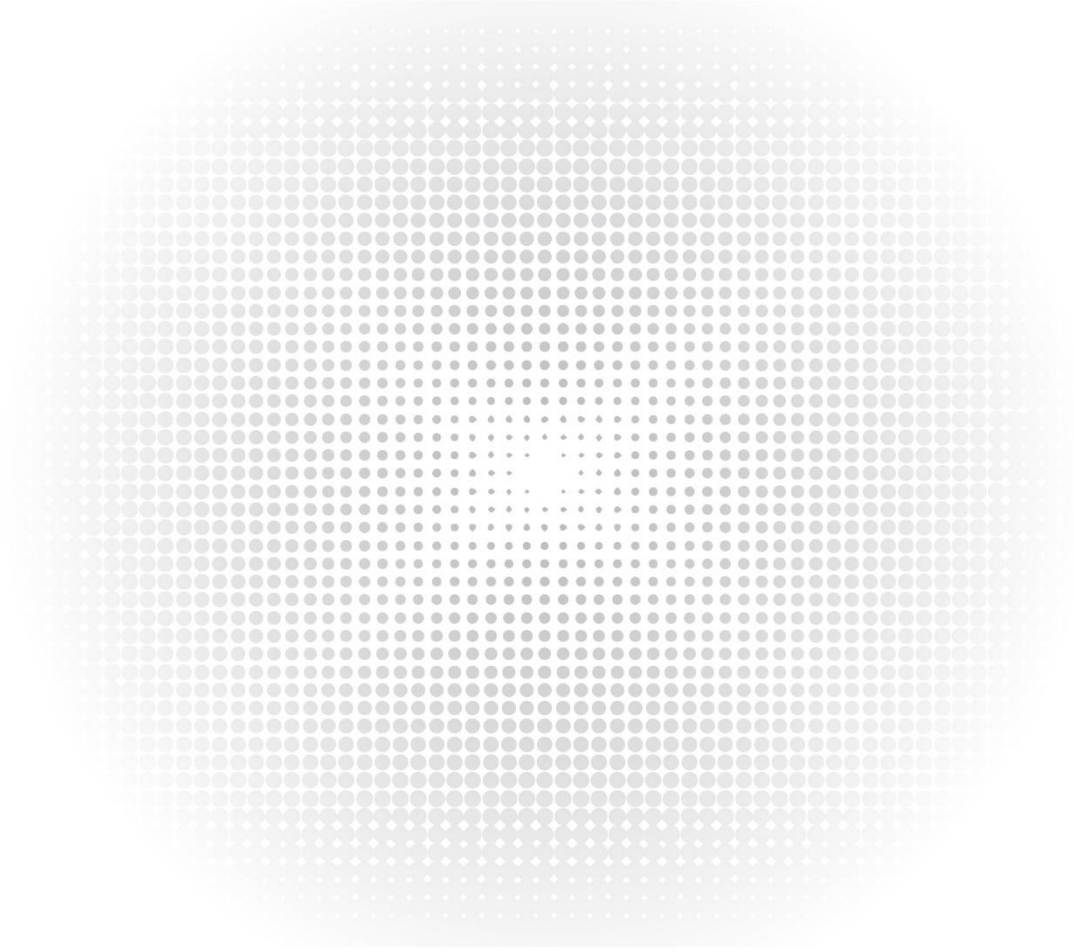
S3410-10TF-P Switch Web Configuration Guide

Model: S3410-10TF-P



Configuration Guide

Contents

1. Web-Based Configuration

1.1 Overview

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

Currently, this file is applicable to only switches.

1.2 Application

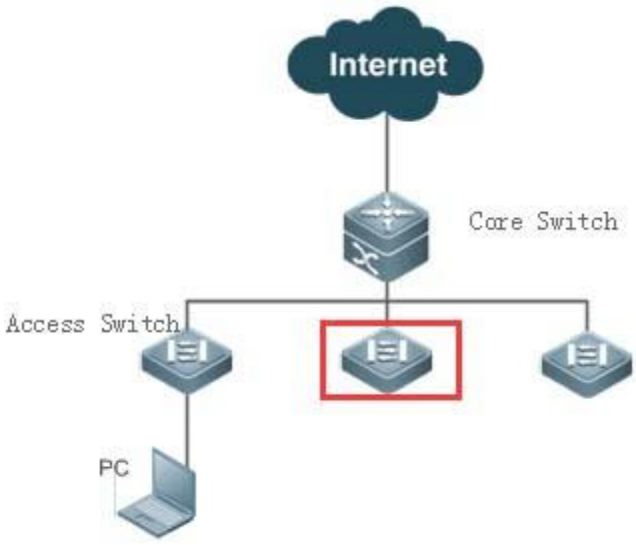
Application	Description
Web-based Management	After finishing relevant configuration, a user can access the Web-based management system through a browser

1.2.1 Web-based Management

Scenario

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

Figure 1- 1



NOTE:

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

Function Deployment

↘ Configuration Environment Requirements

Requirements for Client

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

Requirements for server

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

NOTE:

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

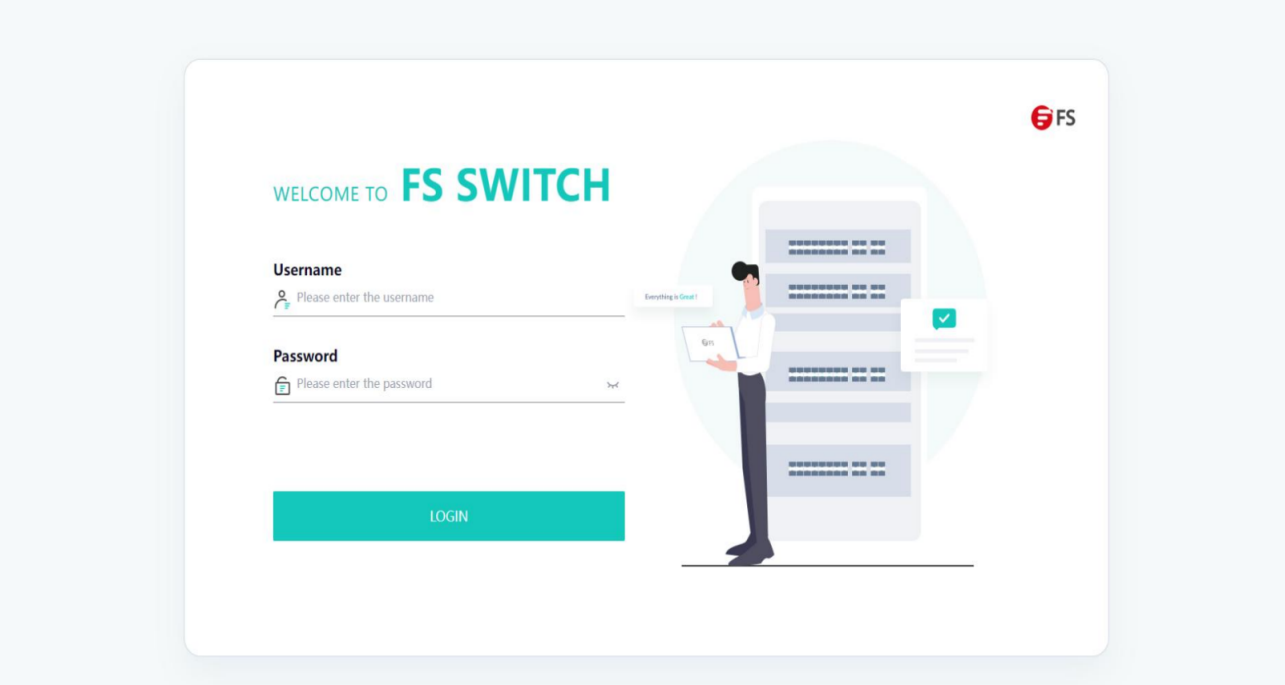
NOTE:

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

Login

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



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

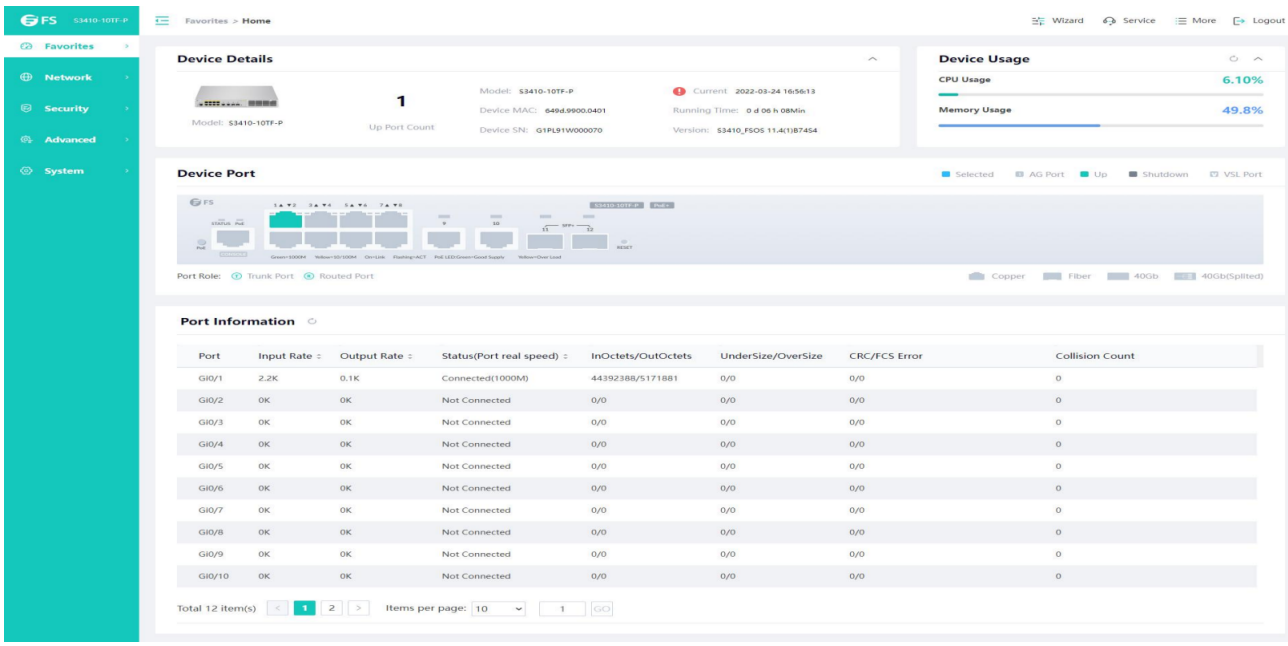
Default Username/Password	Permission Description
admin / admin	Super administrator who possesses all permissions

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



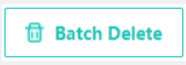
NOTE:

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

1.3 Web Management System

Basic Concepts

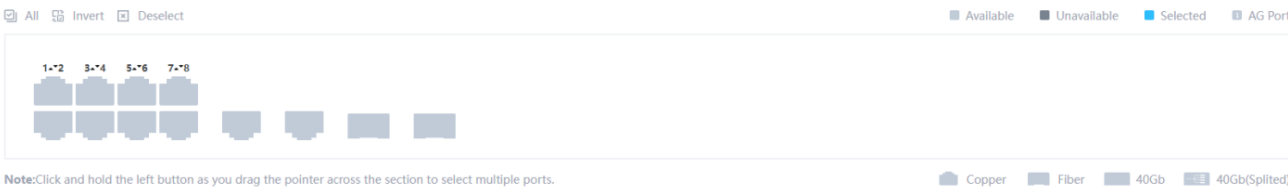
↘ Various Icons and Buttons on the GUI

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

Icon/Button	Note
	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	Save button. You can click this button to submit and save the input information
	Add setting
	Delete setting
All Invert Deselect	Batch processing operations on panel ports. These icons are located on the lower right of the panel. These icons are available only on the panel where you are allowed to select multiple ports
	If this mark is displayed behind a text box, the item corresponding to this text box is mandatory
	Note
	Warning

System Operations

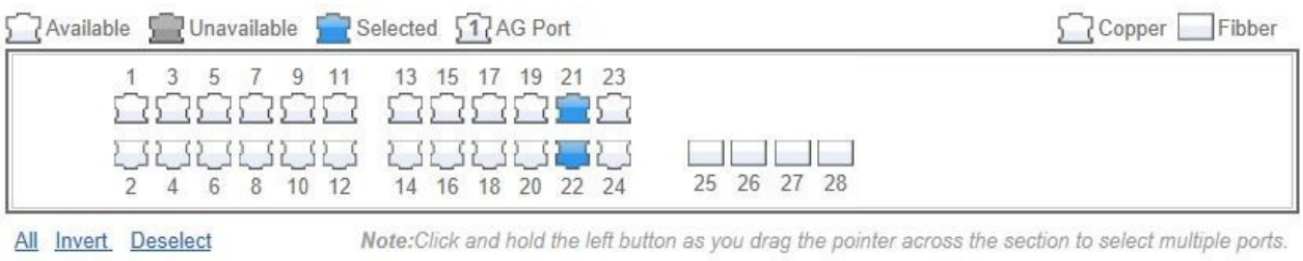
1) Standalone Device Panel



■ 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
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
Feature	**Description**
Anti-ARP-Attack	Allows you to perform anti-ARP-spoofing settings, ARP check settings, DAI settings, and ARP entry settings
IP Source Guard	Allows you to perform port settings and user binding
Port Security	Allows you to perform basic settings and security binding
NFPP	Allows you to view the content related to NFPP anti-attack
Storm Control	Allows you to perform storm control
Port Protection	Allows you to configure port protection
DHCP	Allows you to perform DHCP settings and static address allocation and access the client list
ACL	Allows you to set the ACL list and ACL time and apply ACL
QoS	Allows you to perform classification setting, policy setting, and stream setting
System Settings	Allows you to set the system time, modify the password, restart the system, restore to default factory settings, configure enhanced function, and set the SNMP and DNS
System Upgrade	Allows you to perform local upgrade and online upgrade
Administrator Permissions	Allows you to set the administrator permissions
System Logging	Allows you to configure the log server and view system logs
Network Detection	Allows you to configure ping detection, tracert detection, and cable detection

1.3.1 Favorites

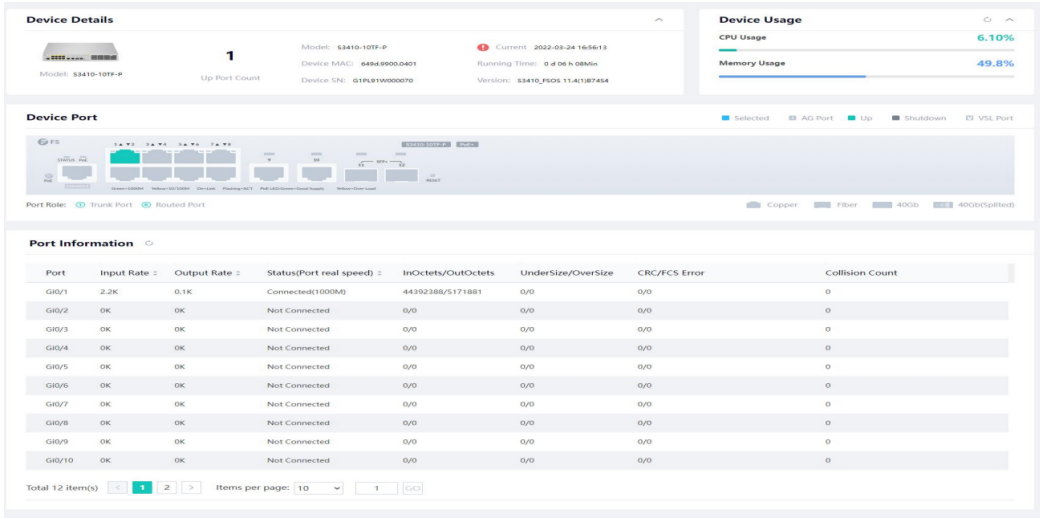
You can access secondary menus through the primary menu Favorites, including Home page, VLAN, Port and Restart.

Home Page

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

The following figure shows the home page.

Figure 1- 4 Home Page



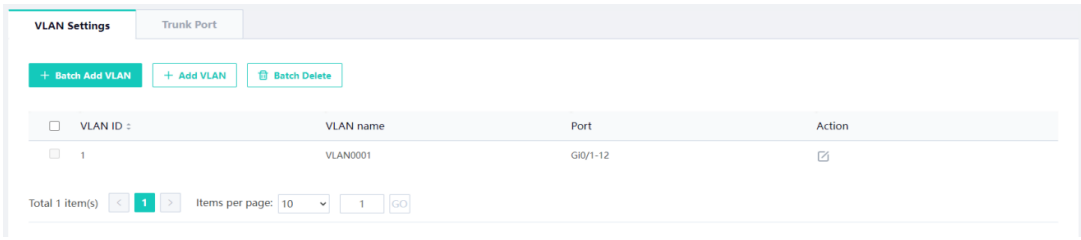
VLAN

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.

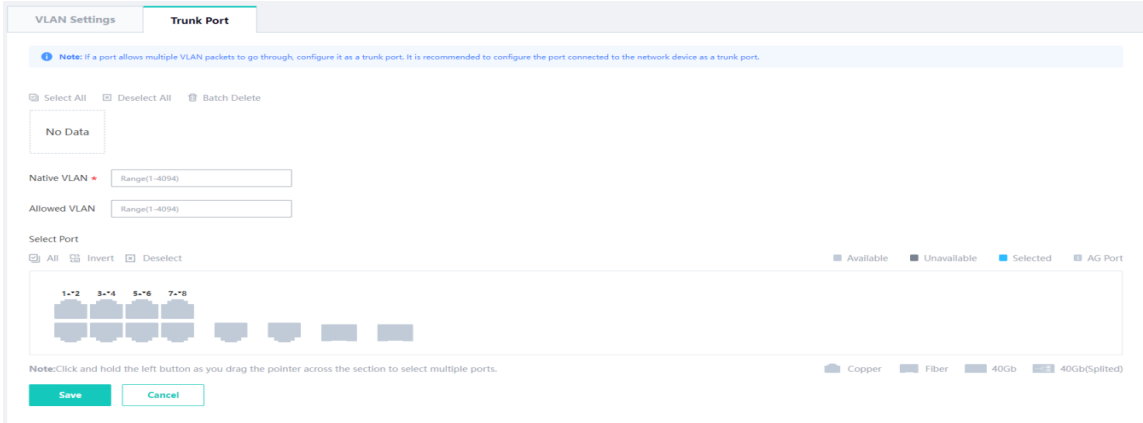
NOTE:

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



- 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.

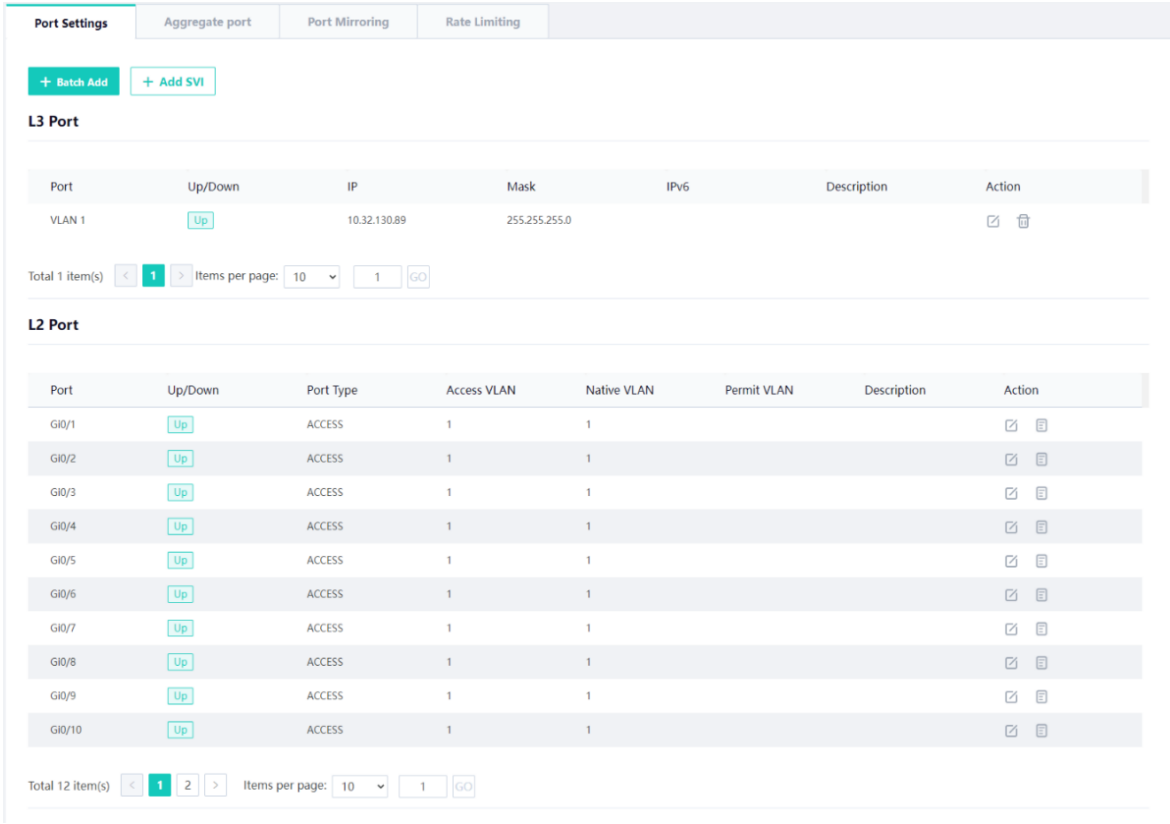
After you confirm the operation, a "Delete succeeded." message is displayed.

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



■ 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.

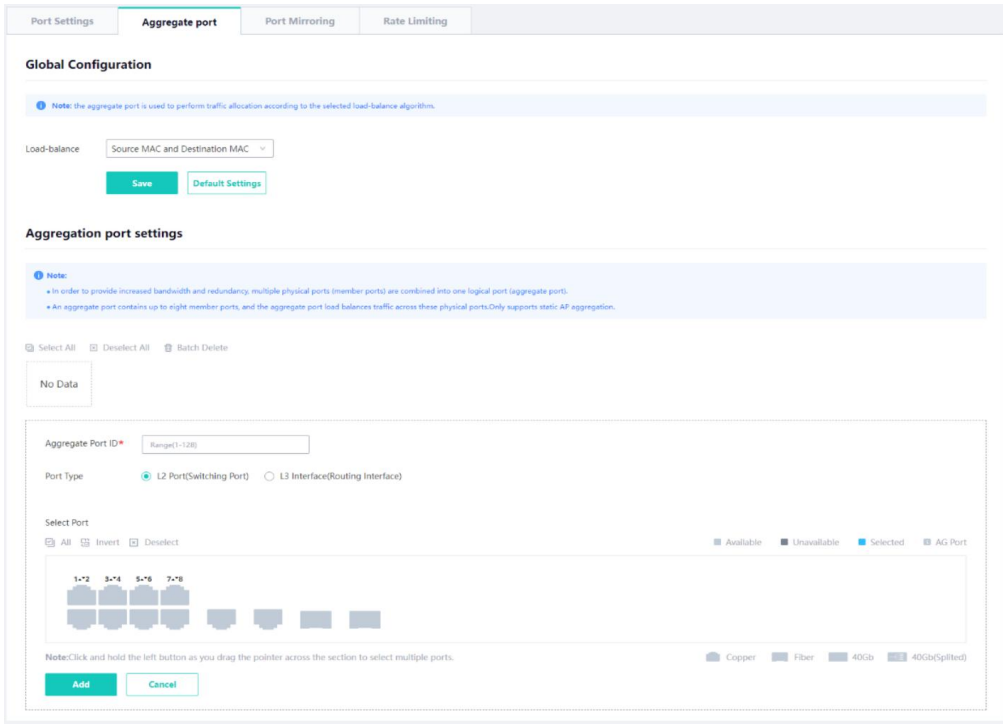
■ Editing port

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



■ 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.

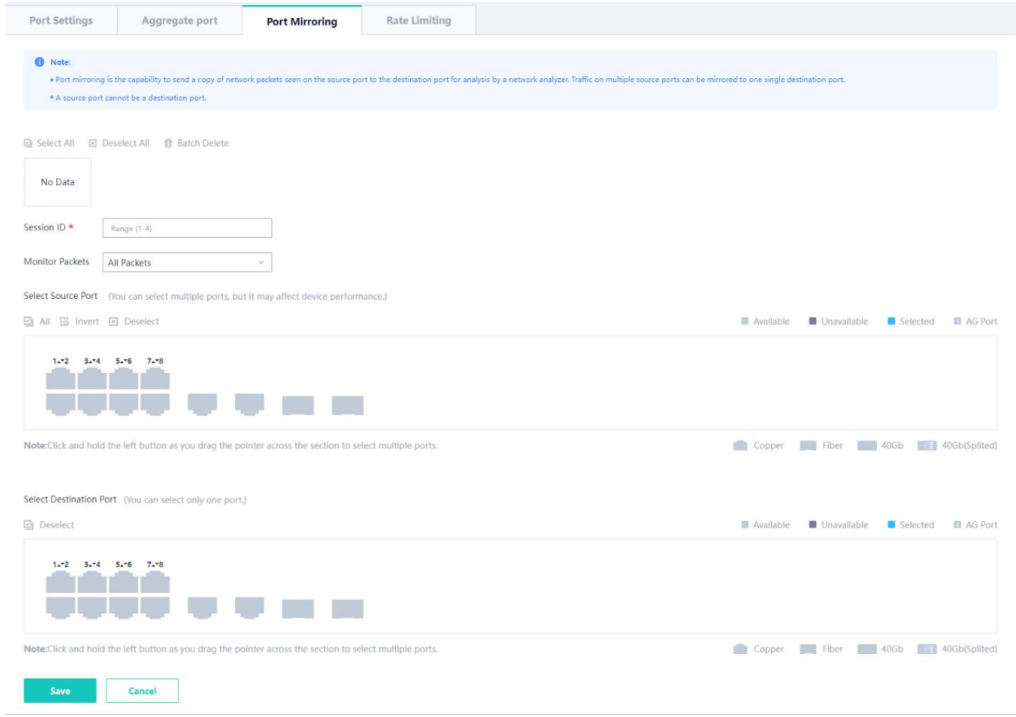
NOTE:

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



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.

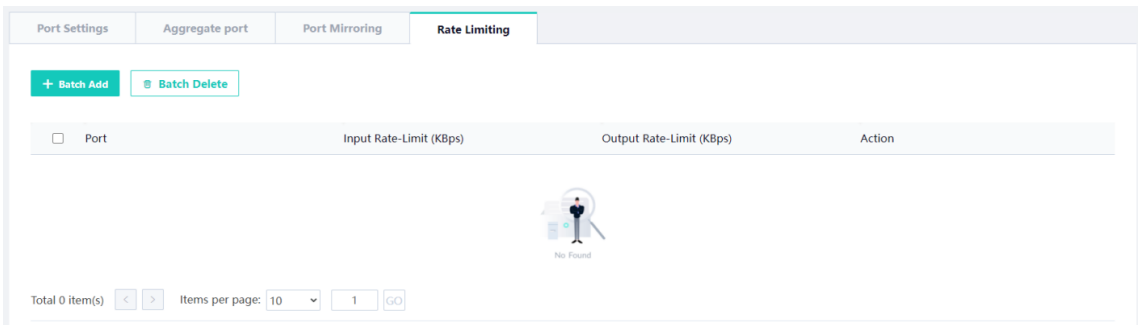
NOTE:

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



■ 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

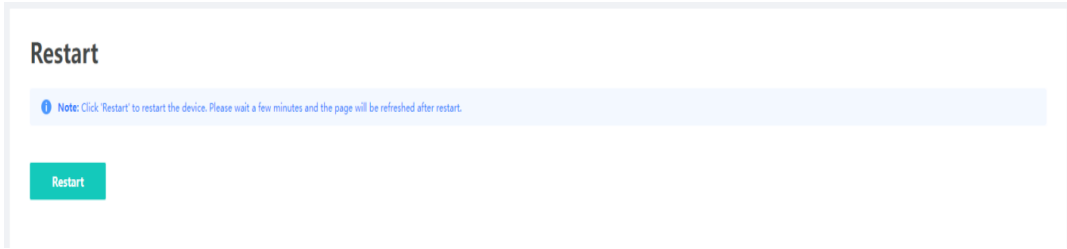
1) You can select multiple ports from the rate limiting port list and click **Batch Delete** to delete the ports in batches.

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



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

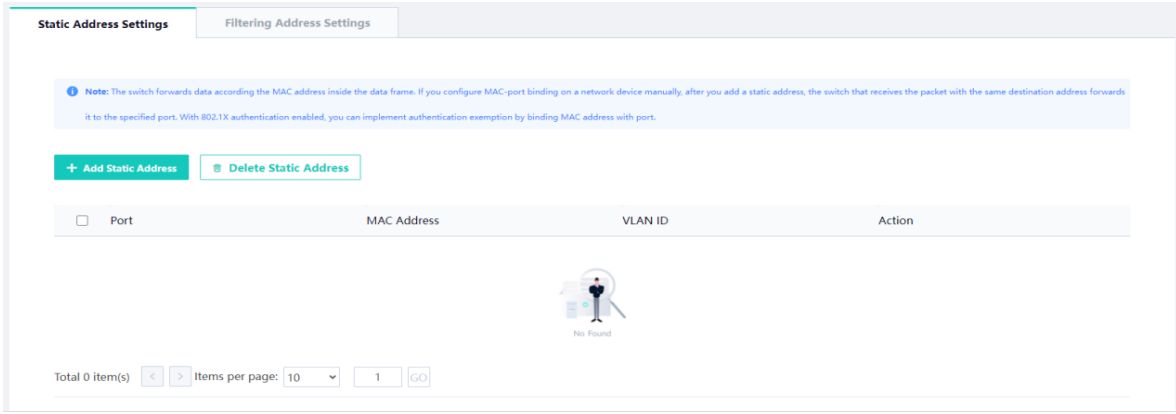
You can access secondary menus through the primary menu Network, including MAC Address, Routing, STP,, IGMP Snooping, Authentication and DHCP Relay.

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

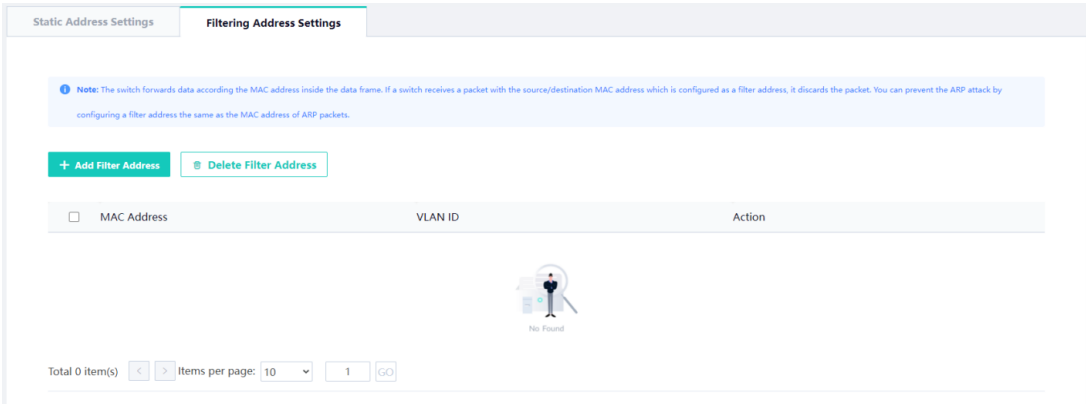
To add a static address, input the MAC address, VLAN ID and select a port, and then click **Save**. The newly added static address is displayed in the address list after a "Configuration succeeded." message is displayed.

- 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.

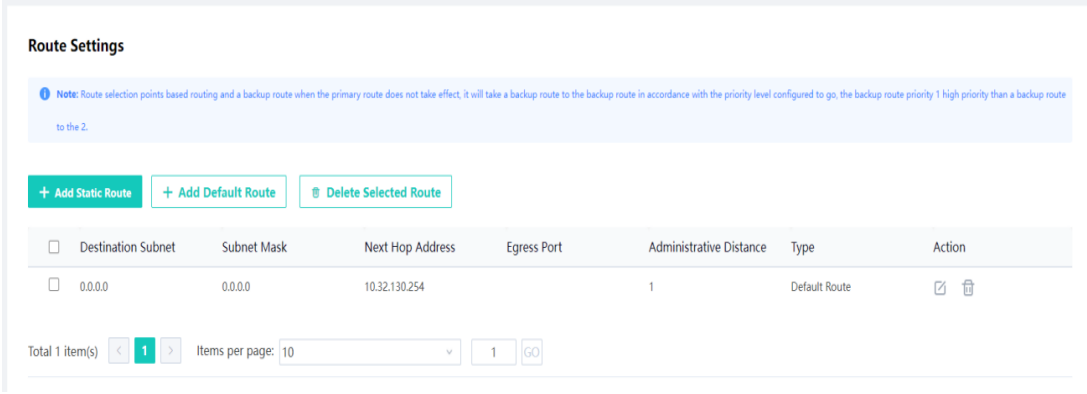
- Deleting Filtering Address

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



■ 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

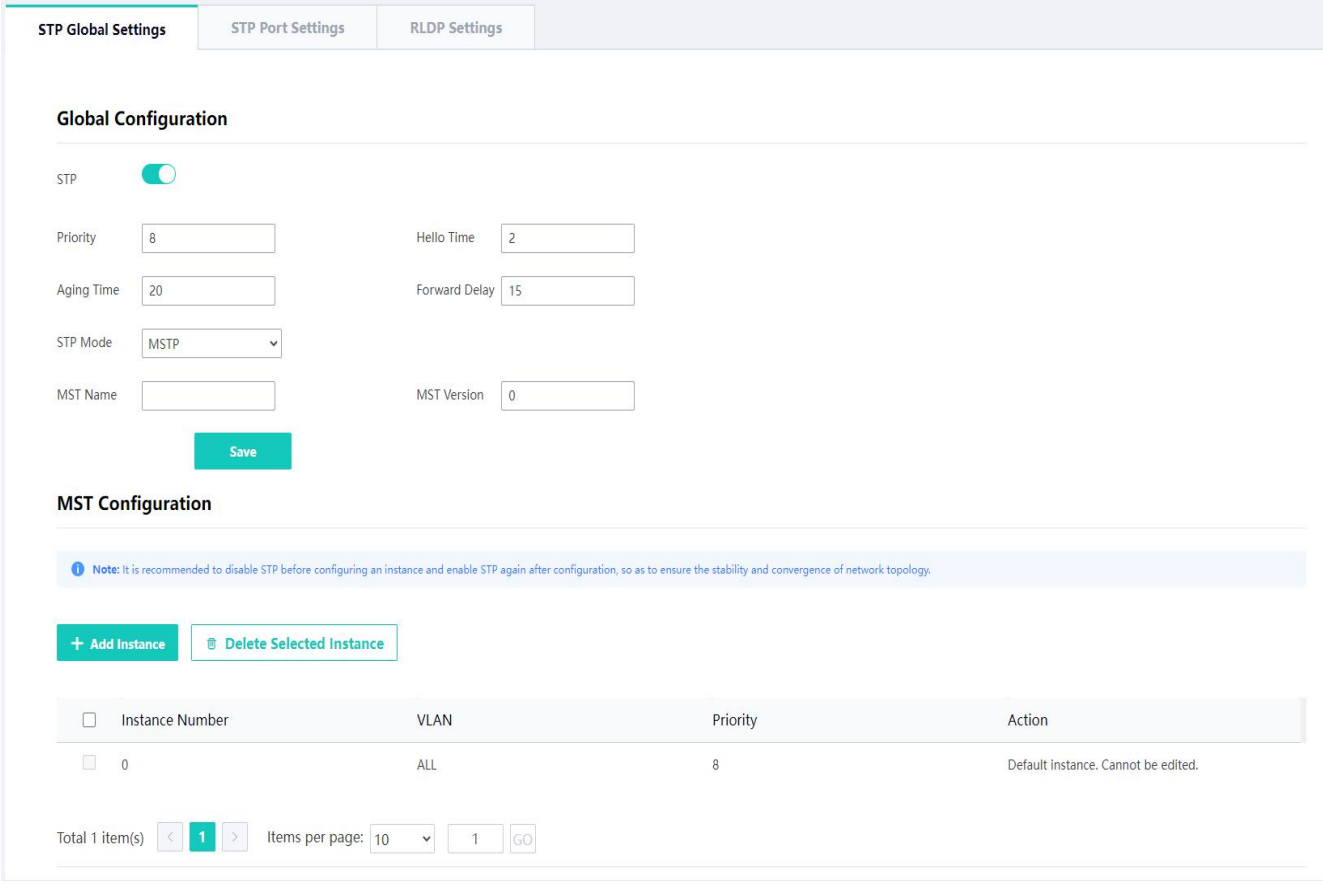
To add the default route, you must set IP Type and Next Hop Address. After that, click **Save**. The newly added route is displayed in the route list after an "Save succeeded." message is displayed.

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



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.

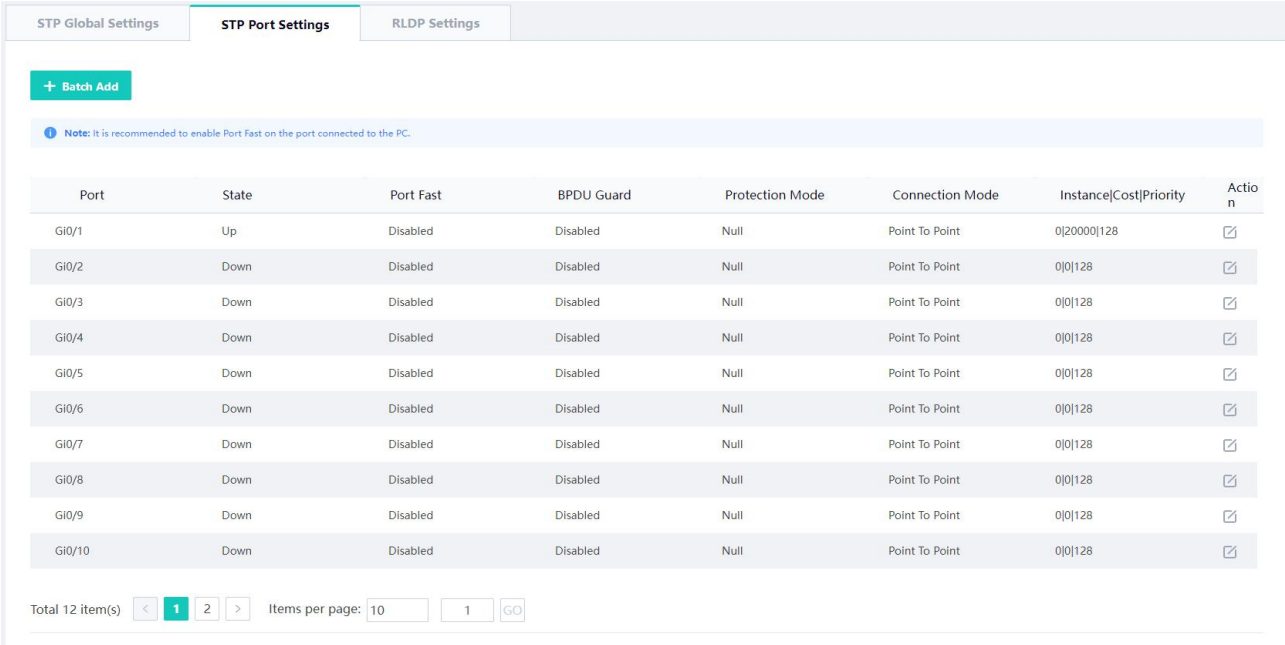
■ Deleting instance

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 setting

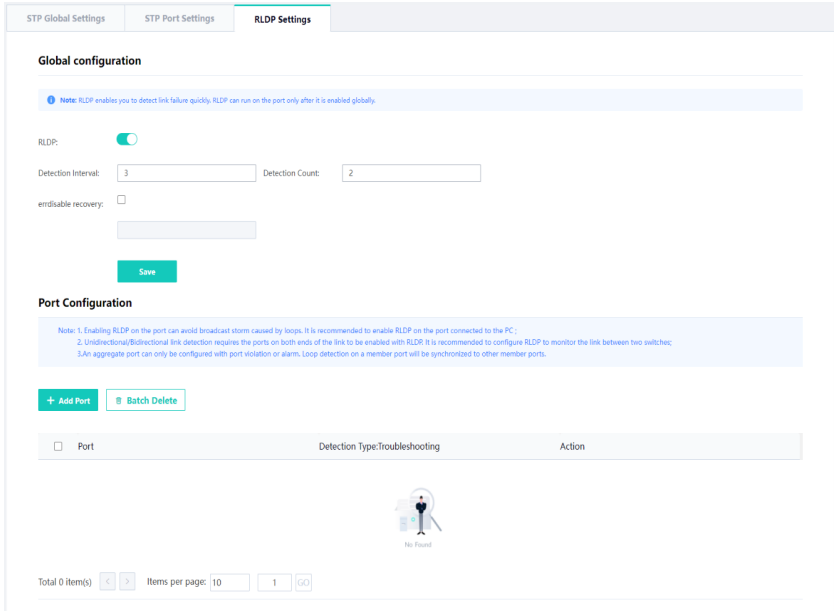
Specify Protection Mode, Port Fast, BPDU Guard, Connection Mode, and Port Priority, and select ports for batch setting.

■ 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



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.

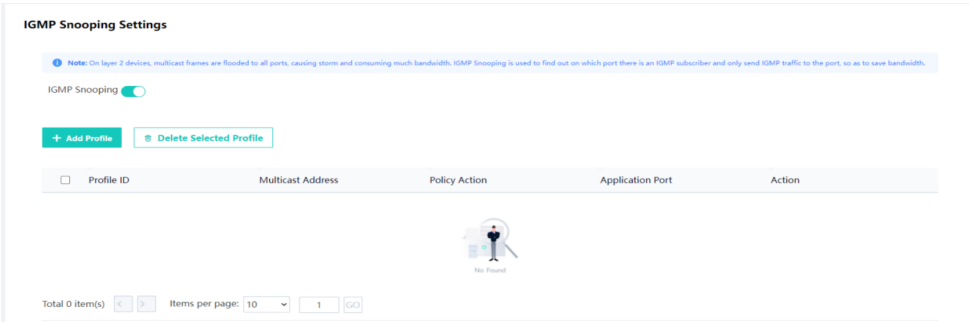
2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the item?" message is displayed.

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.

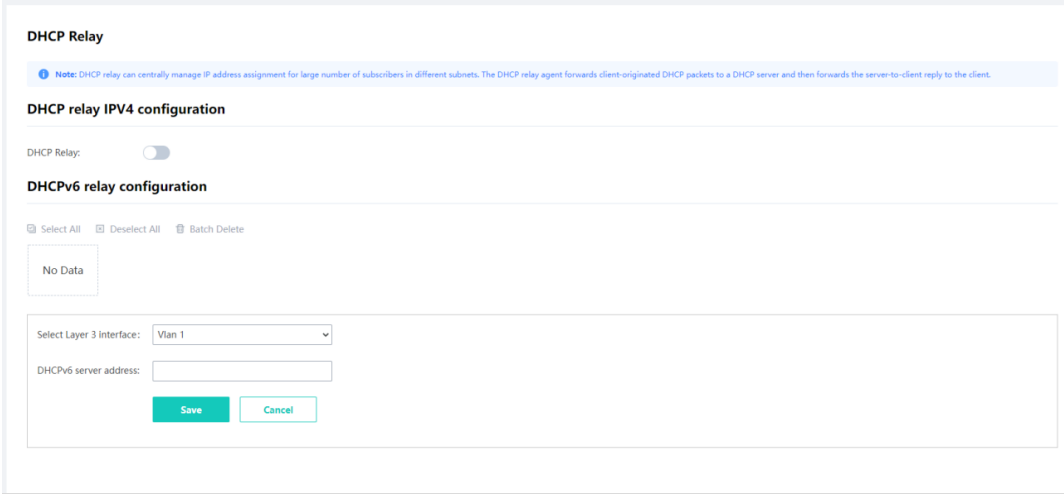
2) After you click **Delete** in the **Action** column an "Are you sure you want to delete the profile?" message is displayed.

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



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

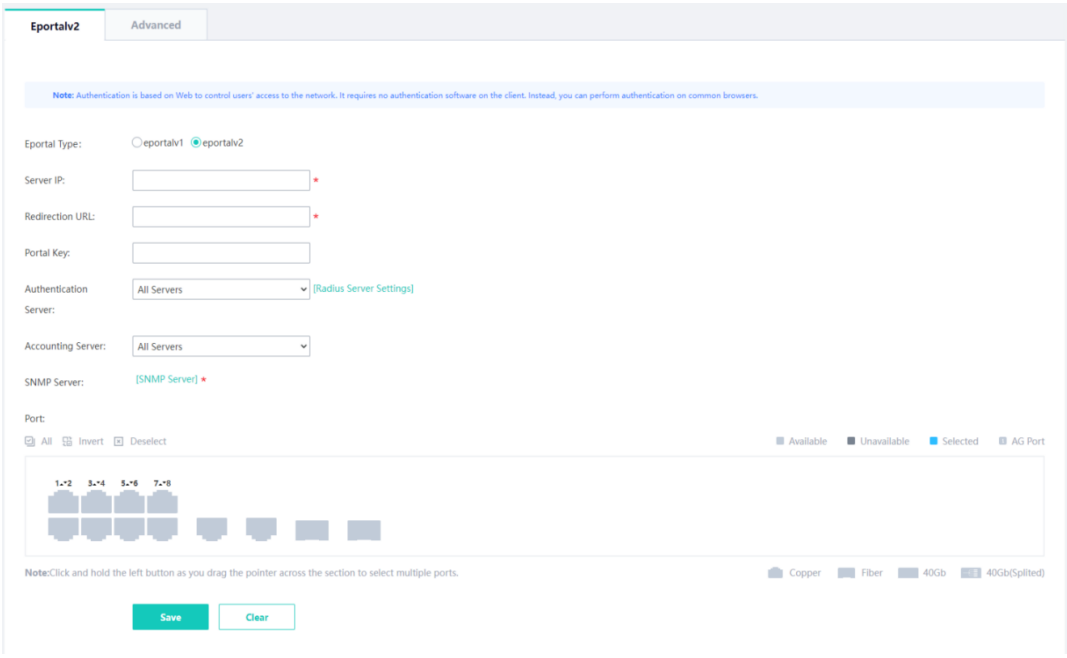
Authentication

The Authentication page allows you to set Eportalv2 and Advanced.

↘ Eportalv2

The following figure shows the Eportalv2 page.

Figure 1-20 Eportalv2

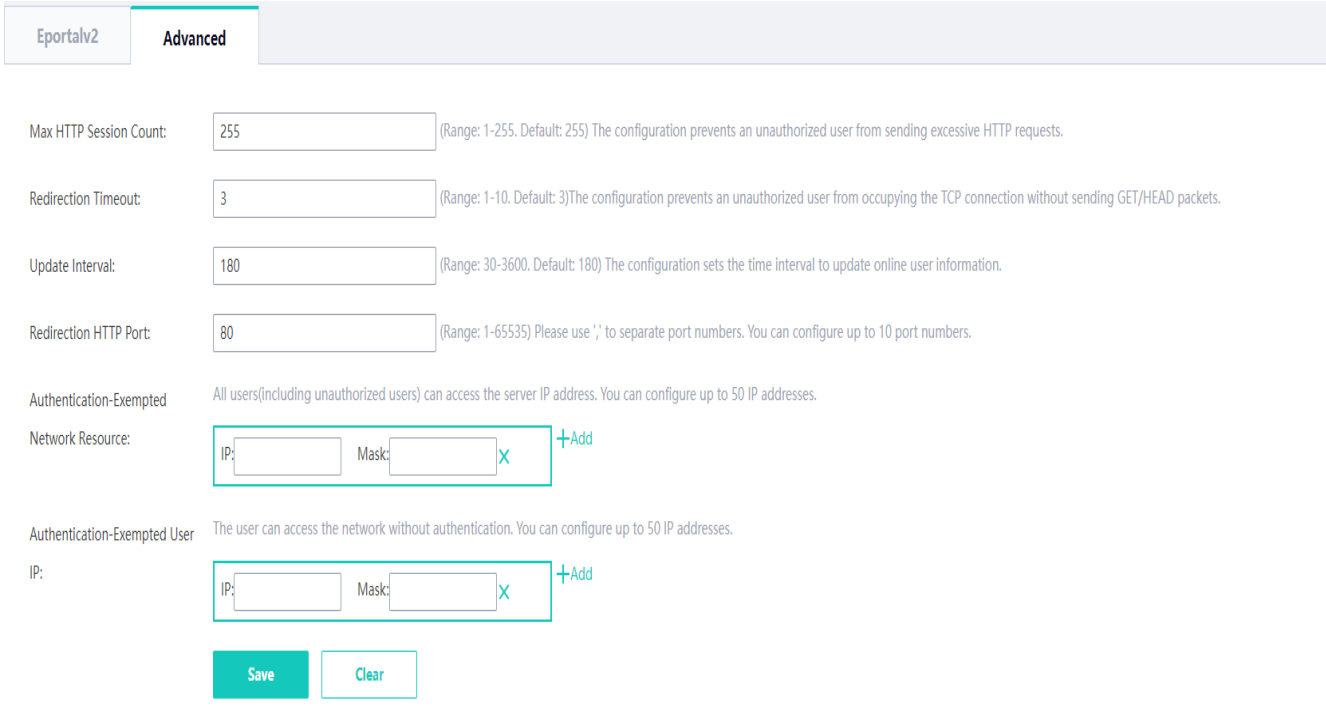


Enter the server IP address and redirection URL, and then click **Save**. A "Configuration succeeded." message is displayed.

↘ Advanced

The following figure shows the Advanced page.

Figure 1-21 Advanced Settings



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

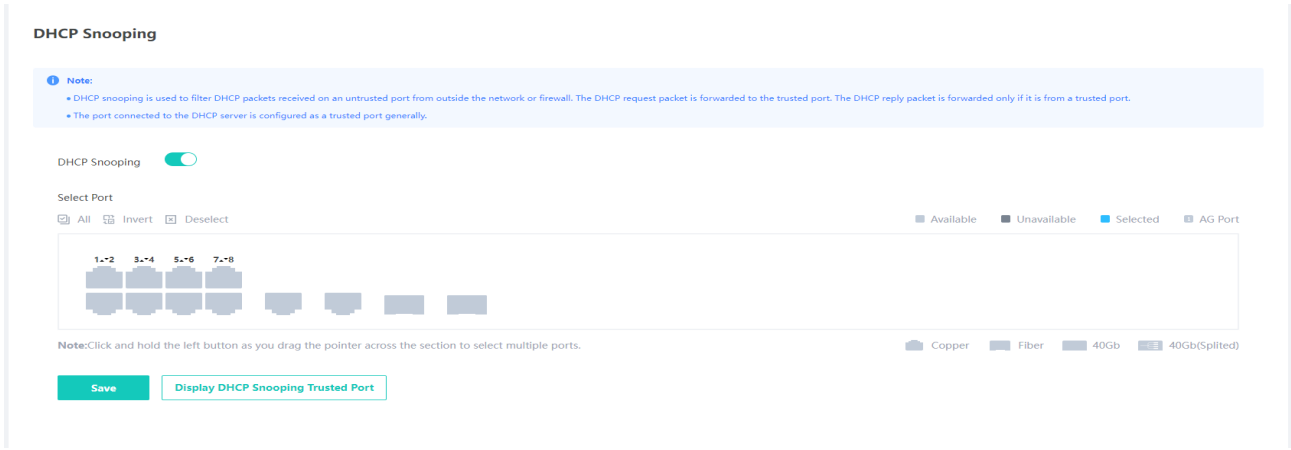
1.3.3 Security

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



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

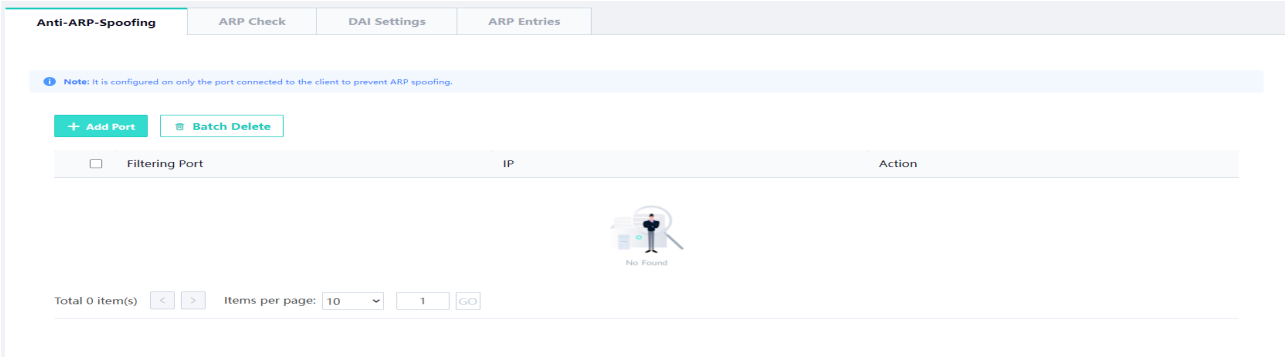
Save button.

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

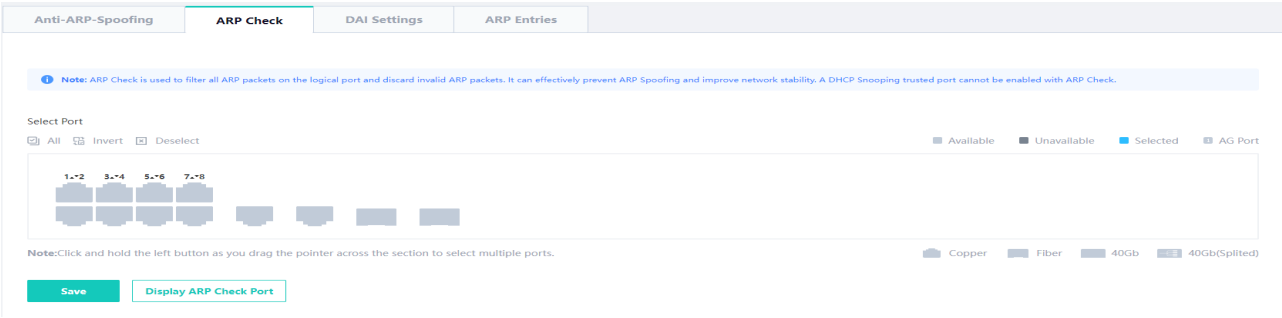
1) You can select multiple filtering ports from the filtering port list and click **Delete Selected Port** to delete the filtering ports in batches.

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.

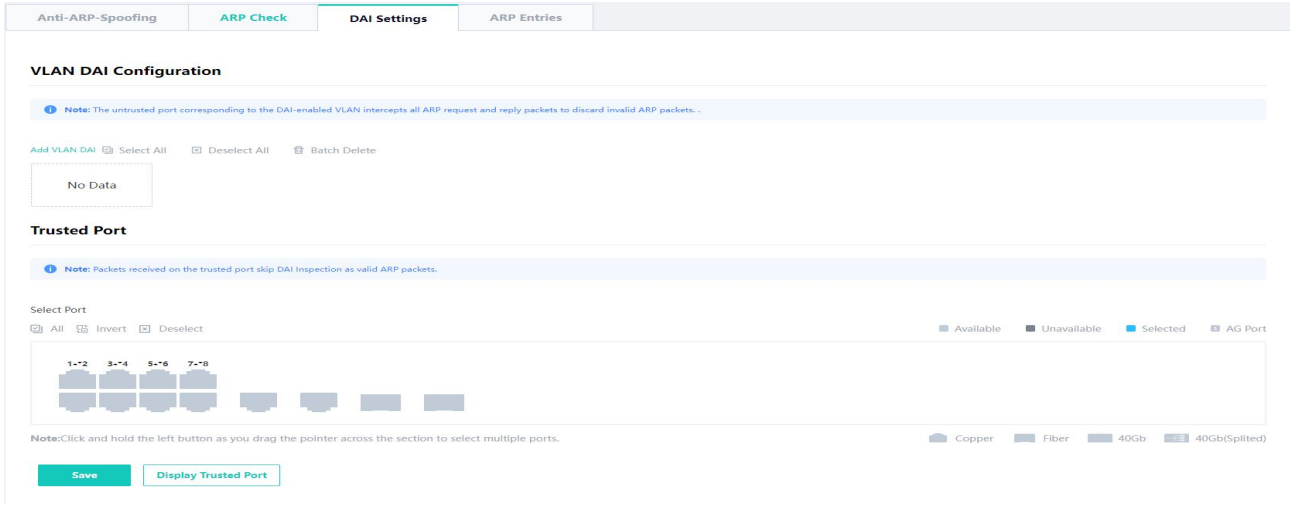
NOTE:

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



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:

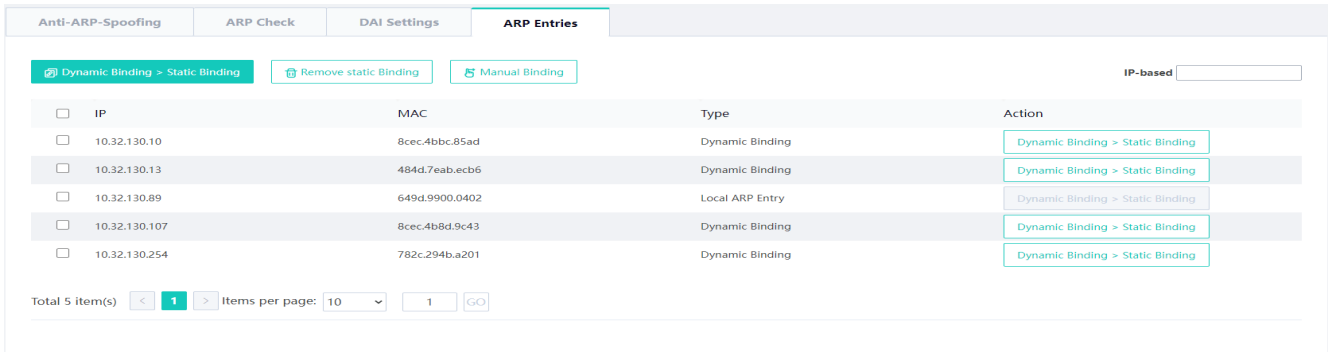
The selected port on the panel is enabled with the DAI function and is in edit state. If you don't want to edit a port after modifying it, you can click Display Trusted Port to make the panel display the current status of the DAI trusted port.

NOTE:

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

↘ ARP Entries

Figure 1-26 ARP Entries



■ 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

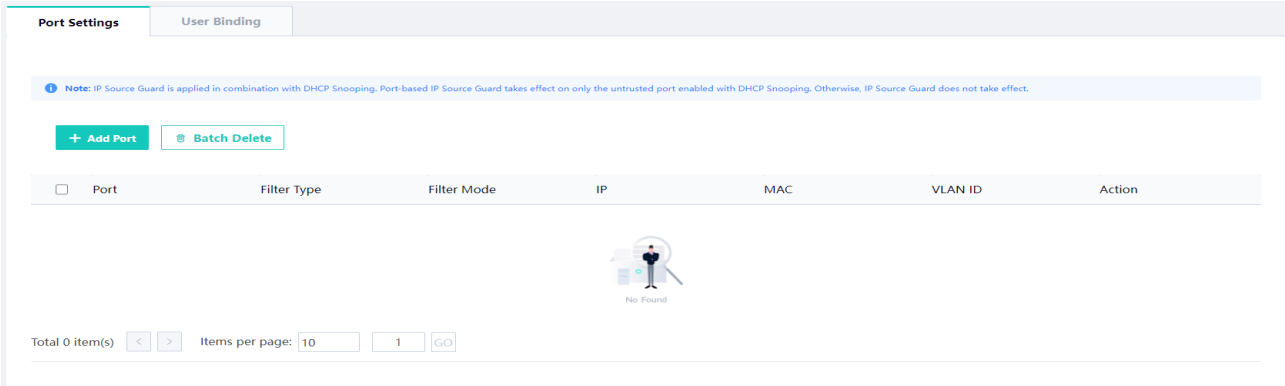
To add a static binding, you must configure IP Address and MAC Address. After that, click **Save**. The newly added static binding is displayed in the ARP entry list after a "Configuration succeeded." message is displayed.

IP Source Guard

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

↘ Port Settings

Figure 1-27 Port Settings



■ 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

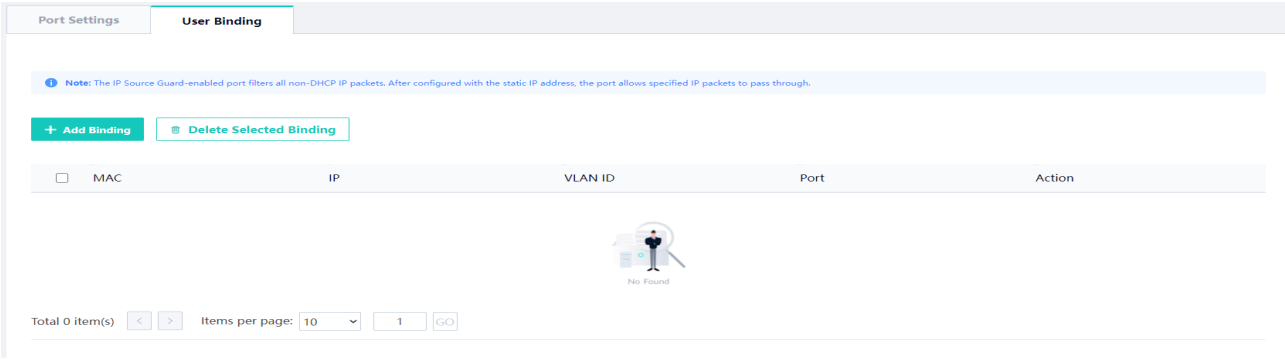
1) You can select multiple ports from the IP Source Guard port list and click **Delete Selected Port** to delete the ports in batches.

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



- 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.

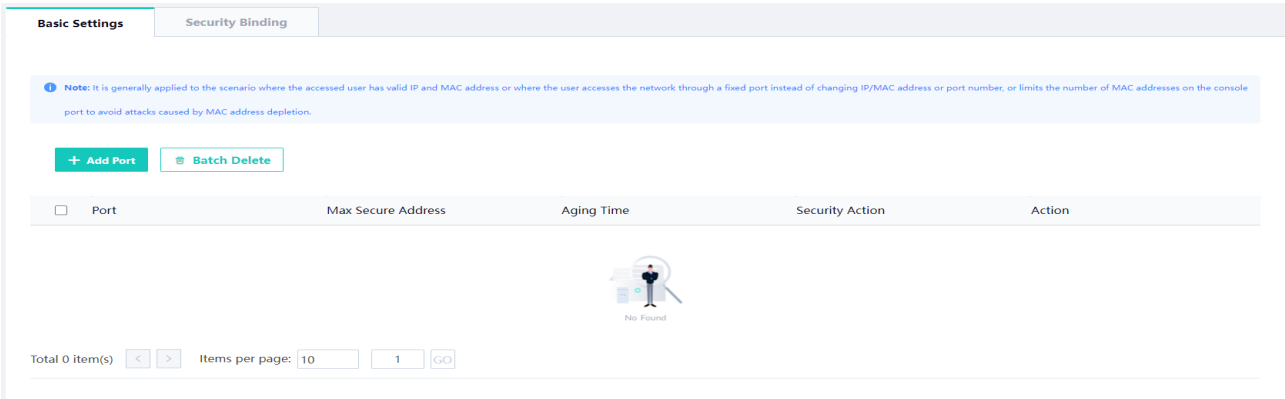
2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the binding?" message is displayed.

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

Port Security

Basic Settings

Figure 1-29 Basic Settings



- 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.

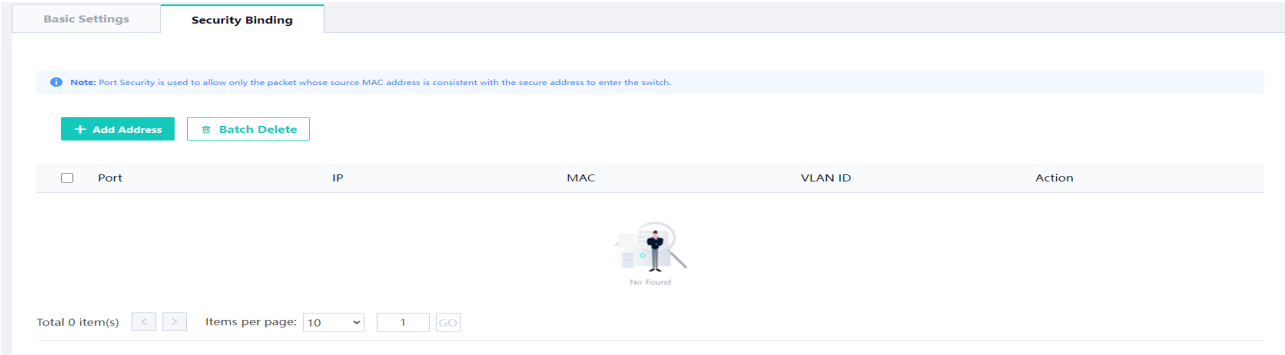
- Deleting security port

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.

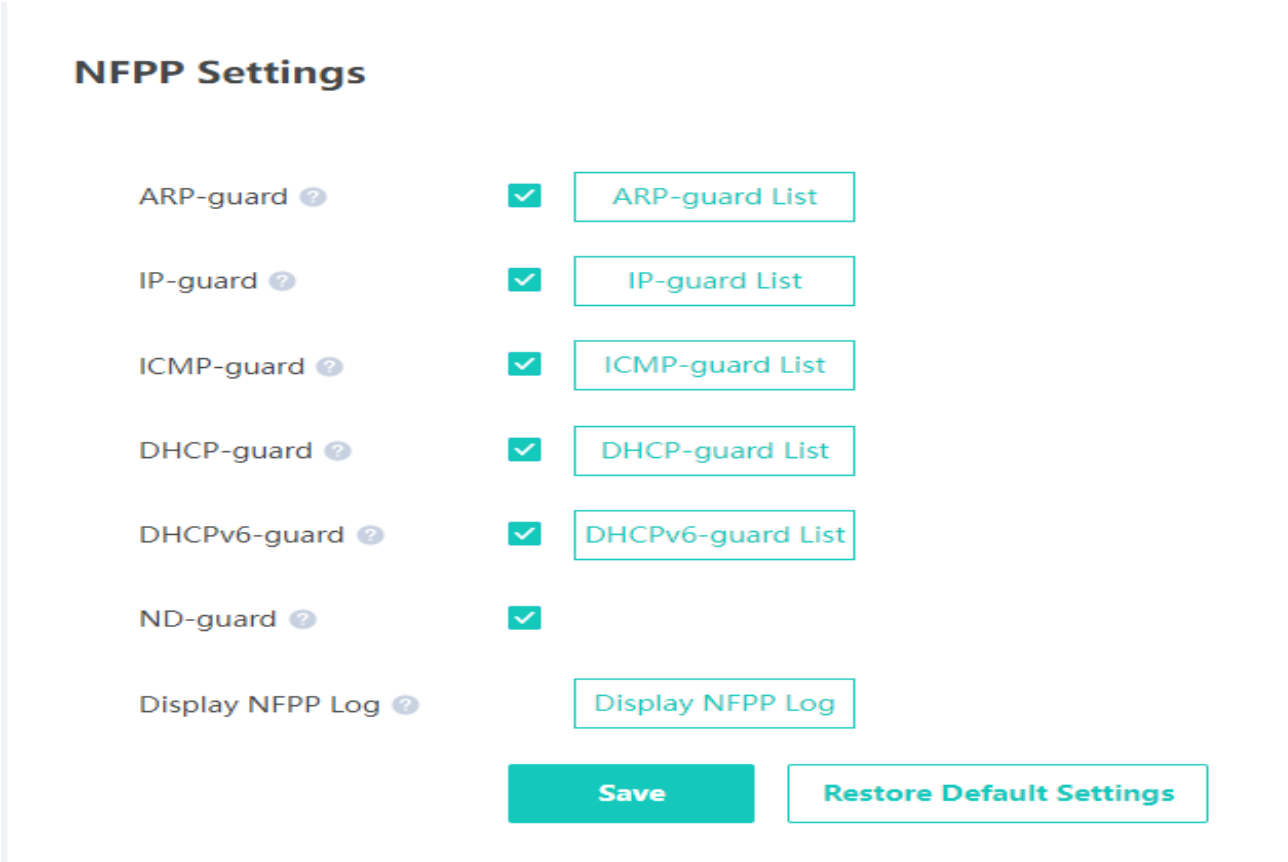
2) After you click **Delete** in the **Action** column, an "Are you sure you want to delete the port?" message is displayed.

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

NFPP

The following figure shows the NFPP Settings page.

Figure 1-31 NFPP

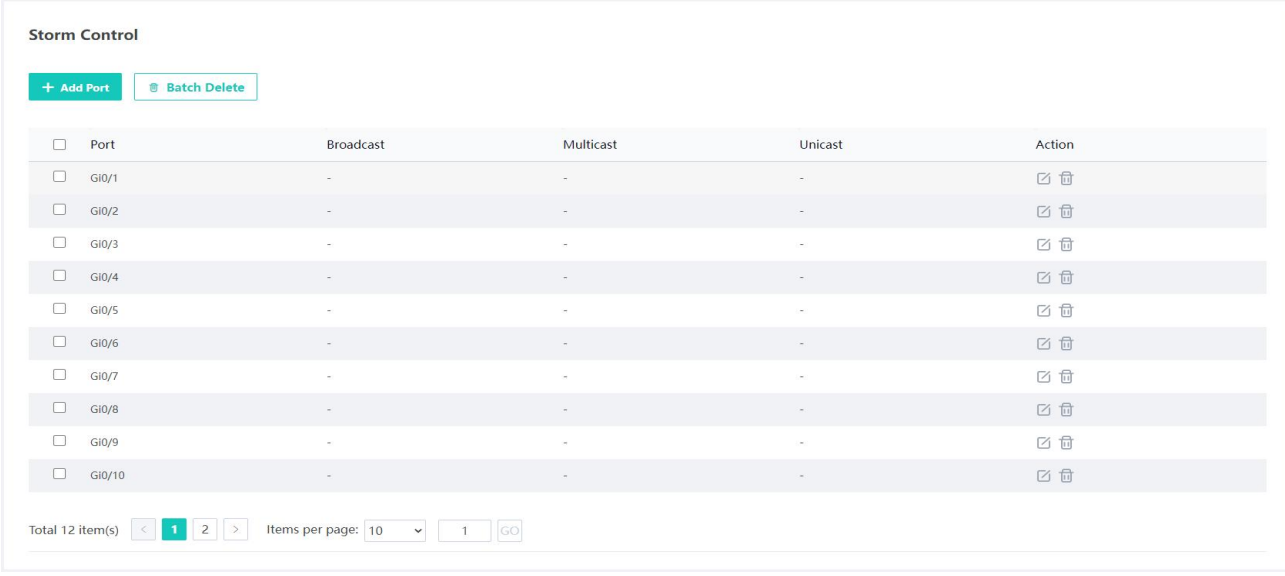


You can enable or disable various guard functions. After the setting, click **Save**. A "Save succeeded." message is displayed. To restore to the default settings, click **Restore Default Settings**.

Storm Control

The following figure shows the Storm Control Settings page.

Figure 1-32 Storm Control Settings



■ 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.

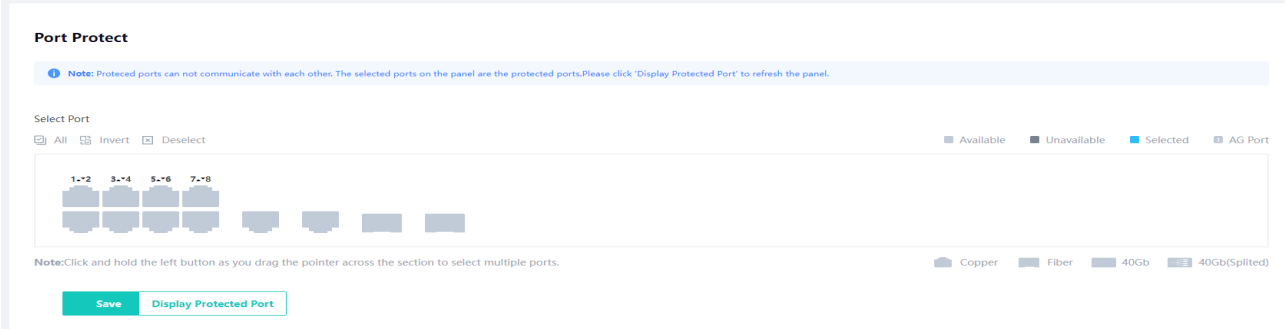
After you confirm the operation, a "Delete succeeded." message is displayed.

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.

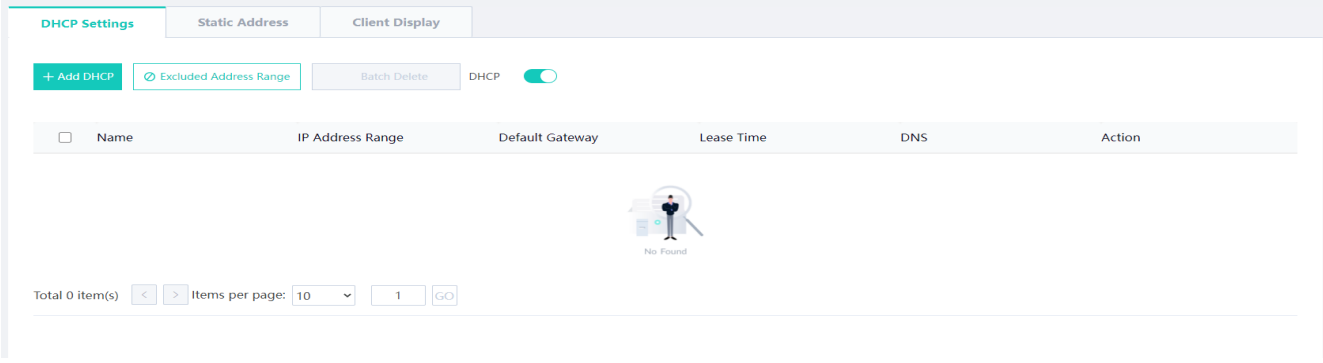
DHCP

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.

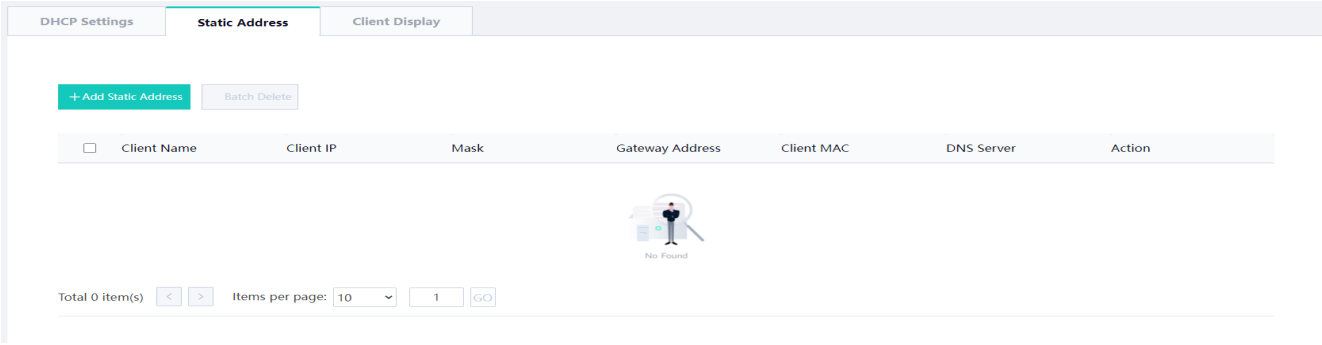
- Enabling DHCP

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

Static Address

The following figure shows the Client Display page.

Figure 1-35 Static Address



- 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

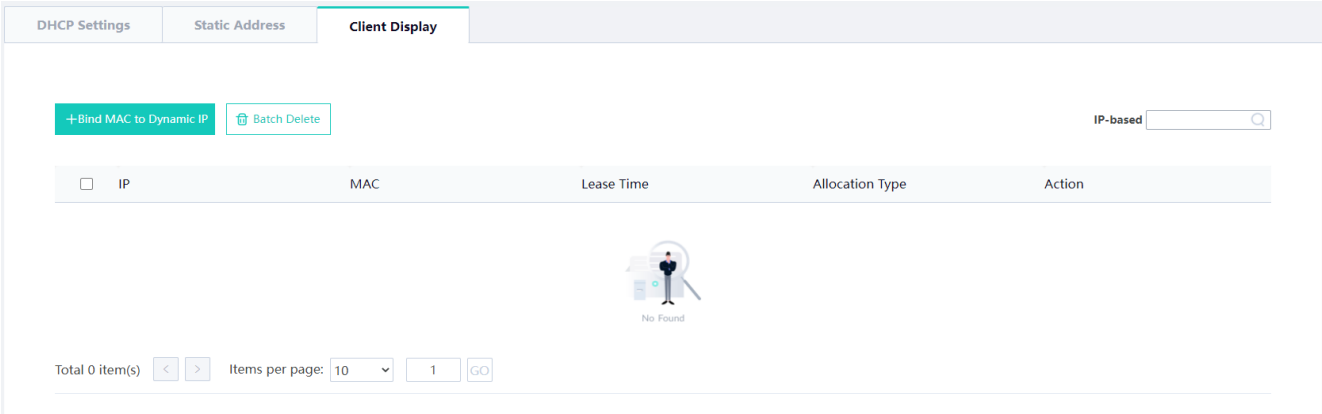
1) You can select multiple static addresses from the static address list and click **Delete Selected Address** to delete the static addresses in batches.

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

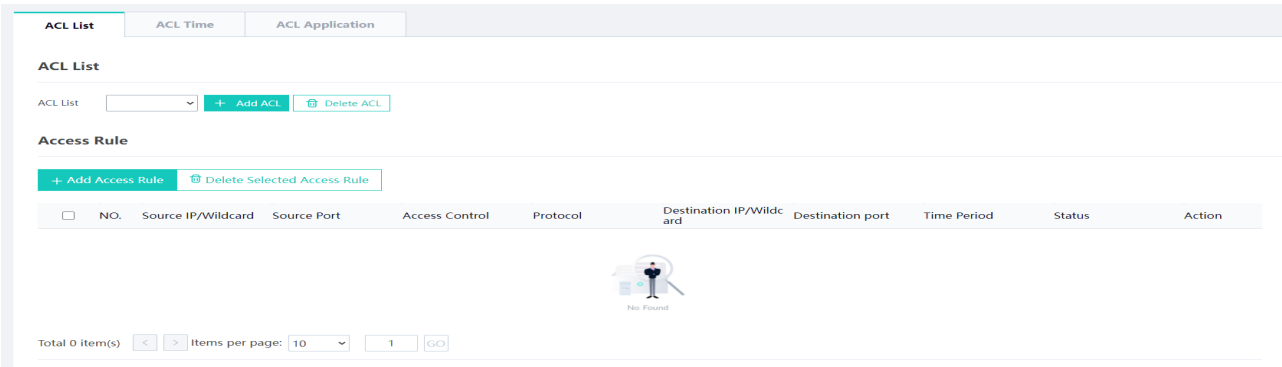
You can select multiple clients from the client list and click Bind MAC to Dynamic IP for binding.

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.

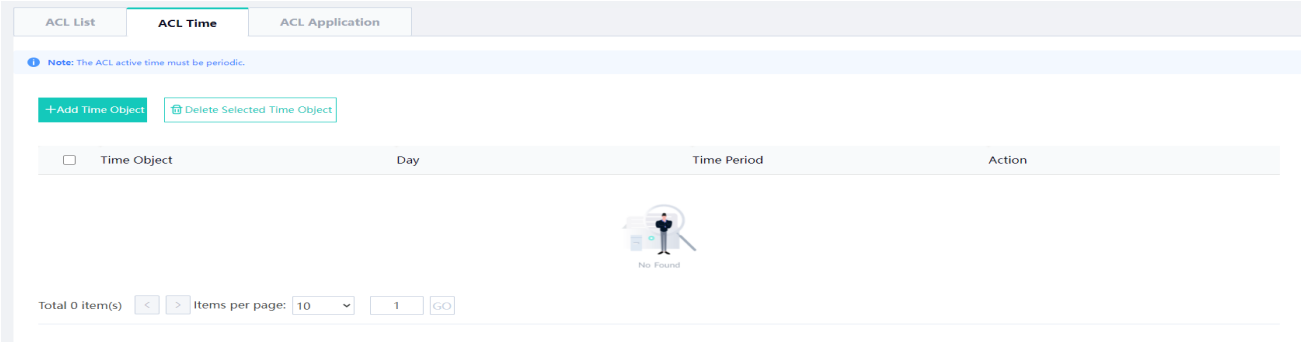
- Moving access rule

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



- 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.

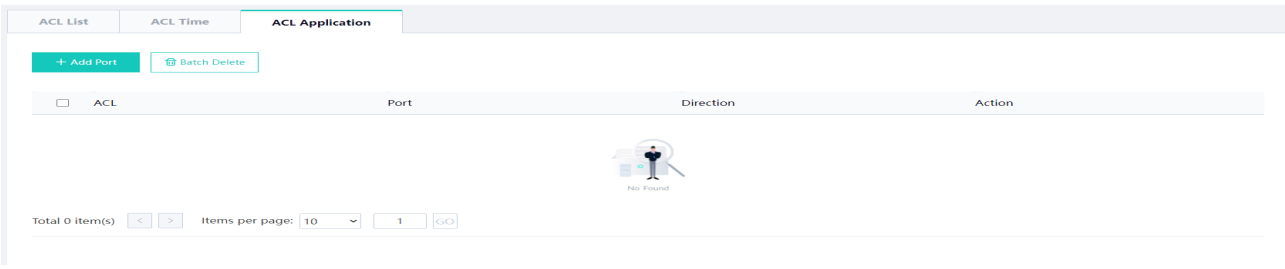
- Deleting ACL time

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



- 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.

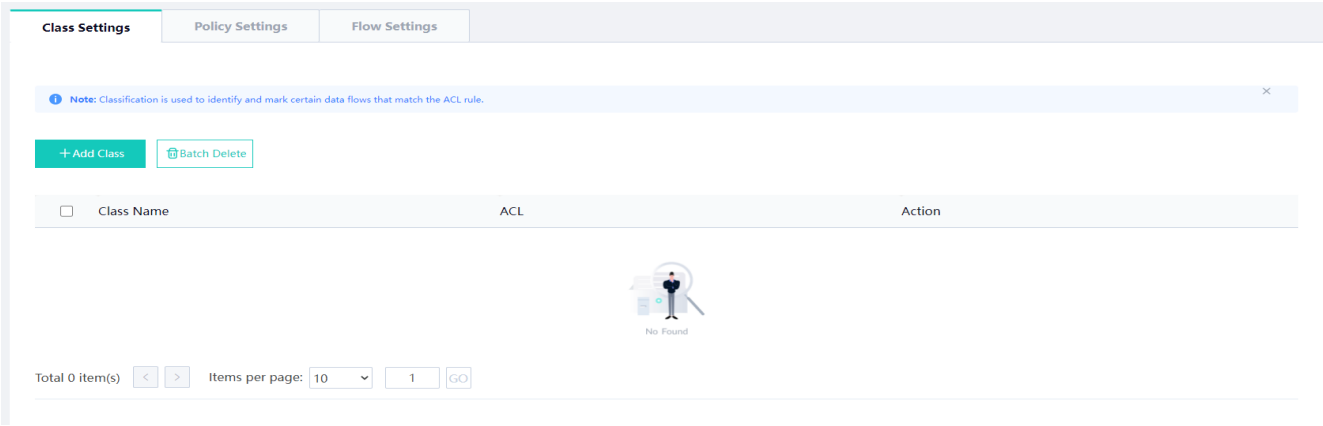
After you confirm the operation, a "Delete succeeded." message is displayed.

QoS

↘ Class Settings

The following figure shows the Class Settings page.

Figure 1-40 Class Settings



■ 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.

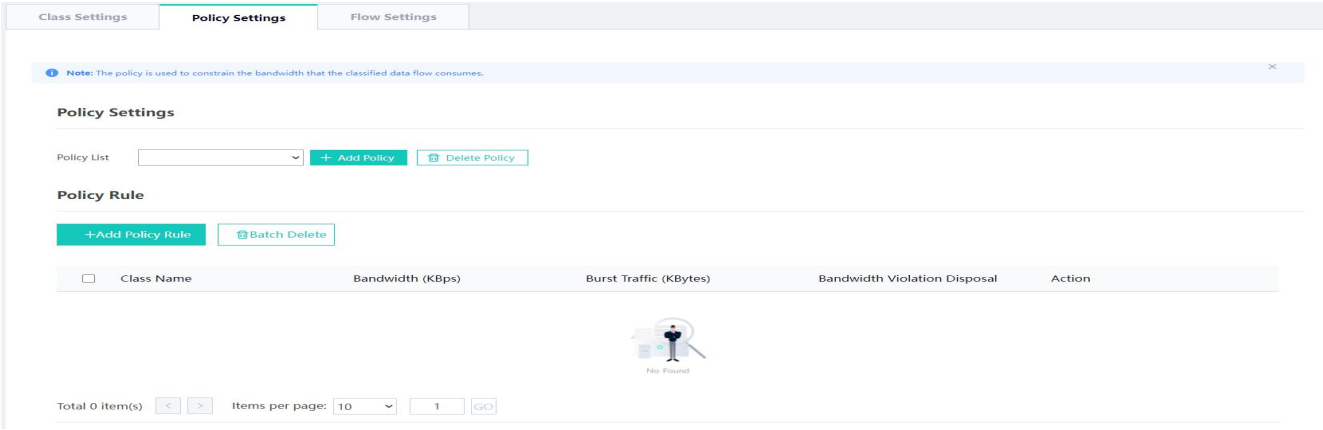
2) After you click Delete in the Action column, an "Are you sure you want to delete the item?" message is displayed.

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



■ 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.

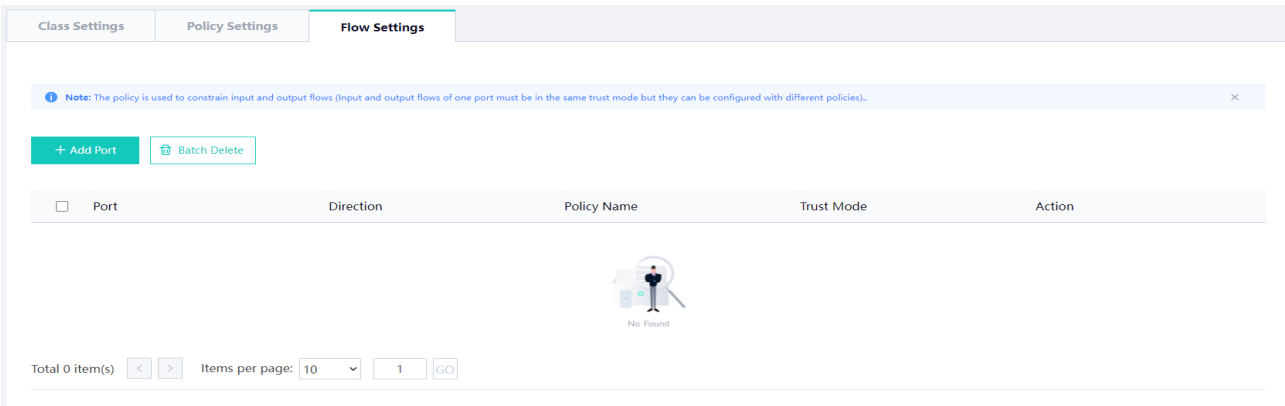
2) After you click Delete in the Action column, an ”Are you sure you want to delete the item?” message is displayed.

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



■ 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.

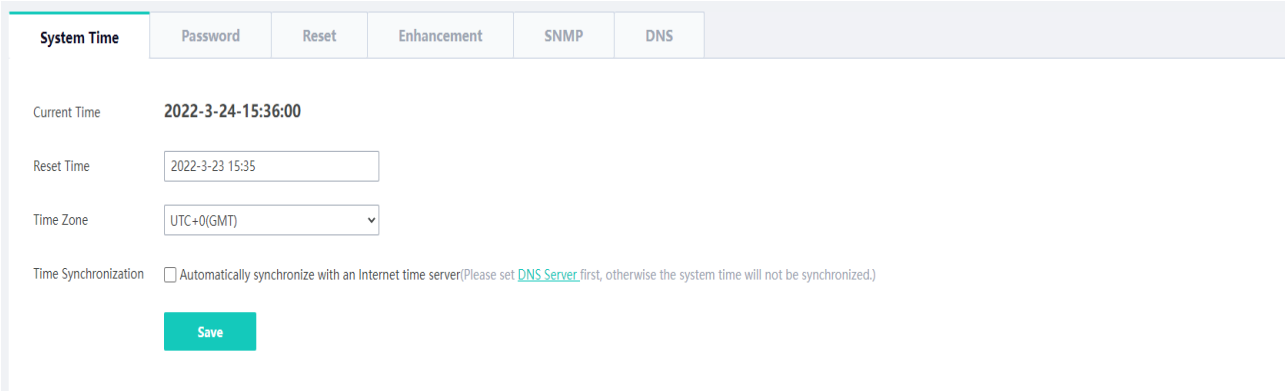
System Settings

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

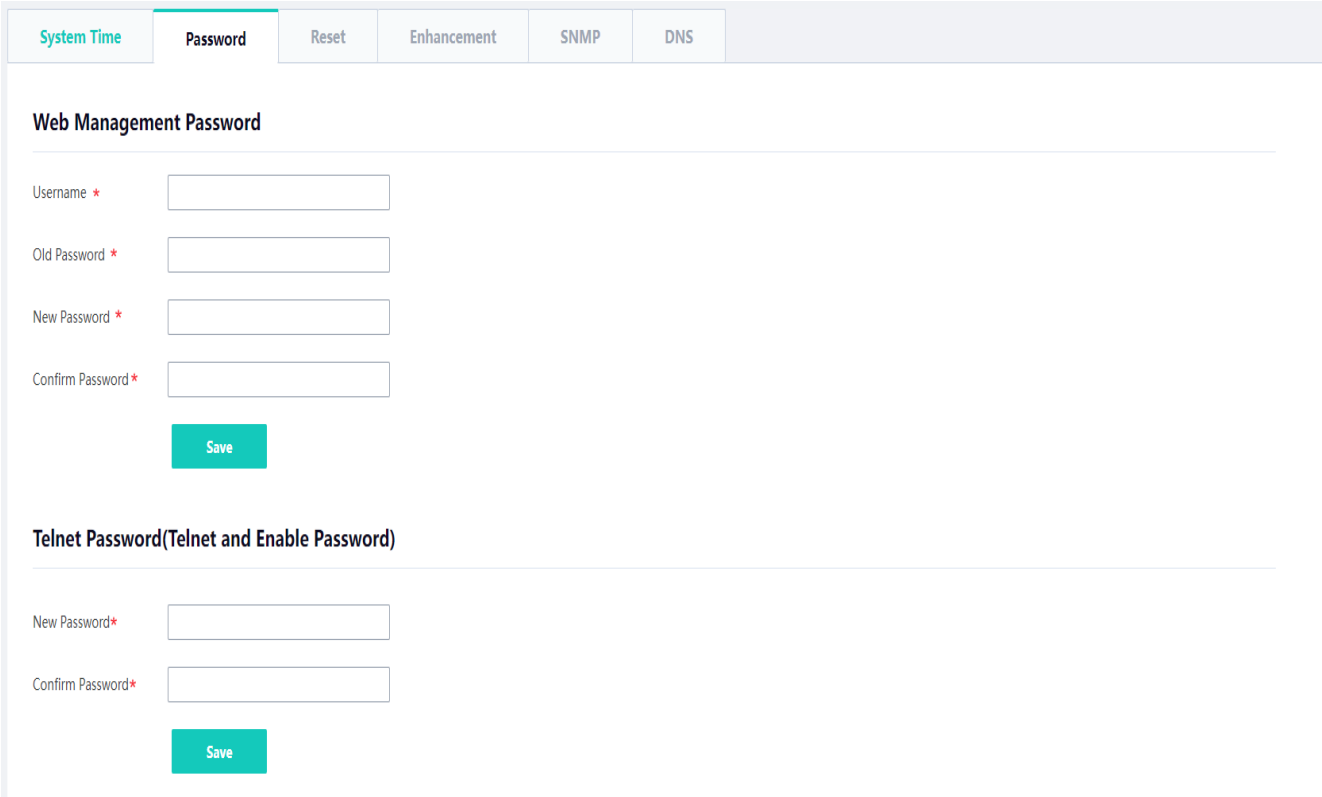
The current system time is displayed on the page. You can set the current system time manually. Alternatively, you can select Automatically synchronize with an Internet time server for time setting. After that, click Save. A "Configuration succeeded." message is displayed.

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

↘ Password

The following figure shows the Password page.

Figure 1-44 Password



■ 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.

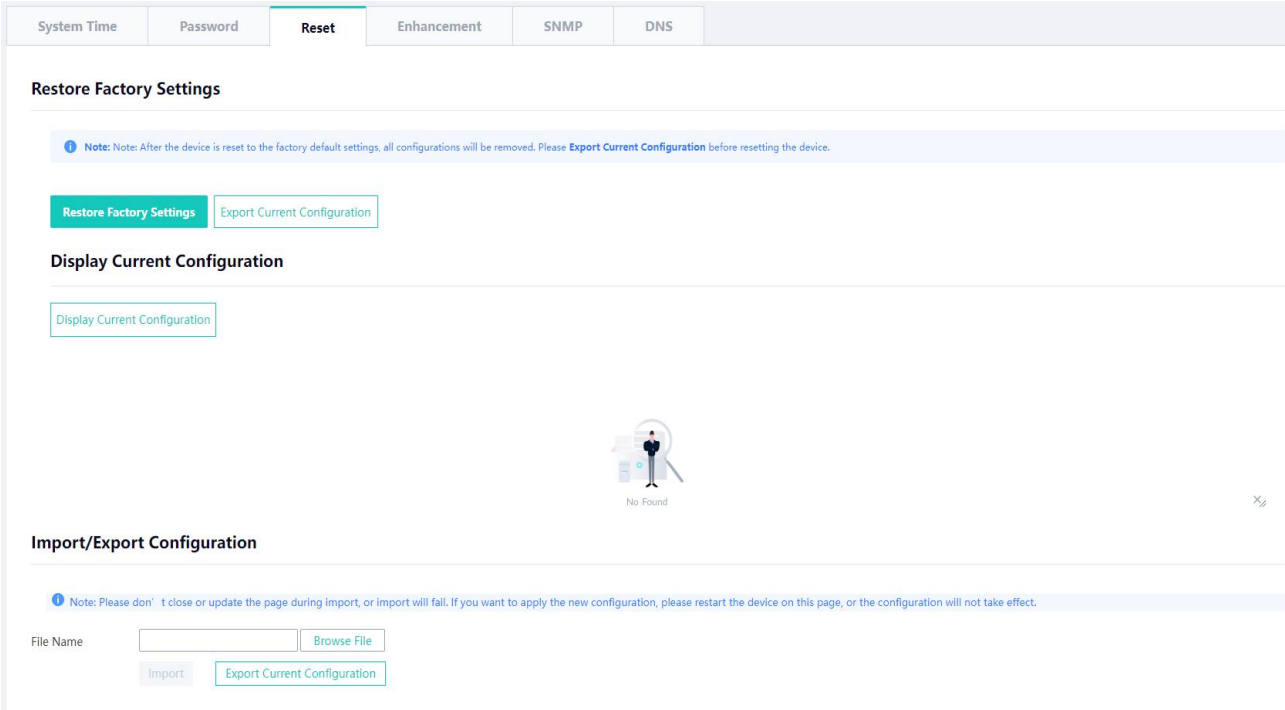
■ Modifying the telnet authentication password

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



- 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.

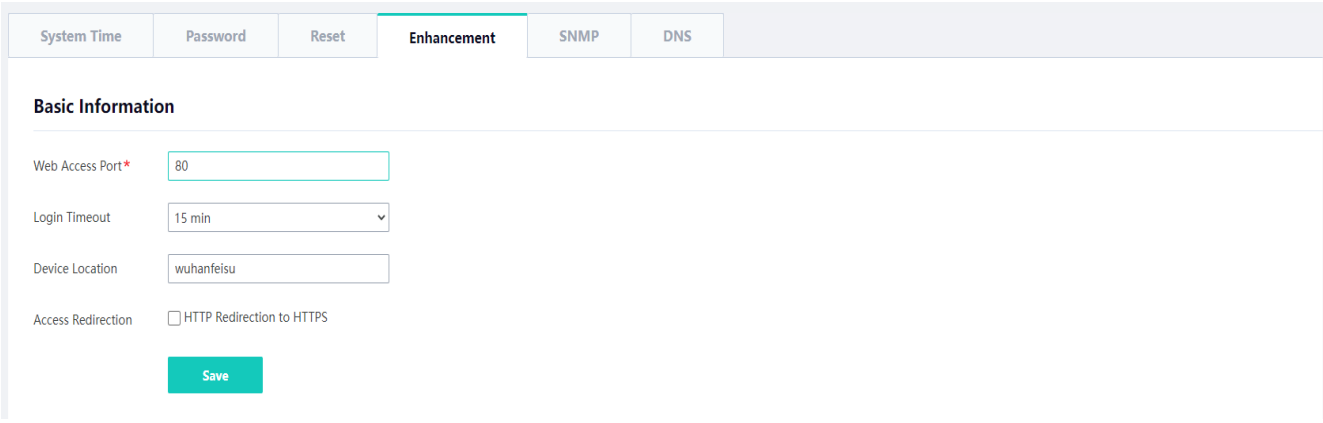
- Restoring factory settings

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

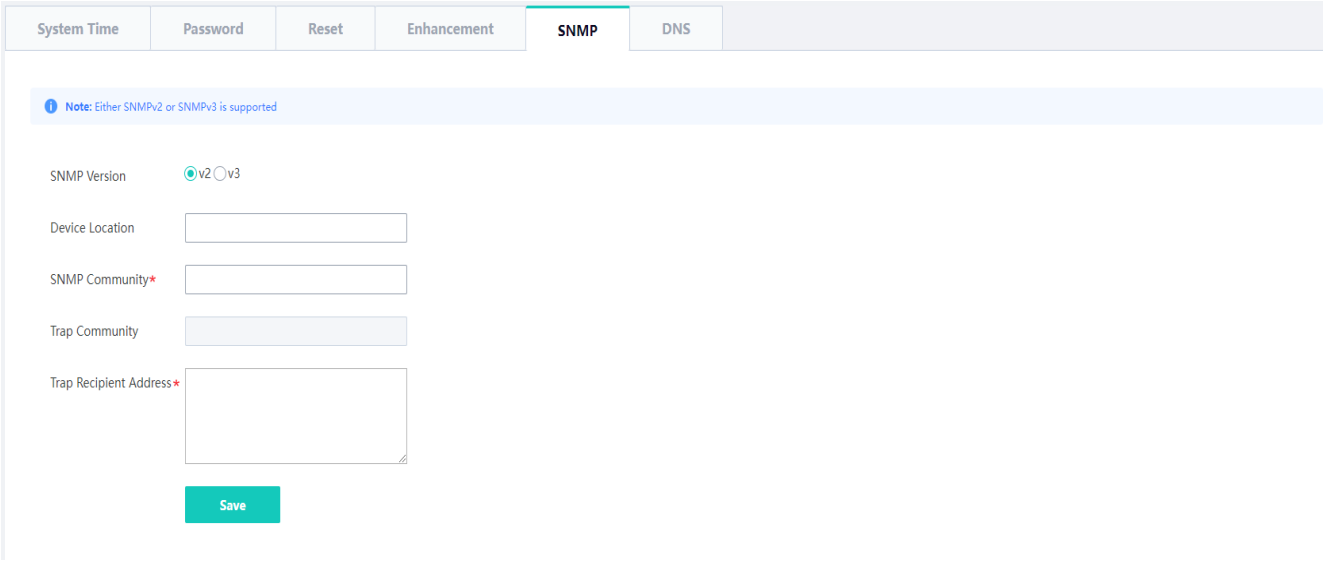


Specify Web Access Port (mandatory) and specify Login Timeout and Device Location as required. After that, click Save. A “Configuration succeeded.” message is displayed.

SNMP

The following figure shows the SNMP page.

Figure 1- 47 SNMP

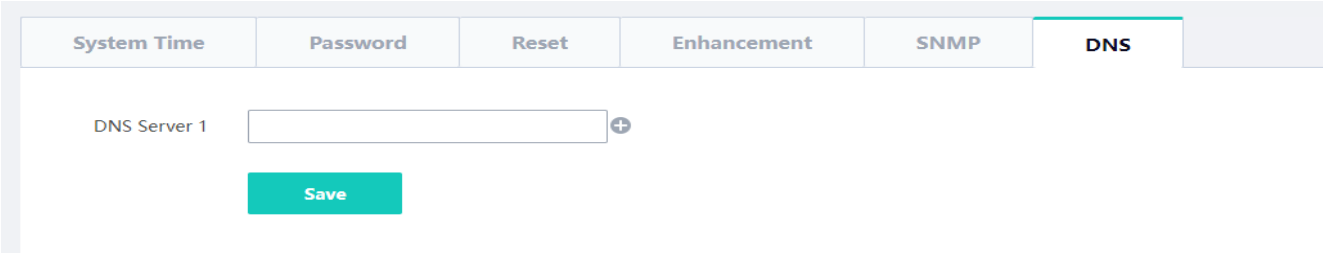


On this page, SNMP Version, Device Location, SNMP Password, and Trap Password are mandatory and other parameters are optional. After the setting, click Save. A “Configuration succeeded.” message is displayed.

DNS

The following figure shows the DNS page.

Figure 1- 48 DNS



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

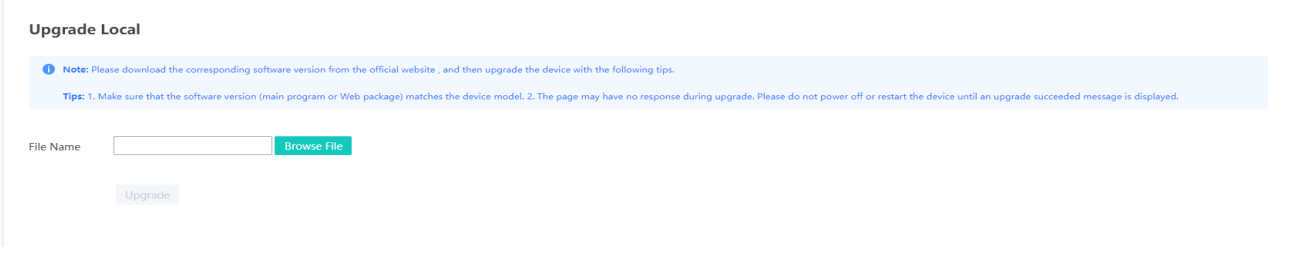
System Upgrade

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.

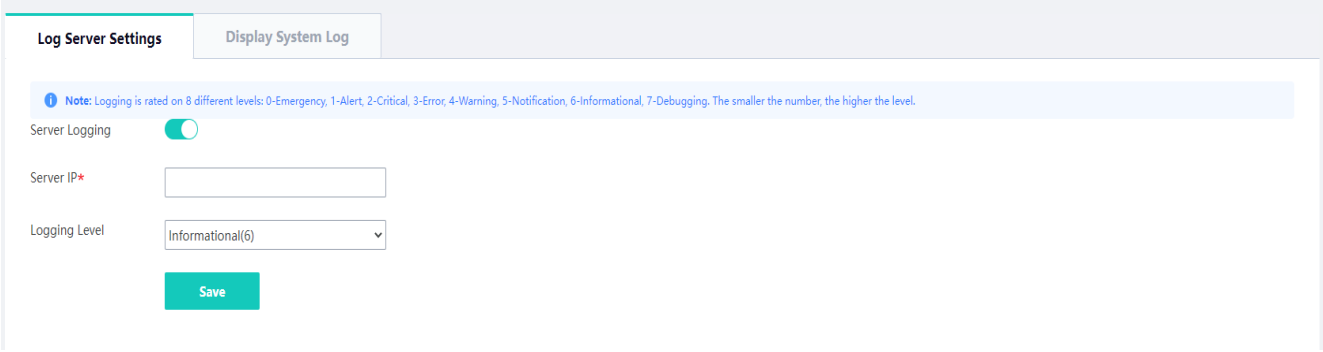
System Logging

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

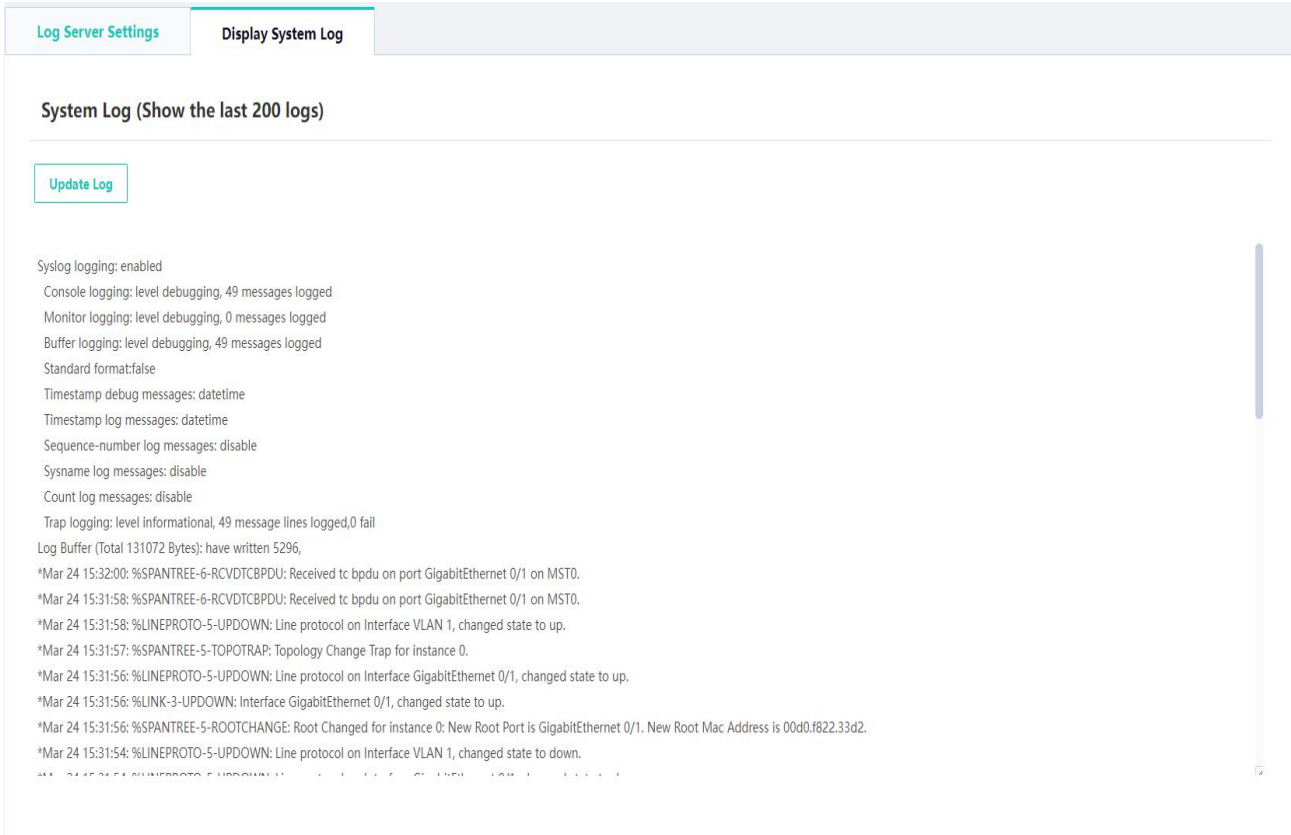


Set various parameters such as Server IP Address and Logging Level. The device sends the SYSLOG log to the corresponding server after the configuration is complete.

Display System Log

The following figure shows the Display System Log page.

Figure 1-51 Display System Log



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

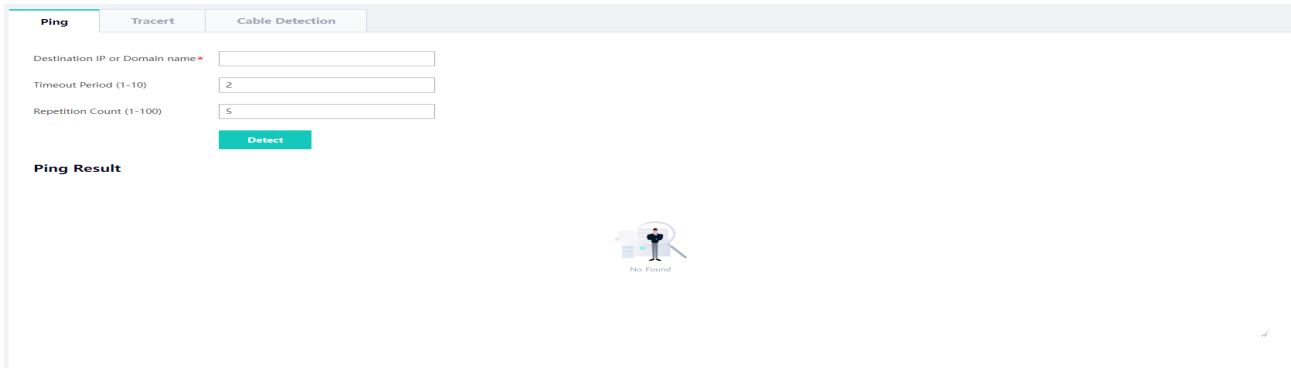
Network Detection

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

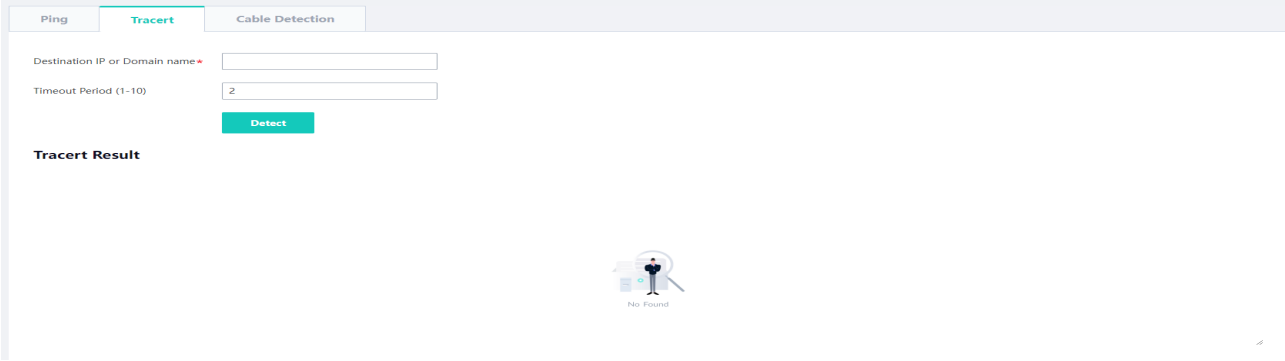


Input the destination IP address and click Detect. The detection result is displayed in the text box after a short while.

↘ Tracert

The following figure shows the Tracert page.

Figure 1-53 Tracert

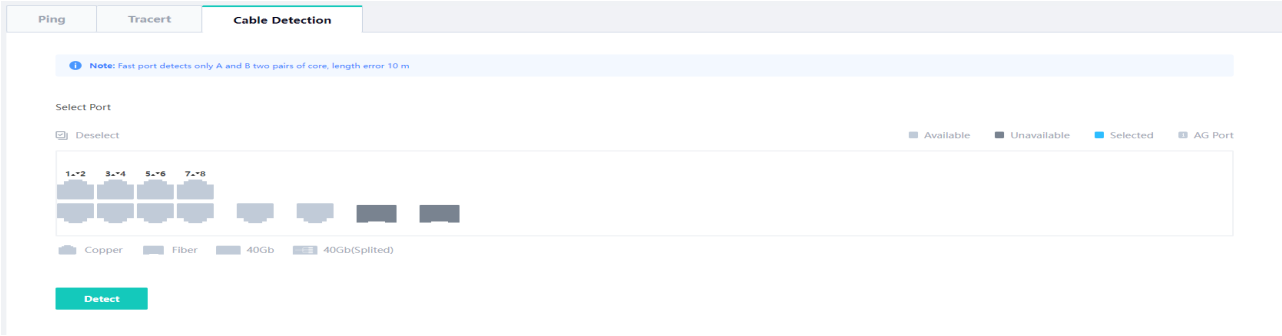


Input the destination IP address and click Detect. The detection result is displayed in the text box after a short while.

Cable Detection

The following figure shows the Cable Detection page.

Figure 1-54 Cable Detection



Select 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