

S3410-24TS-P Switch Web Configuration Guide

Model: S3410-24TS-P

Contents

1. Web Configuration..... 1

1.1 Overview..... 1

1.2 Application..... 1

1.2.1 Web Management..... 1

1.3 Web Management System..... 4

1.3.1 Favorites..... 7

1.3.2 Network..... 13

1.3.3 Security..... 19

1.3.4 Advanced..... 26

1.3.5 System..... 31

1. Web 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

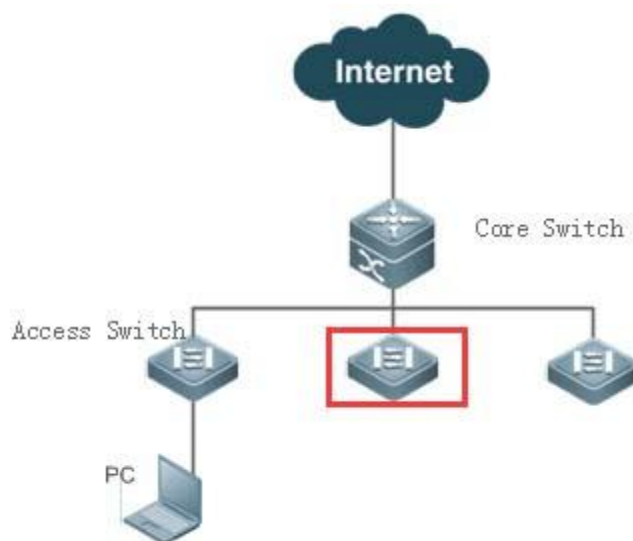
Application	Description
Web Management	After finishing relevant configuration, a user can access the Web management system through a browser.

1.2.1 Web 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

🔗 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.

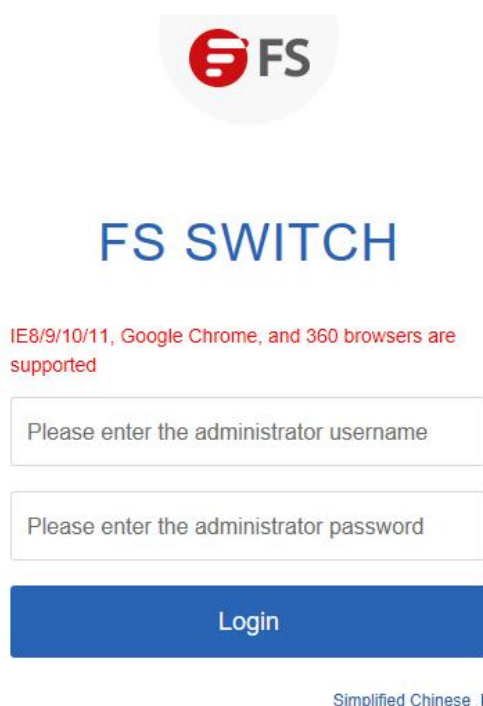
NOTE:

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

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



The login page features the FS logo at the top, followed by the text "FS SWITCH" in large blue letters. Below this, a red message states: "IE8/9/10/11, Google Chrome, and 360 browsers are supported". There are two input fields: "Please enter the administrator username" and "Please enter the administrator password". A blue "Login" button is positioned below the password field. At the bottom right, there is a link for "Simplified Chinese" with a right-pointing arrow.

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

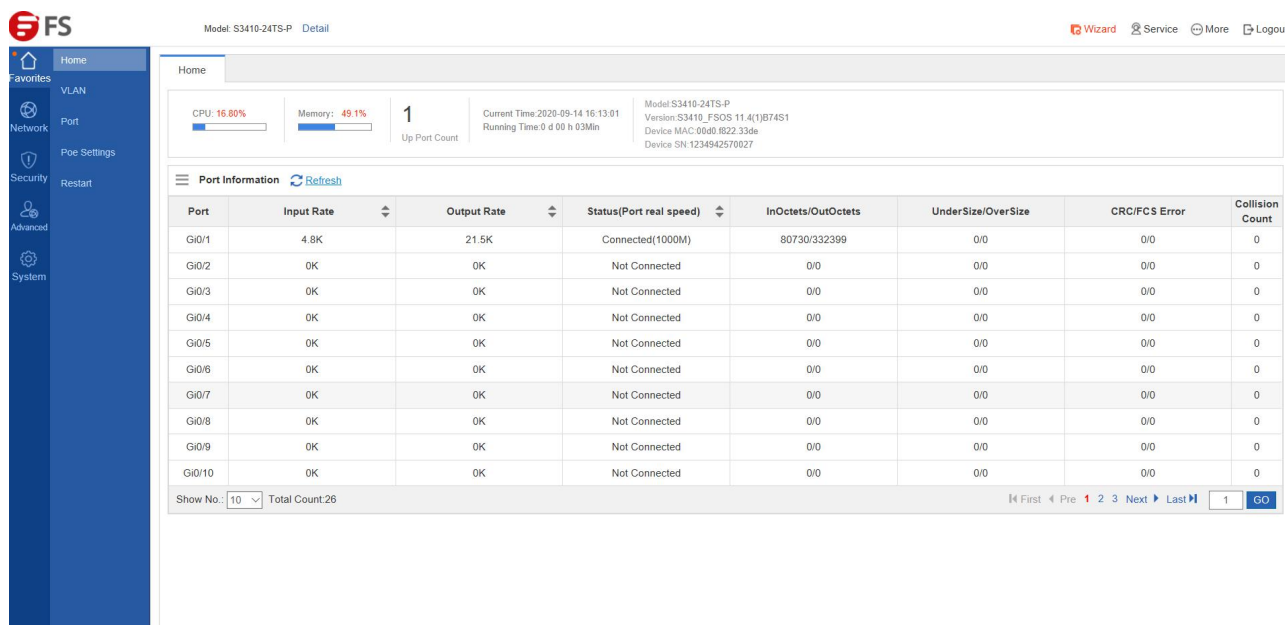
Default Username/Password	Permission Description
admin / admin	Super administrator who possesses all permissions.

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



NOTE:

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

1.3 Web Management System

Basic Concepts

Various Icons and Buttons on the GUI

Icon/Button	Note
	Edit button. You can click this icon to edit the currently selected item.
	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.
	Trunk port. This port is displayed on the panel on the VLAN Management/VLAN Settings page.
	Save button. You can click this button to submit and save the input information.
	Add setting.
	Delete setting.
	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.
	Note.
	Warning.

System Operations

1) Standalone Device Panel


Available
 Unavailable
 Selected
 AG Port
 Copper
 Fiber





1	3	5	7	9	11	13	15	17	19	21	23				
2	4	6	8	10	12	14	16	18	20	22	24	25	26	27	28



[All](#)
[Invert](#)
[Deselect](#)



















































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

2) VSU Device Panel



 Available
 Unavailable
 Selected
 AG Port

 Copper
 Fiber

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51
																									
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52
																									


Note: Click and hold the left button as you drag the pointer across the section to select multiple ports. [All](#) [Invert](#) [Deselect](#)





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




 Available
 Unavailable
 Selected
 AG Port





 Copper
 Fiber



1	3	5	7	9	11	13	15	17	19	21	23				
															
2	4	6	8	10	12	14	16	18	20	22	24	25	26	27	28
															



















































[All](#) [Invert](#) [Deselect](#) **Note:** Click and hold the left button as you drag the pointer across the section to select multiple ports.

2) Selected port on VSU device



 Available
 Unavailable
 Selected
 AG Port

 Copper
 Fiber

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51
																									
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52
																									

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports. [All](#) [Invert](#) [Deselect](#)

Selected:

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.
Quick Configuration	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, tracer detection, and cable detection.

1.3.1 Favorites

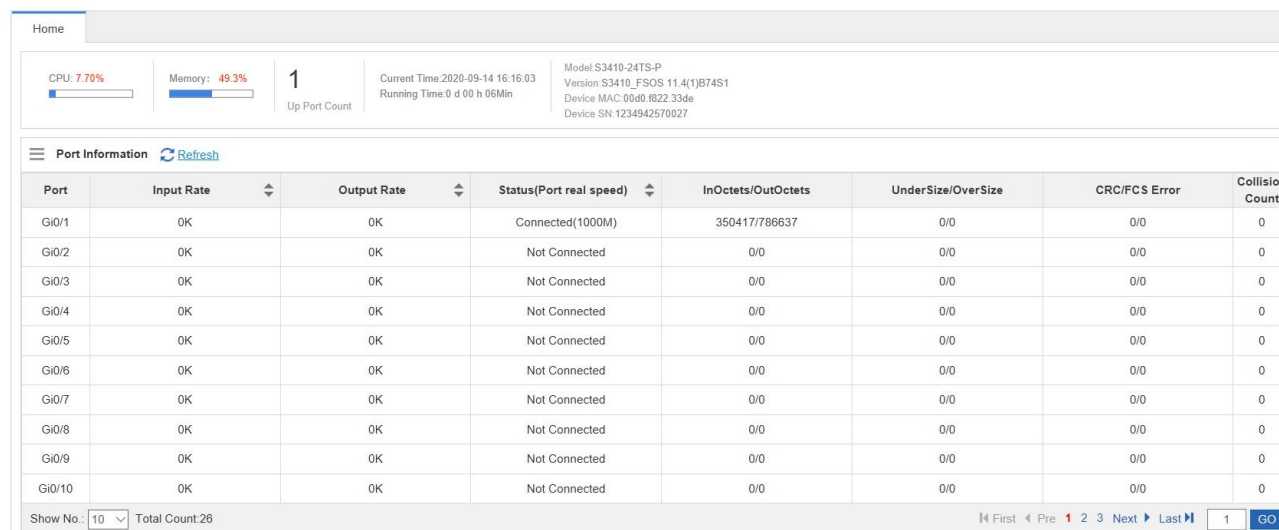
You can access secondary menus through the primary menu Favorites, including Home page, VLAN, Port and Restart.

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



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



● 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.

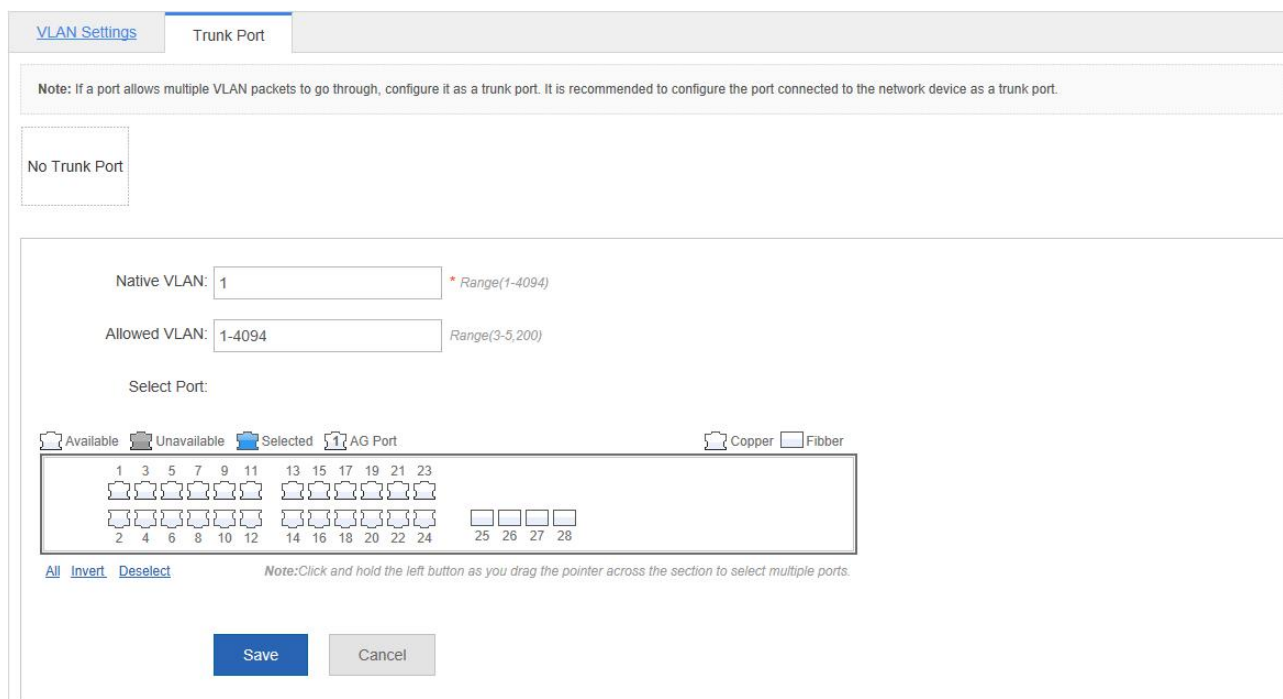
NOTE:

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.

Trunk Port

The following figure shows the Trunk Port page.

Figure 1-6 Trunk Port



The screenshot shows the 'Trunk Port' configuration page. At the top, there are tabs for 'VLAN Settings' and 'Trunk Port'. A note states: '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.' Below this, there is a 'No Trunk Port' button. The main configuration area includes fields for 'Native VLAN' (set to 1) and 'Allowed VLAN' (set to 1-4094). Below these are 'Select Port' options with icons for 'Available', 'Unavailable', 'Selected', and 'AG Port'. A grid of port icons is shown, with ports 1 through 24 selected. Port 1 is also marked as an 'AG Port'. There are also options for 'Copper' and 'Fiber' port types. At the bottom, there are 'Save' and 'Cancel' buttons. A note at the bottom of the port grid says: 'Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.'

- 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

Port Settings
Aggregate port
Port Mirroring
Rate Limiting

+ Batch Add
+ Add SVI

≡ L3 Port

Port	Up/Down	IP	Mask	IPv6	Description	Action
VLAN 1	Up	192.168.1.1	255.255.255.0			Edit Delete

Show No.: 10 ▼ Total Count:1

First
Pre 1 Next Last

1 GO

≡ L2 Port

Port	Up/Down	Port Type	Access VLAN	Native VLAN	Permit VLAN	Description	Action
Gi0/1	Up	ACCESS	1	1			Edit Detail
Gi0/2	Up	ACCESS	1	1			Edit Detail
Gi0/3	Up	ACCESS	1	1			Edit Detail
Gi0/4	Up	ACCESS	1	1			Edit Detail
Gi0/5	Up	ACCESS	1	1			Edit Detail
Gi0/6	Up	ACCESS	1	1			Edit Detail
Gi0/7	Up	ACCESS	1	1			Edit Detail
Gi0/8	Up	ACCESS	1	1			Edit Detail
Gi0/9	Up	ACCESS	1	1			Edit Detail
Gi0/10	Up	ACCESS	1	1			Edit Detail

Show No.: 10 ▼ Total Count:28

First
Pre 1 2 3 Next Last

1 GO

- 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.

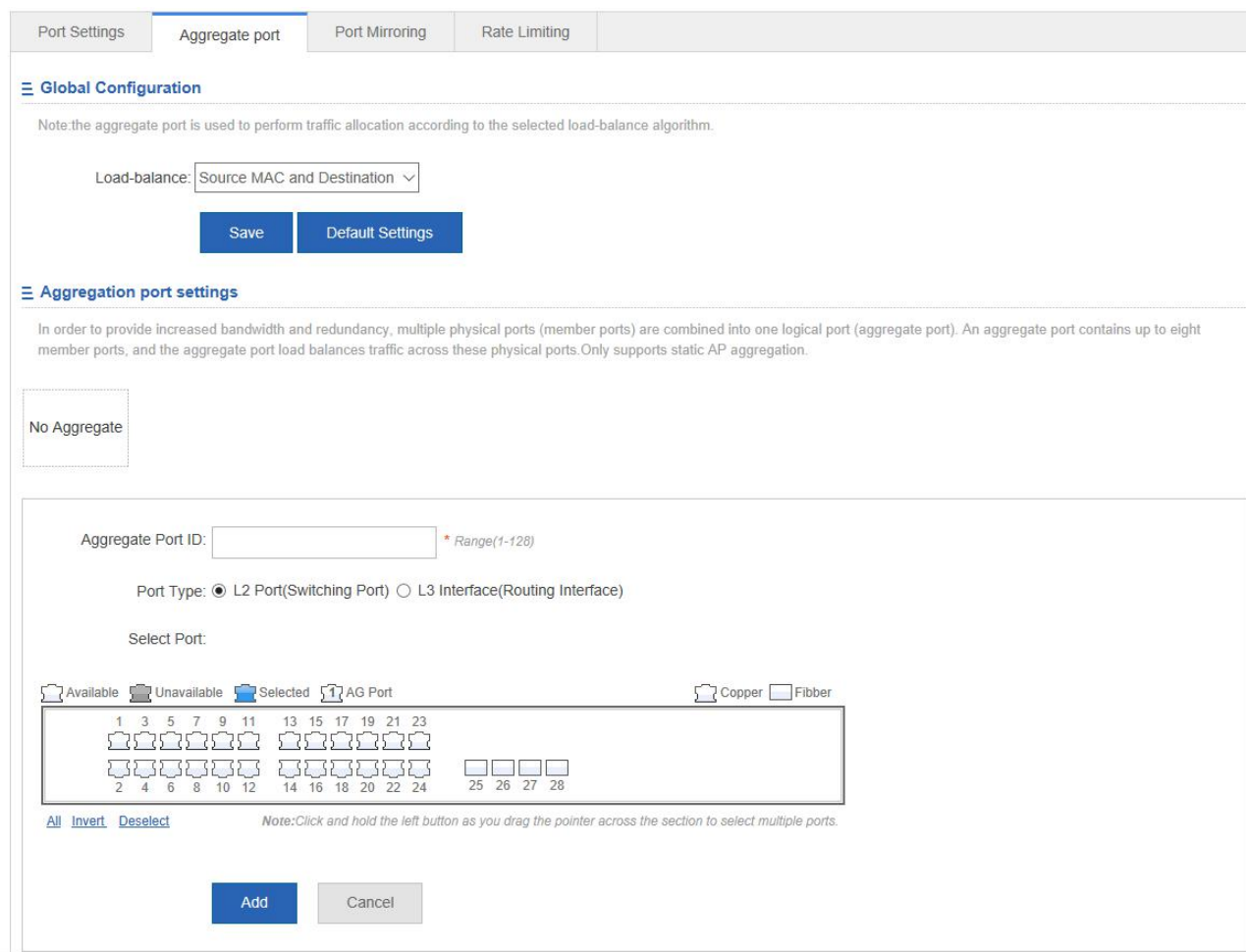
- Editing port

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



The screenshot shows the 'Aggregate port' configuration page. At the top, there are tabs: 'Port Settings', 'Aggregate port' (selected), 'Port Mirroring', and 'Rate Limiting'. Below the tabs is a 'Global Configuration' section with a note: 'Note: the aggregate port is used to perform traffic allocation according to the selected load-balance algorithm.' There is a 'Load-balance:' dropdown menu set to 'Source MAC and Destination'. Below this are 'Save' and 'Default Settings' buttons. The 'Aggregation port settings' section follows, with a note: 'In order to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load balances traffic across these physical ports. Only supports static AP aggregation.' Below the note is a 'No Aggregate' button. The main configuration area includes an 'Aggregate Port ID:' input field with a range hint '* Range(1-128)'. Below this is a 'Port Type:' section with radio buttons for 'L2 Port(Switching Port)' (selected) and 'L3 Interface(Routing Interface)'. A 'Select Port:' section shows a grid of 28 ports (1-28) with icons indicating their status: Available (white), Unavailable (grey), Selected (blue), and AG Port (blue with a plus icon). There are also checkboxes for 'Copper' and 'Fiber'. Below the grid are links for 'All', 'Invert', and 'Deselect'. A note at the bottom of the grid says: 'Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.' At the bottom of the configuration area are 'Add' and 'Cancel' buttons.

- 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.

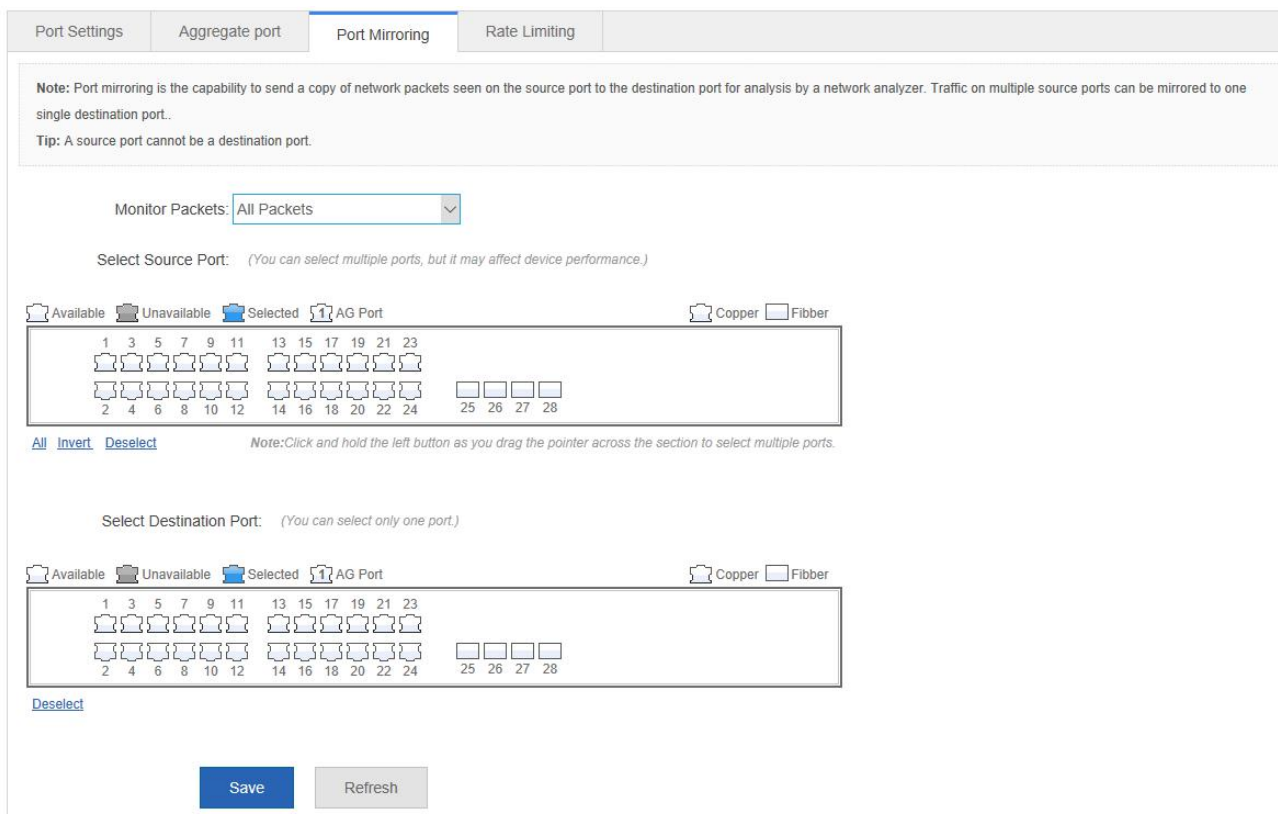
NOTE:

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



Note: Port mirroring is the capability to send a copy of network packets seen on the source port to the destination port for analysis by a network analyzer. Traffic on multiple source ports can be mirrored to one single destination port.

Tip: A source port cannot be a destination port.

Monitor Packets: All Packets

Select Source Port: (You can select multiple ports, but it may affect device performance.)

☐ Available
 ☐ Unavailable
 ☒ Selected
 ☐ AG Port
 ☐ Copper
 ☐ Fibber

1 3 5 7 9 11 13 15 17 19 21 23
 2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

[All](#) [Invert](#) [Deselect](#) *Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.*

Select Destination Port: (You can select only one port.)

☐ Available
 ☐ Unavailable
 ☒ Selected
 ☐ AG Port
 ☐ Copper
 ☐ Fibber

1 3 5 7 9 11 13 15 17 19 21 23
 2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

[Deselect](#)

Save **Refresh**

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 X Batch Delete				
<input type="checkbox"/>	Port	Input Rate-Limit (KBps)	Output Rate-Limit (KBps)	Action
No Record Found				
Show No.: <input type="text" value="10"/>		Total Count: 0		First Pre Next Last <input type="text" value="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
<p>Note: Click 'Restart' to restart the device. Please wait for about two minutes and the page will be refreshed after restart.</p>
<div>Restart</div>

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

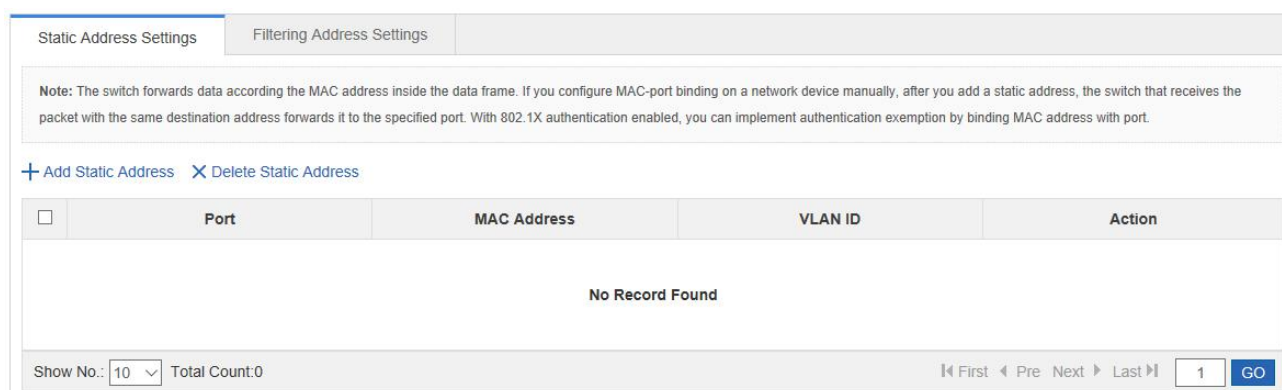
You can access secondary menus through the primary menu Network, including MAC Address, Routing, STP,, IGMP Snooping, Authentication and DHCP Relay.

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



- Adding Static Address

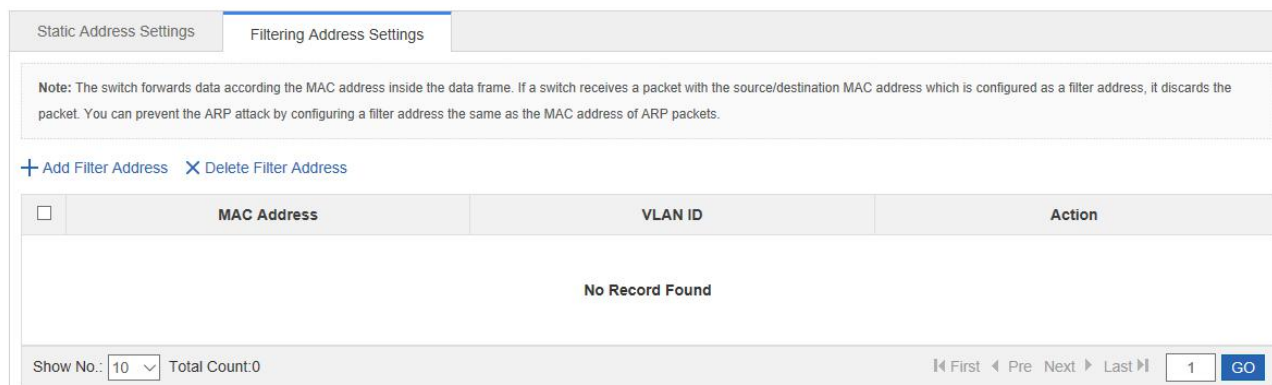
To add a static address, input the MAC address, VLAN ID and select a port, and then click **Save**. The newly added static address is displayed in the address list after a "Configuration succeeded." message is displayed.

- 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



- 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

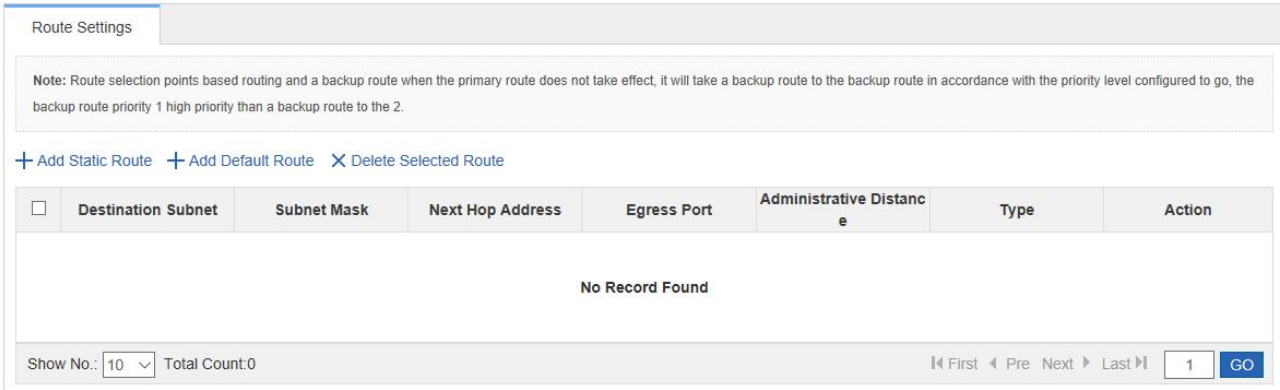
- 1) You can select multiple filtering addresses and click **Delete Filter Address** to delete the addresses in batches.
- 2) After you click **Delete** in the Action column, an "Are you sure you want to delete the filter address?" message is displayed. After you confirm the operation, a "Delete succeeded."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



The screenshot shows the 'Route Settings' page. At the top, there is a note: 'Note: Route selection points based routing and a backup route when the primary route does not take effect, it will take a backup route to the backup route in accordance with the priority level configured to go, the backup route priority 1 high priority than a backup route to the 2.' Below the note, there are three buttons: '+ Add Static Route', '+ Add Default Route', and 'X Delete Selected Route'. A table with the following columns is shown: ☐, Destination Subnet, Subnet Mask, Next Hop Address, Egress Port, Administrative Distance, Type, and Action. The table is currently empty, displaying 'No Record Found'. At the bottom, there is a pagination bar with 'Show No.: 10', 'Total Count: 0', and navigation buttons: First, Pre, Next, Last, and a 'GO' button.

- 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

STP Global Settings

STP Port Settings

RDP Settings

Global Configuration

STP: ☒ ON

Priority: Range(0-15), default 8

Hello Time: Range(1-10s), default 2

Aging Time: Range(6-40s), default 20

Forward Delay: Range(4-30s), default 15

STP Mode:

MST Name: String less than 32-byte

MST Version: Range(0-65535), default 0

Save

MST Configuration

Note: It is recommended to disable STP before configuring an instance and enable STP again after configuration, so as to ensure the stability and convergence of network topology.

+ Add Instance

✕ Delete Selected Instance

<input type="checkbox"/>	Instance Number	VLAN	Priority	Action
<input type="checkbox"/>	0	ALL	8	Default instance. Cannot be edited.

Show No.: Total Count: 1

First
Pre
1
Next
Last
GO

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

STP Global Settings

STP Port Settings

RLDP Settings

+ Batch Add

Note: It is recommended to enable Port Fast on the port connected to the PC.

Port	State	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance Cost Priority	Action
Gi0/1	Up	Disabled	Disabled	Null	Point To Point	0 20000 128	Edit
Gi0/2	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/3	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/4	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/5	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/6	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/7	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/8	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/9	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit
Gi0/10	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit

Show No.:10Total Count:28

FirstPre123NextLast1GO

- 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

STP Global Settings	STP Port Settings	RLDP Settings									
<div>Global configuration</div> <p>Note: RLDP enables you to detect link failure quickly. RLDP can run on the port only after it is enabled globally.</p> <p>RLDP: <input checked="" type="checkbox"/></p> <p>Detection Interval: <input type="text" value="3"/> Range(2-15)</p> <p>Detection Count: <input type="text" value="2"/> Range(2-10)</p> <p>errdisable recovery: <input type="text" value=""/> Range(30-66400s)</p> <p><input type="button" value="Save"/></p>											
<div>Port Configuration</div> <p>Note: 1. Enabling RLDP on the port can avoid broadcast storm caused by loops. It is recommended to enable RLDP on the port connected to the PC; 2. Unidirectional/Bidirectional link detection requires the ports on both ends of the link to be enabled with RLDP. It is recommended to configure RLDP to monitor the link between two switches.</p> <p>+ Add Port -X Delete Port</p> <table border="1"> <thead> <tr> <th>Port</th> <th>Detection Type</th> <th>Troubleshooting</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="4">No Record Found</td> </tr> </tbody> </table>				Port	Detection Type	Troubleshooting	Action	No Record Found			
Port	Detection Type	Troubleshooting	Action								
No Record Found											

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.

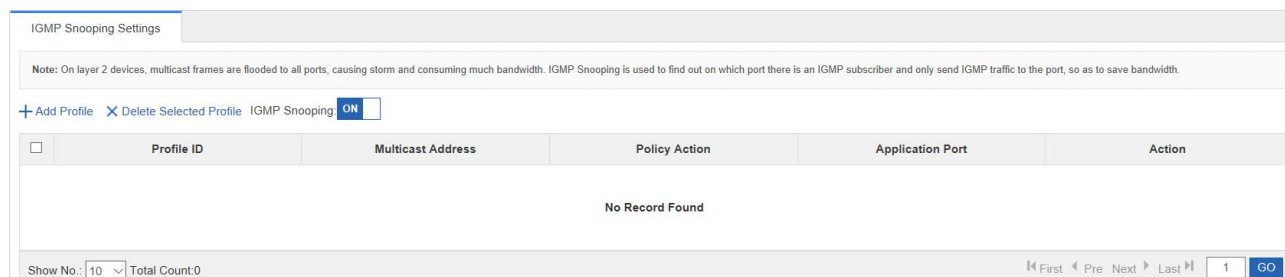
2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the item?" message is displayed.

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



● 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: ☒ ON

DHCP Server Address: [+ Add DHCP Server](#)

Save

[DHCPv6 relay configuration](#)

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

Authentication

The Authentication page allows you to set Eportalv2 and Advanced.

➤ Eportalv2

The following figure shows the Eportalv2 page.

Figure 1-20 Eportalv2

Eportalv2

Advanced

Note: Authentication 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 ☒ eportalv2

Server IP:

Redirection URL:

Portal Key:

Authentication Server: [\[Radius Server Settings\]](#)

Accounting Server:

SNMP Server: [\[SNMP Server\]](#)

Port:

Available

Unavailable

Selected

AG Port

Copper

Fiber

1	3	5	7	9	11	13	15	17	19	21	23				
2	4	6	8	10	12	14	16	18	20	22	24	25	26	27	28

[All](#) [Invert](#) [Deselect](#)

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

Save

Clear

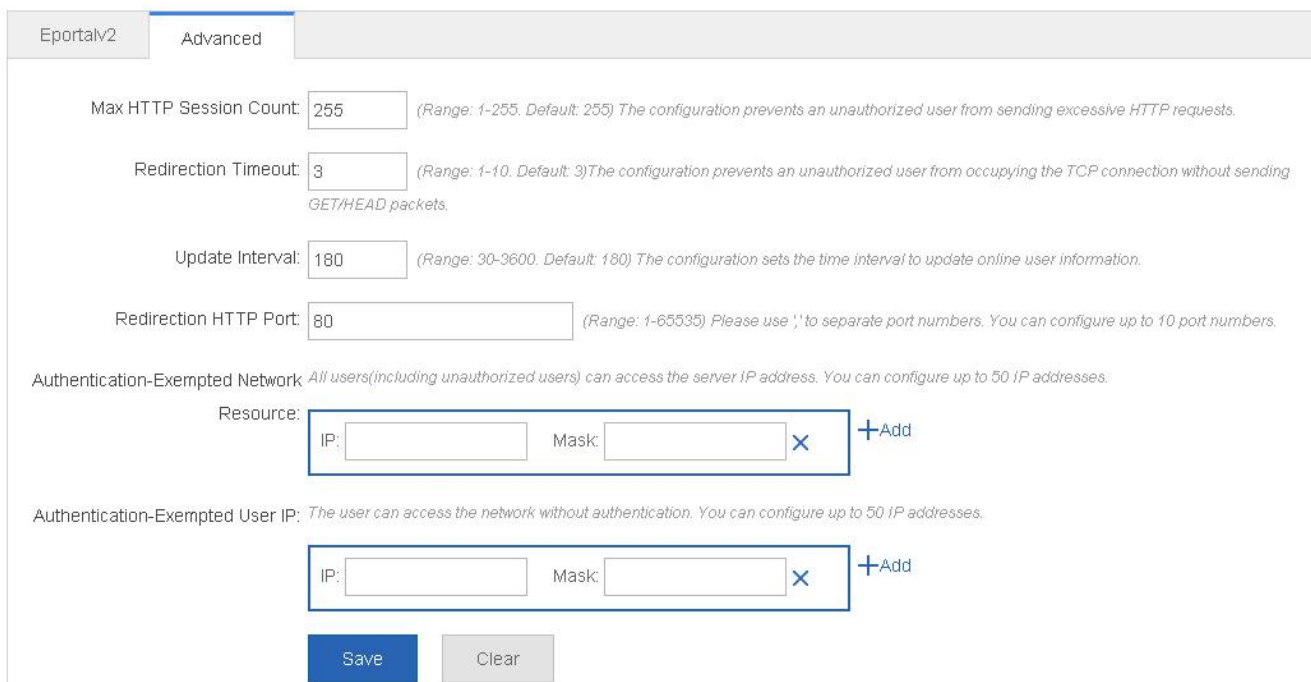
Enter the server IP address and redirection URL, and then click **Save**. A "Configuration succeeded." message is displayed.

www.fs.com

18

Advanced

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



Max HTTP Session Count: (Range: 1-255. Default: 255) The configuration prevents an unauthorized user from sending excessive HTTP requests.

Redirection Timeout: (Range: 1-10. Default: 3) The configuration prevents an unauthorized user from occupying the TCP connection without sending GET/HEAD packets.

Update Interval: (Range: 30-3600. Default: 180) The configuration sets the time interval to update online user information.

Redirection HTTP Port: (Range: 1-65535) Please use ',' to separate port numbers. You can configure up to 10 port numbers.

Authentication-Exempted Network: All users(including unauthorized users) can access the server IP address. You can configure up to 50 IP addresses.

Resource: IP: Mask:

Authentication-Exempted User IP: The user can access the network without authentication. You can configure up to 50 IP addresses.

IP: Mask:

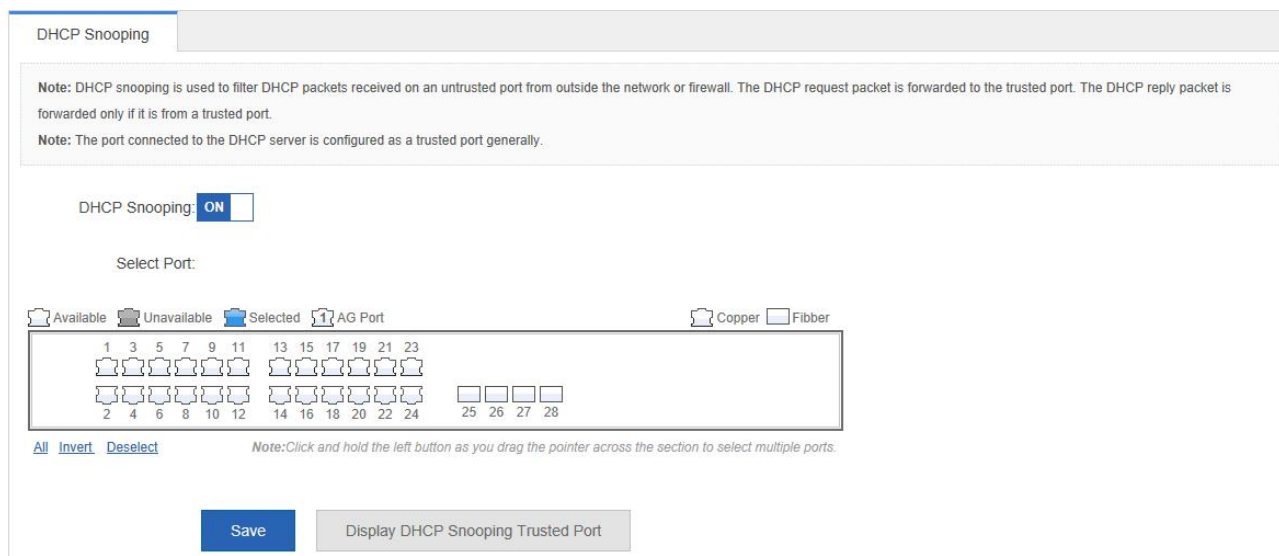
You can set multiple authentication-exempted network resources and user IP addresses. Click **Save**, and a "Configuration succeeded." message is displayed.

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

Note: 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 reply packet is forwarded only if it is from a trusted port.

Note: The port connected to the DHCP server is configured as a trusted port generally.

DHCP Snooping: ☒ ON

Select Port:

Available Unavailable Selected AG Port Copper Fiber

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

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

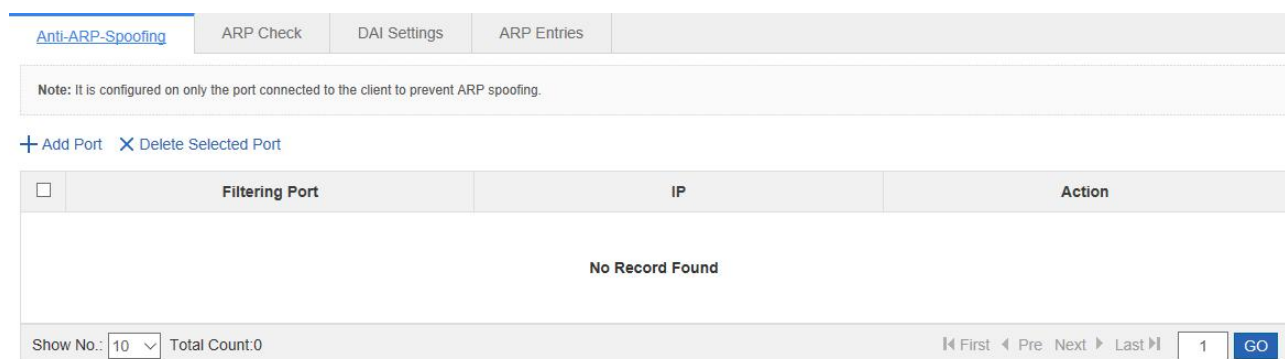
The port connected to the DHCP server must be configured as DHCP trusted port, and the DHCP server connected to a non-trusted port cannot work properly. If the selected port on the panel is a DHCP trusted port. You can directly select a port on the panel and click the **Save** button.

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



- 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.

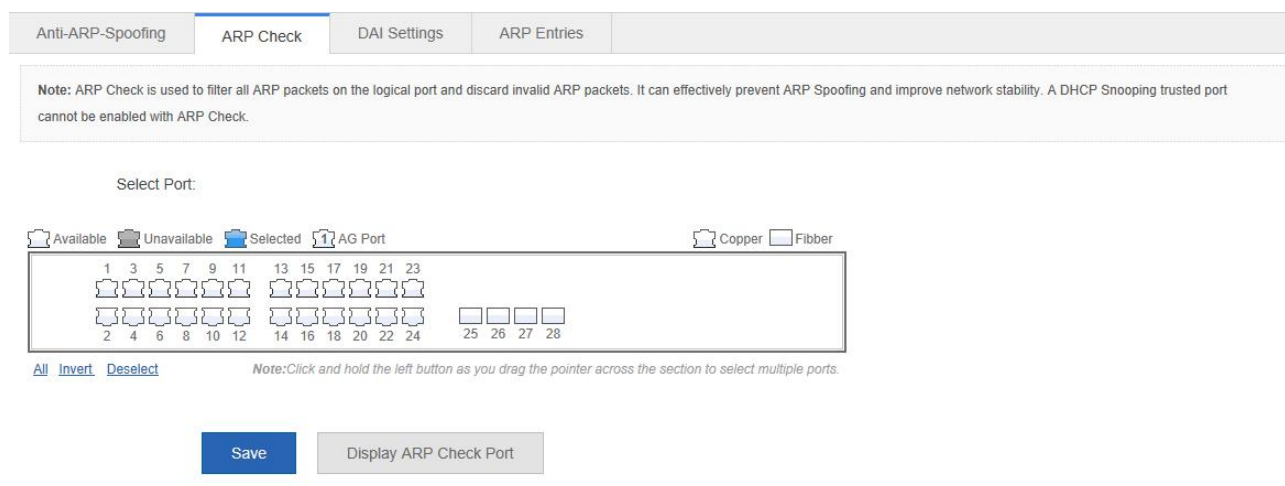
- Deleting filtering port

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

ARP Check

Figure 1-24 ARP Check



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

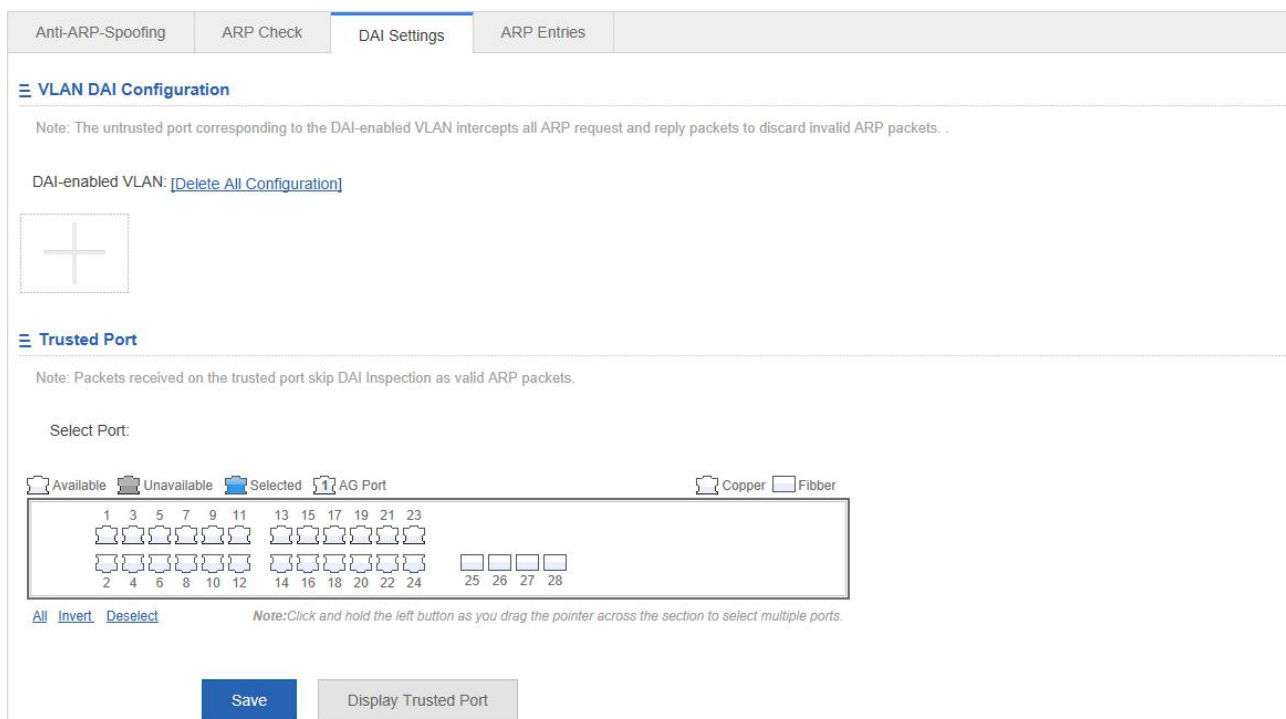
NOTE:

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 Configuration

Note: The untrusted port corresponding to the DAI-enabled VLAN intercepts all ARP request and reply packets to discard invalid ARP packets.

DAI-enabled VLAN: [Delete All Configuration](#)

Trusted Port

Note: Packets received on the trusted port skip DAI Inspection as valid ARP packets.

Select Port:

Available Unavailable Selected AG Port Copper Fiber

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

[All](#) [Invert](#) [Deselect](#) Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.

Save Display Trusted Port

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-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries	
Dynamic Binding>>Static Binding Remove static Binding Manual Binding				IP-based: <input type="text"/> Search
<input type="checkbox"/>	IP	MAC	Type	Action
<input type="checkbox"/>	192.168.182.225	00d0.f822.33b7	Dynamic Binding	Dynamic Binding>>Static Binding
<input type="checkbox"/>	192.168.182.236	1414.4b23.2257	Local ARP Entry	Dynamic Binding>>Static Binding
Show No.: <input type="text" value="10"/> Total Count: 2 First Pre 1 Next Last <input type="text" value="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.

Port Settings

Figure 1-27 Port Settings

Port Settings

User Binding

Note: IP Source Guard is applied in combination with DHCP Snooping. Port-based IP Source Guard takes effect on only the untrusted port enabled with DHCP Snooping. Otherwise, IP Source Guard does not take effect.

+ Add Port

X Delete Selected Port

<input type="checkbox"/>	Port	Filter Type	Filter Mode	IP	MAC	VLAN ID	Action
No Record Found							

Show No.:

10

Total Count:0

First

Pre

Next

Last

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

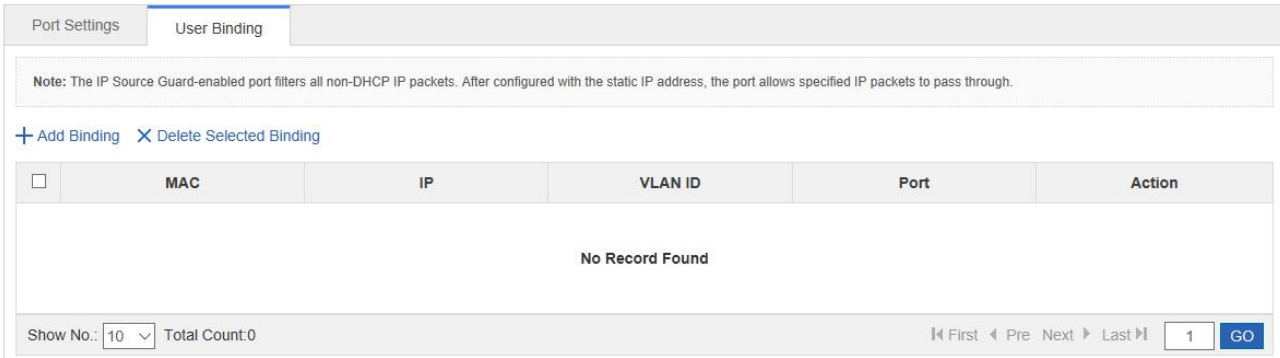
After you click **Edit** in the Action column, the information of the corresponding filtering port is displayed on the page. After editing the information, click **Save**. An "Edit succeeded." message is displayed.

- 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



Note: The IP Source Guard-enabled port filters all non-DHCP IP packets. After configured with the static IP address, the port allows specified IP packets to pass through.

[+ Add Binding](#) [X Delete Selected Binding](#)

	MAC	IP	VLAN ID	Port	Action
No Record Found					

Show No.: 10 Total Count:0

First Pre Next Last 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.

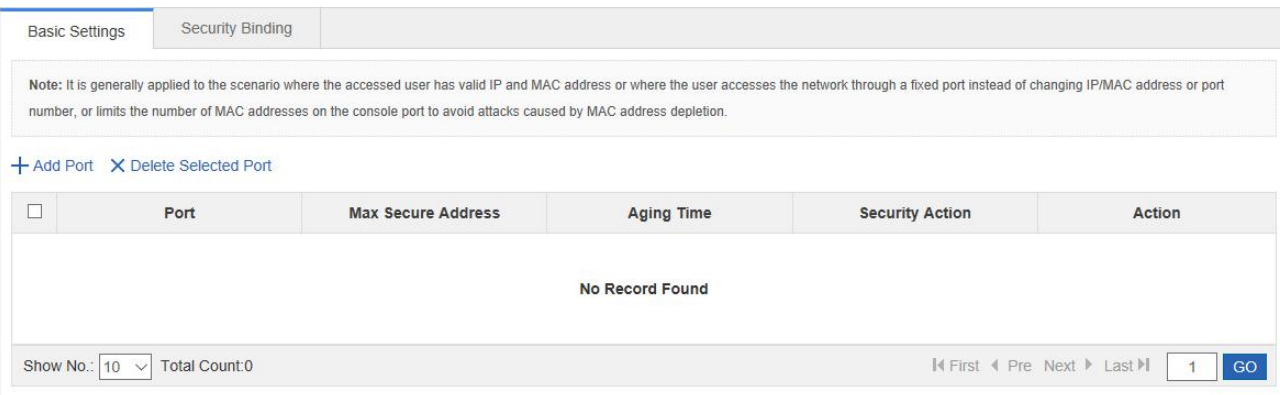
- Deleting user binding

- 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



Note: It is generally applied to the scenario where the accessed user has valid IP and MAC address or where the user accesses the network through a fixed port instead of changing IP/MAC address or port number, or limits the number of MAC addresses on the console port to avoid attacks caused by MAC address depletion.

[+ Add Port](#) [X Delete Selected Port](#)

	Port	Max Secure Address	Aging Time	Security Action	Action
No Record Found					

Show No.: 10 Total Count:0

First Pre Next Last 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

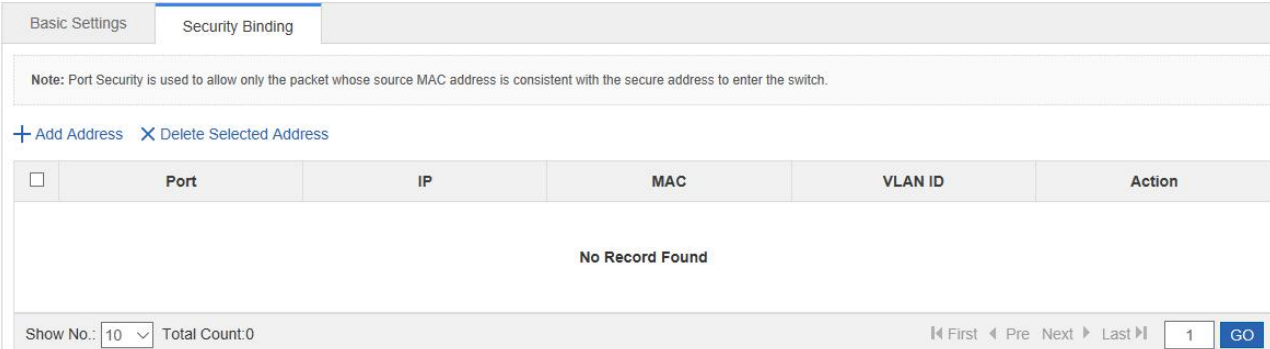
After you click **Edit** in the **Action** column, the binding information of the corresponding user is displayed on the page. After editing the information, click **Save**. A "Configuration succeeded." message is displayed.

- Deleting security port

- 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



- 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: ☒ Enable ARP-guard, so as to prevent a large number of invalid ARP packets from attacking the device. The number of ARP packets handled by the device per second is **no more than 4**.
[\[ARP-guard List\]](#)

IP-guard: ☒ Enable IP-guard, so as to prevent hackers from scanning the entire network and consuming bandwidth. The number of packets handled by the device per second is **no more than 4**.
[\[IP-guard List\]](#)

ICMP-guard: ☒ Enable ICMP-guard, so as to prevent a large number of invalid ICMP packets from consuming bandwidth and CPU resources. The number of ICMP packets handled by the device per second is **no more than 4**.
[\[ICMP-guard List\]](#)

DHCP-guard: ☒ Enable DHCP-guard, so as to prevent malicious requests from exhausting DHCP pools and leaving legitimate users unable to access the Internet.
[\[DHCP-guard List\]](#)

DHCPv6-guard: ☒ Enable DHCPv6-guard, so as to prevent malicious requests from exhausting DHCPv6 pools and leaving legitimate users unable to access the Internet.
[\[DHCPv6-guard List\]](#)

ND-guard: ☒ Enable ND-guard, so as to prevent Neighbor Discovery packets from consuming bandwidth, The number of ND packets handled by the device per second is **no more than 15**.

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 X Delete Selected Port

<input type="checkbox"/>	Port	Broadcast	Multicast	Unicast	Action	
<input type="checkbox"/>	Gi0/1	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/2	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/3	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/4	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/5	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/6	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/7	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/8	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/9	-	-	-	Edit	Delete
<input type="checkbox"/>	Gi0/10	-	-	-	Edit	Delete

Show No.: Total Count:28

First
Pre
1
2
3
Next
Last
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.

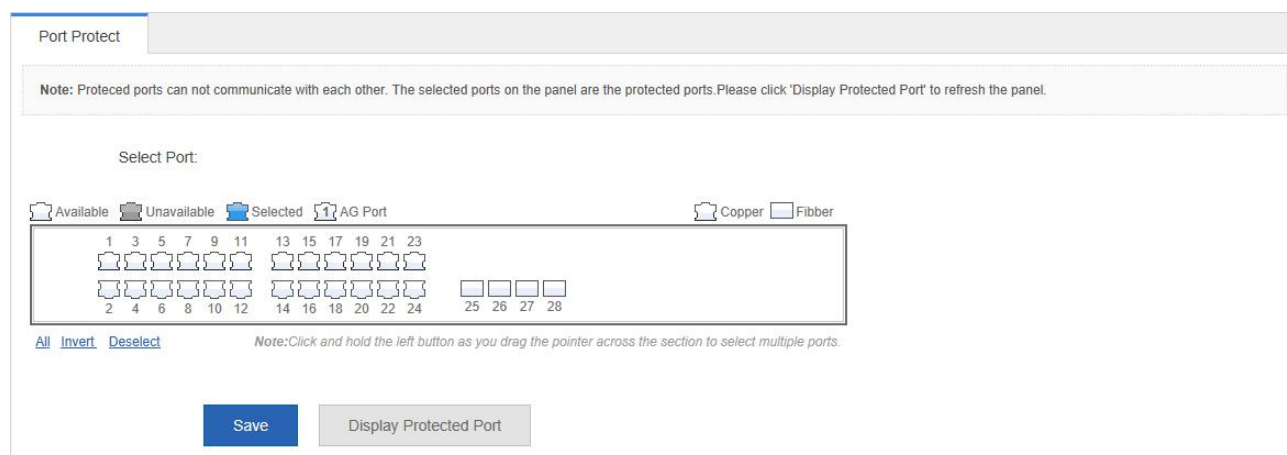
After you confirm the operation, a "Delete succeeded." message is displayed.

1.3.4 Advanced

Port Protection

The following figure shows the Port Protect Settings page.

Figure 1-33 Port Protect Settings



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

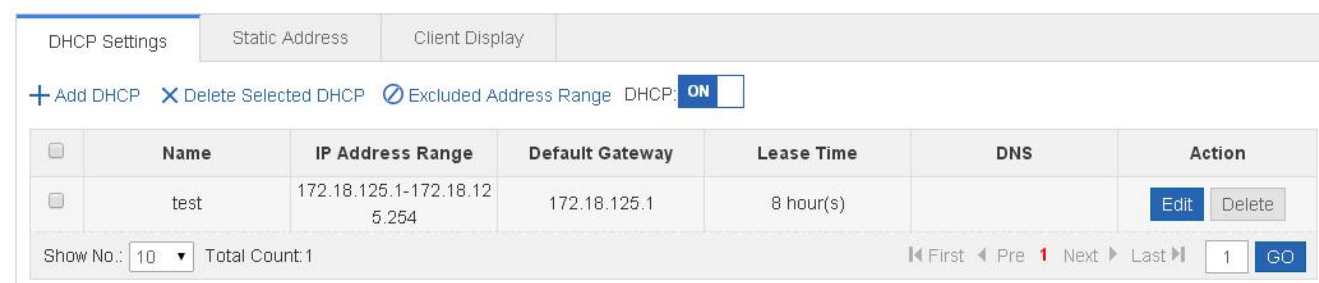
DHCP

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



- 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 Client Display

DHCP Settings

Static Address

Client Display

+ Add Static Address

✕ Delete Selected Address

<input type="checkbox"/>	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
<input type="checkbox"/>	user1	172.18.125.21	255.255.255.0		2244.2828.6262		<div>EditDelete</div>

Show No.:

10

Total Count: 1

⏮ First

◀ Pre

1

Next ▶

Last ⏭

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.

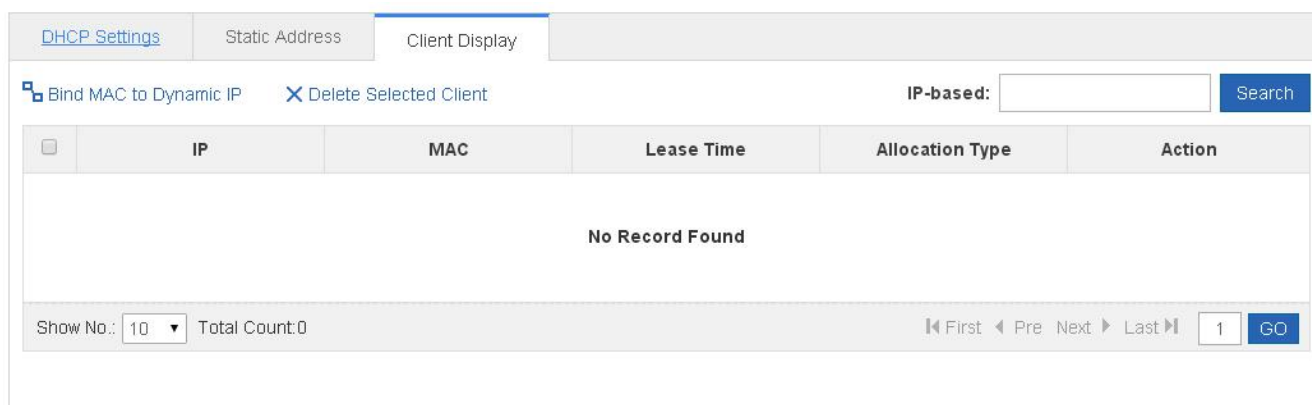
- Deleting static address

- 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.

Client Display

The following figure shows the ACL List page.

Figure 1- 36 Client Display



- Search by IP address

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

- Binding MAC address to dynamic IP address

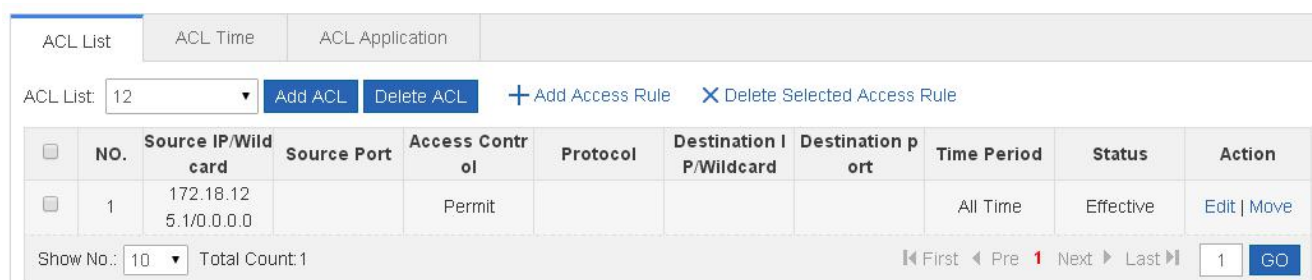
You can select multiple clients from the client list and click Bind MAC to Dynamic IP for binding.

ACL

ACL List

The following figure shows the ACL List page.

Figure 1-37 ACL List



- 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

ACL Application

+ Add Time Object

X Delete Selected Time Object

<input type="checkbox"/>	Time Object	Day	Time Period	Action
<input type="checkbox"/>	time1	Monday Tuesday	2:00-13:00	<div>EditDelete</div>
<input type="checkbox"/>	time2	Weekend	0:00-23:59	<div>EditDelete</div>

Show No.: 10

Total Count:2

First

Pre

1

Next

Last

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

+ Add Port

✕ Delete Port

<input type="checkbox"/>	ACL	Port	Direction	Action
No Record Found				

Show No.:

10

Total Count:0

First

Pre

Next

Last

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

➤ Class Settings

The following figure shows the Class Settings page.

Figure 1-40 Class Settings



	Class Name	ACL	Action
<input type="checkbox"/>	classname1	12	Edit Delete
<input type="checkbox"/>	classname2	12	Edit Delete

Show No.: 10 Total Count: 2

First Pre 1 Next Last 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.

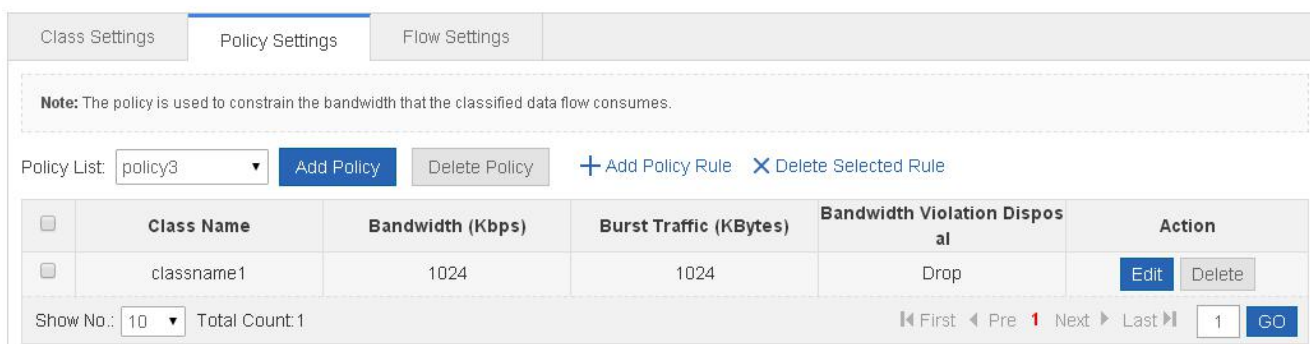
- Deleting class

- 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



	Class Name	Bandwidth (Kbps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
<input type="checkbox"/>	classname1	1024	1024	Drop	Edit Delete

Show No.: 10 Total Count: 1

First Pre 1 Next Last GO

- 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 from 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.

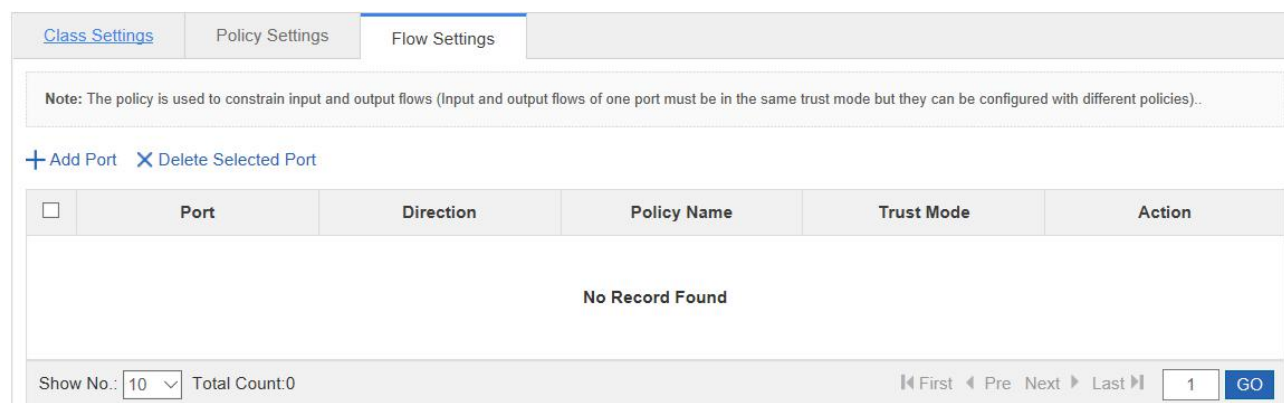
2) After you click Delete in the Action column, an “Are you sure you want to delete the item?” message is displayed.

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



- 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

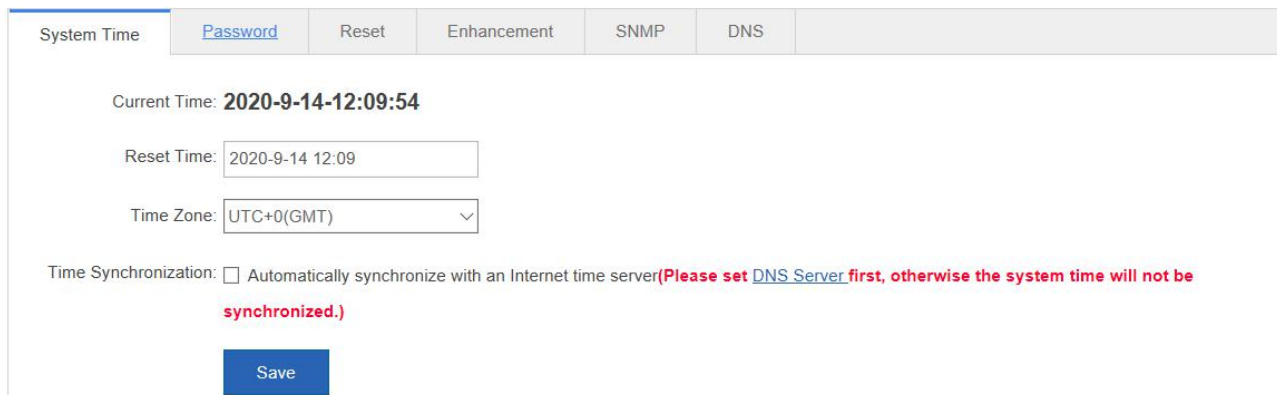
The system management page allows you to perform system settings, system upgrade and configuration management and configure administrator permissions.

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: **2020-9-14-12:09:54**

Reset Time:

Time Zone:

Time Synchronization: ☐ Automatically synchronize with an Internet time server **(Please set [DNS Server](#) first, otherwise the system time will not be synchronized.)**

Save

● System time

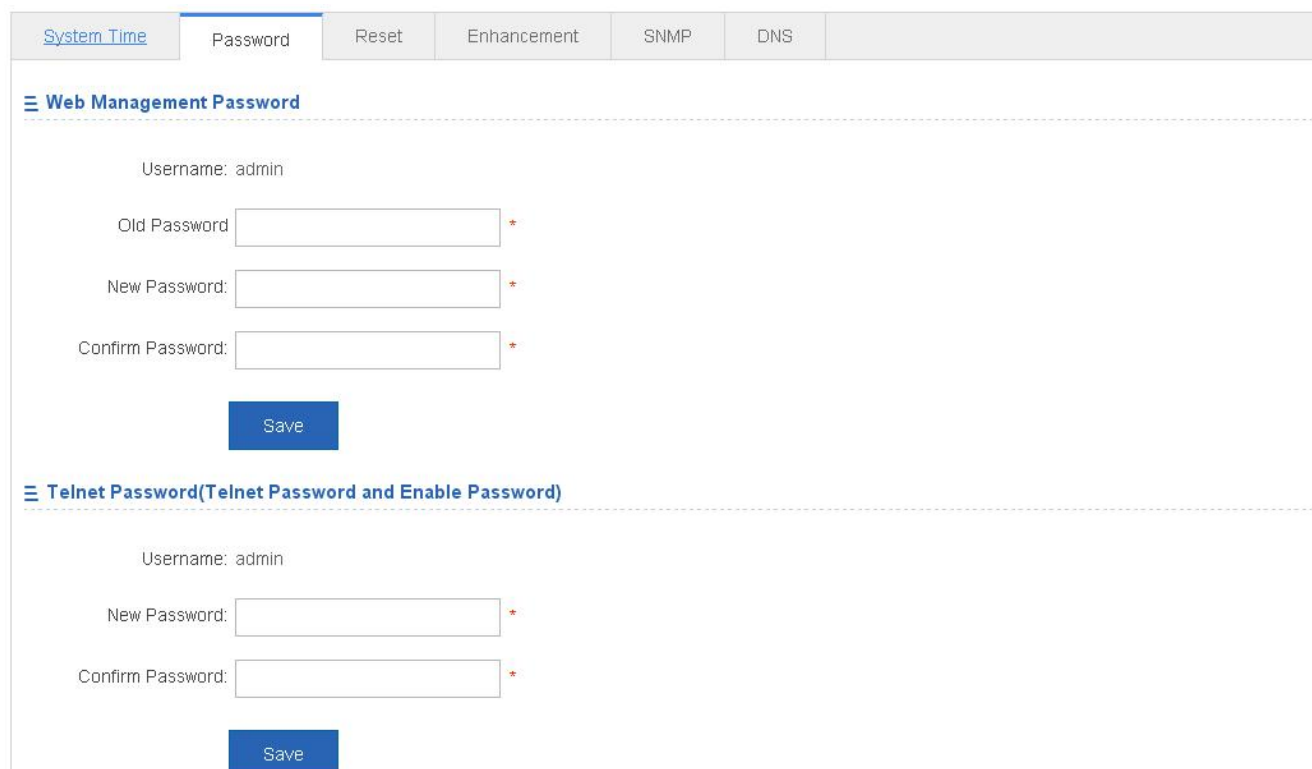
The current system time is displayed on the page. You can set the current system time manually. Alternatively, you can select Automatically synchronize with an Internet time server for time setting. After that, click Save. A "Configuration succeeded." message is displayed.

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.

Password

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



[System Time](#) **Password** Reset Enhancement SNMP DNS

Web Management Password

Username: admin

Old Password:

New Password:

Confirm Password:

Save

Telnet Password(Telnet Password and Enable Password)

Username: admin

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
-------------	----------	-------	-------------	------	-----

Restore Factory Settings

Note: After the device is reset to the factory default settings, all configurations will be removed. Please [Export Current Configuration](#) before resetting the device.

Restore Factory Settings

Display Current Configuration

Import/Export Configuration

Note: Please don't close or update the page during import, or import will fail. If you want to apply the new configuration, please restart the device on this page, or the configuration will not take effect.

File Name:

File...

Import

Export Current Configuration

- **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.

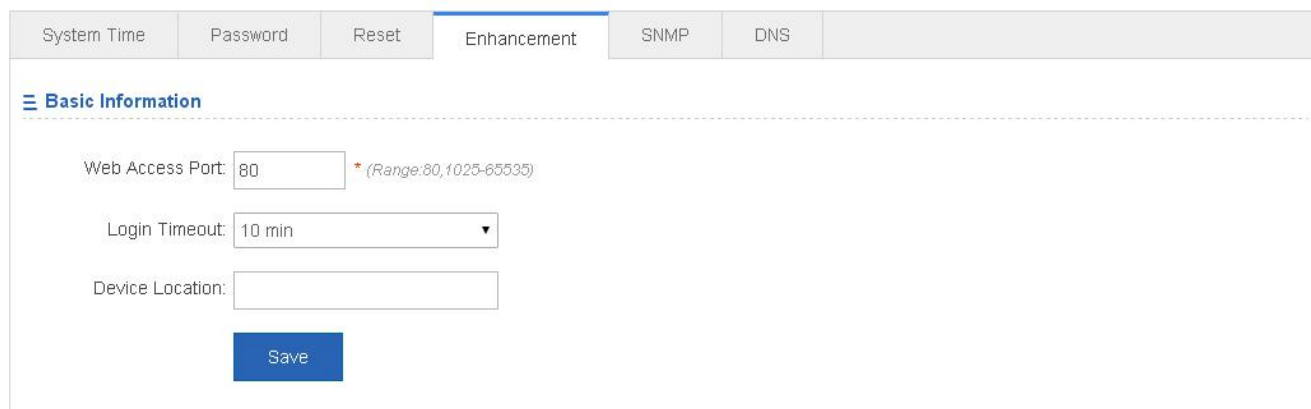
- **Restoring factory settings**

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



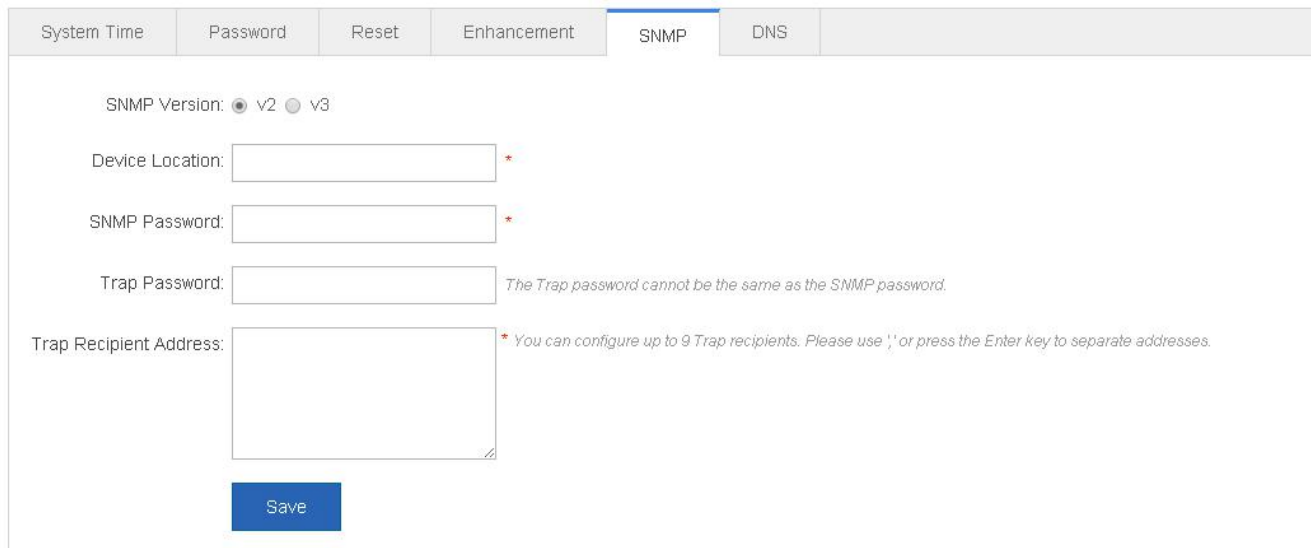
The screenshot shows the 'Enhancement' tab selected in the top navigation bar. Below the tabs, there is a section titled 'Basic Information'. It contains three input fields: 'Web Access Port' with a value of 80 and a range note '(Range:80,1025-65535)', 'Login Timeout' with a value of 10 min, and 'Device Location' which is empty. A blue 'Save' button is located at the bottom of the section.

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



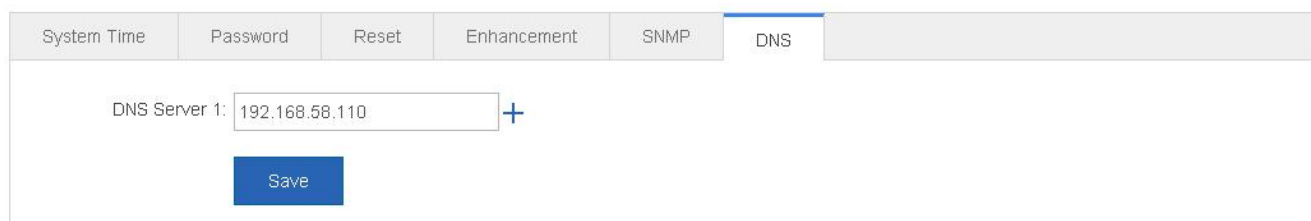
The screenshot shows the 'SNMP' tab selected in the top navigation bar. Below the tabs, there are several configuration options: 'SNMP Version' with radio buttons for v2 (selected) and v3; 'Device Location' (mandatory, marked with a red asterisk); 'SNMP Password' (mandatory, marked with a red asterisk); 'Trap Password' (optional, with a note 'The Trap password cannot be the same as the SNMP password'); and 'Trap Recipient Address' (optional, with a note '* You can configure up to 9 Trap recipients. Please use ',' or press the Enter key to separate addresses.'). A blue 'Save' button is located at the bottom of the section.

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



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

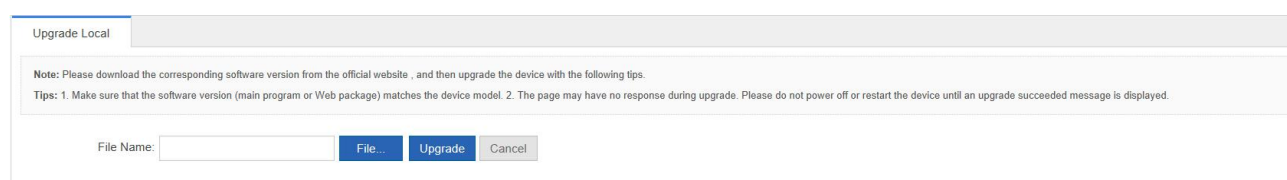
System Upgrade

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



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

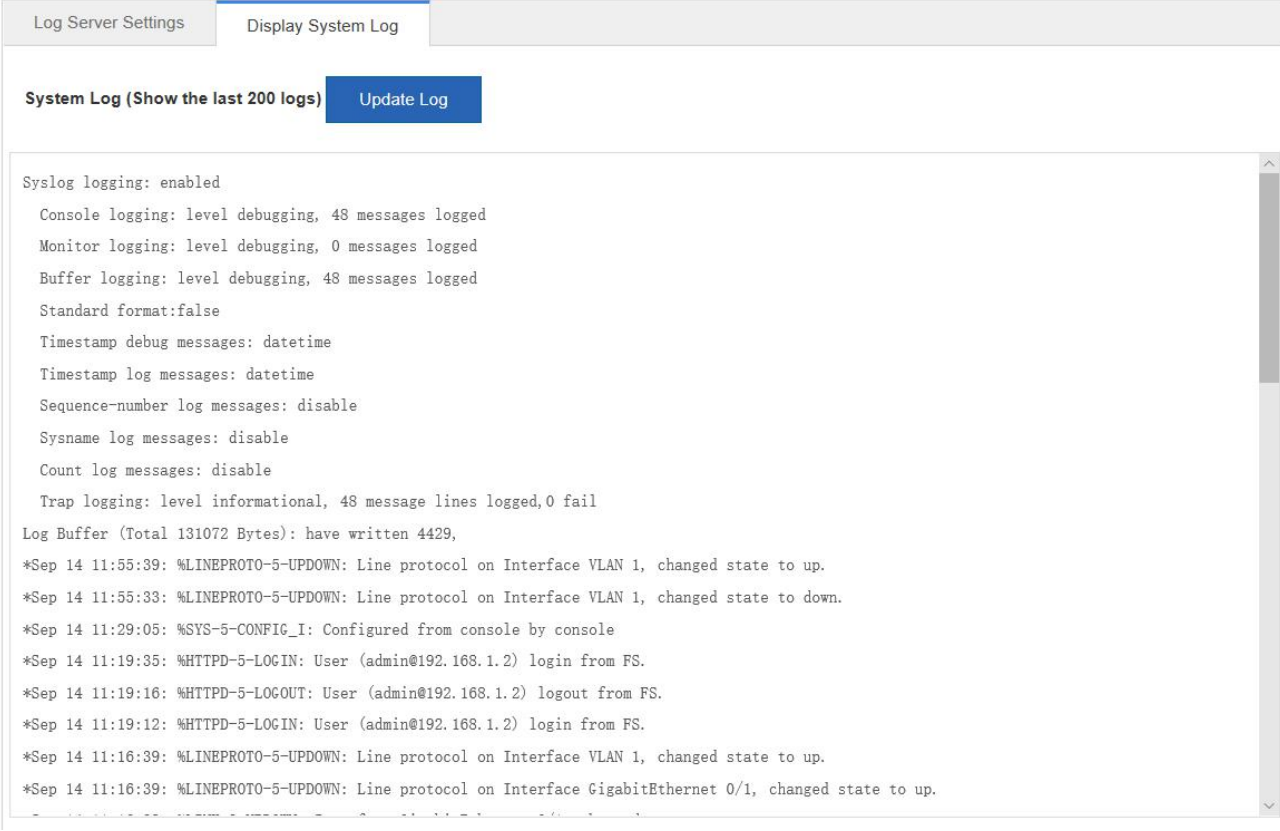


Set various parameters such as Server IP Address and Logging Level. The device sends the SYSLOG log to the corresponding server after the configuration is complete.

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 debugging, 48 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 48 messages logged
Standard format:false
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: disable
Sysname log messages: disable
Count log messages: disable
Trap logging: level informational, 48 message lines logged,0 fail
Log Buffer (Total 131072 Bytes): have written 4429,
*Sep 14 11:55:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to up.
*Sep 14 11:55:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to down.
*Sep 14 11:29:05: %SYS-5-CONFIG_I: Configured from console by console
*Sep 14 11:19:35: %HTTPD-5-LOGIN: User (admin@192.168.1.2) login from FS.
*Sep 14 11:19:16: %HTTPD-5-LOGOUT: User (admin@192.168.1.2) logout from FS.
*Sep 14 11:19:12: %HTTPD-5-LOGIN: User (admin@192.168.1.2) login from FS.
*Sep 14 11:16:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1, changed state to up.
*Sep 14 11:16:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up.
```

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

The following figure shows the Ping page.

Figure 1-52 Ping



Ping Tracert Cable Detection Collection

Destination IP or Domain *

name:

Timeout Period (1-10):

Repetition Count (1-100):

Detect

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

Tracert

The following figure shows the Tracert page.

Figure 1-53 Tracert

Ping

Tracert

Cable Detection

Collection

Destination IP or Domain

*

name:

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

Ping

Tracert

Cable Detection

Collection

Note: Fast port detects only A and B two pairs of core, length error 10 m

Select Port:

Available

Unavailable

Selected

AG Port

Copper

Fiber

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

25 26 27 28

Deselect

Detect

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

Ping

Tracert

Cable Detection

Collection

Note: Fast port detects only A and B two pairs of core, length error 10 m

Select Port:

Available

Unavailable

Selected

AG Port

Copper

Fiber

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

25 26 27 28

Deselect

Detect

Test Results:



 <https://www.fs.com>



The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.