



Ruijie Networks HS2310 Main Telephone Line Unit User Guide

[Home](#) » [Ruijie Networks](#) » Ruijie Networks HS2310 Main Telephone Line Unit User Guide 

Contents

- [1 Ruijie Networks HS2310 Main Telephone Line Unit](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Preface](#)
- [5 Web-Based Configuration](#)
- [6 Web-based Management](#)
- [7 Web Management System](#)
 - [7.1 Favorites](#)
 - [7.2 Network](#)
 - [7.3 Security](#)
 - [7.4 Advanced](#)
 - [7.5 System](#)
- [8 Documents / Resources](#)
 - [8.1 References](#)



Ruijie Networks HS2310 Main Telephone Line Unit



Product Information

Specifications:

- **Product Model:** HS2310-16GH2GT1XS
- **Document Version:** V1.0
- **Release:** RGOS 11.4(1)B90

Product Usage Instructions

Web-Based Configuration

- **Overview**

The web-based configuration allows users to manage and configure the product through a web interface.

- **Web-based Management**

The web-based management provides a user-friendly interface for configuring various settings of the product. Users can access the web management interface by entering the IP address of the product in a web browser.

- **Web Management System**

The web management system includes several features for easy configuration:

- **Wizard**

The wizard feature provides step-by-step instructions for initial configuration, making it easier for users to set up the product.

- **Favorites**

The favorites feature allows users to save frequently accessed settings for quick access. It includes the following sections:

- **Home Page**

The home page section of favorites allows users to save and access their preferred home page layout and settings.

- **VLAN**

The VLAN section of favorites allows users to save and access their preferred VLAN configurations.

FAQ (Frequently Asked Questions):

- **Q: Where can I obtain technical assistance for the product?**

A: You can obtain technical assistance from the following sources:

- **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](https://www.ruijienetworks.com)

- **Q: What is G.hn?**

A: G.hn (Gigabit Home Networking) is a technology that allows for ultra-fast and reliable network connectivity over various physical networking mediums in the home, such as power cables, coaxial cables, and twisted pair cables.

- **Q: What is a Domain Master (DM)?**

A: A Domain Master (DM) is responsible for the operation of all nodes in a G.hn domain, including device



- EP

End Point (EP) refers to the nodes that don't belong to DMs in a G.hn domain.

- **GAM**

G.hn access multiplex (GAM) refers to the device than contains multiple DMs and allows multiple Eps to access.

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.

Web-Based Configuration

Overview

A user accesses and employs the Web-based management system for a switch using a web browser like Google and Firefox. 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.

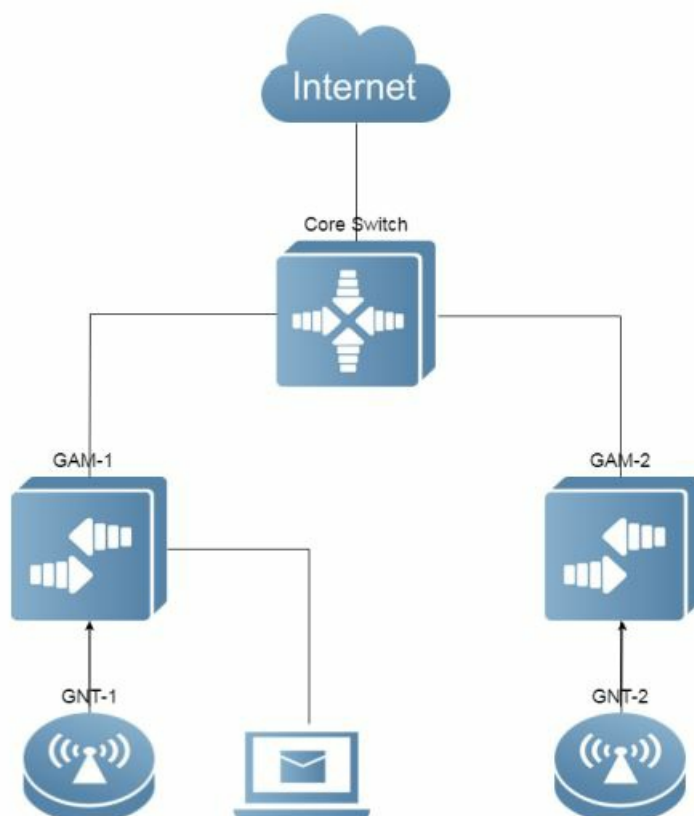
- Currently, this file is applicable to only switches.

Web-based Management

Scenario

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

Figure 1-1



Function Deployment



• Configuration Environment Requirements

An administrator logs in to the Web-based management system using the web browser on a client to manage the GAM. Generally, a client refers to a PC. It may also be other mobile terminal devices like a laptop.

- **Browser:** Google chrome and Firefox browsers are 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 errors may occur after selecting other resolutions.

• GAM Requirements

The Web service must be enabled for the switch. (The Web service is enabled by default, and is automatically redirected from http to https.) The default username and password are both admin. The default password must be changed after the first login. The password must be formed by uppercase, lowercase and digits. A management IP address must be configured for the GAM. The default management IP address is 192.168.1.200/24.

-  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
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.

Figure 1-3 Modify Password

Modify password

Username: admin

New Password:

Please enter a new password...

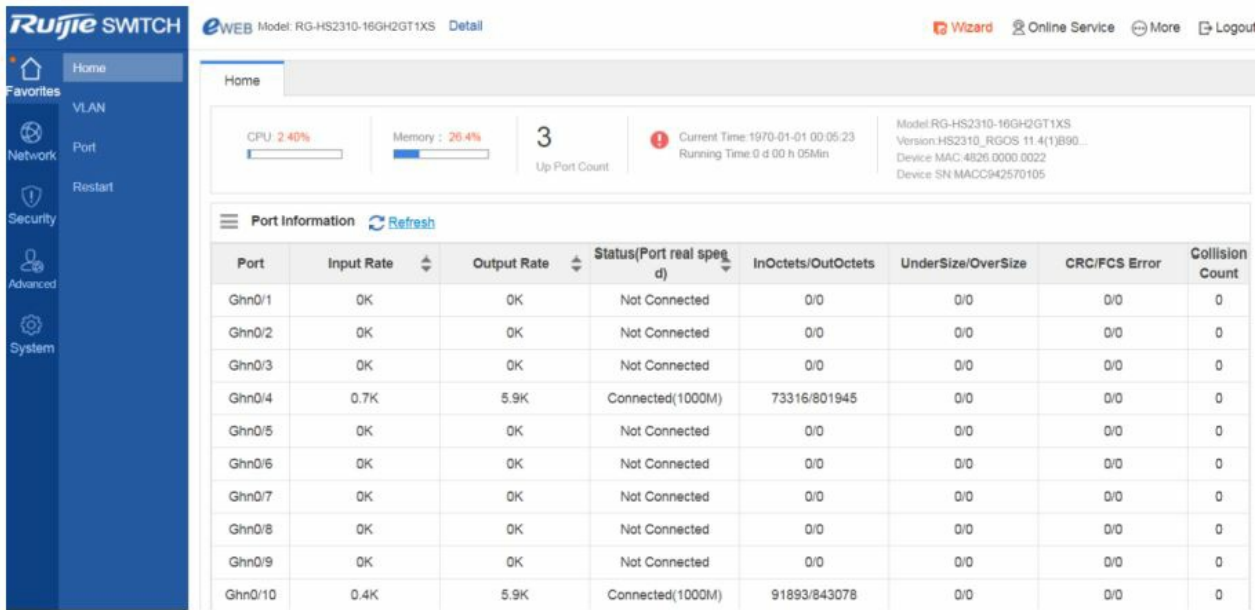
Confirm Password:


Please enter a new password...

Modify

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

Figure 1-4 Home Page


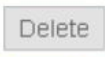











 For details on the Web page, see Web Management System below.

Web Management System

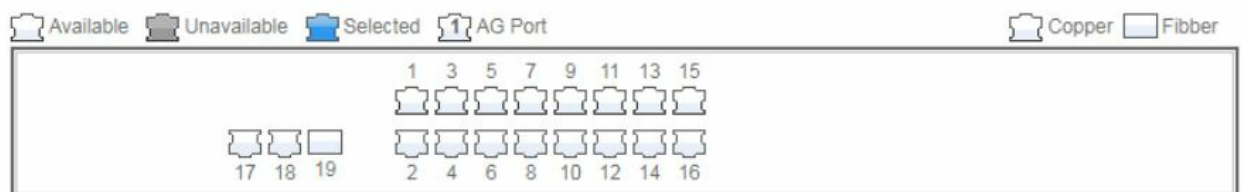
Basic Concepts

- Icons and Buttons on the Web-GUI

Icon/Button	Note
	Edit button. Click this icon to edit the currently selected item.
	Delete button.
	ON/OFF switch.
	Port available for selection. After you click or select this port, it becomes a selected port.
	Port not available for selection.
	Selected port.
	Aggregate port. The number in the port indicates the aggregate port number.
	Trunk port. This port is displayed on the panel on the VLAN Management/VLAN Settings page.
	Save button. 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.

• System Operations

◦ Standalone Device Panel

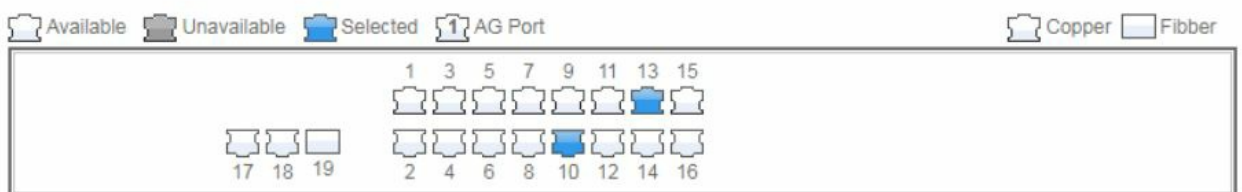


Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G.hn ports.

◦ 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



Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G.hn ports.

Features

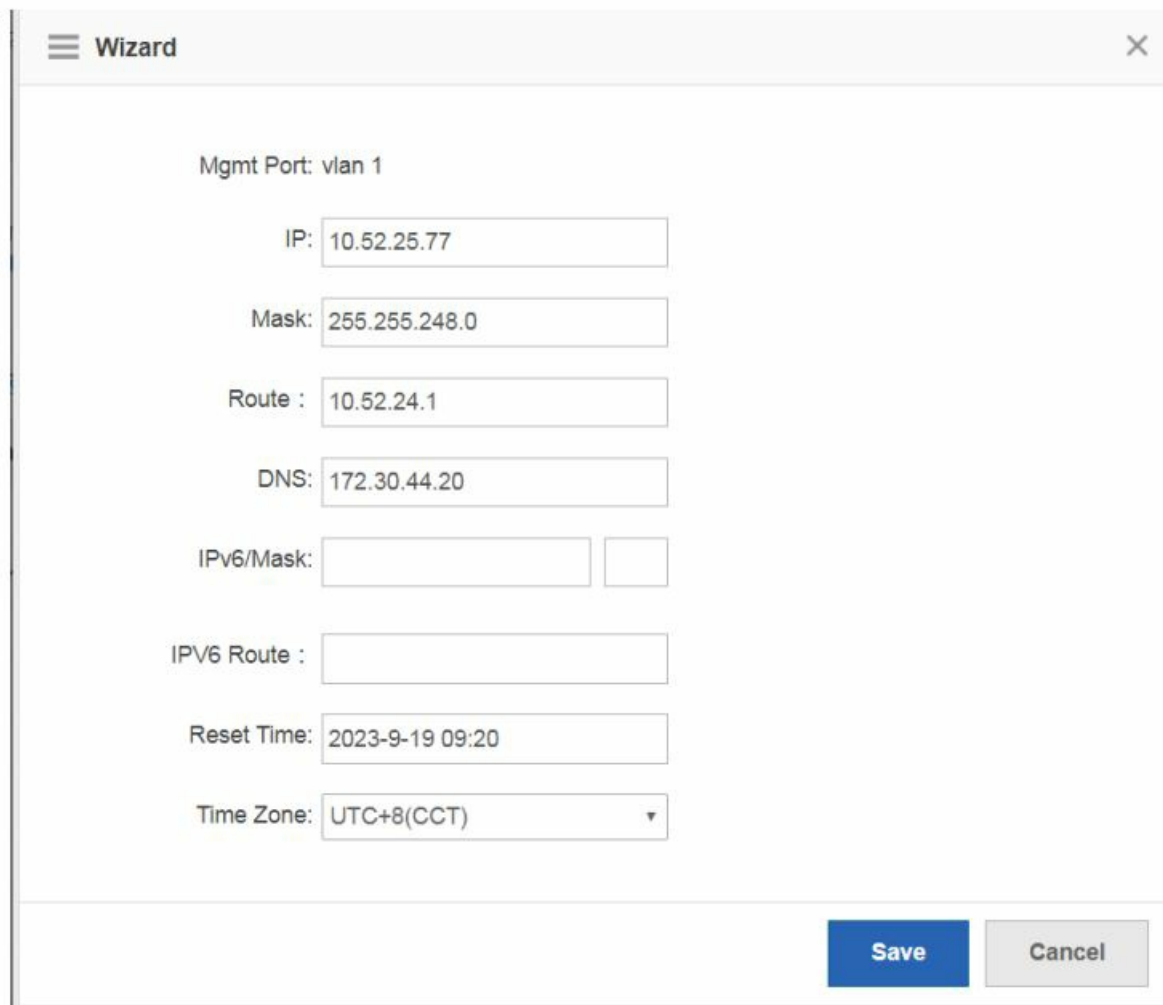
The following table describes the functions in the secondary menu on the left of the Web page.

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.
Restart	For restarting the device.
MAC Address	For configuring the static address and filtering address.
RLDP	Used to configure RLDP.
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 Protection	Used to configure port protection.
ACL	Used to set the ACL list and ACL time and apply ACL.
QoS	Used to guarantee the use and allocation of network resources so as to improve network performance and reliability.
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.
System Logging	Used to configure the log server and view system logs.
Network Detection	Used to configure ping, Traceroute, cable detection and one-click collection.
Web CLI	Used to simulate CLI.

Wizard

Configure the IP address, subnet mask/IPv6 subnet mask, default gateway address, and DNS server address, and click Save. If the message "Configuration succeeded." is displayed, the operation is successful.

Figure 1-5 Wizard



The image shows a 'Wizard' configuration window with a title bar containing a menu icon and the text 'Wizard' and a close button. The main area contains the following fields:

- Mgmt Port: vlan 1
- IP: 10.52.25.77
- Mask: 255.255.248.0
- Route : 10.52.24.1
- DNS: 172.30.44.20
- IPv6/Mask: [] []
- IPv6 Route : []
- Reset Time: 2023-9-19 09:20
- Time Zone: UTC+8(CCT) ▼

At the bottom right, there are two buttons: 'Save' (blue) and 'Cancel' (gray).

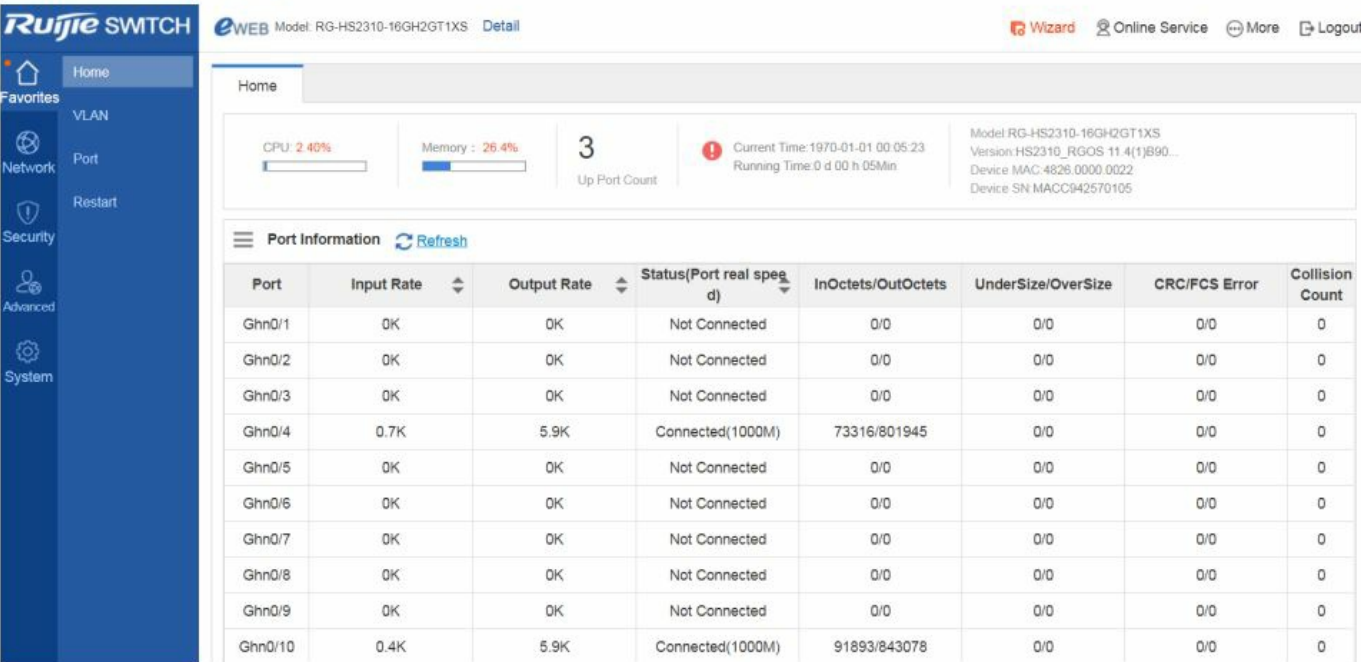
Favorites

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

Home Page

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

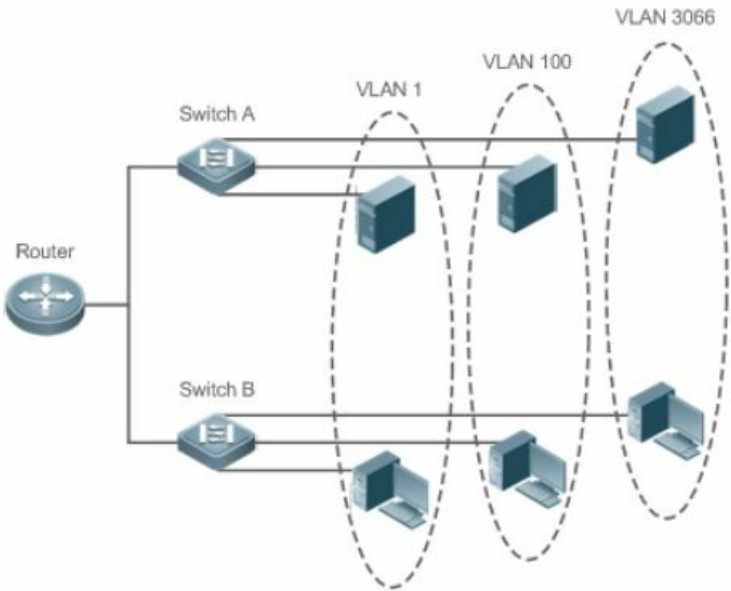
Figure 1-6 Home Page



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 isolated. We may define a port as a member of a VLAN, and all terminals connected to this port are parts of this VLAN. 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.

Figure 1-7



- 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. 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 1-8 VLAN Settings

VLAN Settings				
Trunk Port				
+ Batch Add VLAN + Add VLAN X Delete Selected VLAN				
	VLAN ID	VLAN name	Port	Action
<input type="checkbox"/>	1	VLAN0001	Gi0/1-6, Gi0/9-10	Edit
<input type="checkbox"/>	2	mmmm	Gi0/7-8	Edit Delete
Show No: Total Count:2				
14 First < Pre 1 Next > Last 14 GO				

- **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, or click Delete in the Action column of a VLAN. Then, the message, “Are you sure you want to delete the VLAN?” is displayed.
2. 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 1-9 Trunk Port

VLAN Settings Trunk Port

Note: If a port allows multiple VLAN packets to go through, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.

No Trunk Port

Native VLAN: * Range(1-4094)

Allowed VLAN: The VLAN range is formatted as 3-5,100.

Select Port:

Available Unavailable Selected 1 AG Port Copper Fiber

17 18 19 1 3 5 7 9 11 13 15
2 4 6 8 10 12 14 16

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G.hn ports.

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

Save Cancel

- **Adding a Trunk Port**

Select a port on the panel, 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. Native VLAN must be set when the Allow VLAN is configured, otherwise, the communication between G.hn ports will be abnormal.

- **Editing a Trunk Port**

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

- **Deleting a 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.

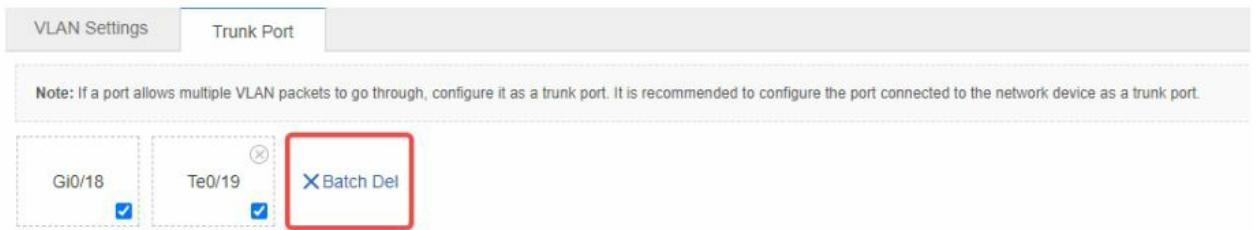
VLAN Settings Trunk Port

Note: If a port allows multiple VLAN packets to go through, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.

Te0/19 X Batch Del

- **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.

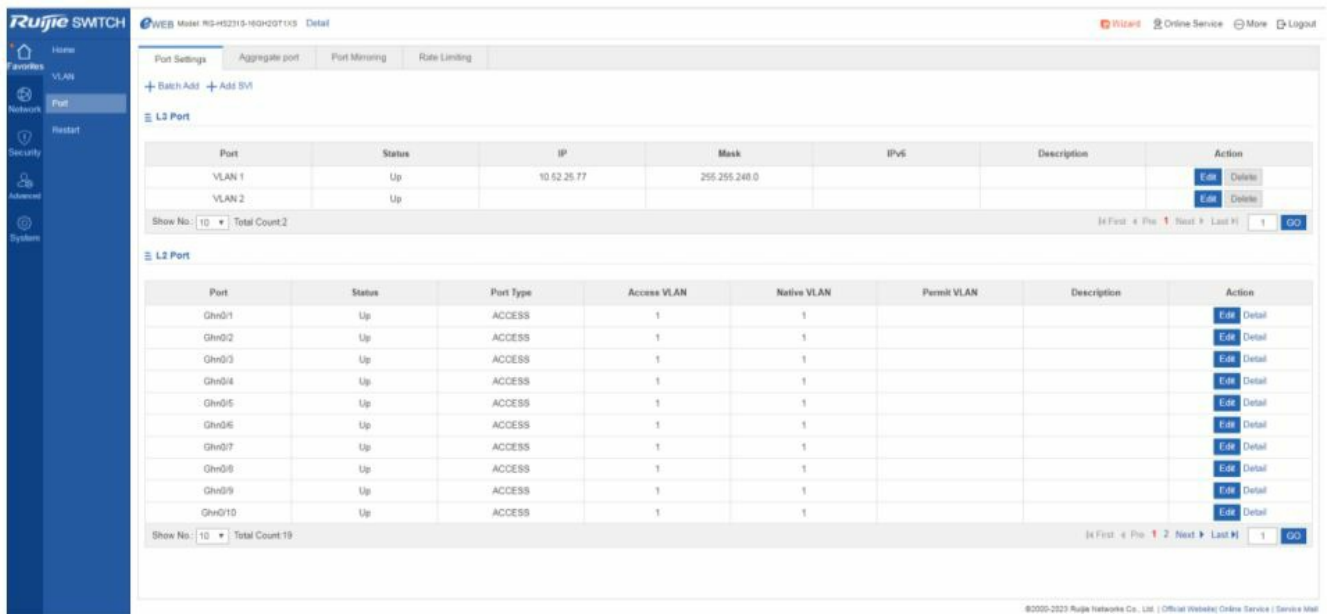


Port

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

- **Port Settings**

Figure 1-10 Port Setting



- **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 a 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 a 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.

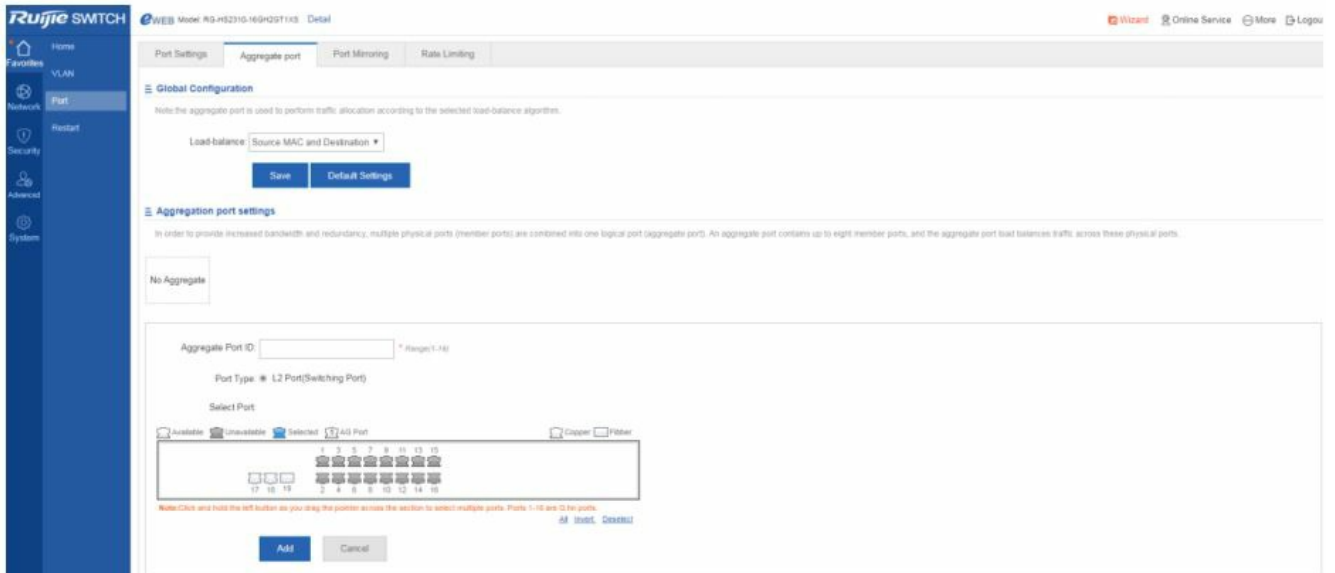
- **Deleting L3 port**

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.

Figure 1-11 Aggregate Port



- **Adding an 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.
-  G.hn ports cannot serve as aggregate ports.

- **Port Mirroring**

The following figure shows the Port Mirroring page.

Figure 1-12 Port Mirroring



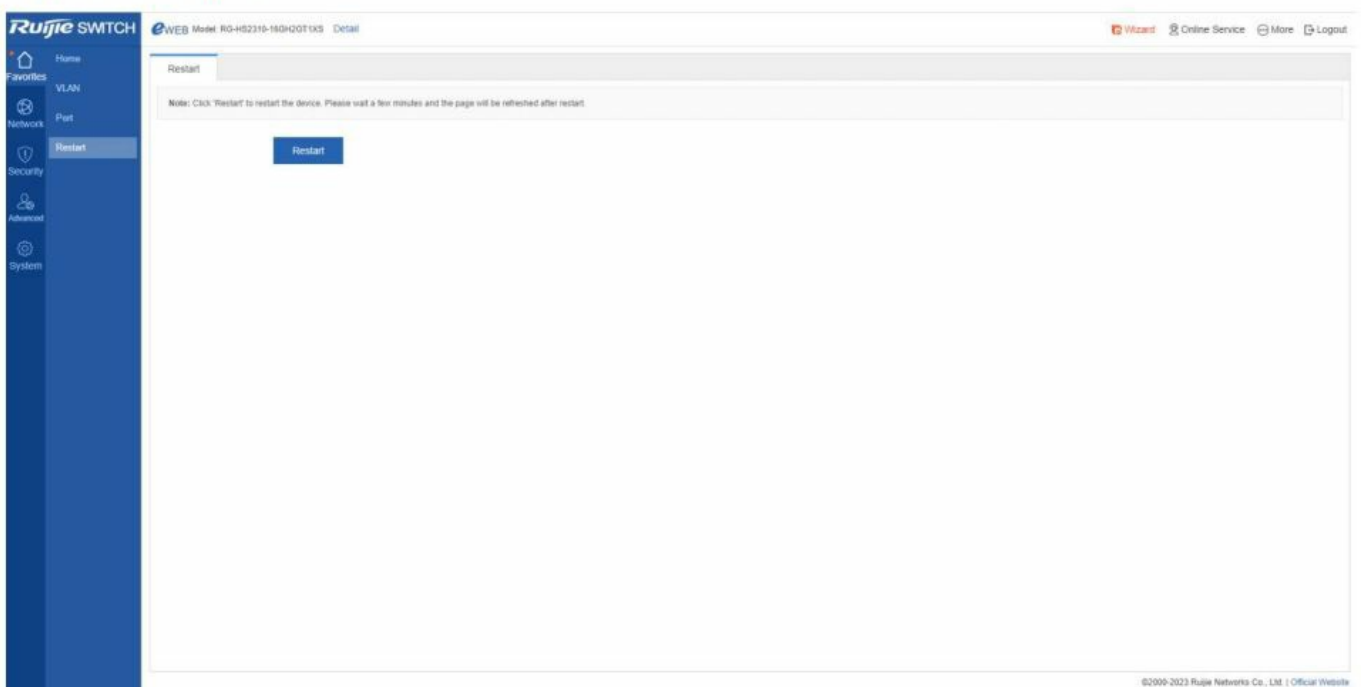
Initially, the Port Mirroring page is in an edit state because only one mirroring port is allowed to be set on the Web. Two panels are available on the page. The port selected from the upper panel will serve as a source port (mirrored port, multiple mirrored ports are allowed). Only one port can be selected 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. G.hn ports cannot serve as destination ports.

Restart

The following figure shows the Restart page.

Figure 1-13 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.

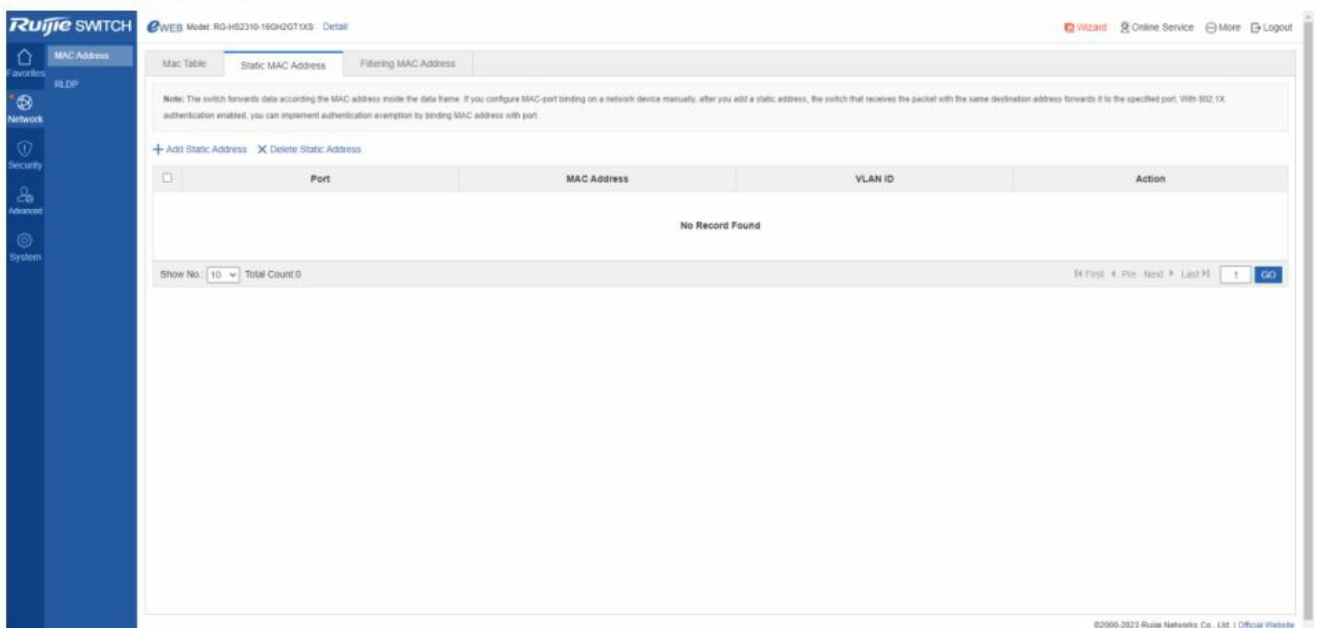
Secondary menus can be accessed through the primary menu Network, including MAC Address and RLDP.

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 functions. 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.

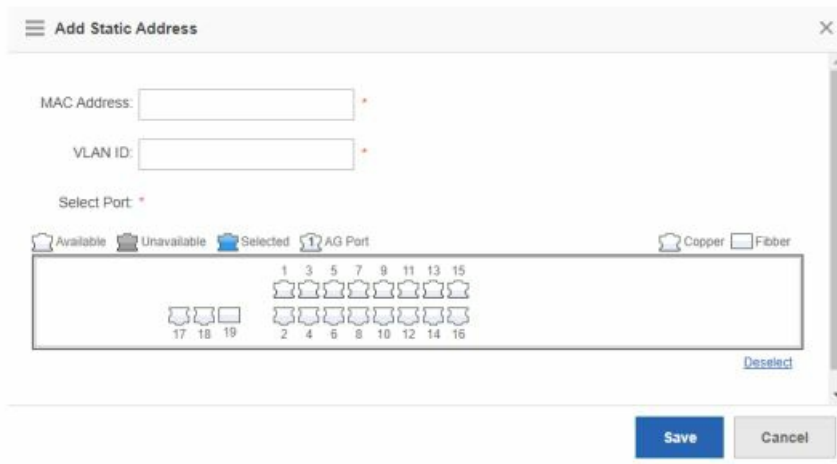
- **Static Address Settings**

Figure 1-14 Static Address Settings



- **Adding a 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.



Add Static Address

MAC Address:

VLAN ID:

Select Port *

Available Unavailable Selected AG Port Copper Fiber

1 3 5 7 9 11 13 15
2 4 6 8 10 12 14 16
17 18 19

[Deselect](#)

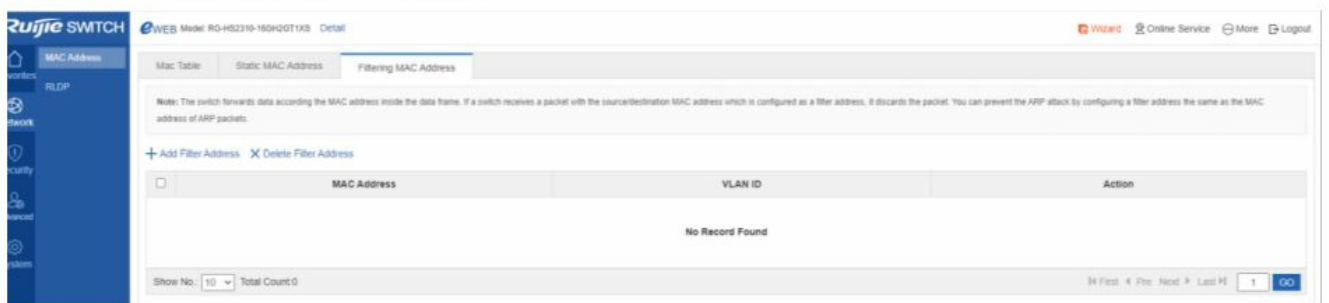
Save **Cancel**

◦ Deleting a 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 1-15 Filtering Address Settings



Ruijie SWITCH eWEB Model: RG-H5210-18QGT1X5 Detail

MAC Table Static MAC Address **Filtering MAC Address** Wizard Online Service More Logout

Note: The switch forwards data according to the MAC address inside the data frame. If a switch receives a packet with the source/destination MAC address which is configured as a filter address, it discards the packet. You can prevent the ARP attack by configuring a filter address the same as the MAC address of ARP packets.

[+ Add Filter Address](#) [X Delete Filter Address](#)

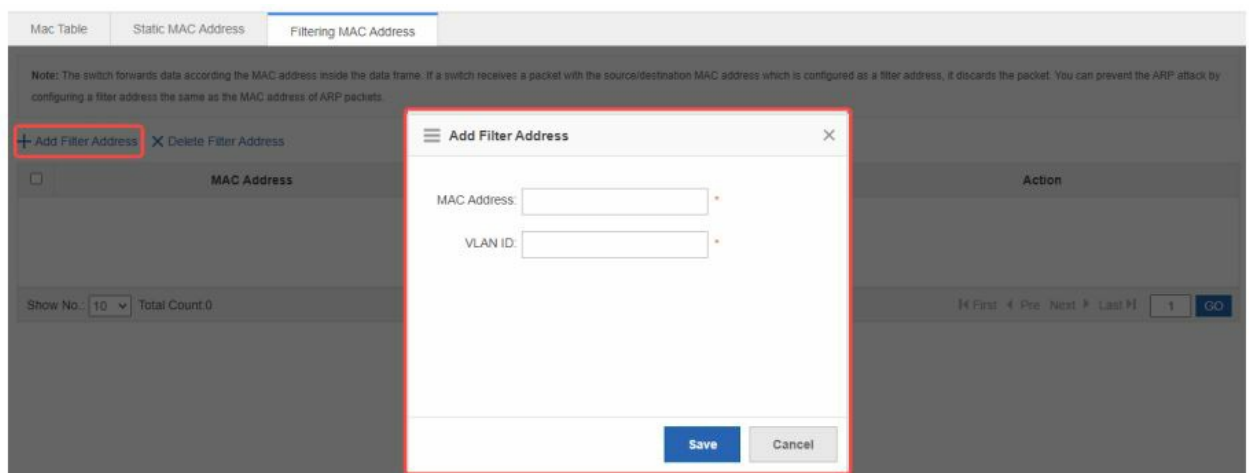
	MAC Address	VLAN ID	Action
No Record Found			

Show No. Total Count: 0

First Prev Next Last 1 **GO**

◦ 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.



Mac Table Static MAC Address **Filtering MAC Address**

Note: The switch forwards data according to the MAC address inside the data frame. If a switch receives a packet with the source/destination MAC address which is configured as a filter address, it discards the packet. You can prevent the ARP attack by configuring a filter address the same as the MAC address of ARP packets.

[+ Add Filter Address](#) [X Delete Filter Address](#)

	MAC Address	VLAN ID	Action
No Record Found			

Show No. Total Count: 0

First Prev Next Last 1 **GO**

Add Filter Address

MAC Address:

VLAN ID:

Save **Cancel**

◦ 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.

Note: The switch forwards data according to the MAC address inside the data frame. If a switch receives a packet with the source/destination MAC address which is configured as a filter address, it discards the packet. You can prevent the ARP attack by configuring a filter address the same as the MAC address of ARP packets.

+ Add Filter Address X Delete Filter Address

<input type="checkbox"/>	MAC Address	VLAN ID	Action
<input type="checkbox"/>	4222.6622.8866	1	Edit Delete

Show No.: 10 Total Count: 1

First < Pre 1 Next > Last 1 GO

• Deleting Filtering Address

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

+ Add Filter Address X Delete Filter Address

<input type="checkbox"/>	MAC Address	VLAN ID	Action
<input checked="" type="checkbox"/>	4222.6622.8866	1	Edit Delete
<input checked="" type="checkbox"/>	4222.6622.8867	4	Edit Delete

Show No.: 10 Total Count: 2

First < Pre 1 Next > Last 1 GO

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.

<input type="checkbox"/>	MAC Address	VLAN ID	Action
<input type="checkbox"/>	4222.6622.8866	1	Edit Delete
<input type="checkbox"/>	4222.6622.8867	4	Edit Delete

Show No.: 10 Total Count: 2

First < Pre 1 Next > Last 1 GO

RLDP

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.

 RLDP is not supported on G.hn ports.

• RLDP Settings

Figure 1-16 RLDP Settings

Ruijie SWITCH WEB Model: RG-H2310-160H20T1X3 Detail

Wizard Online Service More Logout

MAC Address

RLDP

Global configuration

Note: RLDP enables you to detect link failure quickly. RLDP can run on the port only after it is enabled globally.

RLDP: ☒

Detection Interval: 3 (Range: 2-10)

Detection Count: 2 (Range: 2-10)

enable/disable recovery: ☐ (Range: 30-6000s)

Save

Port Configuration

Note: 1. Enabling RLDP on the port can avoid broadcast storm caused by loops. It is recommended to enable RLDP on the port connected to the PC.
2. Unidirectional/directional link detection requires the ports on both ends of the link to be enabled with RLDP. It is recommended to configure RLDP to monitor the link between two switches.

+ Add Port X Delete Port

<input type="checkbox"/>	Port	Detection Type	Troubleshooting	Action
No Record Found				

Show No.: 10 Total Count: 0

First < Pre Next > Last 1 GO

©2000-2023 Ruijie Networks Co., Ltd. | Official Website

• Global Configuration

Enable/Disable RLDP by turning on/off the switch. After setting detection interval and count, click Save.

Secondary menus are accessed through the primary Security menu that includes Anti-ARP-Attack and Storm Control.

Anti-ARP-Attack

You can check ARP entries and bind static addresses.

• ARP Entries

ARP Entries				
<div>Dynamic Binding>>Static Binding Remove static Binding Manual Binding</div>				
		IP-based: <input type="text"/>		<input type="button" value="Search"/>
<input type="checkbox"/>	IP	MAC	Type	Action
<input type="checkbox"/>	192.168.1.200	00e0.4c00.2155	Local ARP Entry	Dynamic Binding>>Static Binding
<input type="checkbox"/>	192.168.21.1	0000.5e00.0115	Dynamic Binding	Dynamic Binding>>Static Binding
<input type="checkbox"/>	192.168.21.138	40b0.3438.536a	Dynamic Binding	Dynamic Binding>>Static Binding
<input type="checkbox"/>	192.168.21.229	00e0.4c00.2155	Local ARP Entry	Dynamic Binding>>Static Binding
Show No.: 10 Total Count: 4				
First Pre 1 Next Last 1 GO				

◦ Dynamic Binding > Static Binding

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

ARP Entries				
<div>Dynamic Binding>>Static Binding Remove static Binding Manual Binding</div>				
		IP-based: <input type="text"/>		<input type="button" value="Search"/>
<input type="checkbox"/>	IP	MAC	Type	Action
<input checked="" type="checkbox"/>	10.52.24.1	ecb9.70b7.00ee	Dynamic Binding	Dynamic Binding>>Static Binding
<input checked="" type="checkbox"/>	10.52.24.35	0023.24e3.f94b	Dynamic Binding	Dynamic Binding>>Static Binding
<input checked="" type="checkbox"/>	10.52.25.61	00d0.f822.3377	Dynamic Binding	Dynamic Binding>>Static Binding
<input checked="" type="checkbox"/>	10.52.25.65	300d.9e3e.ae48	Dynamic Binding	Dynamic Binding>>Static Binding
<input checked="" type="checkbox"/>	10.52.25.76	00e0.4c00.215f	Local ARP Entry	Dynamic Binding>>Static Binding

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

<input type="checkbox"/>	IP	MAC	Type	Action
<input type="checkbox"/>	10.52.24.1	ecb9.70b7.00ee	Dynamic Binding	Dynamic Binding>>Static Binding
<input type="checkbox"/>	10.52.24.35	0023.24e3.f94b	Dynamic Binding	Dynamic Binding>>Static Binding
<input type="checkbox"/>	10.52.25.61	00d0.f822.3377	Dynamic Binding	Dynamic Binding>>Static Binding

◦ Remove Static Binding

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

ARP Entries				
<div>Dynamic Binding>>Static Binding Remove static Binding Manual Binding</div>				
		IP-based: <input type="text"/>		<input type="button" value="Search"/>
<input type="checkbox"/>	IP	MAC	Type	Action
<input checked="" type="checkbox"/>	10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding
<input checked="" type="checkbox"/>	10.52.24.1	ecb9.70b7.00ee	Static Binding	Remove static Binding

2. Click Remove Static Binding in the Action Column.

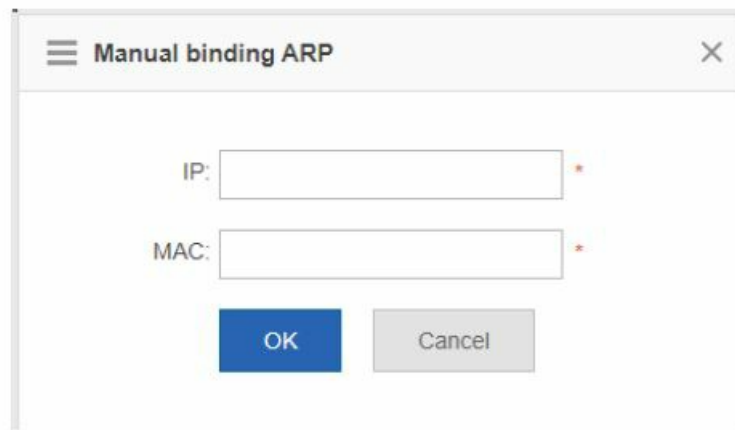
<input type="checkbox"/>	IP	MAC	Type	Action
<input type="checkbox"/>	10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding
<input type="checkbox"/>	10.52.24.1	ecb9.70b7.00ee	Static Binding	Remove static Binding

◦ Manual Binding

1. Click Manual Binding above the list.

ARP Entries				
<div>Dynamic Binding>>Static Binding Remove static Binding Manual Binding</div>				
		IP-based: <input type="text"/>		<input type="button" value="Search"/>
<input type="checkbox"/>	IP	MAC	Type	Action
<input type="checkbox"/>	10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding

2. Enter IP and MAC addresses, and click OK. The entry is displayed in the list



A dialog box titled "Manual binding ARP" with a close button (X) in the top right corner. It contains two input fields: "IP:" and "MAC:", each followed by a text box and a red asterisk indicating a required field. Below the input fields are two buttons: "OK" (blue) and "Cancel" (gray).

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.

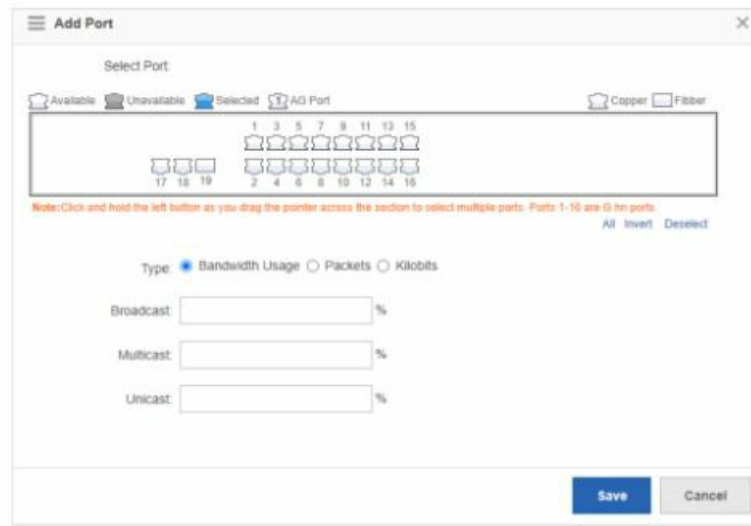
The following figure shows the Storm Control Settings page.

Figure 1-18 Storm Control Settings

Storm Control					
+ Add Port X Delete Selected Port					
	Port	Broadcast	Multicast	Unicast	Action
<input type="checkbox"/>	Gh0/1	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/2	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/3	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/4	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/5	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/6	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/7	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/8	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/9	-	-	-	Edit Delete
<input type="checkbox"/>	Gh0/10	-	-	-	Edit Delete
Show No.: 10 Total Count: 19 First Pre 2 Next Last 					

• 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.



Add Port

Select Port:

Available Unavailable Selected 17 AG Port Copper Fiber

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G hn ports.

All Invert Deselect

Type: ☒ Bandwidth Usage ☐ Packets ☐ Kilobits

Broadcast: %

Multicast: %

Unicast: %

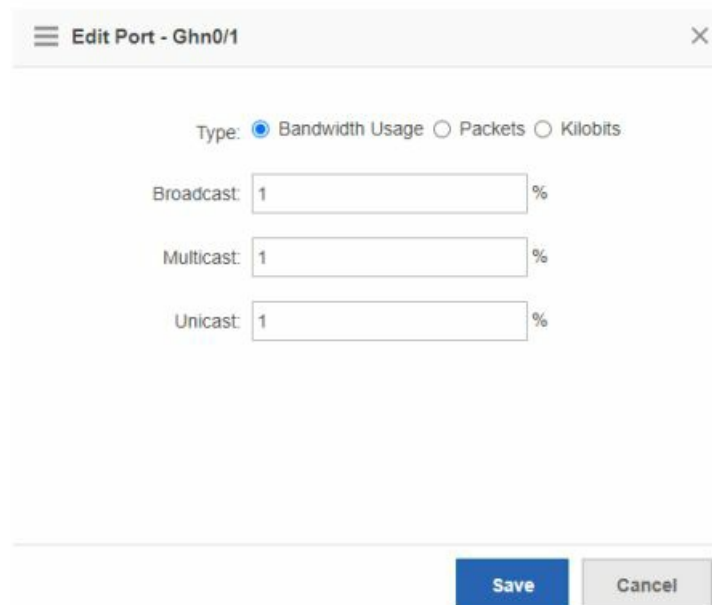
Save Cancel

• Editing Storm Control Ports

After clicking Edit in the Action column, the information of the corresponding storm control port is displayed on the page.

Storm Control					
+ Add Port X Delete Selected Port					
<input type="checkbox"/>	Port	Broadcast	Multicast	Unicast	Action
<input type="checkbox"/>	Ghn0/1	1%	1%	1%	Edit Delete

After editing the information, click Save. The “Configuration succeeded.” message is displayed.



Edit Port - Ghn0/1

Type: ☒ Bandwidth Usage ☐ Packets ☐ Kilobits

Broadcast: %

Multicast: %

Unicast: %

Save Cancel

• Deleting storm control ports

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

Storm Control					
+ Add Port X Delete Selected Port					
<input type="checkbox"/>	Port	Broadcast	Multicast	Unicast	Action
<input checked="" type="checkbox"/>	Ghn0/1	1%	1%	1%	Edit Delete
<input checked="" type="checkbox"/>	Ghn0/2	-	-	-	Edit Delete

- 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.

Storm Control					
+ Add Port X Delete Selected Port					
<input type="checkbox"/>	Port	Broadcast	Multicast	Unicast	Action
<input type="checkbox"/>	Ghn0/1	1%	1%	1%	Edit Delete
<input type="checkbox"/>	Ghn0/2	-	-	-	Edit Delete

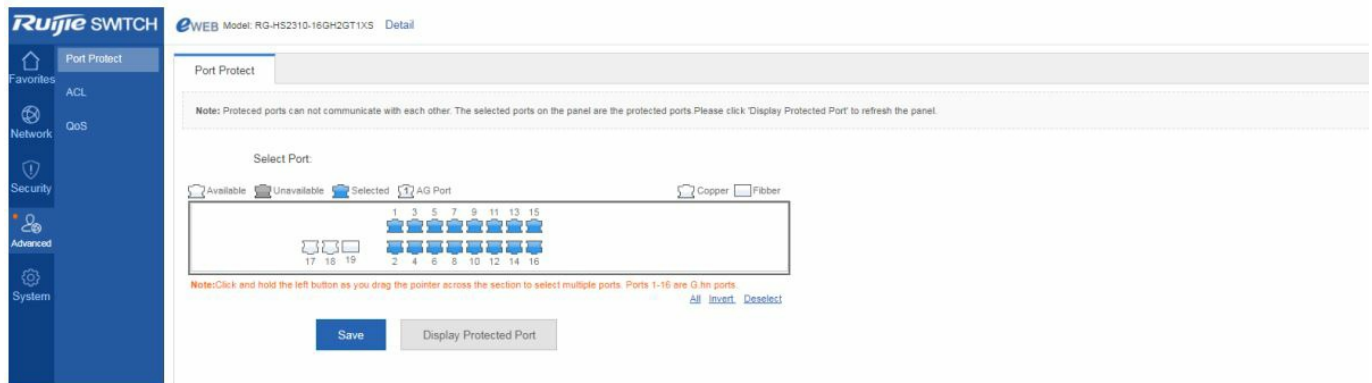
Advanced

Port Protection

In some application environments, it is required that communication be blocked between some ports. For this purpose, you can configure some ports as 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 L3 routing are blocked between protected ports. If a protected port supports both modes, the first mode is used by default.

When an aggregate port is configured as a protected port, all its member ports are configured as protected ports. By default, G.hn ports are set to protected ports. It is recommended that you don't set the G.hn ports to non-protected port. The following figure shows the Port Protect Settings page.

Figure 1-19 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.

ACL

Access control list (ACL) is also called access list or firewall. 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 1-20 ACL List

ACL List										
ACL List: <input type="text"/> Add ACL Delete ACL + Add Access Rule X Delete Selected Access Rule										
<input type="checkbox"/>	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
No Record Found										
Show No.: 10 Total Count: 0 First Pre Next Last 1 GO										

◦ Adding ACLs

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.

Add ACL X

ACL Type: ☒ Standard ACL (Source-address-based Control) ☐ Extended ACL (Flow-based Control)

ACL List: * Both Chinese and English are supported. If you want to configure a number, please make sure that it is in the range of 1-99 or 1300-1999.

OK **Cancel**

ACL List | ACL Time | ACL Application

ACL List: **Add ACL** **Delete ACL** **+ Add Access Rule** **X Delete Selected Access Rule**

	ACL List	Idcard	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
<input type="checkbox"/>	2									

◦ Deleting ACLs

Select the ACL to be deleted from the ACL List drop-down list and click Delete ACL.

ACL List | ACL Time | ACL Application

ACL List: **Add ACL** **Delete ACL** **+ Add Access Rule** **X Delete Selected Access Rule**

	ACL List	Idcard	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
<input type="checkbox"/>	2									

◦ Adding Access Rules

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.

Add Access Rule X

ACL Type: Standard ACL (Source-address-based Control)

ACL List: 2

Access Rule Settings

Access Control: ☒ Permit ☐ Deny Time Period: [Time manager](#)

☐ Any IP: (For all IP)

☐ Single IP: IP:

OK **Cancel**

◦ Editing Access Rules

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.

ACL List ACL Time ACL Application										
ACL List: <input type="text"/> Add ACL Delete ACL + Add Access Rule X Delete Selected Access Rule										
<input type="checkbox"/>	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
<input type="checkbox"/>	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move
Show No.: <input type="text"/> Total Count: 1										

◦ Deleting Access Rules

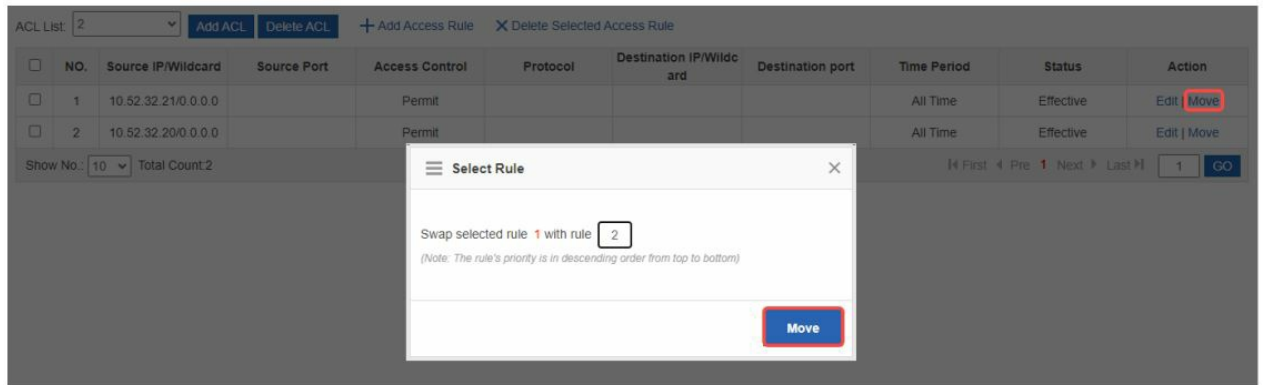
- Multiple access rules from the ACL rule list can be selected. Click Delete Selected Access Rule to batch delete access rules.
- After clicking Delete in the Action column, the “Are you sure you want to delete the access rule?” message is displayed. After confirming the operation, a “Delete succeeded.” message is displayed.

ACL List ACL Time ACL Application										
ACL List: <input type="text"/> Add ACL Delete ACL + Add Access Rule X Delete Selected Access Rule										
<input checked="" type="checkbox"/>	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
<input checked="" type="checkbox"/>	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move
<input checked="" type="checkbox"/>	2	10.52.32.20/0.0.0.0		Permit				All Time	Effective	Edit Move
Show No.: <input type="text"/> Total Count: 2										

◦ Moving Access Rules

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

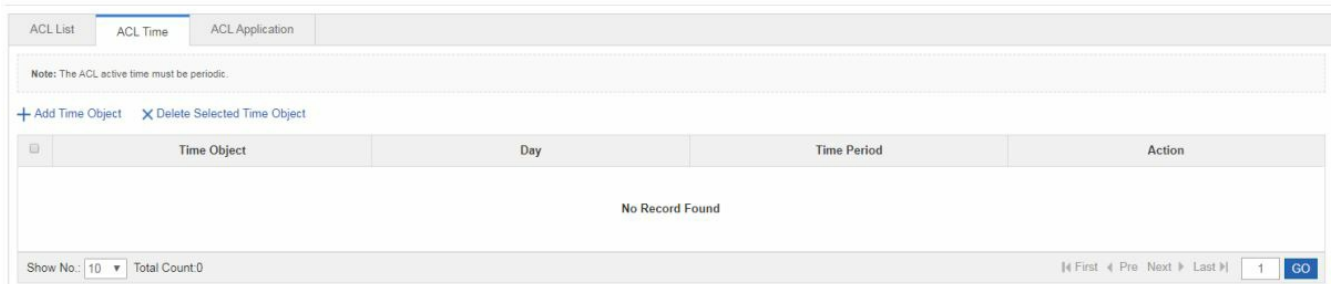
displayed.



- **ACL Time**

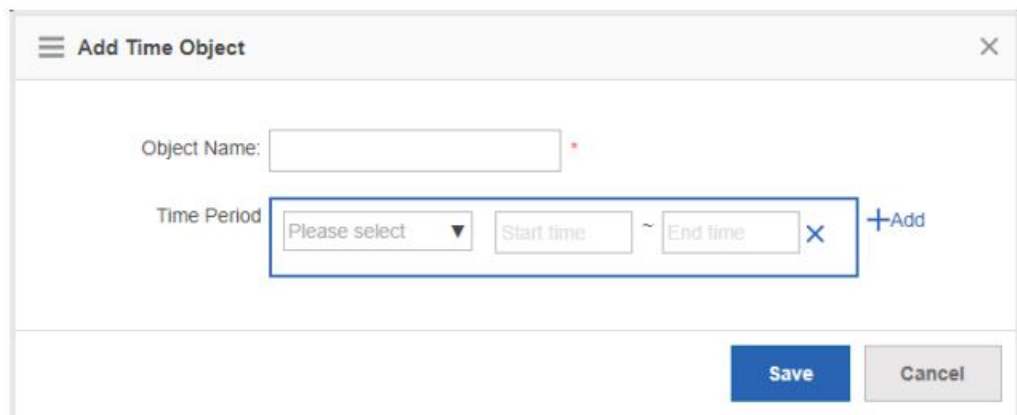
The following figure shows the ACL Time page.

Figure 1-21 ACL Time



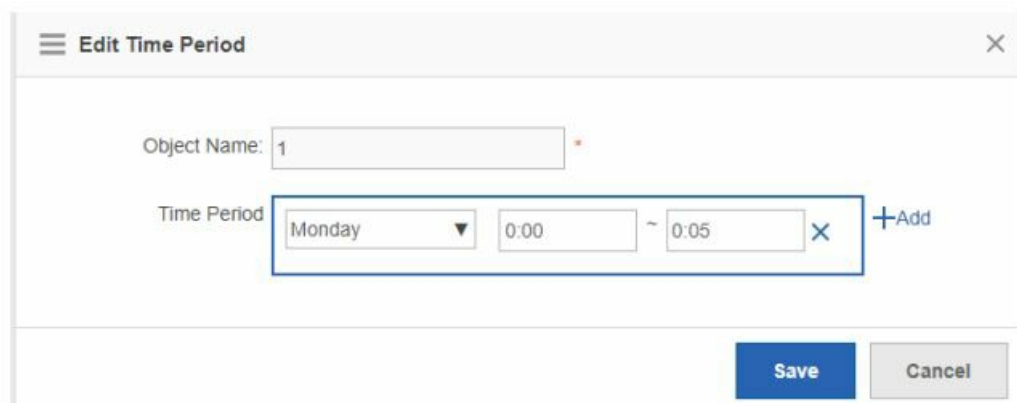
- **Adding ACL Time**

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**

Select multiple time objects in the ACL time list. Click Delete Selected Time Object to batch delete time

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.

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

<input type="checkbox"/>	ACL	Port	Direction	Action
<input type="checkbox"/>	1	Ghn0/1	in	Edit Delete
<input type="checkbox"/>	2	Ghn0/7	in	Edit Delete

Show No.: 10 Total Count: 2 First Pre Next Last 1 [GO](#)

QoS

QoS (Quality of Service) is a set of technologies that work on a network to guarantee its ability to offer good-quality network communications. With the QoS configured in the network environment, it increases the predictability of network performance, makes network bandwidth allocation effective, and uses network resources more rationally.

• Class Settings

The following figure displays the page of Class Settings.

Figure 1-23 Class Settings

Class Settings Policy Settings Flow Settings

Note: Classification is used to identify and mark certain data flows that match the ACL rule.

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

<input type="checkbox"/>	Class Name	ACL	Action
No Record Found			

Show No.: 10 Total Count: 0 First Pre Next Last 1 [GO](#)

◦ Add Class

Click “Add Class”, and specifies the Class Name and ACL List. Then, click “Save”. If the message “Add Succeeded” message is displayed, the configuration is complete.

Add Class

Class Name: * (1-31) Bytes

ACL List: [\[ACL List\]](#)

[Save](#) [Cancel](#)

◦ Delete Class

Select one or multiple classes to be deleted, and then click Delete Selected Class.

Class Settings	Policy Settings	Flow Settings
----------------	-----------------	---------------

Note: Classification is used to identify and mark certain data flows that match the ACL rule.

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

<input checked="" type="checkbox"/>	Class Name	ACL	Action
<input checked="" type="checkbox"/>	1	1	Edit Delete
<input checked="" type="checkbox"/>	3	1	Edit Delete

Show No.: 10 Total Count: 2

First Pre 1 Next Last 1 GO

You also can delete the Delete button in the Action column of a class to be deleted to delete it.

<input type="checkbox"/>	Class Name	ACL	Action
<input type="checkbox"/>	1	1	Edit Delete
<input type="checkbox"/>	3	1	Edit Delete

Show No.: 10 Total Count: 2

First Pre 1 Next Last 1 GO

• Edit Class

Click the Edit button in the Action column of the class to be edited. After editing it, click Save.

Note: Classification is used to identify and mark certain data flows that match the ACL rule.

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

<input type="checkbox"/>	Class Name	ACL	Action
<input type="checkbox"/>	1	1	Edit Delete
<input type="checkbox"/>	3	1	Edit Delete

Show No.: 10 Total Count: 2

Edit Class

Class Name: * (1-31) Bytes

ACL List: [\[ACL List\]](#)

[Save](#) [Cancel](#)

[Edit](#) [Delete](#)

[Edit](#) [Delete](#)

First Pre 1 Next Last 1 GO

• Policy Settings

The following figure displays the Policy Settings page.

Figure 1-24 Policy Settings

Class Settings	Policy Settings	Flow Settings
----------------	-----------------	---------------

Note: The policy is used to constrain the bandwidth that the classified data flow consumes.

Policy List: [Add Policy](#) [Delete Policy](#) [+ Add Policy Rule](#) [X Delete Selected Rule](#)

<input type="checkbox"/>	Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
No Record Found					

Show No.: 10 Total Count: 0

First Pre Next Last 1 GO

• Add a Policy

Click Add Policy. Then, specify the policy name and click Save. If a “Add Succeeded.” message is displayed, the operation is complete.

Add Policy

Policy Name: * (1-31) Bytes

[Save](#) [Cancel](#)

- **Delete Policy**

Select the policy to be deleted, and click Delete Policy.

The screenshot shows the 'Policy Settings' tab with a note: 'The policy is used to constrain the bandwidth that the classified data flow consumes.' Below the note, there is a 'Policy List' dropdown set to '1'. To its right are buttons: 'Add Policy', 'Delete Policy' (highlighted with a red box), '+ Add Policy Rule', and 'X Delete Selected Rule'. Below these buttons is a table with columns: Class Name, Bandwidth (KBps), Burst Traffic (KBytes), Bandwidth Violation Disposal, and Action. The table is currently empty, displaying 'No Record Found'.

- **Add Policy Rule**

Click Add Policy Rule to add a rule for a policy. Specify the policy name, bandwidth, burst traffic, limit violation disposal and class list, and then click Save.

The 'Add Policy Rule' dialog box contains the following fields: 'Policy Name' (value: 1, limit: * (1-31) Bytes), 'Bandwidth' (empty, limit: * (16-10000000) KBps), 'Burst Traffic' (empty, limit: * (1-8192) KBytes), 'Limit Violation Disposal' (radio buttons for 'Drop' (selected) and 'DSCP Priority' (empty, limit: * (0-63))), and 'Class List' (dropdown menu with value: 1). At the bottom right are 'Save' and 'Cancel' buttons.

- **Delete Policy Rule**

Click the policy rule to be deleted, and then click Delete Selected Rule.

The screenshot shows the 'Policy Settings' tab with the same note as before. The 'Policy List' dropdown is set to '1'. The buttons are 'Add Policy', 'Delete Policy', '+ Add Policy Rule', and 'X Delete Selected Rule' (highlighted with a red box). Below the buttons is a table with columns: Class Name, Bandwidth (KBps), Burst Traffic (KBytes), Bandwidth Violation Disposal, and Action. The table contains one record with Class Name '1', Bandwidth '20', Burst Traffic '56', and Disposal 'Drop'. The 'Action' column has 'Edit' and 'Delete' buttons. Below the table, there is a 'Show No.' dropdown set to '10' and 'Total Count: 1'. At the bottom right are navigation buttons: 'First', 'Pre', 'Next', 'Last', and a 'GO' button.

- **Flow Settings**

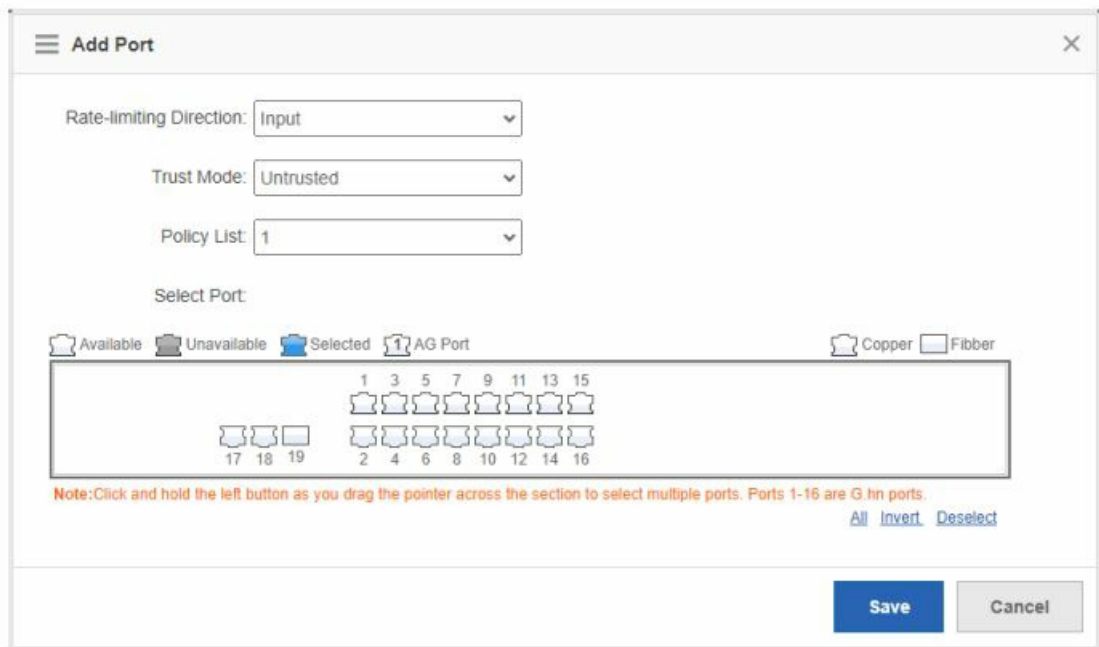
The following page displays the Flow Settings.

Figure 1-25 Flow Settings

The screenshot shows the 'Flow Settings' tab with a 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).' Below the note are buttons: '+ Add Port' and 'X Delete Selected Port'. Below these buttons is a table with columns: Port, Direction, Policy Name, Trust Mode, and Action. The table is empty, displaying 'No Record Found'. At the bottom, there is a 'Show No.' dropdown set to '10' and 'Total Count: 0'. At the bottom right are navigation buttons: 'First', 'Pre', 'Next', 'Last', and a 'GO' button.

- **Add Ports**

Click Add Port to apply a policy to the port. Then, specify the rate-limiting direction, the trust mode, the policy list and select the port to which the policy is applied. Afterwards, click Save.



Add Port

Rate-limiting Direction:

Trust Mode:

Policy List:

Select Port:

Available Unavailable **Selected** 1 AG Port Copper ☐ Fiber ☐

17 18 19 1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 16

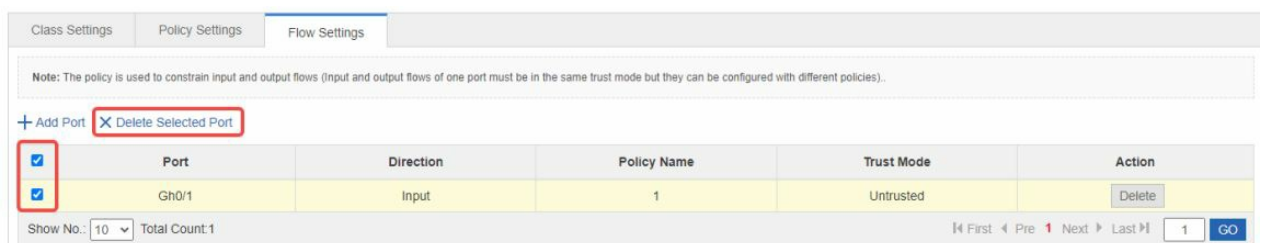
Note: Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G.hn ports.

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

Save **Cancel**

- **Delete Ports**

Click the ports to be deleted, and click Delete Selected Port to delete the port to which the policy is applied.



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).

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

	Port	Direction	Policy Name	Trust Mode	Action
<input checked="" type="checkbox"/>	Gh0/1	Input	1	Untrusted	Delete

Show No.: Total Count: 1

First Pre 1 Next Last 1 **GO**

System

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

System Settings

Five tab pages are available on the system setting page: System Time, Password, Restart, Reset, Web Access Control and SNMP.

- **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 1-26 System Time

Ruijie SWITCH eWEB Model: RG-HS2310-16GH2GT1XS Detail

System Time Password Reset Web Access Control SNMP

Current Time: 1970-1-1-10:06:32


Reset Time: 2023-9-27 16:47

Time Zone: UTC+8(CCT)

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

Save

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 1-27 Password

Ruijie SWITCH eWEB Model: RG-HS2310-16GH2GT1XS Detail

System Time Password Reset Web Access Control SNMP

Web Management Password

Username: admin

Old Password *

New Password *

Confirm Password *

Save

- **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.

System Time Password Reset Web Access Control SNMP

Web Management Password


Username: admin

Old Password *

New Password *

Confirm Password *

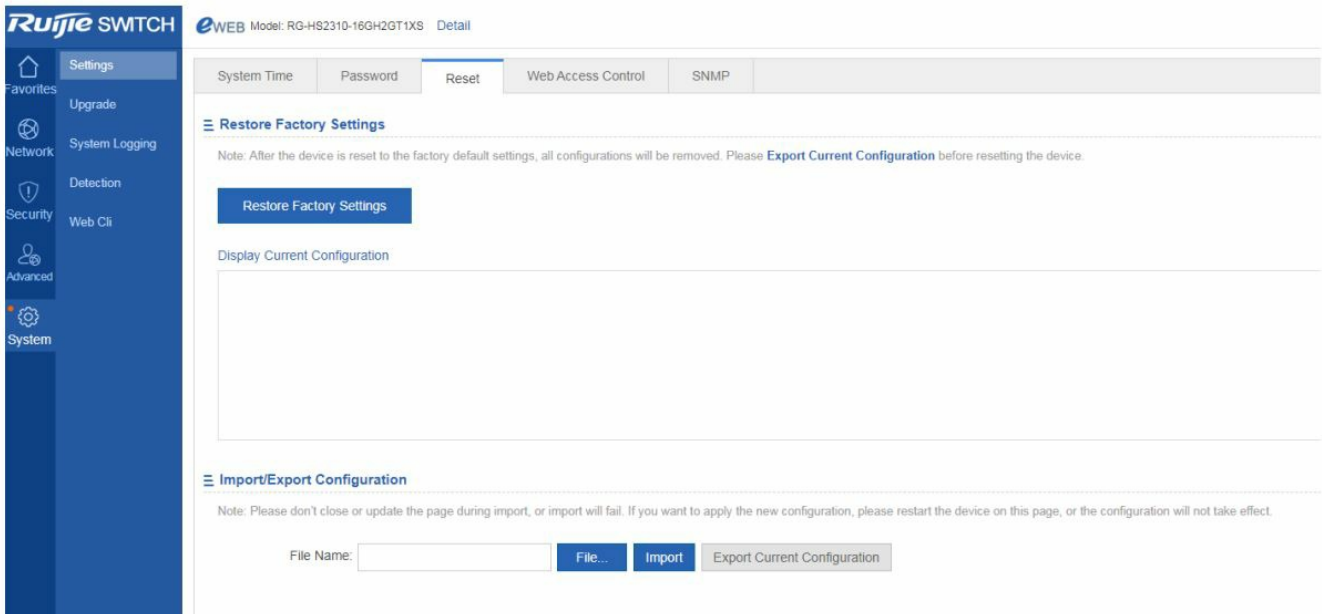
Save

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

- **Restore Factory Settings**

The following figure shows the Reset page.

Figure 1-28 Reset



- **Importing/Exporting Configurations**

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

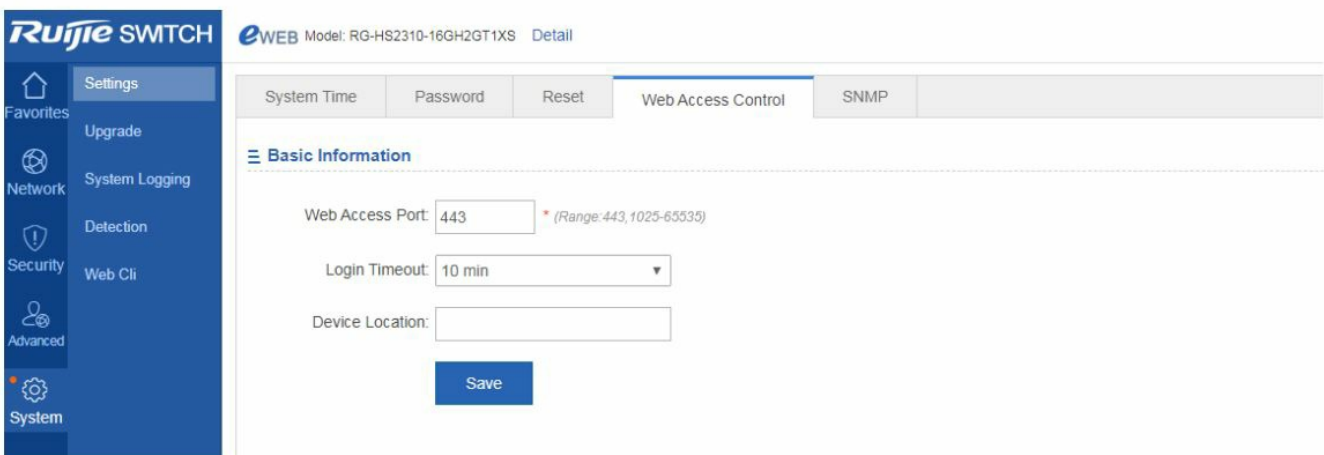
- **Restoring Factory Settings**

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

- **Web Access Control**

The following figure shows the Web Access Control page.

Figure 1-29 Web Access Control



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 1-30 SNMP

The screenshot shows the Ruijie SWITCH eWEB interface for the RG-HS2310-16GH2GT1XS model. The left sidebar contains navigation icons for Favorites, Network, Security, Advanced, and System. The main menu on the left lists Settings, Upgrade, System Logging, Detection, Web Cli, Security, Advanced, and System. The top navigation bar includes System Time, Password, Reset, Web Access Control, and SNMP. The SNMP configuration page displays a note: "Note: Either SNMPv2 or SNMPv3 is supported". Below this, there are radio buttons for SNMP Version (v2 is selected). Fields for Device Location, SNMP Community, and Trap Community are present, with a note that the Trap Community must be the same as the SNMP Community. A large text area for Trap Recipient Address is also shown, with a note that up to 9 trap recipients can be configured. A Save button is located at the bottom.

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.

System Upgrade

- Local Upgrade

The following figure shows the local Upgrade page.

Figure 1-31 Upgrade Locally

The screenshot shows the Ruijie SWITCH eWEB interface for the RG-HS2310-16GH2GT1XS model. The left sidebar contains navigation icons for Favorites, Network, Security, Advanced, and System. The main menu on the left lists Settings, Upgrade, System Logging, Detection, Web Cli, Security, Advanced, and System. The top navigation bar includes Upgrade Local and Upgrade. The Upgrade Local page displays a note: "Note: Please download the corresponding software version from the official website , and then upgrade the device with the following tips." Below this, there are tips for upgrading. A File Name field and File..., Upgrade, and Cancel buttons are at the bottom.

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

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 1-32 Log Server Settings

The screenshot shows the 'Log Server Settings' page. The sidebar on the left contains a 'System' icon at the bottom. The main area has two tabs: 'Log Server Settings' (active) and 'Display System Log'. A note at the top states: 'Note: Logging is rated on 8 different levels: 0-Emergency, 1-Alert, 2-Critical, 3-Error, 4-Warning, 5-Notification, 6-Informational, 7-Debugging. The smaller the number, the higher the level.' Below this, the 'Server Logging' toggle is turned 'ON'. The 'Server IP' field is empty. The 'Logging Level' dropdown is set to 'Informational(6)'. A 'Save' button is located at the bottom of the settings area.

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 1-33 Display System Log

The screenshot shows the 'Display System Log' page. The sidebar is the same. The main area has two tabs: 'Log Server Settings' and 'Display System Log' (active). The active tab shows a 'System Log (Show the last 200 logs)' section with an 'Update Log' button. Below this, a text box displays the following log information:
Syslog logging: enabled
Console logging: level debugging, 29 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 29 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, 29 message lines logged,0 fail
Log Buffer (Total 131072 Bytes): have written 2636,
*Jan 1 08:05:20: %SYS-5-CONFIG_I: Configured from console by console
*Jan 1 08:54:31: %DHCP_CLIENT-6-ADDRESS_ASSIGN: Interface VLAN 1 assigned DHCP address 10.52.25.77, mask 255.255.248.0.
*Jan 1 08:54:26: %SYS-5-CONFIG_I: Configured from console by console
*Jan 1 08:20:47: %SYSLOG-6-DEBUG_PRINT: The debug print time 20 minutes has expired!
*Jan 1 08:03:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface Gbn 0/5, changed state to up.
*Jan 1 08:03:02: %LINK-3-UPDOWN: Interface Gbn 0/5, changed state to up.
*Jan 1 08:03:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface Gbn 0/2, changed state to up.
*Jan 1 08:03:02: %LINK-3-UPDOWN: Interface Gbn 0/2, changed state to up.

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

Network Detection

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

- **Ping**

The ping tool sends an Internet Control Message Protocol (ICMP) Request message to the destination host to request 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 1-34 Ping

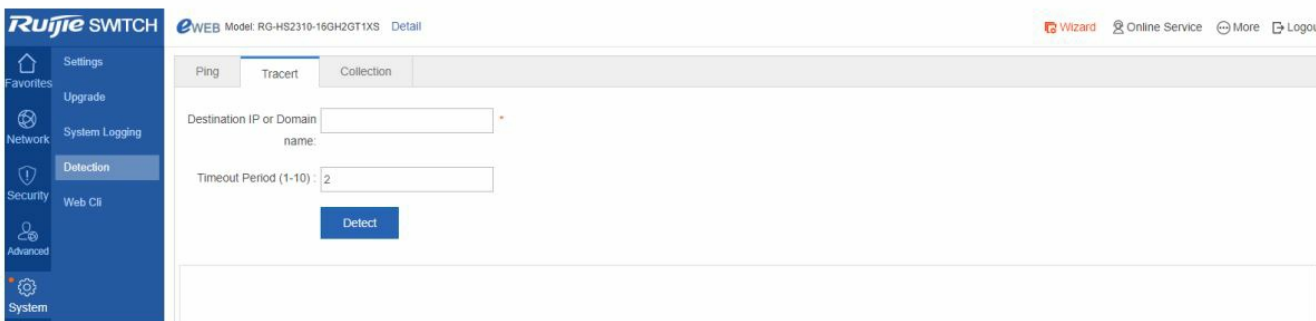


Input the destination IP address and click Detect. The detection result is then displayed in the text box.

- **Tracert**

The tracert tool sends ICMP (Internet Control Message Protocol) messages to the destination hosts to request a ICMP Echo Reply messages to identify all next hops of two devices.

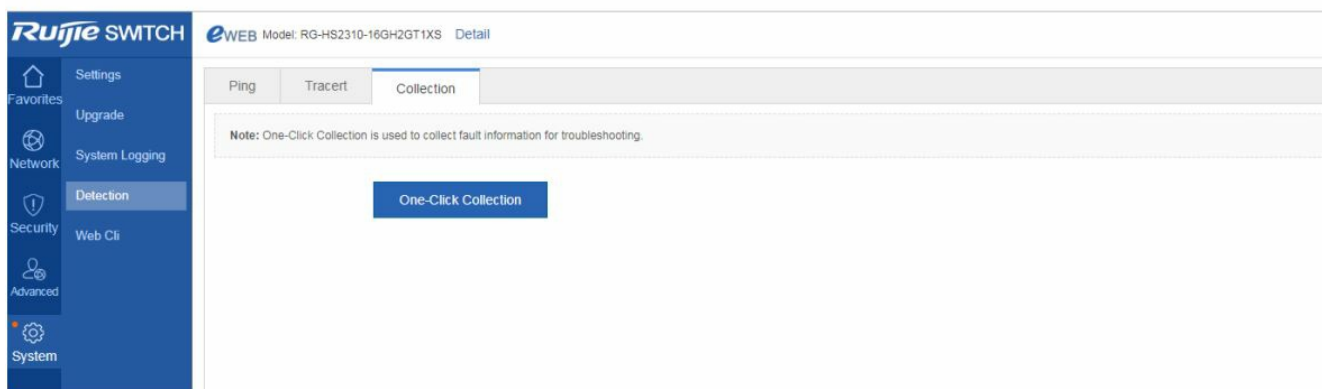
Figure 1-35 Tracert



- **Collection**

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

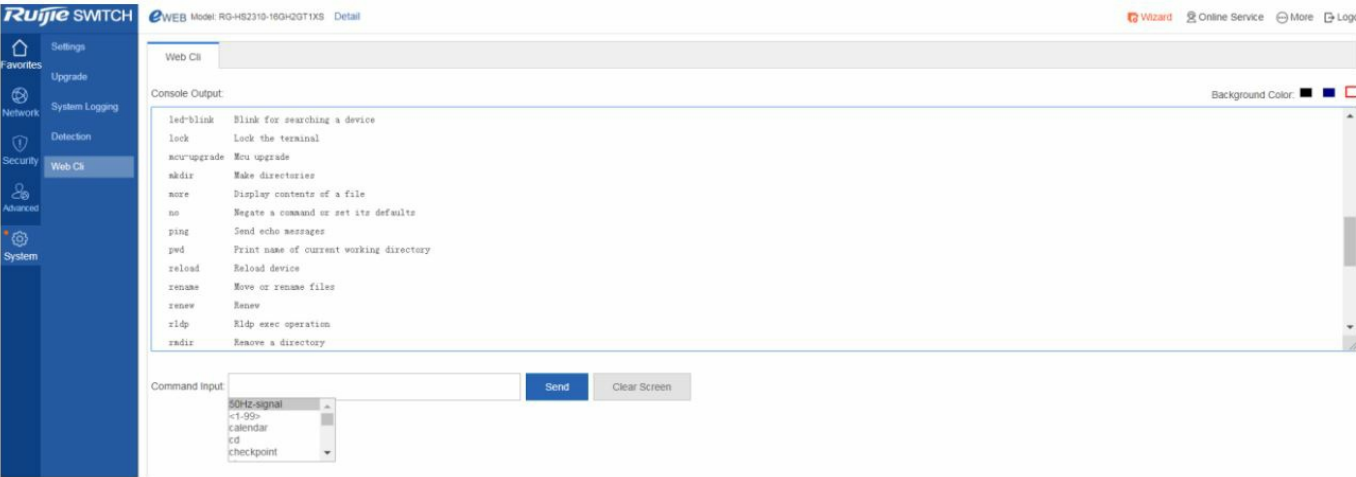
Figure 1-36 One-click Collection



Web CLI

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

Figure 1-37 Web CLI



Document Version: V1.0
Date: 2023.12.08
Copyright © 2023 Ruijie Networks

Documents / Resources

[Ruijie Networks HS2310 Main Telephone Line Unit](#) [pdf] User Guide
HS2310 Main Telephone Line Unit, HS2310, Main Telephone Line Unit, Telephone Line Unit, Line Unit

References

- [R csm](#)
- [R csm](#)
- [R ruijienetworks](#)
- [R ruijienetworks](#)
- [R Support | Ruijie](#)
- [R Ruijie Networks | Network Devices and Solutions Provider](#)
- [User Manual](#)