RG-S5300-E Series Switches Web-based Configuration Guide

RGOS12.5(4)B0701

Document Version: V1.0

Date: 2022-07-29

Preface

Intended Audience

This document is intended for:

1) Network engineers

2) Technical support and servicing engineers

3) Network administrators

Technical Support

4) The official website of Reyee: https://www.ireyee.com/

5) Technical Support Website: https://www.ruijienetworks.com/support

6) Case Portal: https://caseportal.ruijienetworks.com

7) Community: https://community.ruijienetworks.com

8) Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Choose **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

> ⚡ **Danger**
>
> An alert that calls attention to safety operation instructions that if not understood or followed when operating the device can result in physical injury.

> 🛑 Warning
>
> An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

> ⚠️ Caution
>
> An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

---

3.   Note

This manual introduces the features of the product and offers guidance on configuration and testing.

CONTENT

1 Configuring Switch Eweb

1.1 Overview

Users can access the Web management system (that is, Eweb) of switches through a browser (such as Internet Explorer (IE)) to manage the switches.

Web management involves the Web server and Web client. The Web server, integrated into the switch, is used to receive and process requests from a client (reading Web files or executing commands), and return processing results to the client. The Web client is usually a Web browser, such as IE.

> ℹ This document applies only to S5300-E and S5310-E series switches.

> ⚠ The Eweb and device cannot be configured in a hybrid manner. After the device is configured, the Eweb needs to be refreshed, for example, you can press F5 for refreshing.
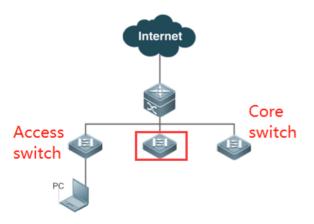
1.2 Applications

Application	Description
Managing Devices by Using the Eweb	After switches are configured, you can access the Eweb through a browser.

1.2.1 Managing Devices by Using the Eweb

Scenario

As shown in the figure below, you can access the Eweb of an access switch or distribution switch through a browser to manage and configure the switch.

Remark s	The device enclosed in the red rectangle in the figure above is the accessed switch. Ensure that the switch can be pinged successfully from the PC. Then, you can access the Eweb of the switch.

Deployment
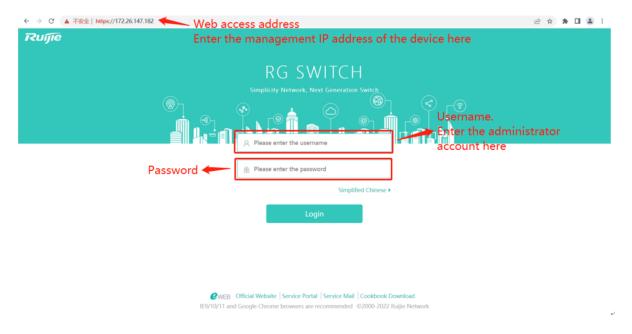
↘ Configuration Environment Requirements

Client requirements:

● Network administrators can log in to the Eweb graphical user interface (GUI) of a switch from a browser to manage the switch. Clients refer to PCs or other mobile terminals such as laptops.

● Browser: IE9–IE11, Google Chrome, and 360 Browser are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.

● Resolution: You are advised to set the resolution to 1024 × 768, 1280 × 1024, 1440 × 960, or 1920 × 1080. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

ⓘ Eweb configuration and command line interface (CLI) configuration can be performed at the same time. After CLI configuration is complete, enter the **write** command to save the configuration. If a Web page is opened, refresh the page to ensure synchronization between the Eweb configurations and CLI configurations.

↘ Logging In to the Web Management Platform

Enter http://X.X.X.X (management IP address) in the browser and press **Enter** to open the login page, as shown in the figures below.
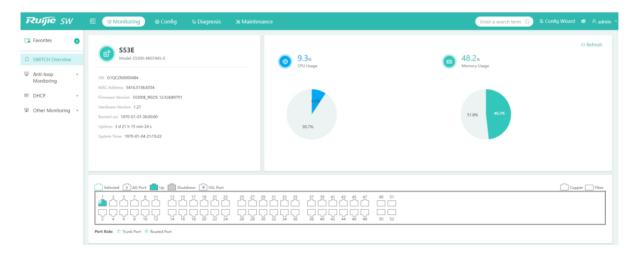
Enter the username and password and click **Login**. The following table provides the default username and password.

Default Username/Password	Permission Description
admin / admin	Super administrator with all permissions

🛈 The default username is displayed in output of the **show running-config** command only after its default password is changed.

After authentication is successful or the password is changed, the homepage of the Eweb is displayed, as shown in the figure below.

🛈 For details about Eweb pages, see "Eweb Management System."

1.3   Eweb Management System
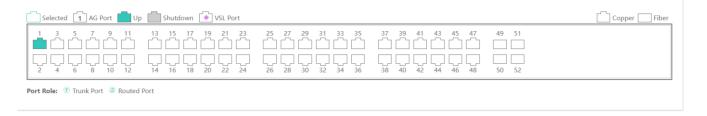
Basic Concepts

↘   **Icons and Buttons on the GUIs**

Icon/Button	Description
Edit	Edit. Click this icon to edit the selected record.
Delete	Delete.
ON	Function enabling/disabling icon.
	Available port. After you click or select the icon, the port becomes selected.
	Shutdown port.
	Selected port.
20	Aggregate port. The digit in the port indicates the aggregate port number.
	Trunk port. It is displayed on the panel of the **VLAN**/**VLAN Settings** page.
	The port is powered on.
	Virtual switching link (VSL) port.
	Bidirectional forwarding detection (BFD) port. It is displayed on the panel of the **SWITCH Overview** page.
	40G port.
	40G port that has been split.
Save	Save. Click it to submit and save input information.
+	Click it to add settings.
×	Click it to delete settings.
*	Required item. An input box marked with this symbol indicates a required item.
ⓘ	Note symbol.
⚠	Caution symbol.

↘   **System Operations**

● Device panel

Overview

The following table describes feature configurations of the second-level menu items in the left navigation tree of the Web GUI.

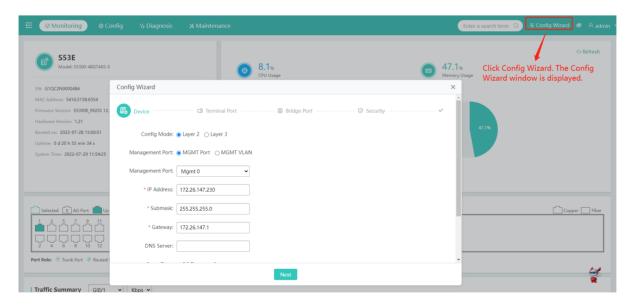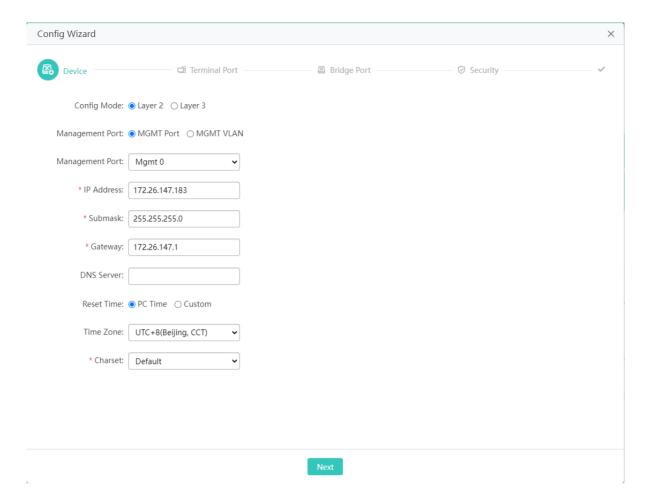| Feature	Description
Config Wizard	Helps you build a network by using the devices.
SWITCH Overview	Displays port information and overall device information.
STP Status	Displays the Spanning Tree Protocol (STP) status and port roles.
RLDP Status	Displays the Rapid Link Detection Protocol (RLDP) status and ports, on which RLDP is enabled.
Client List	Displays addresses allocated by a switch address pool.
Server Status	Displays the DHCP server and configured address pools.
VSU Status	Displays the virtual switching unit (VSU) topology. It exists only when the device works in VSU mode.
VLAN	Sets VLANs and trunk ports.
Port	Configures basic information about ports, aggregate ports, port mirroring, and port rate limit.
Routing	Sets routes.
DHCP	Configures Dynamic Host Configuration Protocol (DHCP), allocates static addresses, and displays the client list.
VRRP	Sets Virtual Router Redundancy Protocol (VRRP).
MAC Address	Sets static addresses and filter addresses.
VSU Settings	Configures the standalone mode and VSU mode for the device for switching.
STP	Configures STP global basic information and STP ports.
RLDP Settings	Configures RLDP globally and port RLDP.
ACL	Configures access control lists (ACLs) and ACL time, and applies ACLs.
Port Security	Configures port security and security binding.
Storm Control	Control storms.
DHCP Snooping	Sets DHCP snooping.
Gateway Anti-ARP-Snooping	Configures anti-ARP spoofing on the gateway, Address Resolution Protocol (ARP) check, dynamic ARP inspection (DAI), and ARP entries.
IP Source Guard	Configures ports and user binding.
NFPP	Displays information related to Network Foundation Protection Policy (NFPP).
IGMP Snooping	Sets Internet Group Management Protocol (IGMP) snooping.

QOS	Configures classes, policies, and flows.
DHCP Relay	Sets the DHCP relay.
Authentication	Configures ePortal and advanced settings.
Ping	Detects the connectivity of an IP address or domain name.
Tracert	Uses tracert to detect an IP address or domain name.
One-click Collection	Collects information on the device in one-click mode.
Display System Log	Sets the syslog server and queries system logs.
Monitor System Log	Queries logs by level or module name.
Upgrade	Performs local upgrade.
Restart	Restarts the device.
Config MGMT	Backs up configurations, restores factory settings, and sets system character sets.
Systime	Sets the system time.
Syslog	Configures whether to enable the logging function on the device.
DNS	Sets domain name system (DNS).
Web	Configures the administrator password, basic settings, and administrator permissions.
Telnet	Configures the telnet and Secure Shell (SSH) functions, and password.
SNMP	Sets SNMPv2 and SNMPv3.

1.3.1   Config Wizard

● Device

Config Wizard   ×

Device ———————— Terminal Port ———————— Bridge Port ———————— Security ———————— ✓

Config Mode: ◉ Layer 2   ○ Layer 3

Management Port: ◉ MGMT Port   ○ MGMT VLAN

Management Port: [Mgmt 0 ▾]

* IP Address: [172.26.147.183]

* Submask: [255.255.255.0]

* Gateway: [172.26.147.1]

DNS Server: [ ]

Reset Time: ◉ PC Time   ○ Custom

Time Zone: [UTC+8(Beijing, CCT) ▾]

* Charset: [Default ▾]

[Next]
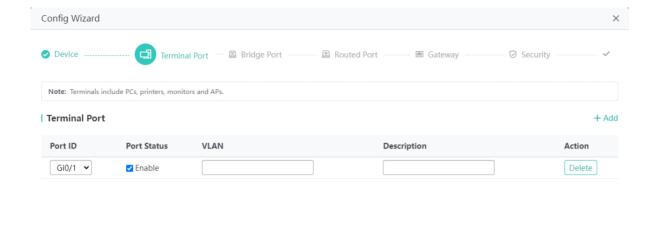
The steps of configuring device management are as follows:

1)   Configure **Config Mode**. This option is displayed for L3 devices.

2)   Select **MGMT Port** and configure **Management Port**.

3)   Configure **Submask**. A network segment that has been assigned to a port cannot be assigned to the port.

4)   **DNS Server** is an incremental parameter.

5)   Configure the system character set in **Charset**.

6)   Click **Next**.

●   Terminal Port

Config Wizard   ×

✓ Device ---------- 🖥 Terminal Port ··· 🖼 Bridge Port ---------- 🖼 Routed Port ---------- 🖼 Gateway ---------- ⊘ Security ---------- ✓

Note: Terminals include PCs, printers, monitors and APs.

| Terminal Port   + Add

Port ID	Port Status	VLAN	Description	Action
Gi0/1 ▾	☑ Enable			Delete

Previous   **Next**

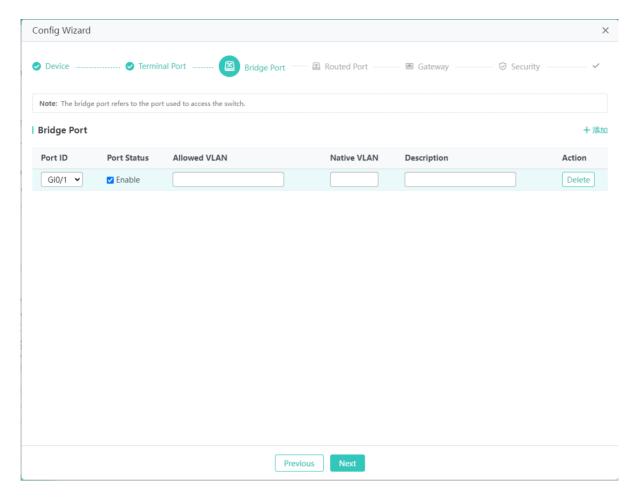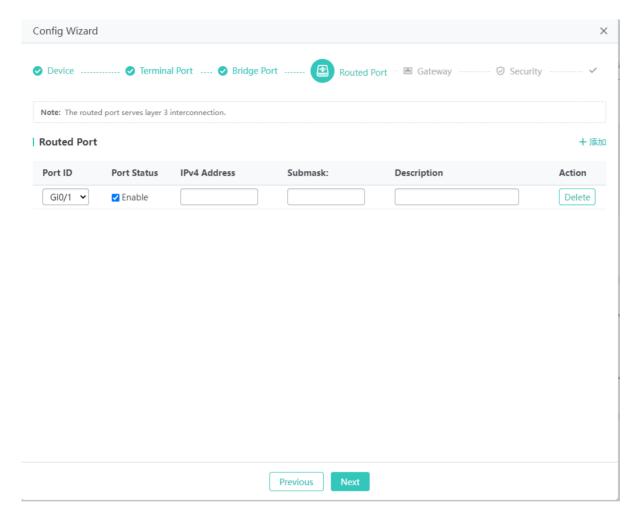The steps of configuring a terminal port are as follows:

1) Click **Add** to add a terminal port.

2) **Port ID** must be unique.

3) Click **Delete** to delete the terminal configuration.

4) Click **Next** after completing the configuration.

● Bridge Port

Config Wizard	✕

✅ Device ················· ✅ Terminal Port ········· 🖥 Bridge Port ······· 🖼 Routed Port ··········· 🖼 Gateway ·············· 🛡 Security ·············· ✓

Note: The bridge port refers to the port used to access the switch.

| Bridge Port   ＋添加

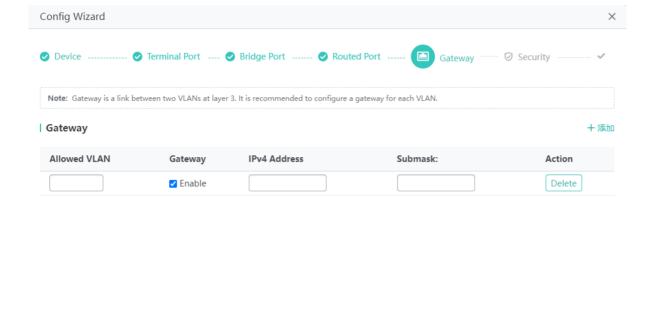| Port ID	Port Status	Allowed VLAN	Native VLAN	Description	Action
Gi0/1 ▼	☑ Enable				Delete

[Previous] [Next]

The steps of configuring a bridge port are as follows:

1)   Click **Add** to add a bridge port.

2)   **Port ID** must be unique.

3)   Click **Delete** to delete the bridge port.

4)   Click **Next** after completing the configuration as prompted.

●   Routed Port

Config Wizard   ✕

✓ Device ············· ✓ Terminal Port ···· ✓ Bridge Port ······· 🔼 Routed Port · 🖳 Gateway ··········· ⊘ Security ············ ✓

Note: The routed port serves layer 3 interconnection.

| Routed Port   ＋ 添加

Port ID	Port Status	IPv4 Address	Submask:	Description	Action
Gi0/1 ⌄	☑ Enable				Delete

Previous   **Next**

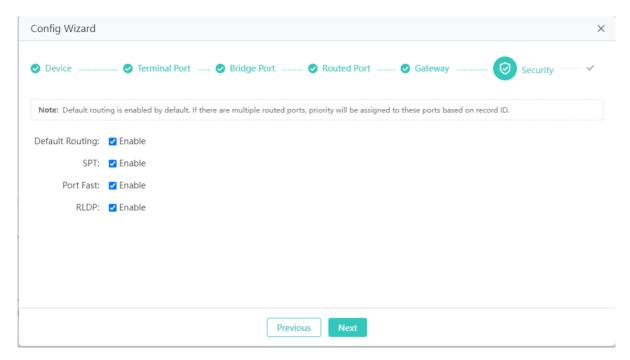The steps of configuring a routed port are as follows:

1)   Click **Add** to add a routed port.

2)   **Port ID** must be unique.

3)   Click **Delete** to delete the routed port.

4)   Click **Next** after completing the configuration as prompted.

●   Gateway

Config Wizard   ✕

✅ Device ············· ✅ Terminal Port ···· ✅ Bridge Port ······· ✅ Routed Port ······ 🖼 Gateway ······· ⊘ Security ·········· ✓

Note: Gateway is a link between two VLANs at layer 3. It is recommended to configure a gateway for each VLAN.

| Gateway   ＋ 添加

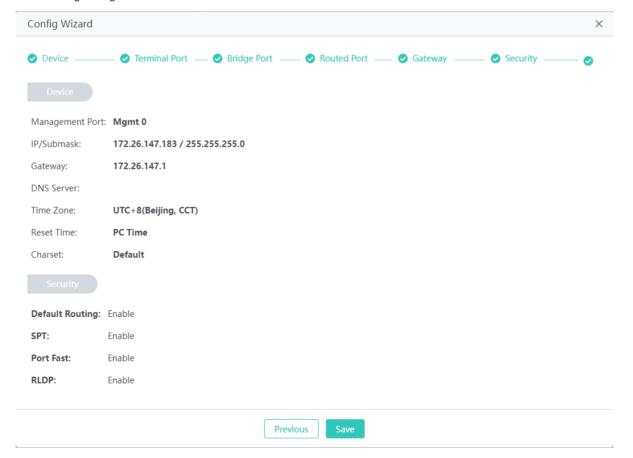| Allowed VLAN	Gateway	IPv4 Address	Submask:	Action
	☑ Enable			Delete

Previous   Next

The steps of configuring a gateway are as follows:

1) Click **Add** to add a gateway.

2) Click **Delete** to delete the gateway.

3) Click **Next** after completing the configuration as prompted.

● Security

Config Wizard   ✕

⊘ Device ----------- ⊘ Terminal Port ---- ⊘ Bridge Port ------- ⊘ Routed Port ------ ⊘ Gateway ----------- 🛡 Security --------- ✓

Note: Default routing is enabled by default. If there are multiple routed ports, priority will be assigned to these ports based on record ID.

Default Routing: ☑ Enable

SPT: ☑ Enable

Port Fast: ☑ Enable

RLDP: ☑ Enable

Previous   **Next**

Select the functions to be enabled and click **Next**.

● Saving configurations

Config Wizard   ✕

⊘ Device ----------- ⊘ Terminal Port ---- ⊘ Bridge Port ------- ⊘ Routed Port ------ ⊘ Gateway ----------- ⊘ Security ----------- ⊘

Device

Management Port: **Mgmt 0**

IP/Submask: **172.26.147.183 / 255.255.255.0**

Gateway: **172.26.147.1**

DNS Server:

Time Zone: **UTC+8(Beijing, CCT)**

Reset Time: **PC Time**

Charset: **Default**

Security

Default Routing: Enable

SPT: Enable

Port Fast: Enable

RLDP: Enable

Previous   **Save**

Check the configurations and click **Save** to deliver configuration commands. After the configuration succeeds, the **Config Wizard** window automatically disappears. If you change the management IP address of the device, determine whether to redirect to the new management address and perform operations above.

1.3.2   Monitoring

Click **Monitoring** to open the level-2 menu, which includes **SWITCH Overview**, **Anti-loop Monitoring**, **DHCP**, and **Other Monitoring**.

1.3.2.1   SWITCH Overview

The **SWITCH Overview** page displays basic information about the device, including the device MAC address, device model, device running time, version information, device CPU and memory, port status, port traffic trend, and port bandwidth usage.

Standalone scenario

For the Top 5 ports in bandwidth usage, click **More**. A dialog box will be displayed.

	Interface	Rx Bandwidth Usage ⇕	Tx Bandwidth Usage ⇕	Status(Port real speed)	UnderSize/OverSize	CRC/FCS Error	Collision Count
☐	Gi0/1	0.010	0.000	Connected(1000M)	0/0	0/0	0

↺ Back   ⟳ Refresh   ✕ Clear Selected   ✕ Clear All

Show No.: 10 ∨ Total Count:1   ⏮ First ‹ Pre ① Next › Last ⏭ 1 GO

1.3.2.2   Anti-loop Monitoring

The **Anti-loop Monitoring** page monitors the loop status based on the STP status and RLDP status.
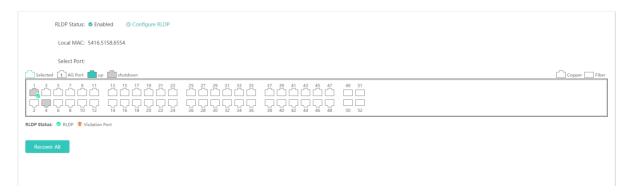
1.3.2.2.1   STP Status

The **STP Status** tab page displays **STP Status**, **STP Mode**, **Root Status**, **Instance**, and port use status.

STP Status: ✔ Enabled   ⚙ Configure STP

STP Mode: MSTP

Root Status: Root

Instance: [0   ∨]

Select Port:

☐ Selected ☐1 AG Port ☐ up ☐ shutdown   ☐ 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
```

Port Role: Ⓡ Root Port Ⓓ Designated Port Ⓐ Alternate Port Ⓜ Master Port   STP Status: ✔ Forwarding ⊗ Blocking ◯ STP Enabled   ◯ Port Fast Enabled

1.3.2.2.2   RLDP Status

The **RLDP Status** tab page displays **RLDP Status**, **Local MAC**, handling method of port violation, and RLDP status.

RLDP Status: ✔ Enabled   ⚙ Configure RLDP

Local MAC: 5416.5158.6554

Select Port:

☐ Selected ☐1 AG Port ☐ up ☐ shutdown   ☐ 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
```

RLDP Status: ✔ RLDP ⊗ Violation Port

[Recover All]
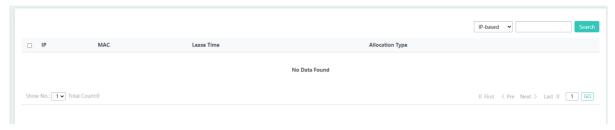
1.3.2.3   DHCP

DHCP is monitored from the DHCP server status and DHCP client list.
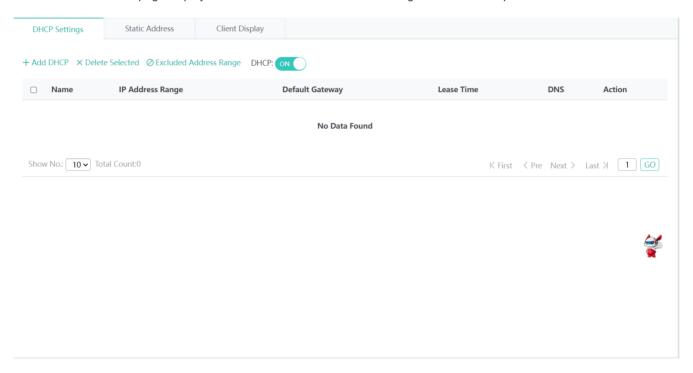
1.3.2.3.1   Client List

The **Client List** tab page displays clients assigned IP addresses in the address pool on the switch.

☐	IP	MAC	Lease Time	Allocation Type
			No Data Found	

Show No.: 1 ▾ Total Count:0   K First   ‹ Pre   Next ›   Last ⟩   1   GO

1.3.2.3.2   Server Status

The **Server Status** tab page displays the DHCP server status and the usage of the address pool.

DHCP Settings	Static Address	Client Display

＋ Add DHCP   ✕ Delete Selected   ⊘ Excluded Address Range   DHCP: ON ⬤

☐	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
			No Data Found			

Show No.: 10 ▾ Total Count:0   K First   ‹ Pre   Next ›   Last ⟩   1   GO

1.3.2.4   Other Monitoring

1.3.2.4.1   VSU Status

The device monitors the VSU status only when the device works in VSU mode. You can check the topology of the VSU composed of devices, BFD status, and the status of ports, on which bidirectional forwarding detection (BFD) is enabled.

1.3.3   Config
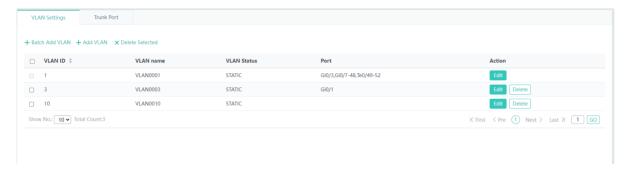
Click **Config** to open level-2 menu, which includes **Network**, **Other**, **Security**, and **Advanced**.

1.3.3.1   Network
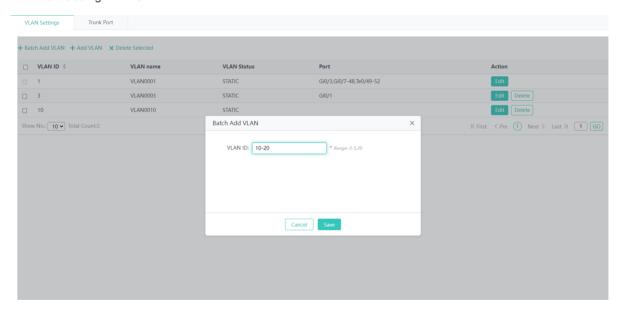
1.3.3.1.1   VLAN

The **VLAN** page consists of **VLAN Settings** and **Trunk Port**.

↘   **VLAN Settings**
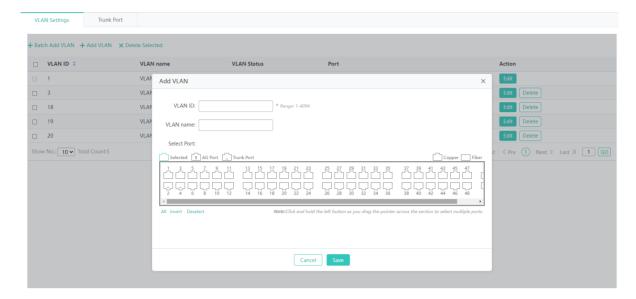
●   Bulk adding VLANs
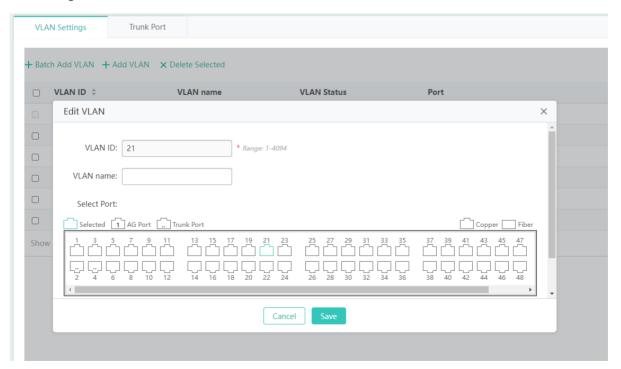
The steps of bulk adding VLANs are as follows:

1)   Click **Batch Add VLAN**.

2)   Enter VLAN IDs or ranges, which can be separated by commas (,).

3)   Click **Save**. The message "Add Succeeded" is displayed and the added VLANs are displayed in the list.

●   Adding a VLAN

The steps of adding a VLAN are as follows:
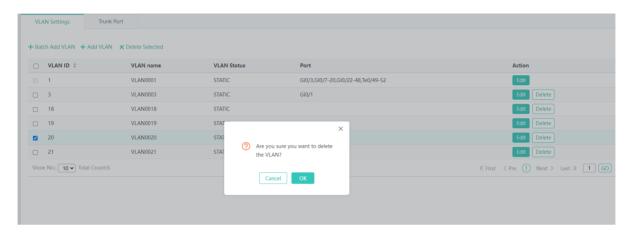
1) Click **Add VLAN**.

2) (Required) Enter the VLAN ID.

3) (Optional) Enter the VLAN name.

4) (Optional) Select ports.

5) Click **Save**. The message "Add Succeeded" is displayed and the added VLAN is displayed in the list.

● Editing a VLAN

The steps of editing a VLAN are as follows:
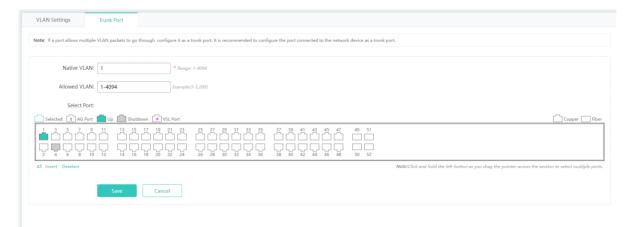
1) Click **Edit** in the **Action** column for a VLAN to be edited. Information about the VLAN is displayed in the pop-up dialog box.

2) Change the VLAN name.

3) Select ports.

4) Click **Save**. The message "Edit Succeeded" is displayed, indicating the editing is successful.

● Deleting a VLAN
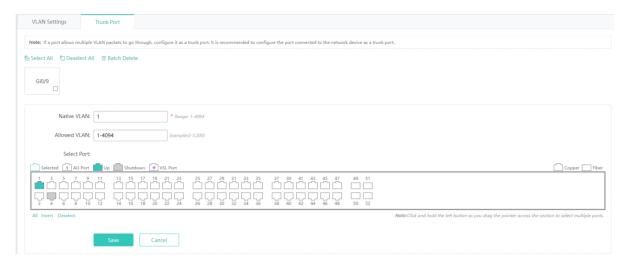
The steps of deleting a VLAN are as follows:

1) In the VLAN list, select multiple records and click **Delete Selected** to bulk delete the records.

2) In the VLAN list, click **Delete** in the **Action** column for a VLAN to be deleted. The message "Are you sure you want to delete the VLAN?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed and the VLAN is deleted.

ⓘ VLAN1 is the default VLAN. It can be only modified but cannot be deleted.

↘ **Trunk Port**

● Adding a trunk port

The steps of adding a trunk port are as follows:
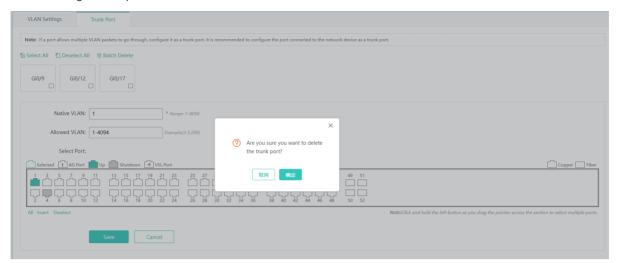
1) Select a port on the panel.

2) Set **Native VLAN** and **Allowed VLAN**. **Native VLAN** is required and **Allowed VLAN** is optional. You can enter a range or a specific VLAN ID.

3) Click **Save**. The message "Configuration Succeeded" is displayed and the add operation is completed. The added trunk port is displayed in the trunk port list.

● Editing a trunk port

The steps of editing a trunk port are as follows:

1) In the trunk port list, click a trunk port to be edited.

2) Edit **Native VLAN** and **Allowed VLAN**. **Native VLAN** is required and **Allowed VLAN** is optional. You can enter a range or a specific VLAN ID.

3) Change the selected port.

4) After editing information about the trunk port, click **Edit**. The message "Configuration Succeeded" is displayed, indicating that the edit operation is completed.

● Deleting a trunk port

The steps of deleting a trunk port are as follows:

1) In the trunk port list, move the cursor over a trunk port to be deleted. The ⊗ icon appears. Click this icon to delete the trunk port.

2) The message "Are you sure you want to delete the trunk port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed.

● Bulk deleting trunk ports
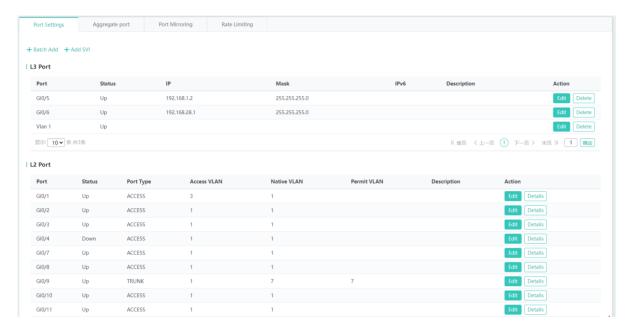
The steps of bulk deleting trunk ports are as follows:

1) In the trunk port list, select trunk ports to be deleted and click **Batch Delete**.

2) The message "Are you sure you want to delete the trunk port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
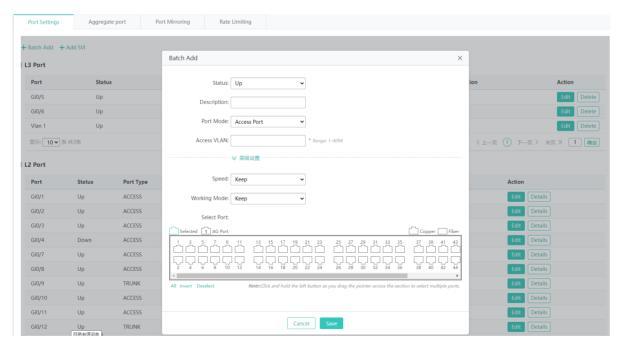
1.3.3.1.2   Port

The **Port** page allows you to configure basic information about ports, and configure aggregate ports, port mirroring, and port rate limit.

↘ **Port Settings**

● Bulk setting ports
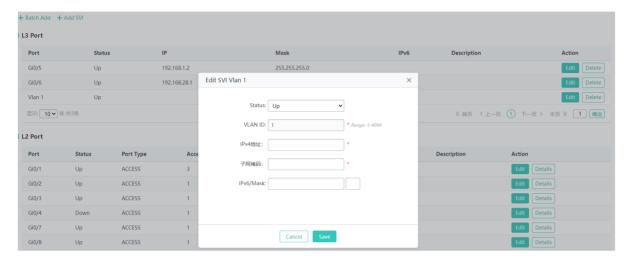
The steps of bulk setting ports are as follows:

1)   Click **Batch Add**. The **Batch Add** dialog box is displayed.

2) Set **Access VLAN**, **Speed**, and **Working Mode**. **Access VLAN** is a required field. **Speed** and **Working Mode** are set to **Keep**, which does not need to be modified.
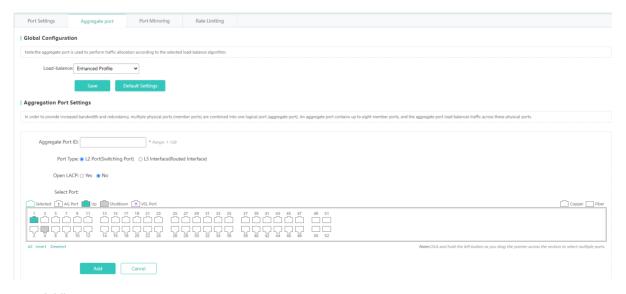
3) Select ports.

4) After setting, click **Save**. The message "Configuration Succeeded" is displayed and the ports are displayed in the list, indicating that the batch setting of the ports is completed.

● Editing a port
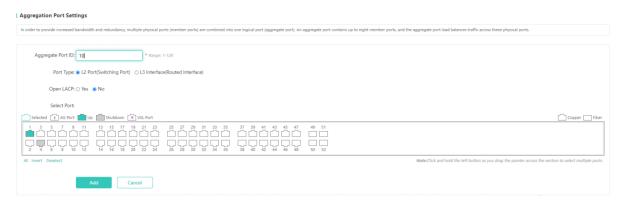
The steps of editing a port are as follows:

1) In the port list, click **Edit** in the **Action** column for a port to be edited. Information about the port is displayed.

2) Edit information. **VLAN ID**, **IPv4 Address**, and **Mask** are required fields.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed and relevant configuration is displayed in the list, indicating that port editing is completed.

↘ **Aggregate Port**
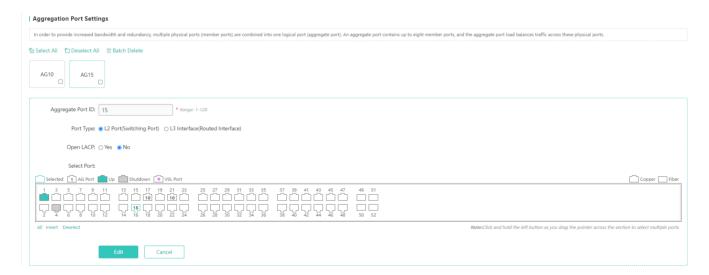
● Adding an aggregate port

The steps of adding an aggregate port are as follows:
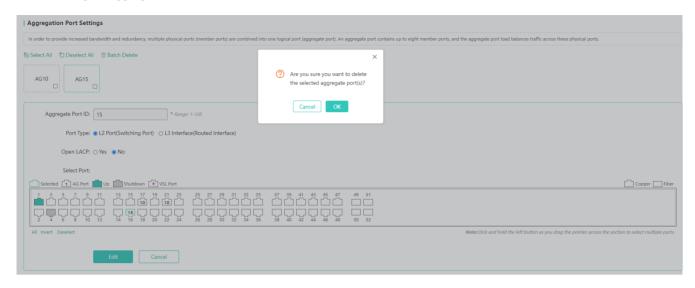
1) Set **Aggregate Port ID**.

2) Set **Port Type** to **L2 Port (Switch Port)** or **L3 Interface (Routed Interface)**.

3) Select whether to enable LACP.

4) Select ports.

5) After configuration, click **Add**. The message "Configuration Succeeded" is displayed, indicating that the aggregate port is added. The port panel displays the successfully added aggregate port.

● Editing an aggregate port

The steps of editing an aggregate port are as follows:
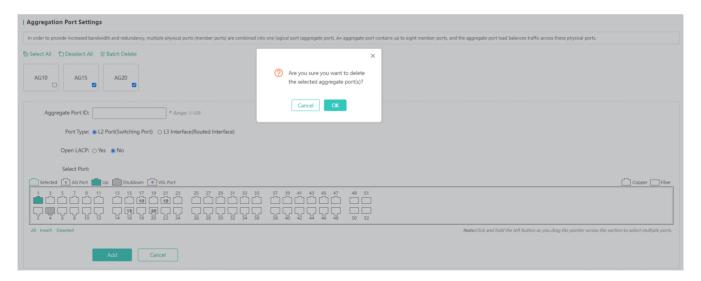
1) Aggregate ports displayed on the panel cannot be selected. To edit an aggregate port, click the aggregate port in the aggregate port list. Its member ports become selected. Click a port to deselect it and then click **Edit** to modify the aggregate port.

2) Modify **Port Type** and **Open LACP**.

3) You can click a selected member port to deselect it.

4) After editing, click **Edit** to complete the editing of the aggregate port.

● Deleting an aggregate port

In the aggregate port list, move the cursor over an aggregate port and click ⊗ . The message "Are you sure you want to delete the selected aggregate port(s)?" is displayed. Click **OK** to delete the aggregate port.

● Bulk deleting aggregate ports
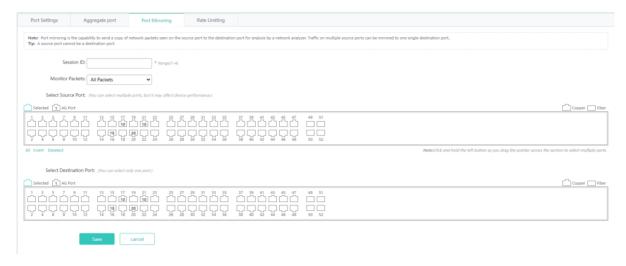
In the aggregate port list, select aggregate ports to be deleted and click **Batch Delete**. The message "Are you sure you want to delete the selected aggregate port(s)?" is displayed. Click **OK** to delete the aggregate ports.

⚠ Ports with the ARP check function, anti-ARP spoofing, or the MAC VLAN function enabled and monitored ports in port mirroring cannot be added to an aggregate port, and these ports are unavailable on the panel. When you move the cursor over an unavailable port, a message is displayed, indicating that the functions are enabled on the port and the port cannot be selected.

↘ **Port Mirroring**
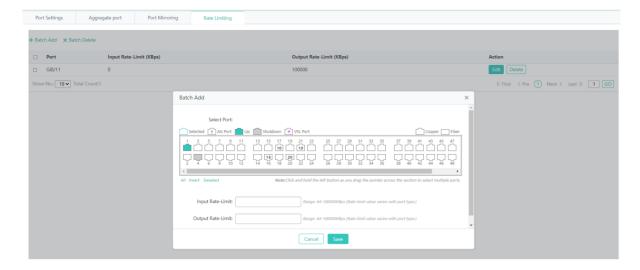
The steps of configuring port mirroring are as follows:

1) Enter the session ID.

2) Select a source port.

3) Select a destination port.

4) Click **Save**. The message "Configuration Succeeded" is displayed. The configured session is displayed on the GUI.

The panel displays the current port mirroring status, and both the source and destination ports can be edited. If you want to abandon a modification to port information, click **Refresh** to restore the panel to the current port mirroring status.

A member port of an aggregate port cannot be configured as the source or destination port, and the source and destination ports cannot be the same.

↘ **Rate Limiting**

● Adding a rate-limited port
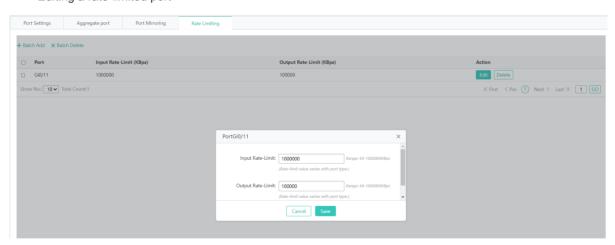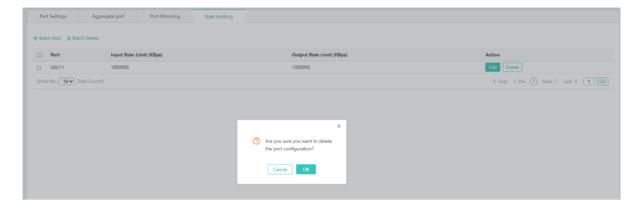
The steps of adding a rate-limited port are as follows:

1) Click **Batch Add**.

2) Select a port.

3) Set the input rate limit and output rate limit.

4) After configuration, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the rate-limited port is added. The port is displayed in the port rate limit list.

● Editing a rate-limited port

The steps of editing a rate-limited port are as follows:

1) In the port rate limit list, click **Edit** in the **Action** column for a port. Rate limits of the port are displayed.

2) Edit **Input Rate-Limit** and **Output Rate-Limit**.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the rate-limited port is edited successfully.

● Deleting a rate-limited port

The steps of deleting a rate-limited port are as follows:
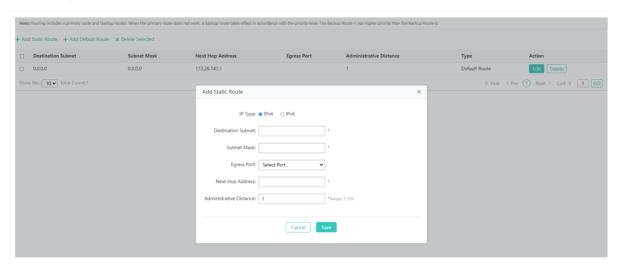
1) Select multiple records in the port rate limit list and click **Batch Delete** to bulk delete the records.

2) In the port rate limit list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the port configuration?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.1.3   Routing

The **Routing** page allows you to manage routes.

● Adding a static route
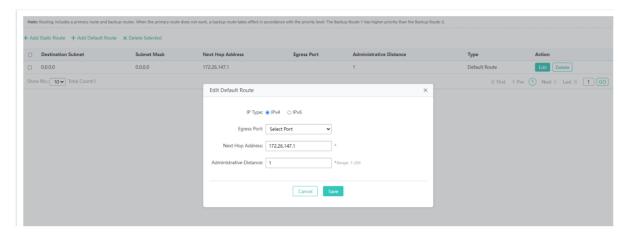
The steps of adding a static route are as follows:

1) Click **Add Static Route**.
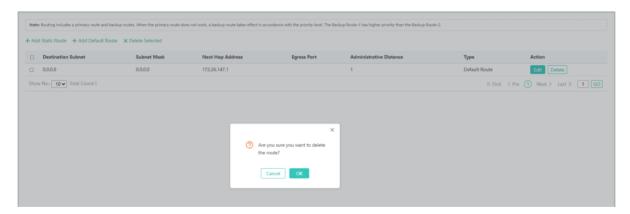
2) Configure **IP Type**, **Destination Subnet**, **Subnet Mask**, **Egress Port**, **Next Hop Address**, and **Administrative Distance**. **Destination Subnet**, **Subnet Mask**, **Next Hop Address**, and **Administrative Distance** fields are required fields.

3) After configuring parameters, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the static route is added successfully. The static route is displayed in the route list.
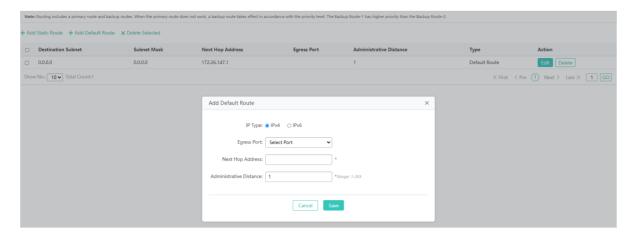
● Editing a route

The steps of editing a route are as follows:

1) In the route list, click **Edit** in the **Action** column for a route. Information about the route is displayed.

2) Configure **IP Type**, **Egress Port**, **Next Hop Address**, and **Administrative Distance**. **Next Hop Address** and **Administrative Distance** fields are required fields.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a route

The steps of deleting a route are as follows:

1) Select multiple records in the route list and click **Delete Selected** to bulk delete the records.

2) In the route list, click **Delete** in the **Action** column for a route. The message "Are you sure you want to delete the route?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

● Adding a default route

Note: Routing includes a primary route and backup routes. When the primary route does not work, a backup route takes effect in accordance with the priority level. The Backup Route-1 has higher priority than the Backup Route-2.

+ Add Static Route   + Add Default Route   ✕ Delete Selected

☐	Destination Subnet	Subnet Mask	Next Hop Address	Egress Port	Administrative Distance	Type	Action
☐	0.0.0.0	0.0.0.0	172.26.147.1		1	Default Route	Edit Delete

Show No.: 10 ⌄ Total Count:1   ⏮ First ‹ Pre ① Next › Last ⏭ 1 GO

Add Default Route   ✕

IP Type: ● IPv4   ○ IPv6

Egress Port: Select Port ⌄

Next Hop Address: [   ] *

Administrative Distance: [1]   *Range: 1-255

Cancel   Save

The steps of adding a default route are as follows:

1) Click **Add Default Route**.

2) Configure **IP Type**, **Egress Port**, **Next Hop Address**, and **Administrative Distance**. **Next Hop Address** and **Administrative Distance** are required fields.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the default route is added successfully. The default route is displayed in the route list.

ℹ️ Routes are classified into primary and backup routes. When a primary route becomes invalid, a backup route takes over services. Backup routes are selected based on their priorities. The priority of backup route 1 is higher than that of backup route 2.
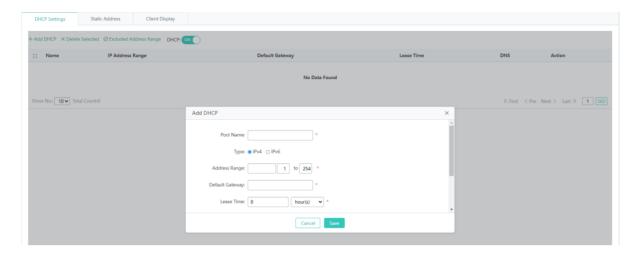
1.3.3.1.4   DHCP

The **DHCP** page allows you to configure DHCP and allocate static addresses, and displays the client list.
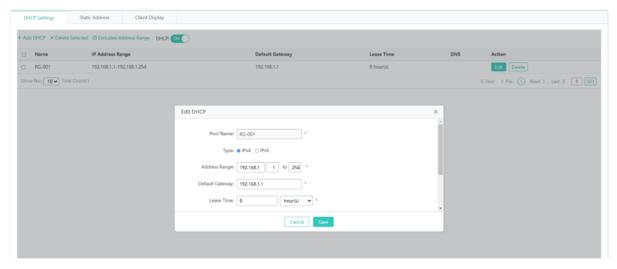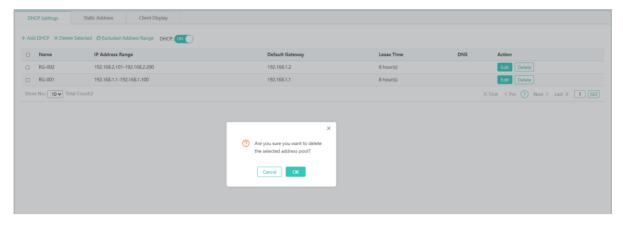
↘ **DHCP Settings**

DHCP Settings	Static Address	Client Display

+ Add DHCP   ✕ Delete Selected   ⊘ Excluded Address Range   DHCP: ON ⬤

☐	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
			No Data Found			

Show No.: 10 ⌄ Total Count:0   ⏮ First ‹ Pre Next › Last ⏭ 1 GO

● Adding a DHCP address pool

The steps of adding a DHCP address pool are as follows:

1) Click **Add DHCP**.

2) Configure **Pool Name**, **Type**, **Address Range**, **Default Gateway**, and **Lease Time**. **Pool Name**, **Type**, **Address Range**, **Default Gateway**, and **Lease Time** are required fields.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added DHCP address pool is displayed in the DHCP list.
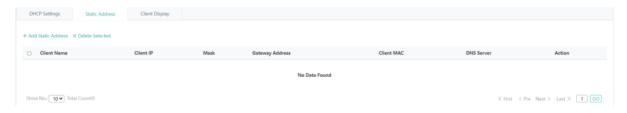
● Editing a DHCP address pool

The steps of editing a DHCP address pool are as follows:

1) In the DHCP list, click **Edit** in the **Action** column for a DHCP address pool. Information about the DHCP address pool is displayed.

2) Modify fields. **Pool Name**, **Type**, **Address Range**, **Default Gateway**, and **Lease Time** are required fields.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a DHCP address pool

The steps of deleting a DHCP address pool are as follows:

1) In the DHCP list, select multiple records and click **Delete Selected** to bulk delete the records.

2) In the DHCP list, click **Delete** in the **Action** column for a DHCP address pool. The message "Are you sure you want to delete the selected address pool?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

● Enabling DHCP
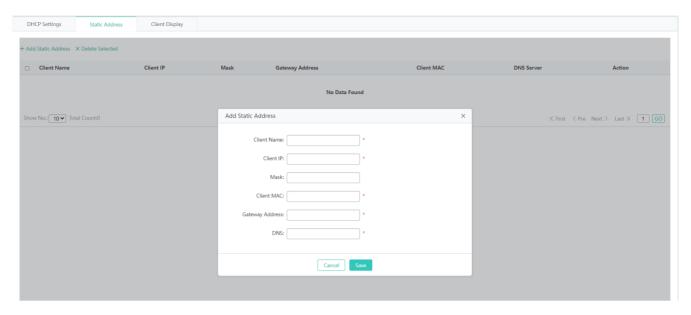
↘ **Static Address**

The figure below shows the **Static Address** tab page.
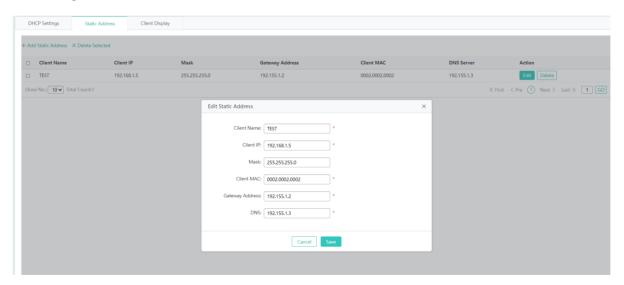
● Adding a static address

The steps of adding a static address are as follows:

1) Click **Add Static Address**.

2) Configure **Client Name**, **Client IP**, **Mask**, **Client MAC**, **Gateway Address**, and **DNS**. **Client Name**, **Client IP**, **Client MAC**, **Gateway Address**, and **DNS** are required fields.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added static address is displayed in the static address list.

● Editing a static address
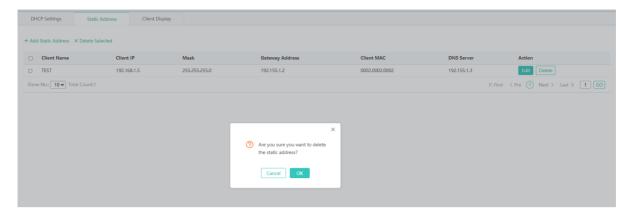
The steps of editing a static address are as follows:

1) In the static address list, click **Edit** in the **Action** column for a static address. Information about the static address is displayed.

2) Edit parameters. **Client Name**, **Client IP**, **Client MAC**, **Gateway Address**, and **DNS** are required fields.

3)   After editing, click **Save**. The message "Edit Succeeded" is displayed.

●   Deleting a static address
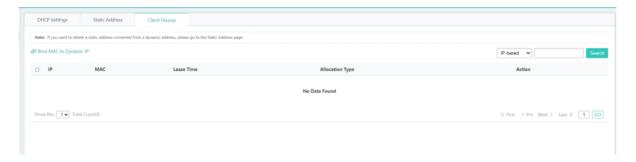
The steps of deleting a static address are as follows:

1)   Select multiple records in the static address list and click **Delete Selected** to bulk delete the records.

2)   In the static address list, click **Delete** in the **Action** column for a static address. The message "Are you sure you want to delete the static address?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

↘   **Client Display**

The figure below shows the **Client Display** tab page.

●   Querying an IP address

●   Binding a MAC address and a dynamic IP address
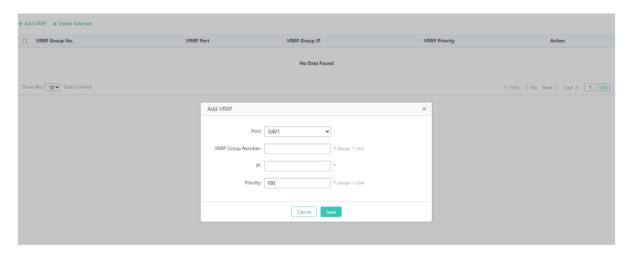
The steps of binding a MAC address and a dynamic IP address are as follows:

1) Select an IP address in the client list.

2) Click **Bind MAC to Dynamic IP** to bind the IP address to the current MAC address.
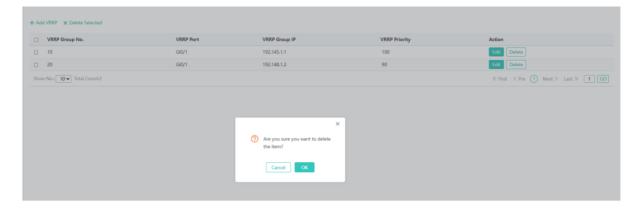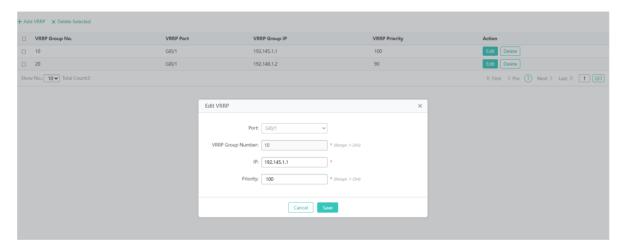
1.3.3.1.5   VRRP

● Adding a VRRP group

The steps of adding a VRRP group are as follows:

1) Click **Add VRRP**.

2) Configure **Port**, **VRRP Group Number**, **IP**, and **Priority**. **VRRP Group Number**, **IP**, and **Priority** are required fields.

3) After configuration, click **Save**. The message "Add Succeeded" is displayed. The added VRRP group is displayed in the VRRP list.

● Deleting a VRRP group

The steps of deleting a VRRP group are as follows:

1)   Select multiple records in the VRRP list and click **Delete Selected** to bulk delete the records.

2)   In the VRRP list, click **Delete** in the **Action** column for a VRRP group. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
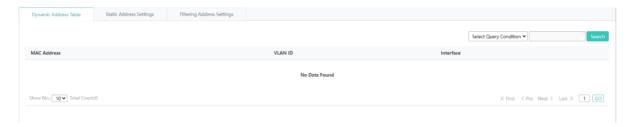
●   Editing a VRRP group

The steps of editing a VRRP group are as follows:

1)   In the VRRP list, click **Edit** in the **Action** column for a VRRP group. Information about the VRRP group is displayed.

2)   Edit parameters. VRRP Group Number, IP, and Priority are required fields.

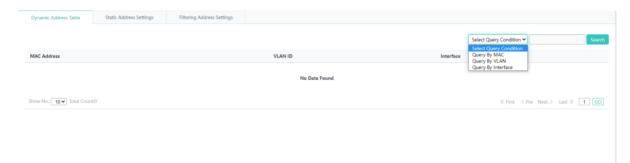3)   After editing, click **Save**. The message "Configuration Succeeded" is displayed.

1.3.3.1.6   MAC Address

The **MAC Address** page includes the **Dynamic Address Table**, **Static Address Settings**, and **Filtering Address Settings** tab pages.
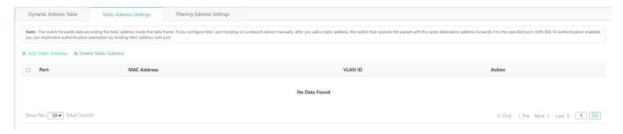
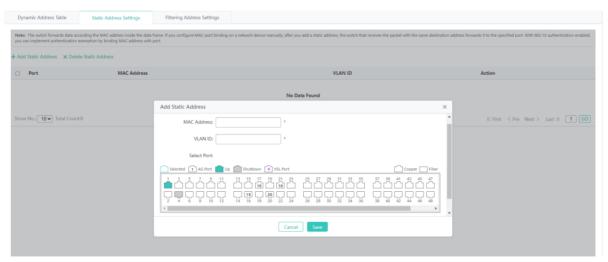**Dynamic Address Table**

- Querying dynamic addresses by conditions

Query conditions include **Select Query Condition**, **Query By MAC**, **Query By VLAN**, and **Query By Interface**.

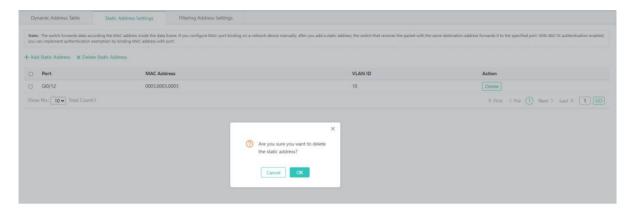## ↘ Static Address Settings

- Adding a static address

The steps of adding a static address are as follows:

1) Click **Add Static Address**.

2)   Configure a static address. **MAC Address**, **VLAN ID**, and port are required fields.

3)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added static address is displayed in the static address list.
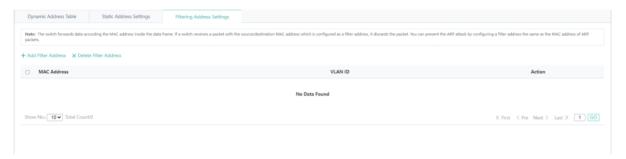
●   Deleting a static address

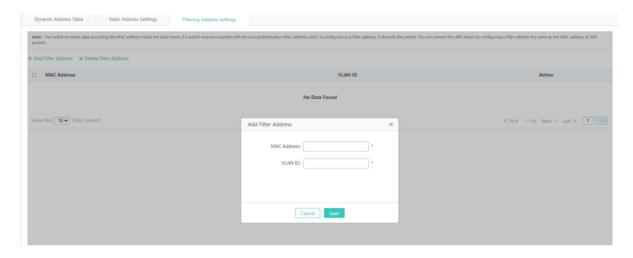The steps of deleting a static address are as follows:

1)   Select multiple records in the static address list and click **Delete Static Address** to bulk delete the records.

2)   In the static address list, click **Delete** in the **Action** column for a static address. The message "Are you sure you want to delete the static address?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

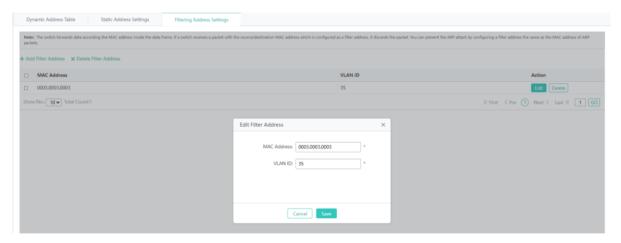↘   **Filtering Address Settings**
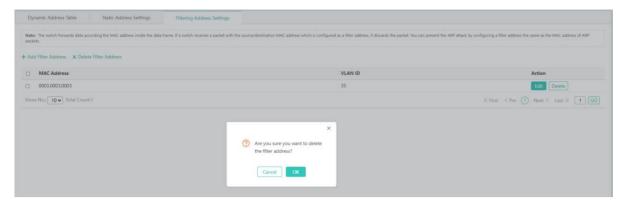

●   Adding a filter address

The steps of adding a filter address are as follows:

1) Click **Add Filter Address**.

2) Configure a filter address. **MAC Address** and **VLAN ID** are required fields.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added filter address is displayed in the filter address list.

● Editing a filter address

The steps of editing a filter address are as follows:

1) In the filter address list, click **Edit** in the **Action** column for a filter address. Information about the filter address is displayed.

2) Edit parameters. **MAC Address** and **VLAN ID** are required fields.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a filter address

The steps of deleting a filter address are as follows:

1)   Select multiple records in the filter address list and click **Delete Filter Address** to bulk delete the records.

2)   In the filter address list, click **Delete** in the Action column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
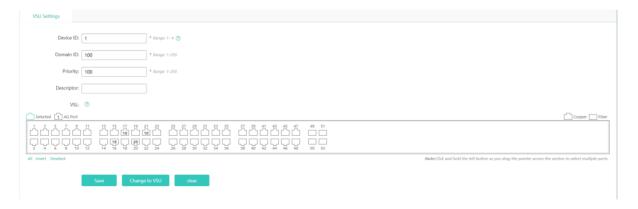
1.3.3.2   Other

1.3.3.2.1   VSU Settings

For devices supporting the VSU mode, the **VSU Settings** page in standalone mode is different from that in VSU mode. The domain IDs of devices composing the VSU must be the same. Device IDs must be unique in a VSU and the device with the highest priority is the master device.

↘   **Standalone Mode**

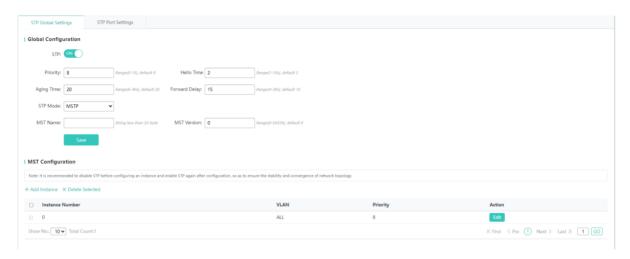The figure below shows the **VSU Settings** page in standalone mode.

In VSU standalone mode, **Device ID**, **Domain ID**, and **Priority** are required fields.

1.3.3.2.2   STP
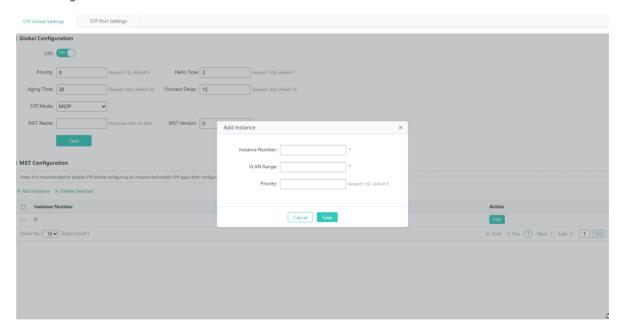
The **STP** page allows you to configure STP global parameters and STP ports.

↘   **STP Global Settings**

You can configure STP global parameters. When **STP Mode** is set to **MSTP**, you can configure an MST instance.
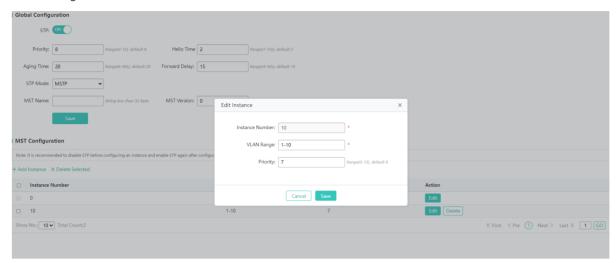
● Adding an instance

The steps of adding an instance are as follows:

1)   Click **Add Instance**.

2)   Configure an instance. **Instance Number** and **VLAN Range** are required fields and other fields are optional.

3)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added instance is displayed in the instance list.

● Editing an instance

The steps of editing an instance are as follows:

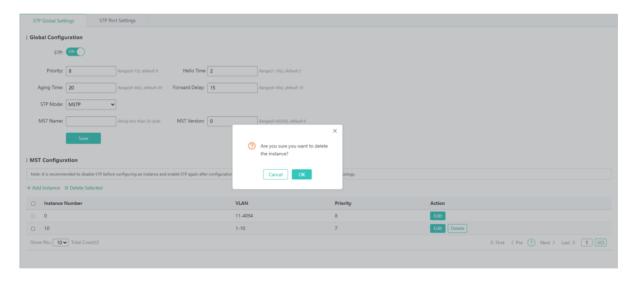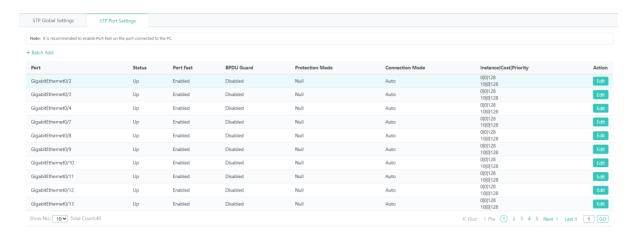1) In the instance list, click **Edit** in the **Action** column for an instance. Information about the instance is displayed.

2) Edit instance information. **Instance Number** and **VLAN Range** are required fields and other fields are optional.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting an instance
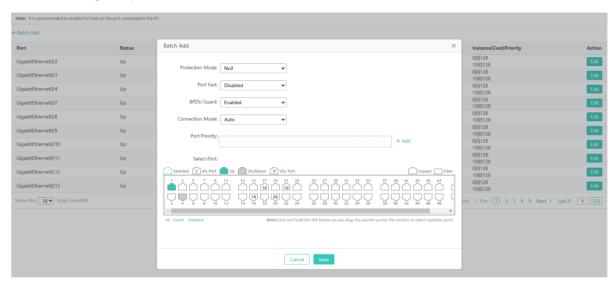
The steps of deleting an instance are as follows:

1) Select multiple records in the instance list and click **Delete Selected** to bulk delete the records.

2) In the instance list, click **Delete** in the **Action** column for an instance. The message "Are you sure you want to delete the instance?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed. Instance 0 is the default instance and cannot be deleted.

↘ **STP Port Settings**

| STP Global Settings | STP Port Settings | | | | | | |

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

+ Batch Add

Port	Status	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance|Cost|Priority	Action
GigabitEthernet0/2	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/3	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/4	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/7	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/8	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/9	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/10	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/11	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/12	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit
GigabitEthernet0/13	Up	Enabled	Disabled	Null	Auto	0|0|128 10|0|128	Edit

Show No.: 10 ▼ Total Count:48   First < Pre ① 2 3 4 5 Next > Last >| 1 GO

● **Bulk setting STP ports**

The steps of bulk setting STP ports are as follows:
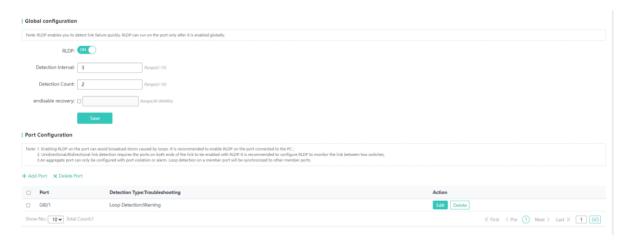
1) Click **Batch Add**.

2) Configure **Protection Mode**, **Port Fast**, **BPDU Guard**, **Connection Mode**, and **Port Priority,** and select ports.

● **Editing an STP port**

The steps of editing an STP port are as follows:

1) In the STP port list, click **Edit** in the **Action** column for an STP port. Information about the port is displayed.

2) Configure parameters.

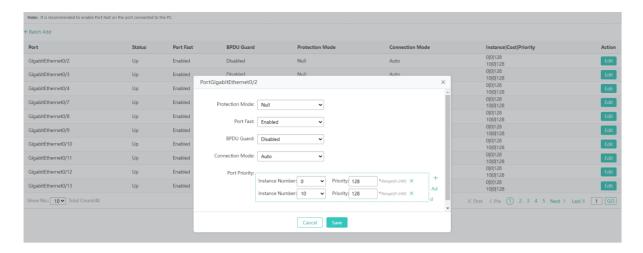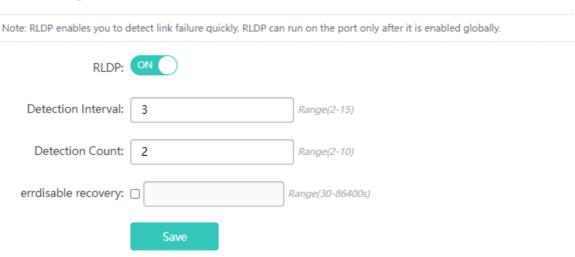3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.
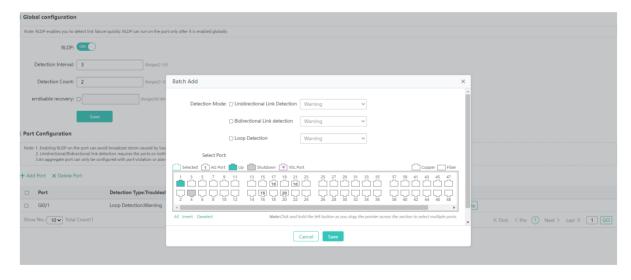
1.3.3.2.3   RLDP Settings

1. RLDP global configuration

The steps of configuring RLDP globally are as follows:

1)   Click **RLDP** to enable/disable the RLDP function.

2)   If RLDP is enabled, configure **Detection Interval**, **Detection Count**, and **errdisable recovery**, and click **Save**. The message "Configuration Succeeded" is displayed.
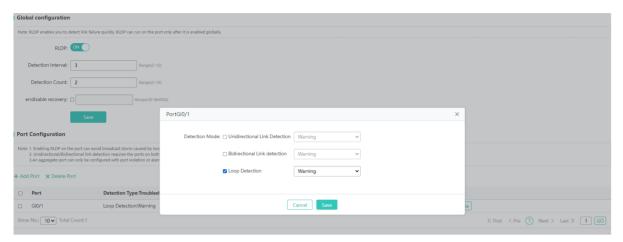
2.   Port RLDP configuration

●   Adding an RLDP port

The steps of adding an RLDP port are as follows:

1)   Click **Add Port**.
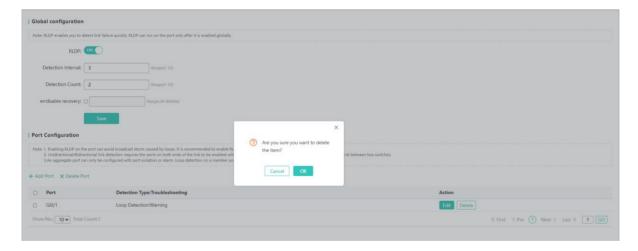
2)   Configure parameters.

3)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the RLDP port is added. The added RLDP port is displayed in the RLDP port list.

●   Editing an RLDP port

The steps of editing an RLDP port are as follows:

1)   In the RLDP port list, click **Edit** in the **Action** column for an RLDP port. Information about the RLDP port is displayed.

2)   Edit parameters.

3)   After editing, click **Save**. The message "Configuration Succeeded" is displayed.

●   Deleting an RLDP port

The steps of deleting an RLDP port are as follows:

1)   Select multiple records in RLDP port list and click **Delete Port** to bulk delete the records.

2)   In the RLDP port list, click **Delete** in the **Action** column for an RLDP port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
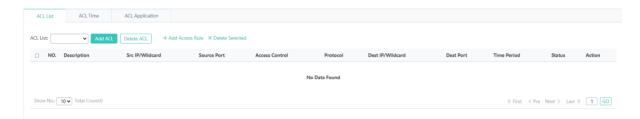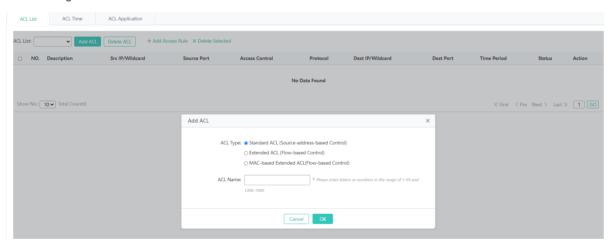
1.3.3.3   Security

1.3.3.3.1   ACL

When receiving a packet, a device port, on which an input ACL is configured, checks whether the packet matches an access control entry (ACE) in the input ACL. When sending out a packet, a device port, on which an output ACL is configured, checks whether the packet matches an ACE in the output ACL.

After different ACEs are configured, multiple ACEs may be applied at the same time or only a few ACEs are applied. Packets matching an ACE are processed (permitted or denied) according to the ACE.
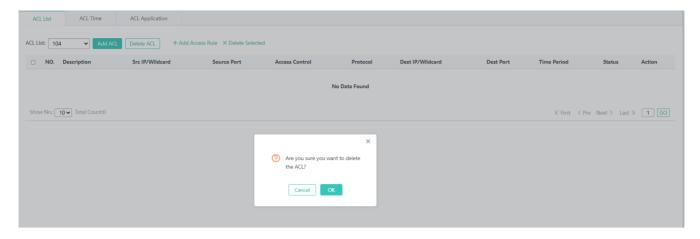
ACL List

● Adding an ACL
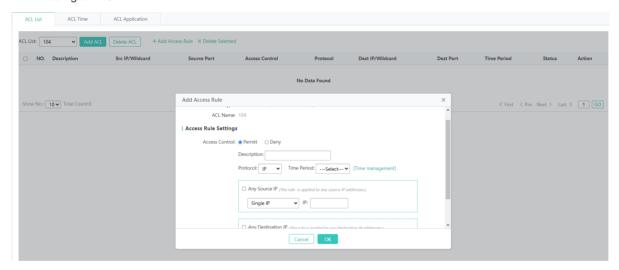
The steps of adding an ACL are as follows:

1) Click **Add ACL**.

2) Configure parameters in the displayed dialog box. **ACL Name** is a required field.

3) After configuration, click **OK**. The message "Configuration Succeeded" is displayed. The added ACL is displayed in the ACL List drop-down list.

● Deleting an ACL
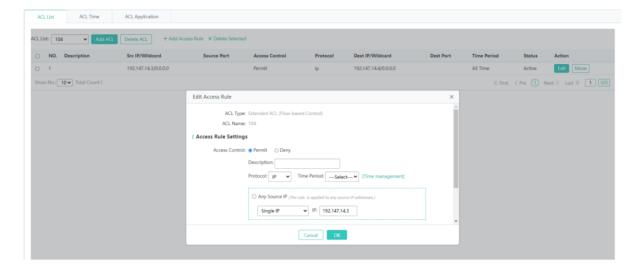
The steps of deleting an ACL are as follows:

1) Select an ACL to be deleted from the **ACL List** drop-down list.

2) Click **Delete ACL**. The message "Are you sure you want to delete the ACL?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed.

● Adding an ACE
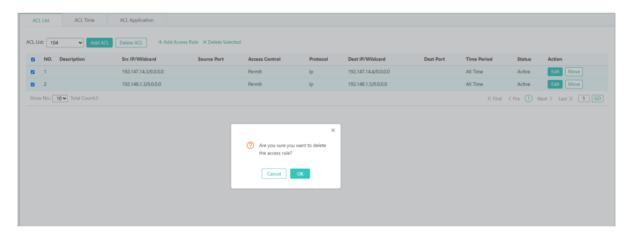
The steps of adding an ACE are as follows:

1) Select an ACL, to which ACEs need to be added, from the **ACL List** drop-down list.

2) Click **Add Access Rule**.

3) In the displayed dialog box, set parameters.

4) Click **OK**. The message "Configuration Succeeded" is displayed. The added ACE is displayed in the ACE list.

● Editing an ACE

The steps of editing an ACE are as follows:

1)   In the ACE list, click **Edit** in the **Action** column for an ACE.

2)   The displayed dialog box displays information about the ACE. Edit the ACE information.

3)   After editing, click **OK**. The message "Configuration Succeeded" is displayed, indicating that the editing operation is completed.

● Deleting an ACE

The steps of deleting an ACE are as follows:
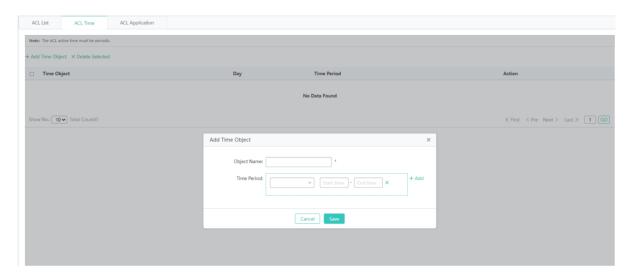
1)   Select one or more records in the ACE list.

2)   Click **Delete Selected**. The message "Are you sure you want to delete the access rule?" is displayed. Click **OK** to complete the deletion operation.

↘   **ACL Time**

You can make an ACL available based on time, for example, make an ACL take effect in some time ranges of a week. For this, you need to first configure a time object.
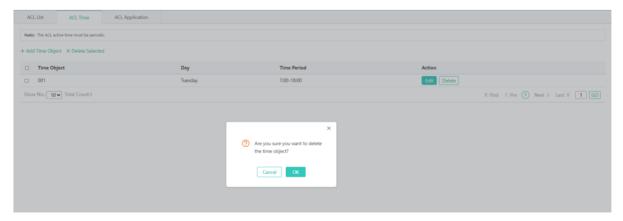
● Adding a time object

The steps of adding a time object are as follows:
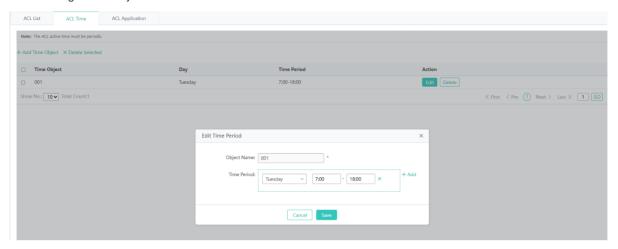
1) Click **Add Time Object**.

2) In the displayed dialog box, set parameters.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the operation is completed.

● Bulk deleting time objects

The steps of bulk deleting time objects are as follows:
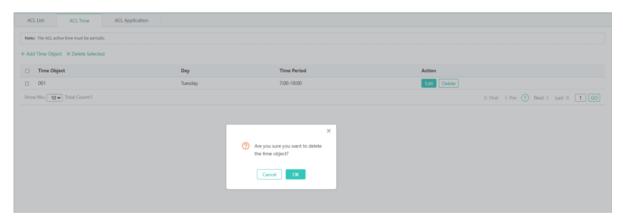
1) Select time objects to be deleted in the list.

2) Click **Delete Selected**. The message "Are you sure you want to delete the time object?" is displayed. Click **OK** to complete the deletion operation.

● Editing a time object

The steps of editing a time object are as follows:

1) Click **Edit** in the **Action** column for a time object in the list.

2) The displayed dialog box displays information about the time object. Edit the information.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the editing operation is completed.
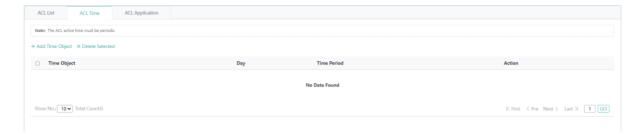
● Deleting a time object
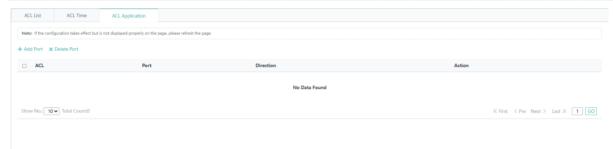
The steps of deleting time objects are as follows:

1) Click **Delete** in the **Action** column for a time object in the list.

2) The message "Are you sure you want to delete the time object?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed.
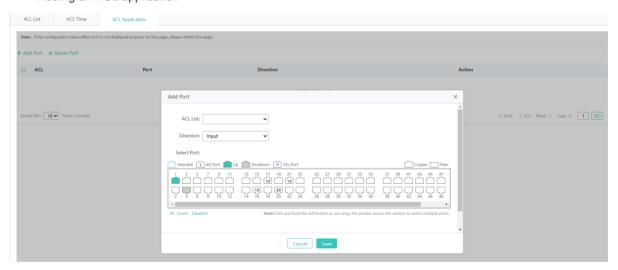
ACL Application

You can configure ACEs and apply them to ports or VLANs to restrict the access of specific users or allow users to access specific networks.

ⓘ   An ACL applied to a port may not displayed in the list immediately after application. You need to refresh the page first.
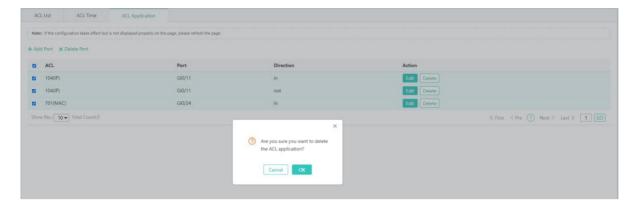
● Adding an ACL application
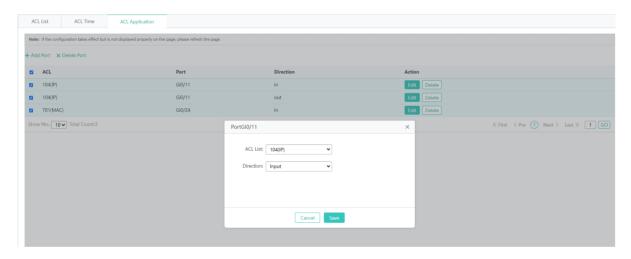
The steps of adding an ACL application are as follows:

1)   Click **Add Port**.

2)   The **Add Port** dialog box is displayed. Set parameters.

3)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added ACL application is displayed in the ACL list.

● Bulk deleting ACL applications
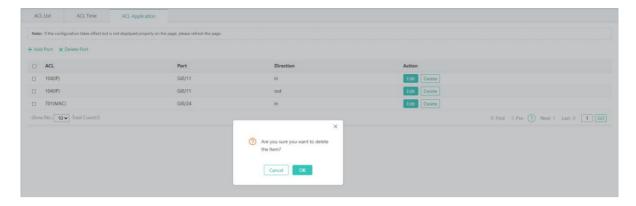
The steps of bulk deleting ACL applications are as follows:

1) Select one or more records in the ACL application list.

2) Click **Delete Port**. The message "Are you sure you want to delete the ACL application?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that deletion operation is completed.

● Editing an ACL application

The steps of editing an ACL application are as follows:

1) In the ACL application list, click **Edit** in the **Action** column for an ACL application.

2) The displayed dialog box displays information about the ACL application. Edit the information.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the editing operation is completed.

● Deleting an ACL application
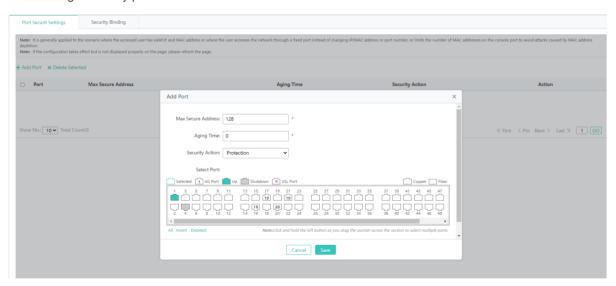
The steps of deleting an ACL application are as follows:

1) In the ACL application list, click **Delete** in the **Action** column for an ACL application.

2) The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is deleted.

1.3.3.3.2 Port Security

↘ **Port Security Settings**

● Adding a security port
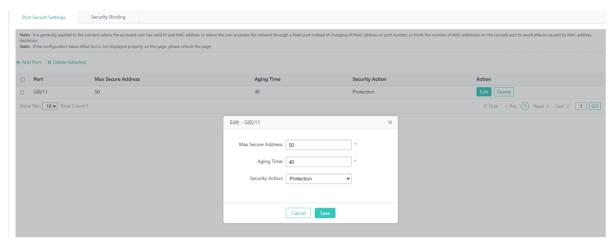
The steps of adding a security port are as follows:
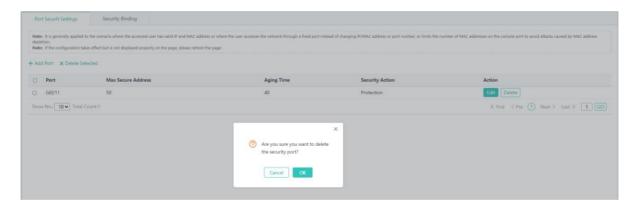
1) Click **Add Port**.

2) (Required) Configure **Max Secure Address**. The maximum value of this parameter is 128.

3) (Required) Configure **Aging Time**. The value range of this parameter is 0 to 1440.

4) Select one port at least.

5) After configuration, click **Save**. The message "Configuration Succeeded" is displayed, indicating that the adding operation is completed.

● Editing a security port


1) In the user security port list, click **Edit** in the **Action** column for a security port. Information about the security port is displayed.

2) Edit information.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a security port
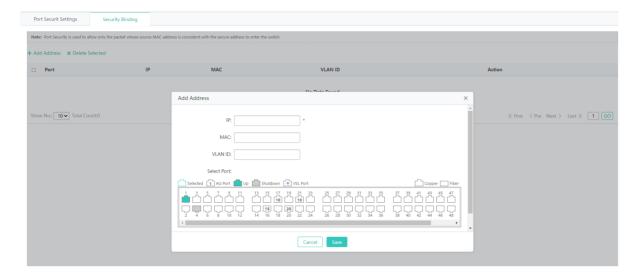
The steps of deleting a security port are as follows:

1) Select multiple records in the security port list and click **Delete Selected** to bulk delete the records.

2) In the security port list, click **Delete** in the Action column for a security port. The message "Are you sure you want to delete the security port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
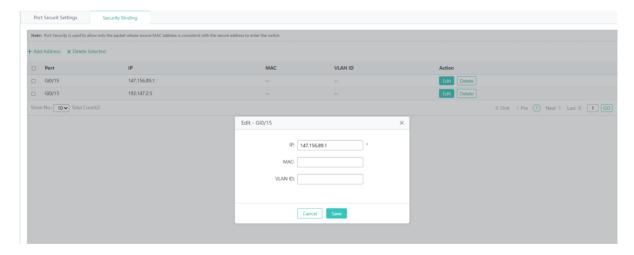
↘ **Security Binding**

● Adding a security address to be bound
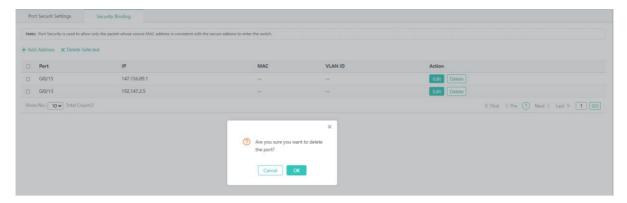
The steps of adding a security address to be bound are as follows:

3) Click **Add Address**.

4) Configure the security address to be bound. **IP** is required and other parameters are optional. Select a port.

5) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added security address is displayed in the list of bound security addresses.

● Editing a bound security address

1) In the list of bound security addresses, click **Edit** in the **Action** column for a bound security address. Information about the security address is displayed.

2) Edit information.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a bound security address

The steps of deleting a bound security address are as follows:

1) Select multiple records in the list of bound security addresses and click **Delete Selected** to bulk delete the records.

2) In the list of bound security addresses, click **Delete** in the **Action** column for a bound address. The message "Are you sure you want to delete the port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.3.3 Storm Control
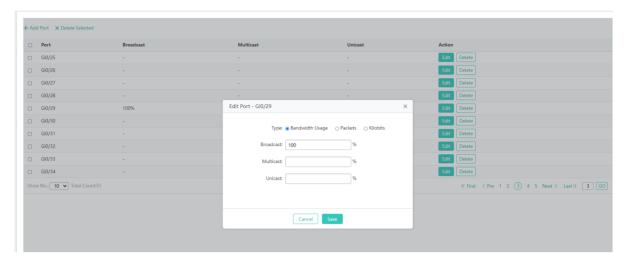
● Adding a storm control port

The steps of adding a storm control port are as follows:
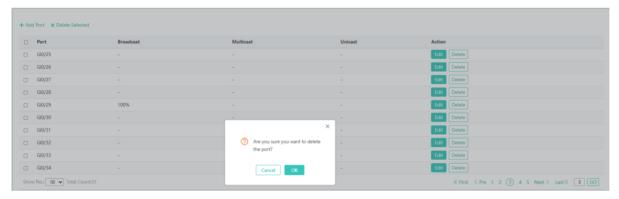
1) Click **Add Port**.

2) Set a storm control port. Set one of the **Broadcast**, **Multicast**, and **Unicast** parameters.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added storm control port is displayed in the storm control port list.

● Editing a storm control port

The steps of editing a storm control port are as follows:

1) In the storm control port list, click **Edit** in the **Action** column for a storm control port. Information about the storm control port is displayed.

2) Edit information.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a storm control port

The steps of deleting a storm control port are as follows:

1) Select multiple records in the storm control port list and click **Delete Selected** to bulk delete the records.

2) In the storm control port list, click **Delete** in the **Action** column for a storm control port. The message "Are you sure you want to delete the port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.3.4   DHCP Snooping

The figure below shows the **DHCP Snooping** page.

Figure 1-1 Setting DHCP Snooping

The steps of setting DHCP snooping are as follows:

1) Click **DHCP Snooping** to enable it.

2) Select the port to be configured.

3) Click **Save** to save the configuration. Click **Display DHCP Snooping Trusted Port** to display the configured ports.
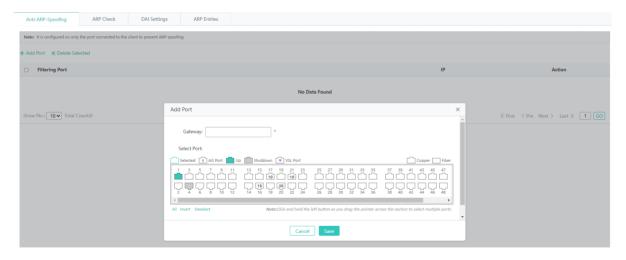
The port connecting to a DHCP server needs to be configured as a DHCP trusted port. The DHCP server connecting to a non-trusted port cannot work properly. A configured trusted port indicates that the DHCP trusted port is enabled on the port. You can select ports on the panel and click **Save**.

1.3.3.3.5 Gateway Anti-ARP-Snooping

The **Gateway Anti-ARP-Snooping** page allows you to configure anti-ARP spoofing, ARP check, DAI settings, and ARP entries.

↘ **Anti-ARP Spoofing**

● Adding a filter port
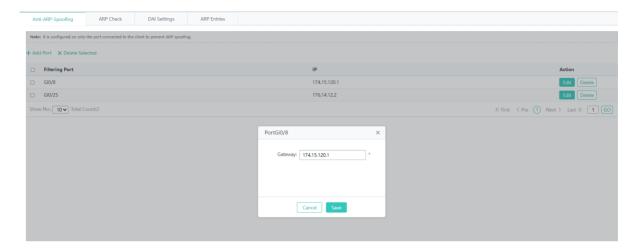
The steps of adding a filter port are as follows:

1) Click **Add Port**.

2) Set a filter port. Gateway is a required field. Select at least one filter port.
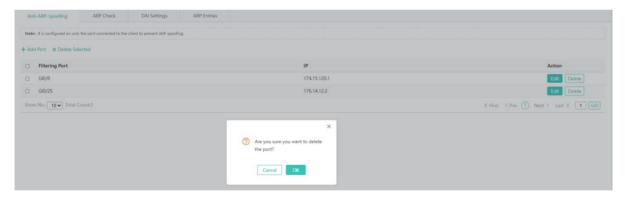
3)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added filter port is displayed in the filter port list.

●   Editing a filter port

The steps of editing a filter port are as follows:

1)   In the filter port list, click **Edit** in the **Action** column for a filter port. Information about the filter port is displayed.

2)   Edit information.

3)   After editing, click **Save**. The message "Configuration Succeeded" is displayed.
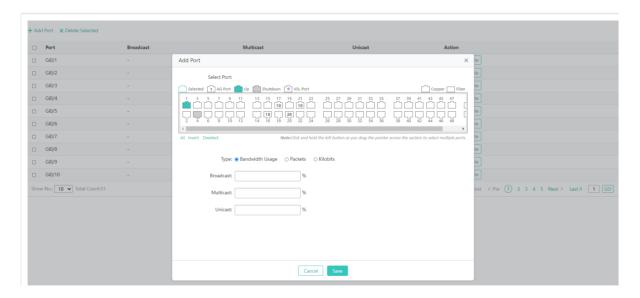
●   Deleting a filter port

The steps of deleting a filter port are as follows:

1)   Select multiple records in the filter port list and click **Delete Selected** to bulk delete the records.

2)   In the filter port list, click **Delete** in the **Action** column for a filter port. The message "Are you sure you want to delete the port?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

↘   **ARP Check**

| Anti-ARP-Spoofing | ARP Check | DAI Settings | ARP Entries |

Note: ARP Check is used to filter all ARP packets on the logical port and discard invalid ARP packets. It can effectively prevent ARP Spoofing and improve network stability. A DHCP Snooping trusted port cannot be enabled with ARP Check.

Select Port:

Selected | 1 AG Port | Up | Shutdown | VSL Port   Copper | Fiber

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

ARP-check Port: ✓

Save   Display ARP Check Port

The steps of configuring ARP check are as follows:

1) Ports, on which ARP check is enabled, are displayed on the page.

2) Select a port, on which ARP check needs to be enabled and click **Save**. The page displays the latest configuration.

3) Click **Display ARP Check Port** to display ports, on which ARP check is enabled.

ℹ The panel displays ports with the ARP check function enabled and the ports can be edited. If you want to abandon the modification to a port, click **Display ARP Check Port** to display the current ARP-check ports on the panel.

⚠ The ARP check function cannot be enabled on DHCP snooping trusted ports.
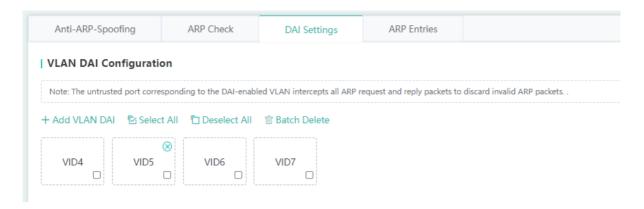
↘ DAI Settings

1. Configuring VLAN DAI

| 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. .

+ Add VLAN DAI

Trusted Port

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

Add VLAN DAI   ×

VLAN Range: [_____]   * *The VLAN range is formatted as 3-5,100.*

Cancel   Save

Selected | 1 AG Port | Up | Shutdown | VSL Port   Copper | Fiber

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

Trusted Port: ✓

Save   Display Trusted Port

The steps of configuring VLAN DAI are as follows:

1) Click **Add VLAN DAI**. The **Add VLAN DAI** dialog box is displayed.

2) Enter the VLAN range.

3) Click **Save**. The list configuration is refreshed.

2. Removing the VLAN DAI configuration

| 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. .

+ Add VLAN DAI   ☑ Select All   ☐ Deselect All   🗑 Batch Delete

| VID4 ☐ | VID5 ⊗ ☐ | VID6 ☐ | VID7 ☐ |

The steps of removing the VLAN DAI configuration are as follows:

1)   Select the required VLAN DAI configuration or click **Select All**, and click **Batch Delete**.

2)   Click the deletion icon in the upper right corner to delete the VLAN DAI configuration.

| Trusted Port

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

☐ Selected 1 AG Port ▮ Up ▮ Shutdown ◆ VSL 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

→ DAI Trusted Port

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

Trusted Port: ✅

Save   Display Trusted Port

The steps of configuring a DAI trusted port are as follows:

1)   Select a port to be configured as a DAI trusted port and click **Save**. The latest configuration is displayed.

2)   Click **Display Trusted Port** to display configured DAI trusted ports.

ℹ The panel displays DAI trusted ports and the ports can be edited. If you want to abandon the modification to a port, click Display Trusted Port to display current DAI trusted ports on the panel.

↘ **ARP Entries**

● Dynamic binding>>static binding

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries	

Dynamic Binding>>Static Binding   Delete Selected   Manual Binding   IP-based:

☐	IP	MAC	Type	Action
☐	1.1.1.1	4e54.3800.0002	Static Binding	Static Binding>>Dynamic Binding
☐	192.168.1.200	5416.5158.6555	Local ARP Entry	Dynamic Binding>>Static Binding

Show No.: 10 ⌄ Total Count: 2   K First   < Pre   Next >
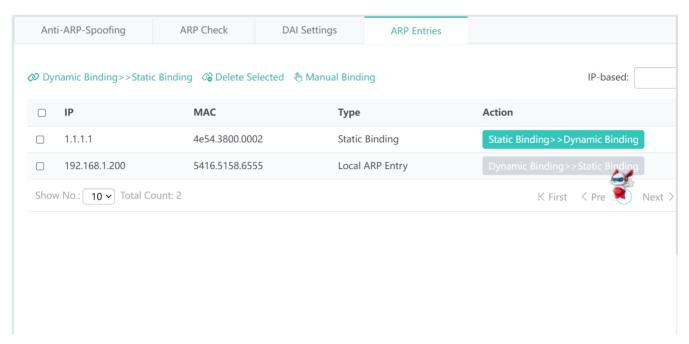
The steps of converting a dynamic binding into a static binding are as follows:
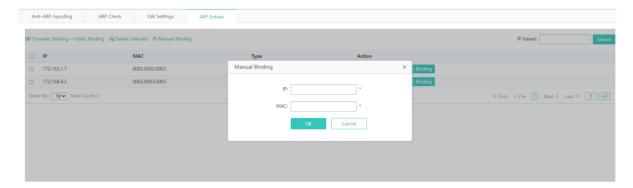
1) Select dynamic binding entries and click **Dynamic Binding>>Static Binding** to bulk convert the dynamic binding entries into static binding entries.

2) In the ARP entry list, click **Dynamic Binding>>Static Binding** in the **Action** column for an ARP entry. The message "Configuration succeeded!" is displayed.

● Deleting static bindings

Anti-ARP-Spoofing	ARP Check	DAI Settings	ARP Entries	

Dynamic Binding>>Static Binding   Delete Selected   Manual Binding   IP-based:

☐	IP	MAC	Type	Action
☐	1.1.1.1	4e54.3800.0002	Static Binding	Static Binding>>Dynamic Binding
☐	192.168.1.200	5416.5158.6555	Local ARP Entry	Dynamic Binding>>Static Binding

Show No.: 10 ⌄ Total Count: 2   K First   < Pre   Next >

The steps of deleting static bindings are as follows:

1) Select static binding entries and click **Delete Selected** to bulk delete the static binding entries.

2) In the ARP entry list, click **Static Binding>>Dynamic Binding** in the **Action** column for a static binding entry. The message "Configuration Succeeded" is displayed.

● Manual binding

The steps of performing manual binding are as follows:
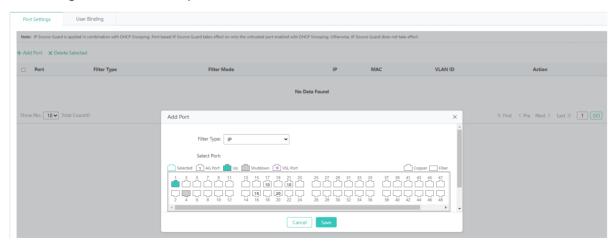
1) Click **Manual Binding**.

2) Configure static binding data. **IP** and **MAC** are required fields.

3) After configuration, click **OK**. The message "Configuration Succeeded" is displayed. The added static binding entry is displayed in the ARP entry list.

1.3.3.3.6   IP Source Guard

The **IP Source Guard** page allows you configure ports and bind users.

Port Settings

● Adding an IP Source Guard port
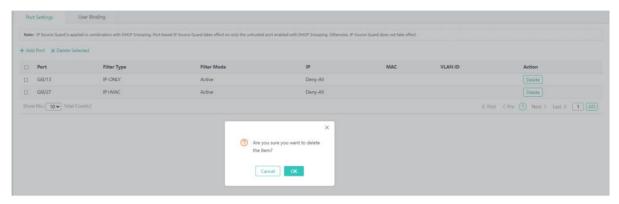
The steps of adding an IP Source Guard port are as follows:

1) Click **Add Port**. The **Add Port** dialog box is displayed.

2)   Set **Filter Type** and select ports.

3)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added IP Source Guard port is displayed in the IP Source Guard port list.

●   Deleting an IP Source Guard port
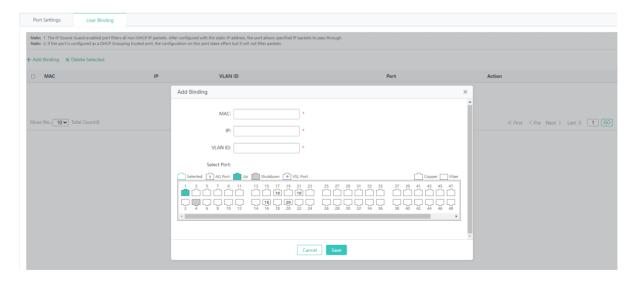
The steps of deleting an IP Source Guard port are as follows:

1)   Select multiple records in the IP Source Guard port list and click **Delete Selected** to bulk delete the records.

2)   In the IP Source Guard port list, click **Delete** in the **Action** column for an IP Source Guard port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

↘   **User Binding**

●   Adding a user binding
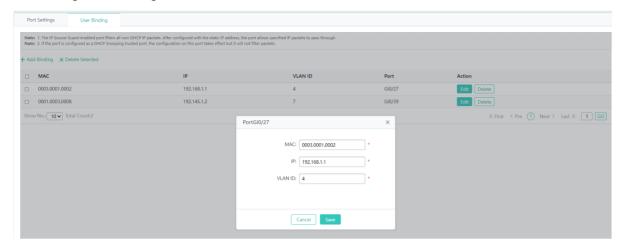
The steps of adding a user binding are as follows:

1)   Click **Add Binding**.

2)   Configure the user binding. **MAC**, **IP,** and **VLAN ID** are required fields.
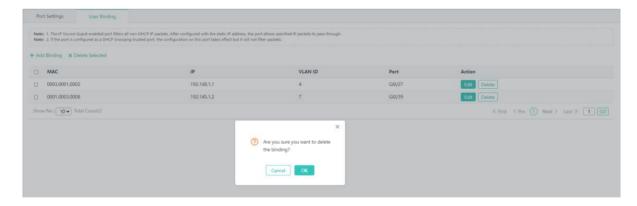
3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added user binding is displayed in the user binding list.

● Editing a user binding

The steps of editing a user binding are as follows:

1) In the user binding list, click **Edit** in the **Action** column for a user binding. Information about the user binding is displayed.

2) Edit information about the user binding.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a user binding
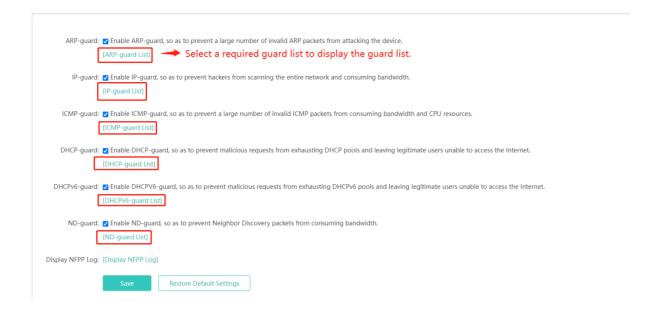
The steps of deleting a user binding are as follows:

1) Select multiple records in the user binding list and click **Delete Selected** to bulk delete the records.

2) In the user binding list, click **Delete** in the **Action** column for a user binding. The message "Are you sure you want to delete the binding?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.3.7 NFPP

The figure below shows the **NFPP** page.

ARP-guard: ☑ Enable ARP-guard, so as to prevent a large number of invalid ARP packets from attacking the device.
[ARP-guard List] → Select a required guard list to display the guard list.

IP-guard: ☑ Enable IP-guard, so as to prevent hackers from scanning the entire network and consuming bandwidth.
[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.
[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.
[ND-guard List]

Display NFPP Log: [Display NFPP Log]

Save   Restore Default Settings

You can enable/disable the attack guard function and click **Save**. The message "Configuration Succeeded" is displayed. To restore default settings, click **Restore Default Settings**.

1.3.3.4 Advanced
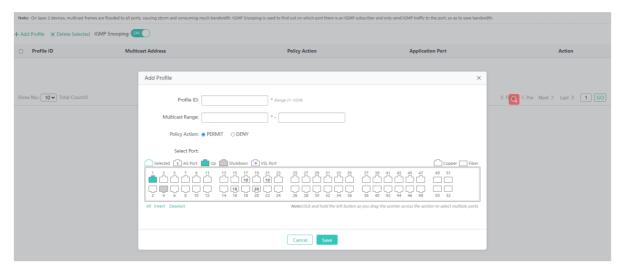
1.3.3.4.1 IGMP Snooping

The figure below shows the **IGMP Snooping** page.

Figure 1-2 Configuring IGMP Snooping

Note: On layer 2 devices, multicast frames are flooded to all ports, causing storm and consuming much bandwidth. IGMP Snooping is used to find out on which port there is an IGMP subscriber and only send IGMP traffic to the port, so as to save bandwidth.

+ Add Profile   ✕ Delete Selected   IGMP Snooping: ON

☐	Profile ID	Multicast Address	Policy Action	Application Port	Action
			No Data Found		

Show No.: 10 ⌄ Total Count:0 |< First   < Pre   Next >   Last >| 1   GO

● Adding a profile

The steps of adding a profile are as follows:

1) Click **Add Profile**.

2) Configure a profile. The **Profile ID** and **Multicast Range** fields are required and other fields are optional.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added profile is displayed in the profile list.

● Editing a profile

The steps of editing a profile are as follows:

1) In the profile list, click **Edit** in the **Action** column for a profile. Information about the profile is displayed.

2) Edit the profile.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a profile

The steps of deleting a profile are as follows:

1) Select multiple records in the profile list and click **Delete Selected** to bulk delete records.

2) In the profile list, click **Delete** in the **Action** column for a profile. The message "Are you sure you want to delete the profile?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

1.3.3.4.2   QOS

↘ **Class Settings**

The figure below shows the **Class Settings** tab page.

Figure 1-3 Class Settings
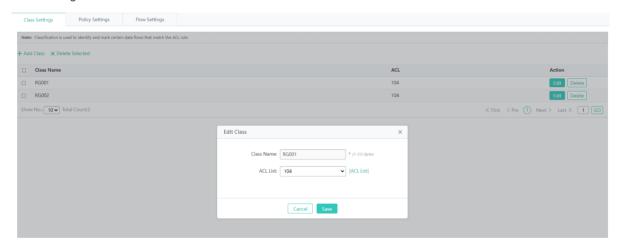
● Adding a class
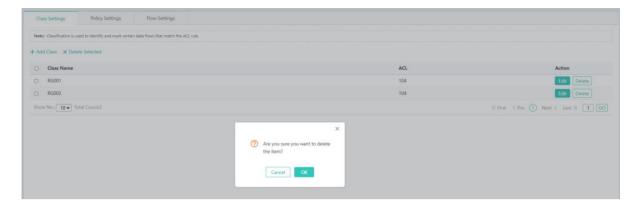
The steps of adding a class are as follows:

1) Click **Add Class**.

2) Configure a class. **Class Name** is a required field. Select an ACL.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added class is displayed in the class list.

● Editing a class

The steps of editing a class are as follows:

1) In the class list, click **Edit** in the **Action** column for a class. Information about the class is displayed.

2) Edit information about the class.

3) After editing, click **Save**. The message "Configuration Succeeded" is displayed.

● Deleting a class

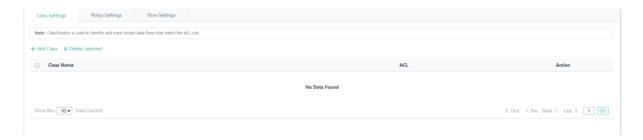The steps of deleting a class are as follows:

1) Select multiple records in the class list and click **Delete Selected** to bulk delete the records.

2) In the class list, click **Delete** in the **Action** column for a class. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
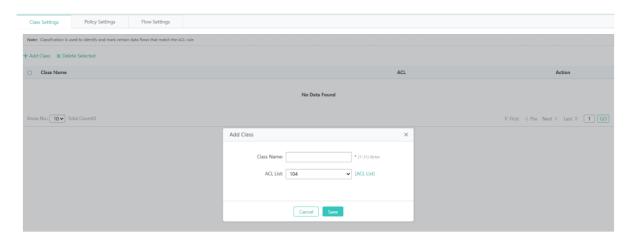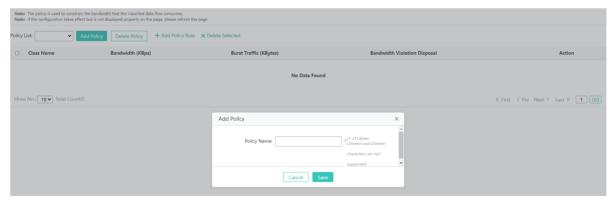
↘ **Policy Settings**

The figure below shows the **Policy Settings** tab page.

Figure 1-4 Policy Settings

● Adding a policy
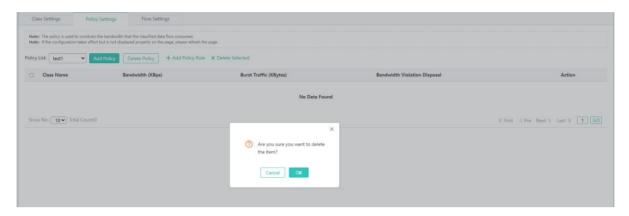
The steps of adding a policy are as follows:

1) Click **Add Policy**.
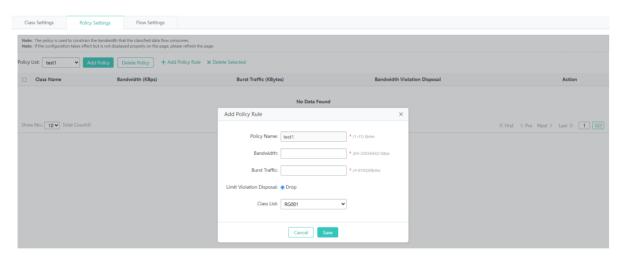
2) Configure a policy. **Policy Name** is a required field.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added policy is displayed in the policy list.

●   Deleting a policy
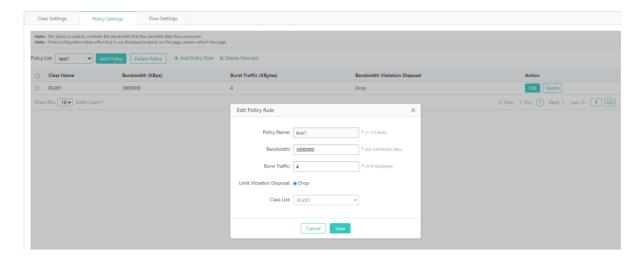
The steps of deleting a policy are as follows:

1) Select a policy in the policy list and click **Delete Policy**.

2) The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.

●   Adding a policy rule
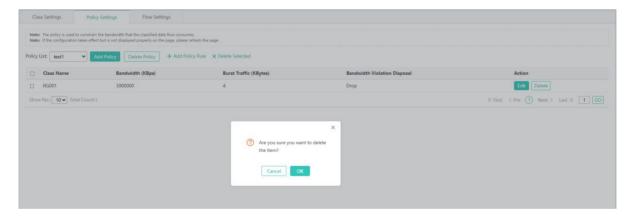
The steps of adding a policy rule are as follows:

1) Click **Add Policy Rule**.

2) Configure a policy rule. **Bandwidth** and **Burst Traffic** are required and other fields are optional.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added policy rule is displayed in the policy rule list.

●   Editing a policy rule

The steps of editing a policy rule are as follows:

1)   In the policy rule list, click **Edit** in the **Action** column for a policy rule. Information about the policy rule is displayed.

2)   Edit the policy rule.

3)   After editing, click **Save**. The message "Configuration Succeeded" is displayed.
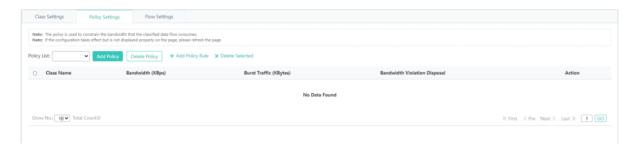
●   Deleting a policy rule

The steps of deleting a policy rule are as follows:

1) Select multiple records in the policy rule list and click **Delete Selected** to bulk delete records.

2) In the policy rule list, click **Delete** in the **Action** column for a policy rule. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
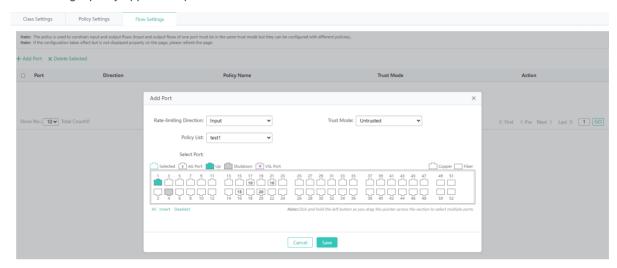
↘ **Flow Settings**

The figure below shows the **Flow Settings** page.

Figure 1-5 Flow Settings

| Class Settings | Policy Settings | Flow Settings | | | |

Note: The policy is used to constrain input and output flows (Input and output flows of one port must be in the same trust mode but they can be configured with different policies)..
Note: If the configuration takes effect but is not displayed properly on the page, please refresh the page.

+ Add Port   ✕ Delete Selected

☐	Port	Direction	Policy Name	Trust Mode	Action
			No Data Found		

Show No.: 10 ▾ Total Count:0

K First   〈 Pre   Next 〉   Last ✕   1   GO

● Adding a policy application port

The steps of adding a policy application port are as follows:

1) Click **Add Port**.

2) Configure a policy application port. Set **Rate-limiting Direction**, **Trust Mode**, **Policy List**, and **Port**.

3) After configuration, click **Save**. The message "Configuration Succeeded" is displayed. The added policy application port is displayed in the policy application port list.

● Deleting a policy application port

The steps of deleting a policy application port are as follows:

1) Select multiple records in the policy application port list and click **Delete Selected** to bulk delete records.

2)   In the policy application port list, click **Delete** in the **Action** column for a policy application port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete Succeeded" is displayed, indicating that the deletion operation is completed.
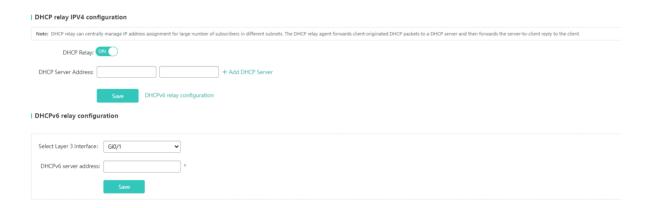
1.3.3.4.3   DHCP Relay

The figure below shows the **DHCP Relay** page.

Figure 1-6 Setting DHCP Relay

Enable/Disable DHCP Relay. When DHCP Relay is enabled, you can set multiple DHCP server addresses.

The steps of configuring DHCP Relay are as follows:

1)   Enable DHCP Relay.

2)   Set a DHCP server address.

3)   You can enable DHCPv6 Relay.

4)   Click **Save**. The DHCP Relay configuration is displayed on the page.

1.3.3.4.4   Authentication

The **Authentication** page allows you to configure ePortal and advanced settings.

↘   **ePortal**

The figure below shows the **ePortal** tab page.
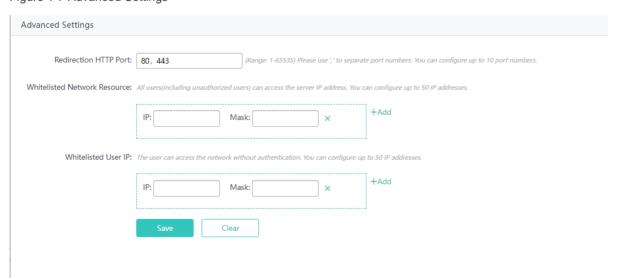
The steps of configuring ePortal are as follows:

1)   Set **Eportal Type** to **ePortalv2**.

2)   Configure parameters. **Portal Server IP**, **Redirection URL**, **Portal Key**, and **SNMP Server** are required fields.

3)   Select a port.

4)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed.

↘   **Advanced Settings**

The figure below shows the **Advanced Settings** page.

Figure 1-7 Advanced Settings

The steps of configuring advanced settings are as follows:

1)   Click **Add**.
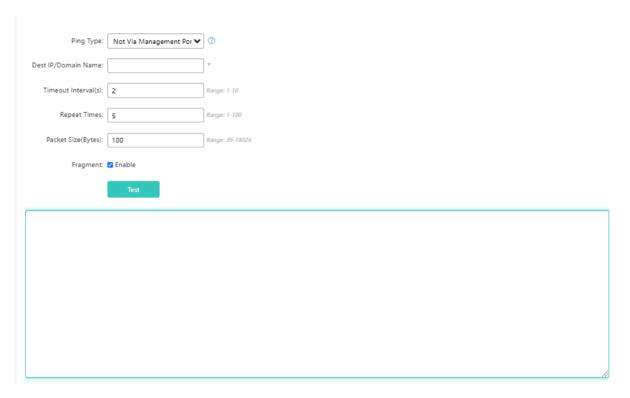
2)   Configure **Whitelisted Network Resource** and **Whitelisted User IP**.

3)   After configuration, click **Save**. The message "Configuration Succeeded" is displayed.

1.3.4 Diagnosis

Click **Diagnosis** to open the level-2 menu, which includes **Network Diagnosis**, One-Click **Collection**, and **Syslog**.

1.3.4.1 Network Diagnosis

1.3.4.1.1 Ping

PING Type

Uses the out-of-band channel. The parameter is supported only on MGMT-supported devices. When a MGMT port is configured as a source port, set the parameter to **Via Management Port**. Otherwise, set it to **Not Via Management Port**.

Dest IP/Domain Name

Indicates the address or domain name to be pinged.

Timeout Interval(s)

Indicates the timeout interval.

Repeat Times

Indicates the number of data packets to be sent.
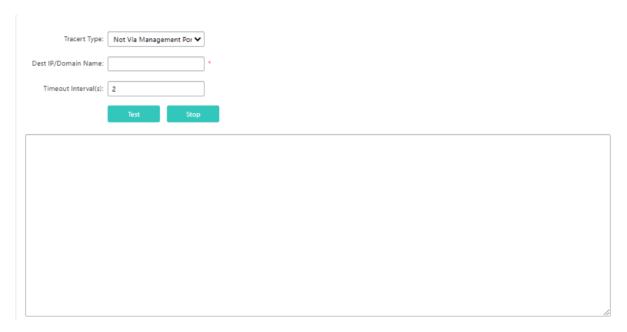
Package Size(Bytes)

Indicates the length of the data padding section in a data packet to be transmitted.

Fragment

Indicates the DF flag bit of an IP address. When the DF flag bit is set to **1**, data packets are not fragmented. The default DF flag bit is **0**.

1.3.4.1.2   Tracert

Tracert Type

Uses the out-of-band channel. The parameter is supported only on MGMT-supported devices. When a MGMT port is configured as a source port, set the parameter to Via Management Port. Otherwise, set it to Not Via Management Port.

Dest IP/Domain Name

Indicates the Tracert destination address or domain name address.

Timeout Interval(s)

Indicates the timeout interval.

1.3.4.2   One-Click Collection
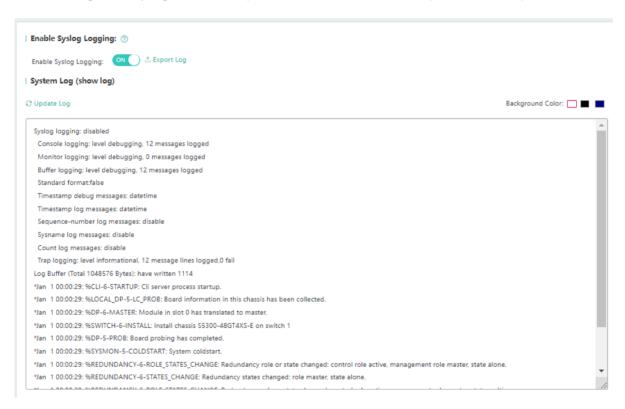
The one-click collection function collects device fault information for troubleshooting.

Note: One-Click Collection is used to collect fault information for troubleshooting.

One-Click Collection

1.3.4.3   Syslog

1.3.4.3.1   Display System Log

You can configure the syslog function to help customers' after-sales and R&D personnel locate problems.

| Enable Syslog Logging: ⑦

Enable Syslog Logging: ON   ⬆ Export Log
| System Log (show log)

⟳ Update Log   Background Color: ☐ ■ ■

```
Syslog logging: disabled
   Console logging: level debugging, 12 messages logged
   Monitor logging: level debugging, 0 messages logged
   Buffer logging: level debugging, 12 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, 12 message lines logged,0 fail
Log Buffer (Total 1048576 Bytes): have written 1114
*Jan  1 00:00:29: %CLI-6-STARTUP: Cli server process startup.
*Jan  1 00:00:29: %LOCAL_DP-5-LC_PROB: Board information in this chassis has been collected.
*Jan  1 00:00:29: %DP-6-MASTER: Module in slot 0 has translated to master.
*Jan  1 00:00:29: %SWITCH-6-INSTALL: Install chassis S5300-48GT4XS-E on switch 1
*Jan  1 00:00:29: %DP-5-PROB: Board probing has completed.
*Jan  1 00:00:29: %SYSMON-5-COLDSTART: System coldstart.
*Jan  1 00:00:29: %REDUNDANCY-6-ROLE_STATES_CHANGE: Redundancy role or state changed: control role active, management role master, state alone.
*Jan  1 00:00:29: %REDUNDANCY-6-STATES_CHANGE: Redundancy states changed: role master, state alone.
```

Click **Enable Syslog Logging** to enable/disable syslog. After syslog is enabled, you can export system logs.

1.3.4.3.2   Monitor System Log

You can query logs by level or module to help customers' after-sales and R&D personnel locate problems.

Severity Level	Module	Mnemonic	Description	Time
(5)Notifications	DEV_MONITOR	CARD_POWER_ON	The power enough, card in slot 0 will be controlled to power on automatically.	1970-01-01 00:00:29
(6)Informational	DP	FAN_OK	Fan 1/1 OK.	1970-01-01 00:00:29
(6)Informational	DP	POWER_OK	Power 1 OK.	1970-01-01 00:00:29
(6)Informational	REDUNDANCY	ROLE_STATES_CHANGE	Redundancy role or state changed: control role active, management role master, state realtime.	1970-01-01 00:00:29
(6)Informational	REDUNDANCY	STATES_CHANGE	Redundancy states changed: role master, state alone.	1970-01-01 00:00:29
(6)Informational	REDUNDANCY	ROLE_STATES_CHANGE	Redundancy role or state changed: control role active, management role master, state alone.	1970-01-01 00:00:29
(5)Notifications	SYSMON	COLDSTART	System coldstart.	1970-01-01 00:00:29
(5)Notifications	DP	PROB	Board probing has completed.	1970-01-01 00:00:29
(6)Informational	SWITCH	INSTALL	Install chassis S5300-48GT4XS-E on switch 1	1970-01-01 00:00:29
(6)Informational	DP	MASTER	Module in slot 0 has translated to master.	1970-01-01 00:00:29

Load More Refresh

1.3.5   Maintenance

1.3.5.1   SWITCH

1.3.5.1.1   Upgrade

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

File Name: [   ] Browse Upgrade Cancel

Click **Browse**, select a local bin file, and then click **Upgrade** to upgrade the device locally.

1.3.5.1.2   Config MGMT

↘   **Backup**

You can back up the configuration file on the device, and import or export configurations to bulk perform operations on the configurations, thereby facilitating user operations.

Backup   Restore   Charset

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

File Name: [   ] Browse Import Export Current Settings

↘   **Restore**

You can clear the configurations to restore the system to the initial state. You need to use the IP address in the factory settings to access the Eweb.

↘ **Charset**

Selected Charset can be set to **GBK**, **UTF-8** or **Default**. You are advised to use **UTF-8** for the Eweb and keep the system character set on SecureCRT or other terminal tools to be consistent with that on the Eweb. Otherwise, garble may occur.

1.3.5.1.3 Systime

You can set the system time of the time zone where the device is located so that the device information is accurate.
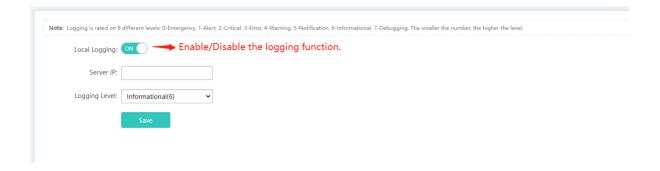
The page displays the current system time. You can set the system time manually or select **Automatically synchronize with an Internet time server**.

Click **Save**. The message "Configuration Succeeded" is displayed, indicating that the operation is completed.

1.3.5.1.4 Syslog

The device can be configured to send local logs to the server for storage for the ease of query.

Set **Server IP** and **Logging Level**. After configuration, the device will send system logs to the server.

1.3.5.1.5   DNS

Domain names can be dynamically parsed only after a DNS server is configured.
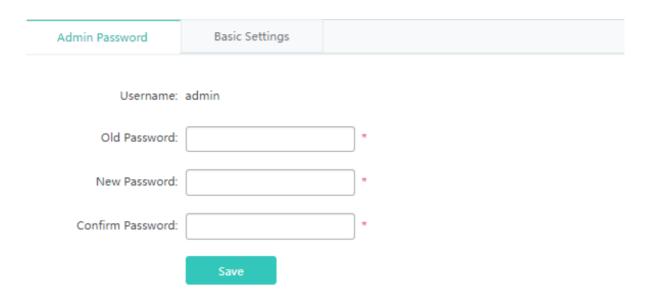

1.3.5.2   System

1.3.5.2.1   Web

↘   **Admin Password**

To enhance the system security and information interaction security, you need to change the default password of the system.
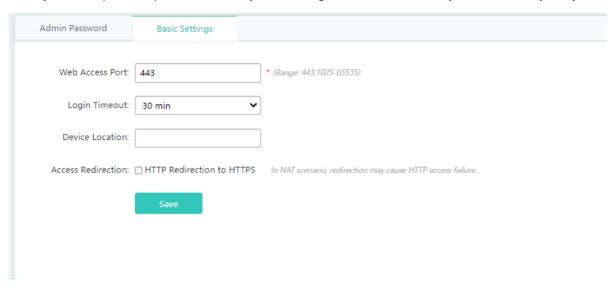
The steps of changing the default password of the system are as follows:

1)   To change a Web user password, enter the old password in **Old Password**, enter the new password in **New Password**, and enter the new password again in **Confirm Password**.

2)   If the entered old password is incorrect, the message "Incorrect old password" in red font is displayed. You are required to enter the correct old password and click **Save** to complete the password change.

ⓘ   The enable password is changed by default when the password of the Eweb is changed.

↘   **Basic Settings**

You can configure the device location to better inspect the device and facilitate device management. Set **Login Timeout**. When you do not perform operations on the system for long, the Eweb automatically exits to ensure your system security.
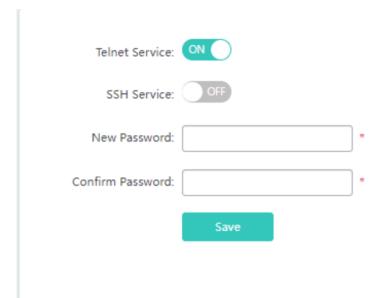
The steps of configuring basic settings are as follows:

1)   Set **Web Access Port**. You need to append the port ID when accessing the Eweb from a browser.

2)   Set **Login Timeout**.

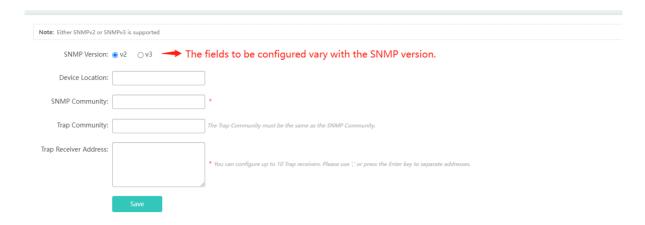3)   Set **Device Location** to facilitate management.

1.3.5.2.2 Telnet

To enhance the system security and information interaction security, you need to configure the Telnet function.

Telnet Service: ON

SSH Service: OFF

New Password: [   ] *

Confirm Password: [   ] *

Save

To change the telnet password, you do not need to enter the old password but need to enter the new password in **New Password** and enter the new password again in **Confirm Password**. Other operations are the same as those of changing the password of the super administrator.

1.3.5.2.3 SNMP

The Simple Network Management Protocol (SNMP) provides a method for collecting network management information from devices on the network. It can be used to manage a large number of network devices.

The steps of configuring SNMP are as follows:

1) Set **Device Location**, **SNMP Community**, **Trap Community**, and **Trap Receiver Address**. The **SNMP Community** and **Trap Receiver Address** fields are required and other fields are optional.

2) After configuration, click **Save**. The message "Configuration Succeeded" is displayed.

1.3.6 Other Functions

1.3.6.1 Favorites

After you add frequently configured functions to favorites, you can click menu items in the favorites and configure the functions rapidly next time.
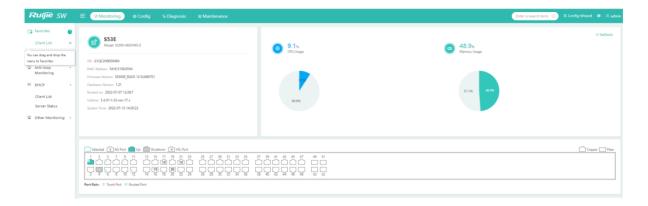
ⓘ Currently, a maximum of 10 menu items can be added to favorites.

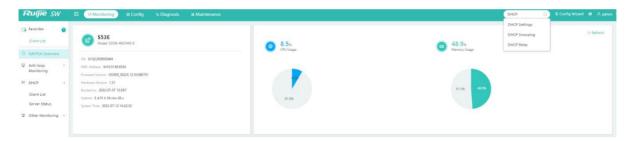● Adding to favorites

Select a menu item and drag it to **Favorites**.

● Canceling favorites

In **Favorites**, select a menu item and click ✕ to remove the menu item from the favorites.
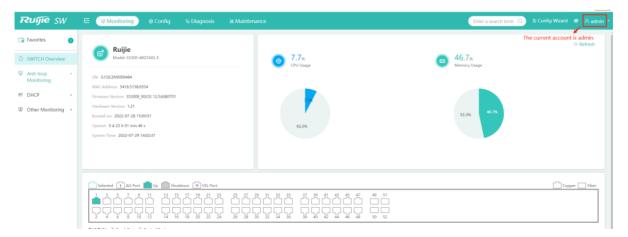
1.3.6.2 Fast Query Menu

There are increasing functions in the system. The fast query menu helps users rapidly search for required functions.
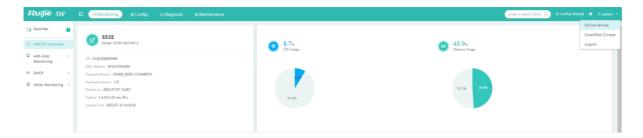

Enter a search condition in the search box. A list of records meeting the search condition are rapidly displayed. Click a function to redirect to the function page.

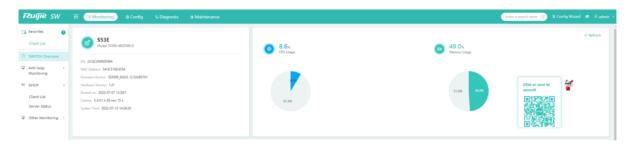### 1.3.6.3 More Functions of the System

● Displaying the current account
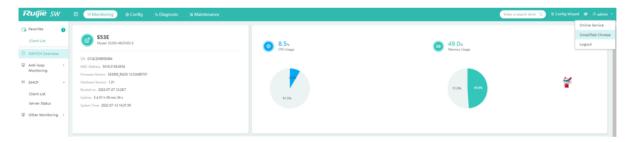
● Online Service

To seek help, click **Online Service**.

Click the RITA icon on the page to redirect to the online customer consulting page or move the cursor over the icon and scan the QR code for access.

● Language switching

Click **Simplified Chinese** to switch to the Chinese version.

The language switching item is displayed based on actual requirements. It is displayed only when both Chinese and English are supported.

● Logging out of the system

Click **Logout** to log out of the system.

1.3.6.4 Help Information

When you are unfamiliar with system functions and need help information, click the cookbook to query required information.

Click to view the cookbook.

1.4 Enabling the Web Server

The Web service is enabled when the switch is delivered. The default IP address is 192.168.1.200. The following describes how to enable the Web service on the CLI.

Configuration	Description and Command	
Configuring the Web Server	**enable service web-server**	Enables the Web service.
	ip address	(Optional) Configures an IP address.
	webmaster level username password	(Optional) Configures the username and password for logging in to the Eweb.

Configuration Steps

↘ **Enabling the Web Service**

● Mandatory.

● Complete the configuration on the switch.

↘ **Configuring an IP Address**

● Optional.

↘ **Configuring the Username and Password for Logging In to the Eweb**

● Optional.

● When the Web service is enabled, the administrator account/password (**admin**/**admin**) are created by default. The account and password can be changed. Users can also create other Eweb accounts.

Verification

Log in to the Eweb by using the configured IP address, Eweb account, and password to check whether the login is successful.

Related Commands

➘ Enabling the Web Service

Command	enable service web-server [http	https	all]
Parameter Description	http	https	all: Enables a service. **Http** enables the HTTP service, **https** enables the HTTPS service, and **all** enables both HTTP and HTTPS services. Both HTTP and HTTPS services are enabled by default.
Command Mode	Global configuration mode

➘ Configuring an IP Address

Command	**ip address** *ip-address ip-mask*
Parameter Description	*ip-address*: IP address. *ip-mask:* Network mask.
Command Mode	Interface configuration mode

➘ Configuring the Username and Password for Logging In to the Eweb

Command	**webmaster level** *privilege-level* **username** *name* **password** { *password*	[**0**	**7**] *encrypted-passw*
Parameter Description	*privilege-level*: User binding permission level, which includes level 0, level 1, and level 2. The default super administrator account (**admin**) has level 0 permissions and other accounts created manually have level 1 permissions. *name*: Username. *password*: Password text. **0	7:** Indicates the password encryption type. **0** indicates no encryption, and **7** indicates simple encryption. The default value is **0**. *encrypted-password:* Encrypted password text.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

➘ Configuring the Web Server

Configuration Steps	● Enable the Web service. ● Configure a management IP address for the device. The default management VLAN is VLAN 1. Configure an IP address for VLAN 1 and ensure that users can ping the management IP address successfully from their PCs.
| | ```
Hostname> enable

Hostname# configure terminal

Hostname(config)#enable service web-server
``` |

| | ```
Hostname(config)# webmaster level 0 username test password test

Hostname(config)#interface vlan 1

Hostname(config-if-VLAN 1)#ip address 192.168.1.200 255.255.255.0

Hostname(config)# end
``` |
| | |
| **Verification** | Run the **show running-config** command to display related commands. |
| | ```
Hostname(config)#show running-config

Building configuration...

Current configuration : 6312 bytes

!

hostname ruijie

!

!

webmaster level 0 username test password test   //Username and password for Eweb
``` authentication. The displayed password is encrypted. ```
http update mode auto-detect

!

!

interface VLAN 1

 ip address 192.168.1.200 255.255.255.0   //Management IP address of
``` the device ```
 no shutdown

!

line con 0

line vty 0 4

 login

!

!

End
``` |