not available for selection
	Selected port

lcon/Button	Note
	Aggregate port. The number in the port indicates the aggregate port number
0	Trunk port. This port is displayed on the panel on the VLAN Management/VLAN Settings page
Save	Save button. You can click this button to submit and save the input information
+	Add setting
	Delete setting
I All 땳 Invert 🗵 Deselect	Batch processing operations on panel ports. These icons are located on the lower right of the panel. These icons are available only on the panel where you are allowed to select multiple ports
*	If this mark is displayed behind a text box, the item corresponding to this text box is mandatory
0	Note
0	Warning
<ul> <li>System Operations</li> <li>Standalone Device Panel</li> </ul>	
All      Invert      Deselect	Available Unavailable Selected AG Port
Note:Click and hold the left button as you drag the pe	ointer across the section to select multiple ports.

#### Panel operations

You can click to select a port or move the cursor to select multiple ports on the panel to change available port(s) into selected port(s). You can perform setting on a selected port, for example, add port description, configure port mirroring, and configure port rate limiting. Selected ports are arranged in the boxes on the lower part of the port panel by slots.

1) Selected port on standalone device



All Invert Deselect

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.

# Feature

The following table describes the functions in the secondary menu on the left of the Web page.

Feature	Description
Home Page	Allows you to view the port information and device configuration
VLAN	Allows you to set the VLAN and Trunk ports
<b>Quick Configuration</b>	Allows you to perform VLAN configuration or other configuration quickly
Port	Allows you to perform basic settings on a port and configure port aggregation, port mirroring, and port rate limiting
Restart	Allows you to restart the device
MAC Address	Allows you to configure the static address and filtering address
'Routing	Allows you to configure the route
STP	Allows you to configure basic STP information, STP ports and RLDP
IGMP Snooping	Allows you to configure IGMP Snooping
DHCP Relay	Allows you to configure DHCP relay
Authentication	Allows you to configure Eportal authentication and perform advanced settings
DHCP Snooping	Allows you to configure DHCP Snooping
Feature	Description
Anti-ARP-Attack	Allows you to perform anti-ARP-spoofing settings, ARP check settings, DAI settings, and ARP entry settings
IP Source Guard	Allows you to perform port settings and user binding
Port Security	Allows you to perform basic settings and security binding
NFPP	Allows you to view the content related to NFPP anti-attack
Storm Control	Allows you to perform storm control
Port Protection	Allows you to configure port protection
DHCP	Allows you to perform DHCP settings and static address allocation and access the client list
ACL	Allows you to set the ACL list and ACL time and apply ACL
QoS	Allows you to perform classification setting, policy setting, and stream setting
System Settings	Allows you to set the system time, modify the password, restart the system, restore to default factory settings, configure enhanced function, and set the SNMP and DNS
System Upgrade	Allows you to perform local upgrade and online upgrade
Administrator Permissions	Allows you to set the administrator permissions
System Logging	Allows you to configure the log server and view system logs
Network Detection	Allows you to configure ping detection, tracert detection, and cable detection

# 1.3.1 Favorites

You can access secondary menus through the primary menu Favorites, including Home page, VLAN, Port and Restart.

# Home Page

Device configuration, basic port information, and port statistics are displayed on the home page.

#### The following figure shows the home page.

#### Figure 1-4 Home Page

							CPU Usage		6.109
Model: \$34		Up Port Cour	Model: \$3410-10TF-P Device MAC: 649d.99	00.0401 Runnin	rrent 2022-03-24 16:56:13		Memory Usage		49.89
		op Fort cour	Device SN: G1PL91W	000070 Verslor	53410_FSO5 11.4(1)87454				
Device Pa	ort						Selected D AG Po	ort 📕 Up 📕 Shutdow	n 🖾 VSL Po
		-10/100M On-Line Ruding-ACT	9 10 11 11 10 10 10 10 10 10 10 10 10 10	BALIOSOFER RECO			Cooper	Fiber 400b	40Gb/Solite
SIT NOIS: U	Trunk Port 🕑 No						Copper	Fiber 4000	40GD(Spirite
Port Info	rmation o								
		Output Rate *	Status(Port real sneed) *	InOctets/OutOctets	UnderSize/OverSize	CRC/ECS Error		Collision Count	
Port Info Port Gi0/1	Input Rate =	Output Rate :	Status(Port real speed) : Connected(1000M)	InOctets/OutOctets 44392388/5171881	UnderSize/OverSize	CRC/FCS Error		Collision Count	
Port Gi0/1	Input Rate : 2.2K	0.1K	Connected(1000M)	44392388/5171881	0/0	0/0		0	
Port	Input Rate :								
Port Gi0/1 Gi0/2	Input Rate : 2.2K 0K	0.1К ОК	Connected(1000M) Not Connected	44392388/5171881 0/0	0/0	0/0		0	
Port Gi0/1 Gi0/2 Gi0/3	Input Rate = 2.2K OK OK	0.1К ОК ОК	Connected(1000M) Not Connected Not Connected	44392388/5171881 0/0 0/0	0/0 0/0 0/0	0/0 0/0 0/0		0	
Port Gi0/1 Gi0/2 Gi0/3 Gi0/4	Input Rate = 2.2К ОК ОК ОК	0.1К ОК ОК	Connected(1000M) Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0	0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0		0 0 0	
Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5	Input Rate : 2.2K OK OK OK	0.1K OK OK OK	Connected(1000M) Not Connected Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0		0 0 0 0	
Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6	Input Rate : 2.2К ОК ОК ОК ОК ОК	0.1K OK OK OK	Connected(1000M) Not Connected Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0		0 0 0 0	
Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7	Input Rate : 2.2K 0K 0K 0K 0K 0K 0K	0.1K OK OK OK OK	Connected(1000M) Not Connected Not Connected Not Connected Not Connected Not Connected	44392388/5171881 0/0 0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0 0/0	0/0 0/0 0/0 0/0 0/0 0/0		0 0 0 0 0	

#### VLAN

Two tab pages are available on the VLAN page, that is, VLAN Settings and Trunk Port.

# **VLAN Settings**

The following figure shows the VLAN Settings page.

#### Figure 1-5 VLAN Settings

VLAN Settings Trunk Port				
+ Batch Add VLAN + Add VLAN	Batch Delete			
VLAN ID =	VLAN name	Port	Action	
			<b>F</b> '	
1	VLAN0001	Gi0/1-12		
	VLAN0001	GIU/1-12		

#### Adding VLAN

To add a VLAN, you must input the VLAN ID and you can input other information as required. After that, click **Save.** The newly added VLAN is displayed in the VLAN list after an "Add succeeded." message is displayed.

#### Editing a VLAN

After you click **Edit** in the Action column, the information of the corresponding VLAN is displayed on the page. After editing the information, click **Save**. An "Edit succeeded." message is displayed.

# Deleting VLAN

1) You can select multiple VLANs from the VLAN list and click Delete Selected VLAN to delete the VLANs in batches.

2) After you click Delete in the Action column, an "Are you sure you want to delete the VLAN?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed. VLAN 1 is the default VLAN and cannot be deleted.

# NOTE:

VLAN 1 is the default management VLAN. This VLAN can only be modified and it cannot be deleted. Before changing the IP address of VLAN 1, ensure that the new IP address is reachable. After the change is successful, the Web page automatically jumps to the login page and the user must log in again. If the Web page does not jump to the login page and a "page not found" message is displayed, it is possible that the IP address is not reachable. In this case, check the network connection.

# L Trunk Port

The following figure shows the Trunk Port page.

# Figure 1-6 Trunk Port

VLAN Settings Trunk Port	
O Note: If a port allows multiple VLAN packets to go through configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.	
Select All Deselect All Batch Delete No Data	
Native VLAN  Runge(1-4094) Allowed VLAN Runge(1-4094)	
Select Port	🖬 Available 📑 Unavailable 📑 Selected 📑 AG Po
Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.           Save         Cancel	Copper 📰 Fiber 📰 40Gb 📷 40Gb(Splitted

## Adding trunk port

Select a panel port, specify Native VLAN and Allowed VLAN (for example, 3-5, 8, and 10), and click **Save**. A "Configuration succeeded." message is displayed. In this case, the newly added trunk port is displayed in the trunk port list.

## Editing trunk port

After you click a certain trunk port in the trunk port list, the information of this trunk port is displayed on the page. After editing the information, click **Edit**. A "Configuration succeeded." message is displayed.

# Deleting trunk port

After you move the cursor to a certain trunk port in the trunk port list and click **Delete**, an "Are you sure you want to delete the trunk port?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

#### Deleting trunk ports in batches

After selecting the trunk ports to be deleted in the trunk port list and click **Batch Del**, an "Are you sure you want to delete the trunk ports?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

# Port

The Port menu allows you to perform basic settings on a port and configure port aggregation, port mirroring, and port rate limiting.

# Basic Settings

Figure 1-7 Basic Settings

+ Batch Add	+ Add SVI						
Port							
Port	Up/Down	IP	Mask	IPv6		Description	Action
VLAN 1	Up	10.32.130.89	255.255.255.0				C D
tal 1 item(s)	1 > Items per page	: 10 v 1 GO					
Port							
Port	Up/Down	Port Type	Access VLAN	Native VLAN	Permit VLAN	Description	Action
Gi0/1	Up	ACCESS	1	1			e e
GI0/2	Up	ACCESS	1	1			e e
GI0/3	Up	ACCESS	1	1			e e
Gi0/4	Up	ACCESS	1	1			
Gi0/5	Up	ACCESS	1	1			e e
Gi0/6	Up	ACCESS	1	1			C E
Gi0/7	Up	ACCESS	1	1			6
GI0/8	Up	ACCESS	1	1			
	Up	ACCESS	1	1			6
Gi0/9							C E

# Basic port settings

Select the port to be configured, and then select Status, Speed, and Working Mode. Keep indicates that the original configuration is retained. During batch setting, you can select Keep to implement batch setting of one or two items.

# Editing port

After you click **Edit** in the **Action** column, the information of the corresponding port is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

# ▶ Aggregate Port

The following figure shows the Aggregate port page.

Figure1-8 Aggregate Port

Port Settings Aggregate port Port Mirroring Rate Limiting	
Global Configuration	
Note: the aggregate port is used to perform traffic allocation according to the selected load-balance algorithm.	
Load-balance Source MAC and Destination MAC V Sove Default Settings	
Aggregation port settings	
Nete:     In order to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined into one logical     + An aggregate port contains up to sight number ports, and the aggregate port load balances traffic areas these physical ports	
Select All     Deselect All     Batch Delete     No Data	
Aggregate Port ID*         Rerepet-120;           Port Type         Is 12 Port(Switching Port)         L3 Interface(Routing Interface)	
Select Port	Available Unavailable Selected ID AG Port
Note:Click and held the left button as you drag the pointer across the section to select multiple ports. Add Cancel	Copper De Piber 40Gb 2003 40Gb(Spilted)

#### Adding aggregate port

After specifying Aggregate Port ID and selecting the member port, click **Add.** A "Configuration succeeded." message is displayed. The newly added aggregate port is displayed on the panel.

#### Editing an aggregate port

The aggregate ports displayed on the panel are unavailable ports. To edit them, you can click a certain aggregate port in the aggregate port list. After that, the member port becomes a selected port. You can click this port to deselect it. After that, you can click **Edit** to modify the aggregate port.

Deleting an aggregate port

After you move the cursor to an aggregate port in the aggregate port list and click **Delete**, an "Are you sure you want to delete the aggregate port?" message is displayed. After you confirm the operation, the aggregate port becomes an available port on the panel.

#### Deleting aggregate ports in batches

After you select the aggregate ports to be deleted in the aggregate port list and click **Batch Del**, an "Are you sure you want to delete the aggregate port?" message is displayed. After you confirm the operation, these aggregate ports become available ports on the panel. **NOTE:** 

The port enabled with ARP check, anti-ARP-spoofing, or MAC VLAN, and the monitoring port in port mirroring cannot be added to the aggregate port, and they are displayed as unavailable ports on the panel. After you move the cursor to an unavailable port, a message is displayed to indicate that some function has been enabled for the port so the port is unavailable.

# **V** Port Mirroring

The following figure shows the Port Mirroring page.

Figure 1-9 Port Mirroring

Port Settings	Aggregate port	Port Mirroring	Rate Limiting							
	the capability to send a copy of networks the sense of th	ork packets seen on the source p	ort to the destination port for an	alysis by a networl	k analyzer. Traffic on	multiple source ports	can be mirrored to one single	e destination port.		
Select All Des	ielect All 🔋 Batch Delete									
	ange (1-4) I Packets	~								
Select Source Port ()	iou can select multiple ports, bu ] Deselect	it it may affect device perform	nance.)				Availabl	le 🔳 Unavailable	Selected	AG Port
1.42 3.44	56 78									
Note:Click and hold th	e left button as you drag the p	ointer across the section to se	elect multiple ports.				Copper	Fiber	40Gb	40Gb(Splited)
	(You can select only one port	0								
Deselect	5-6 7-8		I				Availabi	le 🔳 Unavailable	Selected	AG Port
Note:Click and hold th	e left button as you drag the p	ointer across the section to s	elect multiple ports.				Copper	Fiber	40Gb	40Gb(Splited)
Save	Caricel									

Initially, the Port Mirroring page is in edit state because only one mirroring port is allowed to be set on the Web. Two panels are available on the page. The port selected from the upper panel will serve as a source port (mirrored port, multiple mirrored ports are allowed). Only one port can be selected from the lower panel to serve as the destination port (mirroring port). After selecting or modifying a port on the panel, click **Save.** A "Configuration succeeded." message is displayed.

#### NOTE:

The current port mirroring status is displayed on the panel, which is in edit state. If you don't want to edit a port after modifying it, you can click Refresh to make the panel display the current status of the port mirroring.

#### NOTE:

The member port of the aggregate port cannot serve as a destination or source port. A port cannot serve as a destination port and source port at the same time.

#### ▶ Rate Limiting

The following figure shows the Rate Limiting page.

#### Figure 1-10 Rate Limiting

Port Settings	Aggregate port	Port Mirroring	Rate Limiting			
+ Batch Add	Batch Delete					
Port		Input Rate-L	imit (KBps)	Output Rate-Limit (KBps)	Action	
				-		
				No Found		

#### Adding rate limiting port

To add a rate limiting port, you must specify at least the input rate limit or output rate limit, and click Save. The new rate limiting port is

displayed in the rate limiting port list after a "Configuration succeeded." message is displayed.

#### Editing rate limiting port

After you click **Edit** in the Action column, the information of the corresponding rate limiting port is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

#### Deleting rate limiting port

1) You can select multiple ports from the rate limiting port list and click **Batch Delete** to delete the ports in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the port configuration?" is displayed. After you confirm the operation, a "Delete succeeded." message is displayed.

#### Restart

The following figure shows the Restart page.

#### Figure 1-11 Restart

Restart	
0 Note: Click Restart' to restart the device. Please wait a few minutes and the page will be refreshed after restart.	
Restart	

After you click **Restart**, an "Are you sure you want to restart the device?" message is displayed.

After you confirm the operation, the device is restarted. The restart takes several minutes. Please wait with patience. The page is refreshed automatically after the device is restarted.

#### 1.3.2 Network

You can access secondary menus through the primary menu Network, including MAC Address, Routing, STP,, IGMP Snooping, Authentication and DHCP Relay.

#### **MAC Address**

Two tab pages are available on the MAC Address page, that is, Static Address Settings and Filtering Address Settings.

#### ↘ Static Address Settings

Figure 1-12 Static Address Settings

Note: The switch forwards	data according the MAC address inside the da	sta frame. If you configure MAC-port bindi	ng on a network device manually, after you add a	static address, the switch that receives the packet with the same destination address forwar
it to the specified port. Wit	th 802.1X authentication enabled, you can imp	lement authentication exemption by bindir	ng MAC address with port.	
+ Add Static Address	Delete Static Address			
Port	M	AC Address	VLAN ID	Action
			No Found	
Total 0 item(s)	Items per page: 10 v 1			

#### • Adding Static Address

To add a static address, input the MAC address, VLAN ID and select a port, and then click **Save**. The newly added static address is displayed in the address list after a "Configuration succeeded." message is displayed.

#### • Deleting Static Address

1) You can select multiple static addresses and click Delete Static Address to delete the addresses in batches.

2) After you click **Delete** in the Action column, an "Are you sure you want to delete the static address?" message is displayed. After you confirm the operation, a "Delete succeeded." message is displayed.

# ↘ Filtering Address Settings

#### Figure 1-13 Filtering Address Settings

tatic Address Settings	Filtering Address Settings			
Note: The switch forwards of the switch	lata according the MAC address inside the data fr	ame. If a switch receives a packet with the source/desti	nation MAC address which is configured as a filter address, it discards the packet. W	ou can prevent the ARP attack by
configuring a filter address t	he same as the MAC address of ARP packets.			
+ Add Filter Address	Delete Filter Address			
MAC Address		VLAN ID	Action	
		· •		
		No Found		
Total 0 item(s)	tems per page: 10 v 1			

#### • Adding Filtering Address

To add a filtering address, input the MAC address and VLAN ID, and then click **Save**. The newly added filtering address is displayed in the address list after a "Configuration succeeded." message is displayed.

#### • Editing Filtering Address

After you click **Edit** in the Action column, the information of the corresponding filtering address is displayed on the page. After editing the information, **click** Save. A "Configuration succeeded." message is displayed.

#### • Deleting Filtering Address

You can select multiple filtering addresses and click **Delete Filter Address** to delete the addresses in batches.
 After you click **Delete** in the Action column, an "Are you sure you want to delete the filter address?" message is displayed. After you confirm the operation, a "Delete succeeded." message is displayed.

#### Routing

The Route Settings page allows you to manage routes. The following figure shows the Route Settings page.

#### Figure 1-14 Route Settings

Route	Settings						
1 No	te: Route selection points based routin	g and a backup route when the prima	ry route does not take effect, it will tak	e a backup route to the backup route	in accordance with the priority level co	nfigured to go, the backup route priori	ity 1 high priority than a backup route
to t	the 2.						
+ Ad	d Static Route + Add Do	efault Route 🔋 Delet	e Selected Route				
	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Туре	Action
	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Type Default Route	Action

# Adding static route

To add a static route, you must set IP Type, Destination Subnet, Subnet Mask, and Next Hop Address. After that, click **Save**. The newly added route is displayed in the route list after a "Save succeeded." message is displayed.

#### Editing route

After you click **Edit** in the **Action** column, the information of the corresponding route is displayed on the page. After editing the information, click **Save**. A "Save succeeded." message is displayed.

# Deleting route

1) You can select multiple routes from the route list and click **Delete Selected Route** to delete the routes in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the route?" is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

#### Adding default route

To add the default route, you must set IP Type and Next Hop Address. After that, click **Save**. The newly added route is displayed in the route list after an "Save succeeded." message is displayed.

# STP

The STP Global Settings page allows you to set the global parameters and STP ports.

# **↘** STP Global Settings

Figure 1-15 STP Global Settings

P Global Settings	STP Port Settings	RLDP Settings		
Global Configura	tion			
STP				
Priority 8		Hello Time 2		
Aging Time 20		Forward Delay 15		
STP Mode MSTP	~			
MST Name		MST Version 0		
MST Configurati	Save			
<b>1</b> Note: It is recommen	ded to disable STP before configuring a	n instance and enable STP again after configuration	so as to ensure the stability and convergence of netw	ork topology.
+ Add Instance	Delete Selected Instance	e		
	imber	VLAN	Priority	Action
Instance Nu				
Instance Nu     0		ALL	8	Default instance. Cannot be edited.

You can configure STP global parameters. When MSTP is selected from the STP Mode drop-down list, you can configure the MST instance.

#### Adding instance

To add an instance, you must input the instance value and VLAN range and you can input other information as required. After that, click **Save**. The newly added instance is displayed in the instance list after a "Configuration succeeded." message is displayed.

#### Editing instance

After you click **Edit** in the Action column, the information of the corresponding instance is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

#### Deleting instance

1) You can select multiple instances from the instance list and click **Delete Selected Instance** to delete the instances in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the instance?" message is displayed. After you confirm the operation, a "Delete succeeded." message is displayed. Instance 0 is the default instance and cannot be deleted.

# **↘** STP Port Settings

Figure 1-16 STP Port Settings

TP Global Settings	STP Port Settings	RLDP Settings					
+ Batch Add							
<b>Note:</b> It is recommended t	o enable Port Fast on the port connecte	ed to the PC.					
Port	State	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance Cost Priority	Acti n
Gi0/1	Up	Disabled	Disabled	Null	Point To Point	0 20000 128	
Gi0/2	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/3	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Ø
Gi0/4	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/5	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Ø
Gi0/6	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/7	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Ø
Gi0/8	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/9	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/10	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Ľ

# Batch setting

Specify Protection Mode, Port Fast, BPDU Guard, Connection Mode, and Port Priority, and select ports for batch setting.

# Editing STP port

After you click **Edit** in the **Action** column, the information of the corresponding port is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

# **↘** RLDP Settings

Figure 1-17 RLDP Settings

TP Global Settings	STP Port Settings	RLDP Settings			
Global configurat	tion				
Note: RLDP enables yo	ou to detect link failure quickly. RLDP co	an run on the port only after it is a	mabled globally.		
RLDP:	D				
Detection Interval:	3	Detection Count:	2		
errdisable recovery:					
	Save				
Port Configuratio	on				
Note: 1. Enabling RLD	P on the port can avoid broadcast s		mmended to enable RLDP on the port com		
			e link to be enabled with RLDP. It is recomm section on a member port will be synchroniz	ended to configure RLDP to monitor the link between two switches; ed to other member ports.	
+ Add Port	Batch Delete				
Port		De	tection Type:Troubleshooting	Action	
			No Found		
Total 0 item(s)	> Items per page: 10	1 GO			

#### 1. Global Configuration

Enable/Disable RLDP by turning on/off the switch. After setting detection interval and count, click Save. A "Configuration succeeded." message is displayed.

# 2. Port Configuration

#### Adding RLDP Port

Select detection mode, troubleshooting mode ,and port. After that, click **Save**. The newly added RLDP port is displayed in the RLDP port list after a "Configuration succeeded." message is displayed.

## Editing RLDP Port

After you click **Edit** in the **Action** column, the information of the corresponding RLDP port is displayed on the page. After editing the information, click **Save**. An "Edit succeeded." message is displayed.

## Deleting RLDP Port

1) You can select multiple RLDP ports from the RLDP port list and click **Delete Selected Port** to delete the RLDP ports in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the item?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

#### **IGMP Snooping**

The following figure shows the IGMP Snooping Settings page.

#### Figure 1-18 IGMP Snooping Settings

MP Snooping Settings				
Note: On layer 2 devices, multicast fram	nes are flooded to all ports, causing storm and consumi	ng much bandwidth. IGMP Snooping is used t	o find out on which port there is an IGMP subscriber a	and only send IGMP traffic to the port, so as to save bandwidth
IGMP Snooping				
+ Add Profile 🗑 Delete So	elected Profile			
Profile ID	Multicast Address	Policy Action	Application Port	Action
		No Found		
Total 0 item(s) < > Items	per page: 10 v 1 GO			

#### Adding profile

To add a profile, you must input the profile identifier and multicast address range and you can input other information as required. After that, click **Save**. The newly added profile is displayed in the profile list after an "Add succeeded." message is displayed.

# Editing profile

After you click **Edit** in the Action column, the information of the corresponding profile is displayed on the page. After editing the information, click **Save**. An "Edit succeeded." message is displayed.

#### Deleting profile

1) You can select multiple profiles from the profile list and click **Delete Selected Profile** to delete the profiles in batches.

2) After you click **Delete** in the **Action** column an "Are you sure you want to delete the profile?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

#### **DHCP** Relay

The following figure shows the DHCP Relay Settings page.

#### Figure 1-19 DHCP Relay Settings

DHCP Relay
Note: DHCP relay can centrally manage IP address assignment for large number of subscribers in different subnets. The DHCP relay agent forwards client-originated DHCP packets to a DHCP server and then forwards the server-to-client reply to the client.
DHCP relay IPV4 configuration
DHCP Relay:
DHCPv6 relay configuration
G Select All 🖸 Deselect All 😰 Batch Delete
No Data
Select Layer 3 interface: Vian 1 v
DHCPv6 server address:
Save Cancel

When DHCP Relay is enabled, you can configure multiple DHCP server addresses.

#### Authentication

The Authentication page allows you to set Eportalv2 and Advanced.

# Leportalv2

The following figure shows the Eportalv2 page.

# Figure 1-20 Eportalv2

portal Type:	⊖eportalv1		
erver IP:	*		
edirection URL:	*		
ortal Key:			
uthentication	All Servers V [Radius Server Settings]		
erver:			
ccounting Server:	All Servers 🗸		
NMP Server:	[SNMP Server] *		
ort:			
All 🔡 Invert 🗵	Deselect	🖉 Available 🖉 Unavailable 📃 S	Selected 🛛 🖪 AG

Enter the server IP address and redirection URL, and then click Save. A "Configuration succeeded." message is displayed.

# کا Advanced

The following figure shows the Advanced page.

# Figure 1-21 Advanced Settings

Eportalv2 Advar	nced	
Max HTTP Session Count:	255	(Range: 1-255. Default: 255) The configuration prevents an unauthorized user from sending excessive HTTP requests.
Redirection Timeout:	3	(Range: 1-10. Default: 3)The configuration prevents an unauthorized user from occupying the TCP connection without sending GET/HEAD packets.
Update Interval:	180	(Range: 30-3600. Default: 180) The configuration sets the time interval to update online user information.
Redirection HTTP Port:	80	(Range: 1-65535) Please use ',' to separate port numbers. You can configure up to 10 port numbers.
Authentication-Exempted	All users(including unauthorized users) (	can access the server IP address. You can configure up to 50 IP addresses.
Network Resource:	IP: Mask:	× +Add
Authentication-Exempted User	The user can access the network withou	t authentication. You can configure up to 50 IP addresses.
IP:	IP: Mask:	× +Add
	Save Clear	

You can set multiple authentication-exempted network resources and user IP addresses. Click **Save**, and a "Configuration succeeded." message is displayed.

#### 1.3.3 Security

You can access secondary menus through the primary menu Security, including DHCP Snooping, Anti-ARP-Attack, IP Source Guard, Port Security, NFPP, and Storm Control.

# **DHCP Snooping**

The following figure shows the DHCP Snooping Settings page. Figure 1-22 DHCP Snooping Settings

DHCP Snooping	
<ul> <li>Note:</li> <li>DHCP snooping is used to filter DHCP packets received on an untrusted port from outside the network or firewall. The DHCP request packet is forwarded to the trusted port. The DHCP</li> <li>The port connected to the DHCP server is configured as a trusted port generally.</li> </ul>	reply packet is forwarded only if it is from a trusted port.
DHCP Snooping	
Select Port	
및 All 땳 Invert 또 Deselect	Available Unavailable Selected 🛙 AG Port
Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.	Copper 📰 Fiber 📰 40Gb 📷 40Gb(Splited)
Save Display DHCP Snooping Trusted Port	

The port connected to the DHCP server must be configured as DHCP trusted port, and the DHCP server connected to a non-trusted port cannot work properly. If the selected port on the panel is a DHCP trusted port. You can directly select a port on the panel and click the

Save button.

#### Anti-ARP-Attack

The Anti-ARP-attack page allows you to perform anti-ARP-spoofing settings, ARP check settings, DAI settings, and ARP entry settings.

# ↘ Anti-ARP-Spoofing

Figure 1-23 Anti-ARP-Spoofing

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries	
Note: It is configured on on	ly the port connected to the cl	ient to prevent ARP spoofing.		
+ Add Port	Batch Delete			
Filtering P	ort		IP	Action
				No Found
Total 0 item(s)	> Items per page:	10 ~ 1		

## Adding filtering port

To add a filtering port, you must input the IP address. After that, click **Save.** The newly added filtering port is displayed in the filtering port list after an "Add succeeded." message is displayed.

#### Editing filtering port

After you click **Edit** in the Action column, the information of the corresponding filtering port is displayed on the page. After editing the information, click **Save**. An "Edit succeeded." message is displayed.

#### Deleting filtering port

You can select multiple filtering ports from the filtering port list and click **Delete Selected Port** to delete the filtering ports in batches.
 After you click **Delete** in the Action column, an "Are you sure you want to delete the port?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

# ARP Check

#### Figure 1-24 ARP Check

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries						
1 Note: ARP Check is used to	filter all ARP packets on the	logical port and discard invalid A	RP packets. It can effectively p	revent ARP Spoofing and improve n	etwork stability. A DHCP Snooping trust	ted port cannot be	enabled with ARP Chee	:k.	
Select Port									
의 All 끓 Invert 🗵 Desel	lect					Available	Unavailable	Selected	AG Port
1.*2 3.*4 5.*6	78		1						
Note:Click and hold the left bu	utton as you drag the po	inter across the section to se	elect multiple ports.			Copper	Fiber	40Gb	40Gb(Splited)
Save Display	ARP Check Port								

The selected port on the panel is enabled with ARP Check.

#### NOTE:

The selected port on the panel is enabled with ARP Check and is in edit state. If you don't want to edit a port after modifying it, you can click Display ARP Check Port to make the panel display the current status of the ARP check.

ARP check cannot be enabled on a DHCP Snooping trusted port.

# **凶** DAI Settings

# Figure 1-25 DAI Settings

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries	
VLAN DAI Configura	ation			
Note: The untrusted port of	orresponding to the DAI-enab	led VLAN intercepts all ARP req	uest and reply packets to discard invalid ARP packets	
No Data		atch Delete		
Note: Packets received on t	the trusted port skip DAI Inspe	ction as valid ARP packets.		
Select Port				
🖾 All 🔛 Invert 🗵 Dese	lect			🔳 Available 🛑 Unavailable 🛑 Selected 🔲 AG Po
12 34 56	78		i.	
Note:Click and hold the left b	utton as you drag the poi	nter across the section to se	elect multiple ports.	Copper Fiber 40Gb 40Gb(Splite
Save Displa				

#### 1. VLAN DAI settings

Click the add icon to add a VLAN enabled with the DAI function.

#### 2. DAI trusted port

The selected port on the panel is enabled with the DAI function.

#### NOTE:

The selected port on the panel is enabled with the DAI function and is in edit state. If you don't want to edit a port after modifying it, you can click Display Trusted Port to make the panel display the current status of the DAI trusted port.

# NOTE:

ARP check cannot be enabled on a DHCP Snooping trusted port.

# **↘** ARP Entries

#### Figure 1-26 ARP Entries

Dyn	amic Binding > Static Binding	Remove static Binding Binding		IP-based
	IP	MAC	Туре	Action
	10.32.130.10	8cec.4bbc.85ad	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.13	484d.7eab.ecb6	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.89	649d.9900.0402	Local ARP Entry	
	10.32.130.107	8cec.4b8d.9c43	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.254	782c.294b.a201	Dynamic Binding	Dynamic Binding > Static Binding

#### Remove Static Binding

1) You can select multiple dynamic binding from the ARP entry list and configure them as static binding in batches.

2) Click the **Dynamic Binding**>>**Static Binding** icon in the **Action** column. A "Configuration succeeded." message is displayed.

## Remove Static Binding

1) You can select and remove multiple static bindings from the ARP entry list.

2) Click the Remove static Binding icon in the Action column. A "Configuration succeeded." message is displayed.

#### Manual Binding

To add a static binding, you must configure IP Address and MAC Address. After that, click **Save**. The newly added static binding is displayed in the ARP entry list after a "Configuration succeeded." message is displayed.

#### **IP Source Guard**

The IP Source Guard page allows you to perform port settings and user binding.

# **Y** Port Settings

#### Figure 1-27 Port Settings

Port Settings	User Binding						
1 Note: IP Source Gu	ard is applied in combination with DHCP Snooping.	Port-based IP Source Guard takes eff	ect on only the untrusted port o	enabled with DHCP Snooping. Otherwise,	IP Source Guard does not take effect.		
+ Add Port	Batch Delete						
Port	Filter Type	Filter Mode	IP	MAC	VLAN ID	Action	
			No Found	κ.			
Total 0 item(s)	> Items per page: 10	1 GO					

# Adding IP Source Guard port

Enable the IP Source Guard port, specify Filter Type and Port, and click **Save**. The newly added IP Source Guard port is displayed in the IP Source Guard port list after a "Configuration succeeded." message is displayed.

# Editing IP Source Guard port

After you click **Edit** in the Action column, the information of the corresponding filtering port is displayed on the page. After editing the information, click **Save**. An "Edit succeeded." message is displayed.

#### Deleting IP Source Guard port

1) You can select multiple ports from the IP Source Guard port list and click **Delete Selected Port** to delete the ports in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the item?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

#### **User Binding**

#### Figure 1-28 Use Binding

	e port filters all non-DHCP IP packets. After configure	d with the static IP address, the port allows specified IP	packets to pass through.	
□ MAC	IP	VLAN ID	Port	Action
		Ŷ		

## Adding user binding

To add a user binding, you must set MAC Address, IP Address, and VLAN ID. After that, click **Save**. The newly added user binding is displayed in the user binding list after a "Configuration succeeded." message is displayed.

#### Editing user binding

After you click **Edit** in the Action column, the binding information of the corresponding user is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

## Deleting user binding

1) You can select multiple user bindings from the user binding list and click **Delete Selected Binding** to delete the user bindings in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the binding?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

## **Port Security**

# Basic Settings

Figure 1-29 Basic Settings

Basic Settings	Security Binding				
Note: It is generally	y applied to the scenario where the	accessed user has valid IP and MAC address o	or where the user accesses the network throug	a fixed port instead of changing IP/MAC address or	port number, or limits the number of MAC addresses on the
port to avoid attack	ks caused by MAC address depletion	n.			
+ Add Port	Batch Delete				
Port		Max Secure Address	Aging Time	Security Action	Action
			No Found		
Total 0 item(s)	> Items per page: 1	0 1 GO			

# Adding user binding

To add a user binding, you must input the IP address and you can input other information as required. After that, click **Save**. The newly added user binding is displayed in the security port list after a "Configuration succeeded." message is displayed.

# Editing security port

After you click **Edit** in the **Action** column, the binding information of the corresponding user is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

# Deleting security port

You can select multiple security ports from the security port list and click **Delete Selected Port** to delete the security ports in batches.
 After you click **Delete** in the **Action** column, an "Are you sure you want to delete the security port?" message is displayed. After you confirm the operation, a "Delete succeeded." message is displayed.

# ↘ Security Binding

Figure 1-30 Security Binding

asic Settings	Security Binding				
Note: Port Security is a	used to allow only the packet whose source MAC ac	dress is consistent with the secure address to enter the switch.			
+ Add Address	Batch Delete				
Port	IP	МАС	VLAN ID	Action	
		No Found			
otal 0 item(s)	> Items per page: 10 ~	1 GO			

# Adding security binding address

To add a security binding address, you must input the IP address and you can input other information as required. After that, click **Save**. The newly added security binding address is displayed in the security binding address list after a "Configuration succeeded." message is displayed.

#### Editing security port

After you click **Edit** in the **Action** column, the binding information of the corresponding user is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

# Deleting security binding address

1) You can select multiple addresses from the security binding address list and click **Delete Selected Address** to delete the addresses in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the port?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

#### NFPP

The following figure shows the NFPP Settings page.

Figure 1-31 NFPP



You can enable or disable various guard functions. After the setting, click **Save**. A "Save succeeded." message is displayed. To restore to the default settings, click **Restore Default Settings**.

# Storm Control

The following figure shows the Storm Control Settings page. Figure 1-32 Storm Control Settings

Add	d Port 🔋 🖲 Batch Delet	e			
	Port	Broadcast	Multicast	Unicast	Action
	Gi0/1	-	-	-	6 0
	GI0/2	-	-	-	C D
	GI0/3	-			区面
	GI0/4	-	-	-	<b>区 ①</b>
	GI0/5	-			区面
	GI0/6	-			<b>区 ①</b>
	GI0/7	-			区面
	GI0/8				2 6
	GI0/9				区面
	Gi0/10				

#### Adding storm control port

To add a storm control port, you must set at least Broadcast, Unicast, or Multicast. After that, click **Save**. The newly added storm control port is displayed in the storm control list after a "Configuration succeeded." message is displayed.

#### Editing storm control port

After you click **Edit** in the **Action** column, the information of the corresponding storm control port is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

#### Deleting storm control port

1) You can select multiple ports from the storm control port list and click **Delete Selected Port** to delete the ports in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the port?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

# 1.3.4 Advanced

#### **Port Protection**

The following figure shows the Port Protect Settings page. Figure 1-33 Port Protect Settings

Note: Proteced ports can not communicate with each other. The selected ports on the panel are the protected ports. Please click 'Display Protected Port' to refresh the panel.			
lect Port			
All 🖫 Invert 🗵 Deselect	Available	able Selected	🖪 AG P
		40Gb 4	

To set a port as a protection port, select a port on the panel and click Save. A "Save succeeded." message is displayed.

#### DHCP

DCHP allows you to perform DHCP settings and static address allocation, and access the client list.

# **DHCP Settings**

The following figure shows the DHCP Settings page.

Figure 1-34 DHCP Settings

DHCP Settings	itatic Address Client Displa	у				
+ Add DHCP Ø Excluded	d Address Range Batch Delete	рнср				
Name	IP Address Range	Default Gateway	Lease Time	DNS	Action	
			No Found			
Total 0 item(s)	ems per page: 10 🗸 1					

#### Adding DHCP

To add an address pool name, you must configure IP Address Range, Mask, Default Gateway, and Lease Time. After that, click **Save**. The newly added address pool name is displayed in the DHCP list after a "Save succeeded." message is displayed.

## Editing DHCP

After you click **Edit** in the **Action** column, the information of the corresponding DHCP is displayed on the page. After editing the information, click **Save**. A "Save succeeded." message is displayed.

# Deleting DHCP

1) You can select multiple DHCPs from the DHCP list and click **Delete Selected DHCP** to delete the DHCPs in batches.

2) After you click **Delete** in the Action column, an "Are you sure you want to delete the address pool?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

# Enabling DHCP

Turn on the DHCP service switch to enable the DHCP service.

# Static Address

The following figure shows the Client Display page.

#### Figure 1-35 Static Address

HCP Settings Static Address Client Display				
+ Add Static Address Batch Delete				
Client Name Client IP Mask	Gateway Address	Client MAC	DNS Server	Action
	No Found			
Total 0 item(s) < > Items per page: 10 v 1 GO				

#### Adding static address

To add a static address, you must configure Client Name, Client IP Address, and Client MAC Address and you can configure other parameters as required. After that, click **Save**. The newly added static address is displayed in the static address list after a "Save succeeded." message is displayed.

#### Editing static address

After you click **Edit** in the **Action** column, the information of the corresponding static address is displayed on the page. After editing the information, click **Save**. A "Save succeeded." message is displayed.

#### Deleting static address

1) You can select multiple static addresses from the static address list and click **Delete Selected Address** to delete the static addresses in batches.

2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the static address?" message is displayed. After you confirm the operation, a "Delete succeeded." message is displayed.

# Lient Display

The following figure shows the ACL List page. Figure 1- 36 Client Display

DHCP Settings	Static Address	Client Display				
+Bind MAC to Dy	namic IP 🗊 Batch Delete	e			IP-based	
□ IP		MAC	Lease Time	Allocation Type	Action	
			-			
			No Found			
Total 0 item(s)	< > Items per page	e: 10 • 1				

# Search by IP address

You can type an IP address in the search box for search.

# Binding MAC address to dynamic IP address

You can select multiple clients from the client list and click Bind MAC to Dynamic IP for binding.

#### ACL

# ACL List

The following figure shows the ACL List page. Figure 1-37 ACL List

ACL List ACL Time ACL Application	
ACL List	
ACL List   Add ACL   Delete ACL	
Access Rule	
+ Add Access Rule	
NO. Source IP/Wildcard Source Port Access Control Protocol	Destination IP/Wildc Destination port Time Period Status Action ard
14	Found
Total 0 item(s) < > items per page: 10 ~ 1 60	

#### Adding ACL

To add an ACL, click Add ACL, and perform settings on the displayed page (ACL List is mandatory). After that, click OK. If an "Add succeeded." message is displayed, the add operation is successful. In this case, the newly added ACL is displayed in the ACL List drop-down list.

#### Deleting ACL

Select the ACL to be deleted from the ACL List drop-down list and click Delete ACL. A "Delete succeeded.' message is displayed.

# Adding Access rule

To add an ACL rule, you must select the access control type, protocol, effective time, and IP address. After that, click Save. The newly added ACL rule is displayed in the ACL rule list after an "Add succeeded." message is displayed.

#### Editing access rule

After you click Edit in the Action column, the information of the corresponding ACL rule is displayed on the page. After editing the information, click Save. An "Edit succeeded." message is displayed.

### Deleting access rule

1) You can select multiple access rules from the ACL rule list and click Delete Selected Access Rule to delete the access rules in batches.

2) After you click Delete in the Action column, an "Are you sure you want to delete the access rule?" message is displayed. After you confirm the operation, a "Delete succeeded." message is displayed.

#### Moving access rule

Enter the serial number of the ACL to be moved and click Move. An "Operation succeeded." message is displayed.

# ACL Time

The following figure shows the ACL Time page.

#### Figure 1-38 ACL Time

ACL List ACL Time AC	CL Application			
<b>Note:</b> The ACL active time must be periodic.				
+Add Time Object	a Object			
Time Object	Day	Time Period	Action	
		No Feund		

## Adding ACL time

To add an ACL time, you must configure Time Object, Day and Time Period. After that, click Save. The newly added ACL time is displayed in the ACL time list after a "Save succeeded." message is displayed.

#### Editing ACL time

After you click Edit in the Action column, the information of the corresponding ACL time is displayed on the page. After editing the information, click Save. A "Save succeeded." message is displayed.

#### Deleting ACL time

You can select multiple time objects from the ACL time list and click Delete Selected Time Object to delete the time objects in batches.

# **凶** ACL Application

The following figure shows the ACL Application page.

Figure 1-39 ACL Application

# Add ACL application

To add an ACL application, you must set the ACL application time and select ACL, filtration direction, and port. After that, click Save. The newly added ACL application is displayed in the ACL application list after a "Configuration succeeded." message is displayed.

#### Editing ACL application

After you click Edit in the Action column, the information of the corresponding ACL application is displayed on the page. After editing the information, click Save. A "Configuration succeeded." message is displayed.

# Deleting ACL application

You can select multiple ports from the ACL application list and click Delete Port to delete the ports in batches.
 After you click Delete in the Action column, an "Are you sure you want to delete the ACL application?" message is displayed.
 After you confirm the operation, a "Delete succeeded." message is displayed.

# QoS

# Lass Settings

The following figure shows the Class Settings page. Figure 1-40 Class Settings

Class Settings	Policy Settings	Flow Settings			
<b>()</b> Note: Classification is	s used to identify and mark certain	data flows that match the ACL rule.			;
+ Add Class	🗊 Batch Delete				
Class Name	9	ACL		Action	
			No Found		
otal 0 item(s)	> Items per page: 1	0 × 1 GO			

#### Adding class

To add a class, you must select the class name and select an ACL from the ACL list. After that, click Save. The newly added class is displayed in the class list after an "Add succeeded." message is displayed.

#### Editing class

After you click Edit in the Action column, the information of the corresponding class is displayed on the page. After editing the information, click Save. An "Edit succeeded." message is displayed.

#### Deleting class

1) You can select multiple classes from the class list and click Delete Selected Class to delete the classes in batches.

2) After you click Delete in the Action column, an "Are you sure you want to delete the item?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

# ▶ Policy Settings

The following figure shows the Policy Settings page. Figure 1-41 Policy Settings

ass Settings	Policy Settings	Flow Settings				
Note: The policy is u	sed to constrain the bandwidth th	at the classified data flow consumes.				
Policy Setting	gs					
Policy List	~	+ Add Policy 🗇 Delete Policy	]			
Policy Rule						
+Add Policy	Rule Batch Delet	te				
Class N	Jame	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action	
Class N	lame	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action	
Class N	Vame	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action	
Class N	Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action	
Class N	Vame	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action	
Class N	Name	Bandwidth (KBps)	Ť	Bandwidth Violation Disposal	Action	

# Adding policy

To add a policy, you must set the policy name. After that, click Save. The newly added policy is displayed in the policy list after an "Add succeeded." message is displayed.

#### Deleting policy

Select a certain policy form the policy list and click Delete. An "Are you sure you want to delete the item?" message is displayed. After you confirm the operation, a "Delete succeeded." message is displayed.

## Adding policy rule

To add a policy rule, you must configure Bandwidth and Burst Traffic and you can configure other parameters as required. After that, click Save. The newly added policy rule is displayed in the policy rule list after an "Add succeeded." message is displayed.

## Editing policy rule

After you click Edit in the Action column, the information of the corresponding policy rule is displayed on the page. After editing the information, click Save. An "Edit succeeded" message is displayed.

#### Deleting policy rule

1) You can select multiple rules from the policy rule list and click Delete Selected Rule to delete the rules in batches.

2) After you click Delete in the Action column, an "Are you sure you want to delete the item?" message is displayed.

After you confirm the operation, a "Delete succeeded." message is displayed.

# ▶ Flow Settings

The following figure shows the Flow Settings page.

Figure 1-42 Flow Settings

Class Settings	Policy Settings	Flow Settings				
Note: The policy is	used to constrain input and output	flows (Input and output flows of one port m	ust be in the same trust mode but they can be	onfigured with different policies)		
+ Add Port	🖬 Batch Delete					
Port		Direction	Policy Name	Trust Mode	Action	
			No Found			
otal 0 item(s)	> Items per page: 1	0 • 1 GO				

#### Adding application policy port

To add an application policy port, you must select the rate limiting direction, trust mode, policy list, and port. After that, click Save. The newly added application policy port is displayed in the application policy port list after an "Add succeeded." message is displayed.

# Deleting application policy port

You can select multiple ports from the application policy port list and click Delete Selected Port to delete the ports in batches.
 After you click Delete in the Action column, an "Are you sure you want to delete the item?" message is displayed.
 After you confirm the operation, a "Delete succeeded." message is displayed.

#### 1.3.5 System

The system management page allows you to perform system settings, system upgrade and configuration management and configure administrator permissions.

#### **System Settings**

Seven tab pages are available on the system setting page, that is, System Time, Password, Restart, Reset, Enhancement, SNMP, and DNS.

## System time

The following figure shows the System Time page.

#### Figure 1-43 System Time

System Time	Password	Reset	Enhancement	SNMP	DNS		
Current Time	2022-3-24-15:3	6:00					
Reset Time	2022-3-23 15:35						
Time Zone	UTC+0(GMT)		~				
Time Synchronization	Automatically syn	chronize with an In	 ternet time server(Please set	t <u>DNS Server f</u> irst, c	otherwise the syster	time will not be synchronized.)	
	Save						
				( <u>0110 361 (01</u> 1113), C	and more the system	une un not de granomacos	

#### • System time

The current system time is displayed on the page. You can set the current system time manually. Alternatively, you can select Automatically synchronize with an Internet time server for time setting. After that, click Save. A "Configuration succeeded." message is displayed.

When the management IP address changes, you must ensure that the new IP address is reachable. Otherwise, you cannot login the Web-based management system.

# **凶** Password

The following figure shows the Password page. Figure 1-44 Password

System Time	Password	Reset	Enhancement	SNMP	DNS
Web Managem	ent Password				
5					
Username *					
Old Password *					
New Password *					
Confirm Password *					
Commin Password *					
	Save				
<b>T</b> 1 (D			D.		
Telnet Password	d(leinet and En	able Passwor	d)		
New Password*					
Confirm Password*					
Commin Password*					
	Save				

#### Modifying the Web-based NMS password

To modify a Web user password, you need to input the old password and input the new password twice. When you input an incorrect old password, an "Incorrect old password" message in red is displayed. In this case, you must input a correct old password and click Save. **NOTE:** 

When you change the Web management password, the enable password is changed accordingly by default.

#### Modifying the telnet authentication password

You do not need to input the old password before modifying the telnet password. Instead, you only need to input the same new password twice. Other steps are the same as those for modifying the superuser password.

# **↘** Restoring factory settings

The following figure shows the Reset page. Figure 1-45 Reset

System Time	Password	Reset	Enhancement	SNMP	DNS	
estore Factor	y Settings					
Note: Note: A	fter the device is reset to th	ne factory default setting	gs, all configurations will be rem	noved. Please <b>Export C</b> i	nt Configuration before resetting the device.	
Restore Factory	Settings Export C	urrent Configuration	1			
Display Curr	ent Configuratio	on				
Display Current C	onfiguration					
Display Current C	onfiguration					
Display Current C	onfiguration					
Display Current C	onfiguration				Ý	
Display Current C	onfiguration				No Found	
	onfiguration				No Found	
nport/Export	Configuration	page during import, o	or import will fail. If you want	to apply the new cont	No Found	e effect.
nport/Export	Configuration	page during import, o	_	to apply the new conf		e effect.

# Importing/exporting configuration

You can import configuration to modify the device configuration and restart the device for the configuration to take effect. You can export current configuration as backup.

Restoring factory settings

You can click Restore Factory Settings to restore the current configuration to factory settings.

# کا Enhancement

The following figure shows the Enhancement page.

Figure 1-46 Enhancement

System Time	Password	Reset	Enhancement	SNMP	DNS
Basic Informati	on				
Web Access Port*	80		]		
Login Timeout	15 min		•		
Device Location	wuhanfeisu				
Access Redirection	HTTP Redirection	to HTTPS			
	Save				

Specify Web Access Port (mandatory) and specify Login Timeout and Device Location as required. After that, click Save. A "Configuration succeeded." message is displayed.

# SNMP

The following figure shows the SNMP page.

# Figure 1-47 SNMP

System Time	Password	Reset	Enhancement	SNMP	DNS
1 Note: Either SNMP	Pv2 or SNMPv3 is supported				
SNMP Version	●v2 ○v3				
Device Location					
SNMP Community	*				
Trap Community					
Trap Recipient Add	Iress *				
	Save				

On this page, SNMP Version, Device Location, SNMP Password, and Trap Password are mandatory and other parameters are optional. After the setting, click Save. A "Configuration succeeded." message is displayed.

# DNS 🖌

The following figure shows the DNS page.

Figure 1-48 DNS

System Time	Password	Reset	Enhancement	SNMP	DNS	
DNS Server 1			Ð			
	Save					

Specify DNS Server and click Save. A "Configuration succeeded." message is displayed.

# System Upgrade

Two tab pages are available on the system upgrade page, that is, Upgrade Local and Upgrade Online.

# └ Upgrade Local

The following figure shows the Upgrade Local page.

# Figure 1-49 Upgrade Local

Upgrade	Local
1 Note: Ple	ease download the corresponding software version from the official website, and then upgrade the device with the following tips.
Tips: 1. N	Viake sure that the software version (main program or Web package) matches the device model. 2. The page may have no response during upgrade. Please do not power off or restart the device until an upgrade succeeded message is displayed.
File Name	Browse File

Click file..., select a bin file stored locally, and click Upgrade to start local upgrade.

# System Logging

Two tab pages are available on the system log page, that is, Log Server Settings and Display System Log.

# **└** Log Server Settings

The following figure shows the Log Server Settings page.

Figure 1-50 Log Server Settings

Log Server Settings	Display System Log
1 Note: Logging is rated	l on 8 different levels: 0-Emergency, 1-Alert, 2
Server Logging	
Server IP*	
Logging Level	Informational(6)
	Save

Set various parameters such as Server IP Address and Logging Level. The device sends the SYSLOG log to the corresponding server after the configuration is complete.

# ▶ Display System Log

The following figure shows the Display System Log page. Figure 1-51 Display System Log

Log Server Settings	Display System Log	
System Log (Show	the last 200 logs)	
Update Log		
Syslog logging: enabled		
Console logging: level debu		_
Monitor logging: level debu		_
Buffer logging: level debugg	ing, 49 messages logged	_
Standard format:false		_
Timestamp debug message		
Timestamp log messages: d		
Sequence-number log mess		
Sysname log messages: disa		
Count log messages: disable	e ional, 49 message lines logged,0 fail	
Log Buffer (Total 131072 Byte		
	5, nave written 22:0, E-6-RCVDTCBPDU: Received to bpdu on port GigabitEthernet 0/1 on MST0.	
	E-6-RCVDTCBPDU: Received to bpdu on port GigabitEthernet 0/1 on MST0.	
	TO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to up.	
	E-5-TOPOTRAP: Topology Change Trap for instance 0.	
	TO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up.	
	PDOWN: Interface GigabitEthemet 0/1, changed state to up.	
	E-5-ROOTCHANGE: Root Changed for instance 0: New Root Port is GigabitEthernet 0/1. New Root Mac Address is 00d0.f822.33d2.	
	TO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to down.	
444 - 04 45 04 54 04 INISDOO		

The current log information is displayed in the text box. You can click Update Log to refresh the log information.

#### **Network Detection**

Three tab pages are available on the network connection detection page, that is, Ping, Tracert, and Cable Detection.

# Ping لا

The following figure shows the Ping page.

Figure 1-52 Ping

Ping Tracert	Cable Detection
Destination IP or Domain name*	
Timeout Period (1-10)	2
Repetition Count (1-100)	5
	Detect
Ping Result	
	No Found
	Å

Input the destination IP address and click Detect. The detection result is displayed in the text box after a short while.

# Tracert لا

The following figure shows the Tracert page.

Figure 1-53 Tracert

Ping Tracert	Cable Detection
Destination IP or Domain name*	
Timeout Period (1-10)	2
	Detect
Tracert Result	
	No Found

Input the destination IP address and click Detect. The detection result is displayed in the text box after a short while.

# **└** Cable Detection

The following figure shows the Cable Detection page.

Figure 1-54 Cable Detection

Select Port						
Deselect			Available	Unavailable	Selected	AG Por
	40Gb 40Gb(Splited					

Select a port on the panel and click Detect. After a short while, the detection result is displayed below the Detect button.

# Figure 1-55 Cable detection result

Note: Fast port detects only A and B two pairs of core, length error 10	m				
Select Port					
및 Deselect		Availat	le 🔳 Unavailable	Selected	🖪 AG Po
12 34 56 78	_				
Copper Fiber 40Gb 40Gb 40Gb(Splited)	-				
Copper Fiber 40Gb 40Gb(Splited)	-				
	_				
Detect	Detect	Meters			
Detect Test Results	Detect Open	Meters 0			
Detect Test Results Port:(A / B / C / D represent four cable pairs)					
Detect Test Results Port:(A / B / C / D represent four cable pairs) Gi0/5:A	Open	0			