

# Ruijie RG-S2915-L Series Switches Release S2915-L\_RGOS 11.4(1)B82

Web-based Configuration Guide

Document Version: V1.0 Date: November 16<sup>th</sup>, 2022 Copyright © 2022 Ruijie Networks

# Copyright

Copyright © 2022 Ruijie Networks

All rights are reserved in this document and this statement.

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.



All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

# Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. 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

# Intended Audience

This document is intended for:

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

# **Technical Support**

- Ruijie Networks Website: <u>https://www.ruijienetworks.com/</u>
- Technical Support Website: <u>https://ruijienetworks.com/support</u>
- Case Portal: <u>https://caseportal.ruijienetworks.com</u>
- Community: <u>https://community.ruijienetworks.com</u>
- Technical Support Email: <a href="mailto:service\_rj@ruijienetworks.com">service\_rj@ruijienetworks.com</a>
- Live Chat: https://www.ruijienetworks.com/rita

# Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in <b>bold</b> font.
Italic font	Arguments for which you supply values are in <i>italic</i> font.
[]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

# 2. Signs

The signs used in this document are described as follows:

# Warning

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

#### 🛕 Caution

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

#### 🚺 Note

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



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

# 3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

# **1** Configuring Switch Eweb

# 1.1 Overview

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

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

#### Specification

This document applies only to S2915-L series switches.

# 1.2 Application

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

# 1.2.1 Managing Switches through the Eweb

#### 1. Scenario

As shown in Figure 1-1, you can access the Eweb of an access switch or aggregation switch through a browser to manage and configure the switch.

#### Figure 1-1



#### 🚺 Note

The device enclosed in the red rectangle in Figure 1-1 is the access switch. Ensure that the switch can be pinged successfully from the PC. Then you can access the Eweb of the switch.

#### 2. Deployment

(1) Configuration Environment Requirements

Client requirements:

- You can manage the switch by logging in to the web management interface of the switch through the browser of the web management client. Clients refer to PCs or other mobile terminals such as laptops.
- Browser: IE8–IE11, Google Chrome, and 360 Browsers are supported. Exceptions such as garble or format errors may occur if an unsupported browser is used.
- Resolution: The recommended resolution is 1024\*768, 1280\*1024, 1440\*960, or 1920\*1080. If other resolutions are used, exceptions such as format errors or misalignment occur.

🚺 Note

Eweb configuration and command line interface (CLI) configuration can be performed simultaneously. After CLI configuration is complete, enter the **write** command to save the configuration. If you open the web page, refresh the page to ensure that Eweb and CLI configurations are synchronized.

#### (2) Logging In to the Web Management Platform

Enter http://X.X.X.X (management IP address) in the browser and press Enter to access the **Login** page, as shown in Figure 1-2.

# Figure 1-2 Login Page



150% - + 22

WEB | ©2000-2021 Rulije Networks Co., Ltd. | Official Website | Online Service | Service Portal | Service Mail

Enter the username and password and click **Login**. The following table provides the default username and password.

#### Table 1-1

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

### 1 Note

When you log in by using the default username and password, the system requests you to change the password to ensure security.

After authentication is successful or the password is changed, the Eweb homepage is displayed, as shown in Figure 1-3.

Figure 1-3 Eweb Homepage

Home         Home           Favorites         VLN           Port         Device         Network         Part Count         Lip Port Count         Current Time 2022-10-21 123141         Model           Port         Post Settings         Port Information         Cleant         Current Time 2022-10-21 123141         Model           Processeting         Post Settings         Port Information         Cleant         Status(Port real speed)         In Octots/OutOctets         UnderSize/OverSize         CRC/FCS Error           System         Option         Option         Option         Option         Option         Option         Option           Gi0/1         18.7K         9.3K         Connected (1000M)         2698078163/11586667         Option         Option         Option           Gi0/2         OK         OK         Net Connected         Option         Option         Option           Gi0/3         OK         OK         Net Connected         Option         Option         Option           Gi0/4         OK         OK         Net Connected         Option         Option         Option           Gi0/4         OK         OK         Net Connected         Option         Option         Option           Gi0/4<	ror Collisi
VLN         VLN           Port         Port Security         Memory: 40.9%         1         Durrent Time:2022-10:21 12:31:41         Model           Open Security         Processing         Port Information C Refresh         Durrent Time:2022-10:21 12:31:41         Model           Security         Processing         Port Information C Refresh         Durrent Time:2022-10:21 12:31:41         Model           Security         Processing         Port Information C Refresh         Comment Time:2022-10:21 12:31:41         Model           Security         Processing         Port Information C Refresh         Comment Time:2022-10:21 12:31:41         Model           System         Output Rate         Output Rate         Status(Port real speed)         InOctets/OutOctets         UnderSize/OverSize         CRC/FCS Error           Gi0/1         18.7K         9.3K         Connected(1000M)         2699078163/11580667         Oil 0         Oil 0           Gi0/2         OK         OK         Not Connected         Oil 0         Oil 0         Oil 0           Gi0/3         OK         OK         Not Connected         Oil 0         Oil 0         Oil 0         Oil 0         Oil 0           Gi0/3         OK         OK         Not Connected         Oil 0         Oil 0         Oi	ror Collisi
Pool Settings         Pool Settings           Security         Restart	ror Collisi
Port         Input Rate         Output Rate         Status(Port real speed)         Inoctets/OutOctes         UnderSize/OverSize         CRC/FCS Error           Gi0/1         18.7K         9.3K         Connected(1000M)         2699078163/11586667         0/0         0/0         0/0           Gi0/2         OK         OK         Not Connected         0/0         <	ror Collisi
Gi0/1         18.7K         9.3K         Connected(1000M)         2698078163/11586667         0/0         0/0           System         Gi0/2         0K         0K         Not Connected         0/0         0/0         0/0           Gi0/2         0K         0K         Not Connected         0/0         0/0         0/0         0/0           Gi0/3         0K         0K         Not Connected         0/0         0/0         0/0         0/0           Gi0/4         0K         0K         Not Connected         0/0         0/0         0/0         0/0           Te0/5         0K         0K         Not Connected         0/0         0/0         0/0         0/0         0/0	Coun
Gi0/2         OK         Not Connected         O/O         O/O         O/O           System         Gi0/3         OK         OK         Not Connected         0/O         0/O <td>0</td>	0
Gi0/3         OK         Not Connected         O/O         O/O         O/O           Gi0/4         OK         OK         Not Connected         0/O         0/O         0/O           Te0/5         OK         OK         Not Connected         0/O         0/O         0/O	0
Gi04         0K         Not Connected         0/0         0/0         0/0           Te0/5         0K         0K         Not Connected         0/0         0/0         0/0	0
Te0/5 0K 0K Not Connected 0/0 0/0 0/0	0
	0
Te0/6         0K         Not Connected         0/0         0/0         0/0	0
Show No.: 10 ▼ Total Count6 I4 First 4 Pro 1 Next ▶ Last ▶	) 1 GC

## 1 Note

For details about Eweb pages, see Eweb Management System.

# 1.3 Eweb Management System

# **Basic Concepts**

Icons and Buttons on the GUI

#### Table 1-2

Icon/Button	Description
Edit	Edit the selected record.

Delete	Delete the selected record.			
ON	Enable or disable the function.			
<b></b>	Available port. After you click or select the icon, the port becomes selected.			
宣	Unavailable port.			
<b></b>	Selected port.			
5î	Aggregated port. The digit in the port indicates the number of the aggregated port.			
<u>5</u> 2'	Trunk port. It is displayed on the panel of the VLAN Management/VLAN Settings page.			
Save	Submit and save input information.			
+	Add settings.			
×	Delete settings.			
<u>All Invert</u> Desele	Batch configuration of panel ports, which is on the right bottom corner of the panel. Note:			
	Note: You can use this function only when you can select multiple ports on the panel.			
*	An input box marked with this symbol indicates that the item is mandatory.			

# Features

The following table describes feature configurations of secondary menu items in the left navigation tree of the web GUI.

# Table 1-3

Feature	Description
Home	Displays port information and overall device information.
VLAN Management	Sets VLANs and trunk ports.
Port Management	Configures basic information about ports, aggregated ports, port mirroring, and port rate limit.
POE Settings	Configures PoE in the system and on ports.

Restart	Restart the switch.	
MAC Address	Sets static addresses and filter addresses.	
Routing	Sets routes.	
STP	Configures basic information of global STP, STP ports, and RLDP.	
IGMP Settings	Sets Internet Group Management Protocol (IGMP) snooping.	
DHCP Snooping	Sets DHCP snooping.	
Gateway Anti-ARP- Snooping	Configures anti-ARP-spoofing on the gateway, Address Resolution Protocol (ARP) check, dynamic ARP inspection (DAI), and ARP entries.	
IP Source Guard	Configures ports and user binding.	
NFPP	Displays information related to Network Foundation Protection Policy (NFPP).	
Storm Control	Control storms.	
Port Protection	Configures port protection.	
ACL	Configures access control lists (ACLs), set the ACL time, and applies ACLs.	
Settings	Sets the system time, changes the password, restores to factory settings, and configures the enhancement function, SNMP and DNS.	
Upgrade	Performs local upgrade and online upgrade of web packages.	
System Logging	Sets the log server and queries system logs.	
CWMP	Configures CPE WAN Management Protocol (CWMP).	
Detection	Configures ping test, tracert test, cable detection, and one-click collection.	
Web Console	Imitates the mechanism of CLI commands.	

# **1.3.1 Initialization Configuration**

# Figure 1-4 Initialization Configuration

Wizard		×
Mgmt Port:	Gi0/1	
IP:	172.26.147.230	:
Mask:	255.255.255.0	
Gateway:	172.26.147.1	
DNS:	114.114.114.114	
IPv6/Mask:		
IPv6 gateway:		
Reset Time:	2022-10-21 12:35	
Time Zone:	UTC+8(Beijing, CCT) ~	
	Save Cancel	

Configure the management VLAN ID, IP address, subnet mask, default gateway and DNS server. Click **Save** and the message "Configuration succeeded." is displayed.

# 1.3.2 MACC Management

Figure 1-5 MACC Management

Access MACC	×
The device can connect to MACC.	Î
✓ 1. Local IP:172.26.147.230	7
<ul> <li>2. Default Gateway: 172.26.147.1</li> </ul>	
✓ 3. DNS Server: 114.114.114.114	- 1
Check Connectivity	
Scan the QR code to get easy access to MACC.	
	Cancel

After configuring the device IP, default gateway and DNS server, click **Check Connectivity** to check whether the device connects to MACC. Scan the QR code to add the device to MACC.

# 1.3.3 Common

Click the primary menu **Common** to access the secondary menu, including **Home**, **VLAN Management**, **Port Management**, **PoE Settings** and **Restart**.

# 1. Home

The Home page displays device configurations, basic port information, and port statistics.

Figure 1-6 shows the **Home** page.

## Figure 1-6 Home

Home							
CPU: <b>5.40%</b>	6 Memory: 50.0%	1 C: Up Port Count	urrent Time:2022-10-21 12:37:28 unning Time:1 d 21 h 10Min	Model: Version: Device Device SN:			
	ormation CREfresh						
Port	Input Rate 🌲	Output Rate 🌲	Status(Port real speed)	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count
Gi0/1	27.9K	34.2K	Connected(1000M)	2702243805/12890773	0/0	0/0	0
Gi0/2	ок	0K	Not Connected	0/0	0/0	0/0	0
Gi0/3	ок	0K	Not Connected	0/0	0/0	0/0	0
Gi0/4	ок	0K	Not Connected	0/0	0/0	0/0	0
Te0/5	ОК	0K	Not Connected	0/0	0/0	0/0	0
Te0/6	0К	0K	Not Connected	0/0	0/0	0/0	0
Show No.: 10	0 → Total Count:6				🛿 First 🖣 Pre	e 1 Next ▶ Last ▶	1 GO

# 2. VLAN Management

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

(1) VLAN Settings

Figure 1-7 shows the VLAN Settings page.

# Figure 1-7 VLAN Settings

VLAN Settings	Trunk Port					
+ Batch Add VLAN	+ Add VLAN	X Delete	e Selected VLAN			
	VLAN ID	\$	VLAN name	Port		Action
	1		VLAN0001	Gi0/2,Gi0/4,Te0/5-6		Edit
	2		test2	Gi0/3		Edit Delete
Show No.: 10 V	Total Count:2			🔣 Fir	rst 🖣 Pre	1 Next ▶ Last ▶ 1 GO
			@2000	2024 Ruille Nebuerke Co. 1 tel 1 Offi	aial Mahaita	I Service Redel I Online Service I Service M

# • Adding a VLAN

The VLAN ID is mandatory. Other parameters are optional. Click **Save** and the message "Configuration succeeded." is displayed. The added VLAN is displayed in the list.

• Editing a VLAN

In the VLAN list, click **Edit** in the **Action** column for a VLAN. Information about the VLAN is displayed. Edit the information, click **Save**. The message "Edit succeeded" is displayed.

- Deleting a VLAN
  - o Select multiple records in the VLAN list and click Delete Selected VLAN to delete the records in a batch.
  - in the VLAN list, click **Delete** in the **Action** column for a VLAN. The message "Are you sure you want to delete the VLAN ?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the VLAN is deleted.

#### 🚺 Note

VLAN 1 is the default VLAN. It can be only modified but cannot be deleted.

#### (2) Trunk Port

Figure 1-8 below shows the Trunk Port page.

Figure	1-8	Trunk	Port
--------	-----	-------	------

VLAN Settings Tru	ink Port						
Note: If a port allows multiple	VLAN packets to go throug	, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.					
No Trunk Port							
Native VLAN:	1	* Range(1-4094)					
Allowed VLAN:	1-4094	Range(3-5,200)					
Select Port:							
$\begin{array}{c c} \hline \begin{array}{c} \hline \\ \hline $	Available       Image: Im						
All Invert Deselect	Note:Click and ho	i the left button as you drag the pointer across the section to select multiple ports.					
	Save C	ncel					

#### Adding a Trunk Port

Select a port on the panel, enter the ranges of Native VLAN and Allowed VLAN (3-5,8,10 for example). Click **Save**. The message "Configuration succeeded" is displayed. The added trunk port is displayed in the trunk port list.

#### • Editing a Trunk Port

Select a trunk port in the trunk port list. Its information is displayed. Edit the information and click **Edit**. The message "Configuration succeeded" is displayed.

#### Deleting a Trunk Port

Move the cursor to a trunk port in the trunk port list, click **Delete**. The message "Are you sure you want to delete the trunk port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the trunk port is deleted.

#### Batch Deleting Trunk Ports

In the trunk port list, select trunk ports to be deleted and click **Batch Del**. The message "Are you sure you want to delete the trunk port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the trunk ports are deleted.

#### 3. Port Management

The Port page allows you to configure basic settings about ports, aggregate port, and port mirroring.

(1) Port Settings

#### Figure 1-9 Port Settings

Port Settings	Aggregate port	Port Mirroring									
+ Batch Add + A	+ Batch Add + Add SVI										
E L3 Port											
Port	Up/Down	IP		Ma	ask		IPv6	Des	cription	Act	ion
Gi0/1	Down									Edit	Delete
Gi0/8	Up	10.110.69	9.99	255.25	5.255.0					Edit	Delete
VLAN 1	Up									Edit	Delete
Show No.: 10 V	Total Count:3						H First	t 🖣 Pre	1 Next 🕨 Las	st 🕨 🚺 1	GO
= 12 Port											
Port	Up/Down	Port Type	Acces	ss VLAN	Native V	LAN	Permit VLA	N	Description	A	ction
Gi0/2	Down	ACCESS		1	1					Edit	Detail
Gi0/3	Down	ACCESS		1	1					Edit	Detail
Gi0/4	Down	ACCESS		1	1					Edit	Detail
Gi0/5	Down	ACCESS		1	1					Edit	Detail
Gi0/6	Down	ACCESS		1	1					Edit	Detail
Gi0/7	Down	ACCESS		1	1					Edit	Detail
Gi0/9	Down	ACCESS		1	1					Edit	Detail
Gi0/10	Down	ACCESS		1	1					Edit	Detail
Gi0/11	Down	ACCESS		1	1					Edit	Detail
Gi0/12	Down	ACCESS		1	1					Edit	Detail
Show No.: 10 V	Total Count:30						I4 First ◀ P	re <b>1</b> 2	3 Next 🕨 Las	st 🎽 🚺 1	GO

#### Batch Configuring Ports

Select ports to be configured and select the port status, rate, and mode. **Keep** indicates that the system retains the original configuration. You can set **Keep** for some settings to batch configure only one or two settings.

#### Editing a Port

Click **Edit** in the **Action** column of the port list. The port information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

#### (2) Port Aggregation

Figure 1-10 shows the Aggregate Port page.

#### Figure 1-10 Aggregate Port

Port Settings	Aggregate port	Port Mirroring	
≘ Global Configu	uration		
Note:the aggregat	te port is used to perform	traffic allocation accordi	ig to the selected load-balance algorithm.
Load-ba	alance: Source MAC ar	nd Destination $\mathbf{v}$	
	Save	Default Settings	
Ξ Aggregation p	ort settings		•
In order to provide balances traffic ac	e increased bandwidth an cross these physical ports	nd redundancy, multiple p s.Only supports static AP	hysical ports (member ports) are combined into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load aggregation.
AG1	AG2 A	.G3 AG4	Batch Del
Aggregate	Port ID:	*	Range(1-8)
P	ort Type: 💿 L2 Port(Sv	vitching Port) 🔿 L3 Int	erface(Routing Interface)
Sel	lect Port:		
Available	Unavailable <u> Selecte</u> 9 11 13 15 17	d 11 AG Port	Copper Fiber
			27 28
All Invert Dese	lect Note:C	lick and hold the left buttor	as you drag the pointer across the section to select multiple ports.
	Add	Cancel	

#### Adding an Aggregated Port

Enter an aggregated port ID, select member ports, and click **Add**. The message "Configuration succeeded." indicating that the aggregated port is added. The port panel displays the successfully added aggregated port.

• Editing an Aggregated Port

Aggregated ports displayed on the panel cannot be selected. To edit an aggregated port, click the aggregated port in the aggregated port list. Its member ports become selected. Click a port to cancel selection and then click **Edit** to modify the aggregated port.

• Deleting an Aggregated Port

In the aggregated port list, move the cursor to an aggregated port and click **Delete**. The message "Are you sure you want to delete the aggregate port?" is displayed. Click **OK** to delete the aggregated port. After being deleted, the aggregated port on the panel will become available.

Batch Deleting Aggregated Ports

In the aggregated port list, select aggregated ports to be deleted and click **Batch Del**. The message "Are you sure you want to delete the aggregate port?" is displayed. Click **OK** to delete the aggregated ports. After being deleted, the aggregated ports on the panel will become available.

#### 🛕 Caution

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

#### (3) Port Mirroring

Figure 1-11 shows the **Port Mirroring** page.

#### Figure 1-11 Port Mirroring

Port Settings	Aggregate port	Port Mirroring	
Note: Port mirroring Tip: A source port of	g is the capability to send a cannot be a destination port	copy of network packets s	een on the source port to the destination port for analysis by a network analyzer. Traffic on multiple source ports can be mirrored to one single destination port.
No session			
	Session ID		* Range(1-4)
Moni	tor Packets: All Packets	s v	
Select \$	Source Port: (You can se	elect multiple ports, but it r	nay affect device performance.)
Available	Inavailable         Selected           9         11         13         15         17         12           11         13         15         17         12         12         12         12         12         12         12         12         12         12         13         15         17         12         14         16         18         12         13         15         13         12         12         14         16         18         12         14         16         18         12         12         14         16         18         12         14         16         18         12         14         16         18         12         14         16         18         12         14         16         18         12         14         16         18         12         14         16         18         12         14         16         18         12         12	AG Port           19         21         23           19         21         23           10         12         12           10         12         12           10         12         12         1           10         22         24         25         26           10         22         24         25         26           10         and hold the left button a         1	Copper Fiber 7 28 27 you drag the pointer across the section to select multiple ports.
Select	Destination Port: (You	can select only one port.)	
$\begin{array}{c} \textcircled{\ } \text{Available } \textcircled{\ } \textcircled{\ }          \textbf$	Inavailable         Selected           9         11         13         15         17         15           1         1         15         17         15         17         15           1         1         15         17         15         15         15         15           1         1         13         15         17         15         15         15           1         1         13         15         17         15         15         15           10         12         14         16         18         15         15         16         18         15	19     21     23       19     12     1       10     12     1       11     12     1       12     12     1       12     12     1       12     12     1       12     12     1       12     12     1	Copper Fiber
Deselect	Save	cancel	

The initial port mirroring page is in editing state because only one mirrored port can be configured on the Eweb. There are two panels on the interface. The port selected on the top panel will serve as the mirrored port. You can select multiple mirrored ports. You can select only one port on the bottom panel to serve as the observing port. Select or modify the port on the panel, click **Save**. The message "Configuration succeeded." is displayed.

#### Note

The panel displays the current port mirroring status, and both the source and destination ports can be edited. To cancel modification of port information, click Refresh to restore the panel to the current port mirroring status.

#### 🛕 Caution

A member port of the aggregated port cannot be configured as the mirrored or observing port, and the mirrored and observing ports must be different.

# 4. PoE Settings

You can configure PoE on a port or in the system on the **PoE Settings** page. This page is available only for PoE-capable devices.

(1) PoE Port

#### Figure 1-12 PoE Port Settings

PoE Port	Global Settings									
+ Batch Add										
Port	PoE Status	Power On/Off	Max Power	Current Power	Priority	Non-standard Mod e	Action			
Gi0/1	Enable	Off	N/A	0.0W	Low	Disable	Edit			
Gi0/2	Enable	Off	N/A	0.0W	Low	Disable	Edit			
Gi0/3	Enable	Off	N/A	0.0W	Low	Disable	Edit			
Gi0/4	Enable	Off	N/A	0.0W	Low	Disable	Edit			
Show No.: 10 ∽ Total Count:4 I First 4 Pre 1 Next ▶ Last ▶ 1 GO										

#### • Batch Configuring Ports

Select ports to be configured, and configure the PoE function, power supply priority, maximum power, current power, and non-standard mode. Click **Save**. The message "Configuration succeeded." is displayed.

• Editing a port

Click **Edit** in the **Action** column of the port list and the port information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

(2) Global Settings

#### Figure 1-13 Global Settings

PoE Port	Global Settings
Tota	I Power: 36.0 W
Free	e Power: 36.0 W
Power Mana	agement Power Saving ~ Mode:
	Save

The page displays the total power, free power, and power supply management mode. Select a power supply management mode and click **Save** to configure the port.

#### 5. Restart

Figure 1-15 shows the **Restart** page.

#### Figure 1-14 Restart

Restart	
Note: Click 'F	Restart' to restart the device. Please wait a few minutes and the page will be refreshed after restart.
	Restart

Click **Restart**. The message "Are you sure you want to restart the device?" is displayed. Click **OK** to restart the device. Wait for a few minutes. The page will refresh after restart.

# 1.3.4 Network

Click the primary menu **Network** to access the secondary menu, including **MAC Address**, **Routing**, **STP**, and **IGMP Snooping**.

### 1. MAC Address

The MAC Address page includes Static Address Settings and Filtering Address Settings pages.

(1) Static Address Settings

Figure 1-16 shows the Static Address Settings page.

#### Figure 1-15 Static Address Settings

Stat	Static Address Settings Filtering Address Settings								
Note swite bind	Note: The switch forwards data according the MAC address inside the data frame. If you configure MAC-port binding on a network device manually, after you add a static address, the switch that receives the packet with the same destination address forwards it to the specified port. With 802.1X authentication enabled, you can implement authentication exemption by binding MAC address with port.								
	Port		MA	C Address	VLAN ID		Action		
	GigabitEthernet 0/4 2244.2266.6622 2 Delete								
Show	Show No.: 10 ∨ Total Count:1 II First 4 Pre 1 Next ▶ Last II GO								

• Adding a Static Address

You must enter a MAC address and a VLAN ID and select a port to add a static address. Click **Save**. The message "Configuration Succeeded." is displayed. The added static address is displayed in the static address list.

- Deleting a Static Address
  - Select multiple records in the static address list and click **Delete Static Address** to batch delete the records.
  - In the static address list, click **Delete** in the **Action** column for a static address. The message "Are you sure you want to delete the static address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed.
- (2) Filtering Address Settings

Figure 1-17 shows the Filtering Address Settings page.

#### Figure 1-16 Filtering Address Settings

Static Address Setting	Static Address Settings Filtering Address Settings								
Note: The switch forwards data according the MAC address inside the data frame. If a switch receives a packet with the source/destination MAC address which is configured as a filter address, it discards the packet. You can prevent the ARP attack by configuring a filter address the same as the MAC address of ARP packets.									
	MAC Address	VLAN ID	Action						
0002.0002.0003 4 Edit Delete									
Show No.: 10 V Total Count:1 I GO									

• Adding a Filter Address

You must enter an MAC address, a VLAN ID to add a filter address. Click **Save** and the message "Configuration Succeeded." is displayed. The added filter address is displayed in the filter address list.

• Editing a Filter Address

In the filter address list, click **Edit** in the **Action** column for a filter address. The address information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Filter Address
  - o Select multiple records in the static address list and click Delete Filter Address to batch delete the records.
  - In the filter address list, click **Delete** in the **Action** column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed.

### 2. Routing

The Routing page allows you to manage routes.

Figure 1-18 shows the Routing Settings page.

#### Figure 1-17 Route Settings

Rout	te Settings							
Note: Route selection points based routing and a backup route when the primary route does not take effect, it will take a backup route to the backup route in accordance with the priority level configured to go, the backup route priority 1 high priority than a backup route to the 2.								
	Destination Subnet         Subnet Mask         Next Hop Address         Egress Port         Administrative Dista nce         Type         Action							
	0.0.0.0	0.0.0.0	172.26.147.1		1	Default Route	Edit Delete	
Show No.: 10 V Total Count:1								

#### • Adding a Static Route

You must select an IP type and enter a destination subnet, a subnet mask, and a next-hop address to add a static address. Click **Save**. The message "Configuration Succeeded." is displayed. The added static route is displayed in the route list.

• Editing a Route

In the route list, click **Edit** in the **Action** column for a route. Route information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

Deleting a Route

- o Select multiple records in the route list and click Delete Selected Route to batch delete the records.
- In the filter address list, click **Delete** in the **Action** column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed.
- Adding a Default Route

Select an IP type and enter a next hop address to add a default route. Click **Save**. The message "Configuration Succeeded." is displayed. The added default route is displayed in the route list.

#### 🚺 Note

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

# 3. STP

The STP page allows you to configure STP global parameters, STP ports, and RLDP.

(1) STP Global Settings

#### Figure 1-18 STP Global Settings

STP Global S	Settings STP Port Set	ttings RLDP Settings							
Ξ Global Con	≘ Global Configuration								
STP:	ON								
Priority:	8	Range(0-15), default 8	Hello Time 2	Range(1-10s), default 2					
Aging Time:	20	Range(6-40s), default 20 Fe	orward Delay: 15	Range(4-30s), default 15					
STP Mode:	MSTP ~								
MST Name:		String less than 32-byte	MST Version: 0	Range(0-65535), default 0					
	Save								
E MST Config	guration								
Note: It is reco	ommended to disable STP befo	ore configuring an instance and e	enable STP again after configur	ation, so as to ensure the stability and convergence	of network topology.				
+ Add Instance X Delete Selected Instance									
	Instance Number		VLAN	Priority	Action				
	0		ALL	8	Default instance. Cannot be edited.				
Show No.: 10	Show No.: 10 V Total Count:1 If First 4 Pre 1 Next 1 GO								

You can configure STP global parameters. When **STP Mode** is set to **MSTP**, you can configure an MST instance (MSTI).

• Adding a MSTI

The MSTI ID and VLAN range are mandatory. Other parameters are optional. Click **Save**. The message "Configuration Succeeded." is displayed. The added MSTI is displayed in the MSTI list.

Editing a MSTI

In the MSTI list, click **Edit** in the **Action** column for an MSTI. MSTI information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

Deleting a MSTI

- o Select multiple records in the MSTI list and click Delete Selected Instance to batch delete the records.
- In the MSTI list, click **Delete** in the **Action** column for an MSTI. The message "Are you sure you want to delete the instance?" is deleted. Click **OK**. The message "Delete succeeded." is displayed, indicating that the MSTI is deleted. MSTI 0 is the default one and cannot be deleted.
- (2) STP Port Settings

#### Figure 1-19 STP Port Settings

	STEPOILSE	aungs					
tch Add							
e: It is recommende	ed to enable Port Fast or	n the port connected to the	PC.				
Port	State	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance Cost Priori ty	Actio
Gi0/2	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Gi0/3	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Gi0/4	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Te0/5	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Te0/6	Down	Disabled	Disabled	Null	Point To Point	0 0 128	Edit

#### Batch Adding STP Ports

Select a protection mode, a connection mode, a port priority, and whether to enable Port Fast and BPDU Guard. Select ports to be batch configured and click **Save**.

• Editing an STP Port

In the STP port list, click **Edit** in the **Action** column for an STP port. Port information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

(3) RLDP Settings

#### Configuring Switch Eweb

#### Web-based Configuration Guide

STP Global Settings	STP Port Settings	RLDP Settings						
<b>Ξ</b> Global configuration	n							
Note: RLDP enables you	to detect link failure quickly.	RLDP can run on the port	only after it is enabled globally.					
RLDP: ON								
Detection 3	1	Range(2-15)						
Interval:								
Detection Count: 2	ł	Range(2-10)						
errdisable	F	Range(30-86400s)						
recovery:								
Sav	Save							
⊒ Port Configuration								
Note: 1. Enabling RLDP 2. Unidirectional/B between two switches; 3.An aggregate po	on the port can avoid broadca idirectional link detection requ rt can only be configured with	ast storm caused by loops uires the ports on both en n port violation or alarm. L	b. It is recommended to enable RLDP on ds of the link to be enabled with RLDP. I oop detection on a member port will be	the port connected to the PC ; t is recommended to configure RLDP to monitor the link synchronized to other member ports.				
+ Add Port × Delete Port								
	Port	Detect	tion Type:Troubleshooting	Action				
		No	Record Found					
Show No.: 10 V Tota	al Count:0			I First ∢ Pre Next ▶ Last ▶ 1 GO				

#### (4) RLDP Global Configuration

Click **RLDP** to enable or disable the RLDP function. When the RLDP function is enabled, set a detection interval and detection count. Click **Save**. The message "Configuration Succeeded." is displayed.

(5) RLDP Port Configuration

• Adding an RLDP-enabled Port

Select the detection modes, troubleshooting and a port. Click **Save** and the message "Save Succeeded." is displayed., indicating that an RLDP-enabled port is added. The added RLDP-enabled port is displayed in the RLDP-enabled list.

• Editing an RLDP Port

In the RLDP-enabled port list, click **Edit** in the **Action** column for an RLDP-enabled port. Port information is displayed. Edit the information and click **Save**. The message "Save succeeded" is displayed.

- Deleting an RLDP-enabled Port
  - o Select multiple records in the RLDP-enabled port list and click **Delete Port** to batch delete the records.
  - In the RLDP-enabled port list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port is deleted.

#### 4. IGMP Settings

Figure 1-21 shows the IGMP Snooping page.

#### Figure 1-20 IGMP Snooping Settings

IGMP Snoo	ping Settings				
Note: On lay	er 2 devices, multicast frames id only send IGMP traffic to th	are flooded to all ports, causing storm e port, so as to save bandwidth.	and consuming much bandwidth. I	GMP Snooping is used to find out on w	nich port there is an IGMP
+ Add Profile	e X Delete Selected Pro	file IGMP Snooping: ON			
	Profile ID	Multicast Address	Policy Action	Application Port	Action
			No Record Found		
Show No.:	10 🗸 Total Count:0			I¶ First ∮ Pre Ne	xt ▶ Last № 1 GO

• Adding a Profile

The profile ID and multicast address range are mandatory. Other parameters are optional. Click **Save**. The message "Configuration Succeeded." is displayed. The added profile is displayed in the profile list.

• Editing a Profile

In the profile list, click **Edit** in the **Action** column for a profile. Profile information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Profile
  - o Select multiple records in the profile list and click Delete Selected Profile to batch delete the records.
  - In the profile list, click **Delete** in the **Action** column for a profile. The message "Are you sure you want to delete the profile?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the profile is deleted.

# 1.3.5 Security

Click the primary menu Security to access the secondary menu, including DHCP Snooping, Gateway Anti-ARP-Snooping, IP Source Guard, NFPP and Storm Control.

#### 1. DHCP Snooping

Figure 1-25 shows the DHCP Snooping page.

# Figure 1-21 DHCP Snooping

DHCP Snooping
Note: DHCP snooping is used to filter DHCP packets received on an untrusted port from outside the network or firewall. The DHCP request packet is forwarded to the trusted port. The DHCP reply packet is forwarded only if it is from a trusted port. Note: The port connected to the DHCP server is configured as a trusted port generally.
DHCP Snooping: ON
Select Port:
Available       Invaliable       Selected       A G Port       Copper       Fiber         1       3       5       7       9       11       13       15       17       19       21       23         1       3       5       7       9       11       13       15       17       19       21       23         1       2       4       6       8       10       12       14       16       18       20       22       24       25       26       27       28
All Invert.         Deselect         Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.           Save         Display DHCP Snooping Trusted Port

The port connected to a DHCP server needs to be configured as a DHCP trusted port. The DHCP server connected to a non-trusted port cannot work properly. The selected port is configured as a DHCP trusted port. You can select ports on the panel and click **Save**.

### 2. Gateway Anti-ARP-Snooping

The Gateway Anti-ARP-Snooping page allows you to configure DAI settings and ARP entries.

(1) DAI Settings

#### Figure 1-22 DAI Settings

DAI Settings ARP Entries
E VLAN DAI Configuration
Note: The untrusted port corresponding to the DAI-enabled VLAN intercepts all ARP request and reply packets to discard invalid ARP packets.
DAI-enabled VLAN: [Delete All Configuration]
<u> </u>
Note: Packets received on the trusted port skip DAI Inspection as valid ARP packets.
Select Port:
∫ Available 🚰 Unavailable 🚰 Selected ∫1 AG Port
1 3 5 7 9 11 13 15 17 19 21 23
All Invert Deselect Note: Click and hold the left button as you drag the pointer across the section to select multiple ports.
Save Lispiay Trusted Port
VI AN DAI Settings

- Click the add icon to add a VLAN where DAI is enabled.
- DAI Trusted Port

Select a port on the panel to enable the DAI trusted port.

#### 🚺 Note

The panel displays DAI trusted ports and the ports can be edited. To cancel modification of a port, click **Display Trusted Port** to display current DAI trusted ports on the panel.

#### 🛕 Caution

The ARP check function cannot be enabled on DHCP snooping trusted ports.

#### (2) ARP Entries

#### Figure 1-23 ARP Entries

DAI	Settings <u>ARP Entries</u>			
🔡 Dyn	amic Binding>>Static Binding	🕆 Remove static Binding 🛛 🍒 Manual Binding	IP-based:	Search
	IP	MAC	Туре	Action
	10.110.69.1	8005.889b.1447	Dynamic Binding	Dynamic Binding>>Static Binding
	10.110.69.3	0074.9c03.f1ab	Dynamic Binding	Dynamic Binding>>Static Binding
	10.110.69.31	00d0.f822.3546	Dynamic Binding	Dynamic Binding>>Static Binding
	10.110.69.99	0000.f823.0111	Local ARP Entry	Dynamic Binding>>Static Binding
	10.110.69.111	1082.3d95.47ef	Dynamic Binding	Dynamic Binding>>Static Binding
Show	No.: 10 Y Total Count: 5		I4 First ∢ Pro	e 1 Next ▶ Last ▶ 1 GO

- Dynamic binding >> static binding
  - Select multiple dynamic binding entries in the ARP entry list and click Dynamic Binding >> Static Binding.
  - In the ARP entry list, click Dynamic Binding >> Static Binding in the Action column for an ARP entry.
     The message "Configuration succeeded." is displayed.
- Removing a Static Bindings
  - Select multiple static binding entries in the ARP entry list and click **Remove Static Binding** to batch remove static bindings.
  - In the ARP entry list, click Remove Static Binding in the Action column for a static binding entry. The message "Configuration succeeded." is displayed.
- Manual binding

You must enter an IP address and a MAC address to add a static binding entry. Click **Save**. The message "Configuration Succeeded." is displayed. The added static binding entry is displayed in the port filter list.

#### 3. IP Source Guard

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

(1) Port Settings

#### Figure 1-24 Port Settings

Port Setti	ings User I	Binding						
Note: IP Source Guard is applied in combination with DHCP Snooping. Port-based IP Source Guard takes effect on only the untrusted port enabled with DHCP Snooping. Otherwise,								
IP Source Guard does not take effect.								
Add Por	t X Delete Sele	cted Port						
	Port	Filter Type	Filter Mode	IP	MAC	VLAN ID	Action	
	Gi0/4	IP-ONLY	Active	Deny-All			Delete	
Show No.:         10 ~         Total Count:1         I GO								

#### • Adding a Port Enabled with IP Source Guard

Click **Add Port** and select a filter type and a port to add a port enabled with IP source guard. Click **Save**. The message "Configuration Succeeded." is displayed. The added port is displayed in the list of ports enabled with IP source guard.

Editing a Port Enabled with IP Source Guard

In the list of ports enabled with IP source guard, click **Edit** in the **Action** column for a port. Port information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Port Enabled with IP Source Guard
  - Select multiple records in the list of ports enabled with IP source guard and click **Delete Selected Port** to batch delete records.
  - In the list of ports enabled with IP source guard, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port is displayed.
- (2) User Binding

#### Figure 1-25 User Binding

Port Setti	ngs User Binding							
Note: The IP Source Guard-enabled port filters all non-DHCP IP packets. After configured with the static IP address, the port allows specified IP packets to pass through.								
+ Add Binding X Delete Selected Binding								
	MAC	IP	VLAN ID	Port	Action			
			No Record Found					
Show No.:	: 10 V Total Count:0			li First ∢ Pre No	ext ▶ Last ▶ 1 GO			

#### Adding a User Binding

You must enter a MAC address, an IP address, and a VLAN ID to add a user binding. Click **Save**. The message "Configuration Succeeded." is displayed. The added binding is displayed in the user binding list.

• Editing a User Binding

In the user binding list, click **Edit** in the **Action** column for a user binding. Binding information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is deleted.

- Deleting a User Binding
  - o Select multiple records in the user binding list and click **Delete Selected Binding** to batch delete records.

O In the user binding list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the binding?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the binding is displayed.

#### 4. NFPP

Figure 1-34 shows the NFPP page.

rigure 1-20 NFPP	Figure	1-26	NFPP
------------------	--------	------	------

NFPP Settings	
ARP-guard:	Enable ARP-guard, so as to prevent a large number of invalid ARP packets from attacking the device. [ARP-guard List]
IP-guard:	Enable IP-guard, so as to prevent hackers from scanning the entire network and consuming bandwidth. [IP-guard List]
ICMP-guard:	Enable ICMP-guard, so as to prevent a large number of invalid ICMP packets from consuming bandwidth and CPU resources. [ICMP-guard List]
DHCP-guard:	Enable DHCP-guard, so as to prevent malicious requests from exhausting DHCP pools and leaving legitimate users unable to access the Internet.           [DHCP-guard List]
DHCPv6-guard:	Enable DHCPV6-guard, so as to prevent malicious requests from exhausting DHCPv6 pools and leaving legitimate users unable to access the Internet.           [DHCPv6-guard List]
ND-guard:	Enable ND-guard, so as to prevent Neighbor Discovery packets from consuming bandwidth.
Display NFPP Log:	[Display NFPP Log]
	Save Restore Default Settings

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

#### 5. Storm Control

Figure 1-35 shows the Storm Control page.

Storm Control								
+ Add Port X Delete Selected Port								
	Port	Broadcast	Multicast	Unicast	Action			
	Gi0/1	-	-	-	Edit Delete			
	Gi0/2	-	-	-	Edit Delete			
	Gi0/3	-	-	-	Edit Delete			
	Gi0/4	-	-	-	Edit Delete			
	Te0/5	-	-	-	Edit Delete			
	Te0/6	-	-	-	Edit Delete			
Show No.	.: 10 V Total Count:6			I∢ First ∢ Pre 1 Ne	ext ▶ Last ▶ 1 GO			

• Adding a Port Enabled with Storm Control

You must enter one of the broadcast address, unicast address, and multicast address to add a port enabled with storm control port. Click **Save**. The message "Configuration Succeeded." is displayed. The added port is displayed in the list of ports enabled with storm control.

• Editing a Port Enabled with Storm Control

In the list of ports enabled with storm control, click **Edit** in the **Action** column for a port. Information about the port enabled with storm control is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a Port Enabled with Storm Control
  - Select multiple records in the list of ports enabled with storm control and click **Delete Selected Port** to batch delete records.
  - O In the list of ports enabled with storm control, click **Delete** in the Action column for a port. The message "Are you sure you want to delete the storm control port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port enabled with storm control is deleted.

# 1.3.6 Advanced

#### 1. Port Protection

Figure 1-36 shows the Port Protect page.

#### Figure 1-28 Port Protect

Port Protect
Note: Proteced 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.
Select Port:
Available       Unavailable       Selected       AG Port       Copper       Fiber         1       3       5       7       9       11       13       15       17       19       21       23         2       4       6       8       10       12       14       16       18       20       22       24       25       26       27       28
All Invert Deselect Note:Click and hold the left button as you drag the pointer across the section to select multiple ports.           Save         Display Protected Port

Select a port on the panel to be configured as a protected port. Click **Save**. The message "Configuration Succeeded." is displayed.

# 2. ACL

#### (1) ACL List

Figure 1-40 shows the ACL List page.

#### Figure 1-29 ACL List

AC	L List	ACL Time	ACL Applica	ation							
ACL I	ACL List: Add ACL Delete ACL + Add Access Rule Delete Selected Access Rule										
	NO.	Source IP/Wild card	Source Port	Access Control	Protocol	Destination IP/ Wildcard	Destination por t	Time Period	Status	Action	
	No Record Found										
Sho	w No.:	10 🗸 Total Coun	nt:0				I	IFINIT IFINITE	Next 🕨 Last 🕅	, 1 GO	

Adding an ACL

Click **Add ACL** and configure the ACL to be added. You must enter an ACL. Click **Save**. The message "Configuration succeeded." is displayed. The added ACL is displayed in the ACL list.

• Deleting an ACL

In the ACL list, select the ACL to be deleted and click **Delete ACL**. The message "Delete succeeded." is displayed.

• Adding an ACL Rule

Select an ACL type, a protocol, and a time period, and configure an IP address to add an ACL rule. Click **Save**. The message "Configuration succeeded." is displayed. The added ACL rule is displayed in the ACL rule list.

• Editing an ACL Rule

In the ACL rule list, click **Edit** in the **Action** column for a rule. ACL rule information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting an ACL Rule
  - Select multiple records in the ACL rule list and click **Delete Selected Access Rule** to batch delete records.
  - O In the ACL rule list, click **Delete** in the **Action** column for a rule. The message "Are you sure you want to delete the rule?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the rule is deleted.
- Moving an ACL Rule

Enter the ID of an ACL rule to be moved and click Move. The message "Configuration succeeded." is displayed.

(2) ACL Time

Figure 1-41 shows the ACL Time page.

#### Figure 1-30 ACL Time

ACL List	ACL Time	ACL Application								
Note: The ACL active time must be periodic.										
+ Add Time O	+ Add Time Object X Delete Selected Time Object									
	Time Object	t	Day	Time Period	Action					
	No Record Found									
Show No.: 1	Show No.: 10 → Total Count:0 I First 《 Pre Next » Last » 1 GO									

Adding ACL Time

Enter the time object name and select a time period to add an ACL time. Click **Save**. The message "Configuration succeeded." is displayed. The added ACL time is displayed in the ACL time list.

Editing ACL Time

In the ACL time list, click **Edit** in the **Action** column for an ACL time. ACL time information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

Deleting ACL Time

Select multiple records in the ACL time list and click **Delete Selected Time Object** to batch delete records.

(3) ACL Application

Figure 1-42 shows the ACL Application page.

ACL List	ACL Time ACL Ap	olication						
+ Add Por	t X Delete Port							
	ACL	Port	Direction	Action				
	99	Te0/5	in	Edit Delete				
Show No.	Show No.:         10 ∨         Total Count:1         I ← First ← Pre         1         GO							

Adding an Applied ACL

Select an ACL list, a filter direction and a port and click **Save**. The message "Configuration succeeded." is displayed. The added ACL applied to a port is displayed in the applied ACL list.

• Editing an Applied ACL

In the applied ACL list, click **Edit** in the **Action** column. Applied ACL information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting an Applied ACL
  - o Select multiple records in the applied ACL list and click Delete Port to batch delete records.
  - O In the applied ACL list, click **Delete** in the **Action** column for an applied ACL. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the applied ACL is deleted.

# 1.3.7 System

The **System** page allows you to configure system settings, upload the system, configure system logging, CWMP, and network detection, and use the web console.

#### 1. Settings

The Settings page includes System Time, Password, Reset, Enhancement, SNMP and DNS.

(1) System Time

Figure 1-46 shows the **System Time** page.

#### Figure 1-32 System Time

System Time	Password	Reset	Enhancement	SNMP	DNS				
Curren	t Time: <b>2022-11</b> -	10-14:49:3	32						
Rese	t Time: Select Tim	e							
Time	Zone: UTC+0(GI	MT)	~						
Time Synchroni	zation: 🗹 Automa	tically synchro	nize with an Internet t	ime server <mark>(Ple</mark> a	ase set <u>DNS s</u>	<u>Server first, otherwi</u>	se the system	time will not be s	ynchronized.)
	Save								

• System Time

The page displays the current system time. You can set the system time manually or click **Automatically** synchronize with an Internet time server.

Select either of the two methods to set the system time. Click **Save**. The message "Configuration succeeded." is displayed.

(2) Password

Figure 1-47 shows the **Password** page.

#### Figure 1-33 Password

System Time	Password	Reset	Enhancement	SNMP	DNS	
<b>Ξ Web Managem</b>	ent Password					
User	name: admin					
Old Pas	sword		*			
New Pass	sword:		*			
Confirm Pase	sword:		*			
Ξ Telnet Passwo	Save	nable Passwo	ord)			
New Pass	sword:		*			
Confirm Pass	sword:		•			
	Save					

• Changing the Web Management Password

You need to enter the old password and enter a new password twice to change the web management password. If the input old password is incorrect, the message "Incorrect old password" in red font is displayed. You are required to enter the correct old password and click **Save** to complete the password change.

1 Note

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

• Changing the Telnet Authentication Password

To change the telnet password, you do not need to enter the old password but need to enter a new password twice. Other operations are the same as those of changing the password of the super administrator.

(3) Reset

Figure 1-48 shows the **Reset** page.

Figure	1-34	Reset
--------	------	-------

System Time	Password	Reset	Enhancement	SNMP	DNS			
E Restore Facto	ry Settings							
Note: After the de	vice is reset to the fa	actory default se	ttings, all configuration:	s will be remov	ved. Please <b>Exp</b>	ort Current Configur	ation before rese	tting the device.
Restore Fac	tory Settings							
Display Current	Configuration							
Display Current	Configuration							
∃ Import/Export	Configuration							
Note: Please don' will not take effect	t close or update the	e page during im	port, or import will fail.	lf you want to	apply the new c	onfiguration, please re	start the device o	n this page, or the configuration
File	Name:		File	Import	Export Curre	nt Configuration		

Import/Export Configuration

Import the configuration to modify the device configuration and restart the device to make the configuration take effect. Export the current configuration for backup.

• Restore Factory Settings

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

(4) Enhancement

Figure 1-49 shows the **Enhancement** page.

#### Figure 1-35 Enhancement

System Time	Password	Reset	Enhancement	SNMP	DNS	
<b>Ξ Basic Informat</b>	ion					
Web Acces	s Port: 443	* (Range:44	3,1025-65535)			
Login Tir	meout: 10 min		~			
Device Lo	cation:					
Access Redire	ection: 🗌 HTTP R	edirection to H	TTPS In NAT scene	ario, redirection m	ay cause HTTI	P access failure.
	Save					

You must set a web access port. The login timeout and device location are optional. Click **Save**. The message "Configuration succeeded." is displayed.

# (5) SNMP

Figure 1-50 shows the **SNMP** page.

#### Figure 1-36 SNMP

System Time	Password	Reset	Enhancement	SNMP	DNS	
Note: Either SNMP	/2 or SNMPv3 is sup	ported				
SNMP Ve	ersion: 💿 v2 🔾 v	/3				
Device Loc	ation:					
SNMP Comm	nunity:		*			
Trap Comm	nunity:		The Trap Com	nmunity must be ti	he same as the	SNMP Community.
Trap Recipient Ad	dress:		* You can cont	figure up to 9 Trap	o recipients. Ple	ase use ',' or press the Enter key to separate addresses.
	Save					

Select an SNMP version. The device location, SNMP community, and trap recipient address are mandatory, and other parameters are optional. Click **Save**. The message "Configuration succeeded." is displayed.

(6) DNS

Figure 1-51 shows the **DNS** page.

#### Figure 1-37 DNS

System Time	Password	Reset	Enhancement	SNMP	DNS	
DNS Se	rver 1: 114.114.11	4.114	+			
	Save					

Enter a DNS server address. Click Save. The message "Configuration succeeded." is displayed.

# 2. Upgrade

(1) Local Upgrade

The figure below shows the Upgrade Local page.

#### Figure 1-38 Upgrade Local

Upgrade Local	
Note: Please download	the corresponding software version from the official website, and then upgrade the device with the following tips.
restart the device until a	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 in upgrade succeeded message is displayed.
File Na	ne: Upgrade Cancel

Click File, select the locally saved bin file, and then click Upgrade to perform local upgrade.

# 3. System Logging

The System Logging page includes Log Server Settings and Display System Log

(1) Log Server Settings

Figure 1-53 shows the Log Server Settings page.

#### Figure 1-39 Log Server Settings

Log Server Settings	Display System Log
Note: Logging is rated on 8	ifferent 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.
Server Logging:	ON
Server IP:	•
Logging Level:	Informational(6) ~
	Save

Enter a server IP address and select a log severity. Then the device will send system logs to the corresponding server.

(2) Display System Log

Figure 1-54 shows the **Display System Log** page.

# Figure 1-40 Display System Log

Log Server Settings	Display System Log	
System Log (Show the I	ast 200 logs) Update Log	
Syslog logging: enabled		Î
Console logging: leve	l debugging, 3860 messages logged	
Monitor logging: leve	1 debugging, 0 messages logged	
Buffer logging: level	debugging, 3860 messages logged	
Standard format:false	h.	
Timestamp debug messa	ges: datetime	
Timestamp log message	s: datetime	
Sequence-number log m	uessages: disable	
Sysname log messages:	disable	
Count log messages: d	lisable	
Trap logging: level i	nformational, 3860 message lines logged, 0 fail	
Log Buffer (Total 13107	2 Bytes): have written 131072, Overwritten 96345	
*Oct 21 13:59:58: %NFPF	'_ARP_GUARD-4-RATELIMITED: Port Gi0/1 was ratelimited. (2022-10-21 5:59:58)	
*Oct 21 13:31:53: %HTTF	D-5-LOGIN: User (admin@172.26.1.107) login from eweb.	
*Oct 21 13:31:44: %HTTF	D-5-LOGOUT: User (admin@172.26.1.107) logout from eweb.	
*Oct 21 12:28:39: %HTTF	D-5-LOGIN: User (admin@172.26.1.107) login from eweb.	
*Oct 21 12:27:43: %HTTF	D-5-LOGOUT: User (admin@172.26.1.107) logout from eweb.	
*Oct 21 12:27:19: %HTTF	D-5-LOGIN: User (admin@172.26.1.107) login from eweb.	

The text box displays current system logs. Click Update Log to update logs.

# 4. CWMP

The **CWMP** page allows you to view and configure CWMP.

CWMP		
Note: The server implemen	ts the CPE WAN Management Protocol	(CWMP) to manage, configure and monitor APs, routers and switches.
CWMP:	ON	
Server URL:	https://cloud.ruijie.com.cn/service	
Server Username:		
Server Password:		
Device URL:		
Device Username:		
Device Password:		
CPE inform interval:	60	Range(30-3600s)
	Save	

Enable or disable CWMP. You can configure the server URL, server name, server password, device URL, device name, device password, and device connection interval.

# 5. Detection

The Detection page includes Ping, Tracert and Cable Detection.

# (1) Ping

Figure 1-55 shows the **Ping** page.

# Figure 1-41 Ping

Ping	Tracert	Cable Detection	
Destination	n IP or Domain		*
	name:		
Timeou	It Period (1-5) :	2	
Repetition	Count (1-100):	5	
		Detect	

Enter the destination IP and other parameters, and click **Detect**. Wait for a few minutes. The text box will display the detected results.

(2) Tracert

Figure 1-56 shows the **Tracert** page.

#### Figure 1-42 Tracert

Destination IP or Domain	•
Timeout Period (1-5) : 2	
Det	Detect

The steps of tracert test are the same as those of the ping test. Enter the destination IP and other parameters, and click **Detect**. Wait for a few minutes. The text box will display the detected results.

#### (3) Cable Detection

Figure 1-57 shows the Cable Detection page.

Ping Tracert Cable Detection				
Note: Fast port detects only A and B two pairs of core, length error 10 m				
Select Port:				
Available       Unavailable       Selected       A G Port       Copy         1       3       5       7       9       11       13       15       17       19       21       23         1       3       5       7       9       11       13       15       17       19       21       23         1       1       15       17       19       21       23       23       23       24       24       24       24       24       24       24       24       24       25       26       27       28	per Fiber			
Deselect				
Detect				

Select a port on the panel and click Detect. Wait for a few minutes. Test results will be displayed below Detect.

## Figure 1-44 Test Results

Ping Tracert Cable Detection			
Note: Fast port detects only A and B two pairs of core, length error 10 m			
Select Port:			
🕂 Available 💼 Unavailable 💼 Selected 🗂 AG Port	Copper F	iber	
1 3 5 7 9 11 13 15 17 19 21 23			
Deselect			
Detect			
Test Results:			
Port:(A / B / C / D represent four cable pairs)	State	Meters	
Gi0/13:A	Open	0	
Gi0/13:B	Open	0	
Gi0/13:C	Open	0	
Gi0/13:D	Open	0	

# 6. Web Console

The page stimulates the CLI console. Enter CLI commands in the input box, and press Enter or click **Send** to input commands. The page supports tab completion and ? command.

# Figure 1-45

Web Cli	
Console Output:	Background Color: 🔳 🔲
SF2910-JR-230#aaa	
% Unknown command.	
SF2910-JR-230#	
Command Input: show interface ? Send Clear Screen	
AggregatePort GigabitEthernet	
Loopback	
TenGigabitEthernet	