HS2310-16GH2GT1XS

Web-based Configuration Guide

Document Version: V1.0

Date: 2023.12.08

Preface

Thank you for using our products. This manual matches the RGOS Release RGOS 11.4(1)B90.

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

Glossary

- G.hn

  Gigabit Home Networking (G.hn) is defined to operate over ant physical networking medium in the home, such as power cables, coaxial cables and twisted pair cables. G.hn can be operated over existing physical cable to provide end users with ultra-fast and reliable network connectivity.

- DM

  A Domain Master (DM) is responsible for the operation of all nodes in a domain, such as device access, bandwidth reservation, registration, and management service for other domains.

- 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.

Contents

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 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.

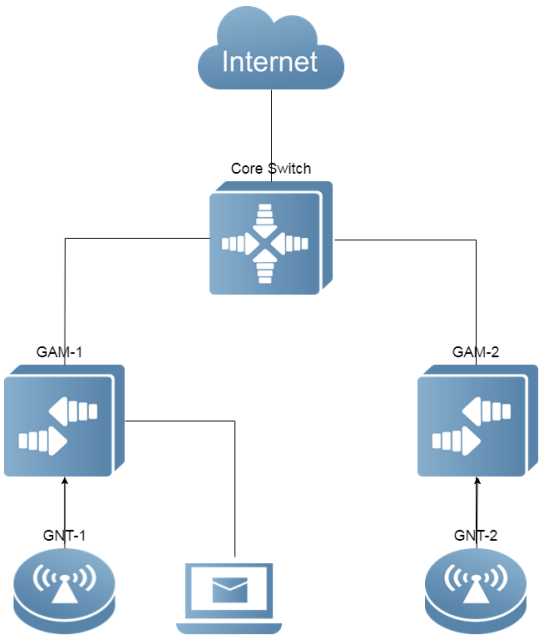
Currently, this file is applicable to only switches.

1.2 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.

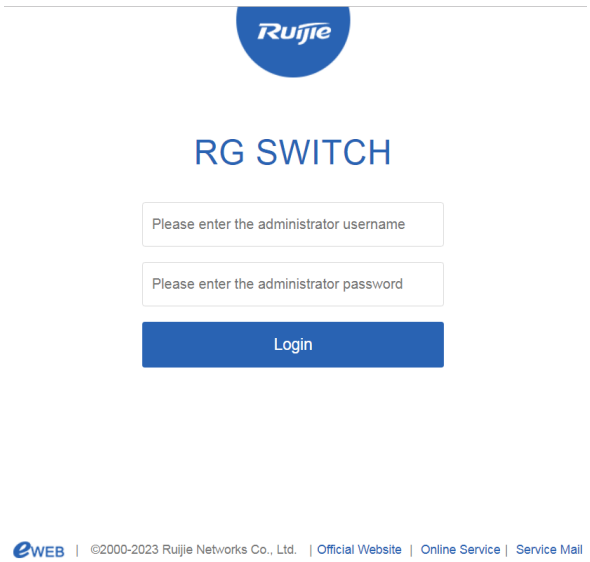
Web configuration and CLI configuration can be performed synchronously.

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



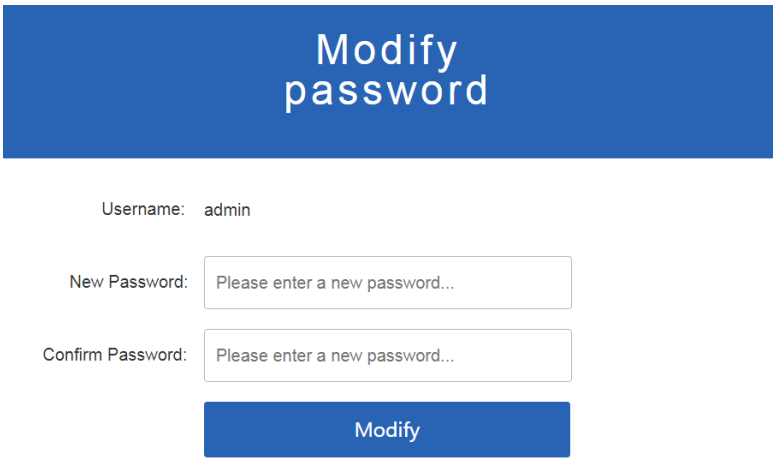
After typing the username and password, click Login. The following table lists the default username and password.

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.

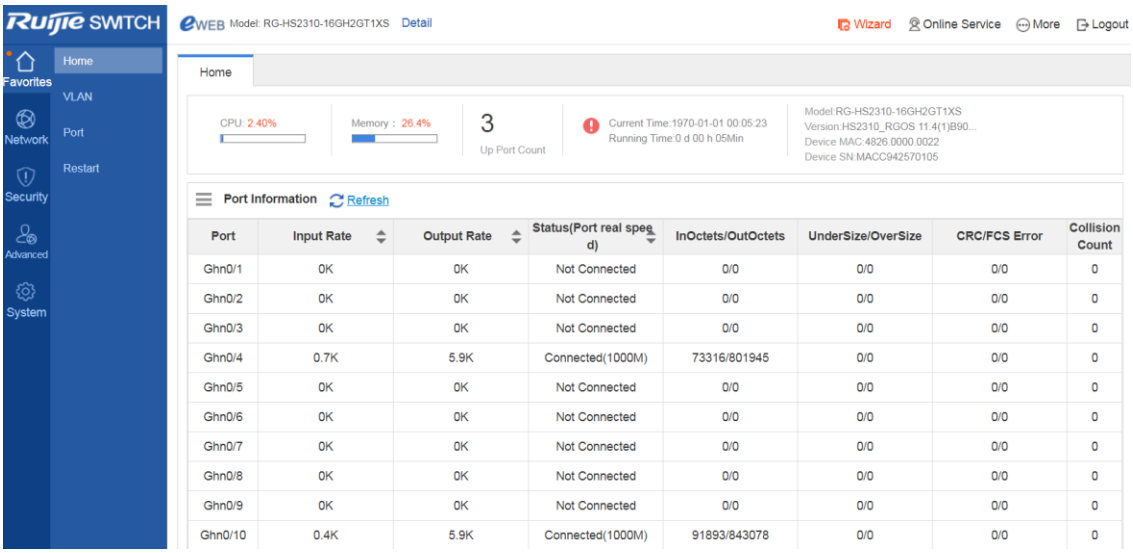
You will be required to modify the password if logging in with the default username and password.

Figure 1-3 Modify Password



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.

1.3 Web Management System

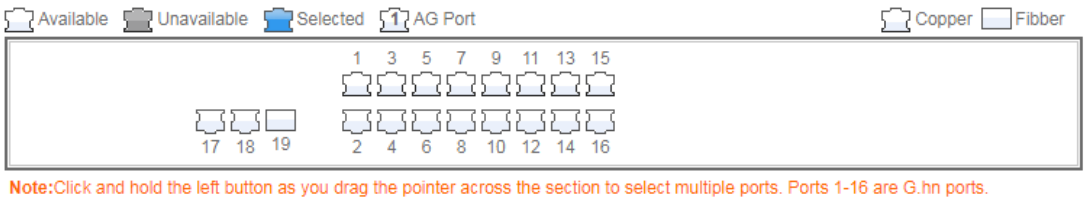
Basic Concepts

Icons and Buttons on the Web-GUI

Icon/Button	Note
Edit	Edit button. Click this icon to edit the currently selected item.
Delete	Delete button.
ON	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.
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.

System Operations

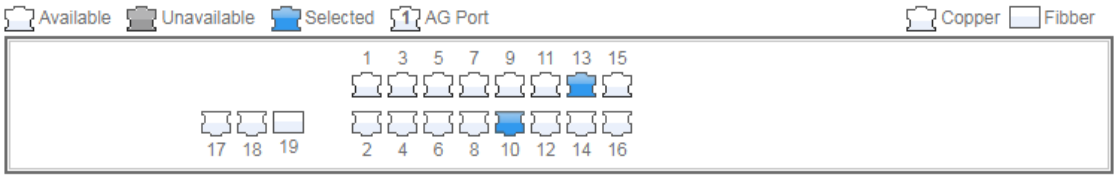
■ Standalone Device Panel



■ 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



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

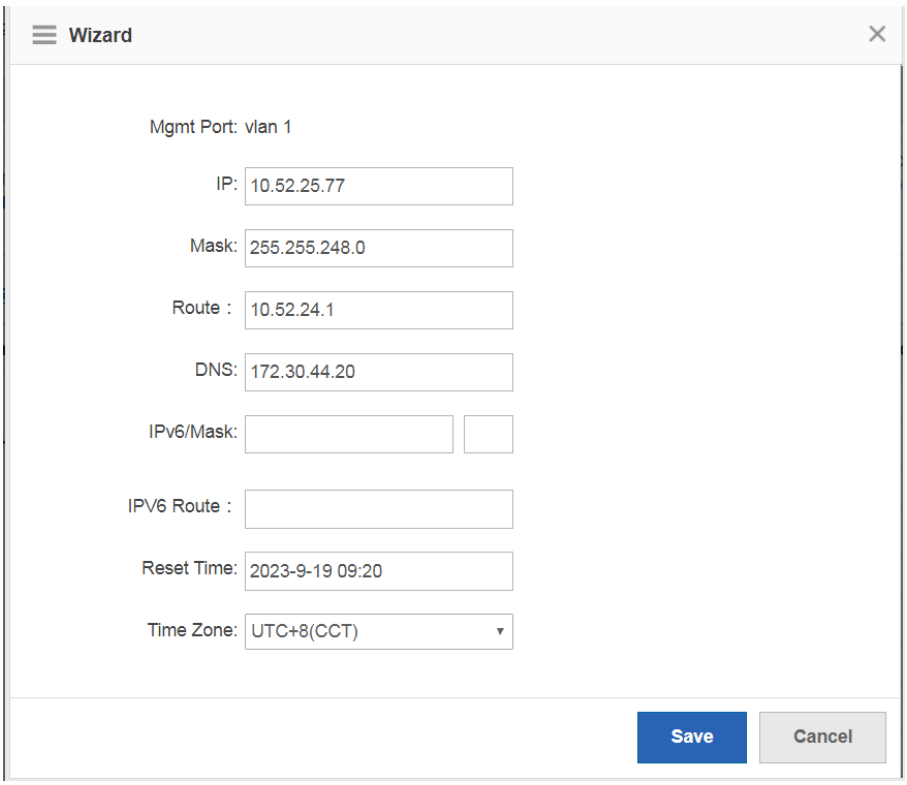
The following table describes the functions in the secondary menu on the left of the Web page.

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.

1.3.1 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



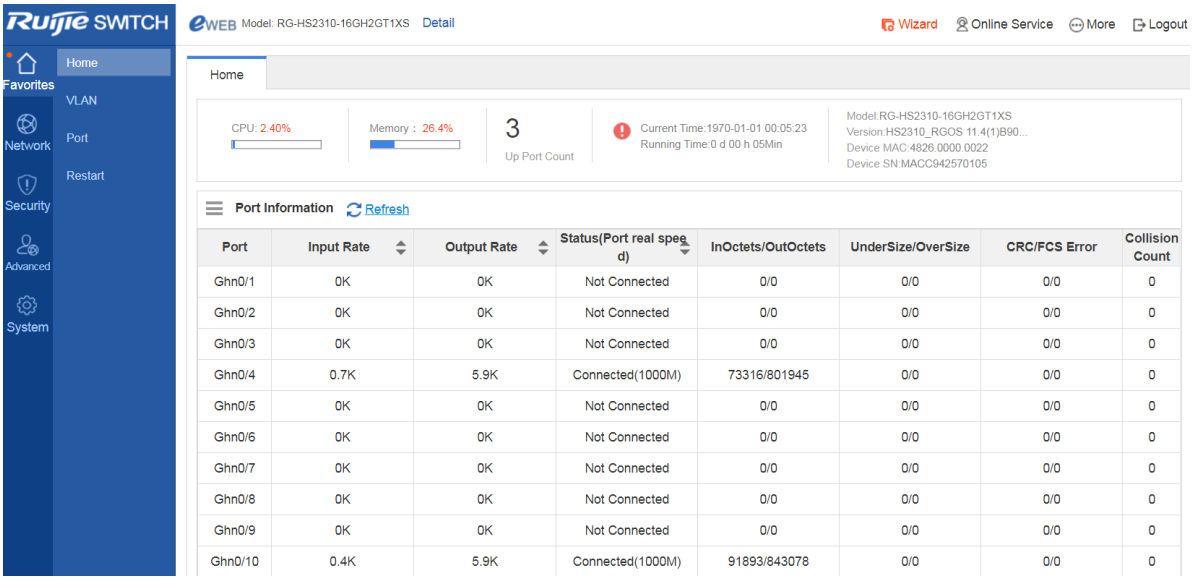
1.3.2 Favorites

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

1.3.2.1 Home Page

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

Figure 1-6 Home Page



Port	Input Rate	Output Rate	Status(Port real speed)	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count
Ghn0/1	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/2	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/3	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/4	0.7K	5.9K	Connected(1000M)	73316/801945	0/0	0/0	0
Ghn0/5	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/6	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/7	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/8	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/9	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/10	0.4K	5.9K	Connected(1000M)	91893/843078	0/0	0/0	0

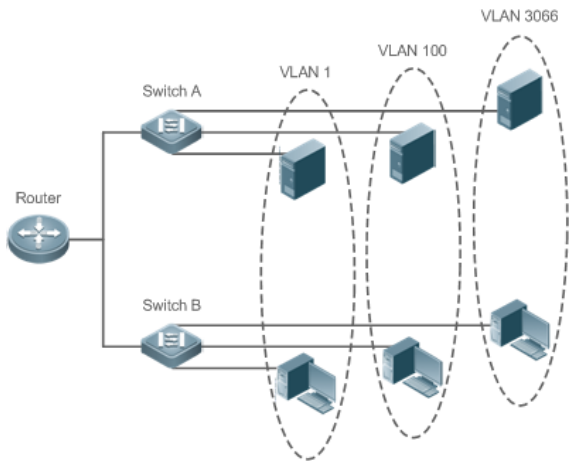
1.3.2.2 VLAN

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 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.

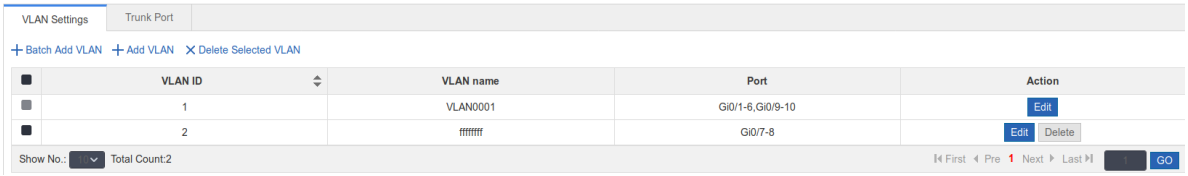
A trunk port can belong to multiple VLANs that receives and sends frames belonging to multiple VLANs.

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



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.

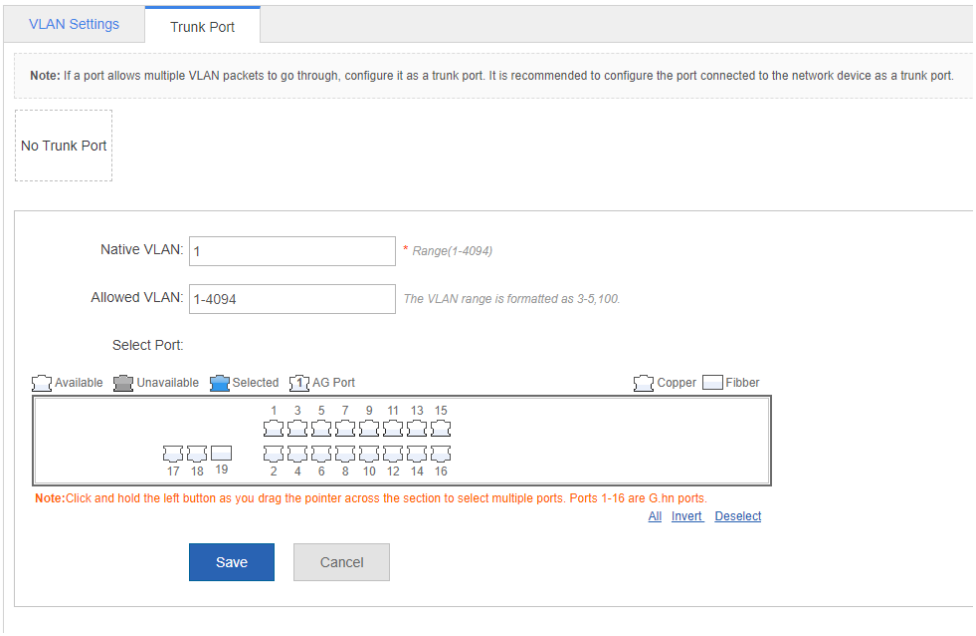
(2) After confirming the operation, the message, “Delete succeeded.” is displayed. VLAN 1 is the default VLAN and cannot be deleted.

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



Adding a Trunk Port

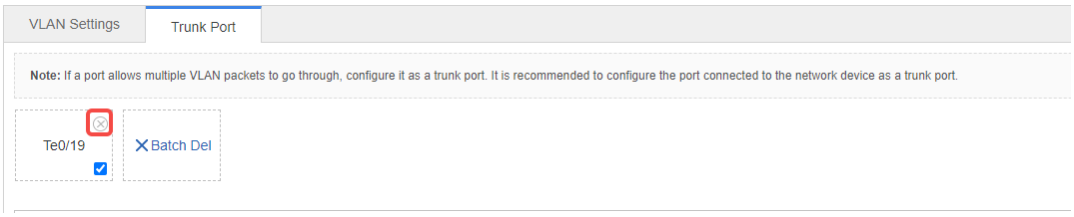
Select a port on the panel, specify Native VLAN and Allowed VLAN (for example, 3-5, 8, and 10), and click Save. The “Configuration succeeded.” message is displayed. In this case, the newly added trunk port is displayed in the trunk port list. Native VLAN must be set when the Allow VLAN is configured,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



Deleting Trunk Ports in Batches

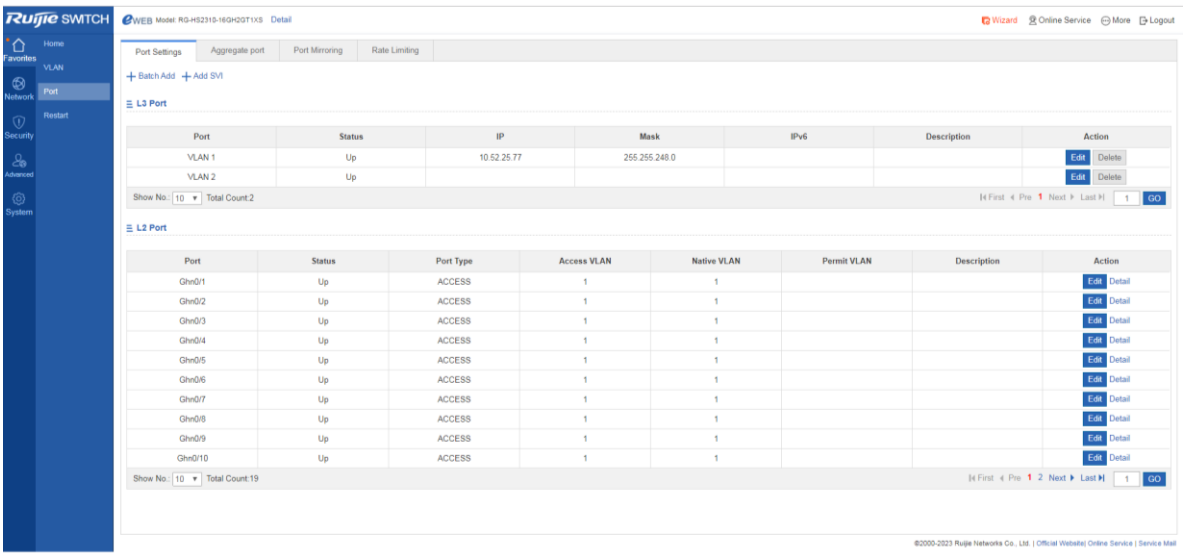
After selecting the trunk ports to be deleted in the trunk port list, click Batch Del. The message, “Are you sure you want to delete the trunk ports?” is displayed. After confirming the operation, a “Delete succeeded.” message is displayed.

1.3.2.3 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.

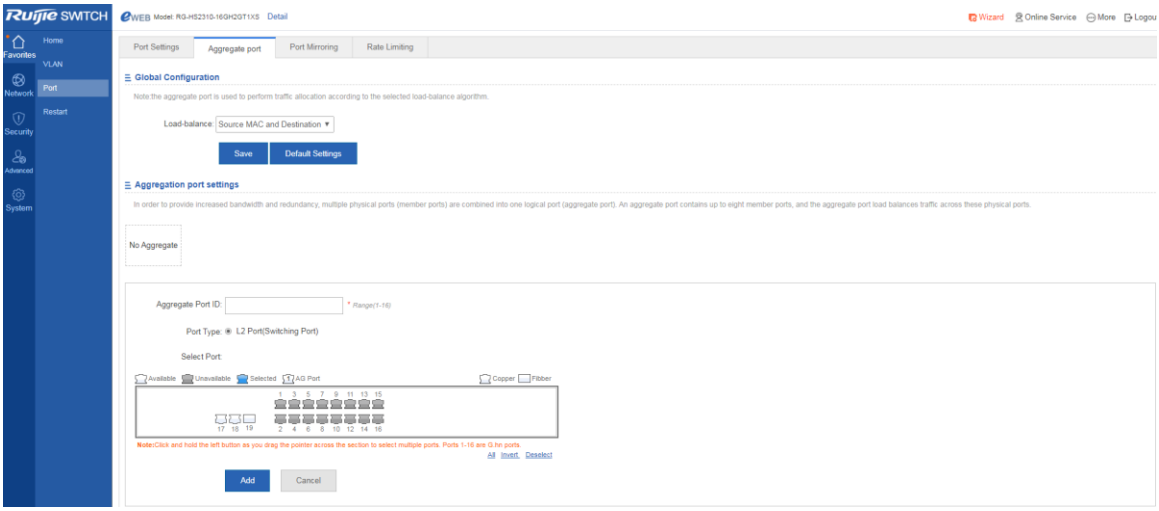
- Deleting L3 port

  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

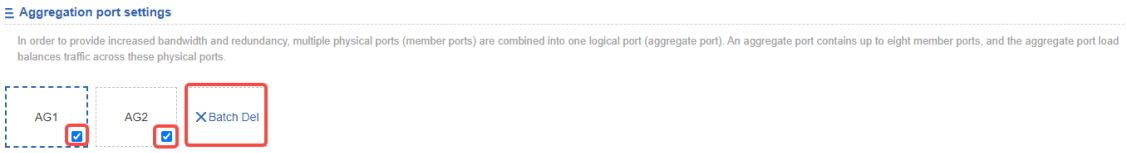
The aggregate ports displayed on the panel are unavailable ports. To edit them, you can click a certain aggregate port in the aggregate port list. Afterwards, the member port becomes a selected port. Click this port to deselect it. Afterwards, you can click Edit to modify the aggregate port.

- 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.



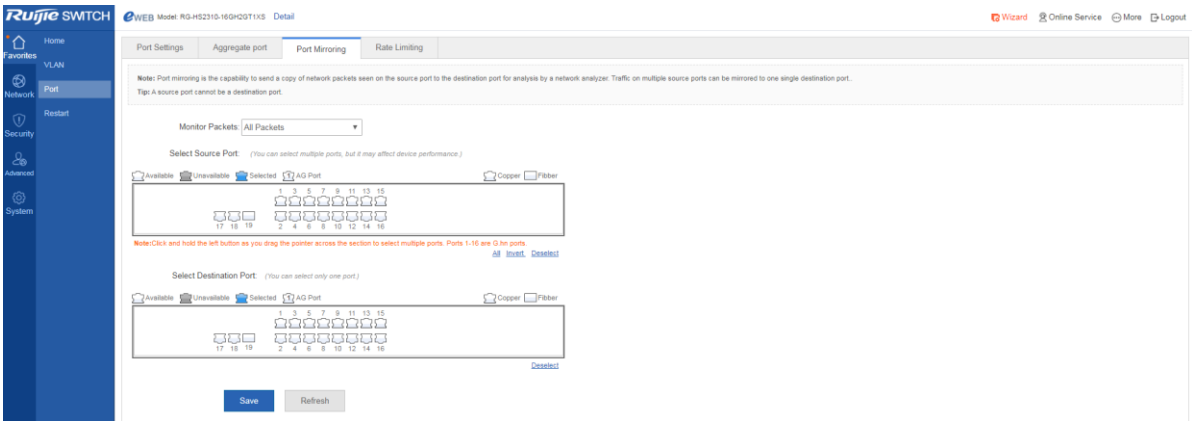
The port enabled with ARP check, anti-ARP-spoofing, or MAC VLAN and the monitoring port in port mirroring cannot be added to the aggregate port. They are displayed as unavailable ports on the panel. After the cursor is moved to an unavailable port, a message is displayed to indicate that a function has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

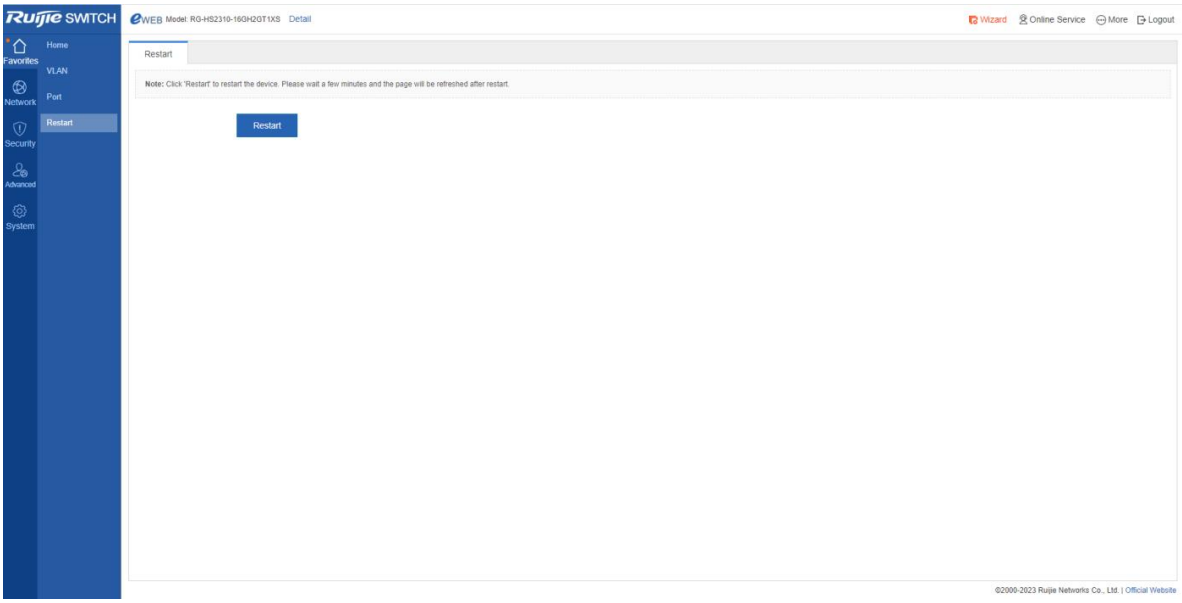
The current port mirroring status is displayed on the panel, which is in edit state. If you do not want to edit a port after modifying it, click Refresh to make the panel display the current status of port mirroring.

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.

1.3.2.4 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.

1.3.3 Network

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

1.3.3.1 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 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.

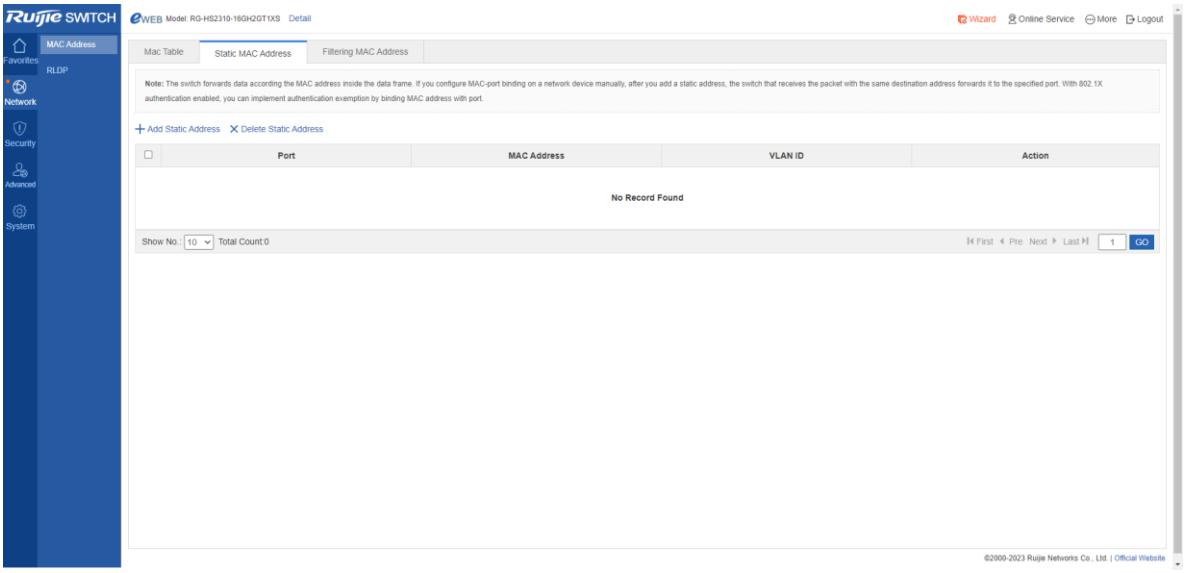
A filtering address is a manually configured MAC address. When a device receives the packets from a filtering address, it will directly discard them. You can only manually add and delete a filtering address rather than age it out. A filtering address is stored in the configuration file and will not be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

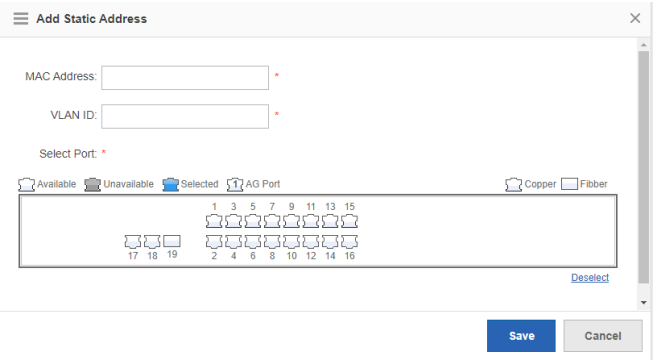
Static Address Settings

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.



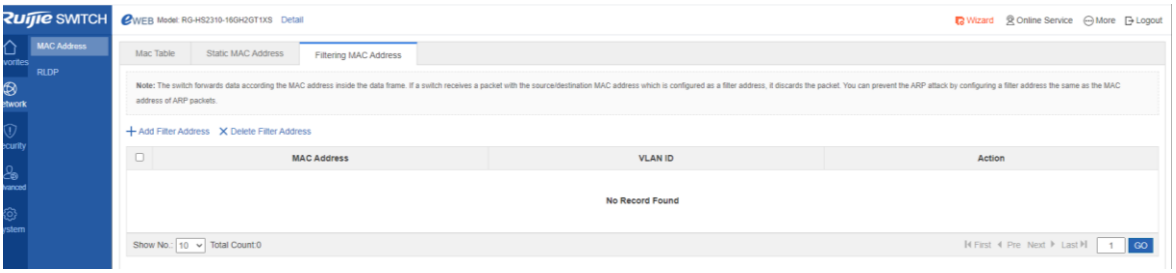
■ Deleting a Static Address

(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.

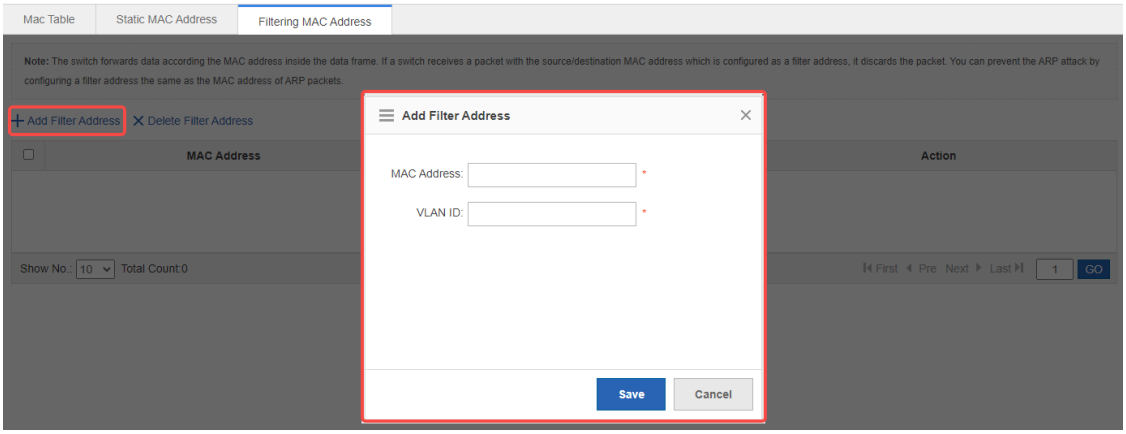
Filtering Address Settings

Figure 1-15 Filtering Address Settings



■ 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.

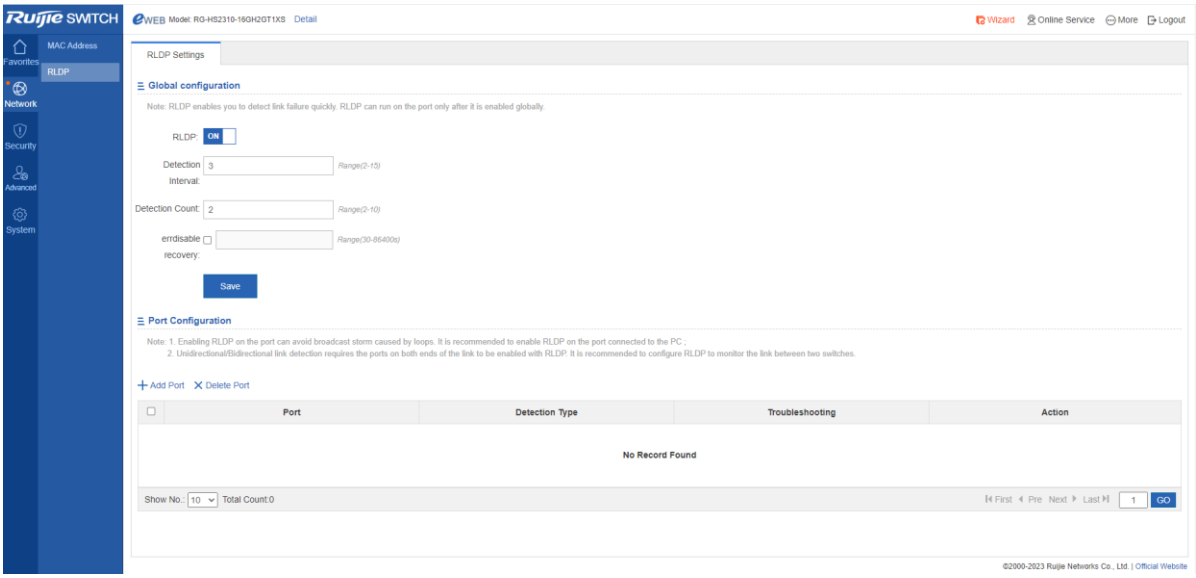
1.3.3.2 RLDP

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.

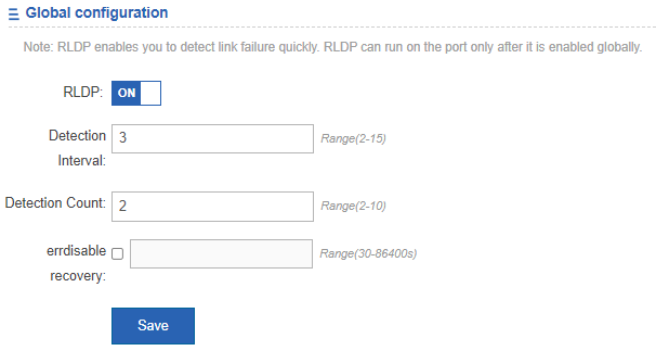
RLDP Settings

Figure 1-16 RLDP Settings



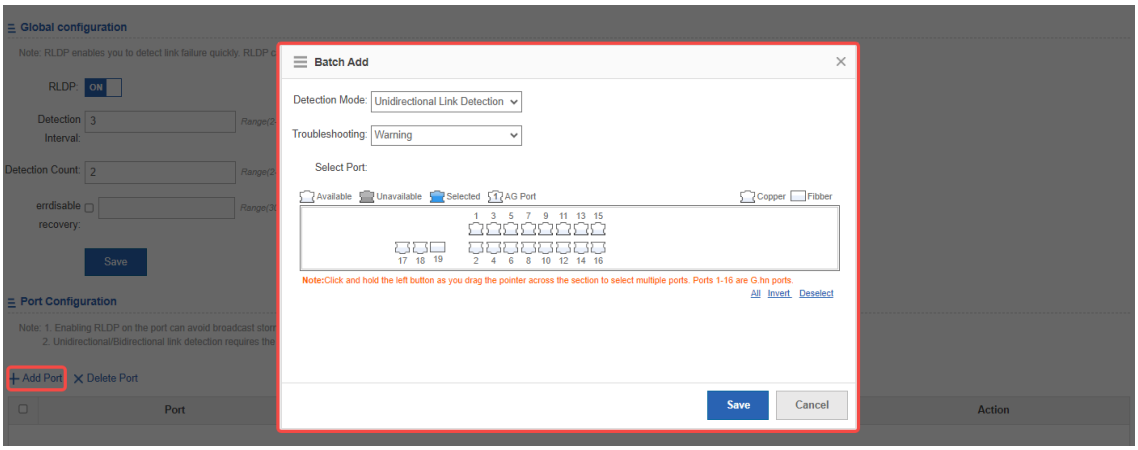
- Global Configuration

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



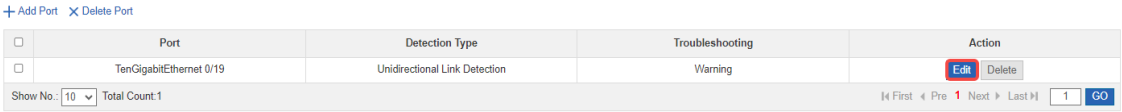
- Adding RLDP Ports

  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

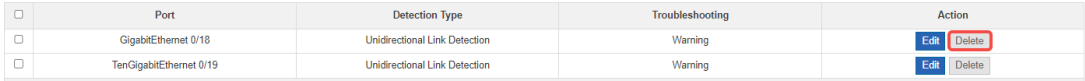
After clicking Edit in the Action column, the information of the corresponding RLDP port is displayed on the page. After editing the information, click Save. An “Edit succeeded.” message is displayed.



■ 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.



1.3.4 Security

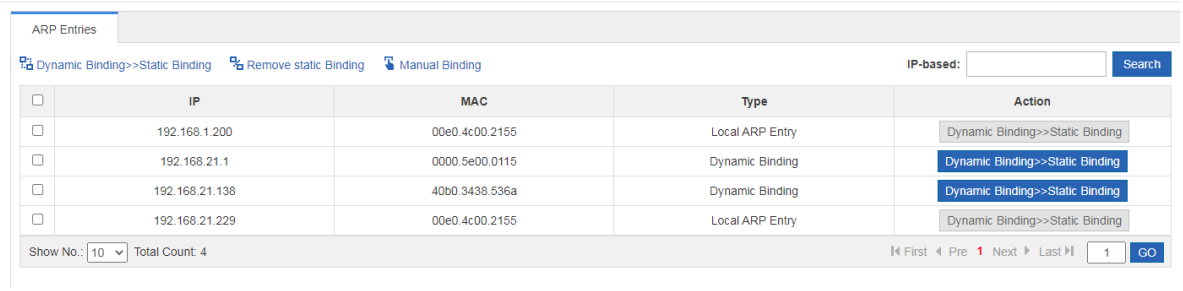
Secondary menus are accessed through the primary Security menu that includes Anti-ARP-Attack and Storm Control.

1.3.4.1 Anti-ARP-Attack

You can check ARP entries and bind static addresses.

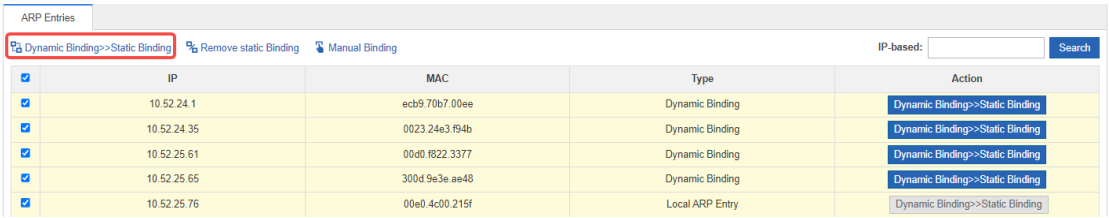
↘ ARP Entries

Figure 1-17 ARP Entries

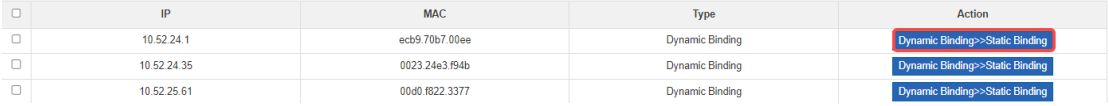


■ Dynamic Binding > Static Binding

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

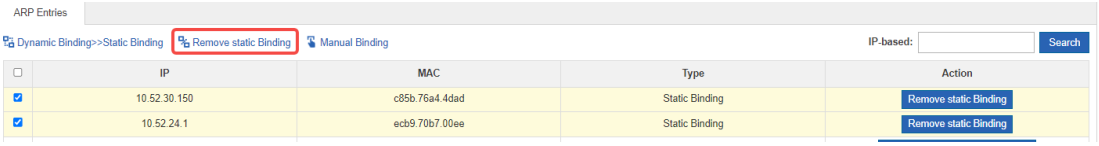


(2) Click Dynamic Binding >> Static Binding in the Action Column.

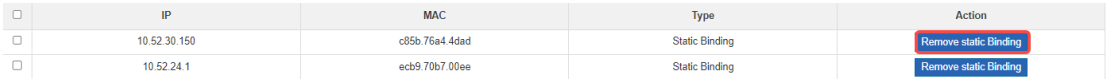


■ Remove Static Binding

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

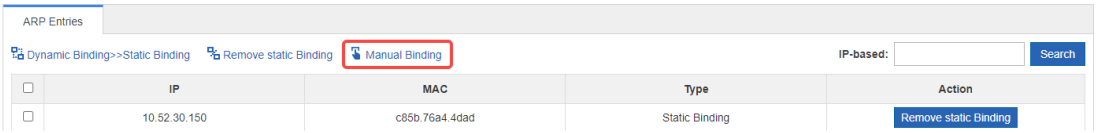


(2) Click Remove Static Binding in the Action Column.

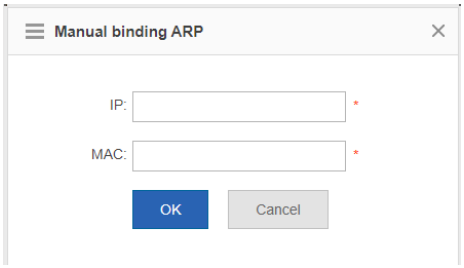


■ Manual Binding

(1) Click Manual Binding above the list.



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



1.3.4.2 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.

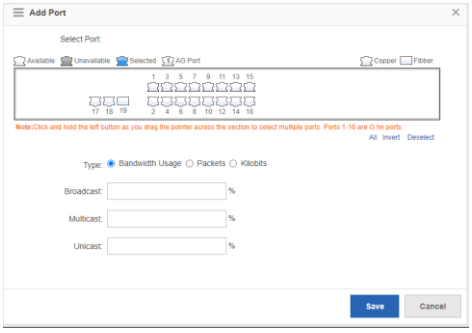
Storm control can be implemented to limit broadcast data flows, multicast data flows, or unknown unicast data flows. If the rate of data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted 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

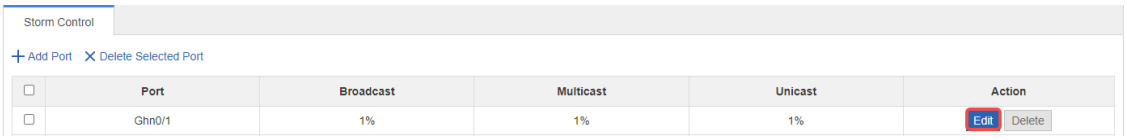
■ Adding storm control ports

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.

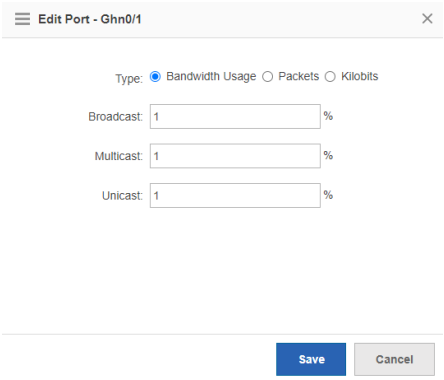


■ Editing Storm Control Ports

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

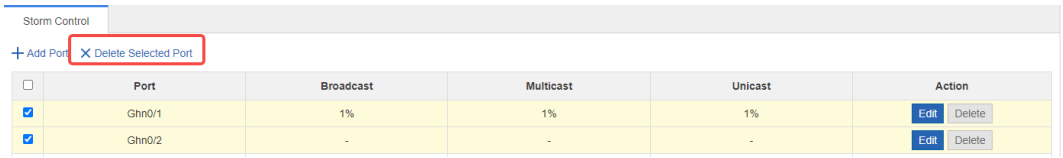


After editing the information, click Save. The “Configuration succeeded.” message is displayed.

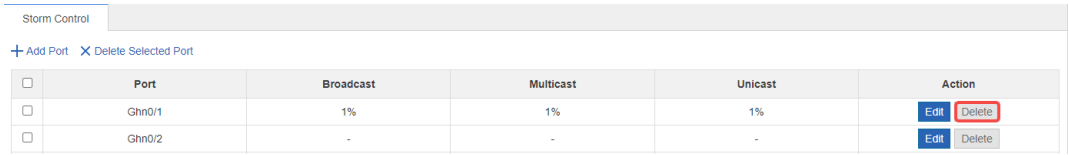


■ Deleting storm control ports

(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.



1.3.5 Advanced

1.3.5.1 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.

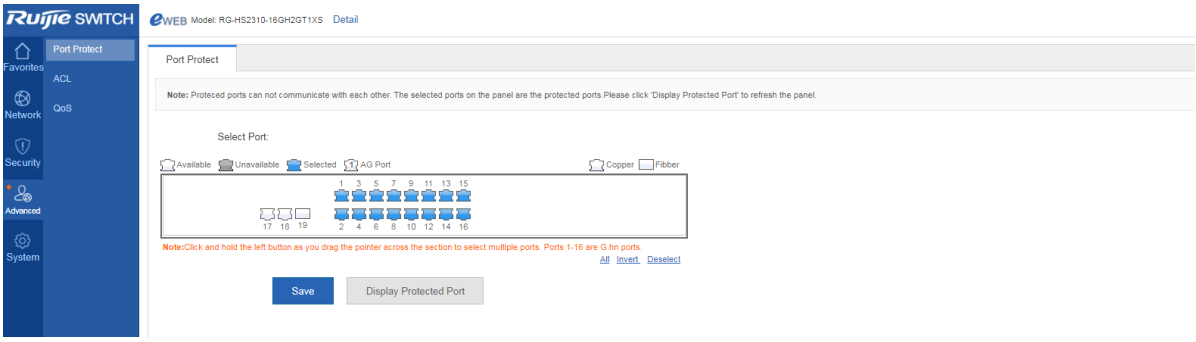
Protected ports work in either of the two modes.

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.

1.3.5.2 ACL

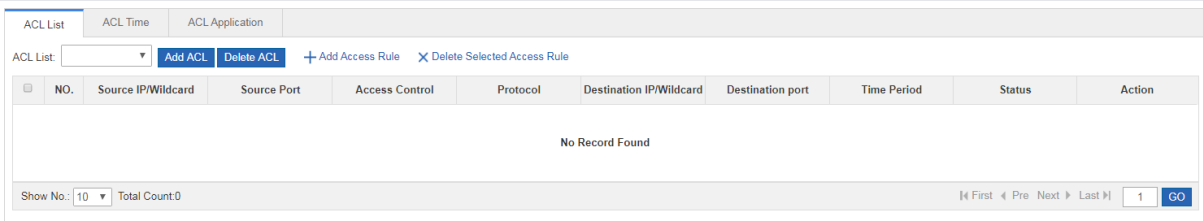
Access control list (ACL) is also called access list or firewall. The ACL defines rules to determine whether to forward or drop data packets arriving at a network interface.

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

ACL List

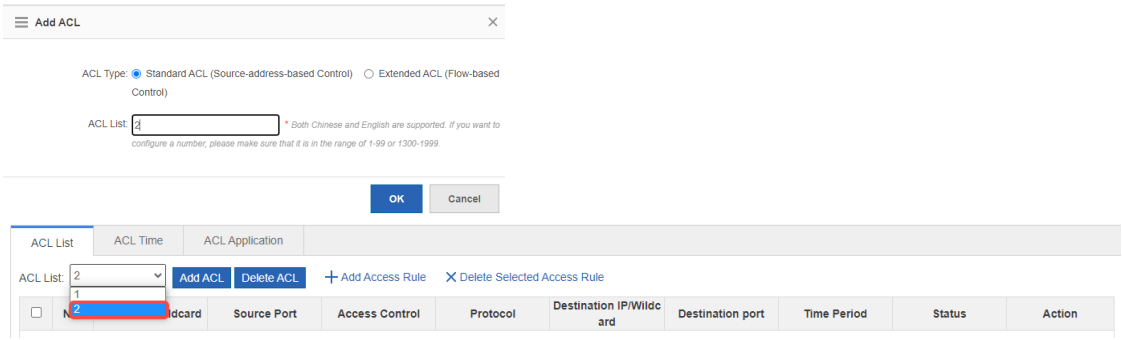
The following figure shows the ACL List page.

Figure 1-20 ACL List



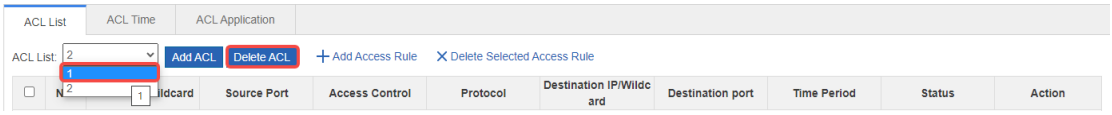
■ Adding ACLs

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.



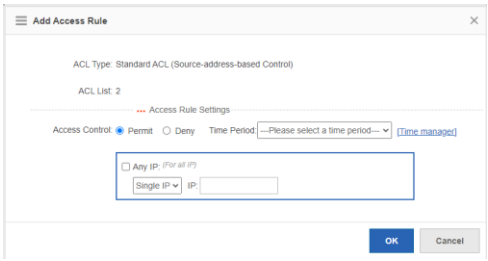
■ Deleting ACLs

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



■ 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.



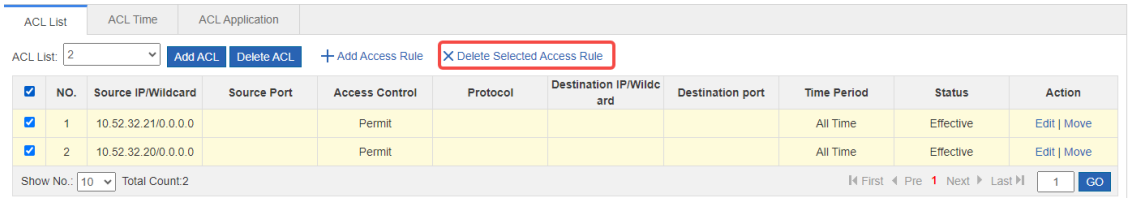
Editing Access Rules

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.

Deleting Access Rules

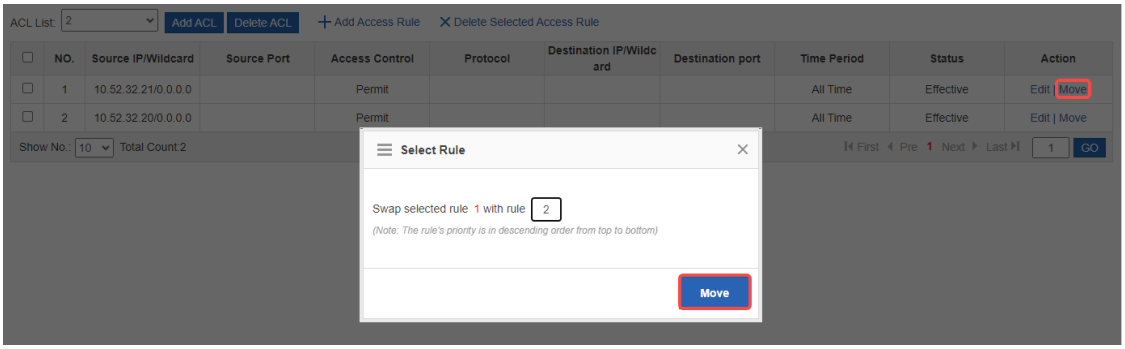
(1) Multiple access rules from the ACL rule list can be selected. Click Delete Selected Access Rule to batch delete access rules.

(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 Rules

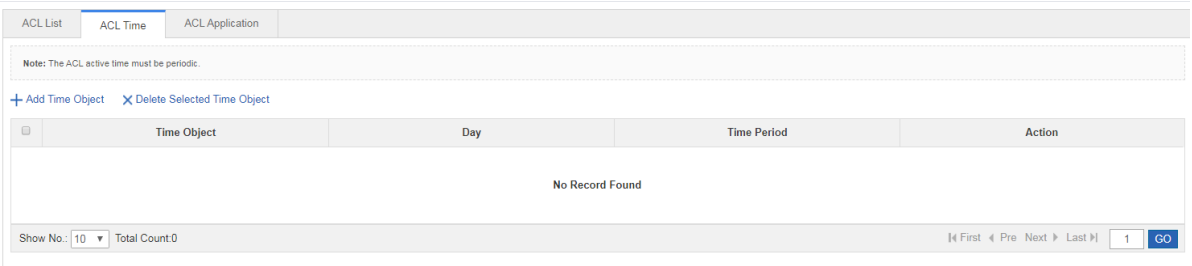
Enter the serial number of the ACL to be moved and click Move. The “Operation succeeded.” message is displayed.



ACL Time

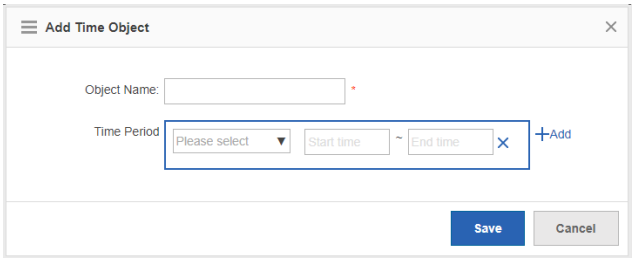
The following figure shows the ACL Time page.

Figure 1-21 ACL Time



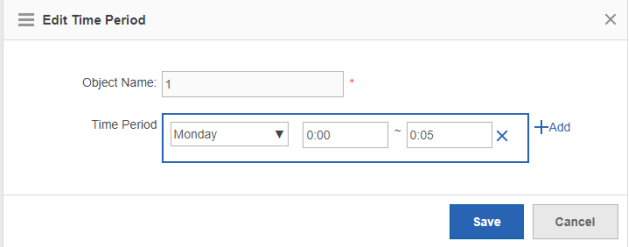
Adding ACL Time

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.



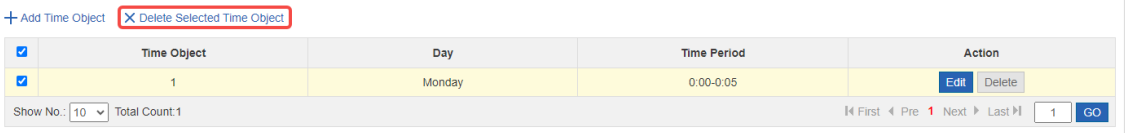
Editing ACL Time

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 objects.



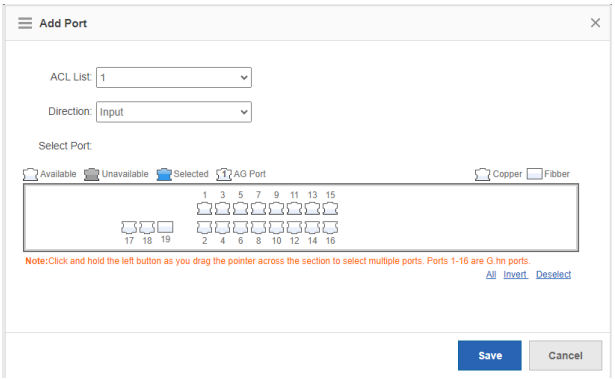
ACL Application

The following figure shows the ACL Application page.

Figure 1-22 ACL Application

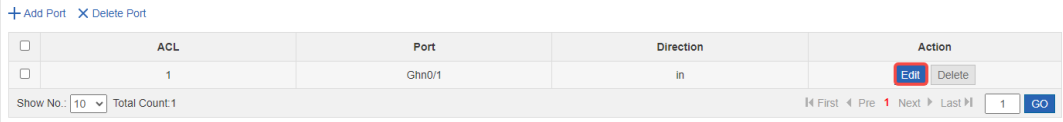
Add ACL Application

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.



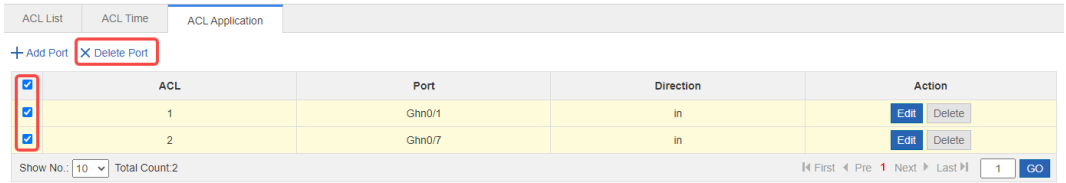
Editing ACL Application

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.

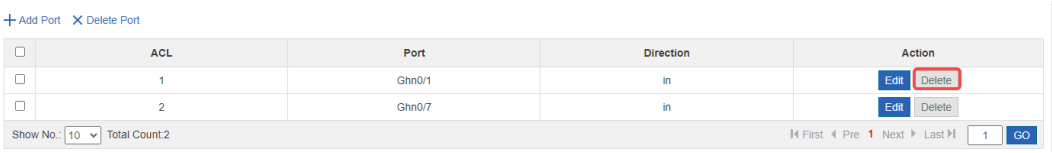


Deleting ACL Application

(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.



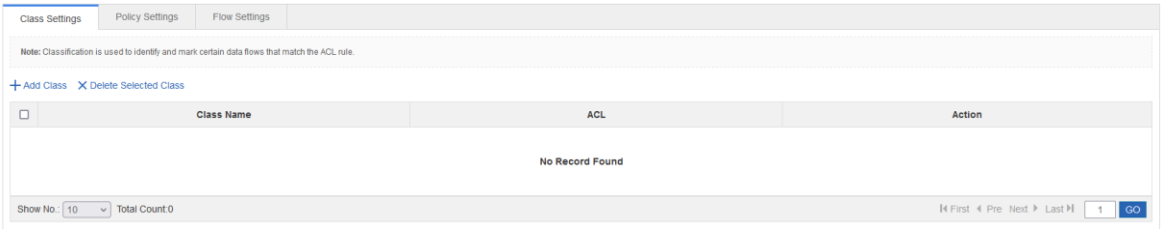
1.3.5.3 QoS

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

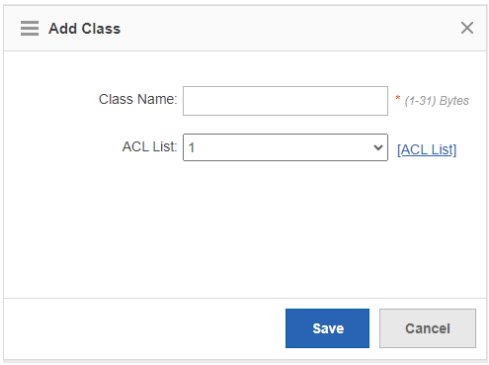
The following figure displays the page of Class Settings.

Figure 1-23 Class Settings



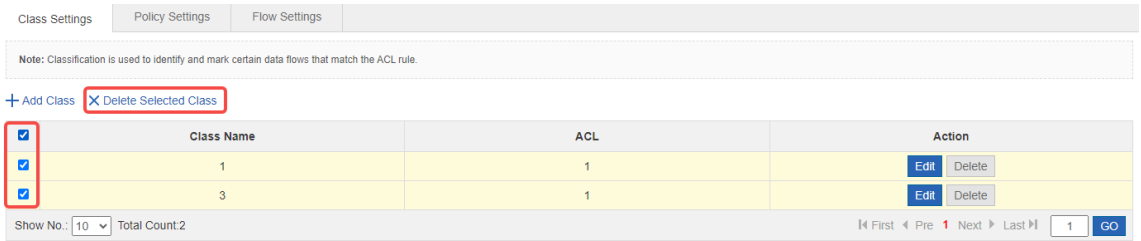
- Add Class

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.



- Delete Class

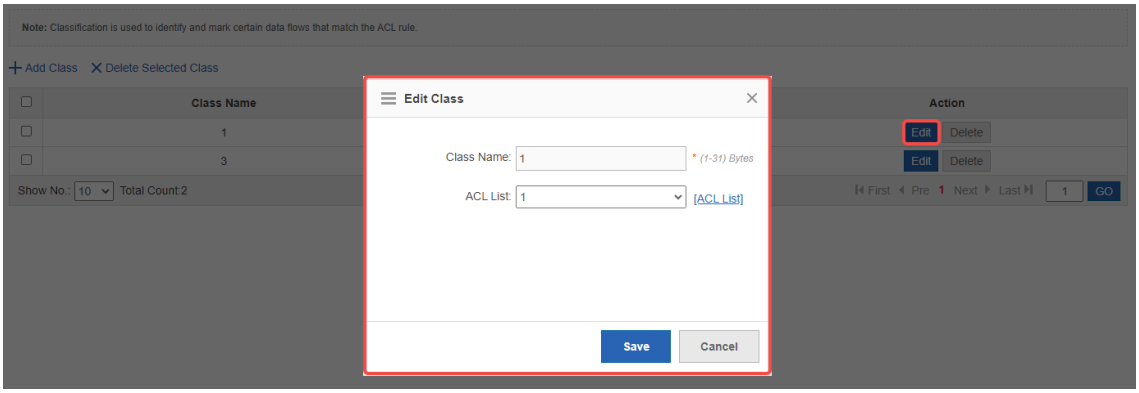
Select one or multiple classes to be deleted, and then click Delete Selected Class.



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

- Edit Class

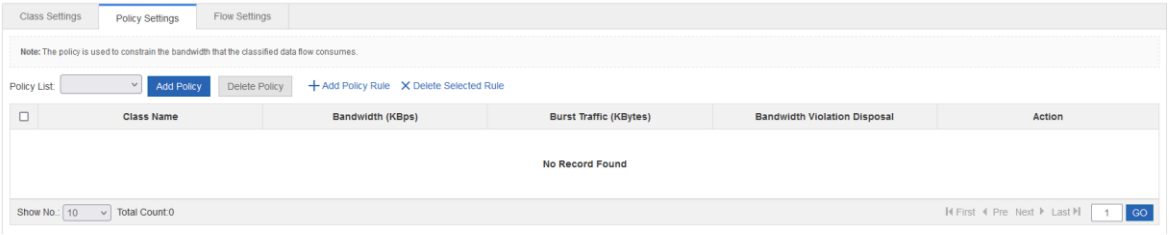
Click the Edit button in the Action column of the class to be edited. After editing it, click Save.



Policy Settings

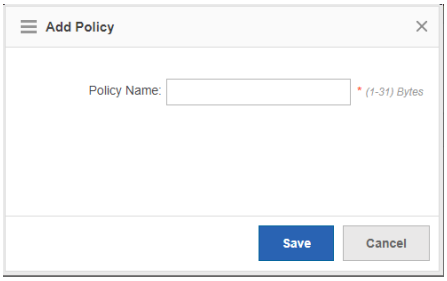
The following figure displays the Policy Settings page.

Figure 1-24 Policy Settings



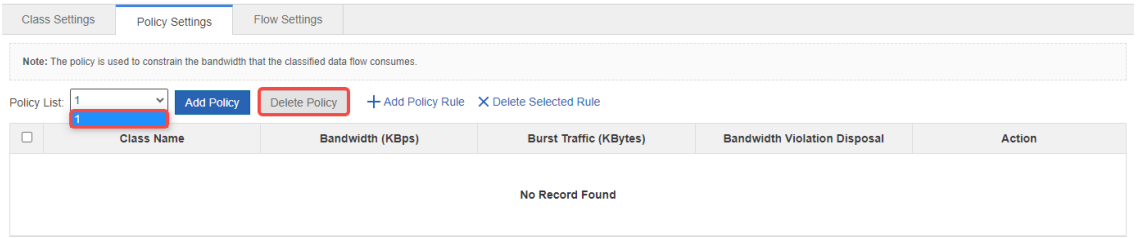
- Add a Policy

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



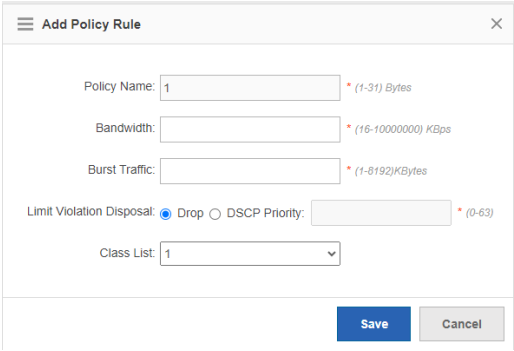
- Delete Policy

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



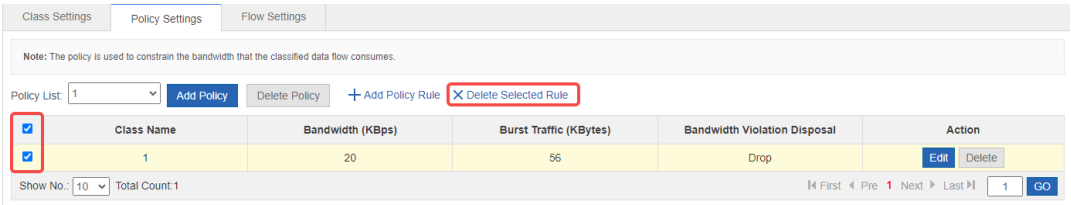
■ Add Policy Rule

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.



■ Delete Policy Rule

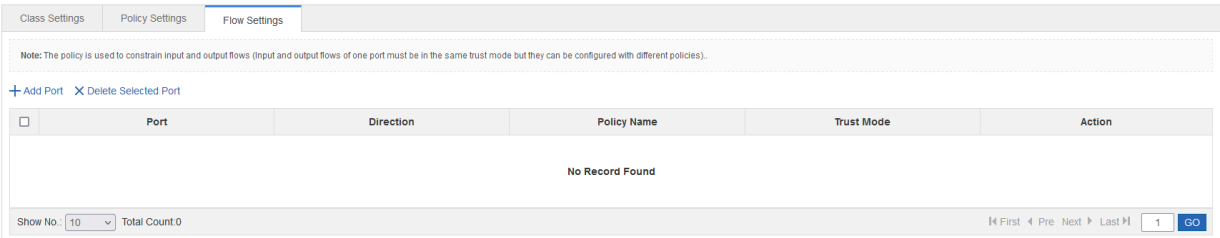
Click the policy rule to be deleted, and then click Delete Selected Rule.



Flow Settings

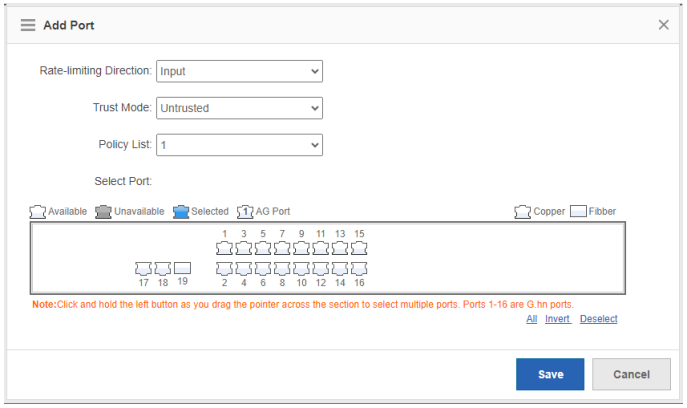
The following page displays the Flow Settings.

Figure 1-25 Flow Settings



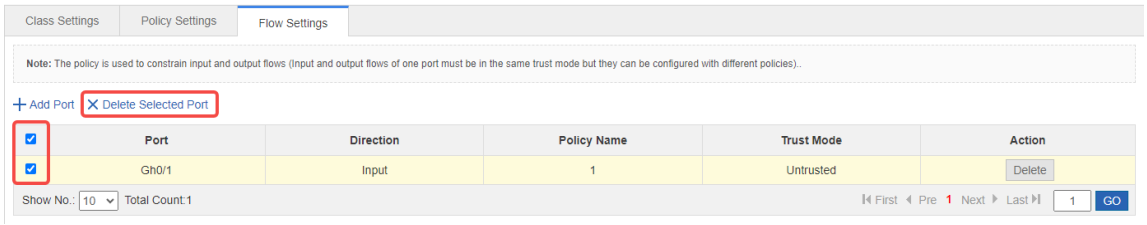
■ Add Ports

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.



■ Delete Ports

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



1.3.6 System

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

1.3.6.1 System Settings

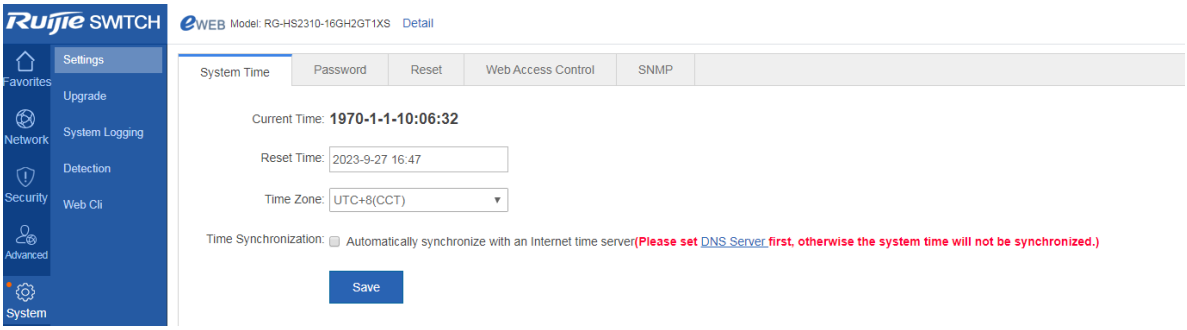
Five tab pages are available on the system setting page: System Time, Password, Restart, Reset, Web Access Control and SNMP.

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



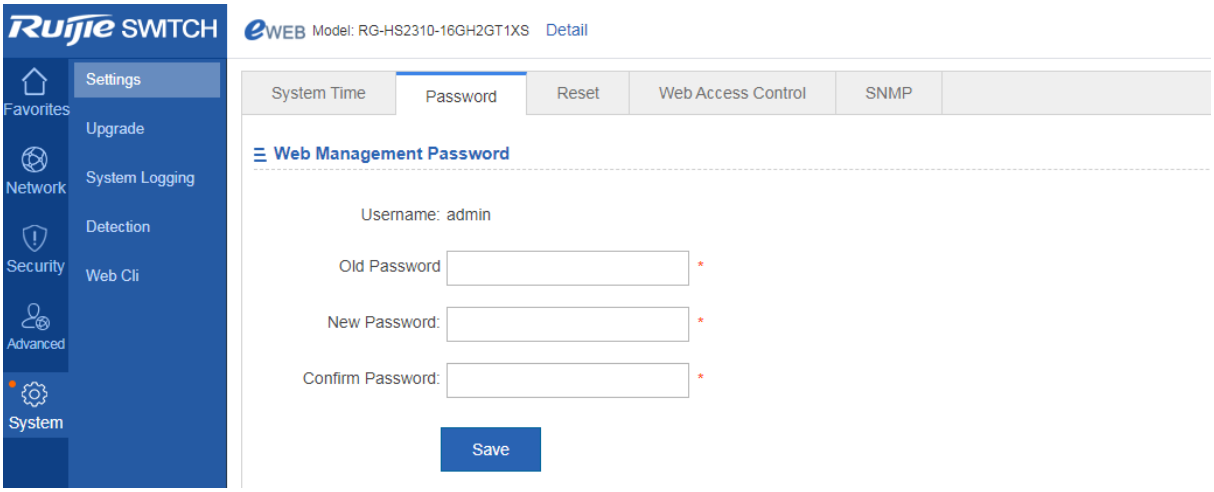
The current system time is displayed on the page. Current system time can be set manually. Alternatively, you can select Automatically synchronize with an Internet time server for setting the time. Afterwards, click Save. The “Configuration succeeded.” message is displayed.

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

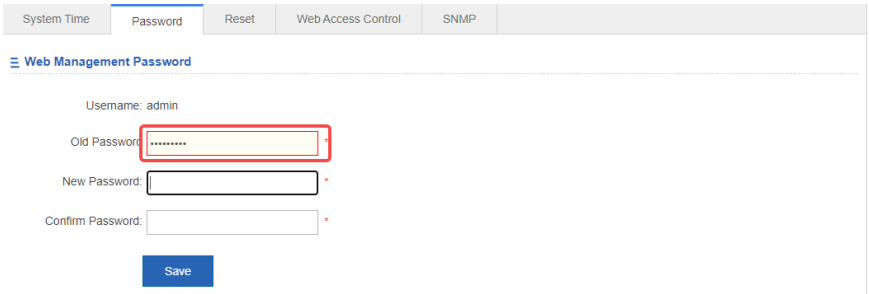
The following figure shows the Password page.

Figure 1-27 Password



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.

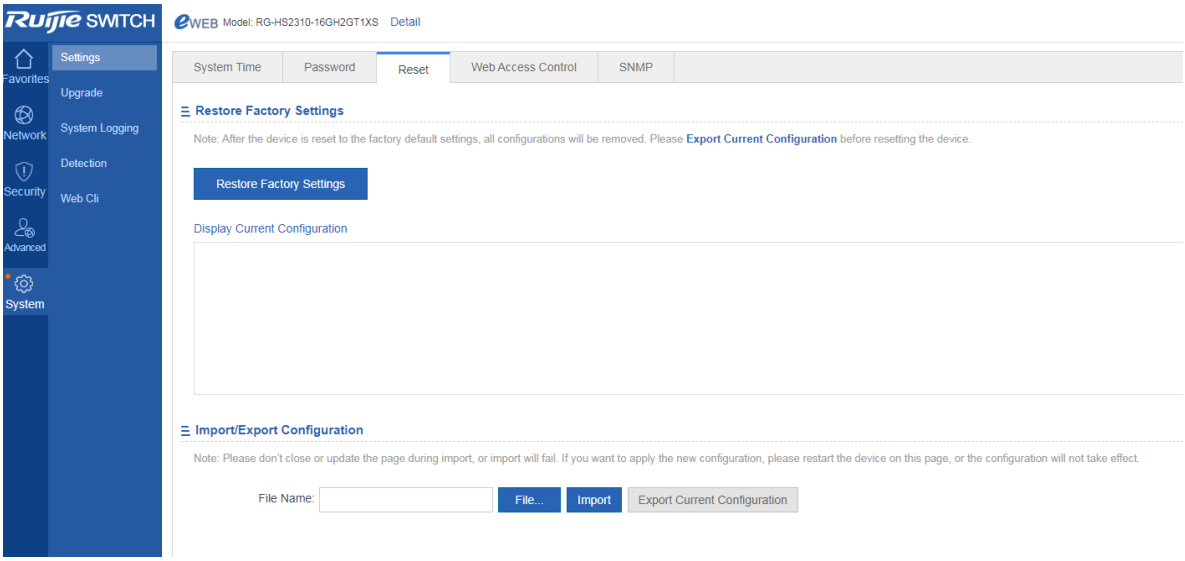


When you change the Web management password, the enable password is changed accordingly by default.

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.

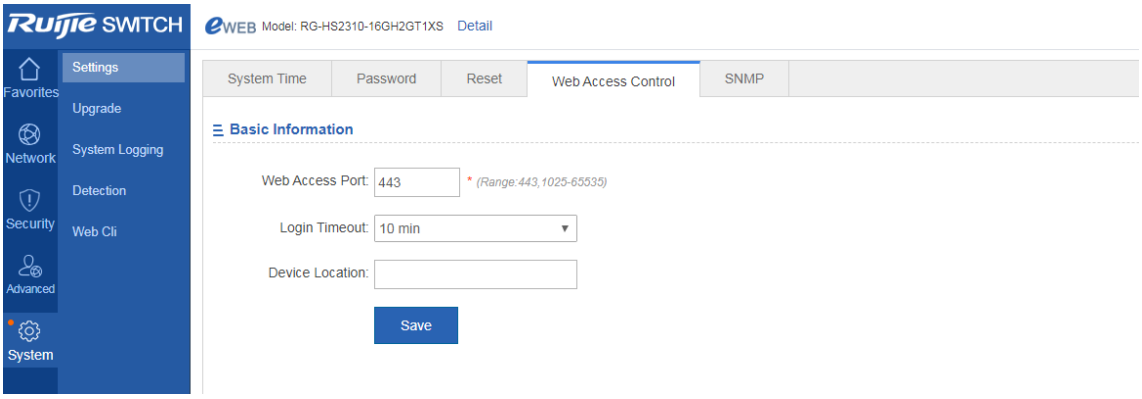
- Restoring Factory Settings

  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.

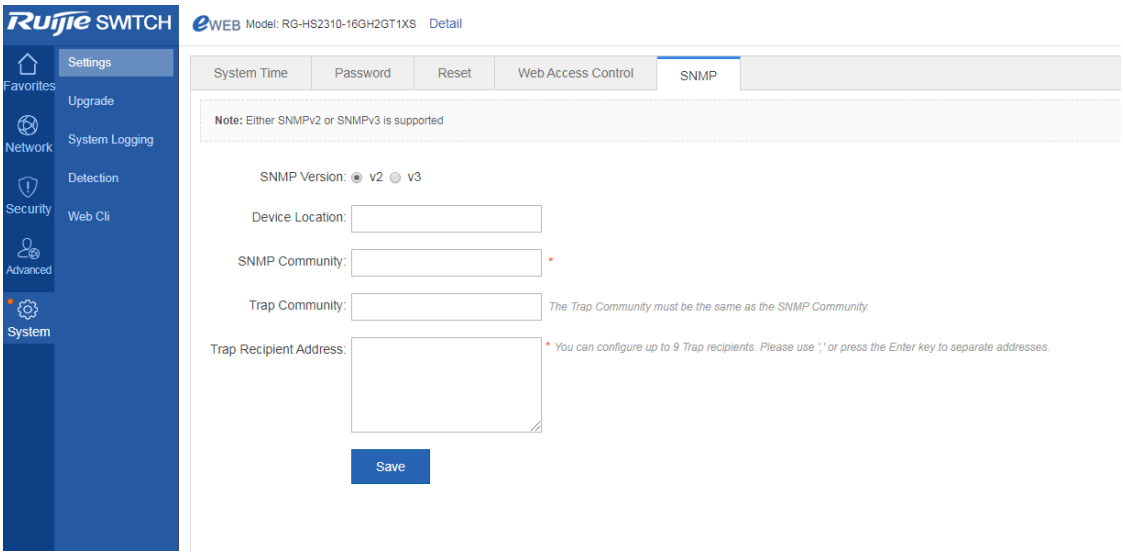
SNMP

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



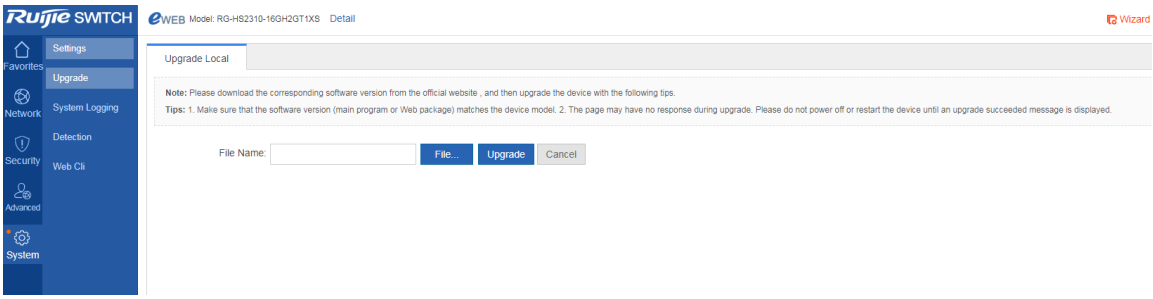
On this page, SNMP Version, Device Location, SNMP Password, and Trap Password are mandatory and other parameters are optional. After setting, click Save. The “Configuration succeeded.” message is displayed.

1.3.6.2 System Upgrade

Local Upgrade

The following figure shows the local Upgrade page.

Figure 1-31 Upgrade Locally



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

1.3.6.3 System Logging

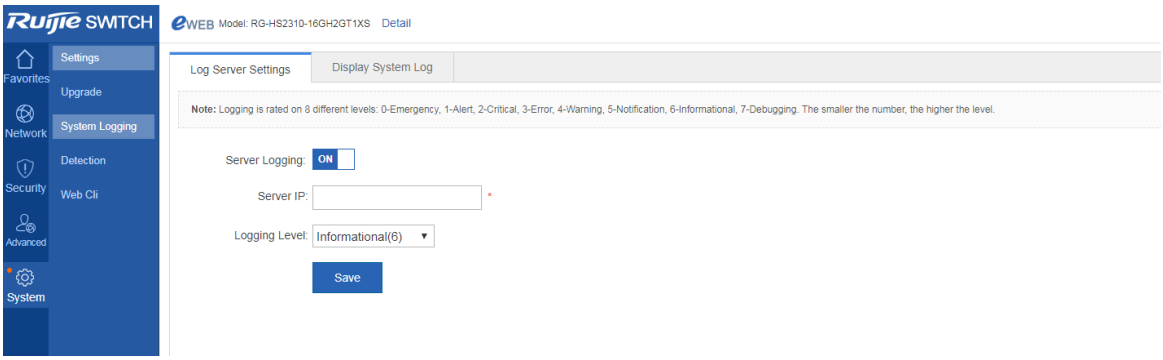
Status changes (such as link up and down) or abnormal events may occur anytime. Ruijie products provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console 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

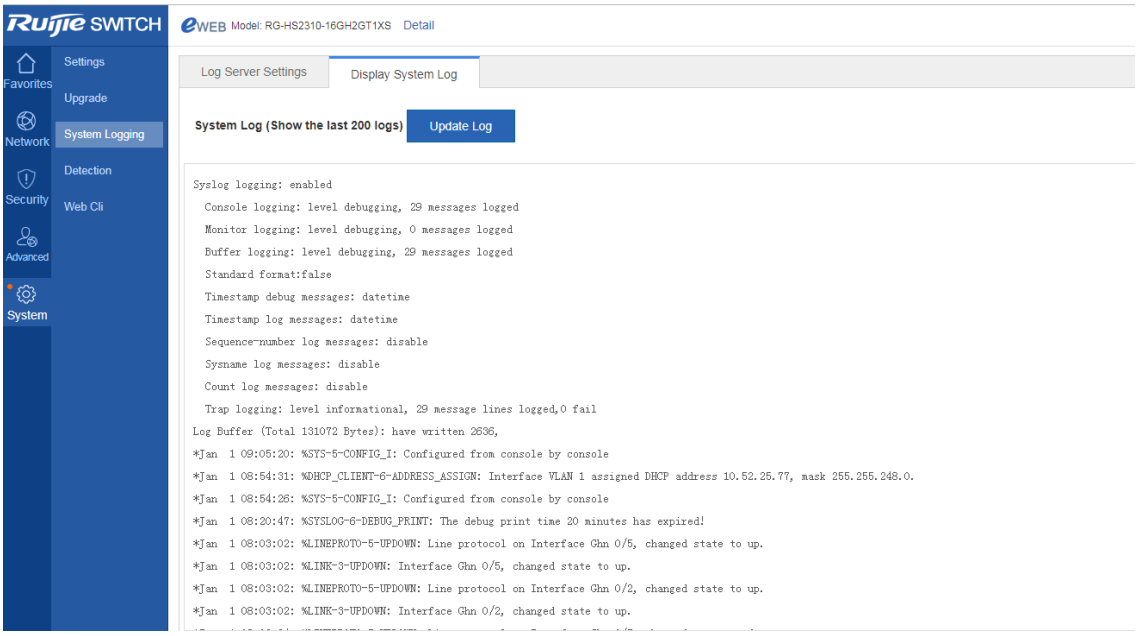


Set various parameters such as Server IP Address and Logging Level. The device sends the SYSLOG log to the corresponding server after the configuration is complete.

Display System Log

The following figure shows the Display System Log page.

Figure 1-33 Display System Log



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

1.3.6.4 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.

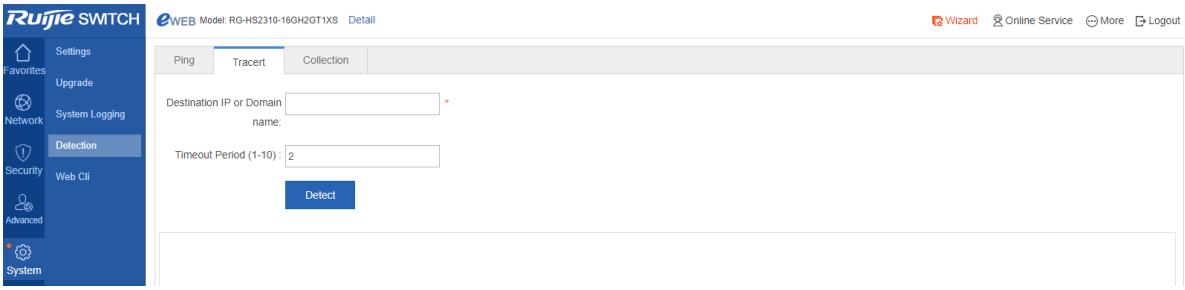
Figure 1-34 Ping

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) massages to the destination hots to request a ICMP Echo Reply messages so as to identify all next hops of two devices.

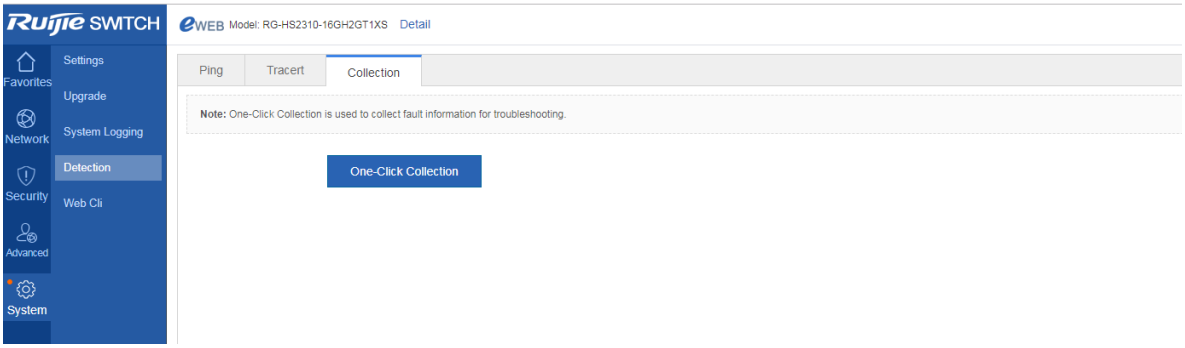
Figure 1-35 Tracert



Collection

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

Figure 1-36 One-click Collection



1.3.6.5 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