

HS2310-16GH2GT1XS

Web-based Configuration Guide

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

Copyright Statement

Ruijie Networks©2023

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

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: <u>https://www.ruijienetworks.com/</u>
- Technical Support Website: <u>https://ruijienetworks.com/support</u>
- Case Portal: <u>http://caseportal.ruijienetworks.com</u>
- Community: <u>http://community.ruijienetworks.com</u>
- Technical Support Email: <u>service rj@ruijienetworks.com</u>
- Skype: <u>service rj@ruijienetworks.com</u>

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.

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

Contents

1	Web-Bas	ed Confi	guration	1
	1.1	Overvie	2W	1
	1.2	Web-ba	ased Management	1
	1.3	Web Ma	anagement System	4
	1.3.1	Wiza	rd	6
	1.3.2	Favo	rites	
	1	.3.2.1	Home Page	7
	-	.3.2.2	VLAN	
		.3.2.3	Port	
		.3.2.4	Restart	
	1.3.3		vork	
	-	.3.3.1	MAC Address	
	-	.3.3.2	RLDP	
	1.3.4	Secu	rity	17
	1	.3.4.1	Anti-ARP-Attack	
	-	.3.4.2	Storm Control	19
	-	.3.4.2	Storm Control	19 21
	1 1.3.5 1	.3.4.2 Adva .3.5.1	Storm Control inced Port Protection	19 21 21
	1 1.3.5 1 1	.3.4.2 Adva .3.5.1 .3.5.2	Storm Control Inced Port Protection ACL	19 21 21 22
	1 1.3.5 1 1 1	.3.4.2 Adva .3.5.1 .3.5.2 .3.5.3	Storm Control Inced Port Protection ACL QoS	19 21 21 22 26
	1 1.3.5 1 1	.3.4.2 Adva .3.5.1 .3.5.2 .3.5.3	Storm Control Inced Port Protection ACL	19 21 21 22 26
	1 1.3.5 1 1 1 1.3.6	.3.4.2 Adva .3.5.1 .3.5.2 .3.5.3	Storm Control Inced Port Protection ACL QoS em System Settings	19 21 21 22 26 29 29
	1 1.3.5 1 1 1 1.3.6 1	.3.4.2 Adva .3.5.1 .3.5.2 .3.5.3 Syste	Storm Control Inced Port Protection ACL QoS em System Settings System Upgrade	19 21 21 22 26 29 29 32
	1 1.3.5 1 1 1 1.3.6 1 1.3.6	.3.4.2 Adva .3.5.1 .3.5.2 .3.5.3 Syste .3.6.1	Storm Control Inced Port Protection ACL QoS em System Settings System Upgrade System Logging	19 21 21 22 26 29 29 32 33
	1 1.3.5 1 1 1 1.3.6 1 1.3.6	.3.4.2 Adva .3.5.1 .3.5.2 .3.5.3 Syste .3.6.1 .3.6.2	Storm Control Inced Port Protection ACL QoS em System Settings System Upgrade	19 21 21 22 26 29 29 32 33

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 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.

1 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

Ruíjie
RG SWITCH
Please enter the administrator username
Please enter the administrator password
Login

WEB | ©2000-2023 Ruijie Networks Co., Ltd. | Official Website | Online Service | Service Mail

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.

(i) 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
--------	-----	------	------

合	Home	Home							
vorites	VLAN	CPU: 2.4	40% Memory :	26.4% 3	Current Ter	e:1970-01-01 00:05:23	Model:RG-HS2310-16GH2G		
twork		CPU: 2.4	40% Memory	Up Port C	Running Tir	ne:0 d 00 h 05Min	Version:HS2310_RGOS 11.4 Device MAC:4826.0000.0022	2	
$\overline{\mathbb{U}}$	Restart						Device SN:MACC942570105		
curity		Port Ir	nformation 📿 <u>Refresh</u>						
2 vanced		Port	Input Rate 🌲	Output Rate t 🌲	Status(Port real speed)	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision
		Ghn0/1	0K	OK	Not Connected	0/0	0/0	0/0	0
ිූි /stem		Ghn0/2	ОK	ОK	Not Connected	0/0	0/0	0/0	0
stern		Ghn0/3	ОK	OK	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	ОК	OK	Not Connected	0/0	0/0	0/0	0
		Ghn0/6	ОK	OK	Not Connected	0/0	0/0	0/0	0
		Ghn0/7	ОK	OK	Not Connected	0/0	0/0	0/0	0
		Ghn0/8	ОK	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/9	ОK	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/10	0.4K	5.9K	Connected(1000M)	91893/843078	0/0	0/0	0

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

1.3 Web Management System

Basic Concepts

Licons 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.
517	Aggregate port. The number in the port indicates the aggregate port number.
<u>5</u>	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.
<u>All Invert Deselect</u>	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

🖸 Available 💼 Unavailable 💼 Se	lected 17 AG Port	Copper Fibber
	1 3 5 7 9 11 13 15 <u>다다다다다</u> 다	

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

Available 🚆 Unavailable 🚍 Se	lected 11 AG Port	Copper Fibber
	1 3 5 7 9 11 13 15	
لية 19 17 18 19		

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.
	Used to set the system time, modify passwords, restart the system, restore to
System Settings	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	Figure	1-5	Wizard
-------------------	--------	-----	--------

■ Wizard			×
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)		
		Save	Cancel

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

Ruj	JIE SWITCH	WEB Mode	I: RG-HS2310-16GH2GT1XS	Detail			🕞 Wizard 🛛 😤 C	Online Service 💮 More	e 🕞 Logou			
• Favorites	Home	Home										
Ø Network	VLAN Port	CPU: 2.	CPU: 2.40% Memory : 26.4% 3 Up Port Count Up									
() Security	Restart	Port I	nformation CRefresh									
2 Advanced		Port	Input Rate 👙	Output Rate	Status(Port real speed)	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count			
		Ghn0/1	0K	ОK	Not Connected	0/0	0/0	0/0	0			
(3)		Ghn0/2	ОK	0K	Not Connected	0/0	0/0	0/0	0			
System		Ghn0/3	ОK	ОK	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	ОK	ОK	Not Connected	0/0	0/0	0/0	0			
		Ghn0/6	ОK	ОK	Not Connected	0/0	0/0	0/0	0			
		Ghn0/7	ОK	ОK	Not Connected	0/0	0/0	0/0	0			
		Ghn0/8	ОК	ОK	Not Connected	0/0	0/0	0/0	0			
		Ghn0/9	ОК	ОK	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

VLAN Setting	s Trunk Port								
+ Batch Add VLAN + Add VLAN X Delete Selected VLAN									
	VLAN ID	\$	VLAN name	Port	Action				
	1		VLAN0001	Gi0/1-6,Gi0/9-10	Edit				
	2		fffffff	Gi0/7-8	Edit Delete				
Show No.: 10 Total Count.2 If First 4 Pre 1 Next 1 Last 1 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 packet	s to go through, configur	e it as a trunk port. It is rec	ommended to configure the port	connected to the net	work device as a trunk port.
No Trunk Port						
Native	VLAN: 1		* Range(1-4094)			
Allowed	VLAN: 1-4094		The VLAN range is form	atted as 3-5,100.		
Sele	ct Port:					
🖸 Available 💼 U	Jnavailable 📄 Seleo	ted 1 AG Port		Copper	Fibber	
	17 18 19		11 13 15 12 14 16			
Note:Click and hold	the left button as you	drag the pointer across t	the section to select multipl	e ports. Ports 1-16 are G.hn port <u>All</u> Inver	s. t 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 allow	s multiple VLAN packet	ts 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	×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.

VLAN Settings	/LAN Settings Trunk Port		
			ph, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.
Gi0/18	⊗ Te0/19 ✓	× Batch Del	

1.3.2.3 Port

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

N Port Settings

Figure 1-10 Port Setting

Home 15	Port Settings	Aggregate port	Port Mirroring	Rate Limiting							
	+ Batch Add +	Add SVI									
Port											
	E L3 Port										
		Port	Status		IP		Mask		IPv6	Description	Action
	v	LAN 1	Up		10.52.25.77	7	255 255 248 0				Edit Delete
	V	LAN 2	Up								Edit Delete
	Show No.: 10	Total Count:2								H First 🕴 P	re 1 Next ⊁ Last ⊁ 1
	≡ L2 Port										
	Pe	ut.	Status	Port	Туре	Access VLAN	Native	VIAN	Permit VLAN	Description	Action
	Ghr		Up		ESS	1	1				Edit Detail
	Ghr		Up		ESS	1	1				Edit Detail
	Ghr		Up		ESS	1	1				Edit Detail
	Ghr		Up		ESS	1	1				Edit Detail
	Ghr	0/5	Up	ACC	ESS	1	1				Edit Detail
	Ghr	0/6	Up	ACC	ESS	1	1				Edit Detail
	Ghr	0/7	Up	ACC	ESS	1	1				Edit Detail
	Ghr	0/8	Up	ACC	ESS	1	1				Edit Detail
	Ghr	0/9	Up	ACC	ESS	1	1				Edit Detail
	Ghn	0/10	Up	ACC	CESS	1	1				Edit Detail
	Show No.: 10	Total Count:19								N First (Pre	1 2 Next > Last > 1
	Show No.: 10	 Total Count:19 								14 First 4 Pre	1 2 Next ► Last ►

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

Ruij	JIE SWITCH	WEB Model: RG-H	S2310-16GH2GT1XS De	tail											,	🕽 Wizard	2 Online Service	∎ ⊖ More	e ⊡ Logou
C Favorites	Home	Port Settings	Aggregate port	Port Mirroring	Rate Limiting														
() Network	VLAN	Ξ Global Configu	iration																
Network	Port	Note:the aggregate	e port is used to perform t	raffic allocation according	g to the selected load-b	alance algorithm.													
① Security	Restart	Load-bal	ance: Source MAC and	Destination *															
2 Advanced			Save	Default Settings															
َنَ System		E Aggregation po		redundancy, multiple ph	vsical ports (member p	orts) are combined into one logical p	l port (aggrej	regate port).	An aggregat	te port contains	s up to eight me	ember ports, and	the aggregate p	rt load balance	a traffic across the	ese physical p	ports.		
No Aggregate																			
		Aggregate	Port ID:	• 8	lange(1-16)														
		Pa	ort Type: L2 Port(Swi	tching Port)															
		Sele	ect Port:																
			17 18 19	1 3 5 7 9 11 2 4 6 8 10 12	14 16	Copper Pibber													
			Add	Cancel															

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.



A 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.

D Port Mirroring

The following figure shows the Port Mirroring page.

Figure 1-12 Port Mirroring

RU	JIC SWITCH	WEB Model: RGHS2315-MGHS0T1X5 Detail	🕞 Wizard	2 Online Service	⊕ More ⊖ Logout
• Favorites	Home	Port Settings Aggregate port Port Mirroring Rate Limiting			
() Network	VLAN Port	Note: For minoring is the capability to send a copy of relator's packets seen on the source port to the destination port for analysis by a network analyzer. Traffic on multiple source ports can be minored to one single destination port. Tige A source port server the a destination port.			
(T) Security	Restart	Montor Packets AI Packets •			
2		Select Source Port: (You can select multiple ports, but it may affect device performance.)			
Advanced		Available 😰 Unavailable 🛣 Selected 😭 A D Pot 😭 Copper 🔤 Pikter			
©) System					
		Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-10 are G hn ports. All Instit. Desetted			
		Select Destination Port: (You can select any one port)			
		Charallable 童Unavailable 童 Selected (요AG Port Copper Carabonation			
		Detelect			
		Save Refresh			

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.

A 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.



Ru	IJIE SWITCH	WEB Model: RG-HS2316-160H20T1XS Detail	C Wizard	2 Online Service	⊖ More [∋ Logout
Favorites	Home S	Restart				
Network	VLAN	Note: Click 'Restart to restart the device. Please wait a few minutes and the page will be refreshed after restart.				
Network Security	Restart	Restart				
Advanced						
ی) System						
			02000	-2023 Ruijie Networks (o., Ltd. Offic	ial Website

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

Ruij	IE SWITCH	WEB Model: R	G-HS2310-16GH2GT1XS Deta	ail							C Wizard	Online Service	More	B Logout
Favorites	MAC Address	Mac Table	Static MAC Address	Filtering MAC Address										
Network	RLDP		ch forwards data according the Mi enabled, you can implement autho			nding on a network device n	nanually, after you add a	static address, the switch	n that receives the packet w	ith the same destination ad	Idress forwards it to t	te specified port. With	302.1X	
() Security		+ Add Static Ad	ddress X Delete Static Add	dress										
2.s			Port		Ν	MAC Address			VLAN ID			Action		
Advanced							No Record Four	d						
 System 														
		Show No.: 10	Total Count:0								I4 First ∢	Pre Next ▶ Last	⊨ 1	GO
											@2000	-2023 Ruijie Networks	Co., Ltd. Off	icial Website

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 Fibber
17 18 19 2 4 6 8 10 12 14 16	
	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	WEB Model: RG-HS2310-16GH2GT1XS Deta	a de la companya de la company		R Wizard 2 Online Service ⊖ More D Logout
Vorites RLDP Stwork	Mac Table Static MAC Address Note: The switch forwards data according the MA address of ARP packets. + Add Filter Address X Delete Filter Addre		achet with the source/destination MAC address which is configured as a filter address, it discards the p	acket. You can prevent the ARP attack by configuring a filter address the same as the MAC
scurity Les vanced		IAC Address	VLAN ID No Record Found	Action
(i) ystem	Show No.: 10 v Total Count 0		no record i roana	KFirst 4 Pre Next > Last H 1 00

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				
	forwards data according the MA r address the same as the MAC		f a switch receives a packet with the source	destination MAC address which i	s configure	d as a filter address, it discards the packet. You can prevent the ARP attack by
+ Add Filter Add	ress 🗙 Delete Filter Addr	ess	Add Filter Address		×	
Show No.: 10	MAC Add	ress	MAC Address:	•		Action KFirst ≪ Pre Next > Last > 1 GO
				Save Can	cel	

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.

	n forwards data according the MAC address inside the data frame. If a ar address the same as the MAC address of ARP packets.	witch receives a packet with the source/destination MAC address which is configure	ed as a filter address, it discards the packet. You can prevent the ARP attack by
+ Add Filter Add	dress X Delete Filter Address		
	MAC Address	VLAN ID	Action
	4222.6622.8866	1	Edit Delete
Show No.: 10	✓ Total Count:1		I 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 Addr	ess X Delete Filter Address		
	MAC Address	VLAN ID	Action
	4222.6622.8866	1	Edit Delete
	4222.6622.8867	4	Edit Delete
Show No.: 10	V Total Count:2		Ill First II Pre 1 Next I Last II 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.

	MAC Address	VLAN ID	Action
	4222.6622.8866	1	Edit Delete
	4222.6622.8867	4	Edit Delete
Show 1	No.: 10 V Total Count:2		I First ∢ Pre 1 Next ▶ Last 1 GO

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.

N RLDP Settings

Figure 1-16 RLDP Settings

Ruj	JIE SWITCH	WEB Model: RG-HS2	2310-16GH2GT1XS Detail			R Wizard	Online Service	→ More	🕒 Logout
C Favorites	MAC Address	RLDP Settings							
•⊗	KLUP	⊟ Global configura	ation						
Network		Note: RLDP enables	s you to detect link failure quickly. RLDP can run on the p	port only after it is enabled globally.					
() Security		RLDP: ON							
2 Advanced		Detection 3 Interval:	Range(2-15)						
ු System		Detection Count: 2	Range(2-10)						
		errdisable	Range(30-86400s)						
			Save						
		≡ Port Configurati	on						
				oops. It is recommended to enable RLDP on the port connected to the ends of the link to be enabled with RLDP. It is recommended to configu					
		+ Add Port X Dele	ete Port						
			Port	Detection Type	Troubleshooting		Action		
				No Record I	Found				
		Show No.: 10 👻	Total Count.0			H First	(Pre Next) Last)	1	GO
						#24	0 2022 Buillin Mohuarice C		

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.

∃ Global confi	guration	
Note: RLDP en	ables you to detect link failure quickly	y. RLDP can run on the port only after it is enabled globally
RLDP:	ON	
Detection Interval:	3	Range(2-15)
Detection Count:	2	Range(2-10)
errdisable recovery:		Range(30-86400s)
	Save	

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.

⊒ Global configuration		
Note: RLDP enables you to detect link failure quickly. RLDP c	Batch Add	×
RLDP: ON	Detection Mode: Unidirectional Link Detection 👻	
Detection 3 Range(2- Interval:	Troubleshooting: Warning	
Detection Count: 2 Range(2-	Select Port:	
errdisable Range(3) recovery:	① Available ② Selected ① AG Port ① Copper □ Fibbe 1 3 5 7 9 11 13 15 1 1 3 5 7 9 11 13 15 1 1 3 5 7 9 11 13 15 1 1 3 5 7 9 11 13 15 1 1 1 1 10 12 14 16	er.
E Port Configuration	Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are C hn ports. All Invert. Desele	<u>ct</u>
Note: 1. Enabling RLDP on the port can avoid broadcast storr 2. Unidirectional/Bidirectional link detection requires the		
+ Add Port X Delete Port		
Port	Save Cance	I.

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.

+ Add	Port 🗙 Delete Port			
	Port	Detection Type	Troubleshooting	Action
	TenGigabitEthernet 0/19	Unidirectional Link Detection	Warning	Edit Delete
Show	No.: 10 V Total Count:1			I∢ First ∢ Pre 1 Next ▶ Last ▶ 1 GO

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

+ Add Port	X Delete Port			
	Port	Detection Type	Troubleshooting	Action
	GigabitEthernet 0/18	Unidirectional Link Detection	Warning	Edit Delete
	TenGigabitEthernet 0/19	Unidirectional Link Detection	Warning	Edit Delete
Show No.	10 V Total Count:2			I∢ First ∢ Pre 1 Next ► Last ► 1 GO

(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.

Port	Detection Type	Troubleshooting	Action
GigabitEthernet 0/18	Unidirectional Link Detection	Warning	Edit Delete
TenGigabitEthernet 0/19	Unidirectional Link Detection	Warning	Edit Delete

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 B	Binding>>Static Binding 🛛 🔓 Remove static Binding	nding 📲 Manual Binding		IP-based: Sea
	IP	MAC	Туре	Action
	192.168.1.200	00e0.4c00.2155	Local ARP Entry	Dynamic Binding>>Static Binding
	192.168.21.1	0000.5e00.0115	Dynamic Binding	Dynamic Binding>>Static Binding
	192.168.21.138	40b0.3438.536a	Dynamic Binding	Dynamic Binding>>Static Binding
	192.168.21.229	00e0.4c00.2155	Local ARP Entry	Dynamic Binding>>Static Binding

Dynamic Binding > Static Binding

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

ARP Entries					
🖫 Dynamic B	Binding>>Static Binding 🗣 Remove static Binding	IP-based: Search			
	IP	MAC	Туре	Action	
	10.52.24.1	ecb9.70b7.00ee	Dynamic Binding	Dynamic Binding>>Static Binding	
	10.52.24.35	0023.24e3.f94b	Dynamic Binding	Dynamic Binding>>Static Binding	
	10.52.25.61	00d0.f822.3377	Dynamic Binding	Dynamic Binding>>Static Binding	
	10.52.25.65	300d.9e3e.ae48	Dynamic Binding	Dynamic Binding>>Static Binding	
	10.52.25.76	00e0.4c00.215f	Local ARP Entry	Dynamic Binding>>Static Binding	

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

IP	MAC	Туре	Action
10.52.24.1	ecb9.70b7.00ee	Dynamic Binding	Dynamic Binding>>Static Binding
10.52.24.35	0023.24e3.f94b	Dynamic Binding	Dynamic Binding>>Static Binding
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				
Ra Dynamic Binding>Static Binding 🔒 Remove static Binding 🖁 Manual Binding Search					
	IP	MAC	Туре	Action	
	10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding	
	10.52.24.1	ecb9.70b7.00ee	Static Binding	Remove static Binding	

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

IP	MAC	Туре	Action
10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding
10.52.24.1	ecb9.70b7.00ee	Static Binding	Remove static Binding

Manual Binding

(1) Click Manual Binding above the list.

ARP	ARP Entries						
🔡 Dyr	🔓 Dynamic Binding>>Static Binding 🐕 Remove static Binding 🕼 Manual Binding 🚺 Search						
	IP MAC Type Action						
	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

■ Manual binding ARP		×
IP:	*	
MAC:	*	
ок	Cancel	

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.

Storm Control					
+ Add Port X Delete Selected Port					
	Port	Broadcast	Multicast	Unicast	Action
	Ghn0/1				Edit Delete
	Ghn0/2	-	-	-	Edit Delete
•	Ghn0/3	-		-	Edit Delete
	Ghn0/4		-	-	Edit Delete
	Ghn0/5	-	-	-	Edit Delete
	Ghn0/6				Edit Delete
	Ghn0/7	-	-	-	Edit Delete
	Ghn0/8	-	-	-	Edit Delete
	Ghn0/9				Edit Delete
	Ghn0/10	-	-	-	Edit Delete
Show No.: 1	0 🔻 Total Count:19			I First	

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.

E Add Port	\times
Select Port	
🖸 Available 💼 Unavailable 💼 Selected 🏦 AG Port 🔅 Copper 🗔 Fibber	
Note: Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are 0.hn ports. All invert Deselect	
Type: 🖲 Bandwidth Usage 🔿 Packets 🔿 Kilobits	
Broadcast %	
Multicast: %	
Unicast %	
Save Ca	icel

Editing Storm Control Ports

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

Storr	Storm Control				
+ Add	+ Add Port X Delete Selected Port				
	Port	Broadcast	Multicast	Unicast	Action
	Ghn0/1	1%	1%	1%	Edit Delete

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

Туре:	Bandwidth Usage Packets	G Kilobits
Broadcast:	1	%
Multicast:	1	%
Unicast:	1	%

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

Starm Control					
+ Add Port X Delete Selected Port					
	Port	Broadcast	Multicast	Unicast	Action
	FOIL	Bioadcast	Multicast	onicast	Action
	Ghn0/1	1%	1%	1%	Edit Delete

(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.

Storm Control						
+ Add Po	+ Add Port X Delete Selected Port					
	Port	Broadcast	Multicast	Unicast	Action	
	Ghn0/1	1%	1%	1%	Edit Delete	
	Ghn0/2	-	-	-	Edit Delete	

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

Ruț	JIE SWITCH	WEB Model: RG-H52310-I6GH2GT1XS Detail						
C Favorites	Port Protect	Port Protect						
0	ACL QoS	Note: Protected ports can not communicate with each other. The selected ports on the panel are the protected ports Please click "Display Protected Port" to refresh the panel.						
Network		Select Port:						
Advanced								
َ System		17 16 19 2 4 8 10 12 14 18 Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G An ports. All Invert						
		Save Display Protected Port						

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

ACL List	ACL Time	ACL Application							
ACL List:	▼ Add /	CL Delete ACL +A	dd Access Rule 🛛 🗙 Dele	te Selected Access Rule					
■ NO.	Source IP/Wildcar	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
	No Record Found								
Show No.:	10 V Total Count:0							I∉ First ∢ Pre Next ▶	Last 🕅 🛛 🖌 🖌 🖌 1

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			×				
ACL Type: Standard Control)	CL (Flow-based						
ACL List: 2		Chinese and English are support					
configure a nu	nber, please make sure that it is i	in the range of 1-99 or 1300-199	9.				
		ок	Cancel				
ACL List ACL Time	ACL Application						
ACL List: 2 · A	dd ACL Delete ACL	+ Add Access Rule	X Delete Selected	Access Rule			
	rd Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status

Deleting ACLs

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

1	ACL List	ACL Time	AC	L Application							
	ACL List: 2	~	Add ACI	L Delete ACL	+ Add Access Rule	X Delete Selected A	Access Rule				
	□ N ²	1_ildo	card	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action

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	×
ACL Type: Standard ACL (Source-address-based Control)	
ACL List: 2	
Access Rule Settings	
Access Control. Permit O Deny Time Period:Please select a time period	et)
Any (P; ^(f) of IP) Single (P ∨) IP	
ок Са	ncel

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	ACL List ACL Time ACL Application									
ACL Li	ACL List: 2 Add ACL Delete ACL		+ Add Access Rule	+ Add Access Rule X Delete Selected Access Rule						
	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action
	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move
Shov	how No.: 10 v Total Count:1 II 60									

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.

ACL List ACL Time ACL Application										
ACL LI	st: 2	Y Add A	CL Delete ACL	+ Add Access Rule	X Delete Selected A	Access Rule				
	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action
	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move
	2	10.52.32.20/0.0.0.0		Permit				All Time	Effective	Edit Move
Shov	show No.: 10 v Total Count 2 If First 4 Pre 1 Next > Last > 1 GO									

Moving Access Rules

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

ACL LI	st: 2	Y Add A	CL Delete ACL	+ Add Access Rule	X Delete Selected	Access Rule					
	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action	
	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move	
	2	10.52.32.20/0.0.0.0		Permit				All Time	Effective	Edit Move	
Shov	v No.: 1	10 🗸 Total Count:2		E Selec	Select Rule			Id First ∢ Pre 1 Next ▶ Last № 1 GO			
					t <mark>ed rule 1 with rule (</mark> le's priority is in descend	2 ing order from top to bottom)	Move				

ACL Time

The following figure shows the ACL Time page.

Figure 1-21 ACL Time

ACL List	ACL Time	ACL Application							
	active time must be								
+ Add Time O	- Add Time Object X Delete Selected Time Object								
•	Tì	me Object	Day	Time Period	Action				
	No Record Found								
Show No.: 10	Total Coun	t:0			I∢ First ∢ Pre Next ▶ Last ▶ 1 GO				

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.

Add Time Object		×			
Object Name:					
Time Period	Please select V Start time C End time X	+Add			
	Save	Cancel			

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.

Edit Time Period					×
Object Name:	1	*			
Time Period	Monday	▼ 0:00	~ 0:05	×	+Add
				Save	Cancel

Deleting ACL Time

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

+ Add	+ Add Time Object X Delete Selected Time Object									
	Time Object	Day	Time Period	Action						
	1	Monday	0:00-0:05	Edit Delete						
Show	Show No.: 10 V Total Count:1									

ACL Application

The following figure shows the ACL Application page.

Figure 1-22 ACL Application

ACL List	ACL Time	ACL Application			
+ Add Port	X Delete Port				
•		ACL	Port	Direction	Action
			No Record	Found	
Show No.: 1	0 🔻 Total Coun	t:0			I∉First ∉ Pre Next I Last II GO

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.

∏ Add Port	×
ACL List 1 v	
Direction: Input v	
Select Port.	
💭 Available 💼 Unavailable 💼 Selected 🚮 AG Port 💭 Copper 🥅	Fibber
1 3 5 7 9 11 13 15 <u>ロロロロロロロロ</u> フロロ 17 18 19 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.	eselect
Save	Cancel

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.

ACL	Port	Direction	Action
1	Ghn0/1	in	Edit Delete

Deleting ACL Application

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

ACL List	ACL Time ACL Application				
+ Add Port X Delete Port					
	ACL	Port	Direction	Action	
	1	Ghn0/1	in	Edit Delete	
	2	Ghn0/7	in	Edit Delete	
Show No.: 10 → Total Count 2 If First 4 Pre 1 Next ▶ Last ▶ 1 GO					

(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.

ort X Delete Port

ACL	Port	Direction	Action
1	Ghn0/1	in	Edit Delete
2	Ghn0/7	in	Edit Delete

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

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						
		Class Name	ACL	Action			
	No Record Found						
Show No.: 10	 Total Count:0 			I4 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: 1		[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.						
	Delete Selected Class					
	Class N	lame	ACL	Action		
	1		1	Edit Delete		
	3		1	Edit Delete		

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

	Class Name	ACL	Action		
	1	1	Edit Delete		
	3	1	Edit Delete		
Shov	Show No.: 10 ▼ Total Count 2				

• Edit Class

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

Note: Classification is use	ed to identify and mark certain data flows	hat match the ACL rule.		
+ Add Class × Delete	e Selected Class			
	Class Name	🗮 Edit Class	×	Action
0	1			Edit Delete
	3	Class Name: 1	* (1-31) Bytes	Edit Delete
Show No.: 10 V Total Count:2		ACL List: 1	✓ [ACL List]	K First ∢ Pre 1 Next ▶ Last ▶ 1 GO
			Save Cancel	

D Policy Settings

The following figure displays the Policy Settings page.

Figure 1-24 Policy Settings

Class Settings	ass Settings Policy Settings Flow Settings					
Note: The policy is us	Note: The policy is used to constrain the bandwidth that the classified data flow consumes.					
Policy List	olicy List Add Policy Delete Policy + Add Policy Rule X Delete Selected Rule					
	Class Name		Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
	No Record Found					
Show No.: 10	 Total Count:0 					If First If Pre Next IF Last II 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.

Class Settings	Policy Settings	Flow Settings									
Note: The policy is us	Note: The policy is used to constrain the bandwidth that the classified data flow consumes.										
Policy List: 1	olicy List Add Policy Delete Policy + Add Policy Rule × Delete Selected Rule										
	Class Name	Bandwidth (KBps) Burst Traffic (KBytes) Bandwidth Violation Disposal Action									
			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.

	×
Add Policy Rule	~
Policy Name: 1	* (1-31) Bytes
Bandwidth:	* (16-10000000) KBps
Burst Traffic:	* (1-8192)KBytes
Limit Violation Disposal:) Drop 🔿 DSCP Pri	ority: (0-63)
Class List: 1	~
	Save Cancel

Delete Policy Rule

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

Class Setti	ings Policy Settings	Flow Settings							
Note: The policy is used to constrain the bandwidth that the classified data flow consumes.									
Policy List: 1 V Add Policy Delete Policy + Add Policy Rule × Delete Selected Rule									
	Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action				
	1	20	56	Drop	Edit Delete				
Show No.: 10 ▼ Total Count 1									

\Science Flow Settings

The following page displays the Flow Settings.

Figure 1-25 Flow Settings

Class Settings	Policy Settings	Flow Settings							
Note: The policy is used to constrain input and output flows (input and output flows of one port must be in the same trust mode but they can be configured with different policies).									
+ Add Port X Del	+ Add Port X Delete Selected Port								
	Port Direction Policy Name Trust Mode Action								
No Record Found									
Show No.: 10	 Total Count:0 				I4 First 4 Pre Next ▶ Last ▶ 1 GO				

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	\times
Rate-limiting Direction: Input	
Trust Mode: Untrusted	
Policy List: 1	
Select Port:	
😭 Available 💼 Unavailable 💼 Selected 🖽 AG Port 🔄 Copper 🗔 Fibber	
1 3 5 7 9 11 13 15 <u>그 그 그 그 그 그 그 그 그 그 그 그 그 그 그 그 그 그 그 </u>	
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. Deseted	
Save Cance	d

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 Pott X Delete Selected Port									
	Port	Direction	Policy Name	Trust Mode	Action				
	2 Gh0/1 Input 1 Untrusted Delete								
Show No:: 10 ▼ Total Count1 If First Pre 1 Next Last 1 GO									

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

Ruij	JIE SWITCH	WEB Model: RG-H	182310-16GH2GT1X	5 Detail										
C Favorites	Settings	System Time	System Time Password Reset Web Access Control SNMP											
avonies	Upgrade													
() Network	System Logging	Curren	Current Time: 1970-1-1-10:06:32											
1	Detection	Rese	Reset Time: 2023-9-27 16:47											
Security	Web Cli	Time	e Zone: UTC+8(C	CT)	Ŧ									
2® Advanced		Time Synchron	ization: 🔲 Automa	tically synchro	onize with an Internet time se	rver(Please se	$t\underline{\text{DNS Server}}first,$ otherwise the system time will not be synchronized.)							
• 💮 System			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

Ruj	JIE SWITCH	WEB Model: RG-H	S2310-16GH2GT1X	3 Detail							
C Favorites	Settings	System Time	Password	Reset	Web Access Control	SNMP					
	Upgrade	= Web Managem	⊒ Web Management Password								
(S) Network	System Logging										
(!)	Detection	Use	Username: admin								
Security	Web Cli	Old Password *									
2 Advanced		New Pas	sword:		*						
ි		Confirm Pas	sword:		*						
System			Save								

Modifying the Web-based NMS Password

accordingly by default.

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 Managem	ent Password				
User	mame: admin				
Old Pas	ssword		*		
New Pas	sword:				
Confirm Pas	sword:		*		
	Save				
 Whe 	n you ch	nange t	he Web man	agem	ent password, the enable passw

4 00 0

Nestore Factory Settings

The following figure shows the Reset page.

Figu	ire 1-28 Re	set								
Ruj	JIE SWITCH	WEB Model: RG-H	HS2310-16GH2GT1X	s Detail						
Favorites	Settings	System Time	Password	Reset	Web Access Control	SNMP				
Ø	Upgrade	⊒ Restore Facto	ory Settings							
Network	System Logging	Note: After the de	evice is reset to the f	actory default se	ettings, all configurations will be	e removed. Plea	se Export Current Configur	ation before resetting the	device.	
	Detection									
Security	Web Cli	Restore Fac	ctory Settings							
2 Advanced		Display Current	Configuration							
• (j) System										
		≘ Import/Export	Configuration							
		Note: Please don	't close or update th	e page during in	nport, or import will fail. If you v	vant to apply the	e new configuration, please re	start the device on this pa	ge, or the configuration will no	t take effect.
		File	Name:		File Imp	oort Export	Current Configuration			

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

Rui	JIE SWITCH	WEB Model: RG-H	S2310-16GH2GT1X	B Detail									
C Favorites	Settings	System Time	Password	Reset	Web Access Control	SNMP							
	Upgrade	Ξ Basic Information											
() Network	System Logging												
0	Detection		Web Access Port: 443 (Range: 443, 1025-65535)										
Security	Web Cli	Login Ti	meout: 10 min		Ŧ								
2 Advanced		Device Lo	cation:										
ି (୍ରି System			Save										

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

Ru	JIE SWITCH	WEB Model: RG-H	S2310-16GH2GT1XS	B Detail									
C Favorites	Settings	System Time	Password	Reset	Web Access Control	SNMP							
Ø	Upgrade	Note: Either SNMP	v2 or SNMPv3 is sup	ported									
Network	System Logging												
1	Detection	SNMP V	ersion: 💿 v2 🔘 v	3									
Security	Web Cli	Device Lo	cation:										
2® Advanced		SNMP Comr	nunity:		*								
<u>ت</u>		Trap Comr	nunity:		The Trap Community I	must be the same as ti	he SNMP Community.						
System		Trap Recipient Ad	dress:		* You can configure up	to 9 Trap recipients. F	Please use ',' or press the Ente	er key to separate addresses.					
			Save										

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

Ruíjie SMTCH		WEB Model: RG-HS2310-160H2GT1XS Detail				
Favorites	Settings	Upgrade Local				
	Upgrade	Note: Please download the corresponding software version from the official website, and then upgrade the device with the following tips.				
Network	System Logging	Tips: 1. Make sure that the software version (main program or Web package) matches the device model. 2. The page may have no response during upgrade. Please do not power off or restart the device until an upgrade succeeded message is displayed.				
	Detection	File Name: File Upgrade Cancel				
Security	Web Cli					
2 Advanced						
@						
System						

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

Ruijie Switch		WEB Model: RG-HS2310-16GH2GT1XS Detail						
Favorites	Settings	Log Server Settings Display System Log						
Ø	Upgrade	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.						
Network	System Logging							
	Detection	Server Logging: ON						
Security	Web Cli	Server IP: •						
2 Advanced		Logging Level: Informational(6) •						
් (ිූි System		Save						

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

Пијје ѕмтсн		WEB Model: RG-HS2310-16GH2GT1XS Detail
C Favorites	Settings	Log Server Settings Display System Log
Ø Network	Upgrade System Logging	System Log (Show the last 200 logs) Update Log
	Detection	Syslog logging: enabled
Security	Web Cli	Console logging: level debugging, 29 messages logged
20		Monitor logging: level debugging, O messages logged
Advanced		Buffer logging: level debugging, 29 messages logged
• ~~~		Standard format:false
<u>ي</u>		Timestamp debug messages: datetime
System		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 09:05:20: %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: %SYSLOC-G-DEBUG_PRINT: The debug print time 20 minutes has expired!
		*Jan 1 08:03:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ghn 0/5, changed state to up.
		*Jan 1 08:03:02: %LINK-3-UPDOWN: Interface Ghn 0/5, changed state to up.
		*Jan 1 08:03:02: %LIMEPROTO-5-UPDOWN: Line protocol on Interface Ghn 0/2, changed state to up.
		*Jan 1 08:03:02: %LINK-3-UPDOWN: Interface Ghn 0/2, changed state to up.

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.

N 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

Ru	JIE SWITCH	WEB Model: RG-HS2310-16GH2GT1XS Detail		🔀 Wizard 🛛 🙎 Online Serv	ice ⊖More ⊡Logout
C Favorites	Settings	Ping Tracert Collection			
austin or	Upgrade				
() Network	System Logging	Destination IP or Domain name:			
	Detection	Timeout Period (1-10) : 2			
Security	Web Cli	Repetition Count (1-100): 5			
Advanced	29 <u>.</u>	Detect			
€ System					
System					

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

Ruíj	JIE SWITCH	WEB Model: RG-HS2310-16GH2GT1XS Detail	R Wizard	Online Service	. More	➡ Logout
C Favorites	Settings	Ping Tracert Collection				
	Upgrade					
(S) Network	System Logging	Destination IP or Domain • name:				
\bigcirc	Detection	Timeout Period (1-10): 2				
Security	Web Cli					
2 Advanced		Detect				
ै (ु) System						

****Collection

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

Figure 1-36 One-click Collection

Пите SMITCH		e web M	odel: RG-HS2310-	3H2GT1XS Detail
Favorites	Settings	Ping	Tracert	Collection
	Upgrade	Note: O	no Click Collection	used to collect fault information for troubleshooting.
() Network	System Logging	Note. Of		used in conect radii monimation noi troubleshooring.
\bigcirc	Detection			One-Click Collection
Security	Web Cli			
2 Advanced				
• {्रे System				

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

Ruíjie SMITCH		WEB Model: R	0+HS2310-M0H20T1XS Detail	🕞 Wizard 🛛 2 Online Service 💮 More 🕞 Logo				
Favorites	Settings	Web Cli						
	Upgrade			Background Color: 💻 💻 🗖				
Ø Network	System Logging	Console Output:	Console Output:					
Network		led-blink	Blink for searching a device	*				
	Detection	lock	Lock the terminal					
	Web Cli	mcu-upgrade	Mcu upgrade					
		nkdir	Make directories					
2 Advanced		nore	Display contents of a file					
Advanced		no	Negate a command or set its defaults					
් (ි) System		ping	Send echo messages					
System		pwd	Print name of current working directory					
		reload	Reload device					
		rename	Move or rename files					
		renew	Renev					
		rldp	Rldp exec operation	•				
		rndir	Remove a directory	1				
		Command Input	Send Clear Screen					
			SRHz simal * (+ SS) calendar cd checkpoint *					