Ruijie XS-S1920 Series Switches

Web-Based Configuration Guide, Release 11.4(1)B41P2

Copyright Statement

Exemption Statement

Preface

Thank you for using our products. This manual matches the RGOS Release 11.4(1)B41P2.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: http://caseportal.ruijienetworks.com
- Community: http://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description

boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Symbols

Means reader take note. Notes contain helpful suggestions or references.

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

1 Web-Based Configuration

1.1 Overview

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

Currently, this file is applicable to only switches.

1.2 Application

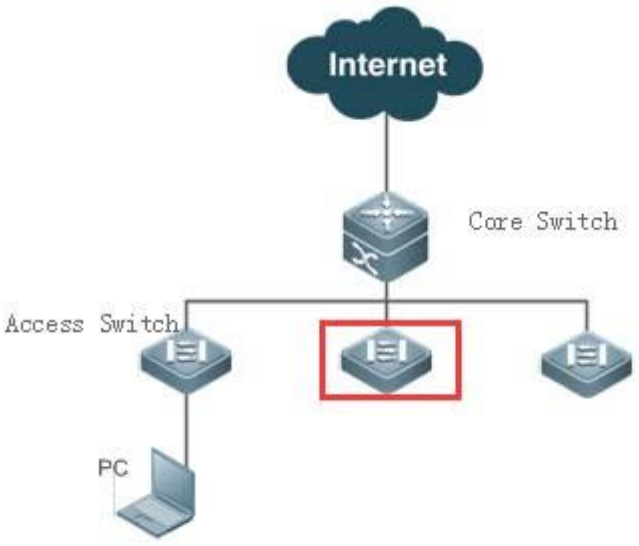
Application	Description
Web-based Management	After finishing relevant configuration, a user can access the web-based management system through a browser.

1.2.1 Web-based Management

Scenario

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

Figure 1-1



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

Function Deployment

Configuration Environment Requirements

Requirements for Client

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

Server Requirements

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

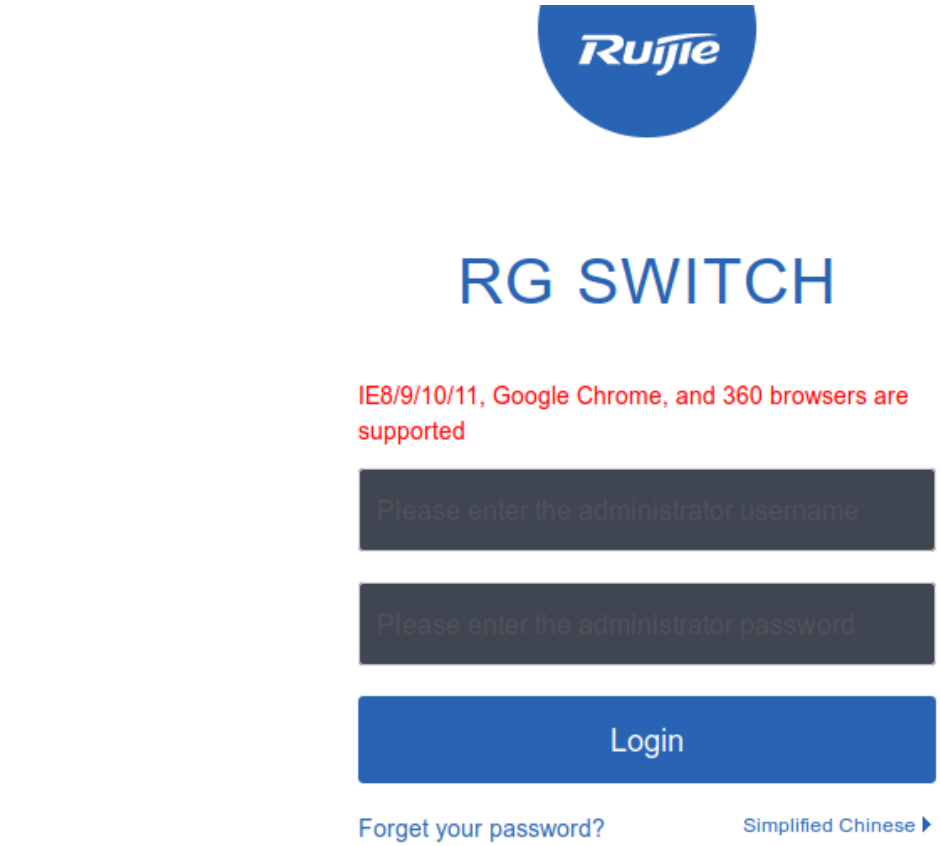
For the detailed configuration of the switch on the command line interface (CLI), see Configuring Web Server.

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

Login

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

Figure 1-2 Login Page



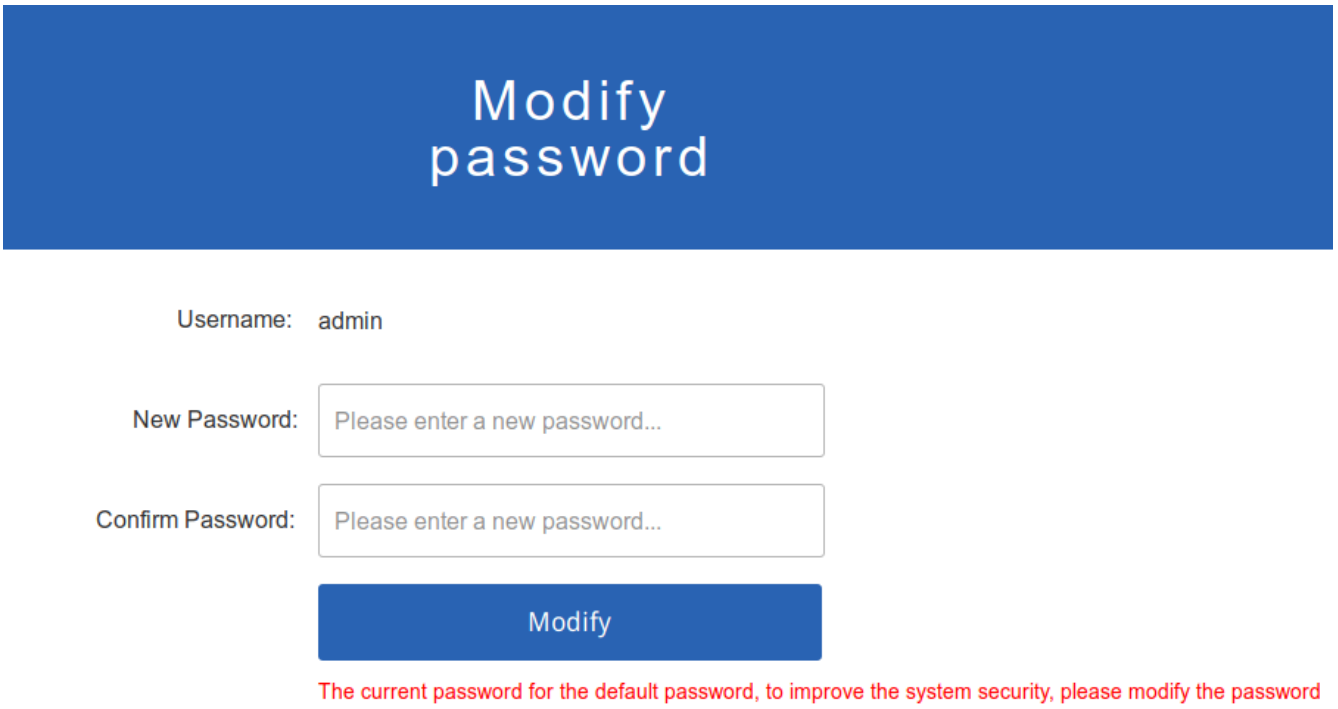
After typing the username and password, click Login. The following table lists the default username and password.

Default Username/Password	Permission Description

admin / admin	Super administrator possessing all permissions.

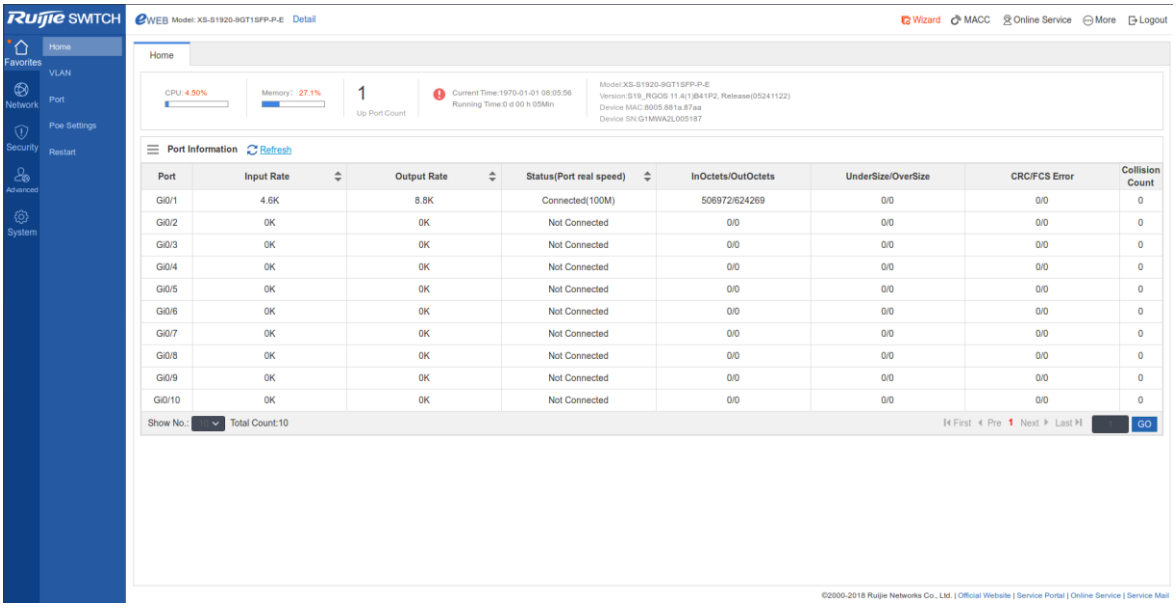
The default username and password are not displayed by running the **show running-config** command.

You will be required to modify the password if logging in with the default username and password.



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

Figure 1-3 Home Page



For details on the web page, see Web Management System below.

1.3 Web Management System

Basic Concepts

Various Icons and Buttons on the GUI

Icon/Button	Note
Edit	Edit button. Click this icon to edit the currently selected item.
Delete	Delete button.
ON	Status icon.
	Port available for selection. After you click or select this port, it becomes a selected port.
	Port not available for selection.
	Selected port.
1	Aggregate port. The number in the port indicates the aggregate port number.
	Trunk port. This port is displayed on the panel on the VLAN Management/VLAN Settings page.
Save	Save button. Click this button to submit and save the input information.
+	Add setting.
×	Delete setting.
All Invert Deselect	Batch processing operations on panel ports. These icons are located on the lower right of the panel. These icons are available only on the panel where selecting multiple ports is allowed.
*	If this mark is displayed behind a text box, the item corresponding to the text box is mandatory.
	Note.
	Warning.

System Operations

- Standalone Device Panel

- Panel Operations

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

- Selected Ports

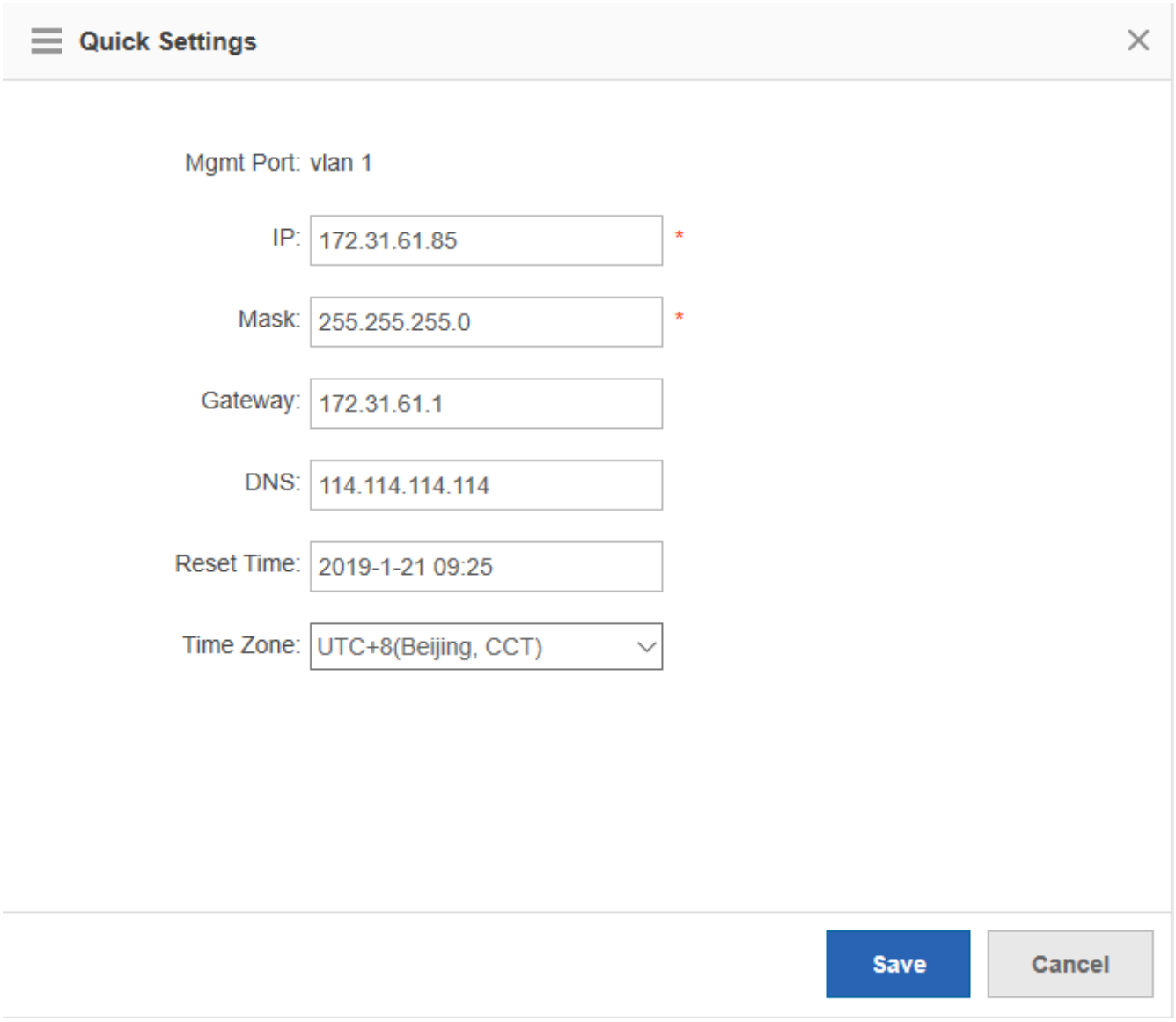
Features

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

Feature	Description
Home Page	For viewing port information and device configuration.
VLAN	Used to set the VLAN and Trunk ports.
Port	Used to perform basic settings on a port and configure port aggregation, port mirroring, and port rate limiting.
PoE Settings	Used to configure PoE on the port or globally.
Restart	For restarting the device.
MAC Address	For configuring the static address and filtering address.
STP	Used to configure basic STP information, STP ports and RLDP.
DHCP Snooping	Used to configure DHCP Snooping.
Anti-ARP-Attack	Used to perform anti-ARP-spoofing settings, ARP check settings, DAI settings, and ARP entry settings.
Storm Control	Used to perform storm control.
Port Security	Used to perform basic settings and security binding.
Port Protection	Used to configure port protection.
ACL	Used to set the ACL list and ACL time and apply ACL.
System Settings	Used to set the system time, modify passwords, restart the system, restore to default factory settings, configure enhanced functions, and set the SNMP and DNS.
System Upgrade	Used to perform local upgrade and online upgrade.
Administrator Permissions	Used to set the administrator permissions.
System Logging	Used to configure the log server and view system logs.
Network Detection	Used to configure ping, Traceroute (tracert.exe), cable detection and one-click collection.
Web CLI	Used to simulate CLI.

1.3.1 Quick Settings

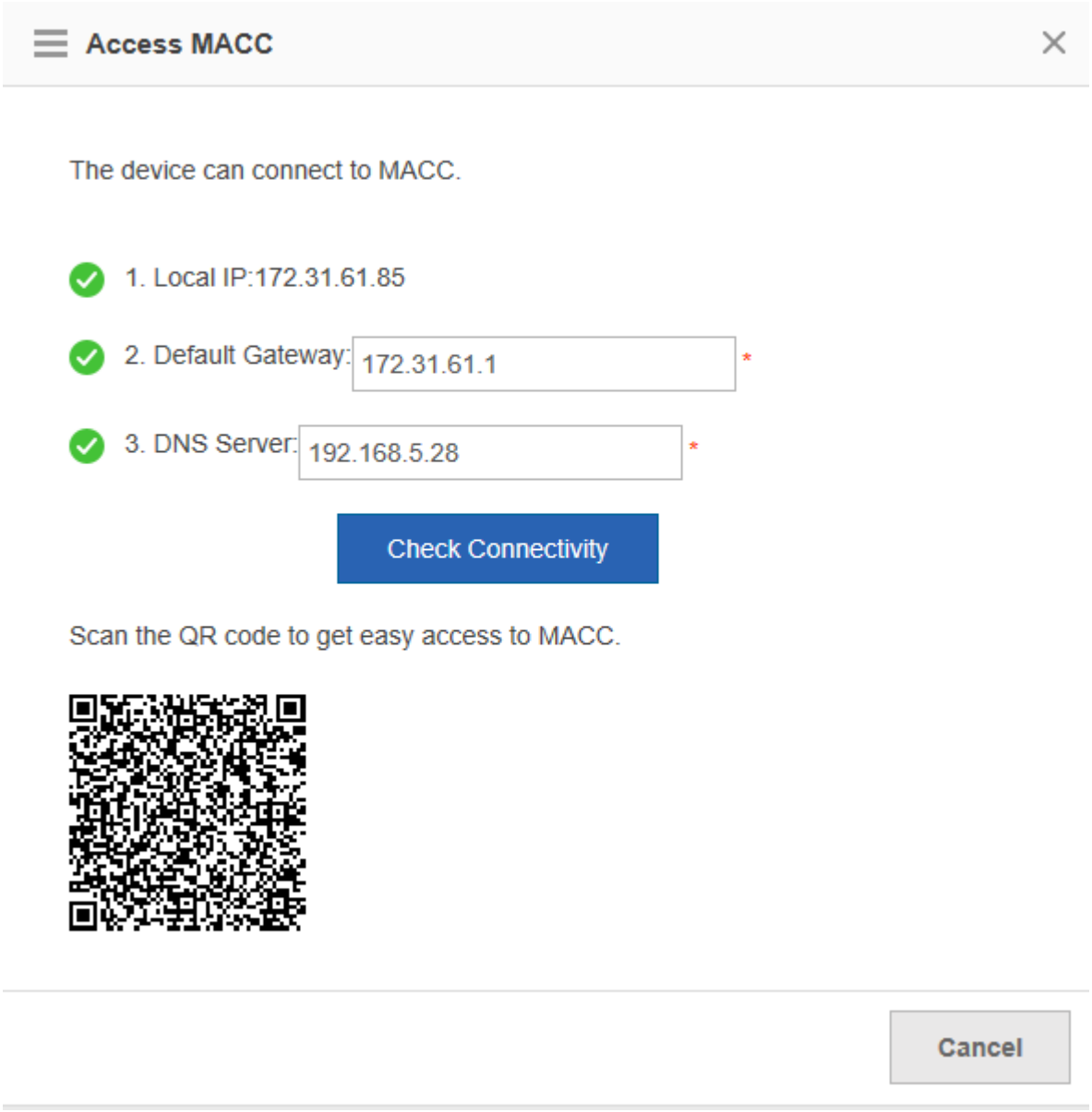
Figure 1-4 Quick Settings



Select the management port mode, configure the VLAN ID, IP address, subnet mask, default gateway, and DNS server, and click **Save**. If the message ”Configuration succeeded.” is displayed, the operation is successful.

1.3.2 MACC Management

Figure 1-5 MACC Management



To check whether the device can connect to MACC, enter the local IP, default gateway and DNS server, and click **Check Connectivity**. After establishing the connection, you can scan the QR code to add devices to MACC.

1.3.3 Favorites

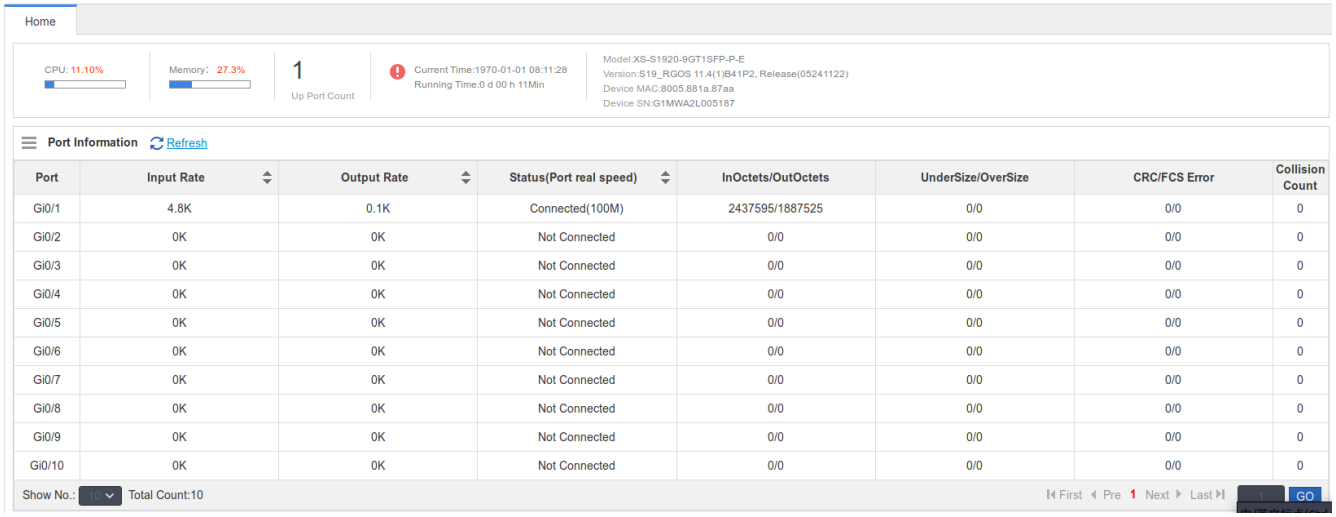
You can access secondary menus through the primary menu Favorites, including Home page, VLAN, Port and Restart.

1.3.3.1 Home Page

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

The following figure shows the home page.

Figure 1-6 Home Page

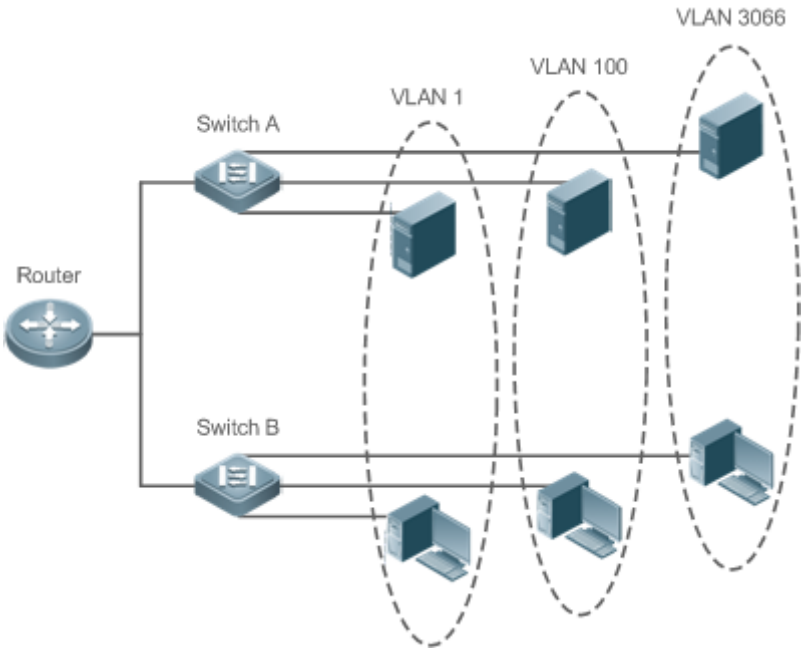


1.3.3.2 VLAN

A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer-2 networks of the OSI model.

A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

We may define a port as a member of a VLAN, and all terminals connected to this port are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing and modifying users. Communication among VLANs is realized through Layer-3 devices, as shown in the following figure.



The VLANs supported by Ruijie products comply with the IEEE802.1Q standard. A maximum of 4094 VLANs (VLAN ID 1-4094) are supported, among which VLAN 1 cannot be deleted.

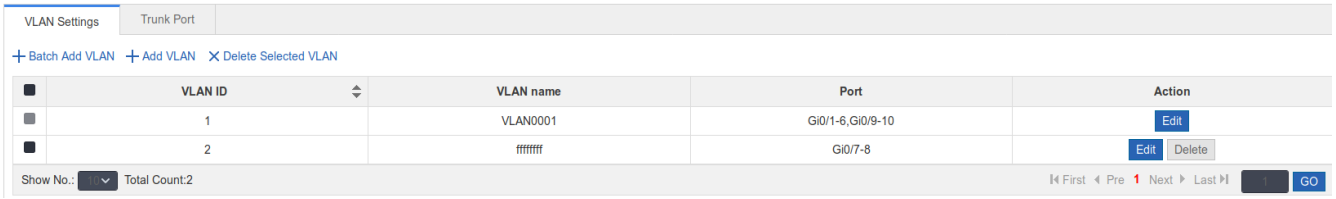
A trunk port can belong to multiple VLANs that receives and sends frames belonging to multiple VLANs. Generally, it is used to connect devices or computers.

Two tab pages are available on the VLAN page: VLAN Settings and Trunk Port.

VLAN Settings

The following figure shows the VLAN Settings page.

Figure 1-7 VLAN Settings



- Adding VLAN

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

- Editing a VLAN

After clicking **Edit** in the Action column, information from the corresponding VLAN is displayed on the page. After editing the information, click **Save**. The ”Edit succeeded.” message is then displayed.

- Deleting a VLAN

1) Select multiple VLANs from the VLAN list and click **Delete Selected VLAN** to delete the VLANs in batches.

2) Click **Delete** in the **Action** column, the message, “Are you sure you want to delete the VLAN?” is then displayed.

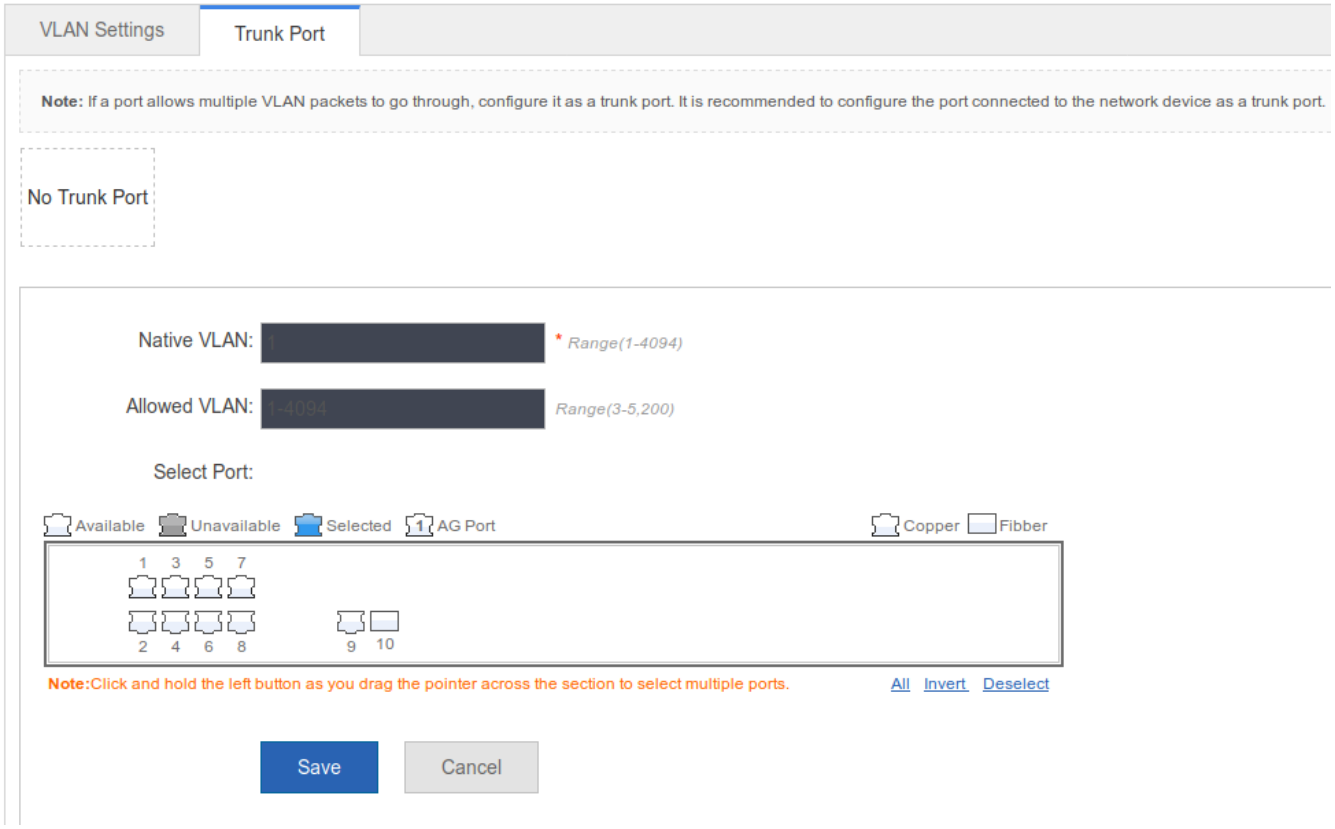
After confirming the operation, the message, “Delete succeeded.” is displayed. VLAN 1 is the default VLAN and cannot be deleted.

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

Trunk Port

The following figure shows the Trunk Port page.

Figure 1-8 Trunk Port



- Adding a trunk port

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

- Editing a trunk port

Click a certain trunk port in the trunk port list, and the information of this trunk port is displayed on the page. After editing the information, click **Edit**. The ”Configuration succeeded.” message is displayed.

- Deleting trunk port

After moving the cursor to a specific trunk port in the trunk port list click **Delete**. The message, ”Are you sure you want to delete the trunk port?” is then displayed.

After confirming the operation, a ”Delete succeeded.” message is displayed.

- Deleting trunk ports in batches

After selecting the trunk ports to be deleted (in the trunk port list) click **Batch Del**. The message, ”Are you sure you want to delete the trunk ports?” is displayed.

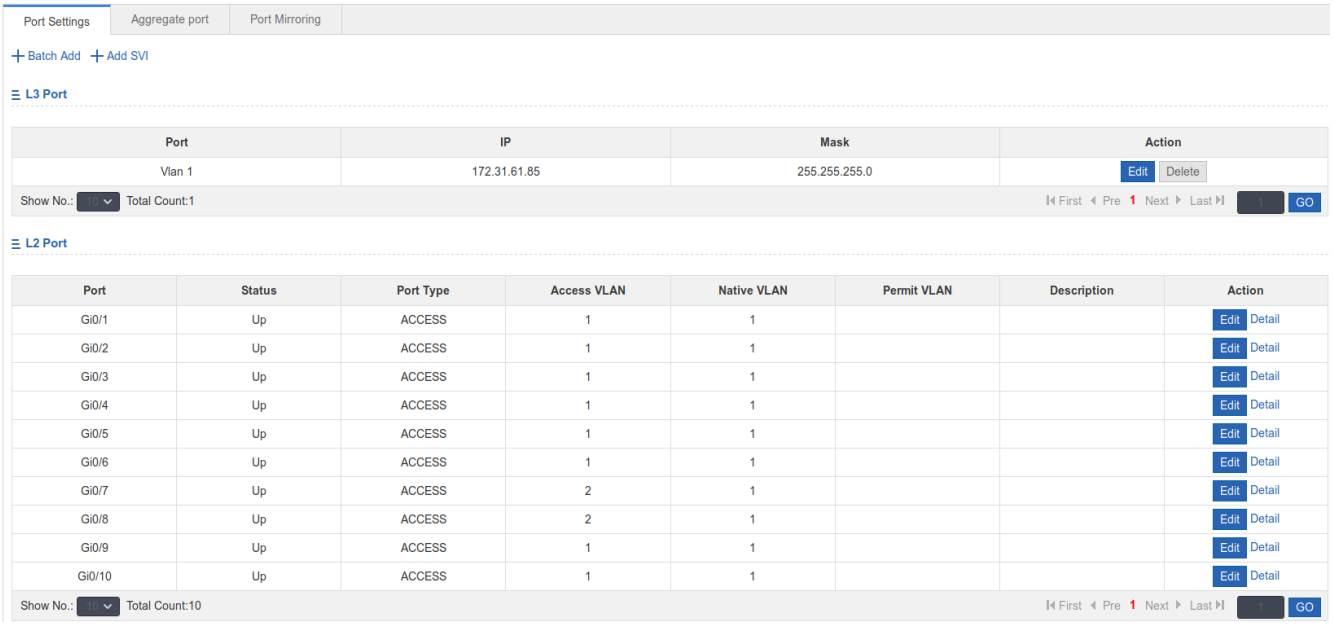
After confirming the operation, a ”Delete succeeded.” message is displayed.

1.3.3.3 Port

A port is a physical entity that is used for connections on the network devices.

Port Settings

Figure 1-9 Port Settings



- Basic port settings

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

- Editing port

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

- Adding SVI port

Click **Add SVI**, enter the VLAN ID, IP address and subnet mask, and click **Save**. A “Configuration succeeded.” message is displayed.

- Detail

Click **Detail** in the **Action** column of **L2 Port** list to check the information of a port, including **Port Status, Speed Settings, Actual Speed, Work Mode, Actual Work Mode** and **Medium**.

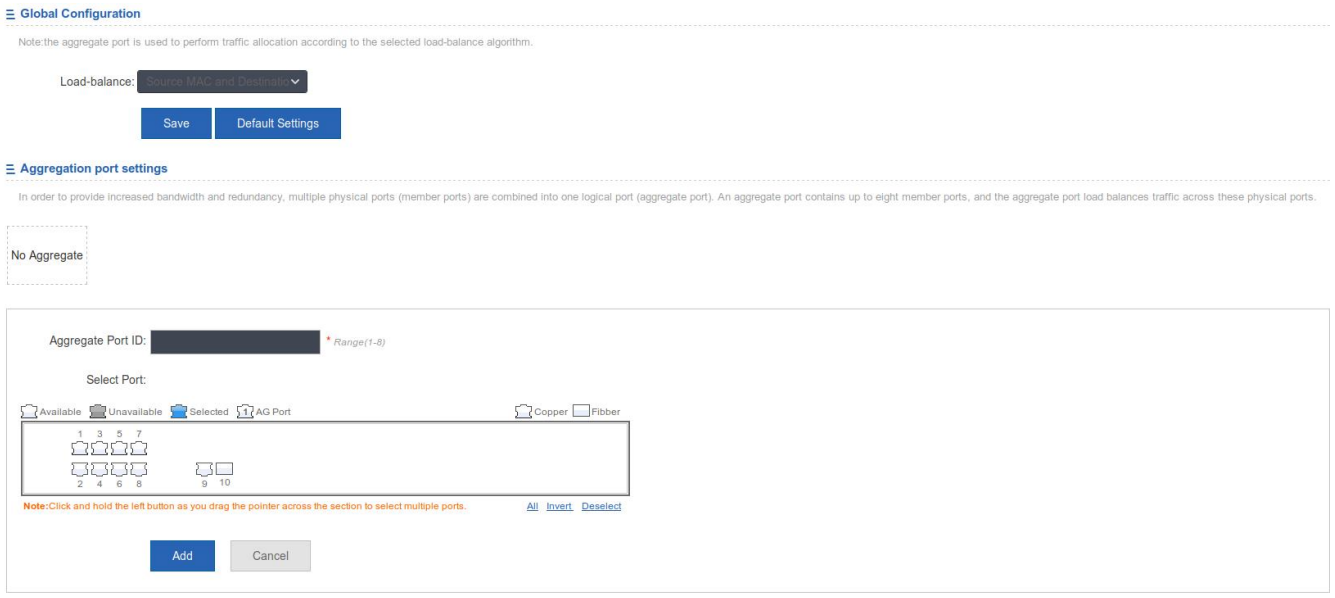
- Deleting L3 port

Click **Delete** in the **Action** column of **L3 Port** list, and click **OK** in the confirmation window.

Aggregate Port

The following figure shows the Aggregate port page.

Figure1-10 Aggregate Port



- Adding aggregate port

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

- Editing an aggregate port

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

- Deleting an aggregate port

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

- Deleting aggregate ports in batches

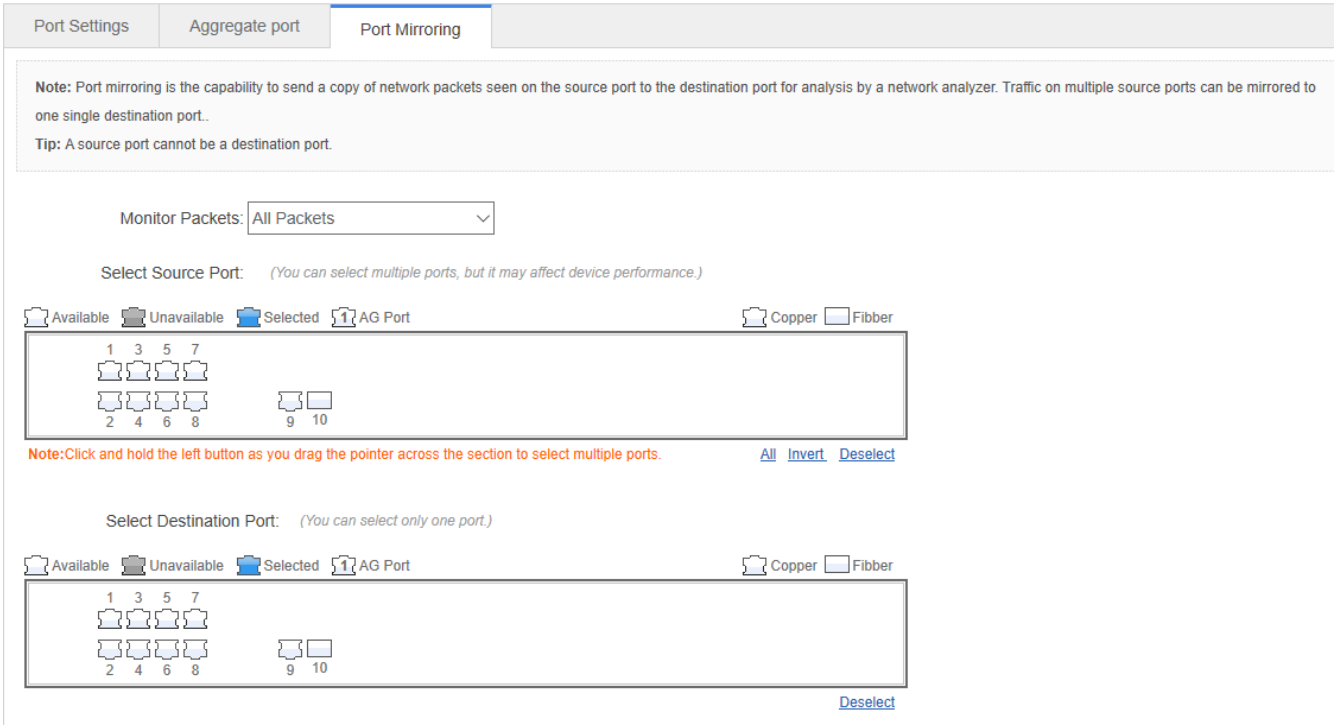
After you select the aggregate ports to be deleted in the aggregate port list and click **Batch Del**, an “Are you sure you want to delete the aggregate port?” message is displayed. After you confirm the operation, these aggregate ports become available ports on the panel.

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

Port Mirroring

The following figure shows the Port Mirroring page.

Figure 1-11 Port Mirroring



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

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

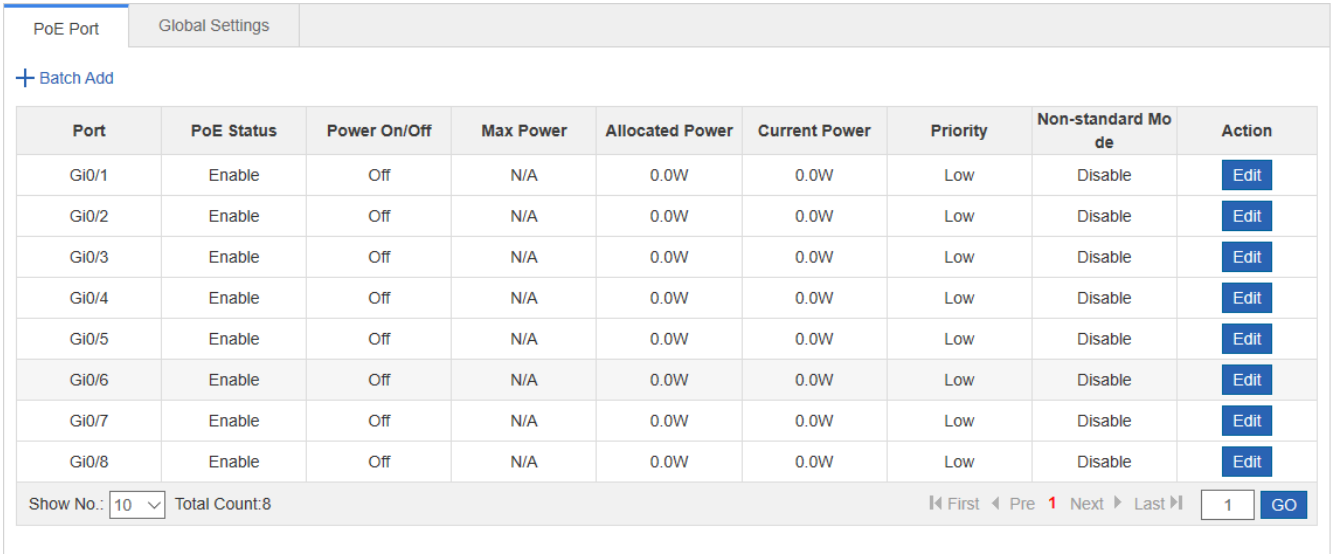
The member port of the aggregate port cannot serve as a destination or source port. A port cannot serve as a destination port and source port at the same time.

1.3.3.4 PoE Settings

You can configure PoE on the port or globally.

PoE Port

Figure 1-6 PoE Port



- Batch adding port

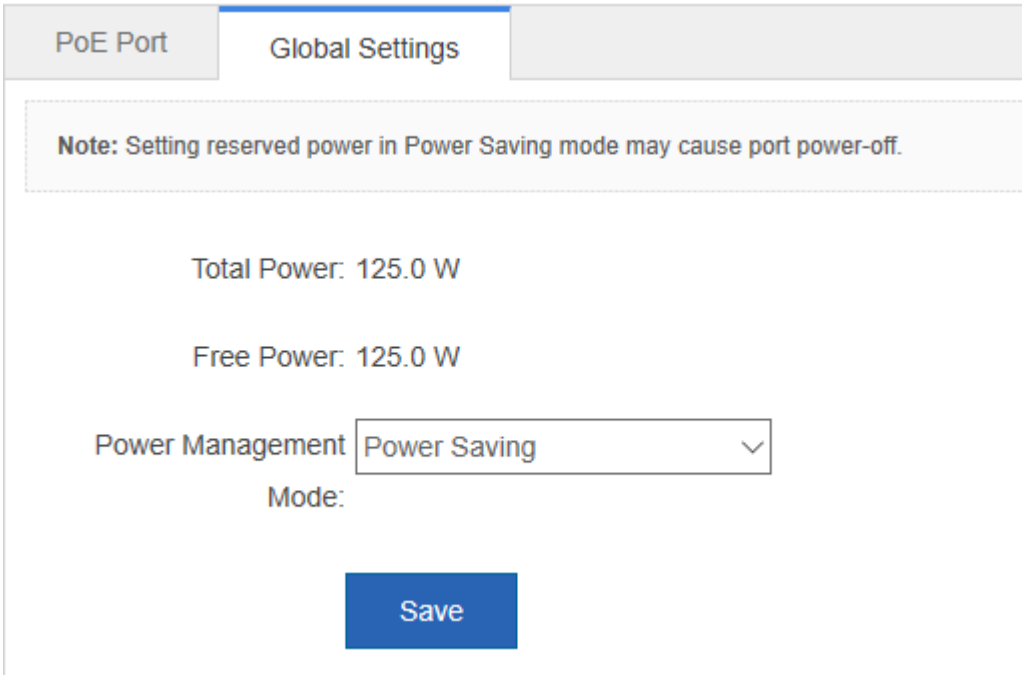
Select multiple ports, configure the **PoE Status, Priority, Max Power, Allocated Power** and **Non-standard Mode**, and click **Save**.

- Editing port

Click **Edit** in the **Action** column to edit the configuration of a port, and click **Save**.

Global Settings

Figure 1-7 Global Settings

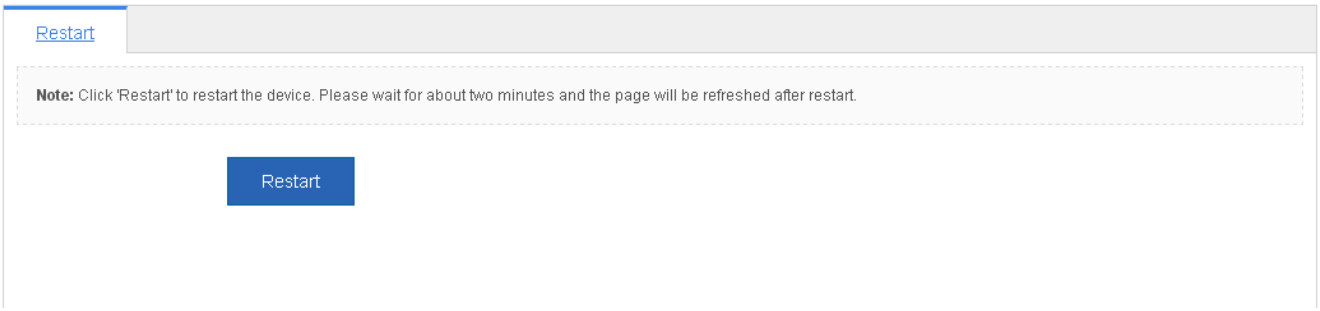


The page displays the total power, free power and power management mode of the device. Select the **Power Management Mode**, and click **Save**.

1.3.3.5 Restart

The following figure shows the Restart page.

Figure 1-14 Restart



After clicking **Restart,** the message, “Are you sure you want to restart the device?” is displayed.

After confirming the operation, the device is restarted. Restart takes several minutes. Please be patient. The page is refreshed automatically after the device is restarted.

1.3.4 Network

Secondary menus can be accessed through the primary menu Network, including MAC Address and STP.

1.3.4.1 MAC Address

A media access control address (MAC address) of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi. Logically, MAC addresses are used in the media access control protocol sub-layer of the OSI reference model.

A static address is a manually configured MAC address. A static address is the same as a dynamic address in terms of function. However, you can only manually add and delete a static address rather than learn and age out a static address. A static address is stored in the configuration file and will not be lost even if the device restarts.

By configuring the static address manually, you can bind the MAC address for the network device with the interface in the MAC address table.

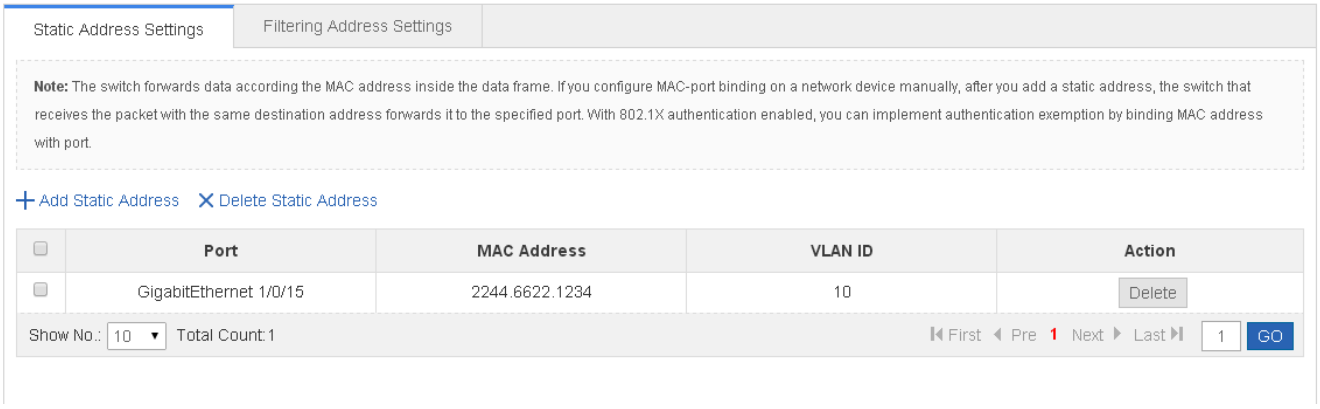
A filtering address is a manually configured MAC address. When a device receives the packets from a filtering address, it will directly discard them. You can only manually add and delete a filtering address rather than age it out. A filtering address is stored in the configuration file and will not be lost even if the device restarts.

If you want the device to filter some invalid users, you can specify their source MAC addresses as filtering addresses. Consequently, these invalid users cannot communicate with outside through the device.

Two tab pages are available on the MAC Address page: Static Address Settings and Filtering Address Settings.

Static Address Settings

Figure 1-15 Static Address Settings



- Adding Static Addresses

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

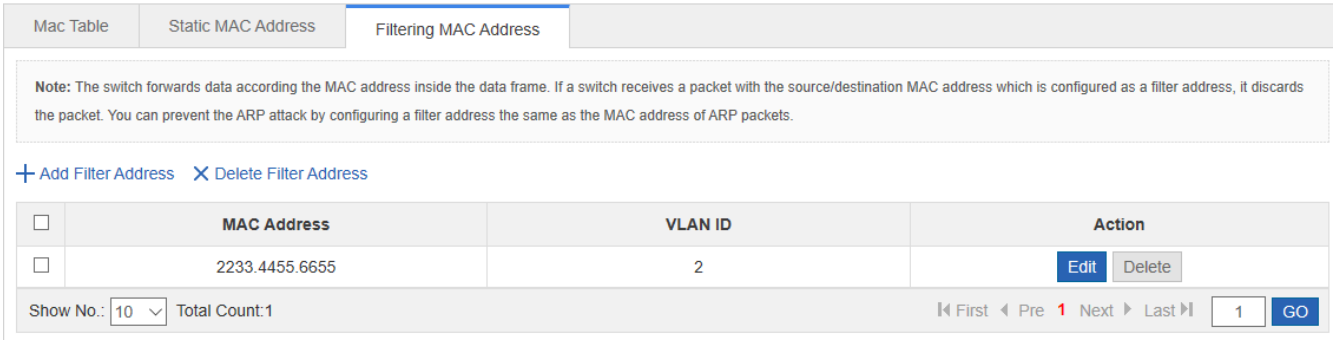
- Deleting Static Address

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

2) After clicking **Delete** in the Action column, the message, “Are you sure you want to delete the static address?” is displayed. After confirming the operation, a ”Delete succeeded.” message is displayed.

Filtering Address Settings

Figure 1-16 Filtering Address Settings



- Adding Filtering Address

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

- Editing Filtering Address

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

- Deleting Filtering Address

1) You can select multiple filtering addresses and click **Delete Filter Address** to batch delete addresses.

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

1.3.4.2 STP

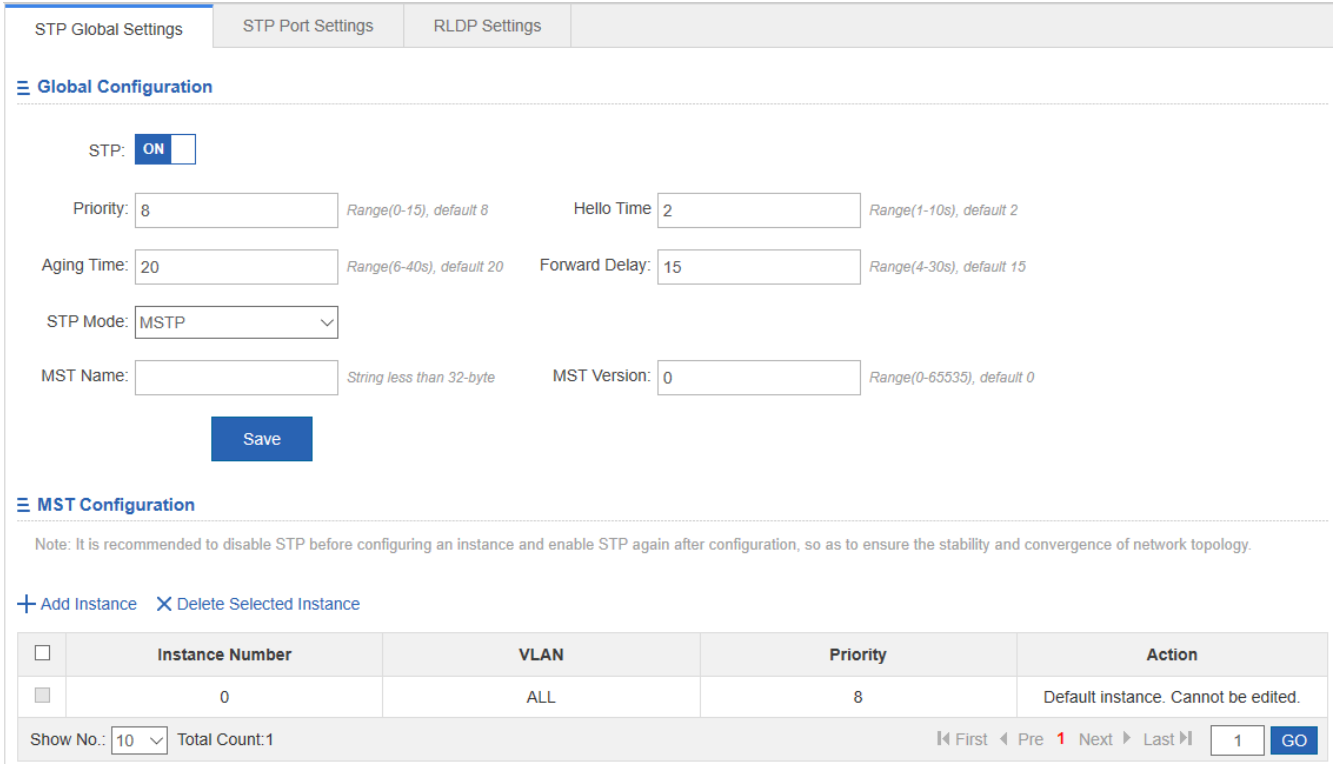
The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths, if an active link fails. This is done without the danger of bridge loops, or the need for manual enabling or disabling of these backup links.

The Rapid Link Detection Protocol (RLDP) achieves rapid detection of unidirectional link failures, directional forwarding failures and downlink loop failures of an Ethernet. When a failure is found, relevant ports will be closed automatically according to failure treatment configuration or the user will be notified to manually close the ports to avoid wrong flow forwarding or an Ethernet layer-2 loop.

The STP Global Settings page enables setting the global parameters and STP ports.

STP Global Settings

Figure 1-17 STP Global Settings



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

- Adding instances

To add an instance, input the instance value and VLAN range and input other information as required. Afterwards, click **Save**. The newly added instance is displayed in the instance list after a “Configuration succeeded.” message is displayed.

- Editing instances

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

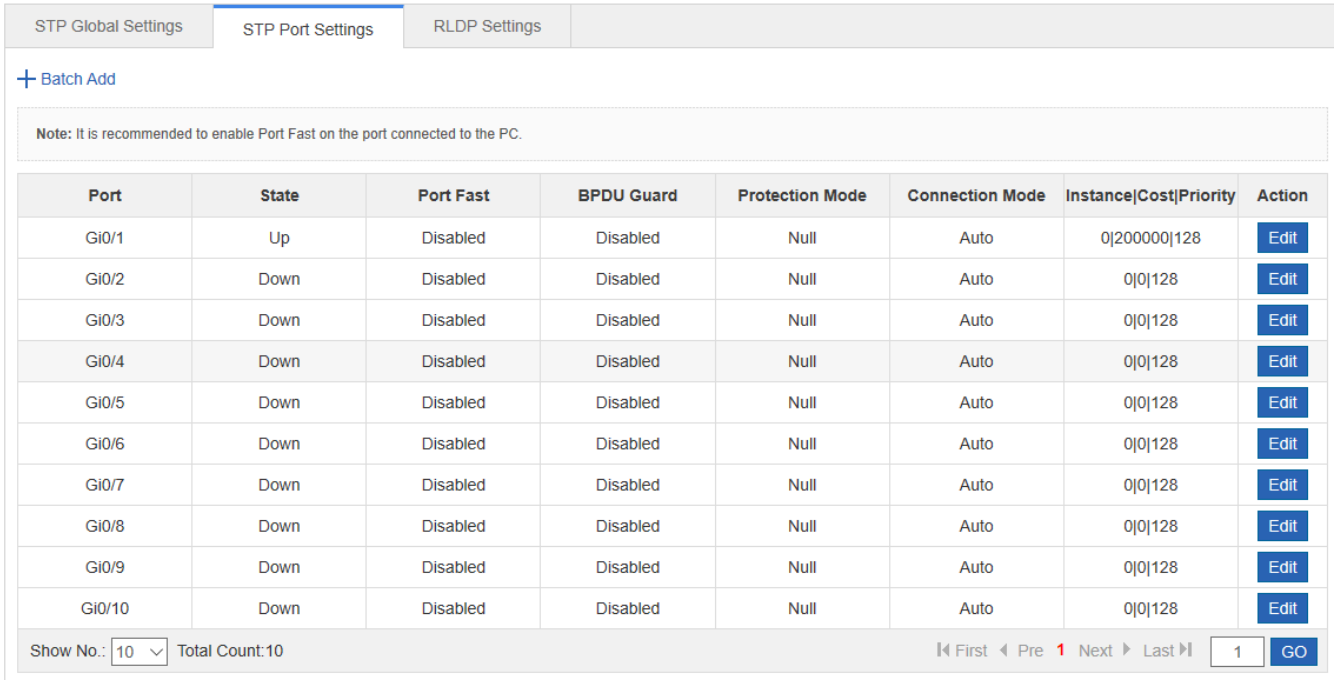
- Deleting instances

1) Multiple instances can be selected from the instance list. Click **Delete Selected Instance** to batch delete instances.

2) After clicking **Delete** in the **Action** column, the message, ”Are you sure you want to delete the instance?” is displayed. After confirming the operation, he ”Delete succeeded.” message is displayed. Instance 0 is the default instance and cannot be deleted.

STP Port Settings

Figure 1-18 STP Port Settings



- Batch setting

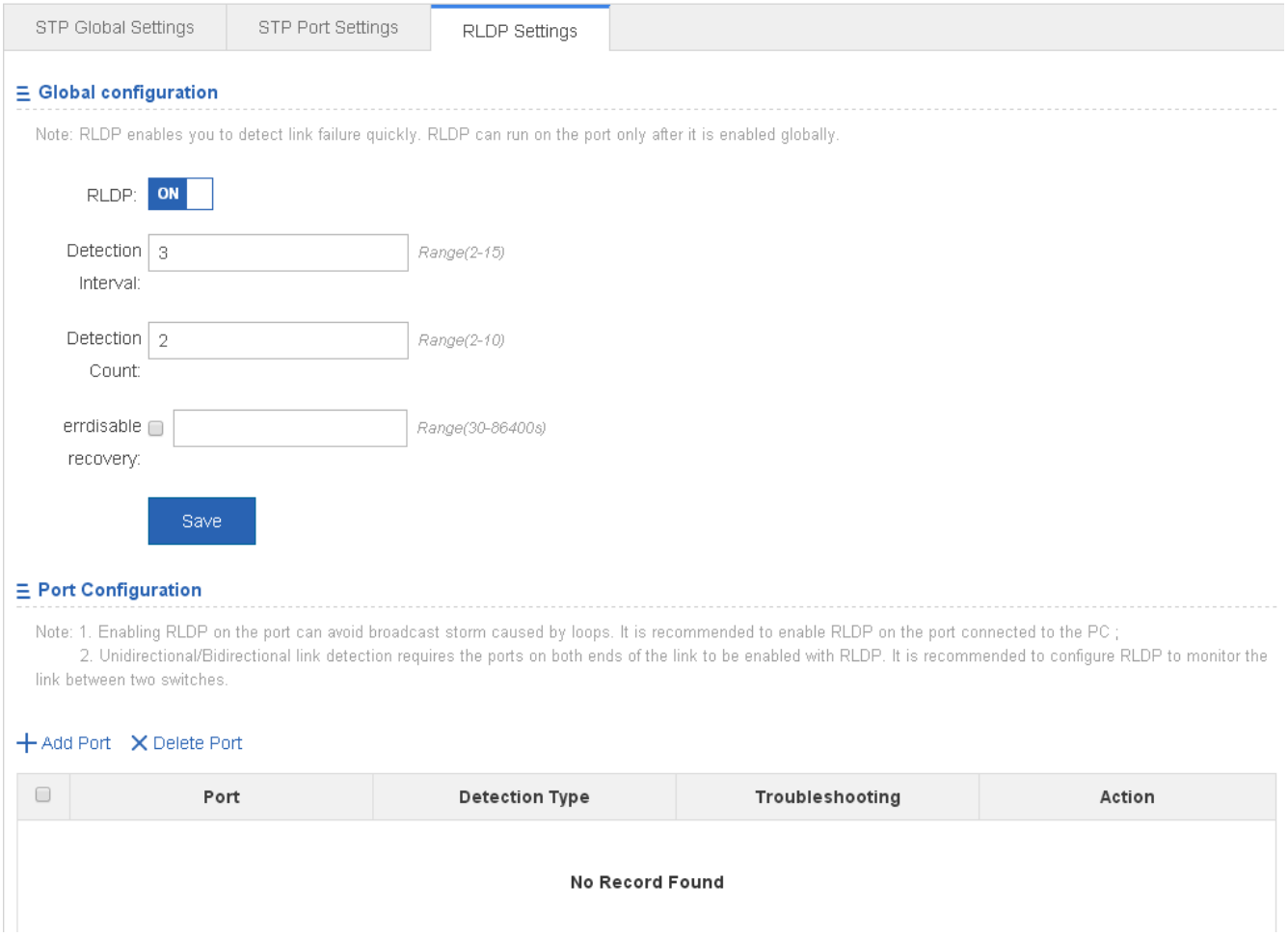
Specify Protection Mode, Port Fast, BPDU Guard, Connection Mode, and Port Priority. Then select ports for batch setting.

- Editing STP ports

After clicking **Edit** in the **Action** column, the information of the corresponding port is displayed on the page. After editing the information, click **Save**. The message, “Configuration succeeded” is displayed.

RLDP Settings

Figure 1-19 RLDP Settings



1. Global Configuration

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

2. Port Configuration

- Adding RLDP Ports

Select detection mode, troubleshooting mode and port. Afterwards, click **Save**. The newly added RLDP port is displayed in the RLDP port list after the message, “Configuration succeeded.” is displayed.

- Editing RLDP Ports

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

- Deleting RLDP Port

1) Multiple RLDP ports can be selected from the RLDP port list. Click **Delete Selected Port** to batch delete RLDP ports.

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

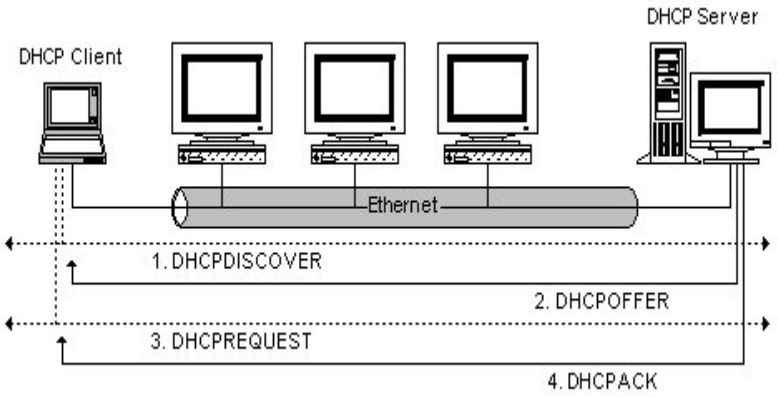
After confirming the operation, the ”Delete succeeded.” message is displayed.

1.3.5 Security

Secondary menus are accessed through the primary Security menu that includes DHCP Snooping, Anti-ARP-Attack, IP Source Guard, Port Security, NFPP, and Storm Control.

1.3.5.1 DHCP Snooping

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP Snooping records may serve security applications like IP Source Guard.



Request packets are sent from a DHCP client to a DHCP server, including DHCP-DISCOVER packets, DHCP-REQUEST packets, DHCP-DECLINE packets, DHCP-RELEASE packets and DHCP-INFORM packets.

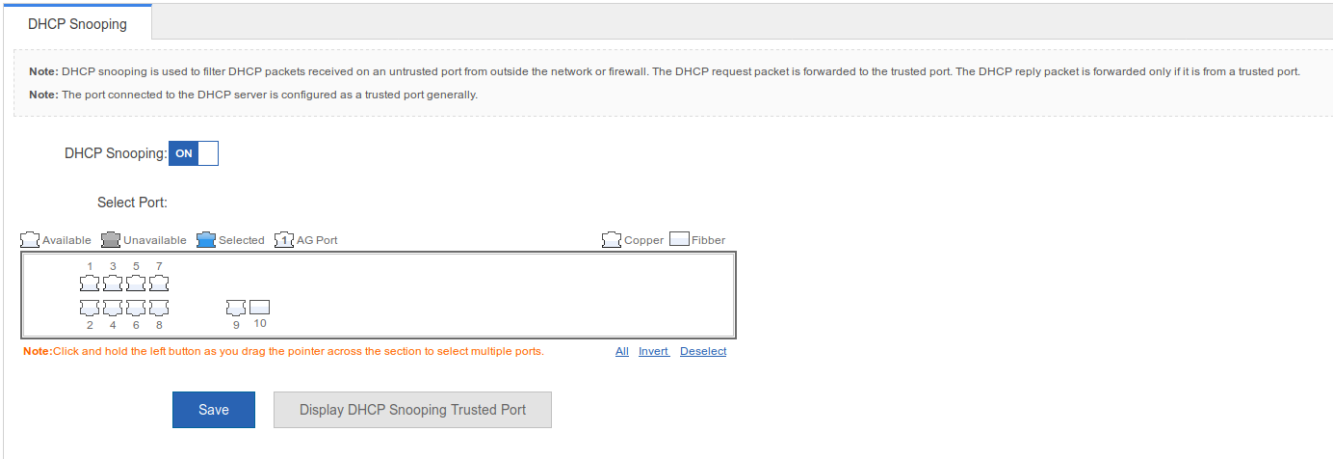
Response packets are sent from a DHCP server to a DHCP client, including DHCP-OFFER packets, DHCP-ACK packets and DHCP-NAK packets.

IP address request interaction is complete via broadcast. Therefore, illegal DHCP services will influence normal clients' acquisition of IP addresses and lead to service spoofing and stealing. To prevent illegal DHCP services, DHCP Snooping ports are divided into two types: trusted ports and untrusted ports. The access devices only transmit DHCP response packets received on trusted ports, while such packets from untrusted ports are discarded. In this way, we may configure the ports connected to a legal DHCP Server as trusted and the other ports as untrusted to shield illegal DHCP Servers.

On switches, all switching ports or layer-2 aggregate ports are defaulted as untrusted, while trusted ports can be specified.

The following figure shows the DHCP Snooping Settings page.

Figure 1-20 DHCP Snooping Settings



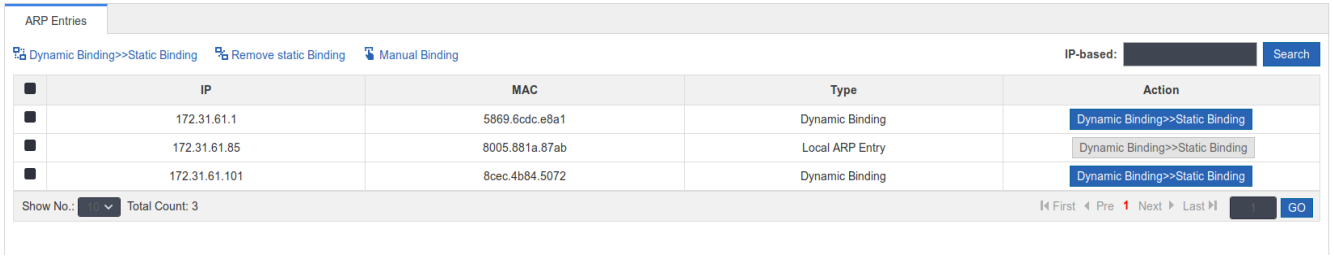
The port connected to the DHCP server must be configured as a DHCP trusted port. The DHCP server connected to a non-trusted port cannot work properly. If the selected port on the panel is a DHCP trusted port, a port can be directly selected on the panel, then click the **Save** button.

1.3.5.2 Anti-ARP-Attack

You can check ARP entries and bind static addresses.

ARP Entries

Figure 1-8 ARP Entries



- Dynamic Binding > Static Binding

1) Select multiple entries, and click **Dynamic Binding >> Static Binding** above the list.

2) Click **Dynamic Binding >> Static Binding** in the **Action** Column.

- Remove Static Binding

1) Select multiple entries, and click **Remove Static Binding** above the list.

2) Click **Remove Static Binding** in the **Action** Column.

- Manual Binding

Click **Manual Binding** above the list, enter IP and MAC addresses, and click **OK**. The entry is displayed in the list.

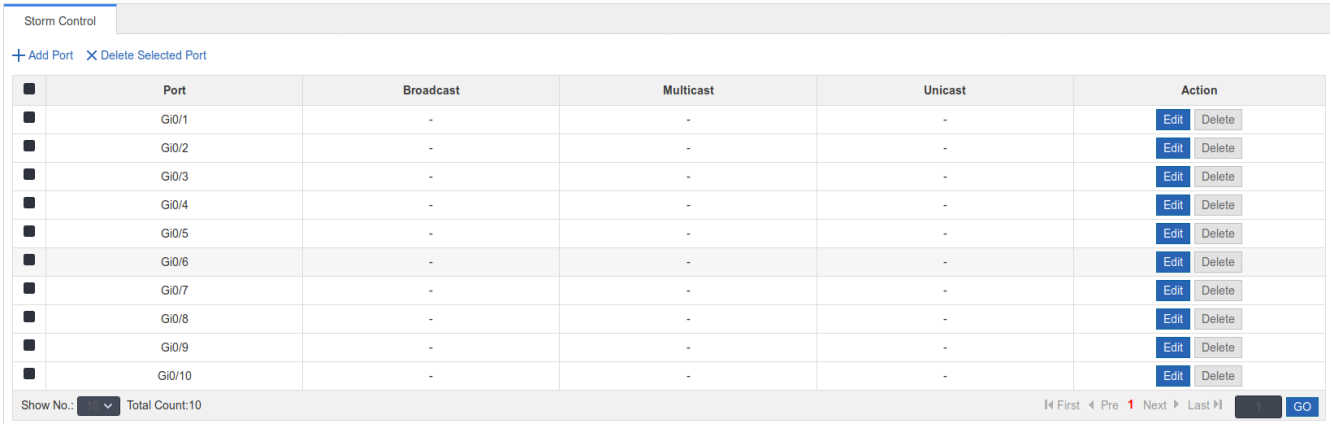
1.3.5.3 Storm Control

When a local area network (LAN) has excess broadcast data flows, multicast data flows, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This situation is called a LAN storm. A storm may occur when topology protocol execution or network configuration is incorrect.

Storm control can be implemented to limit broadcast data flows, multicast data flows, or unknown unicast data flows. If the rate of data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds. This prevents flood data from entering the LAN causing a storm.

The following figure shows the Storm Control Settings page.

Figure 1-22 Storm Control Settings



- Adding storm control ports

To add a storm control port, it is necessary to set at least Broadcast, Unicast, or Multicast. Afterwards, click **Save**. The newly added storm control port is displayed in the storm control list after a “Configuration succeeded.” message is displayed.

- Editing storm control ports

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

- Deleting storm control ports

1) Multiple ports can be selected from the storm control port list. Click **Delete Selected Port** to batch delete ports.

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

After confirming the operation, the ”Delete succeeded.” message is displayed.

1.3.6 Advanced

1.3.6.1 Port Protection

In some application environments, it is required that communication be disabled between some ports. For this purpose, you can configure some ports as protected ports. You can also disable routing between protected ports.

After ports are configured as protected ports, protected ports cannot communicate with each other, but can communicate with non-protected ports.

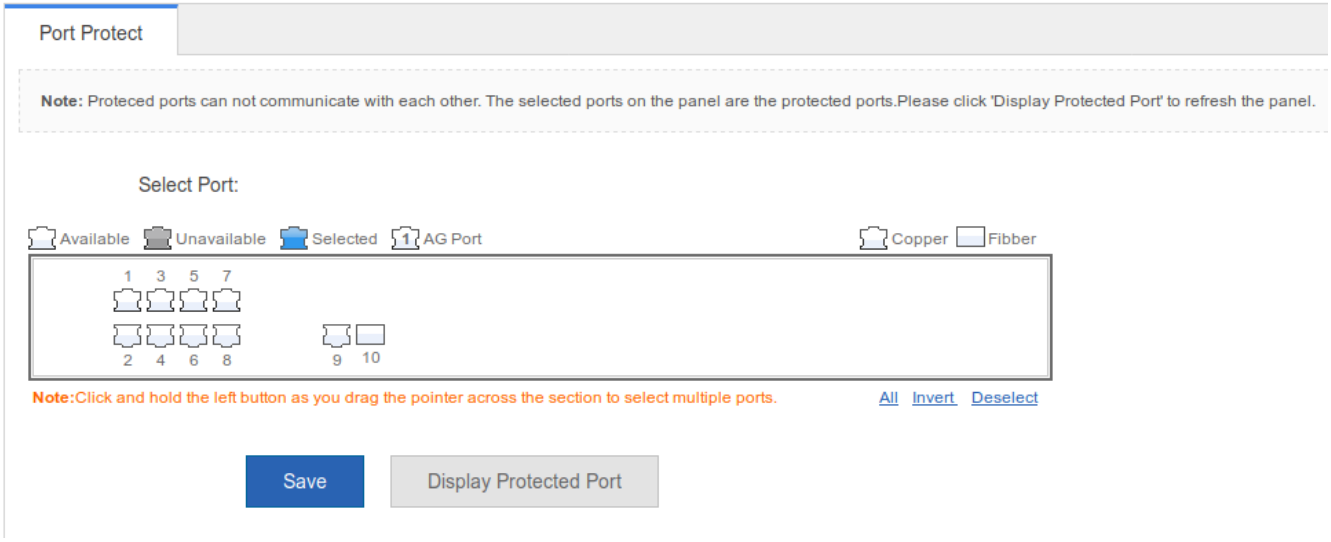
Protected ports work in either of the two modes. In the first mode, L2 switching is blocked but routing is allowed between protected ports. In the second mode, both L2 switching and routing are blocked between protected ports. If a protected port supports both modes, the first mode is used by default.

When two protected port are configured as a pair of mirroring ports, frames sent or received by the source port can be mirrored to the destination port.

Currently, only an Ethernet physical port or AP port can be configured as a protected port. When an AP port is configured as a protected port, all of its member ports are configured as protected ports.

The following figure shows the Port Protect Settings page.

Figure 1-23 Port Protect Settings



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

1.3.6.2 ACL

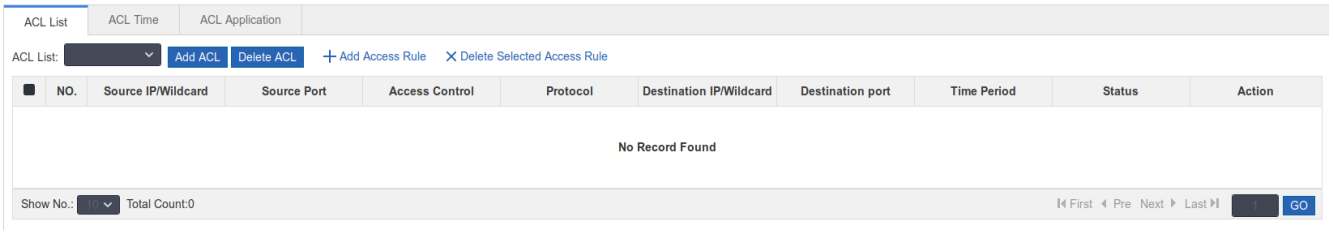
Access control list (ACL) is also called access list or firewall. It is even called packet filtering in some documents. The ACL defines rules to determine whether to forward or drop data packets arriving at a network interface.

Time-bases ACLs are Access Lists that enable you to restrict or allow resources based on time periods.

ACL List

The following figure shows the ACL List page.

Figure 1-24 ACL List



- Adding ACL

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

- Deleting ACL

Select the ACL to be deleted from the ACL List drop-down list and click Delete ACL. The ”Delete succeeded.’ message is displayed.

- Adding Access rule

To add an ACL rule, it is necessary to select the access control type, protocol, effective time, and IP address. Afterwards, click **Save**. The newly added ACL rule is displayed in the ACL rule list after the ”Add succeeded.” message is displayed.

- Editing access rule

After clicking **Edit** in the **Action** column, the information of the corresponding ACL rule is displayed on the page. After editing the information, click **Save**. The “Edit succeeded.” message is displayed.

- Deleting access rule

1) Multiple access rules from the ACL rule list can be selected. Click **Delete Selected Access Rule** to batch delete access rules.

2) After clicking **Delete** in the **Action** column, the “Are you sure you want to delete the access rule?” message is displayed. After confirming the operation, a ”Delete succeeded.” message is displayed.

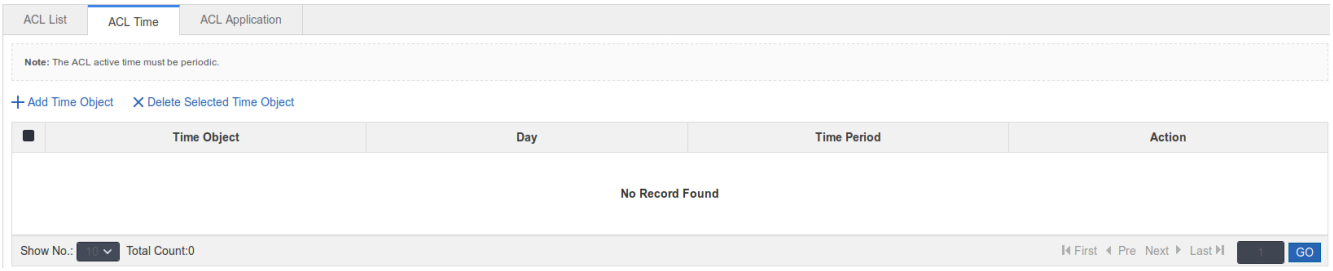
- Moving access rule

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

ACL Time

The following figure shows the ACL Time page.

Figure 1-25 ACL Time



- Adding ACL time

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

- Editing ACL time

After clicking **Edit** in the Action column, the information of the corresponding ACL time is displayed on the page. After editing the information, click **Save**. A “Save succeeded.” message is displayed.

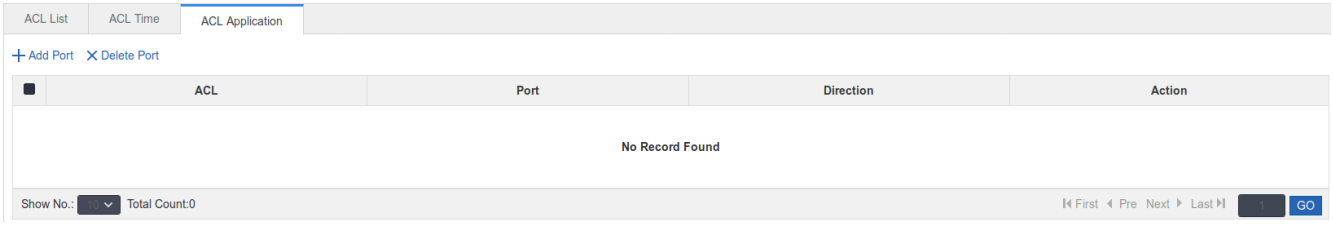
- Deleting ACL time

Multiple time objects can be selected from the ACL time list. Click **Delete Selected Time Object** to batch delete time objects.

ACL Application

The following figure shows the **ACL Application** page.

Figure 1-26 ACL Application



- Add ACL application

To add an ACL application, it is necessary to set the ACL application time and select ACL, filtration direction, and port. Afterwards, click **Save**. The newly added ACL application is displayed in the ACL application list after a “Configuration succeeded.” message is displayed.

- Editing ACL application

After clicking **Edit** in the **Action** column, the information of the corresponding ACL application is displayed on the page. After editing the information, click **Save**. The ”Configuration succeeded.” message is displayed.

- Deleting ACL application

1) Multiple ports from the ACL application list can be selected. Click **Delete Port** to batch delete ports.

2) After clicking **Delete** in the **Action** column, the ”Are you sure you want to delete the ACL application?” message is displayed.

After confirming the operation, the “Delete succeeded.” message is displayed.

1.3.7 System

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

1.3.7.1 System Settings

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

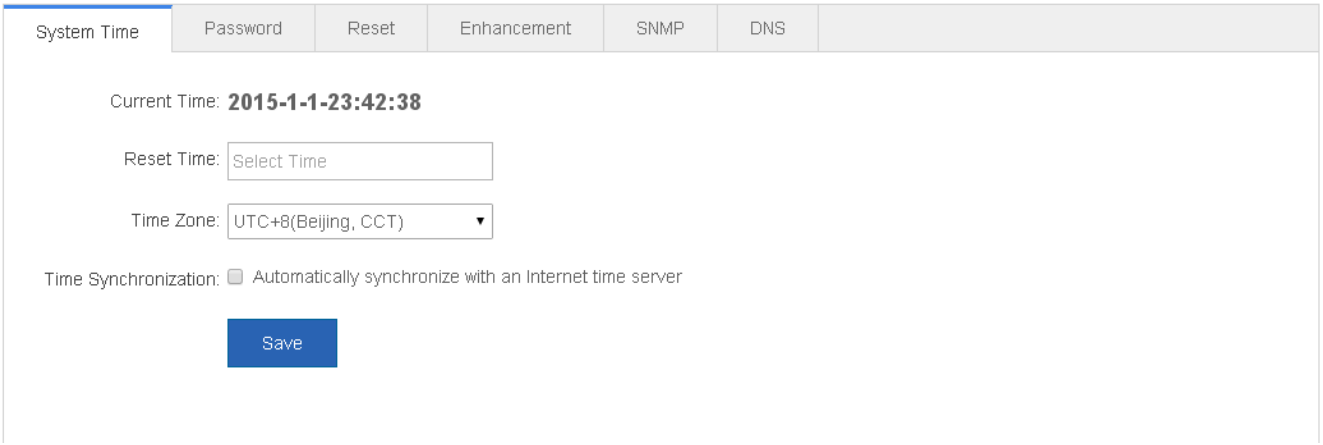
System time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of *year-month-day, hour*:*minute*:*second*, *day of the week*.

When you use a network device for the first time, set its system clock to the current date and time manually.

The following figure shows the System Time page.

Figure 1-27 System Time



- System time

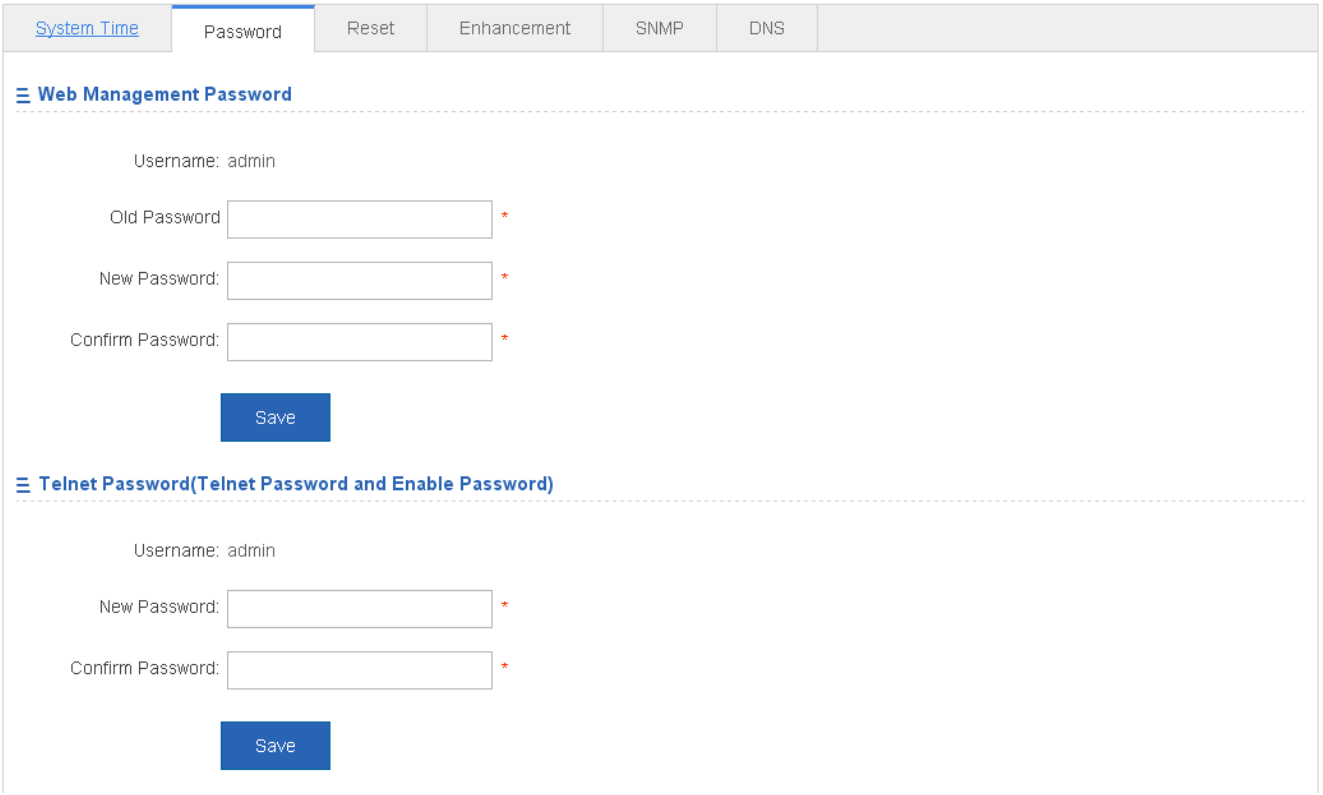
The current system time is displayed on the page. Current system time can be set manually. Alternatively, you can select **Automatically synchronize with an Internet time server** for setting the time. Afterwards, click **Save**. The ”Configuration succeeded.” message is displayed.

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

Password

The following figure shows the Password page.

Figure 1-28 Password



- Modifying the Web-based NMS password

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

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

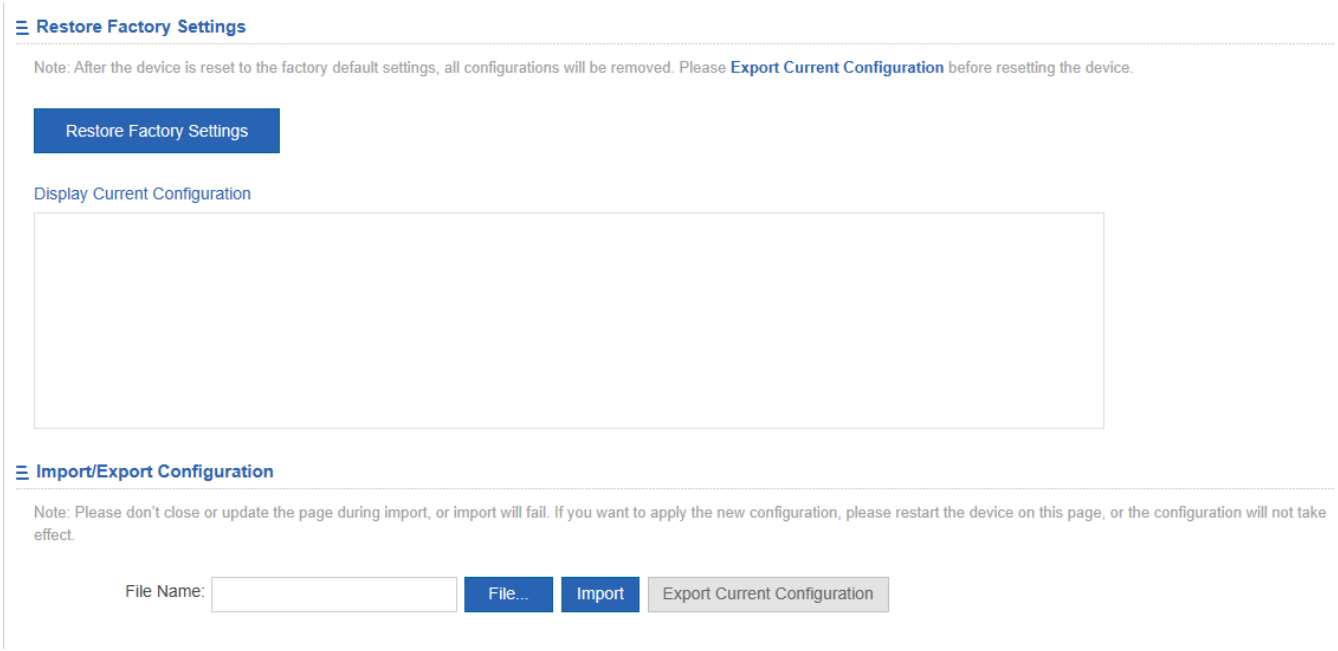
- Modifying the telnet authentication password

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

Restoring factory settings

The following figure shows the Reset page.

Figure 1-29 Reset



- Importing/exporting configurations

Configurations can be imported to modify the device configuration. Restart the device for the new configuration to install. The current configuration can be exported as a backup.

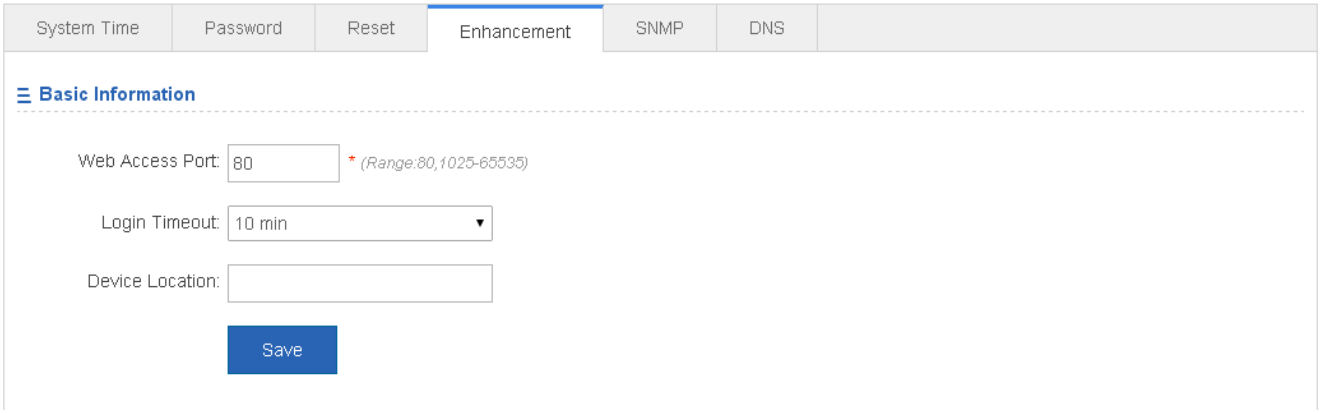
- Restoring factory settings

Click **Restore Factory Settings** to restore the current configuration to factory settings.

Enhancement

The following figure shows the Enhancement page.

Figure 1-30 Enhancement



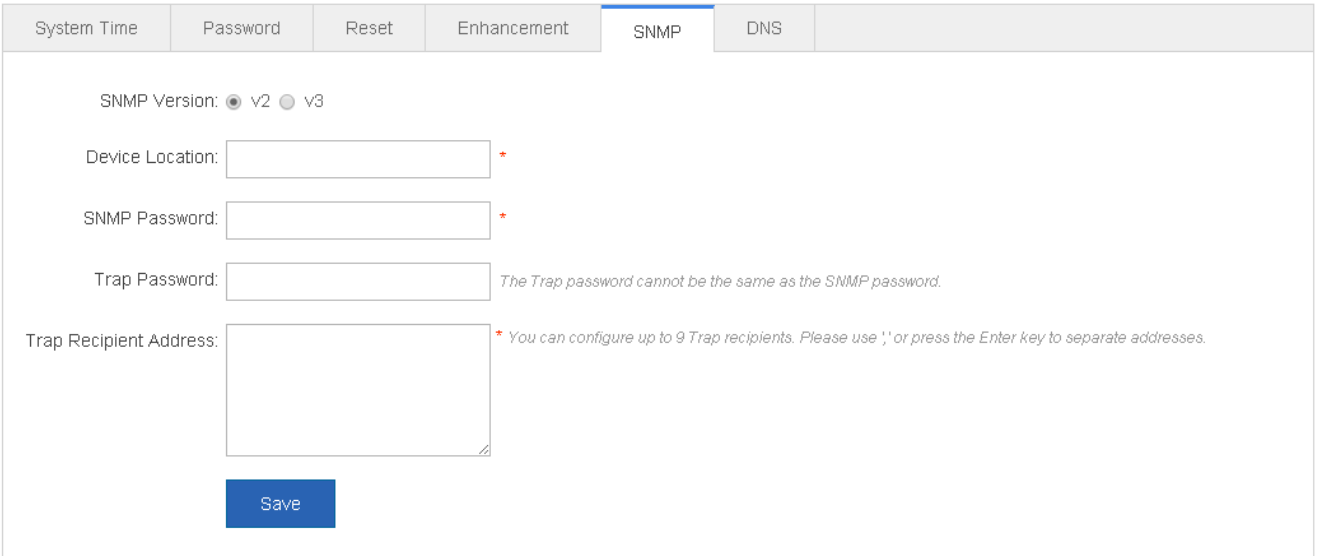
Specify Web Access Port (mandatory) and specify Login Timeout and Device Location as required. Afterwards, click **Save.** The "Configuration succeeded." message is displayed.

SNMP

The Simple Network Management Protocol (SNMP) is by far the dominant protocol in network management. This Protocol (SNMP) was designed to be an easily implementable, basic network management tool that could be used to meet network management needs. It is named Simple Network Management Protocol as it is really easy to understand. A key reason for its widespread acceptance, besides being the chief Internet standard for network management, is its relative simplicity. There are different versions of SNMP, such as SNMP V1, SNMP V2c, and SNMP V3.

The following figure shows the SNMP page.

Figure 1-31 SNMP



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

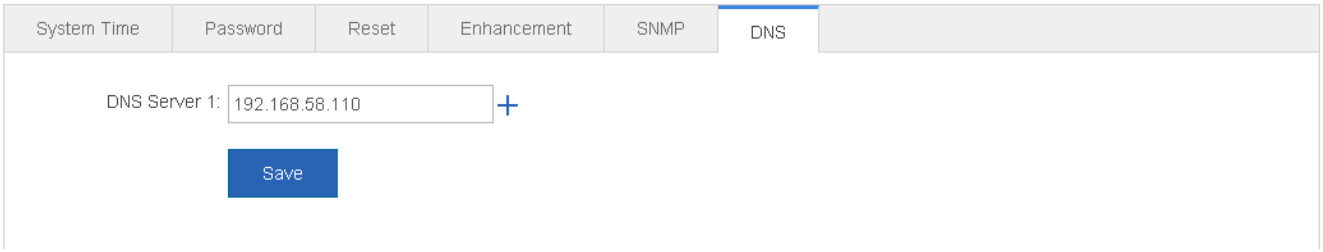
DNS

A Domain Name System (DNS) is a distributed database containing mappings between domain names and IP addresses on the Internet, which facilitate users to access the Internet without remembering IP strings that can be directly accessed by computers. The process of obtaining an IP address through the corresponding host name is called domain name resolution (or host name resolution).

DNS consists of a resolver and a DNS server. The DNS server stores the mappings between domain names and IP addresses of all hosts on the network, and implements mutual conversion between the domain names and IP addresses. Both the TCP and UDP port IDs of DNS are 53, and generally a UDP port is used.

The following figure shows the DNS page.

Figure 1-32 DNS



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

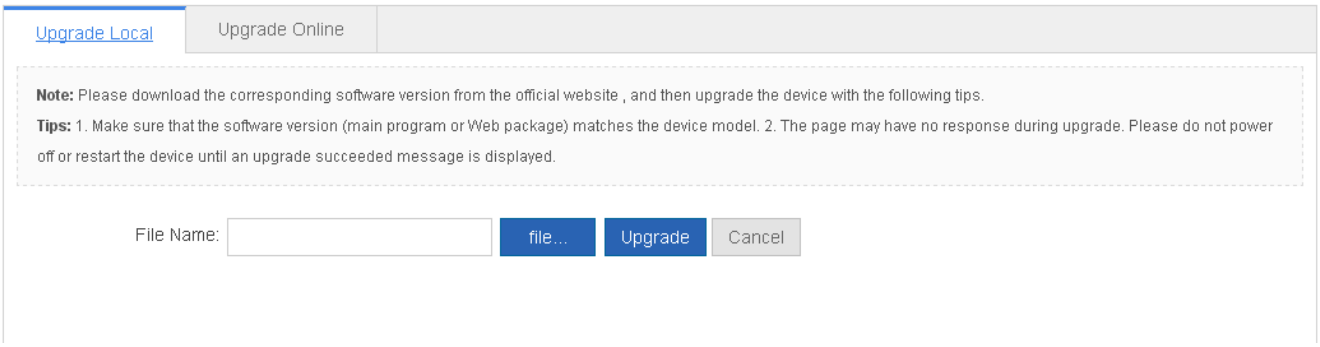
1.3.7.2 System Upgrade

Two tab pages are available on the system upgrade page: Upgrade Local and Upgrade Online.

Upgrade Local

The following figure shows the Upgrade Local page.

Figure 1-33 Upgrade Local

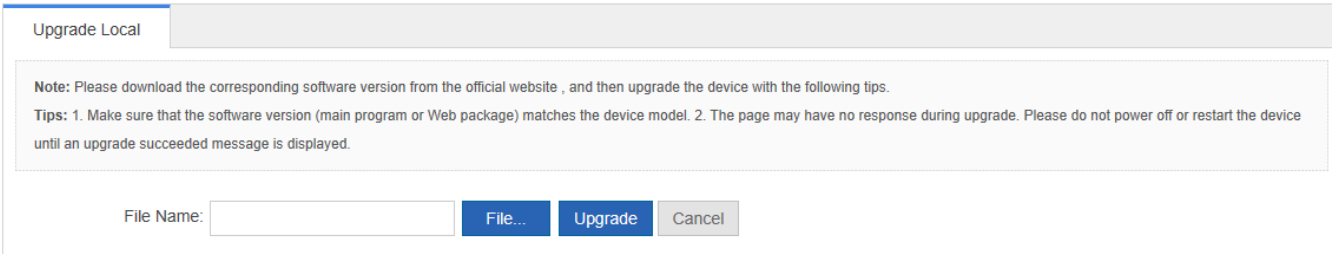


Click **file…**, select a bin file stored locally, and click **Upgrade** to start local upgrade.

Upgrade Online

The following figure shows the Upgrade Online page.

Figure 1-34 Upgrade Online



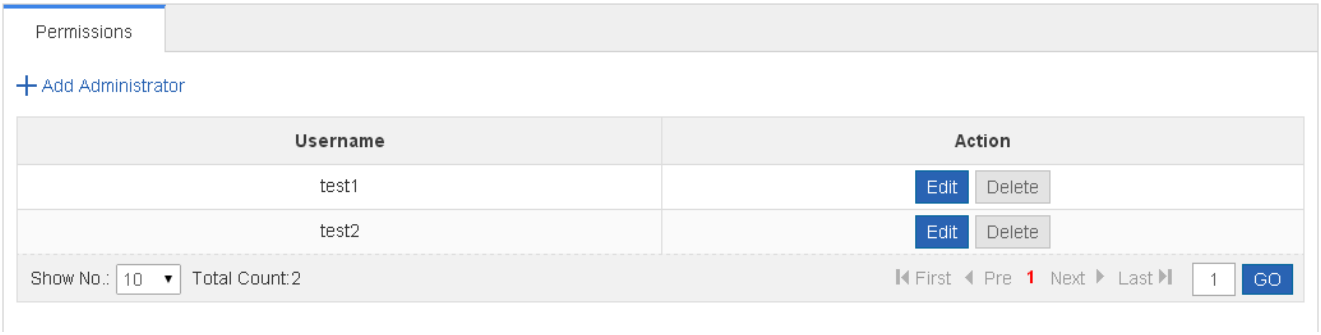
If a version later than the current version is available, click **Detect New Version** to upgrade the Web package to the latest version.

1.3.7.3 Administrator Permissions

The Administrator Permissions page allows configuration of administrator permissions.

The following figure shows the Administrator Permissions page.

Figure 1-35 Administrator Permissions



- Adding user

To add a user, input the username, password, and authorized page (by default, the authorized page is all pages). Afterwards, click **Save**. All users are displayed in the administrator list after a “Configuration succeeded.” message is displayed.

Two default users are available, that is, super administrator (admin) and guest (guest). Super administrator admin can modify the permissions of other administrators. An administrator can access all pages except the **Administrator Permissions** page, while a guest can only access the home page. Default users cannot be deleted.

1.3.7.4 System Logging

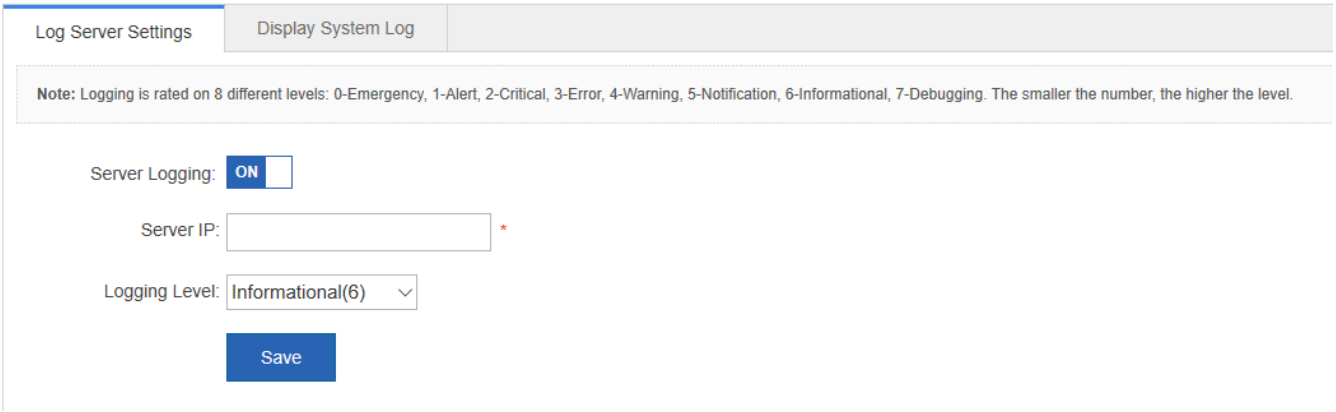
Status changes (such as link up and down) or abnormal events may occur anytime. Ruijie products provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console or monitoring terminal, recorded on media such as the memory buffer or log files, or sent to a group of log servers on the network so that the administrator can analyze network performance and identify faults based on these log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity level so that the administrator can conveniently read and manage log packets.

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

Log Server Settings

The following figure shows the Log Server Settings page.

Figure 1-36 Log Server Settings

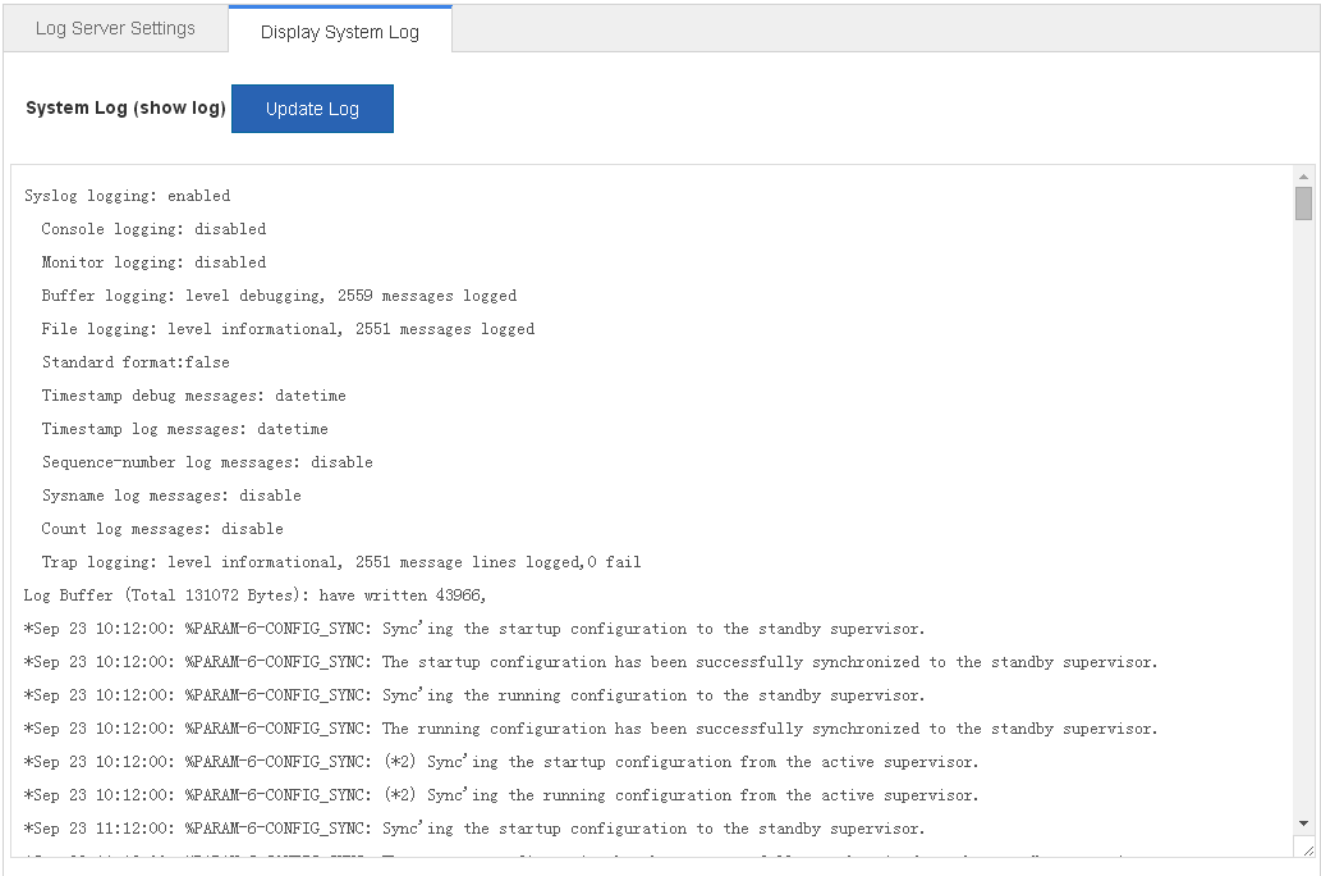


Set various parameters such as Server IP Address and Logging Level. The device sends the SYSLOG log to the corresponding server after the configuration is complete.

Display System Log

The following figure shows the Display System Log page.

Figure 1-37 Display System Log



The current log information is displayed in the text box. Click **Update Log** to refresh log information.

1.3.7.5 Network Detection

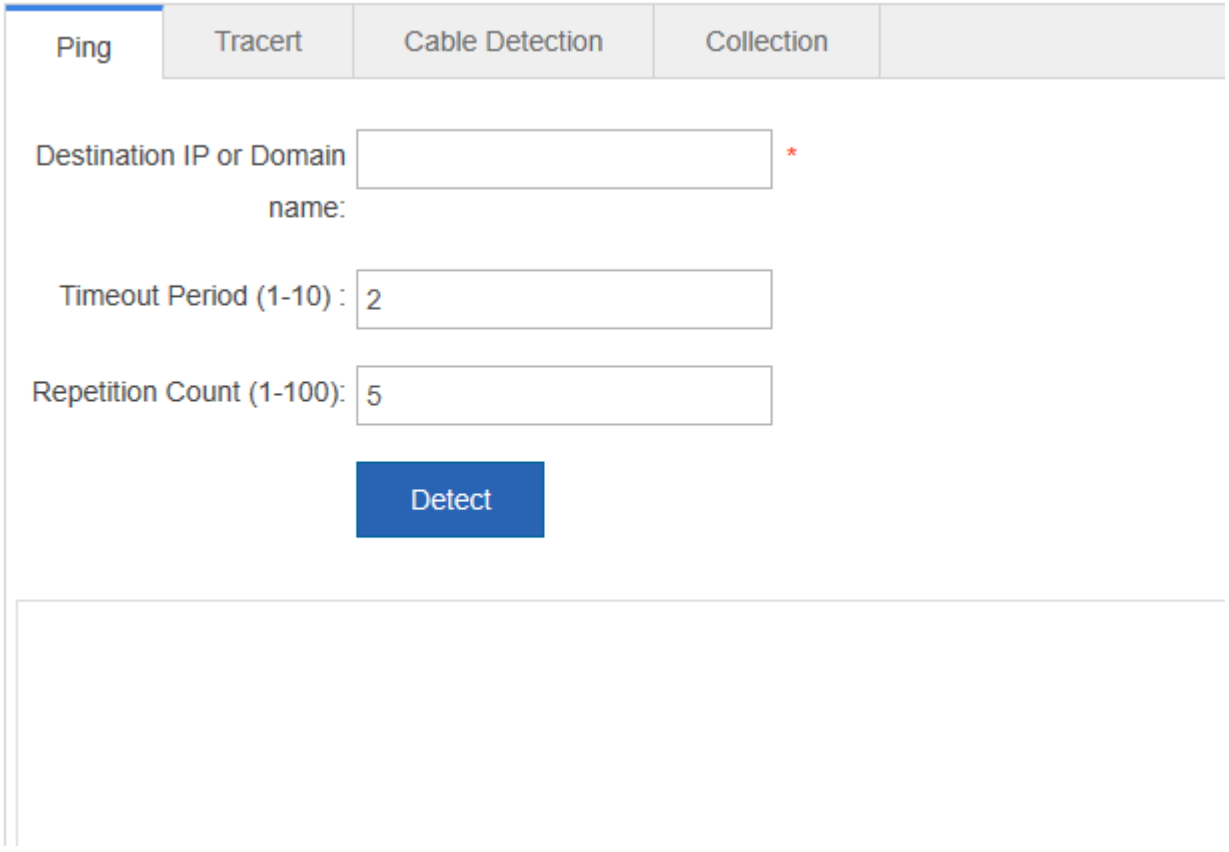
Three tab pages are available on the network connection detection page: Ping, Tracert, and Cable Detection.

Ping

The ping tool sends an Internet Control Message Protocol (ICMP) Request message to the destination host to request the for an ICMP Echo Reply message. In this way, the ping tool determines the delay and the connectivity between the two network devices.

The following figure shows the Ping page.

Figure 1-38 Ping



Input the destination IP address and click **Detect**. The detection result is then displayed in the text box.

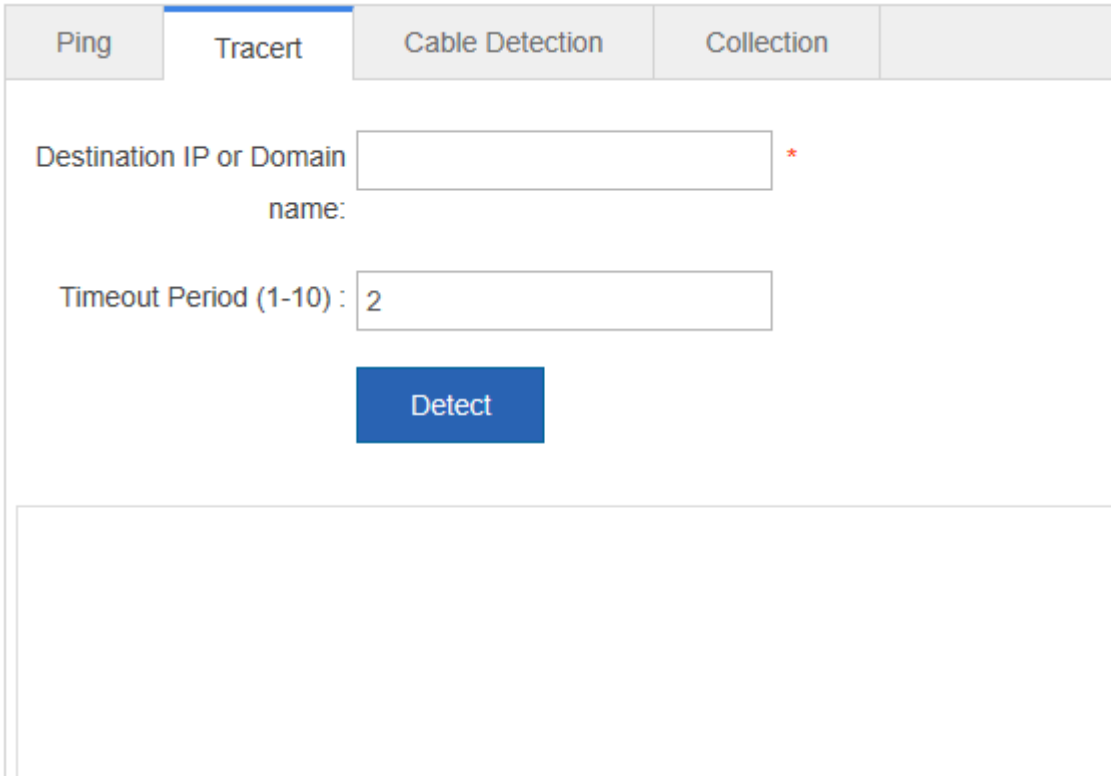
Tracert

The Tracert tool uses the Time To Live (TTL) field in the headers of the ICMP and IP messages for the test First, the Tracert tool on the network device sends an ICMP Request message with TTL 1 to the destination host. After receiving the message, the first router on the path decreases the TTL by 1. As the TTL becomes 0, the router drops the packets and returns an ICMP time exceeded message to the network device. After receiving this message, the Tracert tool learns that this router exists on this path, and then sends an ICMP Request packet with TTL 2 to the destination host to discover the second router. Each time the Tracert tool increases the TTL in the ICMP Request message by 1 to discover one more router. This process is repeated until a data packet reaches the destination host. After the packet reaches the destination host, the host returns an

ICMP Echo message instead of an ICMP time exceeded message to the network device. Then, the Tracert tool finishes the test and displays the path from the network device to the destination host.

The following figure shows the Tracert page.

Figure 1-39 Tracert



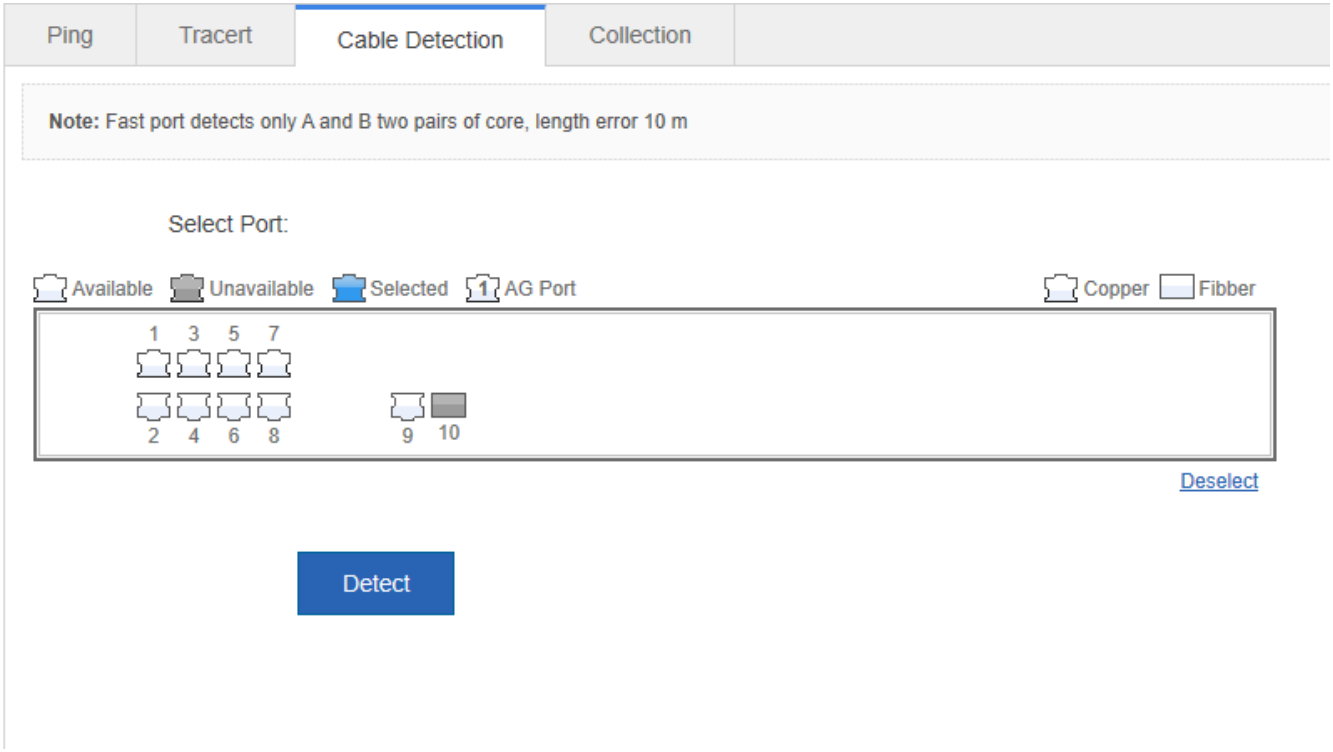
Input the destination IP address and click **Detect**. The detection result is displayed in the text box after a short time.

Cable Detection

When a cable is short-circuited or disconnected, cable detection helps you determine the working status of the cable. Only a physical port using copper as the medium supports cable detection. A physical port using fiber as the medium or an AP port does not support cable detection. When cable detection is performed on an operational interface, the interface will be temporarily disconnected, and then re-connected.

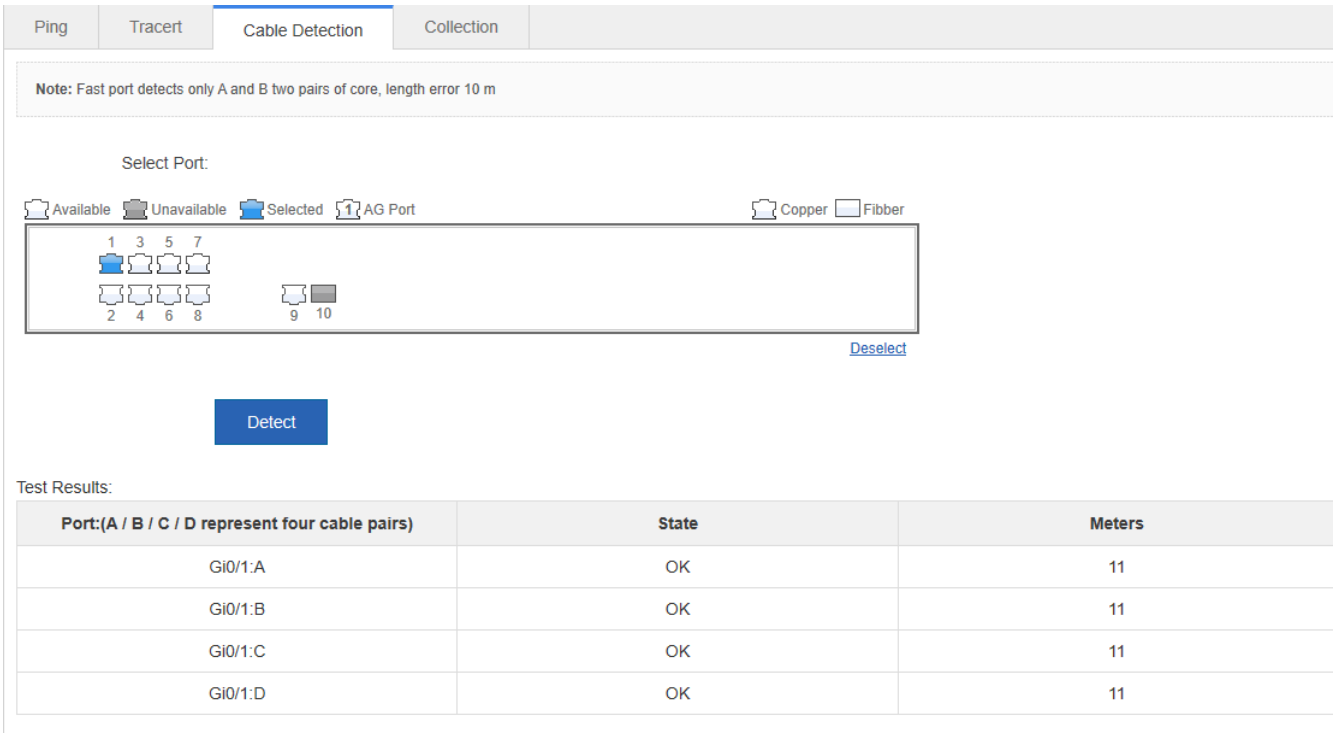
The following figure shows the Cable Detection page.

Figure 1-40 Cable Detection



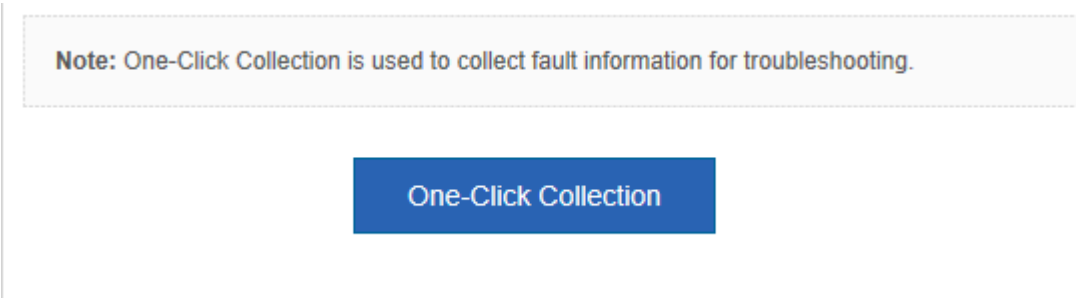
Select a port on the panel and click Detect. After a short time, the detection result is displayed below the Detect button.

Figure 1-41 Cable detection result.



Collection

Click **One-click Collection** to collect the fault information for troubleshooting.



1.3.7.6 Web CLI

The page simulates the CLI. Enter CLI commands, and press enter or click **Send**. Tab completion and "?" command are supported.