

Ruijie Reyee EST_AirMetro Series Wireless Bridges ReyeeOS 1.246.1924

Web-Based Configuration Guide



Document Version: V1.0 Date: 2024.02.04 Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 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.



Trademarks including , are owned by Ruijie Networks. 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

- Official website of Ruijie Reyee: <u>https://www.ruijienetworks.com/products/reyee</u>
- Technical Support Website: <u>https://ruijienetworks.com/support</u>
- Case Portal: <u>https://www.ruijienetworks.com/support/caseportal</u>
- Community: https://community.ruijienetworks.com
- Technical Support Email: service rj@ruijienetworks.com
- Online Robot/Live Chat: https://ruijienetworks.com/rita

Conventions

1. Signs

The signs used in this document are described as below:

🕖 Danger

An alert that calls attention to safety operation instructions that if not understood or followed when operating the device can result in physical injury.

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.

Specification

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

2. Note

This manual provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors. It is intended for the users who have some experience in installing and maintaining network hardware. At the same time, it is assumed that the users are already familiar with the related terms and concepts.

Contents

Preface	
1 Login	1
1.1 Configu	ration Environment Requirements1
1.2 Default	Configuration1
1.3 Login to	b Eweb on a PC1
1.3.1	Connecting to the Device1
1.3.2	Configuring the IP Address of the Management Computer2
1.3.3	Logging in to the Web Page2
1.3.4	Configuring the Wireless Bridge3
2 Wi-Fi Netwo	rk Settings7
2.1 Overvie	w7
2.1.1	NVR and Camera7
2.1.2	WDS Wi-Fi and Management Wi-Fi7
2.2 Scannir	ng and Pairing the Camera (CPE)7
2.3 Switching	ng NVR and Camera Mode8
2.4 Configu	ring the WDS Password for All Bridges in the LAN10
2.5 Configu	rring the Management SSID and Password for All Bridges in the LAN
2.6 Configu	rring the WDS Password for All Bridges in the WDS Group14
2.7 Setting	WDS Wi-Fi for a Single NVR or Camera15
2.7.1	Setting the WDS SSID15
2.7.2	Configuring the WDS Password16
2.7.3	Saving the Settings16
2.8 Optimiz	ing Wireless Network17

2.8.1 Overview	17
2.8.2 Getting Started	17
2.8.3 Configuration Steps	17
2.9 Changing the Country/Region Code	21
2.9.1 Getting Started	21
2.9.2 Configuration Steps	22
2.10 Configuring Antenna Alignment	22
2.11 Displaying WDS Group Information	23
2.12 Displaying the Information About a Single Device	24
2.13 Configuring TDMA Mode	26
2.13.1 Overview	26
2.13.2 Selecting the TDMA Mode	26
2.14 Configuring One-Touch Pairing	28
2.14.1 Overview	28
2.14.2 Configuration Steps	29
3 Network Settings	
3.1 Setting the Address of a LAN Port	30
3.1.1 Setting the Address of a LAN Port for a Single Online Bridge	32
3.1.2 Setting the Address of a LAN Port on the Local Device	33
3.2 Port-based Flow Control	34
3.3 Packet Rate Limiting	35
4 Alarm and Fault Diagnosis	36
4.1 Alarm Information and Suggested Action	36
4.1.1 Default Device Name Is Not Modified	36

4.1.2 Default Admin Password Is Still Used	37
4.1.3 Default WDS Password Is Still Used by All Devices	37
4.1.4 Network Cable Is Disconnected or Incorrectly Connected	
4.1.5 Latency Is High or Bandwidth Is Insufficient	
4.1.6 Radar Signal Interference	
4.2 Network Diagnosis Tools	40
4.2.1 Network Test Tool	40
4.2.2 Collecting Fault Info	41
4.3 Configuring Spectrum Scan	41
5 System Settings	44
5.1 Configuring Management Password	44
5.2 Configuring Session Timeout Duration	45
5.3 Resetting Factory Settings	46
5.4 Rebooting the Device	46
5.5 Configuring System Time	46
5.6 Configuring Config Backup and Import	47
5.7 Performing Update and Displaying the System Version	48
5.7.1 Online Update	48
5.7.2 Local Update	48
5.7.3 Update All Devices	49
5.8 Switching System Language	50
5.9 Configuring SNMP	50
5.9.1 Overview	50
5.9.2 Global Configuration	51

5.9.3 View/Group/Community/User Access Control	.52
5.9.4 SNMP Service Typical Configuration Examples	.60
5.9.5 Configuring Trap Service	.67
5.9.6 Trap Service Typical Configuration Examples	.71

.

1 Login

1.1 Configuration Environment Requirements

Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/Internet Explorer kernel-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.

1.2 Default Configuration

Table 1-1 Default Web Configuration	Table 1-1	Default W	eb Configuration
-------------------------------------	-----------	-----------	------------------

Item	Default Value
IP address	10.44.77.254
Username/Password	A username is not required on your first login. You can enter the initial password "admin" to log in, and directly start the configuration after login.

1.3 Login to Eweb on a PC

1.3.1 Connecting to the Device

You can open the management page and complete the bridge configuration only after connecting a PC to the bridge. You can connect a PC to the bridge in either of the following ways.

Wired Connection

Connect a local area network (LAN) port of the bridge to the network port of the PC, and set the IP address of the PC. See <u>1.3.2</u> Configuring the IP Address of the Management Computer.



🚺 Note

Only RG- AirMetro550G-B, RG-EST100-E and RG-EST350 V2 have two LAN ports.

Wireless Connection

On a mobile phone or laptop, search for wireless network **@Ruijie-b**XXXX. (XXXX is the last four digits of the MAC address of each device, and the MAC address can be found at the rear side of each bridge.) In this mode, you do not need to set the IP address of the management computer, and you can skip the operation in Configuring the IP Address of the Management Computer.

1.3.2 Configuring the IP Address of the Management Computer

Configure an IP address for the management computer in the same network segment as the default IP address of the device (The default device IP address is 10.44.77.254, and the subnet mask is 255.255.255.0.) so that the management computer can access the device. For example, set the IP address of the management computer to 10.44.77.10.

🛕 Caution

The IP address of the management computer cannot be set to 10.44.77.253, because this IP address is reserved by the device. If the management computer uses this IP address, it cannot access the device.

1.3.3 Logging in to the Web Page

(1) Enter the IP address (10.44.77.254 by default) of the bridge in the address bar of the browser to open the login page.

Note

If the static IP address of the device is changed, or the device obtains a new dynamic IP address, the new IP address can be used to access the web management system of the device as long as the management computer and the device are in the same network segment of a LAN.

(2) On the web page, enter the password and click Login to enter the web management system.

Rujje Rcycc Hi, Airmetro460F
É Password Login Forgot Password? Englieh ♥
Google Chrome and IE browser 9, 10 or 11 are supported. Copyright/S2000-2023 Ruijie Networks Co., Ltd.

A username is not required on your first login. You can enter the initial password "admin" to log in, and directly start the configuration after login.

For device security, you are advised to set the management password after your first login to the web management system. After the password is set, you need to enter the password when you log in to the web management system again.

If you forget the IP address or password, hold down the **Reset** button on the device panel for more than 5 seconds when the device is connected to the power supply to restore factory settings. After restoration, you can use the default IP address to log in without entering a password.

A Caution

Restoring factory settings will delete the existing configuration and you are required to configure the device again at your next login. Therefore, exercise caution when performing this operation.

1.3.4 Configuring the Wireless Bridge

🚺 Note

The configuration page is displayed only after the wireless bridge is restored to factory settings.

1. Create a bridge group

If the Bridge Mode is set to BaseStation(at NVR End), click Create New Group to access the configuration page.

Configure Device

Bridge Group	Create New Group Add to Current	Group	
Bridge Mode	••••••••••••••••••••••••••••••••••••••		
	BaseStation (at NVR End) On a bridge network, only one BaseStation can be deployed at the network video recorder (NVR) end.		CPE (at Camera End) On a bridge network, multiple CPEs can be deployed at the camera end.
* Bridge SSID	@Ruijie-wds-A838	\odot	
WDS Password	Default Password		
	Create New Group		

If the **Bridge Mode** is set to **CPE (at Camera End)**, a pop-up window is displayed. Click **Switch to CPE Mode** to proceed.

Configure Device	
Bridge Group 💽 C	reate New Group O Add to Current Group
O de	Tip When creating a new project, you are advised to first add the BaseStation at the NVR end. If the current device needs to serve as a CPE at the camera end, click Switch to CPE Mode. Switch to CPE Mode
Cr	reate New Group

2. Add to the current group

Set the Bridge Group to Add to Current Group, and select the bridge mode as required. If BaseStation (at NVR End) is selected, click Switch to BaseStation Mode on the pop-up window, and then click Add to Current Group to proceed.

Configure Device	
Bridge Group O Create New Group O Add to Current Group	
Bridge Mode Tip On a bridge network, only one BaseStation can be deployed at the network video recorder (NVR) end. Verify that no BaseStation exist on the target network. Switch to BaseStation Mode Skip Add to Current Group	

Bridge Network List (4)		×
Search by SSID		Re-scan
SSID	SN	RSSI
@Ruijie-wds-0625	G1SS60D000434	Good >
@Ruijie-wds-7848	G1SS60G000283	Poor >
@Ruijie-wds-0809	G1SS60G000406	Poor >
@Ruijie-wds-5512	G1SS60D00058A	Good >

No SSID Available?

1. Make sure all devices are powered on and the device mode is correct.

2.If the SSID cannot be scanned, reboot the device or restore it to factory settings.

Please enter the WDS	Password.	×
Default Password		
	Cancel	Bridge Device

If CPE (at Camera End) is selected, then click Add to Current Group to proceed.

Configure Device



2 Wi-Fi Network Settings

2.1 Overview

2.1.1 NVR and Camera

Bridges purchased in pairs in the same package can be paired automatically with each other after poweron. You can also manually pair the devices by setting up a WDS network. See <u>2.7</u> Setting WDS Wi-Fi for <u>a Single NVR or Camera</u>. In a paired WDS group, bridges can work in access point (BaseStation) or Customer Premises Equipment (CPE) mode.

- NVR end (BaseStation): A bridge sending bridging signals is generally connected to the NVR end in a surveillance room. A WDS group can contain at most one BaseStation.
- **Camera end (CPE)**: A bridge that enables customers to access ISP's communication services is generally connected to the camera end. A WDS group can contain multiple CPE.

2.1.2 WDS Wi-Fi and Management Wi-Fi

- WDS Wi-Fi: An BaseStation broadcasts the WDS Wi-Fi signal. A CPE accesses the WDS Wi-Fi and upload videos or other data to the BaseStation.
- **Management Wi-Fi**: Both an BaseStation and a CPE can broadcast management Wi-Fi signal. You can use a mobile phone or laptop to access the management Wi-Fi and log in to the web page to configure bridges.

2.2 Scanning and Pairing the Camera (CPE)

• Log in to the web interface of the NVR (BaseStation), click **Add Device** on the home page, and add a camera (CPE).

WDS Group1 Change WDS Password						
BaseStation 1 (Ruijie)	Channel :153		Latency @. Fluent(1) Jitter(0) Freeze(0)	Bandwidth (). Good(1) Medium(0)	Poor(0)	
CPE: 1. (Online: 1., Offline: 0)	WDS SSID @Rulle-wds-FD6F		Interference @ Good(1) Medium(0) Poor(0)	RSSI @ Good(1) Medium(0) Poor(0	0	
NVR (BaseStation)		Strong Signal:	Medium Signal 🗕 Poor Signal 🗕		○Camera (CPE)	Add Dev
Ruijie 2		Latency Oms Rate	→ 156Mbps	Active Time 01Hr10Min32Sec	Ruijie &	

Check the box next to the target camera (CPE), enter the bridge password in the **WDS Password** field (leave it blank if the default password is used), and click **Bridge Device**.

Other D	evices (1)					\times
	Model	SN	RSSI	Device Info	WDS Password	
	AIRMETRO4 60G	G1SS60D00 058A	Good	default/Ruiji e	Default Password	

Tips

1. If you failed to find the target device, scan the SSID to add the target device or make sure all devices

are powered on and the device mode is correct,

2. If you forgot the password, restore the device to factory settings.

3. Click WDS to add devices by scanning the SSID.

Re-scan	Bridge Device
---------	---------------

2.3 Switching NVR and Camera Mode

If an NVR fails, replace it and switch the new device to NVR (BaseStation). If multiple cameras (CPE) are required, a device newly joining the WDS group needs to be switched to Camera (CPE).

(1) You can check the current mode in the upper right corner of the web page and click **Pair Again** to switch the mode.



(2) In the displayed dialog box, click Start.

Note

 \times

• You can reset the device to restore default pairing status.

Country/Region: 🔆

Pairing Status: Default Work Mode: Camera (CPE)

WDS SSID: @Ruijie-wds-0808

Custom:

- 1. Support one-to-many (one AP to many CPEs).
- 2. Replace the paired device.



(3) Click Next.

Country/Region					
The country/region the country/region of	you select here must t of the WDS network.	be the same as			
Country/Region:	United States (US)	\sim			
Previous		Next			

(4) Select a mode from the Work Mode drop-down list.

Mode Switchov	er		×
Work Mode:	NVR (BaseStation)	^	
Previous	NVR (BaseStation)		Next
	Camera (CPE)		

(5) Click **Scan**. A list of camera (CPE) is displayed. Select the target camera (CPE), enter the WDS password, and click **Next**.

WDS SSID			×		
Scan and	select WDS SSID or enter	WDS SSID.	Password		
* WDS SSID:	WDS SSID	Scan	WDS SSID List (Clic	k to select a	a SSID.) 🛛 🗙
WDS Password	Default Password		Search by SSID		Re-scan
	WDS Password		WDS SSID	RSSI	SN
			@Ruijie-wds-0746	-56	ZASL42D000720
Previous		Nex	@Ruijie-wds-0109	-68	MACC942570009
ID :@Ruijie-wds-065A					
:	Strong Signal: — Mediu	m Signal: —			

(6) Verify the settings on the **Setup** page. Then, click **Save**.

Setup		×
Work Mode:	Switch BaseStation to CPE	
WDS SSID:	@Ruijie-wds-FD6F	
	Default Password	
Password:		
Country/Region:	China	
Previous		Save
Caution		

Switching the mode will reboot the device. Therefore, exercise caution when performing this operation.

2.4 Configuring the WDS Password for All Bridges in the LAN

Choose: Overview > Other Network Config > WDS Password

Web-based Configuration Guide

Country/Region: China (CN) @	curity, please change the network WDS Password.	re to configure WDS Password	IF	Allocation 🛛
Time Zone; (GMT+8:00)Asia/Shanghai 0			S	SID 😧
Network error Cable Connection Error: 1. Suggested Actions				DS Password
Radar Signal Interference Alarm 1 Suggested Actions	005		L	
adal orginal meneration Alam <u>Topgeoter Acc</u>	212		c	ountry/Region
WDS Group1 Change WDS Password				
iseStation 1 (Ruijie)	Channel :153	Latency @ Fluent(1) Jitter(0) Freeze(0) Bandwidth @ Goor	d(1) Medium(0) Poor(0)	
		Interference @ Good(1) Medium(0) Poor(0) RSSI @ Good(1) M		
E: 1. (Online: 1. Offline: 0)	WD5 SSID @Rujje-wds-FD6F	Interterence @ Good(1) Medium(0) Poor(0) RSSI @ Good(1) N	vedum(u) Poor(u)	
		i Signal. 💶 Medium Signal. 🚥 Poor Signal. 🚥		
IVR (BaseStation)			◇ Camera (CPE)	Add D
VR (BaseStation)		ons Rate → 1504bps Flow → 1504bps al 4000 ← 1524bps Flow ← 1744bps Active Time 011e112Ma	Ruile & ∞ ~	Add D

IP Allocation 😮
SSID 3
WDS Password 3
Country/Region 🕑
Other Network Config

Click WDS Password, enter the password in the displayed dialog box, and click Save.

Hover the cursor over So to view the help information.
WDS Password (Change the bridge passwords of the devices in all bridge groups.)
* Password Please enter a password.
There are four requirements for setting the password:
The password must contain at least 8 characters.
The password cannot contain question marks, spaces, and Chinese characters.
* Confirm Password Please enter the password again.

A Caution

When configuring the WDS password for the entire network, ensure that all devices in the network are online. Otherwise, the WDS passwords of the devices will be inconsistent.

Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation.

If there is an unbridged device in the network, the WDS password cannot be configured.

2.5 Configuring the Management SSID and Password for All Bridges in the LAN

Choose: Overview > Other Network Config >SSID

0 Alarm					\sim
Configuration is uninitialized.					
Hostname Not Set: 2 .					
Admin Password Not Set or The Management Pas	sword is Inconsistent: 2 . Click here to change the password.				
	urity, please change the network WDS Password. Click here to config	Jure WDS Password			
Country/Region: China (CN)					IP Allocation 🥹
Time Zone: (GMT+8:00)Asia/Shanghai @					S SID 🕑
Network error Cable Connection Error: 1. Suggested Actions					WDS Password ()
Radar Signal Interference Alarm <u>1 Suggested Actions</u>	INS				Country/Region
					Country/Region
WDS Group info WDS Groups : 1 Local Perf	ormance Mode: O High Bandwidth Mode O Normal Mode	Anti-Interference Mode		Admin Password @	Other Network Config
WD3 Group Into WD3 Groups 1 Local Perio	Intrance mode. C Figir Bandwidti Mode	O Anti-Interierence mode			
WDS Group1 Change WDS Password					
BaseStation: 1. (Ruijie)	Channel :153	Latency (): Fluent(1) Jitter(0) Freeze(0)	Bandwidth (): Good(1) Medium(0)	Poor(0)	~
CPE: 1. (Online: 1, Offline: 0)	WDS SSID :@Ruijie-wds-FD6F	Interference (0: Good(1) Medium(0) Poor(0)			
	Strong Signal:	Medium Signal: — Poor Signal: —			
◇ NVR (BaseStation)				◇ Camera (CPE)	Add Device
Ø ~			_	N (1) V	1
Ruijie 🖉	Latency 2ms Rate	→ 130Mbps → 0.00bps → 0.00bps ↓ 1008.00bps	Active Time 01Hr13Min02Sec	Ruijie 🖉	
MAC: d4:31:27:ac:fd:6f IP: 192.168.110.103				MAC: 58:69:6c:00:06:d8 IP: <u>192.168.110.52</u>	
AIRMETRO550G-B Online				AIRMETRO460F Online	
					·
		1			
	IP Allocation				
	IF Allocation				
	SSID 😮				
	WDS Passw				
	WDS Passw	ora 🐨			
	Country/Reg	gion 😮			
		, -			

Admin Password (2) | Other Network Config

🚺 Note

The management Wi-Fi network is used only for login to the web page and device management, and cannot be used for Internet access. It is isolated from the service network.

The default device management service set identifier (SSID) is **@Ruijie-b**XXXX. (XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with device.) Click **SSID** on the page to set the same management SSID and password for all bridges in the LAN.

Enable WiFi: Choose whether to enable the management Wi-Fi for all devices in the network.

SSID: The SSID is the name of the management Wi-Fi network.

Security: The following encryption types are available: Open, WPA-PSK, WPA2-PSK, and WPA_WPA2-PSK. You are advised to choose WPA_WPA2-PSK and set the password to improve the security.

Hide SSID: When this function is enabled, mobile phones or computers cannot find the Wi-Fi name, and users need to manually enter the correct name and password. This can prevent Wi-Fi from being accessed by unauthorized users and can enhance security.

	\times
broadcast by all devices to the same management SSID.))
@Ruiiie-b124A	
WPA_WPA2-PSK 🗸	
Dassword:	
r assword.	
There are four requirements for setting the pass	word:
. The password must contain at least 8 charac	ters
	, spaces, and
oninoso onardotors.	
	11 N
(The SSID must be manually entered ex	(actiy.)
Save	
	 @Ruijie-b124A WPA_WPA2-PSK Password: There are four requirements for setting the password: The password must contain at least 8 characters. The password cannot contain question marks Chinese characters. (The SSID must be manually entered examples of the password cannot contain question marks the password examples of the password e

🛕 Caution

After the configuration is saved, NVRs and cameras in the network will be reconnected. Therefore, exercise caution when performing this operation.

2.6 Configuring the WDS Password for All Bridges in the WDS Group

Choose Overview > Change WDS Password.

The default WDS password of devices is the same. Changing the WDS password can prevent others from illegally accessing the user network by using a device of the same model.

When configuring the WDS password for bridges in the entire network is unavailable or unnecessary, you can click **Change WDS Password** to configure the WDS password for bridges in the WDS group. If there is an unbridged device in the group, the **Change WDS Password** function will be unavailable.

Configuration is uninitialized. Hostname Not Set 2. Admin Password Not Set 7. Admin Password Not Se								
Hostame Not Set 2, • Hostame Not Set 2, •	4 Alarm							\sim
Admin Password No Set or The Management Password is inconsistent: 2. Click here to configure WDS Password: Country/Region: China (CN) © Time Zone: (kd1*8:00/ksis/Shanghai © Network error Cable Connection Error 1. Suggested Actions Red Signal Interference Alam 1 Suggested Actions Red Signal Interference Alam 1 Suggested Actions Red Signal Interference Country (Kd1) © Normal Mode © Normal Mode © Anti-Interference Mode Anti-Interference Mode Office (Kd1*8) Okasima (Kd1*8) Okas	Configuration is uninitialized.							
The network is using the default password. For security, please change the network WDS Password. <u>Click here to configure WDS Password</u> Contry/Region: Chang (CN) © The Zone: (CM148: 00)/skin/Shanghai © <u>Network error</u> Cable Connection Error 1. <u>Supprested Actions</u> Red Signal Interference Alam 1. <u>Supprested Actions</u> Red Signal Interference Alam 1. <u>Supprested Actions</u> Mode Connection Error 1. <u>Supprested Actions</u> Red Signal Interference Mode Control Interference Mode Contro	Hostname Not Set: 2 . 0							
Country/Region: China (CN) Time Zone: (SMT-8 00)/Skis/Skisniphal Network error Cable Control Fror 1 _ Suggested Actions Radar Signal Interference Alam 1 Suggested Actions Channel 1:53 Channel 1:54 Channel 1:53 Channel 1:	Admin Password Not Set or The Management Passw	and is Inconsistent: $\underline{2}$. Click <u>here</u> to change the	password.					
Time Zone: (skl41+8.00)Asia/Shanghan (*) Native Xe error Cable Connection Error: 1. Suggested Actions Radar Signal Interference Alam 1. Suggested Actions WDS Group Infor WDS Groups 1.1 Local Performance Mode:	The network is using the default password. For securi	y, please change the network WDS Password.	Click here to configu	re WDS Password				
Network error Cable Connection Error: 1. Suppested Actions Radar Signal Interference Alam 1_Suppested Actions Admn Password ① Other Network Cont VDDS Group Info WDS Groups 1 Local Performance Mode:	Country/Region: China (CN) @							
Cable Connection Error: 1. Suggested Actions Radar Signal Interference Alam 1_Suggested Actions VDDS Group Info: WDS Groups: 1_Local Performance Mode:	Time Zone: (GMT+8:00)Asia/Shanghai 0							
Radar Signal Interference Alam 1 Suggested Additors WDS Group Info WDS Group 1 Local Performance Mode: Hale control Mode Anti-Interference Mode Admn Password) Channel Local Performance Mode: Lotters / Admn Password) Control Medium (0) Control Med	Network error							
WDS Group Info WDS Groups 1 Local Performance Mode Month Password Other Network Cont WDS Group Info WDS Groups 1 Local Performance Mode Anti-Interference <	Cable Connection Error: 1 . Suggested Actions							
With B Once: Channel 153 Latency @ Fluent(1) atten(0) Floez(0) Storag Signal = Bandwidth @ Good(1) Medum(0) Floer(0) ~ Base Station 1 (Ruijie) Channel 153 Latency @ Fluent(1) atten(0) Floez(0) Bandwidth @ Good(1) Medum(0) Floer(0) ~ VNK (Base Station) WDS SSID @Ruije wdo-FDEF Interference @ Good(1) Medum(0) Floer(0) RSSI @ Good(1) Medum(0) Floer(0) ~ NVK (Base Station) Camera (CPE) Add Denze Ruijie Q	Radar Signal Interference Alarm 1 Suggested Actions							
NVX (Base Station) NVX (Base Station								
BaseStation 1 Channel 153 Latency © Fluent(1) Jaten(0) Floez(0) Bandwidth © Good(1) Medium(0) Poor(0) ~ CPE 1. (Online: 1). Offline: 0) WDS SSID @Ruije-wds-FD8F Interforence © Good(1) Medium(0) Poor(0) RSSI © Good(1) Medium(0) Poor(0) ~ Strong Signal — Medium Signal — Poor Signal — ~ Camera (CPE) Add Denze NVR (BaseStation) Camera (CPE) Latency 2ms Ruije 2	WDS Group Info WDS Groups : 1 Local Perform	nance Mode: O High Lowidth Mode	Normal Mode	Anti-Interference Mode			Admin Password 🥑	Other Network Config
Base Station: Channel: 153 Latency © Fluer(1) 3tter(0) Fleece(0) Bandwidth © Good(1) Medum(0) Poor(0) ~ CPE: 1. (Online: 0) WDS \$SID @Ruije wds-FD6F Interforence © Good(1) Medum(0) Poor(0) RSSI @ Good(1) Medum(0) Poor(0) RSSI @ Good(1) Medum(0) Poor(0) Camera (CPE) Add Dence • NVR (Base Station) • <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>								
CPE: 1. (Online: 1, Offline: 0) WDS SSID:@Rulle+wdo-FD6F Interference @. Good(1). Medium(0). Poor(0) RSSI @. Good(1). Medium(0). Poor(0) Strong Signal: — Medium Signal: — Poor Signal: — Camera (CPE) Add Dentee • NVR (Base Station) • Camera (CPE) Medium (0). Poor(0) RSSI @. Good(1). Medium(0). Poor(0) RSSI @. Good(1). Medium(0). Poor(0) Mod Dente • NVR (Base Station) • Camera (CPE) Mdd Dente Mod Dente Mod Dente • MAC: d4.3127.ac.fd.6f IP. 192.168.110.103 • 1950/bps Flow • 2.1950/bps Active Time D'H13Mm33Sec • Mod Dente		Channel (152)		Latence @: Elvert(1) Eller(0) Emerge(0)	Developidith @: Cood(4) Madium()) Beer(0)	
Strong Signal — Medium Signal — Poor Signal — Add Device • NVR (Base Station) Camera (CPE) Add Device Image: Rulije 2 Im								Ť
NVR (Base Station) Camera (CPE) Add Device Mdd Device Ruijie 2 MAC: 643127.rac.fd 6f IP: 192:168.110.103 Latency 2ms Rate → 156Mbps Flow → 1.13Kdps rd 4009 ← 108Mbps Flow → 2.18Kdp6 Addive Time D1Hr13Mm33Sec P: 192:168.110.103 MAC: 565656.c00.06.d8 IP: 192:168.110.103 Camera (CPE) MAC: 565656.c00.06.d8 IP: 192:168.110.103 MAC: 565656.c00.06.d8 IP: 192:168.110.103 MAC: 565656.c00.06.d8 MAC: 565656.c00.06.d8 MAC: 565656.c00.06.d8 IP: 192:168.110.52 MAC: 565656.c00.06.d8 IP: 192:168.110.103 MAC: 565656.c00.06.d8 IP: 192:168.110.52 MAC: 565656.c00.06.d8 IP: 192:168.110.52	CPE: 1 . (Online: 1 , Offline: 0)	WDS SSID :@Ruljie-wds-FD6F		Interference (): Good(1) M	edium(0) Poor(0)	RSSI (): Good(1) Medium(0) Po	or(0)	
NVK (Base station) Camera (CPE) Ruijie &			Strong Signal: —	Medium Signal: Po	or Signal: 🛑			
Ruijie 2 Latency 2ms Rate 150Mpps Flow 1.13kps all etcm MAC: 566 96:00 06:05 IP. 192:168.110.103 Flow 2.18kps Flow 2.18kps Active Time 01Hr13Mn338ec Ruijie 2	◇ NVR (BaseStation)						◇ Camera (CPE)	Add Device
	Ruijie 2 MAC: d4:31:27:ac:fd:6f IP: 192.168.110.103		Latency 2ms Rate				Ruijie 2 MAC: 58:69:6c:00:06:d8 IP: <u>192.168.110.52</u>	

WDS Group Info WDS G	Groups : 1 Local Performan
WDS Group1 Change W	DS Password
BaseStation: 1 . (Ruijie)	
CPE: 1 . (Online: 1 , Offline:	0)

Change WDS Password			\times
(Change the bridge passv	vord of the devices in this group.)		
* Password	Please enter a password.		
	There are four requirements for setting the · The password must contain 8 to 31 cha · The password cannot contain question characters.	aracters.	
* Confirm Password	Please enter the password again.		

🛕 Caution

When configuring the WDS password for a WDS group, ensure that all devices in the group are online. Otherwise, WDS passwords of the devices will be inconsistent.

Configuring the WDS password for a WDS group will reconnect devices in the group. Therefore, exercise caution when performing this operation.

If there is an unbridged device in the WDS group, this function will be unavailable.

2.7 Setting WDS Wi-Fi for a Single NVR or Camera

2.7.1 Setting the WDS SSID

Choose Wireless > WDS > WDS

To prevent network exceptions, you are advised to keep the default WDS SSID unless otherwise specified.

If a new WDS SSID is set for a device in a WDS group, other bridges in the group need to change to the new SSID as well to connect with this device.

When a new device is connected, you can either configure a new WDS SSID or click **Scan** to select a target WDS SSID.

To check the WDS SSIDs of WDS groups, choose **Overview** > **WDS Group Info**. For details, see 2.11<u>Displaying WDS Group Information</u>.

A Caution

Configuring a WDS SSID will disconnect the WDS link. Incorrect WDS SSID will cause a WDS connection failure. Therefore, exercise caution when performing this operation.

WDS		
* WDS SSID	@Ruijie-wds-0808	Scan
WDS Password	Default Password	
	Save	

2.7.2 Configuring the WDS Password

Choose Wireless > WDS > WDS

A correct WDS password is required for a successful WDS link. To prevent unauthorized devices from connecting to the WDS Wi-Fi network, high-security passwords are used for devices by default, and the password for devices of the same model is the same. You are advised to change the password for devices in the entire network or in a WDS group to prevent others from accessing the network using a device of the same model.

	WDS				
	* WDS SSID	@Ruijie-wds-0808	S	can	
	WDS Password	Default Password			
		Ruijie123			
		Save			
	Caution				
•	WDS passwords can be	e configured only for came	ras, and not	t for NVF	Rs.

• Configuring a WDS password will disconnect the WDS link. An incorrect WDS password will cause a WDS connection failure. Therefore, exercise caution when performing this operation.

2.7.3 Saving the Settings

After changing the WDS SSID or password, click Save to activate settings at once.

2.8 Optimizing Wireless Network

2.8.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon poweron. However, network stalling caused by wireless environment changes cannot be avoided. You can also analyze the wireless environment around the bridge and manually select appropriate parameters.

2.8.2 Getting Started

Before configuration, you can check the interference in the current environment in the following way to find the optimal channel.

Choose Wireless > WDS > Channel & Transmit Power.

Click **Interference** to check the interference of current channels. The channel with the smallest interference is the optimum.



2.8.3 Configuration Steps

1. Optimizing the Radio Channel

(1) Channel settings

Choose Wireless > WDS > Channel & Transmit Power > 5G Channel.

The default channel is **Auto**, indicating automatic channel adaption based on the surrounding environment upon power-on. Choose the optimal channel identified through the above analysis. Click **Save** to activate settings immediately. Excess STAs connected to a channel can bring stronger wireless interference.

SG Channel Auto Channel Width Auto 36 (5.18Ghz) Transmit Power 40 (5.2Ghz) 44 (5.22Ghz) Distance 48 (5.24Ghz) 52 (5.26Ghz) 56 (5.28Ghz) 60 (5.3Ghz)

The camera mode does not support independent channel settings. After the channel at the NVR end is adjusted, the camera end automatically changes its channel to be the same as the NVR end.

Channel & Trans	mit Power	
5G Channel	Auto	✓
Channel Width	Auto	~
	In CPE mode, the local	channel and channel width are consistent with the peer channel and channel width.
Transmit Power	Auto	~
Distance	1 KM	~
	Save	

🚺 Note

The available channel is related to the country/region code. Select the local country or region.

The above figure provides guidance on 5 GHz channel configuration. Take the same steps for 2.4 GHz channel configuration. The single-radio (2.4 GHz) device does not support 5 GHz configuration.

🛕 Caution

After the channel is changed, the NVR will be reconnected to the camera. Therefore, exercise caution when performing this operation.

(2) One-click optimization

Choose Wireless > WDS > Optimize WDS.

Click **Optimize WDS** so that the device automatically selects the channel again based on the interference in the current environment, ensuring that the device works in the optimal channel. You are advised to optimize WDS when the original channel is not the optimum.

Optimize WDS

Optimize WDS

🛕 Caution

After you click **Optimize WDS**, the NVR will be reconnected to the camera. Therefore, exercise caution when performing this operation.

2. Optimizing the Channel Width

Choose Wireless > WDS > Channel & Transmit Power > Channel Width.

If the interference is severe, choose a lower channel width to avoid network stalling. A 5 GHz bridge supports channel widths of 20 MHz, 40 MHz, and 80 MHz, while a 2.4 GHz bridge supports channel widths of 20 MHz and 40 MHz. The network is stable when the channel width is smaller. A larger channel width is more susceptible to interference. The default channel width of a 2.4 GHz bridge is 20 MHz (recommended configuration). The default channel width of a 5 GHz bridge is 40 MHz (recommended configuration). After changing the channel width, click **Save** to activate settings immediately.

A Caution

After the channel width is changed, the NVR will be reconnected to the camera. Therefore, exercise caution when performing this operation.

SG Channel Auto Channel Width 40MHz Transmit Power Auto 20MHz Distance 40MHz Save

3. Optimizing the Transmit Power

Choose Wireless > WDS > Channel & Transmit Power > Transmit Power.

Greater transmit power indicates larger coverage and brings stronger interference to surrounding wireless devices. The default value is **Auto**, indicating automatic adjustment of the transmit power. In a scenario in which wireless devices are installed densely, a lower power is recommended. **Low**, **Medium**, and **High** indicate 50%, 75%, and 100% power, respectively.

Channel & Transr	nit Power		
5G Channel	Auto	~	⊟ Interference
Channel Width	40MHz	~	
Transmit Power	Auto	^	
Distance	Auto Low		
	Medium		
	High		

4. Configuring the Distance

Choose Wireless > WDS > Channel & Transmit Power > Distance.

It is recommended that the configured distance between the NVR and camera be greater than their actual distance. If the configured distance is much smaller than the actual distance, the wireless performance will deteriorate, and WDS connection may fail.



🚺 Note

Distance configuration is supported on RG-AirMetro460F, RG-AirMetro460G, RG-AirMetro550G-B, RG-EST310, RG-EST310 V2, RG-EST350 and RG-EST350 V2 only. RG-EST310 and RG-EST310 V2 support a maximum actual distance of 1 km, while RG-EST350 and RG-EST350 V2 support a maximum actual distance of 5 km. RG-AirMetro460F, RG-AirMetro460G, RG-AirMetro550G-B support a maximum actual distance of 15 km

2.9 Changing the Country/Region Code

2.9.1 Getting Started

Country/region code change takes effect on all devices in the entire network, that is, all bridges on the **Overview** page. Therefore, before changing the country/region code, confirm that the target device is on the live network and the WDS link works well.

WDS Group1 Change WDS Password						
BaseStation: 1 (Ruijie)	Channel 153		Latency @ Fluent(1) Jitter(0) Freeze(0)	Bandwidth @ Good(1) Medium(0) I	Poor(0)	· · · · · · · · · · · · · · · · · · ·
CPE. 1. (Online: 1., Offline: 0)	WDS SSID @Ruijie-wds-FD6F		Interference (0 Good(1) Medium(0) Poor(0)	RSSI @. Good(1) Medium(0) Poor(0)	
		Strong Signal. 📥	Medium Signal 🛁 🛛 Poor Signal 💻			
NVR (BaseStation)					○ Camera (CPE)	Add Devi
Ruijie 2 MAC: d4.31.27.ac.td.6f		Latency 1ms Rate		Active Time 01Hr14Min44Sec	Ruijie 2.	

🛕 Caution

If you change the country/region code in the case of device disconnection, WDS connection may fail.

2.9.2 Configuration Steps

Choose Wireless > Country/Region > Country/Region.

Choose the target country/region from the drop-down list, and click **Save**.

Country/Region		
Country/Region	United States (US)	~
	Save	

🛕 Caution

After the country/region code is changed, the Wi-Fi network will restart, and the NVR and the camera will be reconnected after the Wi-Fi network is restarted.

The current channel may be switched to **Auto** because it is not supported by the country/region. Therefore, exercise caution when performing this operation.

2.10 Configuring Antenna Alignment

🚺 Note

Antenna Alignment is supported on RG- AirMetro550G-B, RG- AirMetro460F and RG- AirMetro460G only.

Choose Overview > WDS Group Info.

To optimize the usage of the Antenna Alignment feature, ensure that the device is in **Normal Mode**. This feature allow you to quickly and accurately align the antennas for optimal performance when operating the device outdoors. Additionally, as the device moves horizontally, the signal strength values are dynamically updated in real time.

Click on the RSSI. The Antenna Alignment pop-up window is displayed.

Configuration is uninitialized.					
Hostname Not Set: 2 . 0					
Admin Password Not Set or The Management Pa	ssword is Inconsistent: 2 . Click here to change to	he password.			
The network is using the default password. For s	curity, please change the network WDS Passwo	rd. Click here to configure WDS Password			
Country/Region: China (CN) 🛛					
Time Zone: (GMT+8:00)Asia/Shanghai 🛛					
Network error					
Cable Connection Error: 1 . Suggested Actions					
High latency or low bandwidth may cause the car • Low Bandwidth High Latency: <u>1</u> . Suggested					
Radar Signal Interference Alarm 1 Suggested Ac	ions				
S Group Info WDS Groups : 1 Local Pe	formance Mode: 🔿 High Bandwidth Mode	Normal Mode Anti-Interference Mode		Admin Password 🛛 O	Other Network Co
WDS Group1 Change WDS Password		•		Admin Password 🌒 C	Dther Network Co
WDS Group1 Change WDS Password aseStation 1 . (Ruijie)	Channel :153	Latency @: Fluent(1) JEter(0) Freeze(0)	Bandwidth @: Good(1) Medum(0) Poor(0)	Admin Password 🛛 0	Other Network Co
WDS Group1 Change WDS Password asseStation 1 . (Ruijie)		•		Admin Password 🛛 d	Dther Network Co
WDS Group1 Change WDS Password asseStation 1 . (Ruijie)	Channel :153	Latency @: Fluent(1) JEter(0) Freeze(0)		Admin Password 🌒 C	Dither Network Cor
OS Group Info WDS Groups : 1 Local Pe WDS Group: Change WDS Password Base Station: 1 (Ruijie) SPE: 1 . (Online: 1 . Offline: 0) NVR (Base Station)	Channel :153	Latency Ø: Fluen(1) Jitter(0) Freaze(0) Interference Ø: Good(1) Medum(0) Foor(0)	RSSI (): Good(1) Medium(0) Poor(0)	Admin Password	Other Network Cor
WDS Green Change WDS Password Base Station 1 (Ruille) CPE: 1. (Online: 1. Offline: 0) NVR (Base Station)	Channel :153	Latency Ø: Fluen(1) Jitter(0) Freaze(0) Interference Ø: Good(1) Medum(0) Foor(0)	RSSI (): Good(1) Medium(0) Poor(0)	era (CPE)	、
Wos Group1 Change WDS Password Base Station 1 (Ruijie) PPE 1. (Online: 1, Offline: 0)	Channel :153	Latency @: Fluen(1) Jiter(0) Freezo(0) Interference @: Goo(1) Medium(0) Poor(0) Strong Signat — Medium Signat — Poor Signat —	RSSI (): Good(1) Medium(0) Poor(0)	era (CPE) Ruijie 2 © ~ MAC: 58595c0006:d8	、
WOS Grower) Change WDS Password asse Station 1. (Ruijie) PPE 1. (Online: 1. Offline: 0) NVR (Base Station) Ruijie &	Channel :153	Latency @: Fluen(1) Jiter(0) Freezo(0) Interference @: Goo(1) Medium(0) Poor(0) Strong Signat — Medium Signat — Poor Signat —	RSSI @- Good(1) Medium(0) Poor(0)	era (CPE) Ruijie 2	``

1 Note

When the wireless bridge is in Base Station mode, you can view the information of all devices in CPE mode. Conversely, if the wireless bridge is in CPE mode, you can only view information of the local device and other devices in Base Station mode.

The following bridge group information are displayed: the current highest vertical and horizontal signal strengths achieved by the Base Station and CPE in the bridge group, the historical highest signal strength achieved through antenna alignment, and the real-time updates of vertical and horizontal signal strengths.

Ruijie SN: MACC460FSST03		Ruijie SN: G1SS60D00058A	
-49 dBm		-51 dBm	௴ -51 dBm
V -63dBm	······>	V -59dBm	
H -49dBm		H -51dBm	
① The difference between the V value and the H value should be below 5 dBm.	J	① The difference between the \ H value should be below 5 dBm	/ value and the

1 Note

The left pane displays the information about the Base Station device, while the right pane displays the information about the CPE device.

2.11 Displaying WDS Group Information

Choose Overview > WDS Group Info.

Displayed WDS group information includes the number of BaseStations and CPEs in the group, current working channel, SSID, latency, interference, wireless bandwidth and quality, RSSI and quality, data rate, real-time traffic, and uptime. Hover the cursor over to view the detailed information of every item.

	Latency Fluent(1) Jitt	er(0) Freeze(0)		
Ruijie	00:10:f9:50:67:66	0ms -		
Hostname	MAC	Latency	sword	
Ruijie 2. MAC: d43127 nc456f IP: 192:168.110.103 IP: 192:168.110.103	Latency 1ms R	60 → 150/050 Pierr → 3.808/050 ← 162/050 Vierr ← 0.00505	A CON Active Time Other/Bildm15Sec	te © ∼ 38 Ontine
NVR (Base Station)			ି Camera (CPE)	Add Dev
	Strong Signal	- Medium Signal: — Poor Signal: —		
iseStation: 1. (Ruijie) PE. 1. (Online: 1., Offline: 0)	Channel 153 WDS 5SID @Ruije-wds-FD6F	Latency @ Fluent(1) Jitter(0) Freeze(0) Interference @ Good(1) Medium(0) Poor(0)	Bandwidth 0: Good(1) Medium(0) Poor(0) RSSI 0: Good(1) Medium(0) Poor(0)	

BaseStation is at the NVR end, while CPE is at the camera end.

2.12 Displaying the Information About a Single Device

• Choose Overview > WDS Group Info > NVR (BaseStation)/Camera (CPE).



Click the **Let** icon of a device to display the basic information about the device in the right panel of the page, including the hostname, uptime, online status, model, SN, MAC address, software and hardware versions, IP address, subnet mask, LAN port status, noise floor/utilization, distance, channel, transmit power, channel width, RSSI, and band.

Ruíjie | Rcycc = English - NVR (BaseStation) 🖉 Pair Again 🛛 🕁 Log Ou Group 1 / BaseStation / Alarm Configuration is uninitialized, Hostname Not Set 2 . ① Admin Password Not Set or The Management Password is inconsistent 2 . Click <u>here</u> to change the password. The network is using the default password. For security, please change the network WDS Password. <u>Click here to co</u> Country/Region. Clink Tele ColyAsasShanghat ④ Time Zone. (2017:40.00)AsasShanghat ④ 🛞 LAN 0 HOSTNAME: Ruije 2 Uptime: 01H/58Min47Sec Model: AIRMETRO560G-8 SN: G1509BK00625 foftware Ver: AP.3.0(1)B11P246,F iardware Ver: 1.00 MAC: 04:31:27.ac.td.6f % Wireless foure WDS Password Advanced ٢ Network error Cable Connection Error: <u>1</u>. <u>Suggested Actions</u> Radar Signal Interference Alarm <u>1</u> <u>Suggested Actions</u> 𝔣 Diagnostics 💥 System IP Address: 192.168.110.103 Jonet Mask: 255.255.255.0 LAN0: 1000baseT/Full-Dupley LAN1: Disconnected LAN WDS Group Info WDS Groups : 1 Local Performance Mode: O High Bandwidth Mode Normal Mode WD9 Group1 Change WDS Password BaseStation: 1 . (Ruijie) CPE: 1 . (Online: 1 , Offline: 0) olse Floor/Utilization : -91dBm / 3% Distance : 10000M Channel: 153 Insmit Power: 27.0dBm annel Width : RSSI: -Band: 5.8G Channel :153 ncy O: I WDS SSID :@F (ind NVR (Base Station) Ruijie 2 MAC: d4:31:27:ac:fd:6 IP: 192.168.110.103 Latency 1ms Rate → 156Mbps Flow → 1.13Kbps J •4200 ← 40Mbps Flow ← 1.40Kbps Active Time 0G-8 *.*

Device:	Group 1 / BaseStation / <> (Select a device to view its details)
Settings:	LAN WDS Reboot Spectrum Scan
e sys	HOSTNAME: Ruijie 2 Uptime: 01Hr59Min24Sec Model: AIRMETRO550G-B SN: G1S09BK000625 Software Ver: AP_3.0(1)B11P246,Release(10240118) Hardware Ver: 1.00 MAC: d4:31:27:ac:fd:6f
LAN	AND ADDER TOUL Durley
	Noise Floor/Utilization : -91dBm / 3%
Wi-F	Distance: 10000M Channel: 153 Transmit Power: 27.0dBm

🚺 Note

The device at the NVR end does not involve channel width and RSSI, and only the device at the camera end does.

2.13 Configuring TDMA Mode

🚺 Note

TDMA Mode is supported on RG- AirMetro550G-B, RG- AirMetro460F and RG- AirMetro460G only.

2.13.1 Overview

Time Division Multiple Access (TDMA) is specifically designed to address the challenge of CPE nodes being hidden from each other over long distances. In the traditional Wi-Fi mechanism utilizing Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the nodes are unable to listen to each other, leading to significant performance degradation. With the TDMA mode enabled, the traffic of each node remains unaffected by long distances, ensuring high performance.

2.13.2 Selecting the TDMA Mode

Choose Wireless > TDMA.

1. Flexible mode

The flexible mode is the default TDMA mode. When enabled, it employs an algorithm to automatically calculate the necessary time slots for each CPE or BaseStation. Additionally, the ratio between BaseStation and CPE is dynamically adjusted to optimize uplink and downlink traffic for maximum efficiency.

TDMANVR (Base Station) Select the TDMA-based time slot allocation mode.						
TDMA						
TDMA						
Mode ?	• Flexible					
Advanced \vee						
Expert Mode	When expert mode is enabled, time slots will be allocated for each station in station performance. Exercise caution when using the expert mode.					

2. Fixed mode

The fixed mode is designed for scenarios that require traffic balance, consistent latency, and consistent uplink and downlink throughput for each node. By utilizing fix intervals (such as 5 ms, 8 ms, and 10 ms), the duration

of each frame can be fixed to achieve a consistent latency. In terms of the uplink and downlink throughput, you can set the uplink and downlink ratio accordingly. Currently, there are five ratios available: 1:1, 1:2, 1:3, 2:1, and 3:1, which can be selected from the provided drop-down menu.

<i>TDMANVR (BaseStation)</i> Select the TDMA-based time slot allocation mode.							
TDMA							
TDMA							
Mode (?)	◯ Flexible ● Fix						
	TDD Ratio						
	1:1 ✓ The time slot of downlink and uplink base on 1:1						
	TDD Time Slot						
	5ms v						
Advanced >							
	Save						

TDD Ratio



	TDD Time Slot				
	5ms	^			
>	5ms				
	8ms				
	10ms				

3. Expert mode

TDMA				
TDMA				
Advanced \sim				
Expert Mode	When expert mode is enabled, time slots will be allocated for each station in the bridge group based on actual traffic conditions. Ho station performance. Exercise caution when using the expert mode.			
	Enter the time slot value (1 ms or greater). The total time slots of all devices must not exceed 60 ms. Reset			
	BaseStation/Ruijie G1S09BK000625	1	ms	
	Cpe/Ruijie 1234567891234	1	ms	
	Save			

A Caution

The expert mode is designed for situations where a specific node requires a dedicated and fixed time slot, unaffected by algorithm adjustments. In this mode, the desired time slot can be set by the customer. However, it is important to note that the expert mode is not recommended for general customers and should only be configured by individuals with relevant professional knowledge. Incorrect configuration in this mode may result in the device failing to go online.

2.14 Configuring One-Touch Pairing

🚺 Note

One-Touch Pairing is supported on RG- AirMetro550G-B, RG- AirMetro460F and RG- AirMetro460G only.

2.14.1 Overview

When the One-Touch Pairing feature is enabled, a simple press of the One-Touch Pairing button on the device triggers the mesh operation. During the mesh process, the BaseStation promptly forms a mesh connection with the factory-configured and unbridged CPE, streamlining the networking process.
The One-Touch Pairing feature is designed to simplify the process of setting up a network bridge for users who have purchased a wireless bridge that supports this feature. By pressing a physical button on the wireless bridge, the wireless bridge will automatically search for and connect with a factory-configured CPE that has not been connected to any network. This will add the CPE to the LAN of the BaseStation without complex network configuration or setup. The One-Touch Pairing feature enables users to establish a network connection quickly and easily, right out of the box, greatly simplifying the setup and configuration process for the wireless bridge.

2.14.2 Configuration Steps

Choose Wireless > One-Touch Pairing

Toggle on **Enable** and click **Save**.

Check whether the bridge is in BaseStation mode or CPE mode. If the bridge is currently in BaseStation mode, pressing the One-Touch Pairing button on the wireless bridge will bridge it to all nearby devices operating in CPE mode. If the device is currently in CPE mode, pressing the **One-Touch Pairing** button will switch it to BaseStation mode and continue bridging with all nearby devices operating in CPE mode.



🚺 Note

The One-Touch Pairing feature is enabled by default.

3 Network Settings

3.1 Setting the Address of a LAN Port

The address of a LAN port is used only for login to the web page and does not affect the service network.

Allocating IP Addresses to All Bridges in the NetworkChoose: Overview > Other Network Config > IP Allocation

• Static IP address

Configuring static IP addresses for the entire network:

When a large number of devices in the network require static IP addresses, you can use **IP Allocation** to automatically allocate a static IP address for each device. Click **IP Allocation**, set **Internet** to **Static IP Address**, set **Start IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server**, and click **OK**.

Hover the cursor over <a>

to view the help information.

0 Alarm							~
Configuration is uninitialized.							
Hostname Not Set: 2 .							
Admin Password Not Set or The Management Pa							
The network is using the default password. For se	curity, please change the network WDS Passwor	rd. Click here to configu	re WDS Password				
Country/Region: China (CN)							IP Allocation 1
Time Zone: (GMT+8:00)Asia/Shanghai 🔮							SSID 🔞
Network error							WDS Password
Cable Connection Error: 1 . Suggested Actions							WDS Password
Radar Signal Interference Alarm 1 Suggested Act	ons						Country/Region 😫
WDS Group1 Change WDS Password							
BaseStation: 1 . (Ruijie)	Channel :153		Latency (): Fluent(1) Jitter	(0) Freeze(0)	Bandwidth (): Good(1) Medium(0) Poor(0)	~
CPE: 1 . (Online: 1 , Offline: 0)	WD\$ \$\$ID :@Ruijie-wds-FD6F		Interference @: Good(1) M	ledium(0) Poor(0)	RSSI (): Good(1) Medium(0) Po	or(0)	
		Strong Signal: 🛑	Medium Signal: — Po	oor Signal: 🛑			
◇ NVR (BaseStation)						⇔Camera (CPE)	Add Device
Ruijie O MAC: 64.31.27.ac.ht.6f IP: 192.168.110.103 AIRMETROSSO0-8 Online		Latency 1ms Rate	→ 130Mbps ← 162Mbps Flow	→ 0.00bps ← 400.00bps	Active Time 01Hr18Min46Sec	Ruijie 2 MAC: 58:69:60:00:06:d8 IP: 192.168.110.52 ARMETRO486F Online	

IP Allocation 🔞
SSID 😧
WDS Password 😮
Country/Region 3

 \times

IP Allocation

(Change the IP addresses of all devices.)

Internet	Static IP Address \lor	
* Start IP Address	192.168.110.2	8
* Subnet Mask	255.255.255.0	
* Gateway	192.168.110.1	
• 5.110.0		
* DNS Server	Example: 114.114.114.114.	
IP Count	253	
	ок	

A Caution

The start IP address cannot be in the same network segment as the current IP address. Otherwise, the configuration will fail.

After the configuration, the device IP address changes, and the device web page cannot be accessed. You need to enter the new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer. (See <u>1.3.2</u> <u>Configuring the IP Address</u> <u>of the Management Computer</u>) Therefore, exercise caution when performing this operation.

• Dynamic IP address (DHCP)

When a large number of devices in the network require dynamic IP addresses, you can configure dynamic IP addresses (DHCP) for the entire network so that each device can dynamically obtain an IP address. Set **Internet** to **DHCP**, and click **OK**.

 \times

IP Allocation (Change the IP addresses of	all devices.)	
Internet	DHCP	~
	DHCP does not require ar	n account.
	ок	

3.1.1 Setting the Address of a LAN Port for a Single Online Bridge

Choose Overview > WDS Group Info > NVR (BaseStation)/Camera (CPE).

To set the IP address for a single device, click ⁽²⁾, and select LAN from the drop-down list. For the configuration method, see <u>OAllocating IP Addresses to All Bridges in the Network</u>.

NVR (BaseStation)



LAN				×
Internet	DHCP	\sim		
	DHCP does not require an account.			
IP Address	192.168.110.33			
Subnet Mask	255.255.255.0			
Gateway	192.168.110.1			
DNS Server	192.168.110.1			
	Save			

🛕 Caution

After the IP address and subnet mask are changed, the device web page may not be accessed. You need to enter the new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer. (See <u>1.3.2</u> <u>Configuring the IP Address of the Management Computer</u>) Therefore, exercise caution when performing this operation.

3.1.2 Setting the Address of a LAN Port on the Local Device

Open the LAN page.

If a DHCP server is deployed in the network, you are advised to set **Internet** to **DHCP**. If no DHCP server is deployed, set **Internet** to **Static IP Address**, set **IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server**, and click **Save**.

1	LAN Configure LAN se	ttings.
	Internet	DHCP ~
		DHCP does not require an account.
	IP Address	192.168.110.209
	Subnet Mask	255.255.255.0
	Gateway	192.168.110.1
	DNS Server	192.168.110.1
		Save

🛕 Caution

After the IP address and subnet mask are changed, the device web page may not be accessed. You need to enter the new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer. (See <u>1.3.2</u> <u>Configuring the IP Address of the Management Computer</u>) Therefore, exercise caution when performing this operation.

3.2 Port-based Flow Control

Choose Advanced > Flow Control.

Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed. This function is enabled by default and can be manually disabled.

1	Flow Control Flow control can reli	eve the data congestion caused by p	ports at different speeds and improve the network spee	ed.
	Flow Control			
		Save		

(? Ai

3.3 Packet Rate Limiting

Enable rate limiting on broadcast or multicast packets to avoid congestion on the air interface.

The device supports rate limiting on specified broadcast packets (ARP and DHCP), specified multicast packets (MDNS and SSDP), or all broadcast and multicast packets.

🛕 Caution

Packet rate limiting takes effect on all devices over the network, that is, all bridges capable of rate limiting on the homepage.



Choose Advanced > Packet-based Rate Limiting.

4 Alarm and Fault Diagnosis

4.1 Alarm Information and Suggested Action

When bridges fail or lack some necessary security configuration, the system prompts key alarms about the bridges on the homepage, so that users can handle the exceptions promptly.

Choose Overview > Alarm.

Ruíjie	Rcycc ≡		English	VVR (BaseStation) & Pair Again	tog Out
C Overview	• Alarm]		\sim
🛞 LAN	Configuration is uninitialized. Hostname Not Set: 2. •				
% Wireless 🗸 🗸	Admin Password Not Set or The Management Password is Inconsistent: 2. The network is using the default password. For security, please change the				
Advanced	Country/Region: China (CN) ● Time Zone: (GMT+6:00)Asia/Shanghal ●	increases which in a series in contribute in the instantial			
𝔥 Diagnostics ∨	Network error Cable Connection Error: 1 . Suggested Actions				
💥 System 🗸	Radar Signal Interference Alarm 1 Suggested Actions				
	WDS Group Info WDS Groups : 1 Local Performance Mode: High	Bandwidth Mode O Normal Mode O Anti-Interference Mode		Admin Password 🕘 Other Net	work Config
	WDS Group1 Change WDS Password				
	BaseStation: 1. (Ruijie) Channel :153 CPE: 1. (Online: 1. Offline: 0) WDS SSID:@R	Latency 0: Fluent(1) Jiter(0) Free	eze(0) Bandwidth (0: Good(1) Medium(0) Poor(0) 0) Poor(0) RSSI (0: Good(1) Medium(0) Poor(0)		~
	CPE. 1. (Online: 1, Online: 0) WDS SSID (get				
		Strong Signal: - Medium Signal: - Poor Signal:			Add Device
	 NVR (Base Station) 		⇔ Camera (
	Ruijie 2. MAC: 04/31:27.ac.fd:6f IP: 192.168.110.103	Latency tms Rate → 150Mbps Flow → 0 ← 81Mbps Flow ← 1	1008.00bps Active Time 01Hr19Min56Sec	ijje 2	
	AIRMETROSS00-B Onine		ARMETROA	Online	

4.1.1 Default Device Name Is Not Modified

Modifying device names can help you better distinguish each bridge. Unless otherwise specified, you are advised to modify default device names.

When viewing the alarm, hover the cursor over the orange number of the prompt and click in the displayed dialog box to modify the name of each device. (The orange number, 2 in the figure, indicates the number of devices that still use the default name in the network.) Enter the new device name and click **OK** to make the change take effect immediately.

Ruíjie	Rcycc =	WD S Group	Hostname	MAC	
C Overview	Alarm Configuration is up	WDS Group1	Ruijie 🖉	00:d0:f8:15:07:46	
② LAN	Configuration is un Hostname Not Set	WDS Group Ruijie	Edit hostname	90:71:5e	o change the
Advanced	The network is using th Time Zone: (GMT+8:00	WD5 Group	Cancel OK	bd:37:cb	WDS Passwo
🏷 Diagnostics 🗸 🗸	Network error Cable Connection Erro	WDS Group2	Ruijie 💋	ec:b9:70:bd:37:ce	
℅ System →	WDS Group Info WD	S Groups : 2 Lo	cal Performance M	lode: O High Band	width Mode

4.1.2 Default Admin Password Is Still Used

For device and network security, you are advised to configure the admin password for the network to prevent login of unauthorized users.

Click the prompt to configure the admin password for the network. Hover the cursor over the orange number (1 in the figure) of the prompt to configure the device password. For configuration steps, refer to <u>4.1.1 Default</u> <u>Device Name Is Not Modified.</u>



🛕 Caution

The admin password is used to log in to the web page of any device in the network. Therefore, remember the admin password. If you forget the admin password, restore factory settings. For the method, see <u>1.3.3</u> Logging in to the Web Page.

If there is an unbridged device in the network, the function of configuring the admin password will be disabled.

4.1.3 Default WDS Password Is Still Used by All Devices

The default WDS password of devices of the same model is the same. Changing the WDS password can prevent others from illegally accessing the network by using a device of the same model.

Click **Click here to configure WDS Password**, enter the new password, and click **Save** to change the WDS password for the entire network.

• Alarm
Configuration is uninitialized.
Hostname Not Set: 4. 9
Admin Password Not Set or The Management Password is Inconsistent: Click here to change the password.
The network is using the default password. For security, please change the network WDS Password. Click here to configure WDS Password
Time Zone: (GMT+8:00)Asia/Shanghai 🔮
Network error
Cable Connection Error: 2 . Suggested Actions

🛕 Caution

When configuring the WDS password for the entire network, ensure that all devices are online. Otherwise, WDS passwords of the devices will be inconsistent.

Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation.

If there is an unbridged device in the network, the function of configuring the WDS password for the entire network will be disabled.

4.1.4 Network Cable Is Disconnected or Incorrectly Connected

Hover the cursor over the orange number of the prompt to display the alarm details.

Click the suggested action to check the solution.

0	Alarm				
	Configuration is uninitialized.				
	Hostname Not Set: 4 . 2				
	Admin Password Not Set or The Management Password is Inconsistent: Click here to change the password.				
	The network is using the default password. For security, please change the network WDS Password. Click here to configure WDS Password				
	Time Zone: (GMT+8:00)Asia/Shanghai 🕑				
	Network error				
	Cable Connection Error: 2 . Suggested Actions Please check cable connection and then re-plug or replace the cable.				

4.1.5 Latency Is High or Bandwidth Is Insufficient

First, check whether the device latency is too high. If yes, the interference in the environment may be severe. Then, you are advised to change to a channel with smaller interference.

If not, increase the channel width. For channel settings, see <u>2.8.3</u> <u>1. (1)</u> <u>Channel settings</u>. For channel width settings, see <u>2.8.3</u> <u>2</u>. <u>Optimizing the Channel Width</u>.

To check whether the latency is too high, perform as follows:

Hover the cursor over the orange number of the prompt to display all WDS groups, and click a group to display the details.

On the **Overview** page, check whether **Latency** is **Freeze**. If so, the latency is too high. Otherwise, the latency is normal.

C Overview			
		• Alarm	~
LAN		Configuration is uninitialized.	
		Hostname Not Set: 4. 😡	
To Wireless	~	The network is using the default password. For security, please change the network WDS Password. Click here to configure WDS Password	
		Time Zone: (GMT+8.00)Asia/Shanghai 🖗	
Advanced	~	Network error	
		Cable Connection Error: 1 . Suggested Actions	
S Diagnostics		High latency or low bandwidth may cause the camera image to freeze	
		* 2 . Suggested Actions	
💥 System Tools	~		

High latency or low bandwidth may cause the camera image to freeze.

Latenc	cy 1: Fluent(0) Jitter(0) Freeze(1)	
◇ Came	era (CPE)	
EST310- V2	► 16 @ ~ MAC: 00:10:19:50:67:66 IP: 192.168.110.209 Online	

• 3 . Suggested Actions

🛕 Caution

Channel and channel width settings described in this section are performed on the local device. You can click the IP address of a device to open the management page of the device and set the channel and channel width.

4.1.6 Radar Signal Interference

When the device detects a radar signal in a channel, it generates an alarm and automatically switches the channel. Hover the cursor over the orange number of the prompt to display alarm details.

☆ Overview			
		Alarm	~
() LAN		Configuration is uninitialized.	
		Hostname Not Set. 🛓 🚇	
S Wireless		The network is using the default password. For security, please change the network WDS Password. Click here to configure WDS Password	
		Time Zone: (GMT+8:00)Asia/Shanghai 🖗	
Advanced		Network error	
		Cable Connection Error: 1 Suppested Actions	
2. Diagnostics	24C	Radar Signal Interference Alarm 1 Suppested Actions	

Network error

Cable Connection Error: 1 . Suggested Actions	
Radar Signal Interference Alarm 1 Suggested Actions	It is recommended to select a non-DFS channel (36-48/149-165) to maintain the WDS connection.

Network error Cable Connection Error: <u>2</u> . <u>Sugges</u> Radar Signal Interference Alarm 1 2	Group	Hostname	Backoff Channel	Backoff Time	SN	
	WDS Group2	Ruijie 💋	60	2022-02-21 14:57:26	CANL63300035S	

According to the information about the WDS group and back-off channel in the alarm record, check whether the current working channel in the WDS group (group 2 in the example) is consistent with the back-off channel. (See <u>2.1.1 Displaying WDS Group Information</u>.) If so, manually switch the channel to a non-dynamic frequency selection (DFS) channel. For the setting method, see <u>2.8.3 1. (1) Channel settings</u>.

1 Note

Non-DFS channels include 36-48 and 149-165.

Detecting radar signal interference is supported on RG-EST310, RG-EST310 V2, RG-EST350 and RG-EST350 V2 only.

4.2 Network Diagnosis Tools

4.2.1 Network Test Tool

Choose Diagnostics > Network Tools.

When you select the ping tool, you can enter the IP address or URL and click **Start** to test the connectivity between the bridge and the IP address or URL. The message "Ping failed" indicates that the bridge cannot reach the IP address or URL.

The Traceroute tool displays the network path to a specific IP address or URL.

The DNS Lookup tool displays the DNS server address used to resolve a URL.

<i>i</i> Network Tools		
Tool	• Ping	O DNS Lookup
* IP Address/Domain	10.10.10.10	\odot
* Ping Count	4	
* Packet Size	64	
	Start	Stop
Result		

4.2.2 Collecting Fault Info

Choose Diagnostics> Fault Collection.

Click Start to collect fault information and compress it into a file for engineers to identify fault.



4.3 Configuring Spectrum Scan

1 Note

Spectrum Scan is supported on RG- AirMetro550G-B, RG- AirMetro460F and RG- AirMetro460G only.

Choose **Diagnostics** > **Spectrum Scan.**

This feature is only supported when the bridge is in Base Station mode, and is not supported when it is CPE mode.

Click Spectrum Scan, and then click OK on the pop-up window. The Spectrum Scan page is displayed.

<i>Spectrum Scan</i> Evaluate the interference level of each chan	nel to produce an interference score.	
Spectrum Scan		
Spectrum Scan No Data		
_		
Тір	×	
Switching the channel scan may ta		
during which the device may exper disconnection. Continue?	ience a temporary	
disconnection. Continue?		
	Cancel	
Spectrum Scan V Evaluate the interference level of each channel to produce an interference score.		
Spectrum Scan		Low H
	Scanning	

You can click the **20 MHz**, **40 MHz**, or **80 MHz** tabs to view the channel interference. The color gradient from left to right indicates the level of interference, ranging from low to high. Each row represents the channels used by a device.

0/8



Hovering the mouse over it will display detailed information about the current channel, including throughput and estimated number of cameras that can be supported.



To change channels, click on the target channels, and then click **Change Channel**. A pop-up window is displayed. Click **OK**.



The network service will be unavailable for a while. Do you want to continue?

Cancel	ОК
--------	----

5 System Settings

5.1 Configuring Management Password

Choose: Overview > Admin Password



Click Admin Password to change the login password for all devices.

If there is an unbridged device in the network, the link will be unavailable.

Hover the cursor over <a>

to view the help information.

 \times

Admin Password

(Change the management passwords of all devices.)

* Password	Please enter a password.
	There are four requirements for setting the password:
	• The password must contain at least 8 characters.
	The password must contain uppercase and lowercase letters, numbers and three types of special characters.
	· The password cannot contain admin.
	The password cannot contain question marks, spaces, and Chinese characters
* Confirm Password	Please enter the password again.
	Save
* Confirm Password	Chinese characters. Please enter the password again.

🛕 Caution

This password is used to log in to Eweb system of any device in the network.

If there is an unbridged network in the network, the function of configuring the admin password will be disabled.

5.2 Configuring Session Timeout Duration

Choose System > Management > Session Timeout.

If no operation is performed on the page within a period of time, the session will be down. When you need to perform operations again, enter the password to open the configuration page. The default timeout duration is 3600 seconds, that is, 1 hour.

Backup & Import Reset	Session Timeout	
<i>i</i> Session Timeout		
* Session Timeout	3600	Sec
	Save	

5.3 Resetting Factory Settings

Choose System > Management > Reset

Click Reset to restore factory settings.

Backup & I	mport	Reset	Session Timeout
	eset esetting the de	evice will clea	ar the current configuration. If you want to keep the configuration, please Export Config first.
F	Reset		

🛕 Caution

This operation will clear existing settings and restart the device. Therefore, exercise caution when performing this operation. If there is any configuration in the current system, please export the configuration before resetting the device.

5.4 Rebooting the Device

Choose System > Reboot > Reboot

Click Reboot to reboot the device immediately.



Please keep the device powered on during reboot. Otherwise, the device may be damaged.

5.5 Configuring System Time

Choose System > Time.

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the bridge supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.

Configure and view	v time (The device has no RTC i	module. The t	ime settings will not be saved upon reboot).
Current Time	2022-02-18 22:14:28 Edit		
* Time Zone	(GMT+8:00)Asia/Shanghai	~	
* NTP Server	0.cn.pool.ntp.org	Add	
	1.cn.pool.ntp.org	Delete	
	cn.pool.ntp.org	Delete	
	pool.ntp.org	Delete	
	asia.pool.ntp.org	Delete	
	europe.pool.ntp.org	Delete	
	ntp1.aliyun.com	Delete	
	Save		

5.6 Configuring Config Backup and Import

Choose System > Management > Backup & Import

Configure backup: Click **Backup** to download a configuration file locally.

Configure import: Click **Browse**, select a configuration file backup on the local PC, and click **Import** to import the configuration file. The device will restart.

Backu	p & Import	Reset	Session Timeou	t			
1		version is much		ent version, some c porting the configura		pe missing. vill be rebooted automaticall	y later.
1	kup Conf	ig Backup					
Imp	oort Config	9	•				
	File Path	Please select	t a file.	Browse	Import		

5.7 Performing Update and Displaying the System Version

5.7.1 Online Update

Choose System > Update > Online Update.

If there a new version available, you can click it for an update.

A Caution

After being updated, the device will reboot. Therefore, exercise caution when performing this operation.

If no version update is detected or online update cannot be performed, check whether the bridge is connected to the Internet.

Online Update	Local Update	Update All Devices
<i>i</i> Online U Online up		nt configuration. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after update.
Current Version	AP_3.0(1)B11	

5.7.2 Local Update

Choose System > Update > Local Update.

You can view the current software version, hardware version and device model. If you want to update the device with the configuration retained, check **Keep Config**. Click **Browse**, select an update package on the local PC, and click **Upload** to upload the file. The device will be updated.

Online Update	Local Update	Update All Devices	
<i>i</i> Local Upda Please do no		or close the browser.	
Model			
Version	AP_3.0(1		
Development Mode	(It is reco	ommended to be disabled after use.)	
Keep Config	(If the target	t version is much later than the current version, it is recommended not to keep the configu	ıration.)
Update File	Select	Browse Upload	
A Caution			

After being updated, the device will reboot. Therefore, exercise caution when performing this operation.

5.7.3 Update All Devices

Choose System > Update > Update All Devices.

You can view the current software version, hardware version and device model. You are advised to update all devices with configuration data retained.

Click **Browse**, select an update package on the local PC, and click **Upload** to upload the file. In the pop-up page, click **Details** to check the target update package and devices. Click **Update** to start updating all devices.

Online Update	Local Update	Update All Devices
	e All Devices all devices in the network	x. Please do not refresh the page or close the browser.
Model		
Version	AP_3.0(1	
Keep Config	(Uneditable)	
Update File	Select	Browse Upload

A Caution

After being updated, all devices in the network will reboot, which may take a long time. Therefore, exercise caution when performing this operation.

After the update is complete, please log in to Eweb to check the software version number (see <u>2.12</u> <u>Displaying the Information About a Single Device</u>). If update fails, please choose **Local Update** or **Update All Devices** to perform update again.

5.8 Switching System Language

Click in the upper right corner of the page. Select the target language from the drop-down list.

	English ~	
1	中文	
	English	

🚺 Note

Only Chinese and English are available.

5.9 Configuring SNMP

🚺 Note

SNMP is supported on RG- AirMetro550G-B, RG- AirMetro460F and RG- AirMetro460G only.

5.9.1 Overview

The Simple Network Management Protocol (SNMP) is a protocol for managing network devices. Based on the client/server model, it can achieve remote monitoring and control of network devices.

SNMP uses a manager and agent architecture. The manager communicates with agents through the SNMP protocol to retrieve information such as device status, configuration details, and performance data. It can also be used to configure and manage devices.

SNMP can be used to manage various network devices, including routers, switches, servers, firewalls, etc. You can achieve user management through the SNMP configuration interface and monitor and control devices through the third-party software.

5.9.2 Global Configuration

1. Overview

The purpose of global configuration is to enable the SNMP service and make the SNMP protocol version (v1/v2c/v3) take effect, so as to achieve basic configuration of local port, device location, and contact information.

SNMP v1: As the earliest version of SNMP, SNMP v1 has poor security, and only supports simple community string authentication. SNMP v1 has certain flaws, such as plaintext transmission of community strings and vulnerability to attacks. Therefore, SNMP v1 is not recommended for modern networks.

SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

SNMP v3: As the newest version, SNMP v3 supports security mechanisms such as message authentication and encryption compared to SNMP v1 and SNMP v2c. SNMP v3 has achieved significant improvements in security and access control.

2. Configuration Steps

System > SNMP > Global Config

(1) Enable the SNMP service.

Global Config		
SNMP Service		
* SNMP Version	☑ v1 ☑ v2c	Are you sure you want to Enable SNIMP2SNIMP
* Local Port	161	Are you sure you want to Enable SNMP?SNMP v1/v2c is considered unsafe. Therefore, only SNMP v3 is enabled by default. To proceed, please add
* Device Location	Company	 SNMP v3 users by selecting View/Group/Community/User Access Control before using the SNMP service.
* Contact Info	Ruijie@Ruijie.cc	Cancel
	Save	

When it is enabled for the first time, SNMP v3 is enabled by default. Click OK.

(2) Set SNMP service global configuration parameters.

Global Config Vie	w/Group/Community/Client Access Control	Trap Settings
SNMP Service		
* SNMP Version	🗹 v1 🗹 v2c 🗹 v3	
* Local Port	161	
* Device Location	Company	
* Contact Info	Ruijie@Ruijie.com	
	Save	

Table 5-1 Global Configuration Parameters

Parameter	Description
SNMP Server	Indicates whether SNMP service is enabled.
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.
Local Port	The port range is 1 to 65535.
Device Location	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Contact Info	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.

(3) Click Save.

After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

5.9.3 View/Group/Community/User Access Control

1. Configuring Views

Overview

Management Information Base (MIB) can be regarded as a database storing the status information and performance data of network devices. It contains a large number of object identifiers (OIDs) to identify the status information and performance data of these network devices.

Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

A view can have multiple subtrees. The management system can only access MIB nodes in these subtrees, and cannot access other unauthorized MIB nodes. This can prevent unauthorized system administrators from accessing sensitive MIB nodes, thereby protecting the security of network devices. Moreover, views can also improve the efficiency of network management and speed up the response from the management system.

Configuration Steps

System > SNMP > View/Group/Community/Client Access Control

View List			+ Add	Delete Selected
Up to 20 entries are allowed.				
	View Name	Action		
	all			
	none			

(1) Click Add under the View List to add a view.

(2) Configure basic information of a view.

Add			×
* View Name			
OID	Example: .1.3		
	Add Included Rule	Add Excluded Rule	
Rule/OID List			Delete Selected
Up to 100 entries are	e allowed.		
R	Rule	OID	Action
		No Data	
Total 0 10/page V	< 1 →	Go to 1	
			Cancel

Table 5-2 View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.

Parameter	Description	
	There are two types of rules: included and excluded rules.	
Туре	The included rule only allows access to OIDs within the OID range. Click Add Included Rule to set this type of view.	
	Excluded rules allow access to all OIDs except those in the OID range. Click Add Excluded Rule to configure this type of view.	

Note

A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click OK.

2. Configuring v1/v2c Users

Overview

When the SNMP version is set to v1/v2c, user configuration is required.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Se	ervice	
* SNMP Ve	ersion 🗹 v1 🗹 v2c 🗌 v3	
* Loca	al Port 161	
* Device Loo	cation Company	
* Contac	ct Info Ruijie@Ruijie.com	
	Save	

1 Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

Configuration Steps

System > SNMP > View/Group/Community/Client Access Control

(1) Click Add in the SNMP v1/v2c Community Name List pane.

SNMP v1/v2c Community Name List						
				+ Add		
Up to 20	D entries are allowed.					
	Community Name	Access Mode	MIB View	Action		
	Ttttttt8	Read & Write	all	Edit Delete		
	hello_12121	Read & Write	all	Edit Delete		

(2) Add a v1/v2c user.

Add					×
* Community Name					
* Access Mode	Read-Only	~			
* MIB View	all	~	Add	View +	
				Cancel	ОК

Table 5-3 v1/v2c User Configuration Parameters

Parameter	Description
Community Name	At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Access Mode	Indicates the access permission (read-only or read & write) for the community name.
MIB View	The options under the drop-down box are configured views (default: all, none).

Note

- Community names cannot be the same among v1/v2c users.
- Click Add View to add a view.

3. Configuring v3 Groups

Overview

SNMP v3 introduces the concept of grouping to achieve better security and access control. A group is a group of SNMP users with the same security policies and access control settings. With SNMP v3, multiple groups can be configured, each with its own security policies and access control settings. Each group can have one or more users.

• Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Servi	ce 🚺	
* SNMP Versio	on 🗌 v1 🗌 v2c 🔽 v3	
* Local Po	ort 161	
* Device Locatio	Company	
* Contact In	fo Ruijie@Ruijie.com	
	Save	

Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

• Configuration Steps

System > SNMP > View/Group/Community/Client Access Control

(1) Click Add in the SNMP v3 Group List pane to create a group.

SNMP	v3 Group List				+ Add	C Delete Selected
Up to 20	0 entries are allowed.					
	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
	default_group	Auth & Security	all	none	none	Edit Delete

(2) Configure v3 group parameters.

Add				×
* Group Name				
* Security Level	Allowlist & Security \lor			
* Read-Only View	all	Add	View +	
* Read & Write View	all	Add	View +	
* Notification View	none ~	Add	View +	
			Cancel	ОК

Table 5-4 v3 Group Configuration Parameters

Parameter	Description
Group Name	Indicates the name of the group. 1-32 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Security Level	Indicates the minimum security level (authentication and encryption, authentication but no encryption, no authentication and encryption) of the group.
Read-Only View	The options under the drop-down box are configured views (default: all, none).

Parameter	Description
Read & Write View	The options under the drop-down box are configured views (default: all, none).
Notify View	The options under the drop-down box are configured views (default: all, none).

Note

- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click Add View.
- (3) Click **OK**.

4. Configuring v3 Users

• Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Serv	vice	
* SNMP Vers	sion v1 v2c v3	
* Local F	Port 161	
* Device Locat	tion Company	
* Contact I	nfo Ruijie@Ruijie.com	
	Save	

Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

• Configuration Steps

Cancel

System > SNMP > View/Group/Community/Client Access Control

(1) Click Add in the SNMP v3 Client List pane to add a v3 user.							
SNMP v3 Client List							~
						+ Add	Delete Selected
Up to 50 entries are allowed.							
Username Gr	roup Name Security Lev	vel Auth P	Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
			No Data				
(2) Configure v3 use	r parameters.						
							×
Add							~
* 11							
* Username	Username						
* Group Name	default_group	~					
* Security Level	Auth & Security	~					
* Auth Protocol	MD5	\sim		* Auth Passwo	rd		
* Encryption Protocol	AES	~	* Er	ncrypted Passwo	rd		

 Table 5-5
 v3 User Configuration Parameters

Parameter	Description
	Username
	At least 8 characters.
Username	It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.
	Admin, public or private community names are not allowed.
	Question marks, spaces, and Chinese characters are not allowed.
Group Name	Indicates the group to which the user belongs.
Security Level	Indicates the security level (authentication and encryption, authentication but no encryption, and no authentication and encryption) of the user.

Parameter	Description
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

1 Note

- The security level of v3 users must be greater than or equal to that of the group.
- There are three security levels, among which authentication and encryption requires the configuration of authentication protocol, authentication password, encryption protocol, and encryption password. Authentication but no encryption only requires the configuration of authentication protocol and encryption protocol, while no authentication and encryption does not require any configuration.

5.9.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

Application Scenario

You only need to monitor the device information, but do not need to set and deliver it. A third-party software can be used to monitor the data of nodes like 1.3.6.1.2.1.1 if v2c version is configured.

Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "public", and the default port number is 161.

Table 5-6 User Requirement Specification

Item	Description
Read & write permission	Read-only permission.

- Configuration Steps
- (1) In the global configuration interface, select v2c and set other settings as default. Then, click Save.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Se	ervice	
* SNMP Ve	ersion 🗌 v1 🗹 v2c 🗌 v3	
* Loca	l Port 161	
* Device Loc	cation Company	
* Contac	t Info Ruijie@Ruijie.com	
	Save	

- (2) Add a view on the View/Group/Community/Client Access Control interface.
 - a Click Add in the View List pane to add a view.
 - b Enter the view name and OID in the pop-up window, and click Add Included Rule.
 - c Click OK.

Add				×
* View Name	system			
OID	.1.3.6.1.2.1.1			
	Add Included Rule	Add Excluded Rule		
Rule/OID List			🔟 Delete Sele	ected
Up to 100 entries are	e allowed.			
Rul	e	OID	Action	
Includ	ded	.1.3.6.1.2.1.1	Delete	
Total 1 10/page V	< 1 →	Go to page 1		
			Cancel	ОК

- (3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.
 - a Click Add in the SNMP v1/v2c Community Name List pane.
 - b Enter the group name, access mode, and view in the pop-up window.
 - c Click OK.

Add				×
* Community Name	Community1			
* Access Mode	Read-Only	~		
* MIB View	system	~	Add View +	
			Cancel	OK

2. Configuring SNMP v3

Application Scenario

You need to monitor and control devices, and use the third-party software to monitor and deliver device information to public nodes (1.3.6.1.2.1). The security level of v3 is authentication and encryption.

• Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
	Group name: group
	Security level: authentication and encryption
Group configuration	Select public_view for a read-only view.
	Select public_view for a read & write view.
	Select none for a notify view.
	User name: v3_user
	Group name: group
Configuring v3 Users	Security level: authentication and encryption
	Authentication protocol/password: MD5/Ruijie123
	Encryption protocol/password: AES/Ruijie123
Version	For SNMP v3, the default port number is 161.

Table 5-7 User Requirement Specification

Configuration Steps

(1) On the global configuration interface, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Serv	ice 🗾	
* SNMP Versi	ion 🗌 v1 🗌 v2c 🗹 v3	
* Local P	ort 161	
* Device Locati	Company	
* Contact Ir	nfo Ruijie@Ruijie.com	
	Save	

(2) Add a view on the View/Group/Community/Client Access Control interface.

- a Click Add in the View List pane.
- b Enter the view name and OID in the pop-up window, and click Add Included Rule.
- c Click OK.

 \times

Add

* View Name	piblic_view		
OID	.1.3.2.6.1.2.1		
	Add Included Rule	Add Excluded Rule	
Rule/OID List		[Delete Selected
Up to 100 entries ar	e allowed.		
Rul	e	OID	Action
Inclue	ded	.1.3.2.6.1.2.1	Delete
Total 1 10/page 🗸	< 1 →	Go to page 1	
			Cancel

- (3) On the View/Group/Community/Client Access Control interface, add an SNMP v3 group.
 - a Click Add in the SNMP v3 Group List pane.
 - b Enter the group name and security level on the pop-up window. As this user has read and write permissions, select public_view for read-only and read & write views, and select none for notify views.
 - c Click **OK**.

 \times

 \times

Cancel

Add

*

* Group Name	group			
* Security Level	Allowlist & Security			
* Read-Only View	public_view \lor	Add	View +	
Read & Write View	public_view \lor	Add	View +	
* Notification View	none	Add	View +	
			Cancel	ОК

(4) On the View/Group/Community/Client Access Control interface, add an SNMP v3 user.

- a Click Add in the SNMP v3 Client List pane.
- b Enter the user name and group name in the pop-up window. As the user's security level is authentication and encryption, enter the authentication protocol, authentication password, encryption protocol, and encryption password.
- c Click **OK**.

Add

* Username v3_user1 * Group Name group ~	
* Group Name group ~	
* Group Name group ~	
* Security Level Auth & Security \vee	
* Auth Protocol MD5 ~ * Auth Password Ruijie123	
Encryption Protocol AES ~ * Encrypted Password Ruijie123	

5.9.5 Configuring Trap Service

Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring and fault diagnosis services, helping administrators discover and solve network problems in a timely manner.

1. Enabling Trap Service

Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

System > SNMP > Trap Setting

Global Config View/Group/Commu	nity/Client Access Control Tra	p Settings		
Trap Service				
* Trap Version 🗹 v1 🗌 v2d	: 🗍 v3			
Save Trap v1/v2c Client List	 Are you sure you want to 	Enable trap?	+ Add	Delete Selected
Up to 20 entries are allowed.				
Dest Host IP	Version Number	Port ID	Community Name	Action
		No Data		

When the trap service is enabled for the first time, the system will pop up a prompt message. Click OK.

Global Config	View/Group/	Community	/Client Access Control	Trap Settings
Trap Serv	vice 🔵			
* Trap Vers	sion 🗹 v1	v2c	v3	
		Save		

(2) Set the trap version.

The trap versions include v1, v2c, and v3.

(3) Click **OK**.

After the trap service is enabled, click **Save** for the configuration to take effect.

2. Configuring Trap v1/v2c Users

Overview

Trap is a notification mechanism that is used to send alerts to administrators when important events or failures occur on devices or services. Trap v1/v2c are two versions in the SNMP protocol for network management and monitoring.

Trap v1 is the first version that supports basic alert notification functionality. Trap v2c is the second version, which supports more alert notification options and advanced security features.

By using trap v1/v2c, administrators can promptly understand problems on the network and take corresponding measures.

• Prerequisites

Once trap v1 and v2c versions are selected, it is necessary to add trap v1v2c users.

- Procedure
- System > SNMP > Trap Setting
- (1) Click Add in the Trap v1/v2c Client List pane to add a trap v1/v2c user.

Global Config	View/Group/Comm	unity/Client Access Control	Trap Settings				
Тгар	Service 🚺						
* Trap \	Version 🗹 v1 🗹 v2	c v3					
	Save						
Trap v1/v	2c Client List					+ Add	Delete Selected
Up to 20 e	ntries are allowed.						
	Dest Host IP	Version Number	I	Port ID	Community Nam	ie	Action
			No E	Data			

(2) Configure trap v1/v2c user parameters.

* Dest Host IP	Support IPv4/IPv6	
* Version Number	v1 ~	
* Port ID		
* Community	Community Name/Username	
Name/Username		

Cancel OK

 \times

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Version Number	Trap version, including v1 and v2c.
Port ID	The port range of the trap peer device is 1 to 65535.
	Community name of the trap user.
	At least 8 characters.
Community name/User name	It must contain at least three character categories, including uppercase
Community name/Oser name	and lowercase letters, digits, and special characters.
	Admin, public or private community names are not allowed.
	Question marks, spaces, and Chinese characters are not allowed.

Table 5-8 Trap v1/v2c User Configuration Parameters

1 Note

- The destination host IP address of trap v1/ v1/v2c users cannot be the same.
- Community names of trap v1/v1/v2c users cannot be the same.

(3) Click **OK**.

3. Configuring Trap v3 Users

Overview

Trap v3 is a network management mechanism based on the SNMP protocol. It is used to send alert notifications to administrators. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption features.

Trap v3 offers custom conditions and methods for sending alerts, as well as the recipients and notification methods for receiving alerts. This enables administrators to have a more accurate understanding of the status of network devices and to take timely measures to ensure the security and reliability of the network.

• Prerequisites

When the v3 version is selected for the trap service, it is necessary to add a trap v3 user.

Configuration Steps

System > SNMP > Trap Setting

(4) Click Add in the Trap v3 User pane to add a trap v3 user.

Global Config	View/Group/Com	munity/Client Access Co	ntrol Trap Settir	ngs			
Trap	Service 🚺						
* Trap	Version v1	v2c 🗹 v3					
	Sav	e					
Trap v3 C	Client List					+ Add	Delete Selected
Up to 20	entries are allowed.						
	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
				No Data			

(5) Configure trap v3 user parameters.

Add							×
* Dest Host IP	Support IPv4/IPv6		* Port ID				
* Username			* Security Level	Auth & S	Security	~	
* Auth Protocol	MD5	\sim	* Auth Password				
* Encryption Protocol	AES	\sim	* Encrypted Password				
					Cancel	C	Ж

 Table 5-9
 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.
	Name of the trap v3 user.
	At least 8 characters.
Username	It must contain at least three character categories, including uppercase
	and lowercase letters, digits, and special characters.
	Admin, public or private community names are not allowed.
	Question marks, spaces, and Chinese characters are not allowed.

Parameter	Description
Security Level	Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.



The destination host IP address of trap v1/ v1/v2c users cannot be the same.

5.9.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

• Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the thirdparty monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.85 and a port number of 166 to enable the device to send a v2c trap in case of an abnormality.

Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 5-10	User Requirement Specification
------------	--------------------------------

ltem	Description
IP address and	The destination host IP is 192.168.110.85, and the port
port number	number is 166.

Item	Description
Version	Select the v2 version.
Community name/User name	Trap_user

- Configuration Steps
- (1) Select the v2c version in the **Trap Setting** interface and click **Save**.

Global Config	View/Group/Community/Cli	ent Access Control	Trap Settings				
Trap Se	ervice						
* Trap Ve	ersion 🗌 v1 🗹 v2c 🗌) v3					
	Save						
Trap v1/v2	c Client List					+ Add	🖻 Delete Selected
Up to 20 ent	ries are allowed.						
	Dest Host IP	Version Number		Port ID	Community Name		Action
			Ν	o Data			

- (2) Click Add in the Trap v1/v2c Client List to add a trap v2c user.
- (3) Enter the destination host IP address, version, port number, user name, and other information. Then, click **OK**.

A	٩d	d

* Dest Host IP	192.168.110.85	
* Version Number	v2c \lor	
* Port ID	166	
* Community	Trap_user	
Name/Username		

Cancel		O
--------	--	---

 \times

2. Configuring Trap v3

Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the thirdparty monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.87 and a port number of 167 to enable the device to send a v3 trap, which is a safer trap compared with v1/v2c traps.

Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Item	Description		
IP address and port number	The destination host IP is 192.168.110.87, and the port number is 167.		
Version and user name	Select the v3 version and trapv3_user for the user name.		
Authentication protocol/authentication password Encryption protocol/encryption password	Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123		

Table 5-11 User Requirement Specification

Configuration Steps

(1) Select the v3 version in the Trap Setting interface and click Save.

Global Config	View/Group/Com	nmunity/Client Acc	cess Control Trap Se	ttings			
Trap	Service 🚺						
* Trap \	/ersion v1	v2c 🗹 v3					
	Sav	/e					
Trap v3 Cl	ient List					+ Add	Delete Selected
Up to 20 er	ntries are allowed.						
De	est Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
				No Data			
Total 0 10/p	age 🗸 < 🚺	> Go to p	age 1				

- (2) Click Add in the Trap v3 Client List to add a trap v3 user.
- (3) Enter the destination host IP address, port number, user name, and other information. Then, click OK.

* Dest Host IP	Support IPv4		* Port ID			
* Username			* Security Level	Auth & Se	curity	~
* Auth Protocol	MD5	\sim	* Auth Password			
* Encryption Protocol	AES	~	* Encrypted Password			
					Cancel	OK