

# S3910 Series Switches Web Configuration Guide

Models: S3910-48TS; S3910-24TS; S3910-24TF



# 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	4
1.3.1 Favorites	7
1.3.2 Network	13
1.3.3 Security	
1.3.4 Advanced	27
1.3.5 System	32

# 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.

## 1.1 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 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 ES S	WITCH		
S Please enter the username		Everything is Great !	
		_	
Password		05	
Please enter the password	×	4	
EOGIN			

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

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

<b>FS</b> \$3910-48TS	Favorites > Home				ː ∰ Wizard 🎣 Service	⊟ More [→ Logout
2 Favorites >	Home				During Hanna	<u>.</u>
A Network	VLAN			^		0.00%
	Port		Model: \$3910-48TS	Current 2022-03-23 16:27:53	CPU Usage	9.90%
🗟 Security 🔷	SSH	1	Device MAC: 649d.99d0.00e4	Running Time: 0 d 00 h 49Min	Memory Usage	53.0%
ଭି Advanced →	Voice Vlan	Up Port Count	Device SN: G1PH97A00015C	Version: \$3910_FSO\$ 11.4(1)874\$4		
	Restart					
	Device Port				🛢 Selected 🖪 AG Port 🛢 Up 🛢 Shu	tdown 🛛 VSL Port
	FS SA TZ 3A TZ 5A STOLS PWE PWE C BEET COLOR COMPANY AND COMPANY COMPANY AND COMPANY AND COMPANY COMPANY AND COMPANY AND COMPANY	76 74 18 94 19 114 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	II HAYA BAYA DAYA HAYA BAYA DA	22 23478 SAYS 27472 27473 31472 SATM 3347	23 27 47 38 29 47 40 48 47 42 43 47 44 45 47 46 47 47 45 Copper Fiber 406b	49 # 120 51 # 122 5330-4013 40Gb(Splited)

## NOTE:

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

# 1.2 Web Management System

# **Basic Concepts**

# ン 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.
•	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.
② Select All I Deselect All 용 Batch Delete	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.
0	Fail.

# **↘** System Operations

1) Standalone Device Panel



## 2) VSU Device Panel



Available 🚆 Unavailable 📃 Selected 🚮 AG Port	Copper 🔄 Fibber
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 <b></b>	49 51
C         C <thc< th=""> <thc< th=""> <thc< th=""> <thc< th=""></thc<></thc<></thc<></thc<>	50 52
Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.	<u>All Invert Deselect</u>
Selected	
Selected.	

#### 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



# 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.
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

			Model: \$3910-48TS	Current	2022-03-23 16:31:23		CPU Usage	9.7
		1	Device MAC: 649d.99d	0.00e4 Runnin	g Time: 0 d 00 h 53Min		Memory Usage	53
Model: \$3	910-48TS	Up Port Coun	t Device SN: G1PH97A0	0015C Version	: \$3910_FSOS 11.4(1)B7454			
evice Po	ort						Selected 🗈 AG Port 🖷 Up 🖷 Shutd	lown 🖸 VSL
FS	Creater 1000M Vision	54 46 74 48 74 4 1 1 -50/2004 On-Link Flashing-ACT			23 4 736 27 4 738 27 4 730 31 4			47 A V 50 51P+ 51 A V 1
rt Role: 🕚	Trunk Port 💿 Ro	uted Port					Copper Fiber 40Gb	40Gb(Sp
ort Info	rmation <sup>c</sup>							
Port	Input Rate :	Output Rate :	Status(Port real speed) =	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count	
Gi0/1	5.4K	0.1K	Connected(1000M)	5560333/5424078	0/0	0/0	0	
GI0/2	ок	ок	Not Connected	0/0	0/0	0/0	0	
	ок	ок	Not Connected	0/0	0/0	0/0	0	
Gi0/3								
GI0/3	ок	ок	Not Connected	0/0	0/0	0/0	0	
Gi0/3 Gi0/4 Gi0/5	ок ок	ок ок	Not Connected	0/0	0/0	0/0	0	
Gi0/3 Gi0/4 Gi0/5 Gi0/6	ок ок ок	ок ок ок	Not Connected Not Connected Not Connected	0/0 0/0 0/0	0/0 0/0 0/0	0/0 0/0 0/0	0 0 0	
Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7	ок ок ок	ок ок ок	Not Connected Not Connected Not Connected Not Connected	0/0 0/0 0/0	0/0 0/0 0/0	0/0 0/0 0/0 0/0	0 0 0 0	
GI0/3 GI0/4 GI0/5 GI0/6 GI0/7 GI0/8	ок ок ок ок	ок ок ок ок	Not Connected Not Connected Not Connected Not Connected Not Connected	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	
GI0/3 GI0/4 GI0/5 GI0/6 GI0/7 GI0/8 GI0/9	ок ок ок ок	ок ок ок ок ок	Not Connected Not Connected Not Connected Not Connected Not Connected Not Connected	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	
Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7 Gi0/8 Gi0/9 Gi0/10	ок ок ок ок ок ок	ок ок ок ок ок ок	Not Connected Not Connected Not Connected Not Connected Not Connected Not Connected Not Connected	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 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
- I	VLAN0001	GI0/1-4,GI0/7,GI0/9-16,GI0/19-24,GI0/27-48,Te0/49-52 AG: Ag1	2
2	VLAN0002	GI0/10	
	VLAN0003	GI0/10	2 8
🗆 s	VLAN0005	Gi0/8,Gi0/10	
6	VLAN0006	GI0/8,GI0/10	
7	VLAN0007	GI0/10	
- a	VLAN0008	GI0/10	2 0
12	VLAN0012	GI0/10	2 1
12	VLAN0013	GI0/10	6 8
14	VLAN0014	Gi0/10	
Total 11 item(s)	1 2 > Items per page: 10 × 1 (20)		

#### 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

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

## Y Trunk Port

The following figure shows the Trunk Port page.

#### Figure 1-6 Trunk Port

VLAN Settings Trunk Port	
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 t	runk port.
🖾 Select All 🗉 Deselect All 🗊 Batch Delete	
Gi0/8 Gi0/10	
Native VLAN * Range(1-4094)	
Allowed VLAN Range(1-4094)	
Select Port	
의 All \$ Invert I Deselect	Available Unavailable Selected AG Port
1.*2 3.*4 5.*6 7.*8 9.*10 11.*12 13.*14 15.*16 17.*18 19.*20 21.*22 23.*24 25.*26 27.*28 29.*30 31.*32 33.*34 35.*36 3 3 4 5 5 6 7.*8 9.*10 11.*12 13.*14 15.*16 17.*18 19.*20 21.*22 23.*24 25.*26 27.*28 29.*30 31.*32 33.*34 35.*36 3 4 5 5 6 7.*8 9.*10 11.*12 13.*14 15.*16 17.*18 19.*20 21.*22 23.*24 25.*26 27.*28 29.*30 31.*32 33.*34 35.*36 3 4 5 5 6 7.*8 9.*10 11.*12 13.*14 15.*16 17.*18 19.*20 21.*22 23.*24 25.*26 27.*28 29.*30 31.*32 33.*34 35.*36 3 4 5 5 6 7.*8 9.*10 11.*12 13.*14 15.*16 17.*18 19.*20 21.*22 23.*24 25.*26 27.*28 29.*30 31.*32 33.*34 35.*36	3738 3940 4142 4344 4546 4748 4950 5152
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 Cancel	

#### • 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

ort Settings	Aggregate port	Port Mirroring	Rate Limiting				
+ Batch Add	+ Add SVI						
Port							
Port	Up/Down	IP	Mask	IPv6		Description	Action
Ag3	Up	3.3.3.3	255.255.255.0	5			C D
VLAN 1	Up	10.32.130.116	255.255.255.0	)			
VLAN 12	Up	2.2.2.2	255.255.255.	)			6
al 3 item(s)	Items per page:	10 ~ 1 GO					
Port							
Port							
Port Port	Up/Down	Port Type	Access VLAN	Native VLAN	Permit VLAN	Description	Action
Port Gi0/1	Up/Down Up	Port Type ACCESS	Access VLAN	Native VLAN	Permit VLAN	Description	Action
Port Gi0/1 Gi0/2	Up/Down Up Up	Port Type Access Access	Access VLAN 1 1	Native VLAN 1 1	Permit VLAN	Description	Action C E
Port Gi0/1 Gi0/2 Gi0/3	Up/Down Up Up Up	Port Type Access Access Access	Access VLAN 1 1 1	Native VLAN 1 1	Permit VLAN	Description	Action C E C E C E
Port Port Gi0/1 Gi0/2 Gi0/3 Gi0/4	Up/Down Up Up Up	Port Type Access Access Access Access	Access VLAN 1 1 1 1 1	Native VLAN 1 1 1 1	Permit VLAN	Description	Action       IV     II
Port GI0/1 GI0/2 GI0/3 GI0/4 GI0/5	Up/Down Up Up Up Up Up	Port Type ACCESS ACCESS ACCESS ACCESS	Access VLAN 1 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN	Description	Action         III           IV         III
Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6	Up/Down Up Up Up Up Up	Port Type Access Access Access Access	Access VLAN 1 1 1 1 1	Native VLAN 1 1 1 1	Permit VLAN	Description	Activation         E           IV         E
Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7	Up/Down Up Up Up Up Up Up Up	Port Type ACCESS ACCESS ACCESS ACCESS ACCESS ACCESS ACCESS	Access VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Native VLAN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Permit VLAN	Description	Activation         E           IV         E
Port Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7 Gi0/8	Up/Down Up Up Up Up Up Up Up Up	Port Type Access Access Access Access Access Access TRUNK	Access VLAN	Native VLAN           1           1           1           1           1           1           5	Permit VLAN	Description	Activation         III           IV         IIII           IV         IIII
Port Cont	Up/Down Up Up Up Up Up Up Up Up Up Up	Port Type ACCESS ACCESS ACCESS ACCESS ACCESS ACCESS TRUNK ACCESS	Access VLAN	Native VLAN	Permit VLAN	Description	Action         III           IV         IIII           IV         IIII           IV         IIII           IV         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

#### 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			
lobal Configu	ration					
Note: the aggregat	e port is used to perform traffic allo	ocation according to the selected	load-balance algorithm.			
ad-balance So	ource MAC and Destination M.	AC ~				
	Save Default Set	ttings				
agregation needs	et cottings					
ggregation po	int settings					
<ul> <li>Note:</li> <li>In order to provide</li> </ul>	increased bandwidth and redundar	ncy, multiple physical ports (meml	per ports) are combined into one lo	gical port (aggregate port).		
• An aggregate port	contains up to eight member ports	, and the aggregate port load bal	ances traffic across these physical p	orts.Only supports static AP aggregation.		
AG1	AG3					
Aggregate Port ID	* Range(1-128)					
Port Type	L2 Port(Switching Pc	ort) 🔿 L3 Interface(Routin	ng Interface)			
Select Port						
🖾 All 躍 Invert	⊠ Deselect				📕 Available 🛛 📕 Unava	ilable Selected 🖪 AG Port
12 34	1 5**6 7**8 9**10 11* 1	-12 1314 1516 1718 3 3	3 19-720 21-722 23-724 2	3 3	5738 3940 4142 4344 4546	4748 4950 5152
Note:Click and ho	ld the left button as you drag	the pointer across the section	to select multiple ports.		Copper 📕 Fiber	40Gb 🗐 40Gb(Splited)

#### • 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.

## ▶ Port Mirroring

The following figure shows the Port Mirroring page.

## Figure 1-9 Port Mirroring

Port Settings	Aggregate port	Port Mirroring	Rate Limiting			
<ul> <li>Note:</li> <li>Port mirroring is</li> <li>A source port car</li> </ul>	he capability to send a copy of netw not be a destination port.	ork packets seen on the source po	rt to the destination port for analy:	s by a network analyzer. Traffic on mult	ple source ports can be mirrored to one single de	tination port.
Select All Des	elect All 🛛 🔀 Batch Delete					
ession ID *	ange (1-4)					
Alonitor Packets A	Packets	~				
elect Source Port (Y	ou can select multiple ports, bu Deselect	t it may affect device perform	ance.)		Available	Unavailable Selected 🛛 AG
1.*2 3.*4	56 78 910 1112 1	1814 1516 1718 19 3 3	20 21-22 23-24 25-26	2728 2930 3132 3334 35.	-36 3738 3940 4142 4344 45	46 4748 4950 5152
lote:Click and hold th	e left button as you drag the p	pinter across the section to sel	ect multiple ports.		Copper	Fiber 40Gb 40Gb(Sp
-last Daskinstian Dask	0/					
Deselect	(rou can select only one port	J			Available	Unavailable
1.*2 3.*4	5.*6 7.*8 9.*10 11.*12 1	1314 1516 1718 191	20 21-22 23-24 25-26	2728 2930 3132 3334 35.	*36 37.*38 39.*40 41.*42 43.*44 45.*	46 4748 4950 5152
lote:Click and hold th	e left button as you drag the p	pinter across the section to sel	ect multiple ports.		Copper	Fiber 40Gb 40Gb

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						
	_					
Port		Input Rate-L	imit (KBps)	Output Rate-Limit (KBps)	Action	
				No Found		
Total 0 item(s)	> Items per page: 1	0 • 1 GO				

#### • 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	
1 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

Static Address Settings	Filtering Address Settings			
Note: The switch forwards it to the specified port. Wit	data according the MAC address inside the dat	a frame. If you configure MAC-port binding on a network	device manually, after you add a static address, the switch that with port.	receives the packet with the same destination address forwards
+ Add Static Address	Delete Static Address			
Port	MA	AC Address	VLAN ID	Action
GigabitEthernet 0	/31 365	2.9685.ac16	16	1
GigabitEthernet 0	/31 acd	4.9685.1111	16	1
Total 2 item(s)	> Items per page: 10 -	1 GO		

#### 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

nic Address Settings	Filtering Address Settings		
1 Note: The switch forwards	data according the MAC address inside the data fram	e. If a switch receives a packet with the source/destination	n MAC address which is configured as a filter address, it discards the packet. You can prevent the ARP attack by
configuring a filter address	the same as the MAC address of ARP packets.		
- Add Ellers Address	🐡 Delete Filter Address		
+ Add Filter Address	U Delete Filter Address		
MAC Address		VLAN ID	Action
		12	C 🗊
6425.2542.3659			
<ul> <li>6425.2542.3659</li> <li>6425.2542.3369</li> </ul>		13	
6425.2542.3659           6425.2542.3369		13	

#### • 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

1) You can select multiple filtering addresses and click **Delete Filter 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 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

Coute Settings  Note: Route selection points based ro route to the 2.	uting and a backup route when the	primary route does not take effect, it wil	take a backup route to the back	up route in accordance with the priority level	configured to go, th	he backup route priority 1 high priority than a backup
+ Add Static Route + Add	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Туре	Action
			No Found			
Fotal 0 item(s)	per page: 10	~ 1				

## 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

	tion			
STP				
Priority 8		Hello Time 2		
Aging Time 20		Forward Delay 15		
STP Mode MSTP	~			
vIST Name		MST Version 0		
MST Configuratio	n ed to disable STP before configuring	an instance and enable STP again after co	figuration, so as to ensure the stability and convergence of netwo	vik topology.
MST Configuratic Note: It is recommend Add Instance	de disable STP before configuring     Delete Selected Instar	an instance and enable STP again after co	figuration, so as to ensure the stability and convergence of netwo	rk topology.
MST Configuratic Note: It is recommend Add Instance	n ed to disable STP before configuring Delete Selected Instar nber	an instance and enable STP again after co ICCE VLAN	riguration, so as to ensure the stability and convergence of netwo Priority	rk topology. Action

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

Batch Add							
Note: It is recommended	to enable Port Fast on the port connecte	d to the PC.					
Port	State	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance Cost Priority	Ac 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	
Gi0/4	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Ø
GI0/7	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/8	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/19	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/20	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/21	Down	Disabled	Disabled	Null	Point To Point	0 0 128	
Gi0/22	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Ø

## 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

P Global Settings	STP Port Settings	RLDP Settings			
Global configura	ation				
diobal configure					
1 Note: RLDP enables	you to detect link failure quickly. RLDP c	an run on the port only after it is	s enabled globally.		
NOD					
REDP.					
Detection Interval:	3	Detection Count:	2		
errdisable recovery:					
	Save				
Port Configurati	Save				
Port Configurati	Save	storm caused by loons. It is re	commended to anable RIND on the port connected to the	he 91 +	
Port Configurati Note: 1. Enabling RI 2. Unidirectio 3 An angress	Save	storm caused by loops. It is re es the ports on both ends of t	commended to enable RLDP on the port connected to the link to be enabled with RLDP. It is recommended to to the sourchorate to other	he PC ; onfigure RLDP to monitor the link between two switches; r member posts	
Port Configurati Note: 1. Enabling R 2. Unidirectio 3.An aggrega	Save ion LDP on the port can avoid broadcast s avoid broadcast in a solid broadcast s LDP on the port can avoid broadcast s te port can only be configured with p	storm caused by loops. It is re es the ports on both ends of 1 ort violation or alarm. Loop d	commended to enable RLDP on the port connected to t he link to be enabled with RLDP. It is recommended to etection on a member port will be synchronized to othe	he PC ; onligure RLDP to monitor the link between two switches; r member ports.	
Port Configurati Note: 1. Enabling R 2. Undirectio 3.An aggrega	Save CDP on the port can avoid broadcast t nal/Bildirectional link detection requin te port can only be configured with p Batch Delete	storm caused by loops. It is re es the ports on both ends of t ort violation or alarm. Loop d	commended to enable RLDP on the port connected to the link to be enabled with RLDP. It is recommended to detection on a member port will be synchronized to othe	he PC ; onfigure RLDP to monitor the link between two switches; r member ports.	
Port Configurati Note: 1. Enabling RI 2. Unidirectio 3.An aggrega + Add Port	Save DDP on the port can avoid broadcast s na/Biddirectional link detection requin te port can only be configured with p B Batch Delete	storm caused by loops. It is re es the ports on both ends of f oort violation or alarm. Loop d	commended to enable RLDP on the port connected to t he link to be enabled with RLDP. It is recommended to etection on a member port will be synchronized to othe	he PC ; onfigure RLDP to monitor the link between two switches; r member ports.	
Port Configurati Note: 1. Enabling R 2. Undifrectio 3.An aggrega + Add Port 1	Save CDP on the port can avoid broadcast DDP on the port can avoid broadcast unal/Bildirectional link detection requin te port can only be configured with p Batch Delete	storm caused by loops. It is re es the ports on both ends of t rort violation or alarm. Loop d	commended to enable RLDP on the port connected to the link to be enabled with RLDP. It is recommended to detection on a member port will be synchronized to othe velocition Type:Troubleshooting	he PC ; onfigure RLDP to monitor the link between two switches; r member ports.	
Port Configurati Note: 1. Enabling R 2. Unidirectio 3.An aggrega + Add Port	Save Save LDP on the port can avoid broadcast t nat/Bidirectional link detection requin te port can only be configured with p Batch Delete	storm caused by loops. It is re es the ports on both ends of 1 iort violation or alarm. Loop d	commended to enable RLDP on the port connected to the link to be enabled with RLDP. It is recommended to etection on a member port will be synchronized to othe etection Type:Troubleshooting	he PC ; onfigure RLDP to monitor the link between two switches; r member ports.	
Port Configurati Note: 1. Enabling R 2. Unidirectio 3.An aggrega + Add Port 1	Save Save LDP on the port can avoid broadcast t na/Biddirectional link detection requin te port can only be configured with p B Batch Delete	storm caused by loops. It is re es the ports on both ends of 1 iort violation or alarm. Loop d D	commended to enable RLDP on the port connected to the link to be enabled with RLDP. It is recommended to detection on a member port will be synchronized to othe retection Type:Troubleshooting	he PC ; onfigure RLDP to monitor the link between two switches; r member ports.	

#### 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

Note: On layer 2 devices, multicast frame	mes are flooded to all ports, causing storm and consumi	ng much bandwidth. IGMP Snooping is used to	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	contraction of the party classing scotts and conterna	ing the second se		
+ Add Profile 🛛 🕫 Delete Se	elected Profile			
Profile ID	Multicast Address	Policy Action	Application Port	Action
Profile ID	Multicast Address	Policy Action	Application Port	Action

## 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

-	
Note: DHCP relay can cer	ntrally 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.
HCP relay IPV4 co	onfiguration
HCP Relay:	
HCP Server Address:	+ Add DHCP Server
HCP Server Address:	+ Add DHCP Server
HCP Server Address:	Save
HCP Server Address:	Save iguration
HCP Server Address:	Save jguration
HCP Server Address:	Save

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

Eportalv2	Advanced
Note: Authenticat	tion is based on Web to control users' access to the network. It requires no authentication software on the client. Instead, you can perform authentication on common browsers.
Eportal Type:	⊖eportalv1
Server IP:	*
Redirection URL:	*
Portal Key:	
Authentication Server:	All Servers
Accounting Server:	All Servers V
SNMP Server:	[SNMP Server] *
Port:	
🖾 All 🖫 Invert [	🗵 Deselect 🖉 Available 🗮 Unavailable 🗮 Selected 🗳 AG
1.*2 3.*4	5-6 7-8 9-10 11-12 13-14 15-16 17-18 19-20 21-22 23-24 25-26 27-28 25-30 31-32 33-34 35-36 37-38 39-40 41-42 43-44 45-46 47-48 49-50 51-52 3 3 4 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4
Note:Click and hold the	he left button as you drag the pointer across the section to select multiple ports.
	Save Clear

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

# ⊾ Advanced

The following figure shows the Advanced page. Figure 1-21 Advanced Settings

Eportalv2 Advan	iced	
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) ca	an 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 without	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

Note:	
DHCP snooping is used to filter DHCP packets received on an untrusted port from outside the network or f	firewall. The DHCP request packet is forwarded to the trusted port. The DHCP reply packet is forwarded only if it is from a trusted port.
<ul> <li>The port connected to the DHCP server is configured as a trusted port generally.</li> </ul>	
DHCP Snooping	
Select Port	
Select Port 과 All 뜒 Invert 또 Deselect	Available Unavailable Selected AG Por
Select Port 과 All ዤ Invert 핀 Deselect	Available Unavailable Selected S AG Por
Select Port All B Invert Deselect 12 34 56 78 910 1112 1314 1516 1718 1920 2122	Available Unavailable Selected AG Por 23-24 25-26 27-28 29-30 31-32 33-34 35-36 37-38 39-40 41-42 43-44 45-46 47-48 49-50 51-52
Select Port All 😳 Invert 💌 Deselect 12 34 56 78 910 1112 1314 1516 1718 1920 2122 3	Available Unavailable Selected AG Por 2324 2526 2728 2930 3132 3334 3536 3738 3940 4142 4344 4546 4748 4950 5152
Select Port           All 12: Invert 10 Deselect           12         34         56         78         910         1112         1314         1516         1718         1920         2122           3         3         3         3         3         3         3	Available Unavailable Selected AG Por 2324 2526 2728 2930 3132 3334 3536 3738 3940 4142 4344 4546 4748 4950 5152
Select Port           All B Invert Deselect           12 34 56 78 910 1112 1314 1516 1718 1920 2122           3           3           3	Available Unavailable Selected AG Por 23-24 25-26 27-28 29-30 31-32 33-34 35-36 37-38 39-40 41-42 43-44 45-46 47-48 49-50 51-52 3 3 4 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4

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			
<b>Note:</b> It is configured on or	nly the port connected to the c	lient to prevent ARP spoofing.				
+ Add Port	+ Add Port S Batch Delete					
Filtering F	Port		IP	Action		
To sound						
fotal 0 item(s) < > Items per page: 10 • 1 GO						

#### • 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			
<b>()</b> Note: ARP Check is used to filter	all ARP packets on the	logical port and discard invalid <i>i</i>	ARP packets. It can effectively	prevent ARP Spoofing and improve network stability.	A DHCP Snooping trusted port cannot be enabled with	ARP Check.
Select Port						
의 All 답 Invert 🗵 Deselect					🔳 Available 🛛 Unava	ilable 🔲 Selected 🔲 AG Port
1.*2 3.*4 5.*6 7.*8 1	9.*10 11.*12	1314 1516 1718 19- 3	•20 21 <b>.</b> •22 23 <b>.</b> •24 25	3	3738 3940 4142 4344 4546 4748	49-*50 51-*52
		3		3		
Note:Click and hold the left button	as you drag the po	pinter across the section to s	elect multiple ports.		💼 Copper 📰 Fiber	40Gb 40Gb(Splited)

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.

# 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	oled VLAN intercepts all ARP req	uest and reply packets to dis	card invalid ARP packets	
Add VLAN DAL 🖓 Select All	🗵 Deselect All 🛛 🛱 R	atch Delete			
	E Deselect All E b	atti Delete			
No Data					
Trusted Port					
1 Note: Packets received on t	he trusted port skip DAI Insp	ection as valid ARP packets.			
Select Port					
의 All La Invert 🗵 Desei	lect				Available Unavailable Selected
1-*2 3-*4 5-*6	7-*8 9-*10 11-*12	13-*14 15-*16 17-*18 19-*	•20 21-•22 23-•24 2!	5.*26 27.*28 29.*30 31.*32 33.*34 35.*3	36 37-*38 39-*40 41-*42 43-*44 45-*46 47-*48 49-*50 51-*52
1		3		3	
		3			
Note:Click and hold the left be	utton as you drag the poi	nter across the section to se	elect multiple ports.		Copper Tiber 406b EE 406b

#### 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

Anti-Al	RP-Spoofing ARP	Check DAI Settings ARP Entries		
ළු Dyn	amic Binding > Static Binding	Remove static Binding     Manual Binding		IP-based
	IP	MAC	Туре	Action
	10.32.130.2	649d.99d0.0138	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.13	484d.7eab.ecb6	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.107	8cec.4b8d.9c43	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.116	649d.99d0.00e5	Local ARP Entry	
	10.32.130.125	8cec.4bd1.491d	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.134	509a.4c12.1e79	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.145	8cec.4bbc.4ba2	Dynamic Binding	Dynamic Binding > Static Binding
	10.32.130.254	782c.294b.a201	Dynamic Binding	Dynamic Binding > Static Binding
Total 8 it	em(s) < 1 > Items	per page: 10 🗸 1 GO		

#### 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						
Note: IP Source Gu	ard is applied in combination with DHCP Snooping. F	Port-based IP Source Guard takes e	ffect on only the untrusted port er	nabled 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				
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

Port Settings User Bin	ding			
Note: The IP Source Guard-enabled p	ort filters all non-DHCP IP packets. After configured with the stati	c IP address, the port allows specified IP packets to pas	s through.	
+ Add Binding 😂 Delete S	Selected Binding			
□ MAC	IP	VLAN ID	Port	Action
		No Found		
Total 0 item(s) < > Items	per page: 10 v 1 GO			

#### • 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 a	accessed user has valid IP and MAC addres	s or where the user accesses the network throug	h a fixed port instead of changing IP/MAC address or j	port number, or limits the number of MAC addresses on the
port to avoid attact	is caused by MAC address depiction				
+ Add Port	Batch Delete				
Port		Max Secure Address	Aging Time	Security Action	Action
The Found					
	Items per page: 1				

#### • 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

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

2) 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

Basic Settings	Security Binding				
1 Note: Port Security is	s used to allow only the packet whose	e source MAC address is consistent with the secure a	ddress to enter the switch.		
+ Add Address	Batch Delete				
Port		IP	MAC	VLAN ID	Action
The Found					
Total 0 item(s)	> Items per page: 10	<ul><li>✓ 1 GO</li></ul>			

#### • 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

NFPP Settings	
ARP-guard 📀	ARP-guard List
IP-guard 📀	IP-guard List
ICMP-guard 🥥	✓ ICMP-guard List
DHCP-guard 📀	✔ DHCP-guard List
DHCPv6-guard 📀	☑         DHCPv6-guard List
ND-guard 📀	
Display NFPP Log 📀	Display NFPP Log
	Save Restore Default Settings

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

Storm Control  Add Port  Batch Delete	]			
Port	Broadcast	Multicast	Unicast	Action
Gi0/1	-	12	2	
Gi0/2	-	-	-	C D
Gi0/3		-	-	C D
Gi0/4	-	-		
Gi0/5		12 C	а.	AggregatePort member
Gi0/6	-	-	-	AggregatePort member
Gi0/7		12 C	а.	C tu
Gi0/8	-	-	-	
Gi0/9		12 C	а.	C tu
Gi0/10	-	-	-	
otal 54 item(s) < 1 2 3	4 5 > Items per page:	1 GO		

## • 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

Port Protect  Note: Proteced ports can not communicate with each other. The selected ports on the panel are the protected p	orts.Please click 'Display Protected Port' to refresh the panel.
Select Port ② All 强 Invert 🖸 Deselect	🔳 Available 🔳 Unavailable 🔳 Selected 🕫 AG Por
12 34 56 78 910 1112 1314 1516 1718 1920 2122 2324 3	2526 2728 2930 3132 3334 3536 3738 5940 4142 4344 4546 4748 4950 5152 3

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	Static Address Client Di	splay				
+ Add DHCP Ø E	xcluded Address Range Batch De	lete DHCP				
Name	IP Address Range	Default Gateway	Lease Time	DNS	Action	
123	192.168.1.1-192.168.	1.254 192.168.1.1	8 hour(s)		C D	

## 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

DHCP Settings	Static Address	Client Display					
+ Add Static Addr	Batch Delete						
Client N	Name Client	IP Ma	ask Gatewa	y Address	Client MAC	DNS Server	Action
			No I	Found			
Total 0 item(s)	< > Items per page	x 10   ▼ 1					

## 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.

# ↘ Client Display

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

DHCP Settings	Static Address	Client Display			
+Bind MAC to Dy	ynamic IP 🗊 Batch Delete	]			IP-based (
_ IP		MAC	Lease Time	Allocation Type	Action
			No Found	<b>\</b>	
Total 0 item(s)	< > Items per page:	10 • 1 G			

#### • 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 10	• • • A	dd ACL 🗇 Delete ACL							
Access Rule	2								
+ Add Acce	ss Rule 🗇 Delete	Selected Access Rule							
NO.	Source IP/Wildca	d Source Port	Access Control	Protocol	Destination IP/Wildo ard	Destination port	Time Period	Status	Action
1	Any		Permit				All Time	Effective	6 0
Total 1 item(s)	< 1 > Item	ns per page: 10 🗸	1 GO						

#### 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

You can select multiple access rules from the ACL rule list and click Delete Selected Access Rule to delete the access rules in batches.
 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 ACL App	lication			
1 Note: The ACL active time must be periodic.				
+Add Time Object	]			
Time Object	Day	Time Period	Action	
		No Found		
Total 0 item(s) < > Items per page: 10	▶ 1 GO			

## 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.

## ▶ ACL Application

The following figure shows the ACL Application page.

Figure 1-39 ACL Application

ACL List ACL Time	ACL Application			
- Auto David	-			
- Add Fort	c			
ACL	Port	Direction	Action	
		•		
		No Found		
Total 0 item(s) < > Items	per page: 10 ¥ 1 GO			

#### 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

1) You can select multiple ports from the ACL application list and click Delete 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 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>Note:</b> Classification	is used to identify and mark certair	n data flows that match the ACL rul	e.		×
+ Add Class	Batch Delete				
Class Nam	e		ACL	Action	
Class Nam	e		ACL 10	Action	

#### 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
```

lass Settings	Policy Settings	Flow Settings				
Note: The policy is used	d to constrain the bandwidth th	at the classified data flow consumes.				
Policy Settings						
Policy List	~	+ Add Policy 🔯 Delete Policy	]			
Policy Rule						
+Add Policy R	ule Batch Delet	e				
Class Na	me	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action	
			No Found			

## 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				
<b>1</b> Note: The policy is u	used to constrain input and output	flows (Input and output flows of	one port must be in the same trust mode but they can	be configured with different policies)		2
+ Add Port	<u> Batch Delete</u>					
Port		Direction	Policy Name	Trust Mode	Action	
			No Found			
Total 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

1) You can select multiple ports from the application policy 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.

#### 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	2022-3-23-17:0	0:22			
Reset Time	Select Time				
Time Zone	UTC+0(GMT)		~		
Time Synchronization	✓ Automatically syn	chronize with an In	ternet time server(Please set	: <u>DNS Server</u> first, o	therwise the syste
	Save				

#### 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.

## NOTE:

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.

## **Y** Password

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

System Time	Password	Reset	Enhancement	SNMP	DNS	
Web Managem	ent Password					
Username *			]			
Old Password *			]			
New Password *						
Confirm Password *						
	Save					
Telnet Password	d(Telnet and En	able Passwor	d)			
New Password*						
Confirm 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	
lestore Factory	Settings					
1 Note: Note: Al	ter the device is reset to t	he factory default setting	gs, all configurations will be rem	ioved. Please Export C	urrent Configuration before resetting the device.	
Restore Factory	Settings Export C	urrent Configuration				
Display Curre	ent Configurati	on				
Display Current Co	onfiguration					
					No Found	×
nport/Export	Configuration					
		1.1.1.1	1	1.0		
<ul> <li>Note: Please dor</li> </ul>	t close or update the	page during import, o	r import will fall. If you want f	o apply the new con	figuration, please restart the device on this page, or the configuration will not take effect.	
le Name		Browse File				

## • 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.

# **└** Enhancement

The following figure shows the Enhancement page.

## Figure 1-46 Enhancement

System Time	Password	Reset	Enhancement	SNMP	DNS
Basic Informati	ion				
Web Access Port*	80				
Login Timeout	10 min		~		
Davica Location					
Device Location					
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	v2 or SNMPv3 is supported				
SNMP Version	<b>●</b> v2 ○v3				
Device Location					
SNMP Community*	k				
Trap Community					
Trap Recipient Add	ress *				

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.

# ע dns

The following figure shows the DNS page.

Figure 1-48 DNS

System Time	Password	Reset	Enhancement	SNMP	DNS		
DNS Server 1			9				
	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 I	Local
Note: Ple	ease download the corresponding software version from the official website , and then upgrade the device with the following tips.
Tips: 1. M	date 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 Setting	s Display System Log
<b>1</b> Note: Logging is ra	ted on 8 different levels: 0-Emergency, 1-Alert, 2-Critical, 3-Error, 4-Warning, 5-Notification, 6-Informational, 7-Debugging. The smaller the number, the higher the level.
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	r the last 200 logs)	
Update Log		
Syslog logging: enabled		1
Console logging: level deb	ugging, 60 messages logged	
Monitor logging: level deb	ugging, 0 messages logged	
Buffer logging: level debug	gging, 60 messages logged	
Standard format:false		
Timestamp debug message	les: datetime	
Timestamp log messages: (	datetime	
Sequence-number log mes	ssages: disable	
Sysname log messages: dis	sable	
Count log messages: disab	le	
Trap logging: level informa	ational, 60 message lines logged,0 fail	
Log Buffer (Total 131072 Byt	tes): have written 5937,	
*Mar 23 16:27:48: %HTTPD-	-5-LOGIN: User (admin@10.32.130.145) login from FS.	
*Mar 23 16:26:07: %HTTPD-	-5-LOGOUT: User (admin@10.32.130.145) logout from FS.	
*Mar 23 16:24:51: %HTTPD-	-5-LOGIN: User (admin@10.32.130.145) login from FS.	
*Mar 23 16:24:42: %HTTPD-	-5-LOGOUT: User (admin@10.32.130.145) logout from FS.	
*Mar 23 16:21:48: %HTTPD-	-5-LOGIN: User (admin@10.32.130.125) login from FS.	
*Mar 23 16:18:42: %HTTPD-	-5-LOGOUT: User (admin@10.32.130.125) logout from FS.	
*Mar 23 16:09:14: %LINEPRC	DTO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to up.	
*Mar 23 16:09:08: %LINEPRO	DTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up.	
ANT - 22 47 00 00 00 00 00 0		

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 Per	iod (1-10)	2
epetition C	Count (1-100)	5
		Detect

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	r Domain name <b>*</b>	
Timeout Period (	(1-10)	2
		Detect

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

Deselect			🔳 Available 🛛 🔳 Unavailab	le 🗧 Selected 🛛 🖪 AG Por
1 <u>-*</u> 2 3 <u>-*</u> 4 5 <u>-*</u> 6 7 <u>-*</u> 8 9 <u>-*</u> 10				
	1112 1314 1516 1718 1920 2122 2324	2526 2728 2930 3132 3334 3536	3738 3940 4142 4344 4546 4748	49

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

19	macere	Cable Detection					
	ote: Fast port detects o	ity A and 5 two pairs of core, length error 10	um				
Select Po	ort						
Dese	elect				Available	Unavailable	Selected 🛛 AG F
1.*2	3*4 5*6 7*	3 910 1112 1314 1516	1718 1920 2122 2324	2526 2728 2930 3132 3334 3536	3738 3940 4142 4344 4	4546 4748 491	0 5152
Co	opper Fiber	40Gb 🚺 40Gb(Splited)					
De Test F	opper Fiber	40Gb 10 40Gb(Spilted)					
Dee Test F	etect Results	40Gb 40Gb(Splited)	Detect		Meters		
Test F	Popper Fiber Fitect Results rt:(A / B / C / D reg V/7:A	40Gb 40Gb(Splited)	Detect Open		Meters 0		
Co De Test F Por Gi0, Gi0,	Results rt:(A / B / C / D rep //7:A	40Gb 22 40Gb(Splited)	Detect Open Open		Meters 0		
Test F Por Gio, Gio, Gio,	oppper         Fiber           otect         Fiber           Results         Fitch           rt:(A / B / C / D reg         Fitch           //7.A         Fitch           //7.B         Fitch           //7.C         Fitch	40Gb 22 40Gb(Splited)	Detect Open Open Open		Meters         0 <td></td> <td></td>		