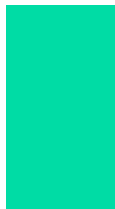
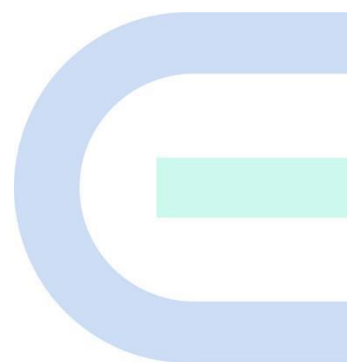


Ruijie Reyee Series Wireless Bridge

Implementation Cookbook



Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.



and other Ruijie networks logos are trademarks of 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, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

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

Technical Support

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


Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click OK . 2. Select Config Wizard . 3. Click the Download File link.
>	Multi-level menus items	Select System > Time .

2. Signs


This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

 Warning


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

 Note

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

 Instruction

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.

3. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

- The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

Contents

Preface	I
1 Product Introduction	1
1.1 RG-EST100-E	1
1.1.1 Appearance	1
1.1.2 Device Specification.....	2
1.1.3 Ports and WPS Hole	4
1.2 RG-EST310 V2	6
1.2.1 Appearance	6
1.2.2 Device Specification.....	7
1.2.3 Port & Button.....	8
1.3 RG-EST350 V2	9
1.3.1 Appearance	9
1.3.2 Device Specification.....	11
1.3.3 Port & Button	12
1.4 RG-AirMetro460G	14
1.4.1 Appearance	14
1.4.2 Technical Specifications.....	15
1.4.3 Ports, Buttons and LEDs	16
1.5 RG-AirMetro460F	18
1.5.1 Appearance	18
1.5.2 Technical Specifications.....	18
1.5.3 Ports, Buttons and LEDs	20

1.6 RG-AirMetro550G-B	22
1.6.1 Appearance	22
1.6.2 Technical Specifications	23
1.6.3 Ports, Buttons and LEDs	25
2 Installation	27
2.1 Safety Suggestions	27
2.1.1 Installation	27
2.1.2 Movement	27
2.1.3 Electricity	27
2.1.4 Static Discharge Damage Prevention	27
2.1.5 Laser	28
2.2 Installation Site Requirement	28
2.2.1 Ventilation	28
2.2.2 Temperature and Humidity	28
2.2.3 Cleanness	28
2.2.4 Grounding	28
2.2.5 EMI	29
2.3 Installing the Device	29
2.3.1 Installation Tools	29
2.3.2 Before Installation	30
2.3.3 Precautions	30
2.3.4 Wall Mounting (Connection with Cables in Advance)	30
2.3.5 Pole Mounting	31
2.3.6 Installing the RG-AirMetro460G	33

2.3.7 Installing the RG-AirMetro460F	35
2.3.8 Installation RG-AirMetro550G-B	37
3 Device Management	48
3.1 Logging In to the Device	48
3.2 Configuring the Wireless Bridge	48
3.3 Configuring Management Password	51
3.4 Setting the System Time.....	52
3.5 Configuring Backup and Import.....	53
3.6 Restoring Factory Settings	54
3.7 Setting the Session Timeout.....	54
3.8 Upgrade	55
3.8.1 Online Upgrade.....	55
3.8.2 Local Upgrade.....	56
3.8.3 Upgrading All Devices.....	56
3.9 Restart.....	57
3.10 Configuring SNMP	58
3.10.1 Overview	58
3.10.2 Global Configuration	58
3.10.3 View/Group/Community/User Access Control	60
3.10.4 SNMP Service Typical Configuration Examples.....	68
3.10.5 Configuring Trap Service	75
3.10.6 Trap Service Typical Configuration Examples.....	79
4 Wi-Fi Network Settings.....	83
4.1 Overview	83

4.1.1 NVR and Camera.....	83
4.1.2 WDS Wi-Fi and Management Wi-Fi	83
4.2 Scanning and Pairing the Camera (CPE).....	83
4.3 Switching NVR and Camera Mode.....	84
4.4 Configuring the WDS Password for All Bridges in the LAN	87
4.5 Configuring the Management SSID and Password for All Bridges in the LAN.....	88
4.6 Configuring the WDS Password for All Bridges in the WDS Group.....	90
4.7 Setting WDS Wi-Fi for a Single NVR or Camera.....	91
4.7.1 Setting the WDS SSID	91
4.7.2 Configuring the WDS Password	92
4.7.3 Saving the Settings	93
4.8 Optimizing Wireless Network.....	93
4.8.1 Overview	93
4.8.2 Getting Started.....	93
4.8.3 Configuration Steps	94
4.9 Changing the Country/Region Code.....	97
4.9.1 Getting Started.....	97
4.9.2 Configuration Steps	98
4.10 Configuring Antenna Alignment.....	98
4.11 Displaying WDS Group Information.....	99
4.12 Displaying the Information About a Single Device	100
4.13 Configuring TDMA Mode	102
4.13.1 Overview	102
4.13.2 Selecting the TDMA Mode	102

4.14 Configuring One-Touch Pairing.....	104
4.14.1 Overview	104
4.14.2 Configuration Steps	105
5 Network Settings	106
5.1 Setting the Address of a LAN Port.....	106
5.1.1 Allocating IP Addresses to All Bridges in the Network.....	106
5.1.2 Setting the Address of a LAN Port for a Single Online Bridge	108
5.1.3 Setting the Address of a LAN Port on the Local Device	109
5.2 Port-based Flow Control	109
5.3 Packet Rate Limiting	111
6 Alarm and Fault Diagnosis	112
6.1 Alarm Information and Suggested Action.....	112
6.1.1 Default Device Name Is Not Modified.....	112
6.1.2 Default Admin Password Is Still Used	113
6.1.3 Default WDS Password Is Still Used by All Devices	114
6.1.4 Network Cable Is Disconnected or Incorrectly Connected.....	114
6.1.5 Latency Is High or Bandwidth Is Insufficient.....	114
6.1.6 Radar Signal Interference.....	116
6.2 Network Diagnosis Tools	116
6.2.1 Network Test Tool.....	116
6.2.2 Collecting Fault Info	117
6.3 Configuring Spectrum Scan.....	117
7 Reye FAQs	120
7.1 Reye Password FAQ	120

7.2 Reyee EST Bridge FAQ.....	120
7.3 Reyee Series Devices Parameters Tables.....	120
7.4 Reyee Parameter Consultation FAQ.....	120
8 Appendix: Monitoring.....	121
8.1 WDS Group Information	121
8.1.1 IP Allocation	122
8.1.2 Configuring the SSID	124
8.1.3 Displaying Information About a Single Device.....	124

1 Product Introduction

1.1 RG-EST100-E

The RG-EST100-E is a dual-stream wireless bridge launched by Ruijie Reyeer for the scenario of surveillance video backhaul. Compliant with the IEEE 802.11n standard, the wireless bridge can work in the 2.4 GHz radio and delivers a maximum data rate of 300 Mbps.

1.1.1 Appearance

Front View



Rear View




1.1.2 Device Specification

Table 1-1 Specification

Radio Design	Single-radio and dual-stream
Standard & Protocol	IEEE 802.11n
Operating Frequency	802.11b/g/n: 2.4000 GHz to 2.483 GHz Note: The operating radio is country-specific.
Antenna Type	Built-in directional antenna
Lobe Angle	Horizontal lobe angle of 70° and vertical lobe angle of 70°
Antenna Gain	6 dBi
Spatial Streams	2.4 GHz: 2 x 2 MIMO
Max. Data Rate	2.4 GHz: 300 Mbps
Modulation	OFDM: BPSK@6/9 Mbps, QPSK@12/18 Mbps, 16-QAM@24 Mbps, and 64-QAM@48/54 Mbps DSSS: DBPSK@1 Mbps, DQPSK@2 Mbps, and CCK@5.5/11 Mbps OFDM: BPSK, QPSK, 16QAM, and 64QAM

Receiver Sensitivity	11b: –91 dBm (1 Mbps), –88 dBm (5 Mbps), –85 dBm (11 Mbps) 11a/g: –89 dBm (6 Mbps), –80 dBm (24 Mbps), –76 dBm (36 Mbps), –71 dBm (54 Mbps) 11n: –83 dBm@MCS0, –65 dBm@MCS7, –83 dBm@MCS8, –65 dBm@MCS15
Max. Transmit Power	100mw
Power Adjustment	Configurable in increments of 1 dBm
Dimensions (W x D x H)	165.5 mm x 68.7 mm x 42 mm (6.52 in. x 2.70 in. x 1.65 in.)
Weight	0.30 kg (0.66 lbs.)
Service Port	Two 10/100Base-T Ethernet ports (LAN1 supports 12 V passive PoE power supply.)
Management Port	N/A
Status LED	One system status LED Two LAN status LEDs Three RSSI LEDs
Power Supply	a. 12 V passive PoE power supply (A passive PoE adapter is delivered with the wireless bridge.) b. 12 V DC power supply (A 12 V DC power adapter is delivered with the wireless bridge.)
Max. Power Consumption	5 W
Temperature	Working Temperature: –30°C to +60°C (–22°F to +140°F)
	Storage Temperature: –40°C to +70°C (–40°F to +158°F)
Humidity	Working Humidity: 5% to 95% (non-condensing)
	Storage Humidity: 5% to 95% (non-condensing)
Installation Method	Wall mounting and pole mounting (Hose clamps are delivered with the wireless bridge.)
Certification	CE
MTBF	> 400,000 hours

 **Caution**

In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

1.1.3 Ports and WPS Hole

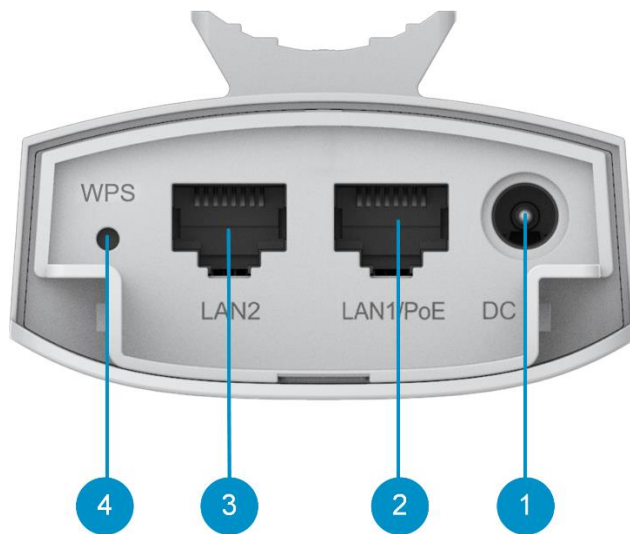


Table 1-2 Ports & WPS Hole

No.	Ports and WPS Hole	Description
1	12 V DC Connector	12 V DC/1 A power supply
2	LAN1/PoE	10/100Base-T Ethernet port, supporting 12 V passive PoE power supply
3	LAN2	10/100Base-T Ethernet port
4	WPS Hole	<ul style="list-style-type: none"> ● Press and hold the pin to the WPS hole for less than 10 seconds: No action is triggered. ● Press and hold the pin to the WPS hole for at least 10 seconds: Restore the wireless bridge to factory settings.



Table 1-3 LED

No,	LED	Status	Description
1	RSSI LEDs	STR1 on	-78 dBm < RSSI < -72 dBm
		STR1 and STR2 on	-72 dBm < RSSI < -65 dBm
		STR1, STR2, and STR3 on	RSSI > -65 dBm
		Blinking	RSSI < -78 dBm
		Off	The device is not bridged.
2	LAN1/LAN2 Port Status LED	Solid on	The LAN port is connected and not receiving or transmitting data.
		Blinking	The LAN port is connected and receiving or transmitting data.

No,	LED	Status	Description
3	System Status LED	Off	The device is not powered on.
		Fast blinking	Possible cases: 1. Restoring the wireless bridge to factory settings. 2. Upgrading the firmware. 3. Handling alarms automatically. 4. Starting up the wireless bridge.
		Solid on	The device is working properly.

1.2 RG-EST310 V2

The RG-EST310 V2 is an 802.11ac wireless bridge launched by Ruijie Reyee. It provides services such as surveillance video backhaul and wireless remote transmission in elevators, tower cranes, factories, parks, construction sites and other scenarios. RG-EST310 V2 works in the 5GHz frequency band, supports two spatial streams and 2 x 2 MIMO, and provides a wireless transmission speed of up to 867Mbps, which is sufficient to meet the bandwidth requirements of user services for data links.

1.2.1 Appearance

Front View



Rear View



1.2.2 Device Specification

Table 1-4 Specification

Radio Design	Single-Frequency Dual-Stream
Transmission Protocol	802.11 a/n/ac
Operating Frequency	802.11a/n/ac: 5.150-5.350GHz, 5.470-5.725GHz, 5.725-5.850GHz United States:802.11a/n/ac:5.180~5.240GHz , 5.745~5.825GHz
Antenna Type	Built-in Directional Antenna, Horizontal 60°, Vertical 30°
Spatial Streams	2
Max Throughput	The 5GHz frequency band provides a wireless transmission speed of up to 867Mbps.
Modulation Types	OFDM: BPSK@6/9Mbps, QPSK@12/18Mbps, 16-QAM@24Mbps, 64-QAM@48/54Mbps OFDM: BPSK, QPSK,16QAM, 64QAM, 256QAM
Receiver sensitivity	802.11a: -89 dBm (6 Mbps), -80 dBm (24 Mbps), -76 dBm (36 Mbps), -71 dBm (54 Mbps) 802.11n: -83 dBm@MCS0, -65 dBm@MCS7, -83 dBm@MCS8, -65 dBm@MCS15 802.11ac: -86 dBm(MCS0), -63 dBm(MCS9)

Max Transmit Power	400mw (26dBm) (Single-Stream)
Transmit Power Adjustment	1 dBm
Dimensions (L x W x H, without bracket)	147 mm x 76 mm x 37 mm (5.78 in. x 2.99 in. x 1.46 in.)
Weight	0.35 kg (0.77 lbs.)
Service Ports	One 10/100BASE-T port, supporting 24 V Passive PoE power supply
Management Ports	N/A
Status LED	One system LED, one Ethernet port LED, and three signal LEDs
Power Supply Method	12 VDC and 24 V Passive PoE power supply
Max Power Consumption	7 W
Bluetooth 5.0	Not supported
Temperature	Operating Temperature: -30°C to 55°C (-22°F to 131°F)
	Storage Temperature: -40°C to 70°C (-40°F to 158°F)
	Operating Humidity: 5% to 95% RH (non-condensing)
	Storage Humidity: 5% to 95% RH (non-condensing)
Installation Methods	Wall Mounting/Pole Mounting
Certification	CE
MTBF	>400000H

1.2.3 Port & Button

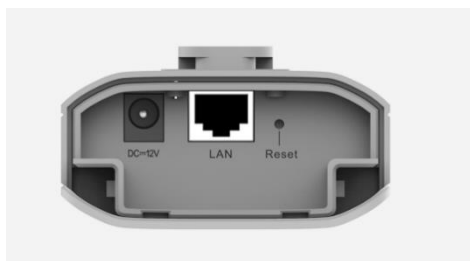


Table 1-5 Ports and Buttons

Item	Description
12 V DC port	Support 12 V/1 A DC power supply

Item	Description
LAN port	10/100Base-T Ethernet port with auto negotiation, supporting 24 V PoE
Reset button	<ul style="list-style-type: none"> ● Press the button for less than 2 seconds, and the device will be rebooted. ● Press the button for over 5 seconds, and the device will be reset.

Table 1-6 LED Description

LED	Status	Description
System Status LED	Off	System is not powered on.
	Solid On	Initiation process is complete.
	Slow Blinking	System is working but there is an alert.
	Fast Blinking	System is being initialized.
Port Status LED	Solid On	The LAN port is not receiving or transmitting data.
	Blinking	The LAN port is receiving or transmitting data.
Signal LED	LED 1 is solid on.	-73 dBm < RSSI < -59 dBm
	LED 1 and LED 2 are solid on.	RSSI > -59 dBm
	LED 1, LED 2 and LED 3 are solid on.	RSSI > -49 dBm
	Off	There is no signal.

1.3 RG-EST350 V2

The RG-EST350 V2 is an 802.11ac wireless bridge launched by Ruijie Reyee. It provides surveillance video backhaul function. RG-EST350 V2 works in the 5GHz frequency band, supports two spatial streams and 2 x 2 MIMO, and provides a wireless link speed of up to 866.7Mbps. The design of RG-EST350 V2 adapts to inclement outdoor environments such as the cold and humidity. This substantially simplifies installation and maintenance.

1.3.1 Appearance

Front View



Rear View



1.3.2 Device Specification

Table 1-7 Specification

Radio Design	Single-Frequency Dual-Stream
Transmission Protocol	802.11 a/n/ac
Operating Frequency	802.11a/n/ac: 5.150-5.350GHz, 5.470-5.725GHz, 5.725-5.850GHz United States:802.11a/n/ac:5.180~5.240GHz , 5.745~5.825GHz
Antenna Type	Built-in Directional Antenna
Bridging Distance	5 km
Spatial Streams	2 x 2MIMO
Max Throughput	The 5GHz frequency band provides a wireless link speed of up to 866.7Mbps.
Modulation Types	OFDM: BPSK@6/9Mbps, QPSK@12/18Mbps, 16-QAM@24/36Mbps, 64-QAM@48/54Mbps MIMO-OFDM: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Receiver sensitivity	11a: -89dBm(6Mbps), -80dBm(24Mbps), -76dBm(36Mbps), -71dBm(54Mbps) 11n: -83dBm@MCS0, -65dBm@MCS7, -83dBm@MCS8, -65dBm@MCS15 11ac VHT20: -83dBm(MCS0), -57dBm(MCS9) 11ac VHT40: -79dBm(MCS0), -57dBm(MCS9) 11ac VHT80: -76dBm(MCS0), -51dBm(MCS9)
Max Transmit Power	400 mw (26 dBm) (adjustable)
Transmit Power Adjustment	1 dBm
Dimensions (L x W x H, without bracket)	230 mm x 132 mm x 48 mm (9.05 in. x 5.19 in. x 1.89 in.)
Weight	0.5 kg (1.1 lbs.)
Service Ports	Two 10/100/1000BASE-T Ethernet ports, LAN1/PoE port supports 24 V PoE power supply
Button	One reset button
Status LED	One system status LED, two LAN port status LEDs and three RSSI LEDs
Power Supply Method	12 V/1 A DC and 24 V/0.5 A PoE power supply
Max Power Consumption	10 W

Temperature	Working Temperature: -30°C to 65°C (-22°F to 149°F)
	Storage Temperature: -40°C to 85°C (-40°F to 185°F)
Humidity	Working Humidity: 5% to 95% (non-condensing)
	Storage Humidity: 5% to 95% (non-condensing)
Installation Methods	Wall Mounting/Pole Mounting
Certification	CE
MTBF	>250000H

Note

The weight refers to the weight of the main unit.

1.3.3 Port & Button

Figure 1-1 Port

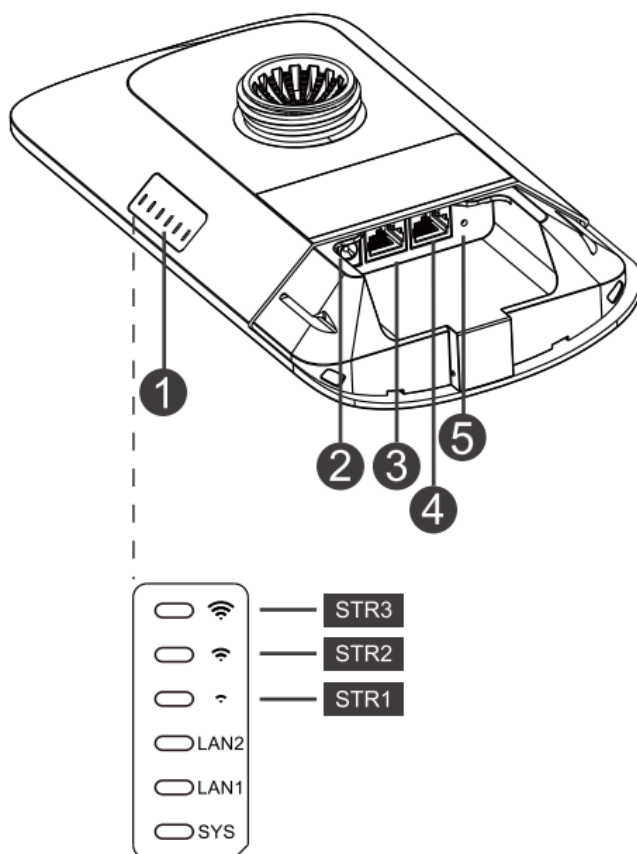


Table 1-8 Port

No.	LED, Button and Port	Meaning
1	Status LED	6 status LEDs (1 system status LED, 2 LAN port status LEDs and 3 RSSI LEDs)
2	12 V DC Port	Support 12 V/1 A DC power supply
3	LAN2 Port	10/100/1000Base-T Ethernet port
4	LAN1/PoE Port	10/100/1000Base-T Ethernet port, support 24 V/0.5 A PoE
5	Reset Button	<ul style="list-style-type: none"> ● Press the button for less than 2 seconds, and the device will be rebooted. ● Press the button for over 5 seconds, and the device will be reset.

Table 1-9 LED

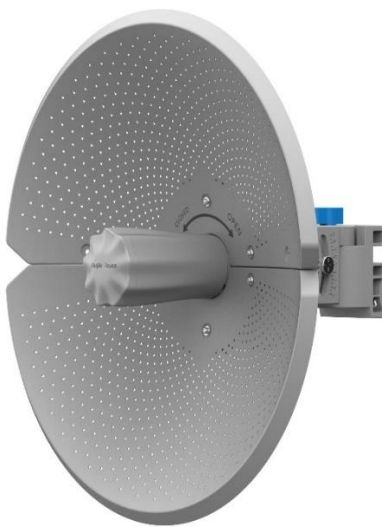
LED	State	Meaning
System Status	Solid green	The device is working properly.
	Blinking green	The system is initializing, restoring factory settings, upgrading or resetting.
	Off	The device is not powered on.
LAN1/LAN 2 Port Status	Solid green	The LAN port is link up and not receiving or transmitting data.
	Blinking green	The LAN port is link up and receiving or transmitting data.
	Off	The LAN port is not connected.
STR [1:3] RSSI (3 LEDs in Total)	STR1 blinking/on	The device is bridged.
	STR1 on	RSSI > -75 dBm
	STR1 on + STR2 blinking	RSSI > -73 dBm
	STR1 on + STR2 on	RSSI > -71 dBm
	STR1 on + STR2 on + STR3 blinking	RSSI > -68 dBm
	STR1 on + STR2 on + STR3 on	RSSI > -64 dBm

1.4 RG-AirMetro460G

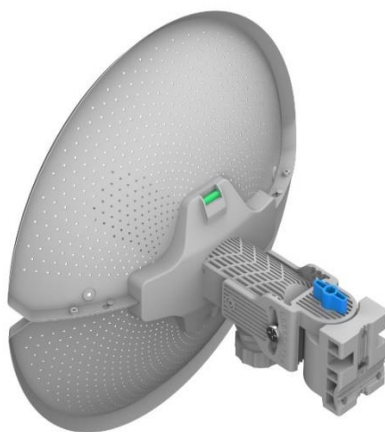
The RG-AirMetro460G wireless bridge is designed for transmitting surveillance video data or wireless data remotely in scenarios such as tower cranes, factory buildings, campuses, construction sites, and forest fire prevention. It utilizes the IEEE 802.11ac standard for efficient and reliable communication. Operating in the 5 GHz band and supporting 2x2 MIMO technology, this product delivers a maximum wireless rate of 867 Mbps for bridging, ensuring more than sufficient bandwidth for delivering point to point (PTP) and point to multi-point (PTMP) services. Moreover, the RG-AirMetro460G wireless bridge also supports the IEEE 802.11n standard. It offers a maximum data rate of 150 Mbps at 2.4 GHz, empowering efficient remote device management.

1.4.1 Appearance

Figure 1-2 Appearance of the RG-AirMetro460G Wireless Bridge



(Front view)



(Back view)

1.4.2 Technical Specifications

Table 1-10 Specifications

Radio Design	2.4 GHz single-band single-stream 5 GHz single-band dual-stream
Operating Frequency Bands	2.4 GHz: 802.11 b/g/n: 2.4000 GHz to 2.483 GHz 5 GHz: 802.11a/n/ac: 5.150 GHz to 5.350 GHz, 5.470 GHz to 5.725 GHz, 5.725 GHz to 5.850 GHz (Note: Country-specific restrictions apply.)
Antenna Type	Directional antenna (horizontal 9°, vertical 9°, point to point) Antenna gain: 23 dBi
Spatial Streams	2.4 GHz single-stream 5 GHz, 2x2, MIMO
Data Rate	2.4 GHz: 150 Mbps 5 GHz: 867 Mbps
Modulation Technology	OFDM: BPSK@6/9Mbps, QPSK@12/18Mbps, 16-QAM@24Mbps, 64-QAM@48/54Mbps DSSS: DBPSK@1Mbps, DQPSK@2Mbps, CCK@5.5/11Mbps MIMO-OFDM: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Receive Sensitivity	11b: -91dBm (1Mbps), -88dBm (5Mbps), -85dBm (11Mbps) 11a/g: -89dBm (6Mbps), -80dBm (24Mbps), -76dBm (36Mbps), -71dBm (54Mbps) 11n: -83dBm@MCS0, -65dBm@MCS7, -83dBm@MCS8, -65dBm@MCS15 11ac VHT20: -83dBm (MCS0), -57dBm (MCS9) 11ac VHT40: -79dBm (MCS0), -57dBm (MCS9) 11ac VHT80: -76dBm (MCS0), -51dBm (MCS9)
Max. Transmit Power	2.4 GHz: ≤ 100 mW (20 dBm) (adjustable) 5 GHz: ≤ 400 mW (26 dBm) (single stream)
Power Step	1 dBm
Dimensions	386.50 mm (length) × 271.00 mm (diameter) (14.50 in. × 10.70 in)
Net Weight	2.33 kg (5.15 lbs.)
Service Ports	1 × 10/100/1000Base-T port, supporting 24 V Passive PoE input
Management Port	N/A
LED	1 × system LED, 1 × port LED, and 3 × signal LED

Power Supply	24 V Passive PoE input (shipped with a 24 V PoE adapter)
Max. Power Consumption	≤ 12 W
Bluetooth 5.0	Not supported
Environment	Operating temperature: -40°C to 70°C (-40°F to +158°F)(excluding the power adapter) (Note: When a power adapter is used, the maximum operating temperature for both the device and the power adapter is 60°C (140°F).)
	Storage temperature: -40°C to 85°C (-40°F to +185°F)
	Operating humidity: 5% to 95% RH (non-condensing)
	Storage humidity: 5% to 95% RH (non-condensing)
Installation	Pole-mounted (shipped with metal clamps)
Wind Resistance Level	17
IP Rating	IP65
Certification	CE
MTBF	> 400000 hrs

1.4.3 Ports, Buttons and LEDs

Figure 1-3 Ports, Buttons and LEDs of the RG-AirMetro460G Wireless Bridge



(Bottom view)

Table 1-11 Ports

Mark	Item	Description
1	Ethernet port	10/100/1000 Base-T port, supporting 24 V Passive PoE input

 Warning

Do not use other models of PoE adapters or switches for power supply as it may lead to irreparable damage to the device.

Table 1-12 LEDs

Mark	Item	Description
2	System LED	Off: The device is NOT receiving power.
		Solid on: The device is operating normally.
		Slow blinking: The device is operating, but an alarm or a power failure occurs.
		Fast blinking (8 to 10 times/second): The device is starting up.
		Fast blinking (2 times/second): The device is initializing.
		Fast blinking (2 times/second): The device is upgrading.
3	Port LED	Off: No port link is established.
		Solid on: A valid link is established, but the port is not receiving or sending data.
		Fast blinking: A valid link is established, and the port is receiving or sending data.
4	Signal LEDs	Off: The device is not bridged.
		LED 1 on/blinking: The device is bridged.
		LED 1 on: The RSSI is above -75 dBm.
		LED 1 on, LED 2 blinking: The RSSI is above -73 dBm.
		LEDs 1 and 2 on: The RSSI is above -71 dBm.
		LEDs 1 and 2 on, LED 3 blinking: The RSSI is above -68 dBm.
		LEDs 1, 2, and 3 on: The RSSI is above -64 dBm.
		LEDs 1, 2, and 3 blinking: The mesh pairing is in progress.

Table 1-13 WPS/Reset Button

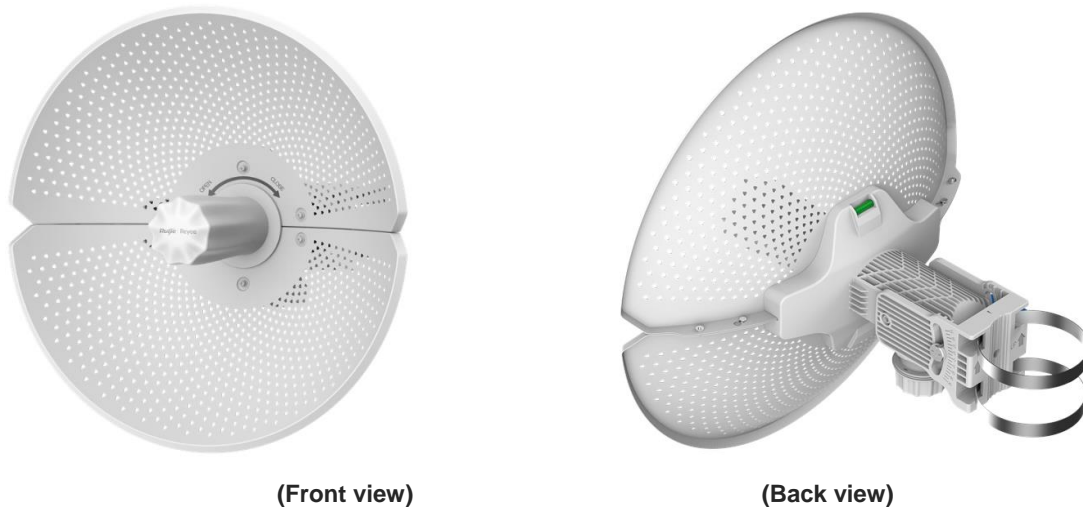
Mark	Item	Description
5	WPS/Reset button	Press and hold for less than 2 seconds: The device establishes a mesh connection with other devices in 30 seconds.
		Press and hold for more than 10 seconds: Restore the device to factory settings.

1.5 RG-AirMetro460F

The RG-AirMetro460F wireless bridge is designed for transmitting surveillance video data or wireless data remotely in scenarios such as tower cranes, factory buildings, campuses, construction sites, and forest fire prevention. It utilizes the IEEE 802.11ac standard for efficient and reliable communication. Operating in the 5 GHz band and supporting 2x2 MIMO technology, this product delivers a maximum wireless rate of 867 Mbps for bridging, ensuring more than sufficient bandwidth for delivering user services. Moreover, the RG-AirMetro460F wireless bridge also supports the IEEE 802.11n standard. It offers a maximum data rate of 150 Mbps at 2.4 GHz, empowering efficient remote device management.

1.5.1 Appearance

Figure 1-4 Appearance of the RG-AirMetro460F Wireless Bridge



1.5.2 Technical Specifications

Table 1-14 Specifications

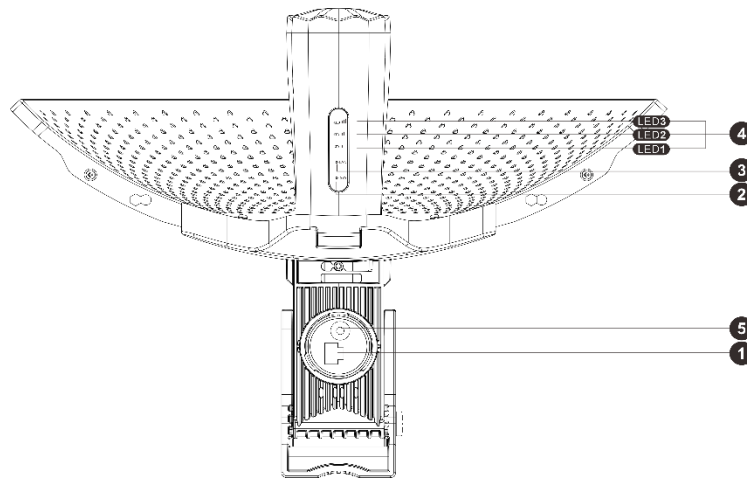
Radio Design	2.4 GHz single-band single-stream
	5 GHz single-band dual-stream

Operating Frequency Bands	2.4 GHz: 802.11 b/g/n: 2.4000 GHz to 2.483 GHz 5 GHz: 802.11 a/n/ac: 5.150 GHz to 5.350 GHz, 5.470 GHz to 5.725 GHz, 5.725 GHz to 5.850 GHz (Note: Country-specific restrictions apply.)
Antenna Type	Directional antenna (horizontal 9°, vertical 9°, point to point) Antenna gain: 23 dBi
Spatial Streams	2.4 GHz single-stream 5 GHz, 2x2, MIMO
Data Rate	2.4 GHz: 150 Mbps 5 GHz: 867 Mbps
Modulation Technology	OFDM: BPSK@6/9Mbps, QPSK@12/18Mbps, 16-QAM@24Mbps, 64-QAM@48/54Mbps DSSS: DBPSK@1Mbps, DQPSK@2Mbps, CCK@5.5/11Mbps OFDM: BPSK, QPSK, 16QAM, 64QAM
Receive Sensitivity	11b: -91dBm (1Mbps), -88dBm (5Mbps), -85dBm (11Mbps) 11a/g: -89dBm (6Mbps), -80dBm (24Mbps), -76dBm (36Mbps), -71dBm (54Mbps) 11n: -83dBm@MCS0, -65dBm@MCS7, -83dBm@MCS8, -65dBm@MCS15
Max. Transmit Power	2.4 GHz: ≤ 100 mW (20 dBm) (adjustable) 5 GHz: ≤ 400 mW (26 dBm) (single stream)
Power Step	1 dBm
Dimensions	368.50 x 271.00 mm (14.50 x 10.70 in.)
Net Weight	2.33 kg (5.15 lbs.)
Service Ports	1 x 10/100Base-T port, supporting 24 V Passive PoE input
Management Port	N/A
LED	1 x system LED, 1 x port LED, and 3 x signal LED
Power Supply	24 V Passive PoE input (shipped with a 24 V PoE adapter)
Max. Power Consumption	≤ 9 W
Bluetooth 5.0	Not supported
Environment	Operating temperature: -40°C to 70°C (-40°F to +158°F)(excluding the power adapter)

	(Note: When a power adapter is used, the maximum operating temperature for both the device and the power adapter is 60°C (140°F).)
	Storage temperature: -40°C to 85°C (-40°F to +185°F)
	Operating humidity: 5% to 95% RH (non-condensing)
	Storage humidity: 5% to 95% RH (non-condensing)
Installation	Pole-mounted (shipped with metal clamps)
Wind Resistance Level	17
IP Rating	IP65
Certification	CE
MTBF	> 400000 hrs

1.5.3 Ports, Buttons and LEDs

Figure 1-5 Ports, Buttons and LEDs of the RG-AirMetro460F Wireless Bridge



(Bottom view)

Table 1-15 Ports

Mark	Item	Description
1	Ethernet port	10/100Base-T port, supporting 24 V Passive PoE input

Warning

Do not use other models of PoE adapters or switches for power supply as it may lead to irreparable damage to the device.

Table 1-16 LEDs

Mark	Item	Description
2	System LED	Off: The device is NOT receiving power.
		Solid on: The device is operating normally.
		Slow blinking: The device is operating but an alarm or a power failure occurs.
		Fast blinking (8 to 10 times/second): The device is starting up.
		Fast blinking (2 times/second): The device is initializing.
		Fast blinking (2 times/second): The device is upgrading.
3	Port LED	Off: No port link is established.
		Solid on: A valid link is established, but the port is not receiving or sending data.
		Fast blinking: A valid link is established, and the port is receiving or sending data.
4	Signal LEDs	Off: The device is not bridged.
		LED 1 on/blinking: The device is bridged.
		LED 1 on: The RSSI is above -75 dBm.
		LED 1 on, LED 2 blinking: The RSSI is above -73 dBm.
		LEDs 1 and 2 on: The RSSI is above -71 dBm.
		LEDs 1 and 2 on, LED 3 blinking: The RSSI is above -68 dBm.
		LEDs 1, 2, and 3 on: The RSSI is above -64 dBm.
		LEDs 1, 2, and 3 blinking: The mesh pairing is in progress.

Table 1-17 WPS/Reset Button

Mark	Item	Description
5	WPS/Reset button	Press and hold for less than 2 seconds: The device establishes a mesh connection with other devices in 30 seconds.
		Press and hold for more than 10 seconds: Restore the device to factory settings.

Note

- Upon pressing the WPS button, the device will automatically switch to AP mode regardless of whether it was functioning as an AP or CPE.
- During mesh pairing, the signal LED on AP side will blink for 3 minutes, and that on CPE side will continue blinking until the bridging process is completed.
- Once the CPE is successfully bridged to the AP via the WPS button, the Reyee Mesh feature must be disabled on the CPE.
- The Reyee Mesh feature is enabled by default. You can manually disable it on the web interface.

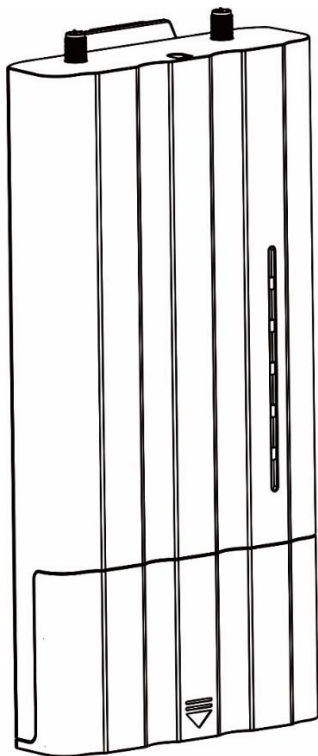
1.6 RG-AirMetro550G-B

The RG-AirMetro550G-B wireless bridge is launched by Ruijie Reyee. Supporting the 2.4 GHz single-stream and the 5 GHz dual-stream 2×2 MIMO technologies, this product delivers a maximum data rate of 150 Mbps at 2.4 GHz and 866.7 Mbps at 5 GHz. When mounted vertically, this wireless bridge can be adjusted within a range of ± 15 to 20 degrees, while when mounted horizontally, it can be adjusted along with the antenna. The RG-AirMetro550G-B wireless bridge can establish a mesh connection with other wireless bridges in 30 seconds by a simple press of the WPS button on this device.

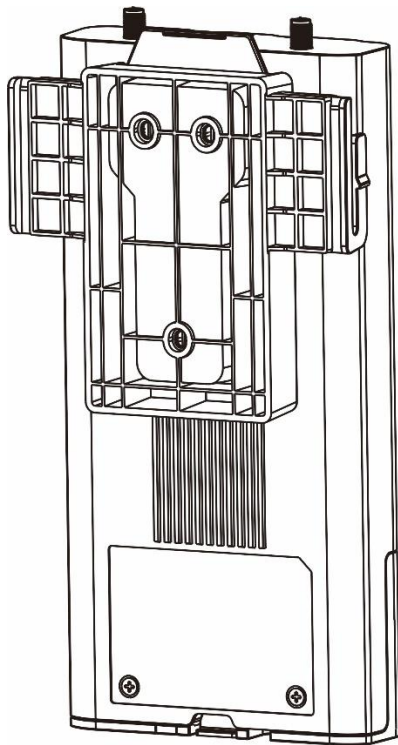
1.6.1 Appearance

Figure 1-6 Appearance of the RG-AirMetro550G-B Wireless Bridge

Front view



Back view



1.6.2 Technical Specifications

Table 1-18 Specifications

Radio Design	2.4 GHz single-stream 5 GHz dual-stream 2x2 MIMO
Protocol and Standard	IEEE 802.11 a/b/g/n/ac
Operating Frequency Bands	2.4 GHz: 802.11 b/g/n: 2.4000 GHz to 2.483 GHz 5 GHz: 802.11a/n/ac: 5.150 GHz to 5.350 GHz, 5.470 GHz to 5.725 GHz, 5.725 GHz to 5.850 GHz (Note: Country-specific restrictions apply.)
Antenna Type	Internal 2.4 GHz PCB onboard antenna and external 5 GHz antenna
Bridging Signal Strength	2/5/10 km (when mounted on a 360°, 120°, or 90° antenna)
Spatial Streams	2x2 MIMO
Data Rate	2.4 GHz: 150 Mbps 5 GHz: 866.7 Mbps
Modulation Technology	OFDM: BPSK@6/9Mbps, QPSK@12/18Mbps, 16-QAM@24/36Mbps, 64-QAM@48/54Mbps

	MIMO-OFDM: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Receive Sensitivity	11a: -89dBm (6Mbps), -80dBm (24Mbps), -76dBm (36Mbps), -71dBm (54Mbps) 11n: -83dBm@MCS0, -65dBm@MCS7, -83dBm@MCS8, -65dBm@MCS15 11ac VHT20: -83dBm (MCS0), -57dBm (MCS9) 11ac VHT40: -79dBm (MCS0), -57dBm (MCS9) 11ac VHT80: -76dBm (MCS0), -51dBm (MCS9)
Max. Transmit Power	≤ 400 mW (26 dBm) (adjustable)
Power Step	1 dBm
Dimensions (L x W x H)	200 mm x 98.5 mm x 29 mm (7.87 in. x 3.88 in. x 1.14 in.) (excluding the mounting bracket)
Net Weight	0.68 kg (1.50 lbs.)
Service Ports	2 x 10/100/1000Base-T auto-negotiation ports, where LAN1/PoE port supports 24 V PoE input
Buttons	1 x reset/WPS button
LED	1 x system LED, 2 x port LED, and 3 x signal LED
Power Supply	24 V Passive PoE input (shipped with a 24 V PoE adapter) 12 V 1 A DC adapter for DC power input
Max. Power Consumption	≤ 12 W
Environment	Operating temperature: -40°C to +80°C (-40°F to +176°F) (excluding the power adapter) (Note: When a power adapter is used, the maximum operating temperature for both the device and the power adapter is 60°C (140°F).) Storage temperature: -40°C to 85°C (-40°F to +185°F) Operating humidity: 5% to 95% RH (non-condensing) Storage humidity: 5% to 95% RH (non-condensing)
Installation	Directly mounted onto an antenna
IP Rating	IP55
Flame Rating	UL94V-0
Certification	CE
MTBF	> 400000 hrs

Note

The weight in the above table indicates the net weight of a single unit.

1.6.3 Ports, Buttons and LEDs

Figure 1-7 Ports, Buttons and LEDs of the RG-AirMetro550G-B Wireless Bridge

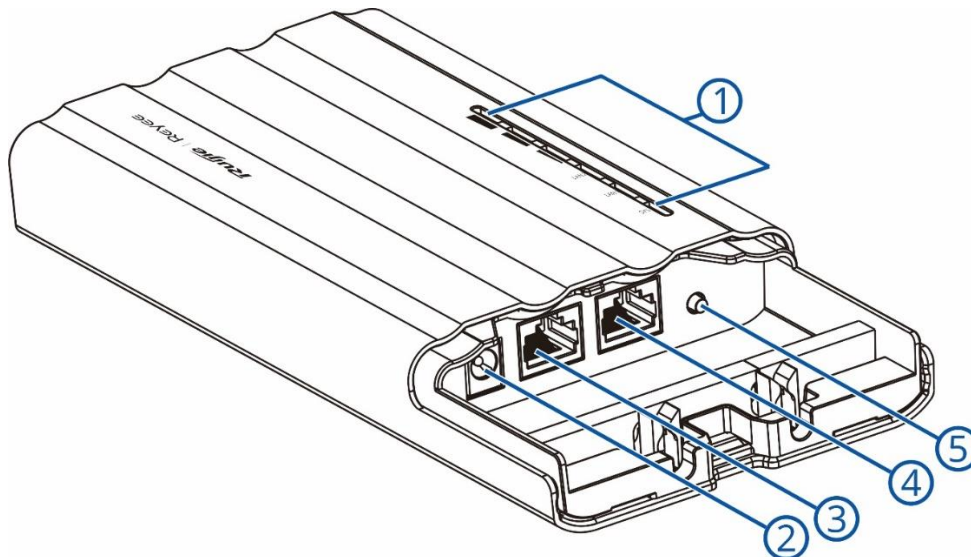


Table 1-19 Ports, Buttons and LEDs of the RG-AirMetro550G-B Wireless Bridge

Mark	Item	Description
1	Status LEDs	6 status LEDs, including 1 × system LED, 2 × port LED and 3 × signal LED
2	12 V DC power port	Connects to a 12 V 1 A DC adapter
3	LAN2 port	10/100/1000Base-T auto-negotiation port
4	LAN1/PoE port	10/100/1000Base-T auto-negotiation port, supporting power input from the shipped 24 V 0.5 A PoE adapter
5	Reset/WPS button	<p>Press and hold for less than 2 seconds: The device establishes a mesh connection with other devices in 30 seconds. (During mesh pairing, the signal LED on the device will continue blinking until the bridging process is completed.)</p> <p>Press and hold for 2 to 10 seconds: No action is triggered.</p> <p>Press and hold for more than 10 seconds: Restore the device to factory settings.</p>

Table 1-20 LEDs

LED	Status	Description
System LED	Solid green	The device is operating normally.
	Blinking	Fast blinking (8 to 10 times/second): The device is starting up. Fast blinking (2 times/second): The device is initializing. Fast blinking (2 times/second): The device is upgrading.
	Off	The device is NOT receiving power.
LAN1/LAN2 port LED	Solid green	A valid link is established, but the port is not receiving or sending data.
	Blinking green	A valid link is established, and the port is receiving or sending data.
	Off	No link is established.
Signal LEDs	Off	The device is not bridged.
	LED 1 on/blinking	The device is bridged.
	LED 1 on	The RSSI is above -75 dBm.
	LED 1 on, LED 2 blinking	The RSSI is above -73 dBm.
	LEDs 1 and 2 on	The RSSI is above -71 dBm.
	LEDs 1 and 2 on, LED 3 blinking	The RSSI is above -68 dBm.
	LEDs 1, 2, and 3 on	The RSSI is above -64 dBm.
	LEDs 1, 2, and 3 blinking	The mesh pairing is in progress.

2 Installation

2.1 Safety Suggestions

To avoid personal injury and equipment damage, read safety suggestions carefully before you install each device. The following safety suggestions do not cover all possible dangers.

2.1.1 Installation

- Keep the chassis clean and free from any dust.
- Do not place devices in a walking area.
- Do not wear loose clothes or accessories that may be hooked or caught by devices during installation and maintenance.

2.1.2 Movement

- Do not frequently move devices.
- When moving devices, keep the balance and avoid hurting legs and feet or straining the back.
- Before moving devices, turn off all power supplies and dismantle all power modules.

2.1.3 Electricity

- Observe local regulations and specifications when performing electric operations. The operators must be qualified.
- Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp or wet ground or floor.
- Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.
- Try to avoid maintaining the switch that is powered-on alone.
- Make a careful check before you cut off the power supply.
- Do not place the equipment in a damp location. Do not let any liquid enter the chassis.

2.1.4 Static Discharge Damage Prevention

To prevent damage from static electricity, pay attention to the following points:

- Properly ground grounding screws on the back panel of the device. Use a three-wire single-phase socket with protective earth wire (PE) as the AC power socket.
- Prevent indoor dust.
- Ensure proper humidity conditions.

2.1.5 Laser

Some devices support varying models of optical modules that are Class I laser products sold on the market. Improper use of optical modules may cause damage. Therefore, pay attention to the following points when you use them:

- When a fiber transceiver is working, ensure that the device port has been connected to an optical fiber or is covered with a dust cap, to keep out dust and avoid burning your eyes.
- When the optical module is working, do not pull out the fiber cable or look directly into a transceiver. The transceiver emits laser light that can damage your eyes.

2.2 Installation Site Requirement

To ensure normal working and a prolonged durable life of EST products, the installation site must meet the following requirements.

2.2.1 Ventilation

When installing devices, reserve at least 10 cm distances from both sides and the back plane of the cabinet at ventilation openings to ensure good ventilation. After cables have been connected, bundle or place the cables on the cabling rack to prevent them from blocking the air inlets. It is recommended that the device be cleaned at regular intervals. In particular, avoid dust from blocking the screen mesh on the back of the cabinet.

2.2.2 Temperature and Humidity

To ensure normal operation and prolong the service life of the device, keep proper temperature and humidity in the equipment room.

If the temperature and humidity in the equipment room do not meet the requirements for a long time, the device may be damaged.

- In an environment with a high humidity, insulating materials may have bad insulation or even leaking electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.
- In an environment with a low humidity, insulating strips may dry and shrink. Static electricity may occur easily and endanger circuits on the device.
- In an environment with a high temperature, the device is subject to more serious harm. Its performance may degrade drastically and various hardware faults may occur.

2.2.3 Cleanness

Dust poses a severe threat to the running of the device. The indoor dust falling on the device may be adsorbed by the static electricity, causing bad contact of the metallic joint. Such electrostatic adsorption may occur more easily when the relative humidity is low. This affects the lifecycle of the devices and causes communication faults.

2.2.4 Grounding

A good grounding system is the basis for stable and reliable operation of the device, preventing lightning strokes and resisting interference. Carefully check the grounding conditions at the installation site according to the grounding requirements, and perform grounding operations properly as required.

Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, down conductor, and connector to the grounding system, which usually shares the power reference ground and ground cable. The lightning discharge ground is targeted for the facility.

EMC Grounding

The grounding required for EMC design includes the shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The resistance of earth wires should be less than 1 Ω .

2.2.5 EMI

Electro-Magnetic Interference (EMI), from either outside or inside the device or application system, affects the system in the conductive ways such as capacitive coupling, inductive coupling, and electromagnetic radiation.

There are two types of electromagnetic interference: radiated interference and conducted interference, depending on the type of the transmission path.

When the energy, often RF energy, from a component arrives at a sensitive component through the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conducted interference results from an electromagnetic wire or signal cable connection between the source and the sensitive component, along which cable the interference conducts from one unit to another. Conducted interference often affects the power supply of the device, but can be controlled by a filter. Radiated interference may affect any signal path in the device and is difficult to shield.

- For the TN AC power supply system, the single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through filtering circuits.
- Do not use the grounding device of the device cannot be used for an electrical device or anti-lightning grounding device. In addition, the grounding device of the device must be deployed far away from the grounding device of the electrical device and anti-lightning grounding device.
- Keep the device away from the high-power radio transmitter, radar transmitting station, and high-frequency large-current device.
- Take measures to shield static electricity.
- Lay interface cables inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device signal interfaces caused by over-voltage or over-current of lightning.

2.3 Installing the Device

2.3.1 Installation Tools

Tools	Marker, Phillips (crosshead) screwdriver, slotted screwdriver, drill, paper knife, crimping pliers, diagonal pliers, wire stripper, network cable tester, power and fiber cables, wrench, hammer, hose clamp, ESD tools, multimeter
--------------	---

2.3.2 Before Installation

Before you install the device, verify that all the parts in the parts list are ready and make sure that the following conditions are met:

- The installation site meets temperature and humidity requirements.
- The installation site is equipped with a proper power supply.
- Network cables are in place.

2.3.3 Precautions

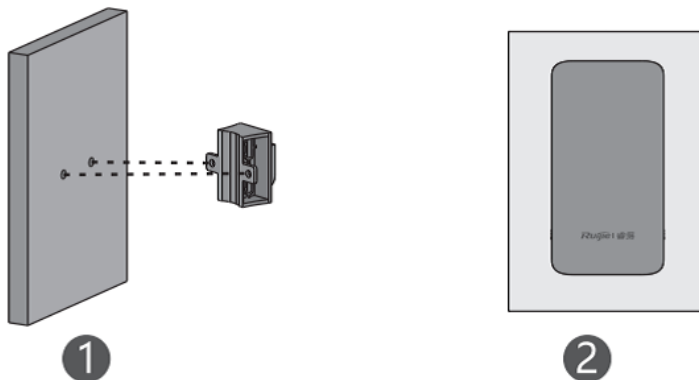
The device can be mounted on a wall and a pole (diameter: 35 mm to 89 mm). If the diameter of the pole is out of the range, the hose clamp should be prepared by customers themselves. In this case, you are advised to use a hose clamp with thickness of 2.5 mm at least. Otherwise, the device may fall down to cause injuries. When multiple bridges are installed at close range, to avoid interference between bridges, the horizontal distance between two bridges should be 2 m and the vertical distance be 0.5 m, or the horizontal angle of the two bridges should be greater than 120 degrees. The installation site can vary due to the onsite survey conducted by technical personnel.

- Before connecting the power supply, use the PoE adapter delivered with the device or use a PoE adapter with the same specification.
- Before connecting the power cord, make sure that the power switch is in the OFF position.
- Make sure that the power supply is properly connected.

2.3.4 Wall Mounting (Connection with Cables in Advance)

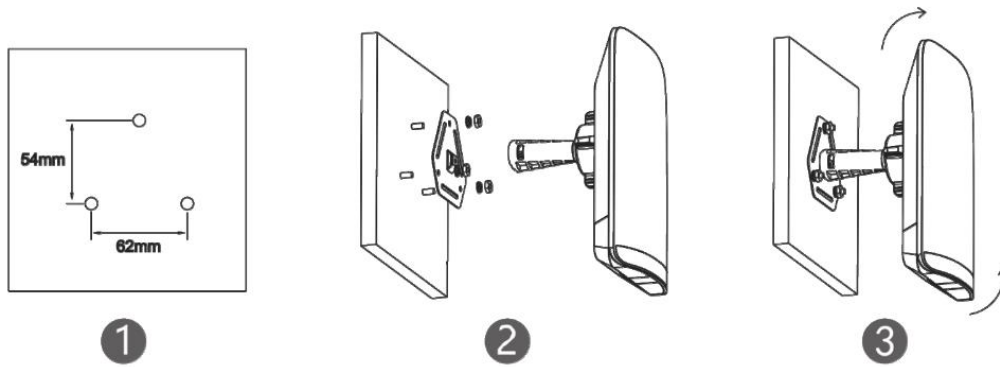
Installing the RG-EST310 V2

- (1) Secure the mounting bracket on the wall using wall anchors and screws.
- (2) Attach the device to the mounting bracket.



Installing the RG-EST350 V2

- (1) Drill holes into the marked positions and insert wall anchors. The head of the wall anchor should be at least 10 mm above the wall surface.
- (3) Assemble the mounting kit.
- (4) Adjust the orientation.



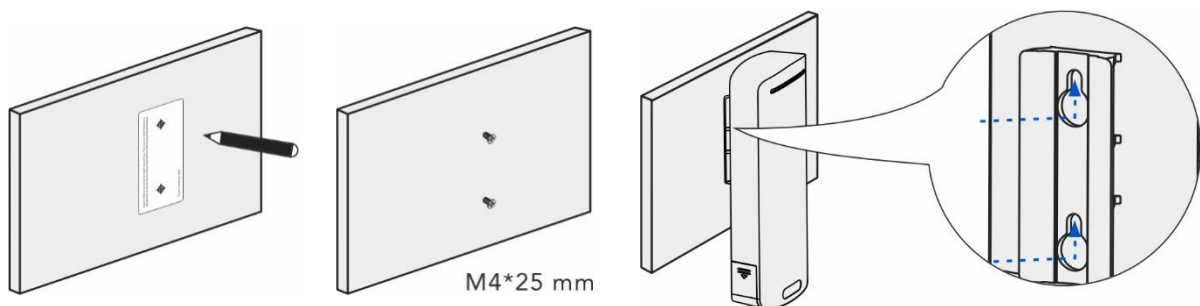
Installing the RG-EST100-E

Use the mounting template to mark where the holes need to be drilled. Then, drill the holes and insert screws into each hole. Mount the device onto the screws to securely hang it in place.

i Note

To mount the device on a wall, prepare two screws (M4 25 kA screws are recommended) by yourself. Make sure the nuts are 8-9mm away from the wall.

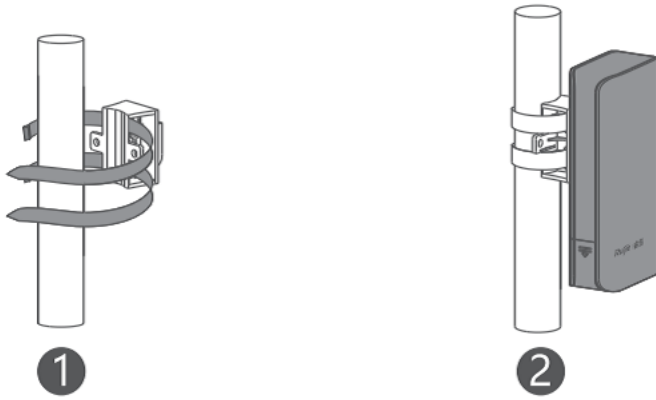
Figure 2-1 Wall Mounting



2.3.5 Pole Mounting

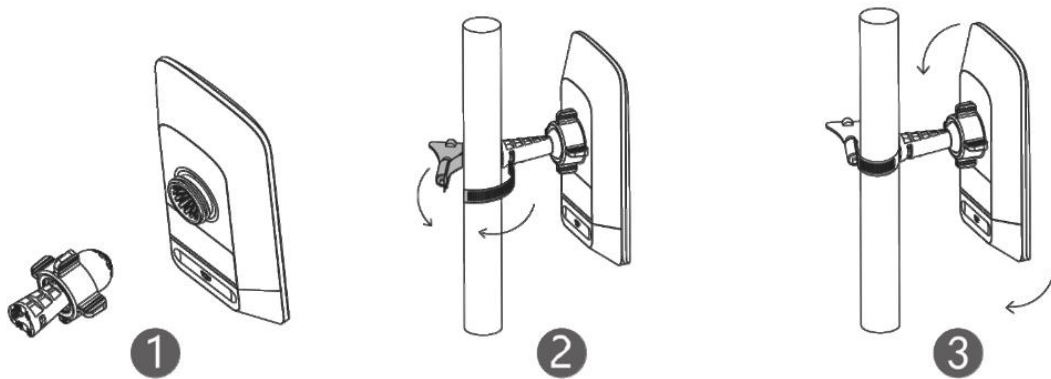
Installing the RG-EST310 V2

- (1) Secure the mounting bracket to the pole by threading two clamps through the mounting bracket.
- (2) Attach the device to the mounting bracket.



Installing the RG-EST350 V2

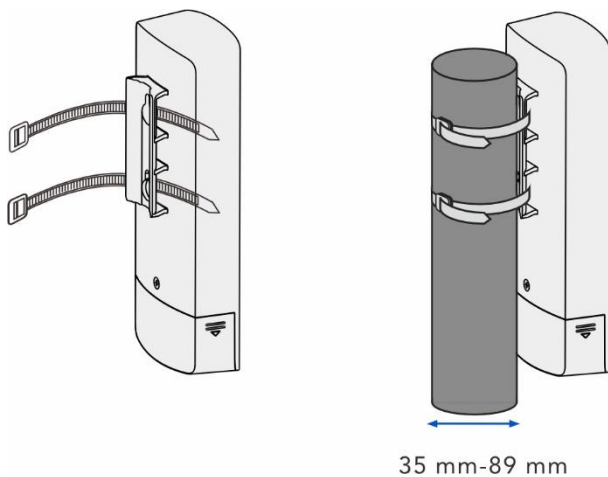
- (1) Assemble the mounting kit.
- (2) Secure the device on a pole by using a hose clamp.
- (3) Adjust the orientation.



Installing the RG-EST100-E

Thread the cable ties through the bracket at the back of the device, and pull the cable ties tight to secure the device to the pole.

Figure 2-2 Pole Mounting

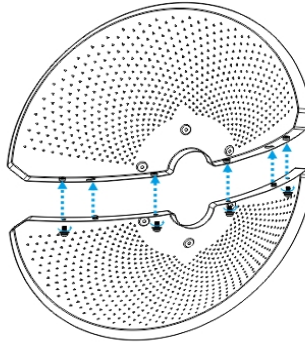


2.3.6 Installing the RG-AirMetro460G

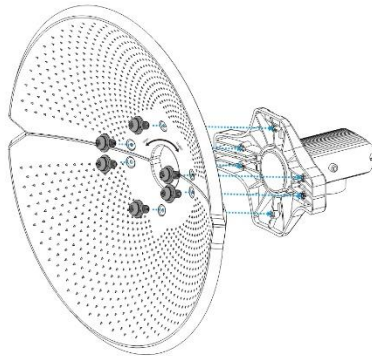
⚠ Caution

- Install the device in a manner that maximizes the coverage area of the antenna.
- The schematic diagram provided is for reference purposes only. The actual product should be installed based on its physical specifications and design.

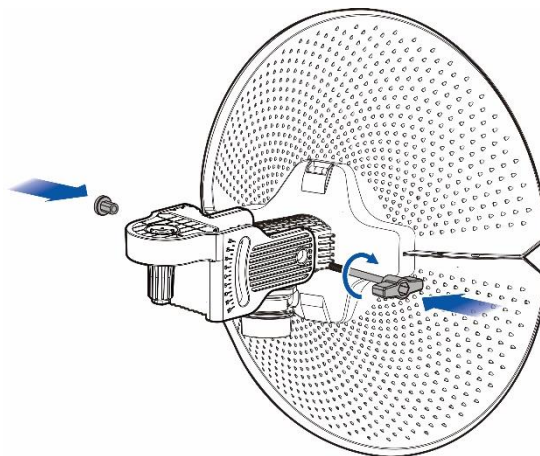
(1) Connect the two reflectors using four screws.



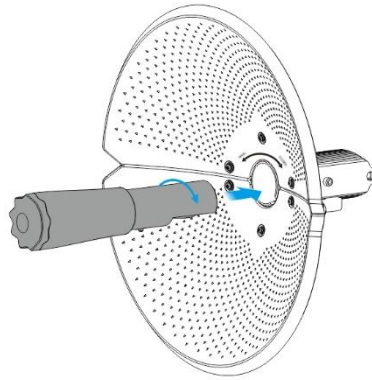
(2) Attach the supporting piece to the back of the assembled reflectors using six screws.



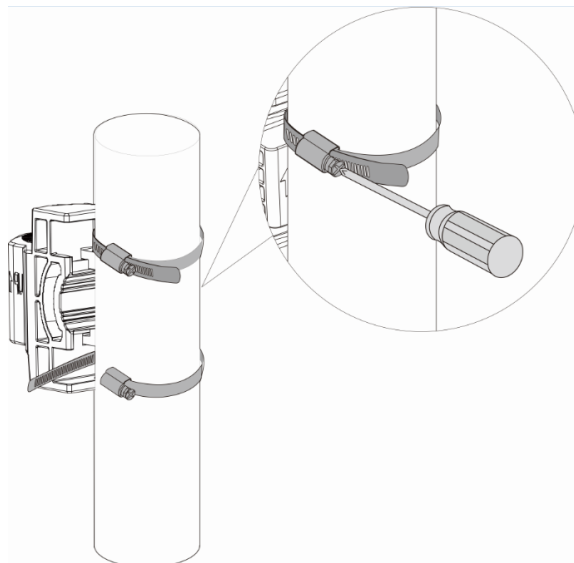
(3) Attach the antenna mounting bracket to the supporting piece using the long screw and the nut.



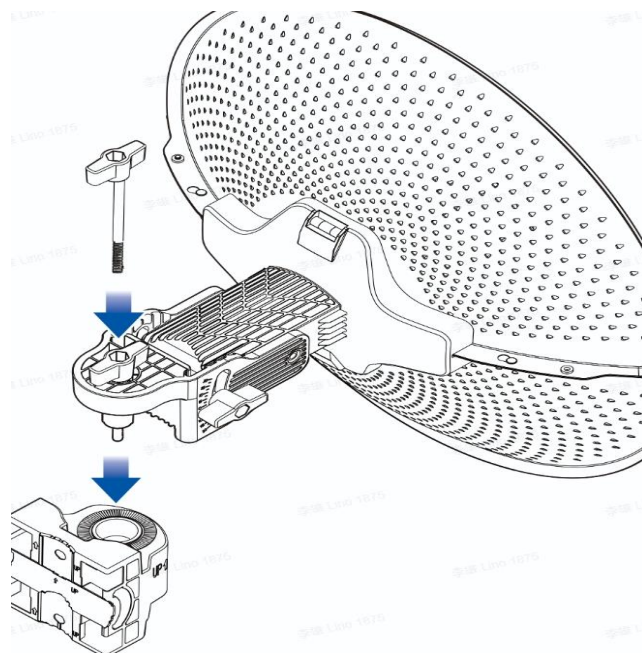
(4) Attach the wireless bridge to the front of the assembled reflectors.



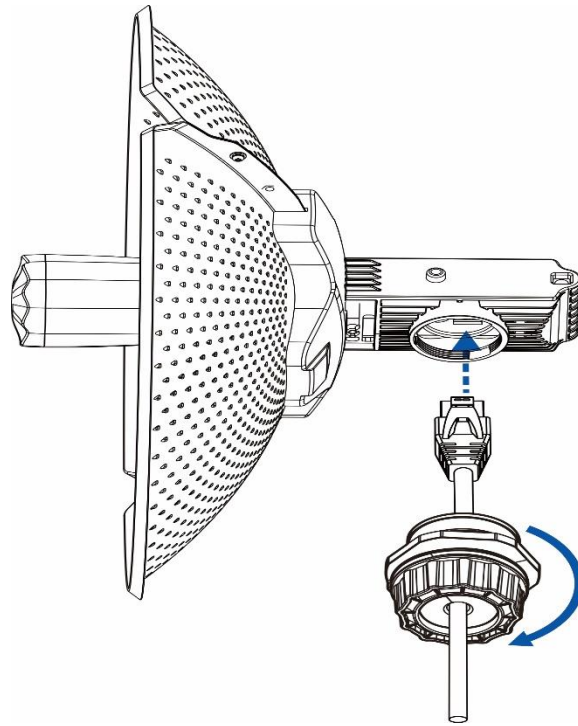
- (5) Mount the pole mounting bracket to the pole, and tighten the clamps.



- (6) Mount the assembled wireless bridge to the pole mounting bracket and tighten the long screw.



- (7) Properly connect the Ethernet cable, and then install the waterproof cover. The installation is complete.

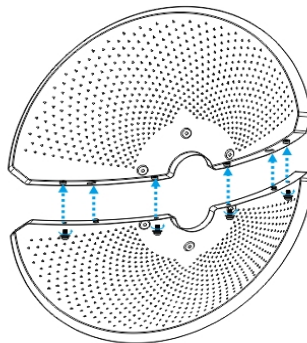


2.3.7 Installing the RG-AirMetro460F

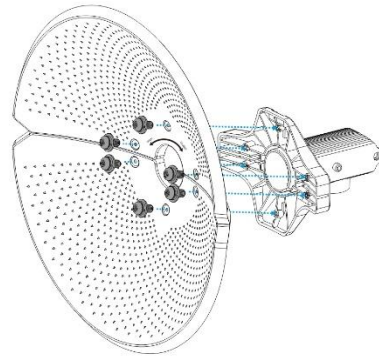
⚠ Caution

- Install the device in a manner that maximizes the coverage area of the antenna.
- The schematic diagram provided is for reference purposes only. The actual product should be installed based on its physical specifications and design.

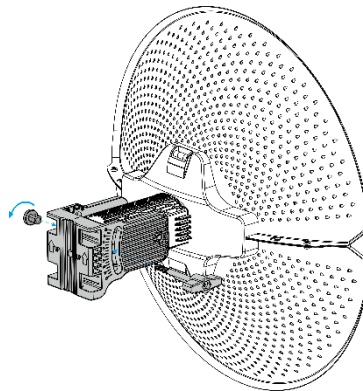
- (1) Connect the two reflectors using four screws.



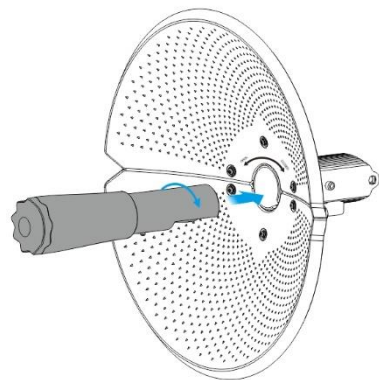
- (2) Attach the supporting piece to the back of the assembled reflectors using six screws.



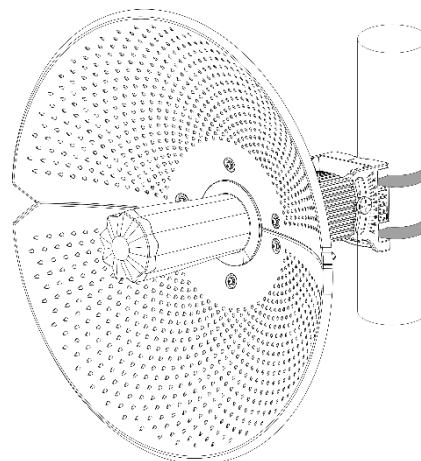
(3) Attach the mounting bracket to the supporting piece using the long screw and the nut.



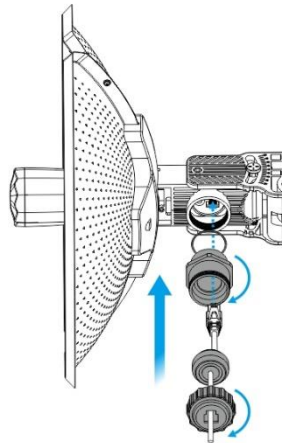
(4) Attach the wireless bridge to the front of the assembled reflectors.



(5) Mount the assembled unit to the pole, and tighten the clamps.



- (6) Properly connect the Ethernet cable, and then install the waterproof cover. The installation is complete.



2.3.8 Installation RG-AirMetro550G-B

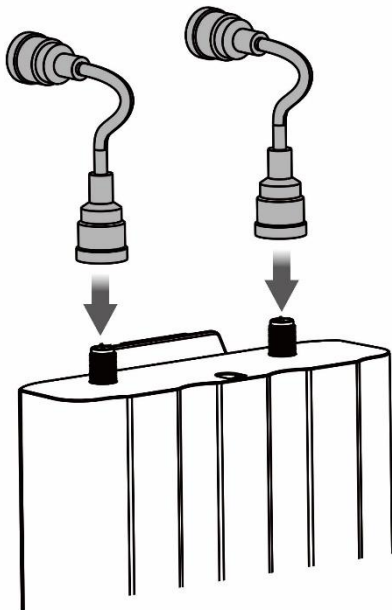
⚠ Caution

- Install the device in a manner that maximizes the coverage area of the antenna.
- The schematic diagram provided is for reference purposes only. The actual product should be installed based on its physical specifications and design.

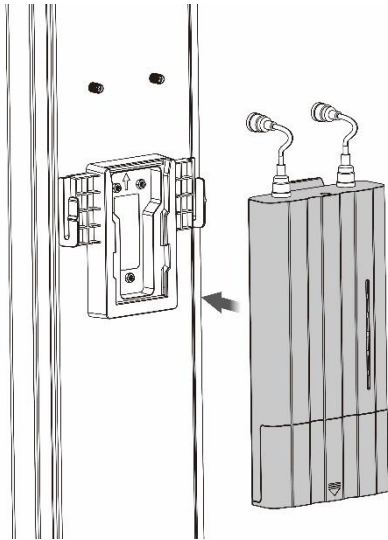
1. Installing the Wireless Bridge

This wireless bridge can be mounted onto 90°, 120°, or 360° antennas. The installation procedure is the same. The following section describes the installation procedure for the 90° antenna.

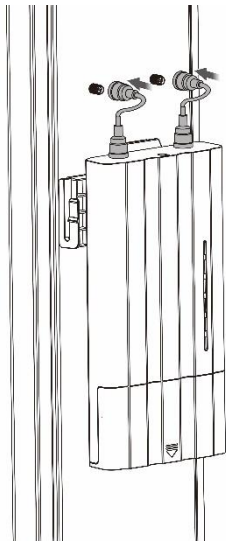
- (1) Connect the RF cable to the SMA connector of the wireless bridge.



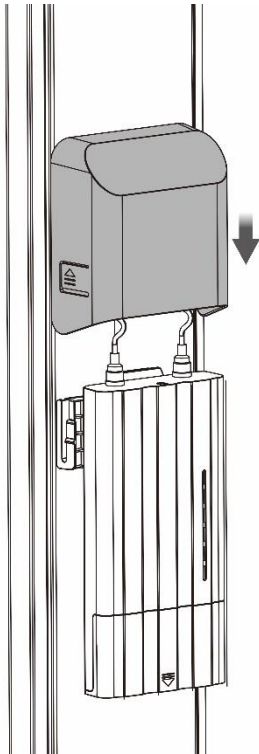
- (2) Attach the wireless bridge to the antenna.



(3) Connect the SMA connector of the wireless bridge to that of the antenna.

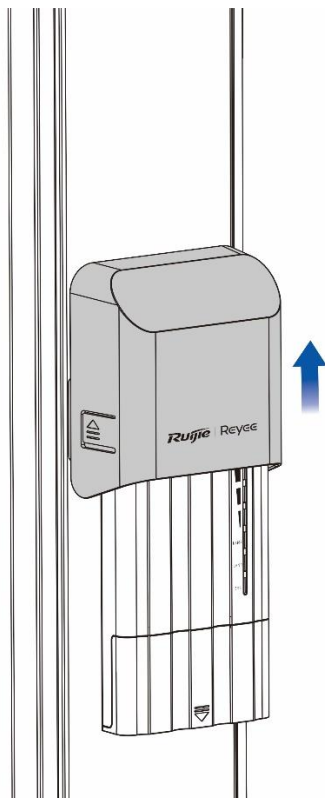


(4) Install the protective cover.



2. Removing the Wireless Bridge

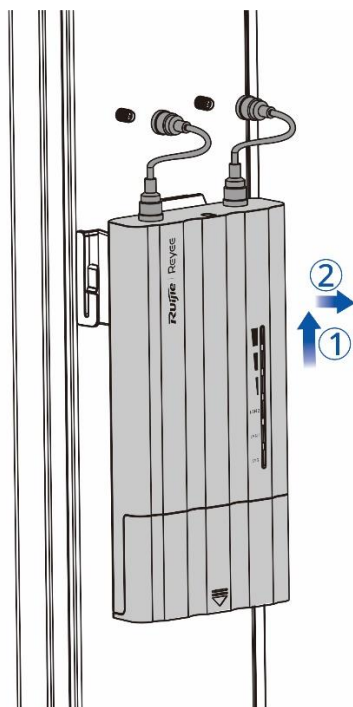
- (1) Remove the protective cover by pulling it upward.



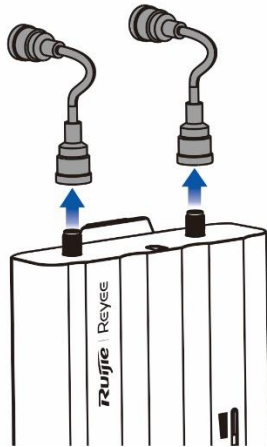
- (2) Unscrew the RF cable.



(3) Remove the wireless bridge by pulling it upward and then outward.



(4) Remove the RF cable.



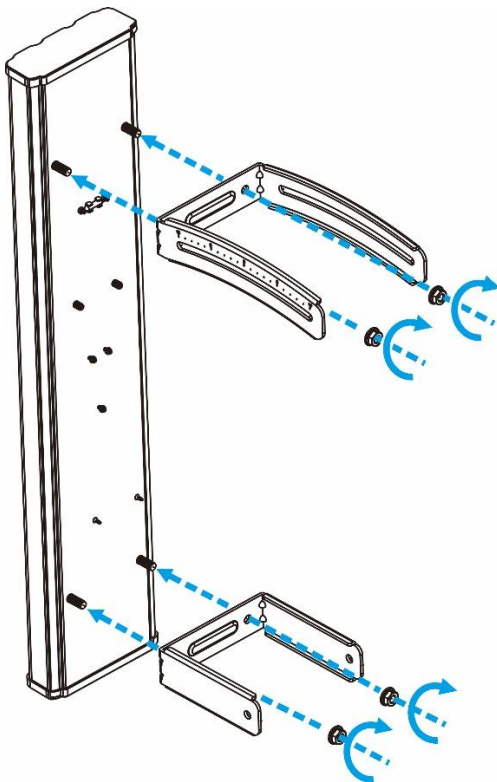
3. Installing the Antenna

i Note

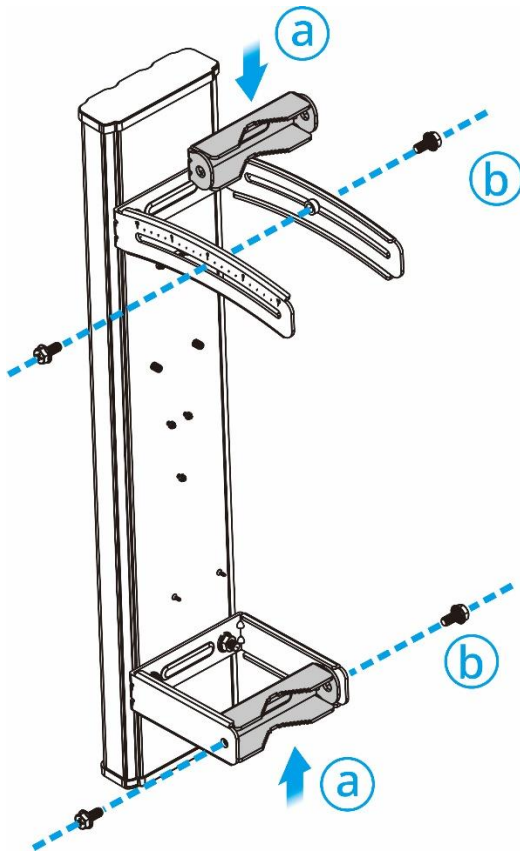
You are advised to use the following three Ruijie antenna models: RG-ANT20S-90, RG-ANT16S-120, and RG-ANT13-360.

- Installing a 90° antenna

(1) Secure the upper and lower brackets to the antenna with four screws, two for each bracket.



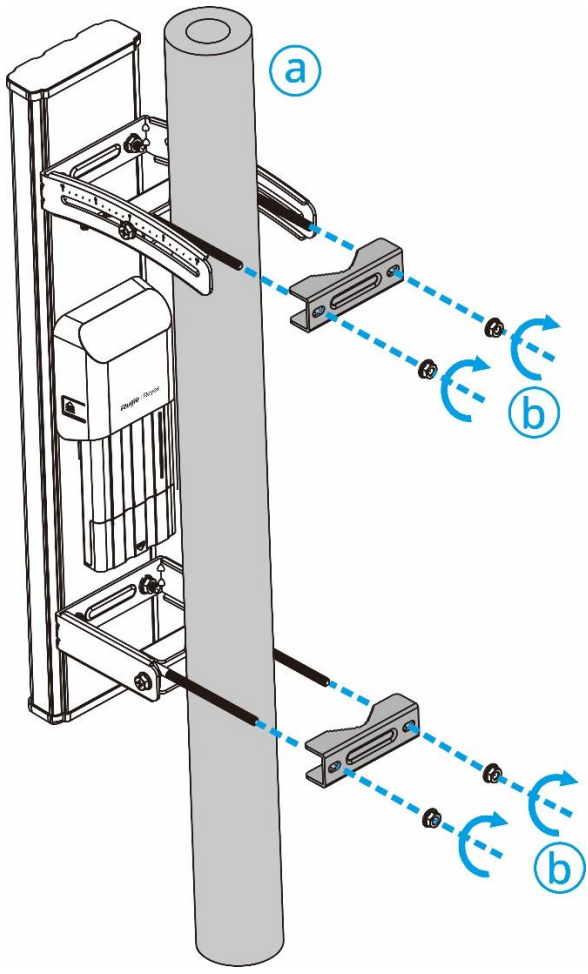
(2) Secure the two fastening pieces to the upper and lower brackets with four screws, two for each.



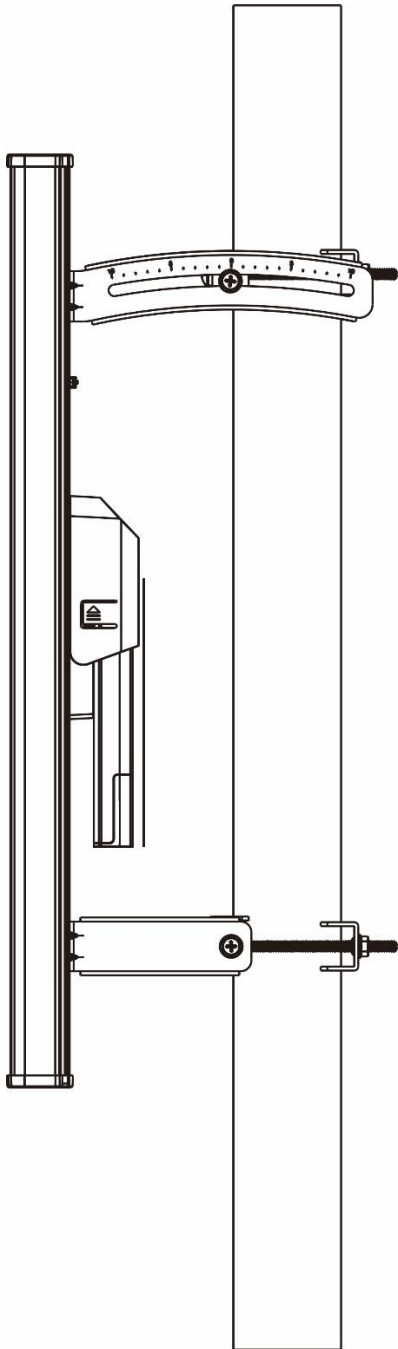
(3) Secure the antenna to the pole.

i Note

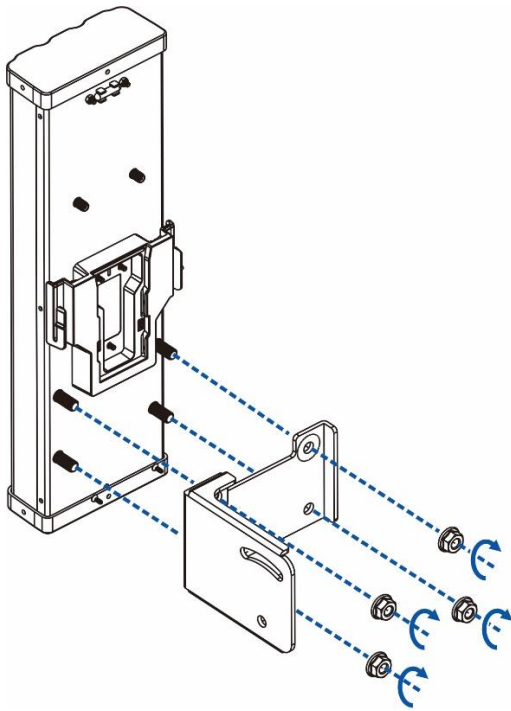
M8 x 150 mm screws are recommended.



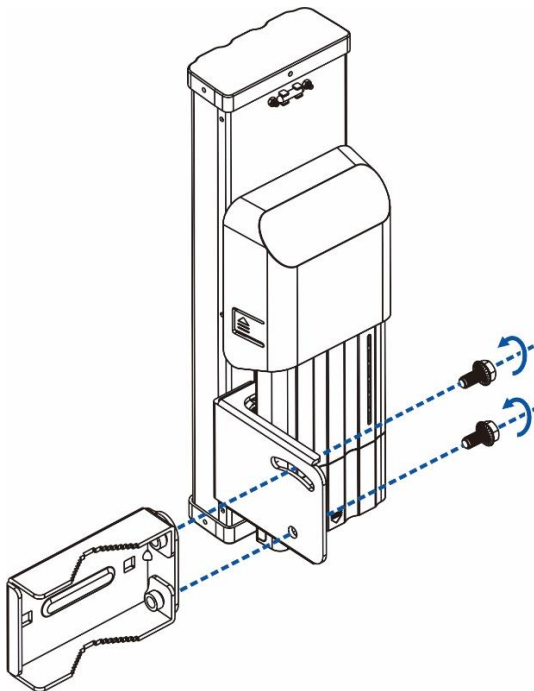
(4) The installation is complete.



- Installing a 120° antenna
- (1) Secure the mounting bracket to the antenna with four screws.



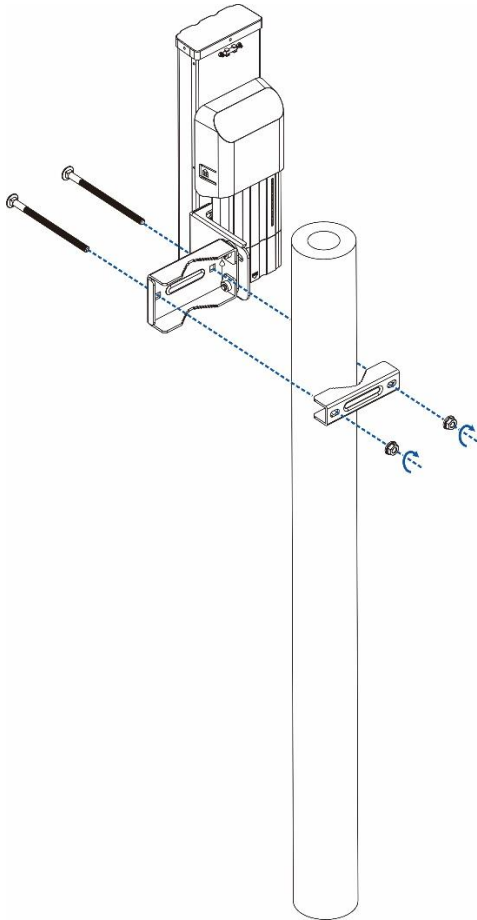
(2) Attach the bracket holder to the bracket with two screws.



(3) Secure the antenna to the pole.

i Note

M8 x 150 mm screws are recommended.

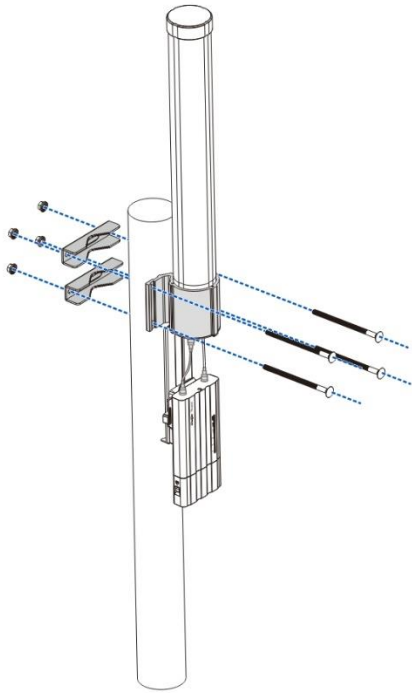


- Installing a 360° antenna

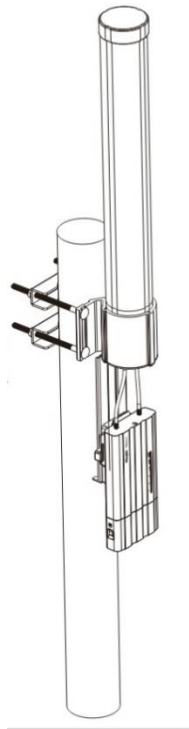
(1) Secure the antenna to the pole.

i Note

M8 x 150 mm screws are recommended.



(2) The installation is complete.



3 Device Management

3.1 Logging In to the Device

- (1) Power on the device.

Plug one end of a cable into a PoE port of the PoE injector and plug the other end into a LAN port of the device; connect the LAN port of the PoE injector to a server or camera; connect the PoE adapter to the DC port of the PoE injector. Or, connect the PoE adapter to a DC port of the device; plug one end of the cable to the LAN port of the device and plug the other end to a server or camera.

- (2) Select the SSID of the device.

The default device management service set identifier (SSID) is **@Ruijie-bXXXX**. XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with devices.

- (3) Enter 10.44.77.254 in the browser to log in to the web page.

3.2 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)

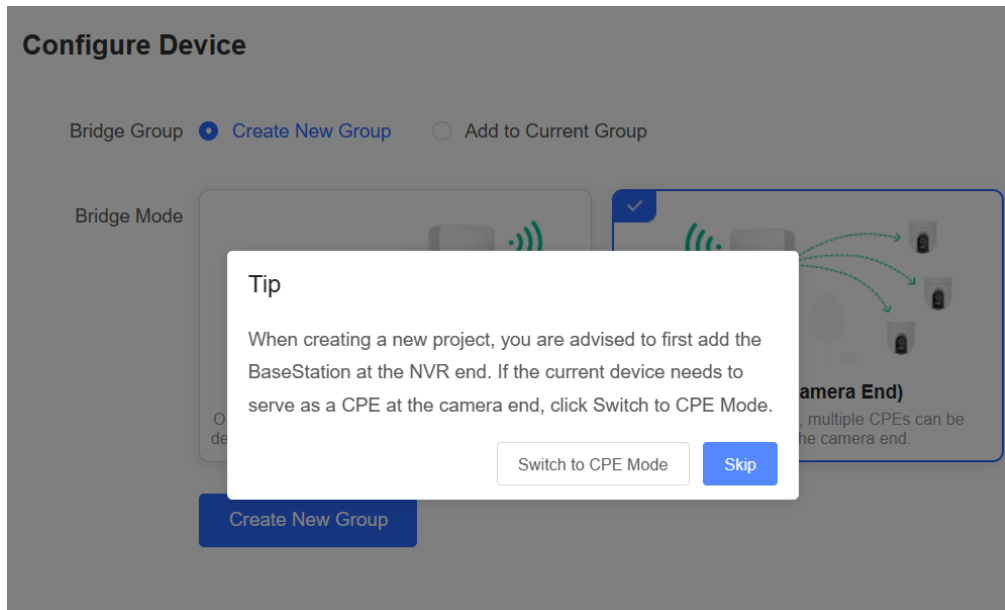
On a bridge network, multiple CPEs can be deployed at the camera end.

* Bridge SSID

* WDS Password Default Password

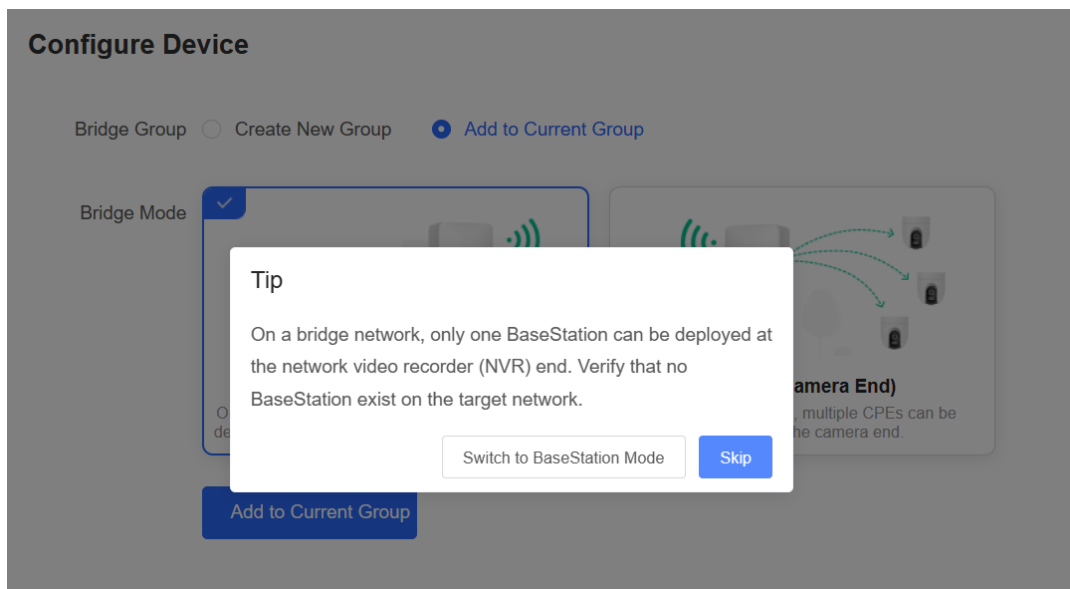
[Create New Group](#)

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



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.



Bridge Network List (4) ×

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

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

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.

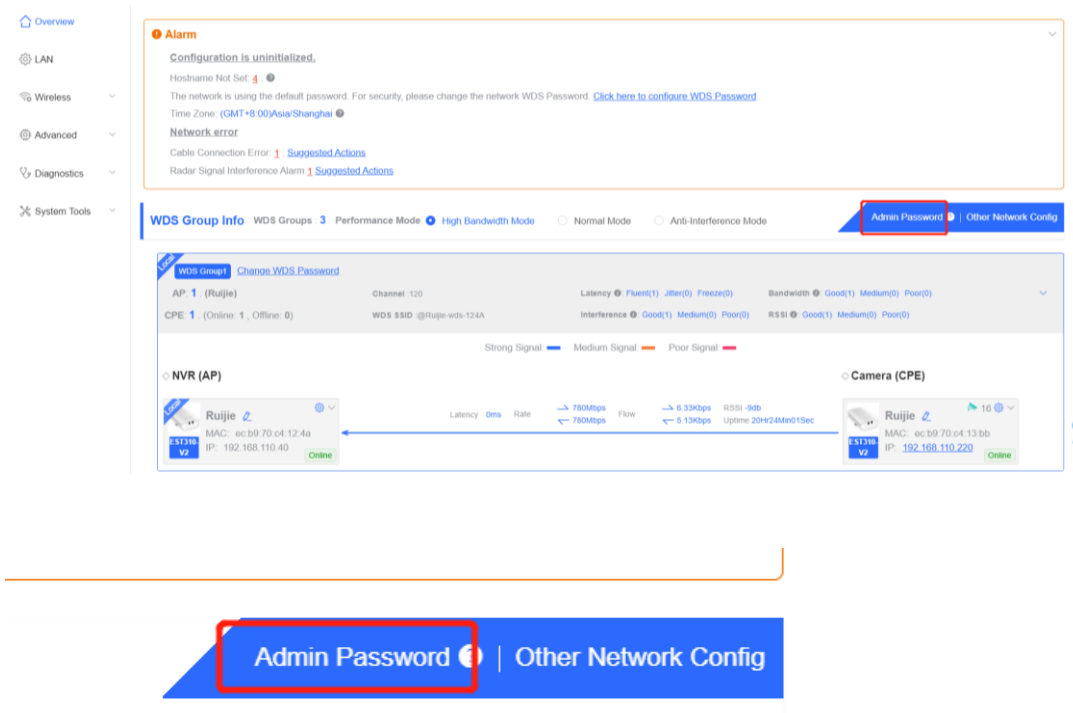


CPE (at Camera End)
On a bridge network, multiple CPEs can be deployed at the camera end.

Add to Current Group

3.3 Configuring Management Password


Choose **Overview > Admin Password**



The screenshot shows the 'Admin Password' configuration page in a network management system. The page includes a navigation sidebar on the left with options like Overview, LAN, Wireless, Advanced, Diagnostics, and System Tools. The main content area displays an 'Alarm' section with messages about uninitialized configuration and network errors. Below this is the 'WDS Group Info' section, which shows details for a WDS group named 'Ruijie' with 3 devices. The 'Admin Password' link is highlighted with a red box. At the bottom of the page, a blue navigation bar contains the 'Admin Password' link, also highlighted with a red box, and the 'Other Network Config' link.

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  to view the help information.

Admin Password

(Change the management passwords of all devices.)



* 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

 **Caution**

This password is used to log in to the 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.

3.4 Setting the System Time

Choose **System Tools > Time**. Set parameters of the system time and click **Save**.

The screenshot shows a web interface for configuring system time. On the left is a navigation menu with items: Overview, LAN, Wireless, Diagnostics, System Tools (expanded), Time (selected), Management, Update, and Reboot. The main content area is titled 'Time' and contains an information banner stating: 'Configure and view time (The device has no RTC module. The time settings will not be saved upon reboot)'. Below this, the 'Current Time' is shown as '2022-04-14 14:41:32' with an 'Edit' button. A 'Time Zone' dropdown menu is set to '(GMT+8:00)Asia/Shanghai'. Under 'NTP Server', there are seven entries, each with a 'Delete' button: '0.cn.pool.ntp.org' (with an 'Add' button), '1.cn.pool.ntp.org', 'cn.pool.ntp.org', 'pool.ntp.org', 'asia.pool.ntp.org', 'europe.pool.ntp.org', and 'rdate.darkorb.net'. A large blue 'Save' button is at the bottom.

Current 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 the time is still incorrect, click **Edit** to manually set the time.

Time Zone: Select the time zone based on your address.

NTP Server: 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.

3.5 Configuring Backup and Import

Choose **System Tools > Management > Backup & Import**.

The screenshot shows the 'Backup & Import' configuration page. The left sidebar contains navigation options: Overview, LAN, Wireless, Diagnostics, System Tools (expanded), Time, Management (selected), Update, and Reboot. The main content area has three tabs: 'Backup & Import' (active), 'Reset', and 'Session Timeout'. Under the active tab, there is an information message: 'If the target version is much later than the current version, some configuration may be missing. It is recommended to choose [Reset](#) before importing the setup. The device will be rebooted automatically later.' Below this, the 'Backup Setup' section includes a 'Backup Setup' label and a blue 'Backup' button. The 'Import Setup' section includes a 'File Path' input field containing 'backup-TestVCR-EST310-20', a blue 'Browse' button, and a blue 'Import' button.

You can import a configuration file to the bridge or export the current configuration of the bridge.

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

3.6 Restoring Factory Settings

Choose **System Tools > Management > Reset**. Click **Reset** to restore factory settings.

The screenshot shows the 'Reset' configuration page. The left sidebar is the same as in the previous screenshot, with 'Management' selected. The main content area has three tabs: 'Backup & Import', 'Reset' (active), and 'Session Timeout'. Under the active tab, there is an information message: 'Resetting the device will clear the current configuration. If you want to keep the configuration, please [Export Setup](#) first.' Below this, there is a large blue 'Reset' button.

3.7 Setting the Session Timeout

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

Choose **System Tools > Management > Session Timeout**. Set the session timeout and click **Save**.

The screenshot shows the configuration page for 'Session Timeout'. On the left is a navigation menu with items: Overview, LAN, Wireless, Diagnostics, System Tools (expanded), Time, Management (selected), Update, and Reboot. The main content area has tabs for 'Backup & Import', 'Reset', and 'Session Timeout'. Below the tabs is a blue header with an information icon and the text 'Session Timeout'. A form field labeled '* Session Timeout' contains the value '3600' and is followed by the unit 'Sec'. A blue 'Save' button is positioned below the form field.

3.8 Upgrade

3.8.1 Online Upgrade

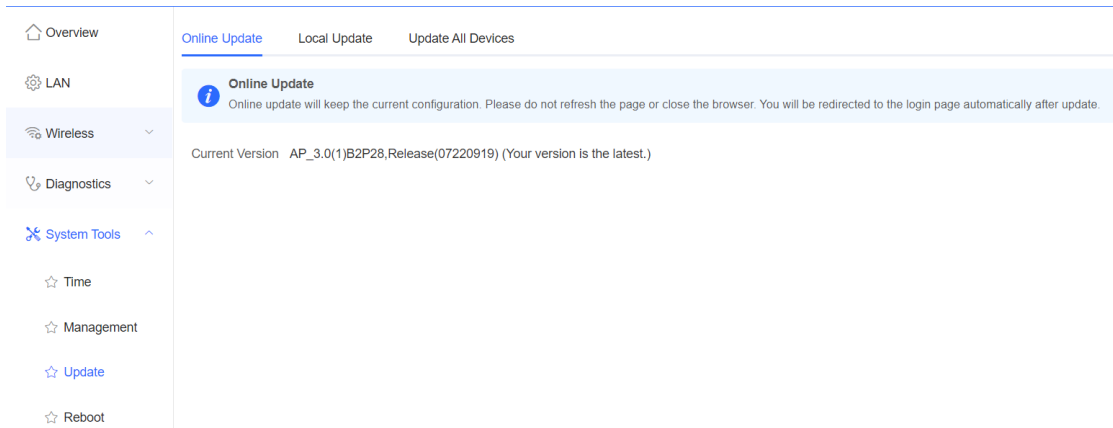
Choose **System Tools > Update > Online Update**.

- If a new version is available, you can click it for an upgrade. The upgrade operation does not affect the current configuration. Do not refresh the page or close the browser during the upgrade. You will be redirected to the login page automatically after the upgrade.

 Note

After being upgraded, the device will restart. Therefore, exercise caution when performing this operation. If no version upgrade is detected or online upgrade cannot be performed, check whether the bridge is connected to the Internet.

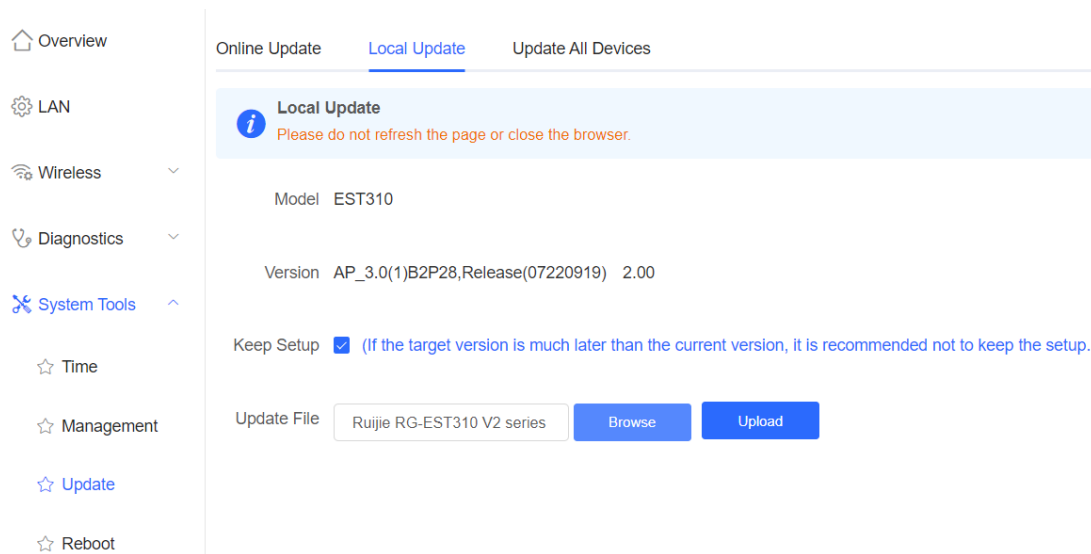
- If there is no new version, the system displays a message indicating that the current version is the latest.



3.8.2 Local Upgrade

Choose **System Tools > Update > Local Update**.

You can view the current software version, hardware version, and device model. To upgrade the device with the configuration retained, check **Keep Setup**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. After the file is uploaded successfully, the pop-up page displays upgrade package information. You can click **OK** to start the upgrade.



3.8.3 Upgrading All Devices

Choose **System Tools > Update > Update All Devices**.

You can view the current software version, hardware version, and device model. You are advised to upgrade all devices with configuration data retained. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. On the pop-up page, click **Details** to check the target upgrade package and devices. Click **Update** to start upgrading all devices.

The screenshot shows the 'Update All Devices' page. On the left is a navigation menu with items: Overview, LAN, Wireless, Diagnostics, System Tools (highlighted), Time, Management, Update, and Reboot. The main content area has three tabs: 'Online Update', 'Local Update', and 'Update All Devices' (which is underlined). Below the tabs is a light blue information box with an 'i' icon and the text: 'Update All Devices' followed by 'Update all devices in the network. Please do not refresh the page or close the browser.' Below this, the device model is listed as 'EST310' and the version as 'AP_3.0(1)B2P28,Release(07220919) 2.00'. There is a 'Keep Setup' checkbox which is checked and labeled '(Uneditable)'. At the bottom, there is an 'Update File' section with a text input containing 'Ruijie RG-EST310 V2 series', a 'Browse' button, and an 'Upload' button.

3.9 Restart

Choose **System Tools** > **Reboot** and click **Reboot** to restart the local device. Keep the device powered on during restart.

The screenshot shows the 'Reboot' page. The left navigation menu is the same as in the previous screenshot, but 'Reboot' is now highlighted. The main content area features a light blue information box with an 'i' icon and the text: 'Reboot' followed by 'Please keep the device powered on during reboot.' Below this information box is a large blue button labeled 'Reboot'.

3.10 Configuring SNMP

Note

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

3.10.1 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.

3.10.2 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.

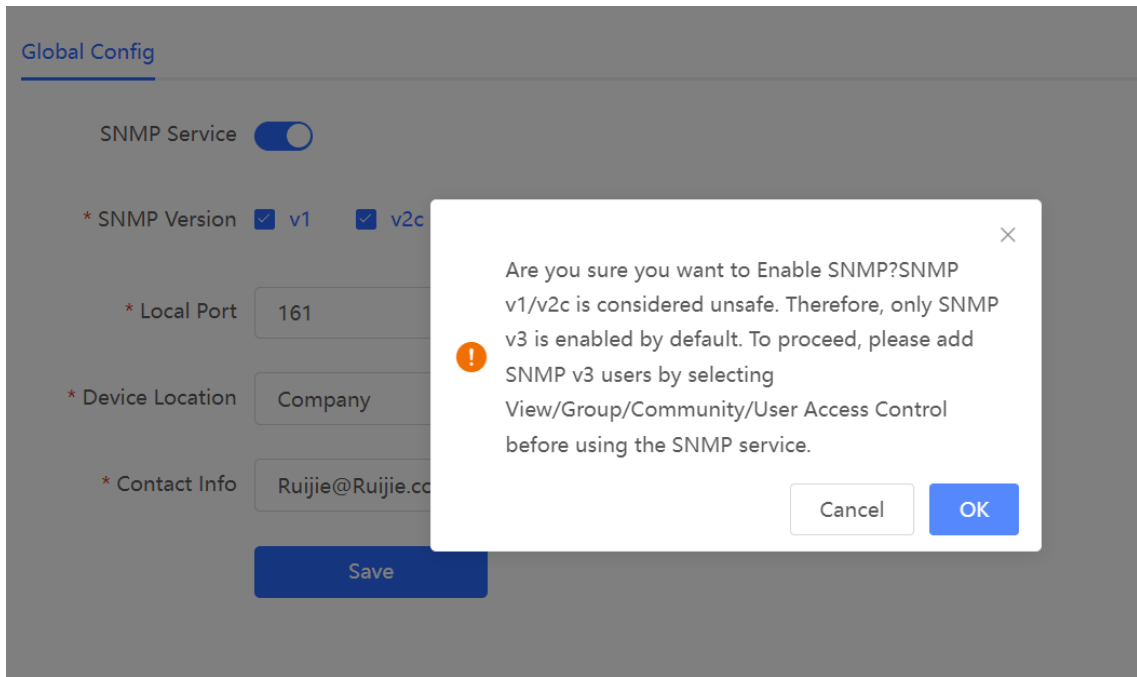
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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.



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

(2) Set SNMP service global configuration parameters.

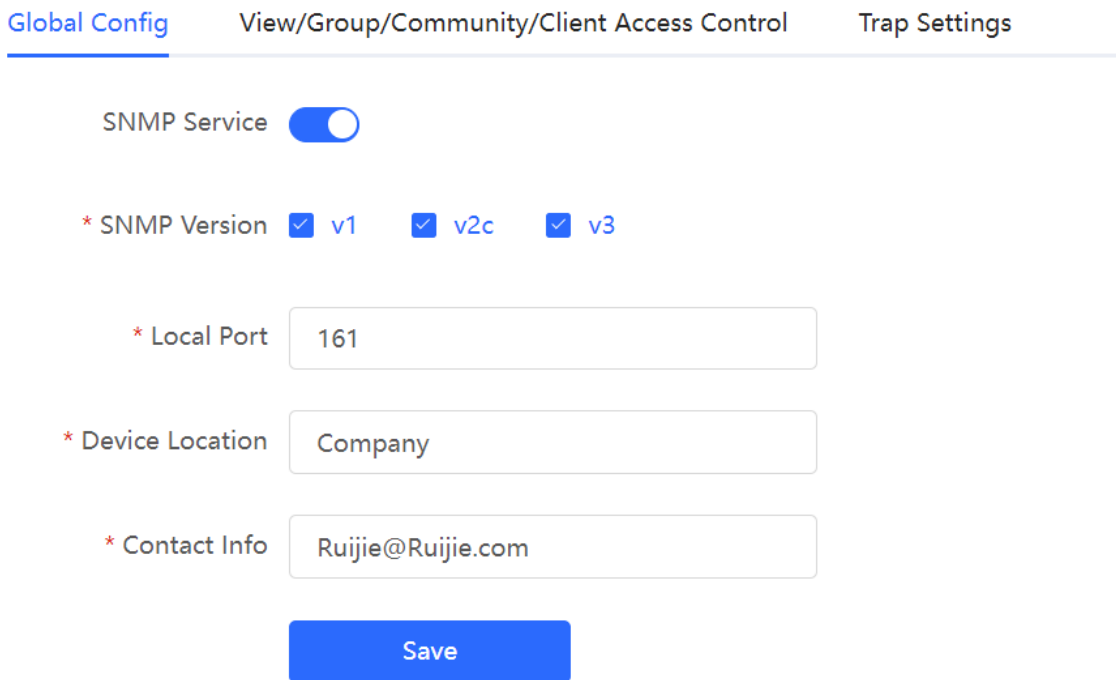


Table 3-1 Global Configuration Parameters

Parameter	Description
SNMP Server	Indicates whether SNMP service is enabled.

Parameter	Description
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.

3.10.3 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.

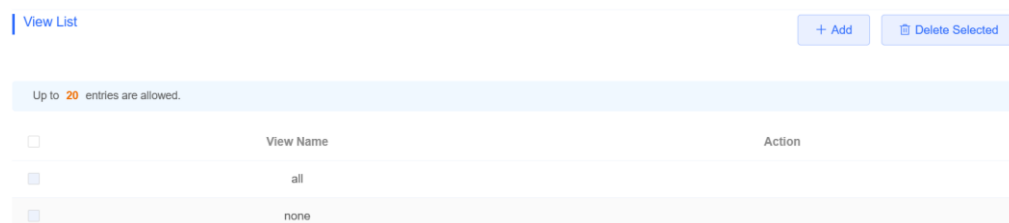
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

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

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



(2) Configure basic information of a view.

Add
×

* View Name

OID

Add Included Rule
Add Excluded Rule

Rule/OID List Delete Selected

Up to **100** entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
No Data			

Total 0 10/page < 1 > Go to 1

Cancel
OK

Table 3-2 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.
Type	There are two types of rules: included and excluded rules. 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 Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

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

Up to 20 entries are allowed.

<input type="checkbox"/>	Community Name	Access Mode	MIB View	Action
<input type="checkbox"/>	Tttttt8	Read & Write	all	Edit Delete
<input type="checkbox"/>	hello_12121	Read & Write	all	Edit Delete

(2) Add a v1/v2c user.

Add
×

* Community Name

* Access Mode

* MIB View [Add View +](#)

Table 3-3 v1/v2c User Configuration Parameters

Parameter	Description
Community Name	<p>At least 8 characters.</p> <p>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.</p> <p>Question marks, spaces, and Chinese characters are not allowed.</p>
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 Service * SNMP Version v1 v2c v3* Local Port * Device Location * Contact Info **i** 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	Delete Selected
Up to 20 entries are allowed.								
<input type="checkbox"/>	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action		
<input type="checkbox"/>	default_group	Auth & Security	all	none	none	Edit Delete		

(2) Configure v3 group parameters.

Add
×

* Group Name

* Security Level Allowlist & Security ▼

* Read-Only View all ▼ [Add View +](#)

* Read & Write View all ▼ [Add View +](#)

* Notification View none ▼ [Add View +](#)

Cancel OK

Table 3-4 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).
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 Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Save

i 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 Client List** pane to add a v3 user.

SNMP v3 Client List + Add Delete Selected

Up to 50 entries are allowed.

<input type="checkbox"/>	Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
No Data								

(2) Configure v3 user parameters.

Add
×

* Username

* Group Name ▾

* Security Level ▾

* Auth Protocol ▾ * Auth Password

* Encryption Protocol ▾ * Encrypted Password

Table 3-5 v3 User Configuration Parameters

Parameter	Description
Username	Username 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.
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.
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.

Parameter	Description
Encryption Protocol, Encryption Password	<p>Encryption protocols supported: DES/AES/AES192/AES256.</p> <p>Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption.</p>

 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.

3.10.4 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:

Table 3-6 User Requirement Specification

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.
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 Service * SNMP Version v1 v2c v3

* Local Port

161

* Device Location

Company

* Contact 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

OID

Add Included Rule
Add Excluded Rule

Rule/OID List

🗑️ Delete Selected

Up to **100** entries are allowed.

	Rule	OID	Action
<input type="checkbox"/>	Included	.1.3.6.1.2.1.1	Delete

Total 1

10/page

<
1
>

Go to page

1

Cancel

OK

- (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

* Access Mode

* MIB View 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:

Table 3-7 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.
Configuring v3 Users	User name: v3_user Group name: group 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.

- 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 Service * SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

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

Add

×

* View Name

OID

Rule/OID List

Up to **100** entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
<input type="checkbox"/>	Included	.1.3.2.6.1.2.1	Delete

Total 1 < **1** > Go to page

- (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**.

Add



* Group Name	<input type="text" value="group"/>
* Security Level	<input type="text" value="Allowlist & Security"/>
* Read-Only View	<input type="text" value="public_view"/> Add View +
* Read & Write View	<input type="text" value="public_view"/> Add View +
* Notification View	<input type="text" value="none"/> Add View +

Cancel

OK

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

- Click **Add** in the **SNMP v3 Client List** pane.
- 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.
- Click **OK**.

Add



* Username	<input type="text" value="v3_user1"/>		
* Group Name	<input type="text" value="group"/>		
* Security Level	<input type="text" value="Auth & Security"/>		
* Auth Protocol	<input type="text" value="MD5"/>	* Auth Password	<input type="text" value="Ruijie123"/>
* Encryption Protocol	<input type="text" value="AES"/>	* Encrypted Password	<input type="text" value="Ruijie123"/>

Cancel

OK

3.10.5 Configuring Trap Service

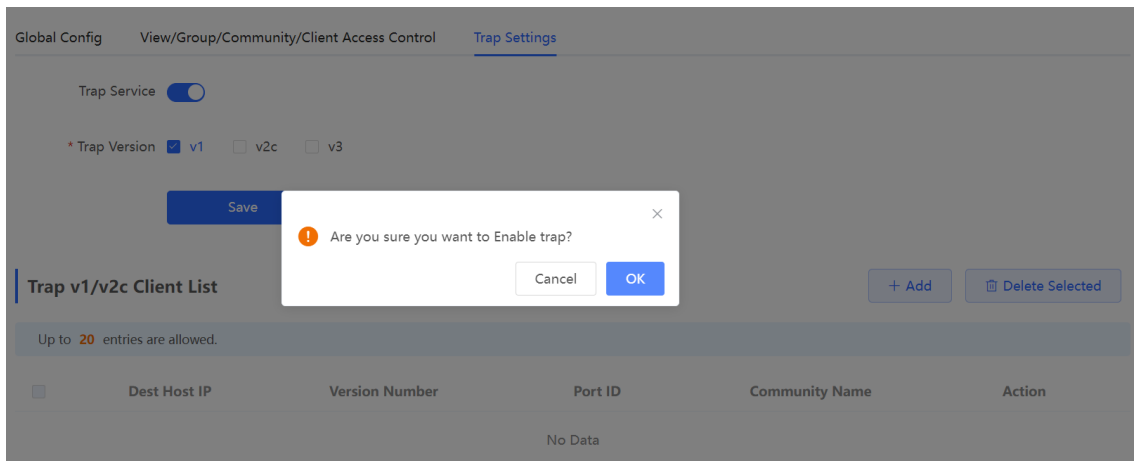
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring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

1. Enabling Trap Service

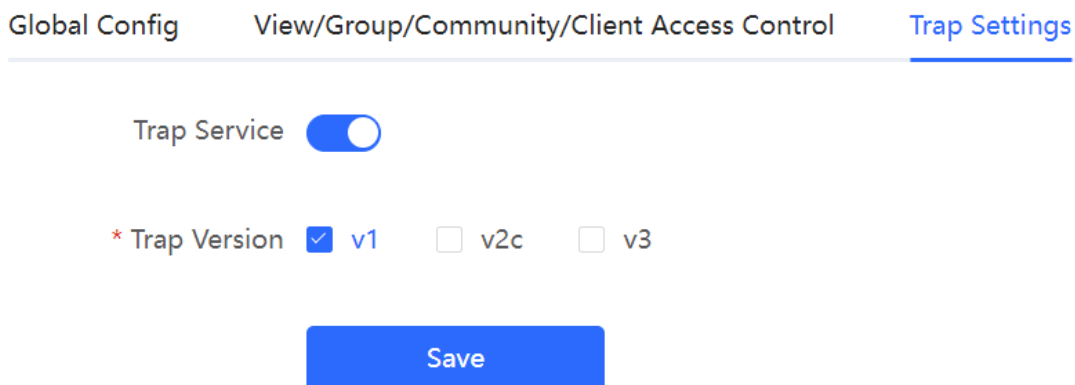
Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

System > SNMP > Trap Setting

(1) Enable the trap service.



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



(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.

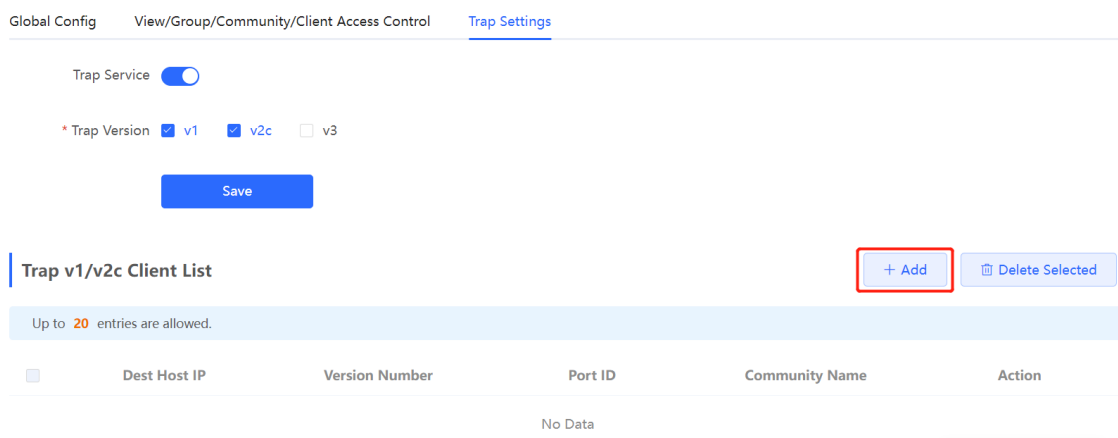
- Prerequisites

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

- Procedure

System > SNMP > Trap Setting

(1) Click **Add** in the **Trap v1/v2c Client List** pane to add a trap v1/v2c user.



(2) Configure trap v1/v2c user parameters.

Add
×

* Dest Host IP

* Version Number

* Port ID

* Community

Name/Username

Table 3-8 Trap v1/v2c User Configuration Parameters

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/User name	Community name of the trap user. 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.

 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

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

Global Config View/Group/Community/Client Access Control Trap Settings

Trap Service

* Trap Version v1 v2c v3

Trap v3 Client List

Up to 20 entries are allowed.

<input type="checkbox"/>	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
No Data							

(2) Configure trap v3 user parameters.

Add ×

* Dest Host IP	<input type="text" value="Support IPv4/IPv6"/>	* Port ID	<input type="text"/>
* Username	<input type="text"/>	* Security Level	<input type="text" value="Auth & Security"/>
* Auth Protocol	<input type="text" value="MD5"/>	* Auth Password	<input type="text"/>
* Encryption Protocol	<input type="text" value="AES"/>	* Encrypted Password	<input type="text"/>

Table 3-9 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.
Username	Name of the trap v3 user. 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.

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.

 Note

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

3.10.6 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 third-party 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:

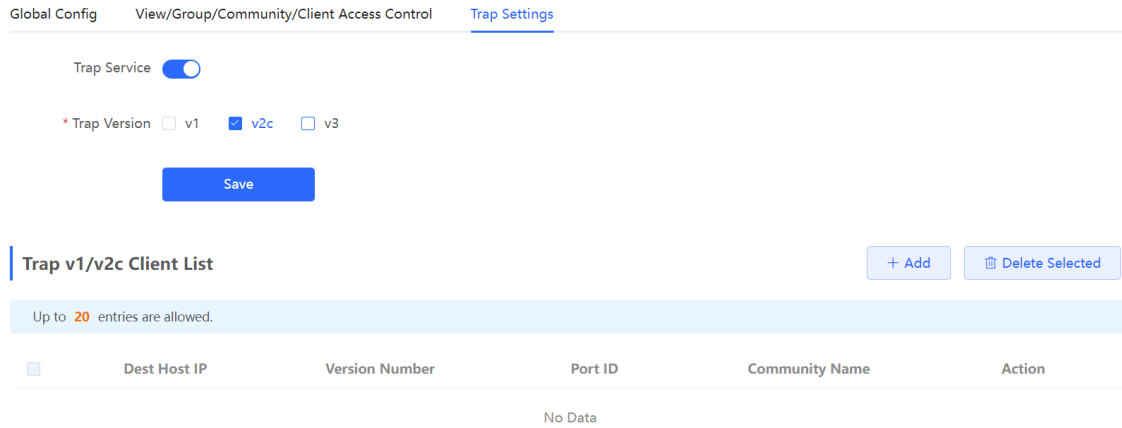
Table 3-10 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port 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**.



(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**.

Add
×

* Dest Host IP

* Version Number

* Port ID

* Community Name/Username

2. Configuring Trap v3

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party 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:

Table 3-11 User Requirement Specification

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	Authentication protocol/password: MD5/Ruijie123
Encryption protocol/encryption password	Encryption protocol/password: AES/Ruijie123

- Configuration Steps

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

The screenshot shows the 'Trap Settings' interface. At the top, there are navigation links: 'Global Config', 'View/Group/Community/Client Access Control', and 'Trap Settings'. Below this, the 'Trap Service' is toggled on. Under '* Trap Version', the 'v3' option is selected with a checked radio button. A blue 'Save' button is visible below the version selection. Below the settings, there is a section titled 'Trap v3 Client List' with '+ Add' and 'Delete Selected' buttons. A message states 'Up to 20 entries are allowed.' Below this is a table with columns: Dest Host IP, Port ID, Username, Security Level, Auth Password, Encrypted Password, and Action. The table currently contains no data. At the bottom, there is a pagination control showing 'Total 0', '10/page', and 'Go to page 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**.

Add

×

* Dest Host IP	<input type="text" value="Support IPv4"/>	* Port ID	<input type="text"/>
* Username	<input type="text"/>	* Security Level	<input type="text" value="Auth & Security"/>
* Auth Protocol	<input type="text" value="MD5"/>	* Auth Password	<input type="text"/>
* Encryption Protocol	<input type="text" value="AES"/>	* Encrypted Password	<input type="text"/>

Cancel

OK

4 Wi-Fi Network Settings

4.1 Overview

4.1.1 NVR and Camera

Bridges purchased in pairs in the same package can be paired automatically with each other after power-on. You can also manually pair the devices by setting up a WDS network. See [Setting WDS Wi-Fi for a Single NVR or Camera](#). In a paired WDS group, bridges can work in access point (AP) or Customer Premises Equipment (CPE) mode.

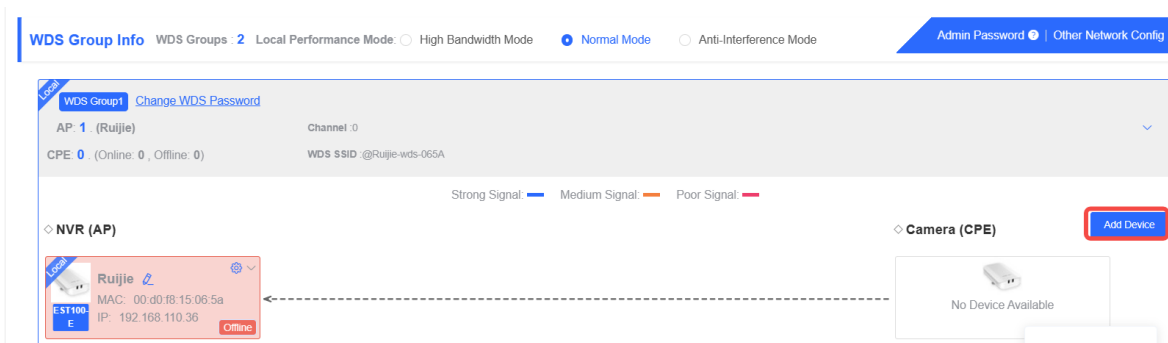
- **NVR end (AP):** A bridge sending bridging signals is generally connected to the NVR end in a surveillance room. A WDS group can contain at most one AP.
- **Camera end (CPE):** A bridge that enables customers to access ISP's communication services is generally connected to the camera end. A WDS group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

4.1.2 WDS Wi-Fi and Management Wi-Fi

- **WDS Wi-Fi:** An AP broadcasts the WDS Wi-Fi signal. A CPE accesses the WDS Wi-Fi and upload videos or other data to the AP.
- **Management Wi-Fi:** Both an AP 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.

4.2 Scanning and Pairing the Camera (CPE)

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



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 Devices (1) ×

<input type="checkbox"/>	Model	SN	RSSI	Device Info	WDS Password
<input checked="" type="checkbox"/>	YST250F	ZASL42D00 0720	Good	default/Ruijie	Default Password

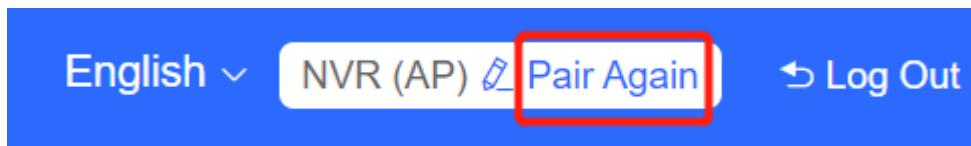
Tips

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.

4.3 Switching NVR and Camera Mode

If an NVR fails, replace it and switch the new device to NVR (AP). 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 ×

! 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.

Start

(3) Click **Next**.

Country/Region ×

The country/region you select here must be the same as the country/region of the WDS network.

Country/Region:

Previous

Next

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

Mode Switchover ×

Work Mode:

Previous

- NVR (AP)
- Camera (CPE)**

Next

(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.

* WDS SSID:

WDS Password Default Password

WDS SSID List (Click to select a SSID.)

Search by SSID

WDS SSID	RSSI	SN
@Ruijie-wds-0746	-56	ZASL42D000720
@Ruijie-wds-0109	-68	MACC942570009

Strong Signal: ■ Medium Signal: ■

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

Setup

Work Mode: [Switch AP to AP](#)

WDS SSID: @Ruijie-wds-0746

WDS Password: Default Password

Password:

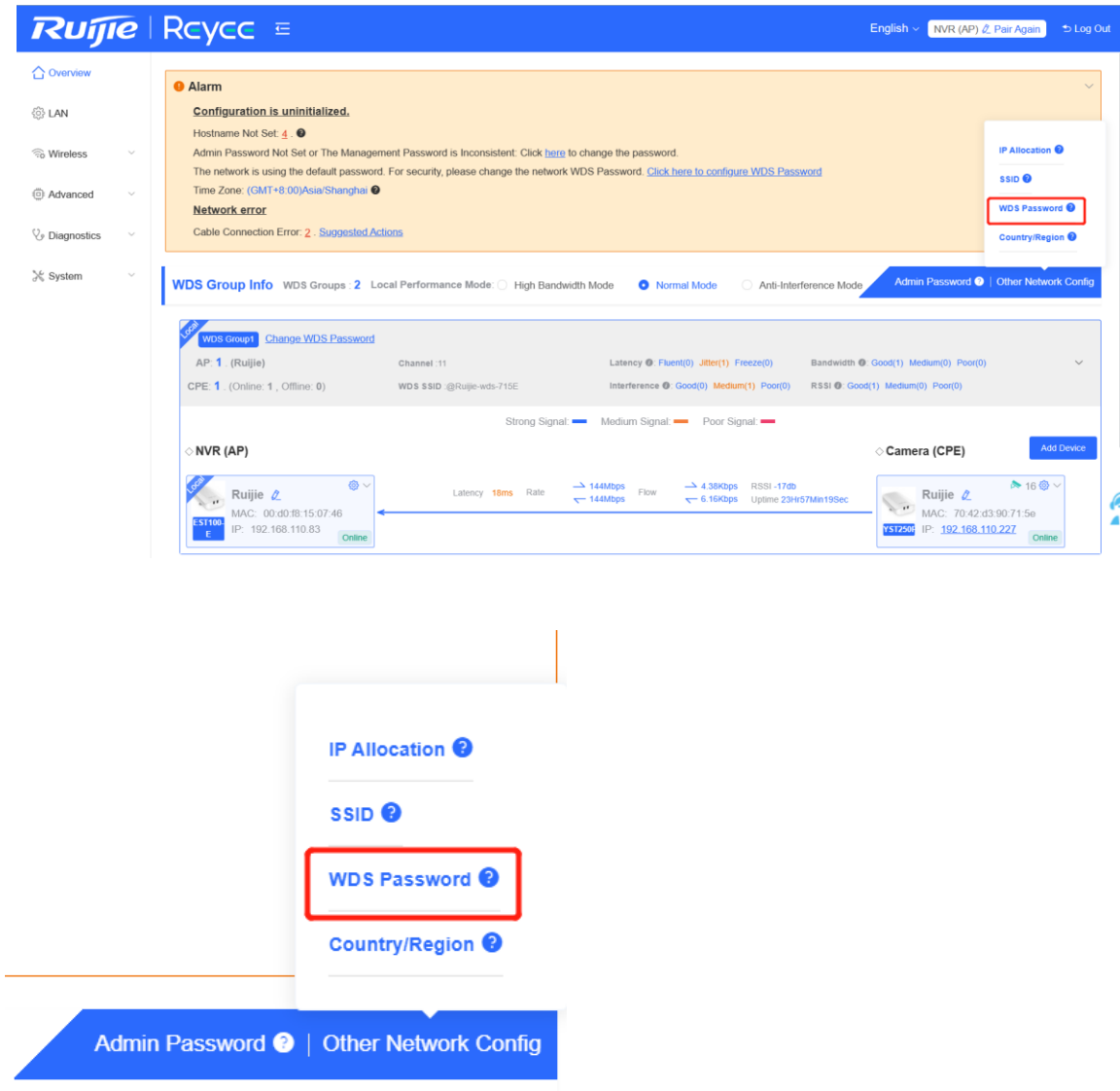
Country/Region: China

⚠ Caution


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

4.4 Configuring the WDS Password for All Bridges in the LAN

Choose: **Overview > Other Network Config > WDS Password**



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

Hover the cursor over  to view the help information.

✕

WDS Password
(Change the bridge passwords of the devices in all bridge groups.)

* 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

Caution

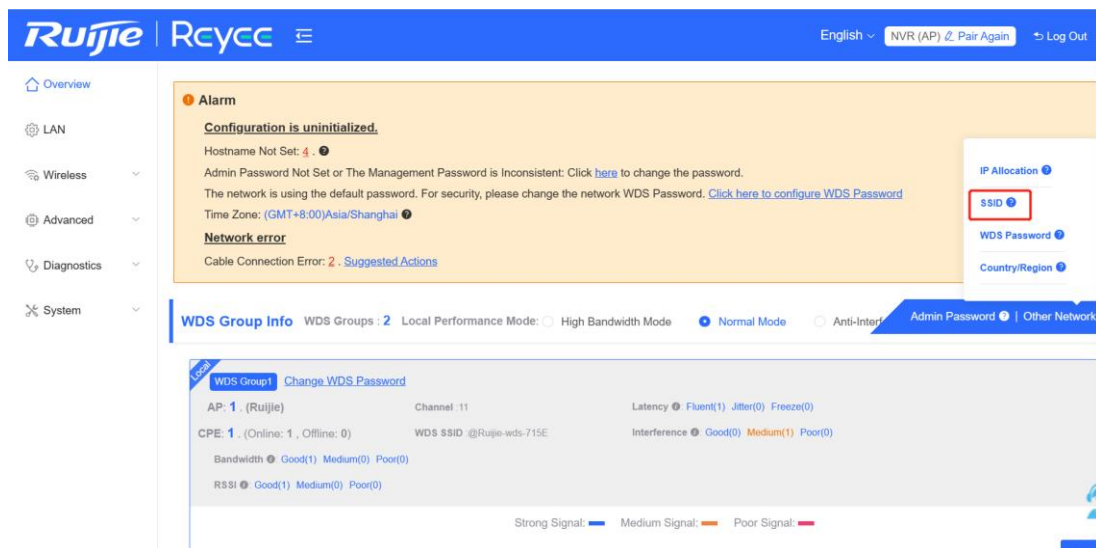
When configuring the WDS password for the entire network, ensure that all devices in the network are online. Otherwise, the WDS passwords of the devices will be inconsistent.

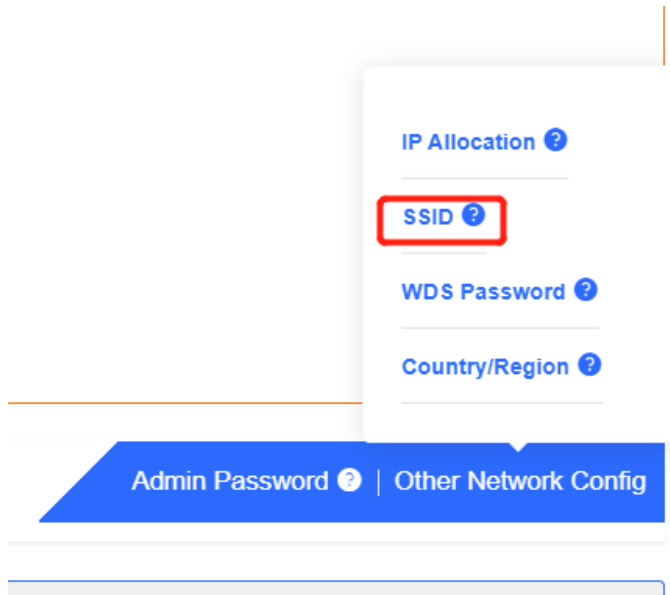
Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation.

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

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

Choose: **Overview > Other Network Config > SSID**





i 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-bXXXX**. (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.

SSID Settings



(Edit all management SSIDs broadcast by all devices to the same management SSID.)

Enable WiFi

* SSID:

Security:

* 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.

Hide SSID: (The SSID must be manually entered exactly.)

Save

 **Caution**

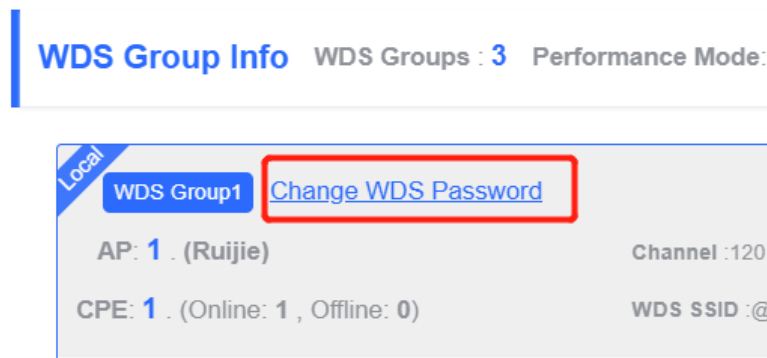
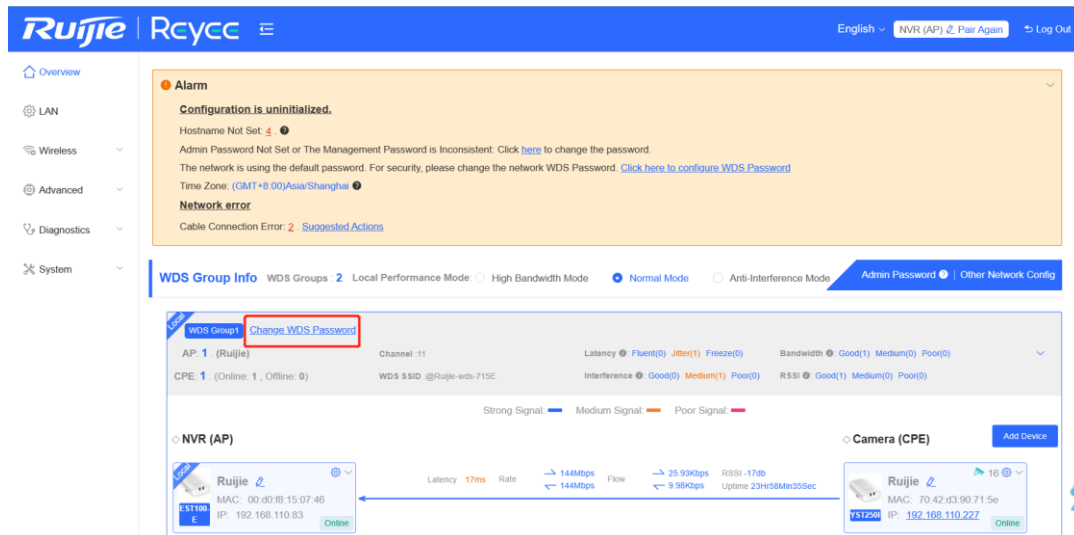
After the configuration is saved, NVRs and cameras in the network will be reconnected. Therefore, exercise caution when performing this operation.

4.6 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.



⚠ 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.

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

4.7.1 Setting the WDS SSID

Choose **Wireless > 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 [Displaying WDS Group Information](#).

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

WDS Password Default Password

.....

Save

4.7.2 Configuring the WDS Password

Choose **Wireless > 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

WDS Password Default Password



Save

Caution

- WDS passwords can be configured only for cameras, and not for NVRs.
- 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.

4.7.3 Saving the Settings

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

4.8 Optimizing Wireless Network

4.8.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. 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.

4.8.2 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.

Channel	36	40	44	48	52	56	60	64	149	153	157	161
RFI Count	56	31	12	5	0	2	0	2	0	0	1	0

4.8.3 Configuration Steps

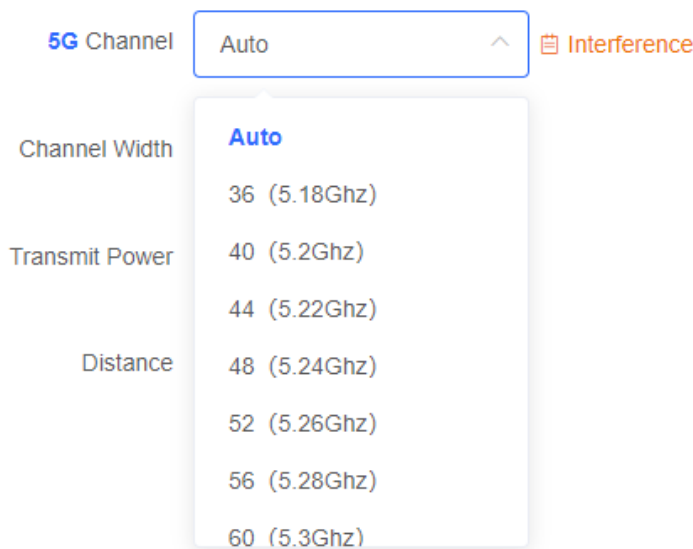
1. Optimizing the Radio Channel

(1) Channel settings

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

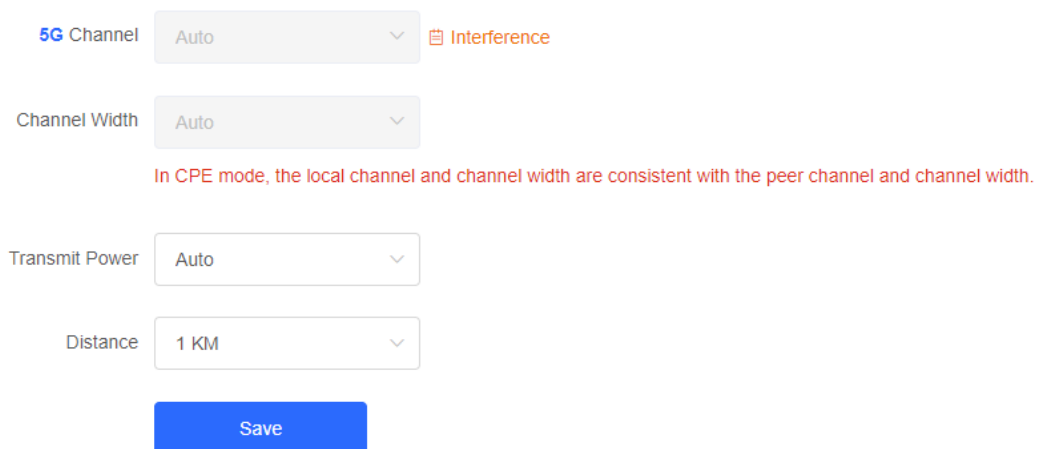
The default channel is **Auto**, indicating automatic channel adaption based on the surrounding environment upon power-on. Choose the optimal channel identified through the above analysis. Click **Save** to activate settings immediately. Excess STAs connected to a channel can bring stronger wireless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

Channel & Transmit Power



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 & Transmit Power



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.

The image shows a blue button with the text "Optimize WDS" in white. To the left of the button is a vertical blue line, and the text "Optimize WDS" is written in blue above the button.

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.

Caution

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

Channel & Transmit Power

5G Channel Interference

Channel Width

Transmit Power

Distance

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 & Transmit Power

5G Channel Interference

Channel Width

Transmit Power

Distance

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.

Channel & Transmit Power

5G Channel Interference

Channel Width

Transmit Power

Distance

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

4.9 Changing the Country/Region Code

4.9.1 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.

The screenshot displays the WDS configuration page for a Ruijie network. At the top, it shows 'WDS Group 1' and 'Change WDS Password'. Below this, there are several status indicators: AP: 1 (Ruijie), Channel: 11, Latency: Fluent(1) Jitter(0) Freeze(0), Bandwidth: Good(1) Medium(0) Poor(0), CPE: 1 (Online: 1, Offline: 0), WDS SSID: @Ruijie-wds-715E, Interference: Good(0) Medium(1) Poor(0), and RSSI: Good(1) Medium(0) Poor(0). A legend indicates signal strength: Strong Signal (blue), Medium Signal (orange), and Poor Signal (red). The main area shows two connected devices: an NVR (AP) and a Camera (CPE). The NVR (AP) is a Ruijie device with MAC address 00:d0:f8:15:07:46 and IP address 192.168.110.83, marked as 'Online'. The Camera (CPE) is also a Ruijie device with MAC address 70:42:d3:90:71:5e and IP address 192.168.110.227, also marked as 'Online'. Between the two devices, performance metrics are shown: Latency 10ms, Rate 144Mbps, Flow 26.24Kbps, RSSI -16db, and Uptime 23Hr59Min19Sec. An 'Add Device' button is visible next to the Camera (CPE) section.

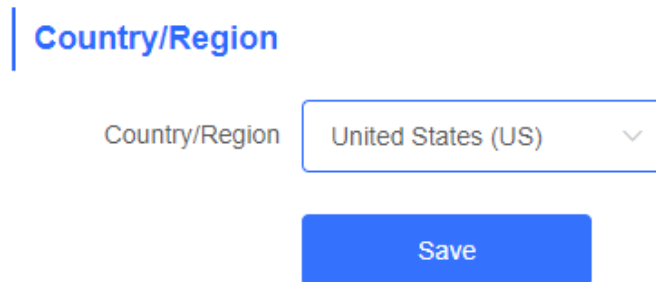
⚠ Caution

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

4.9.2 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.

4.10 Configuring Antenna Alignment

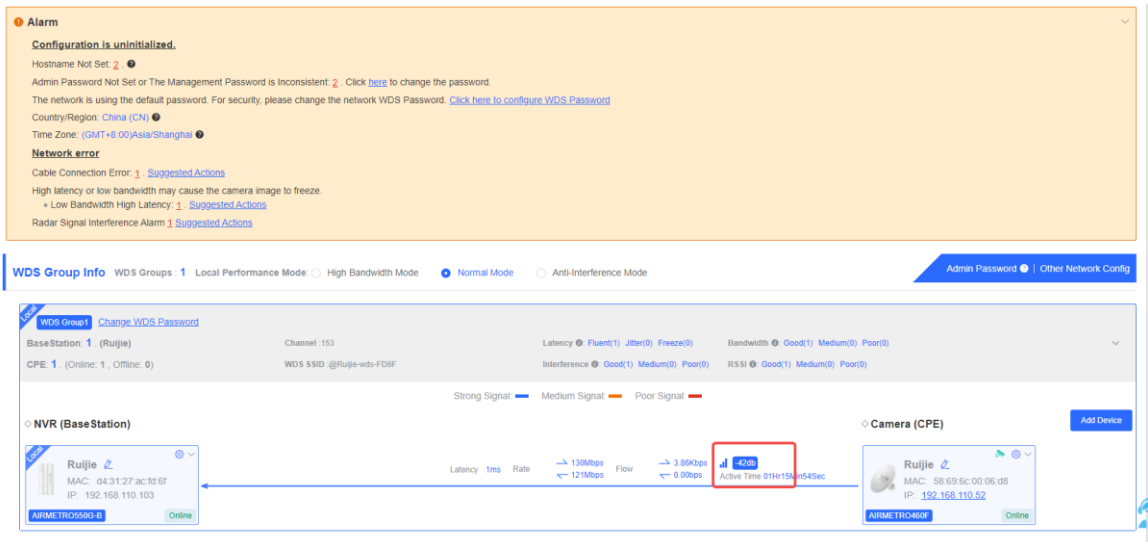
i Note

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.



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.




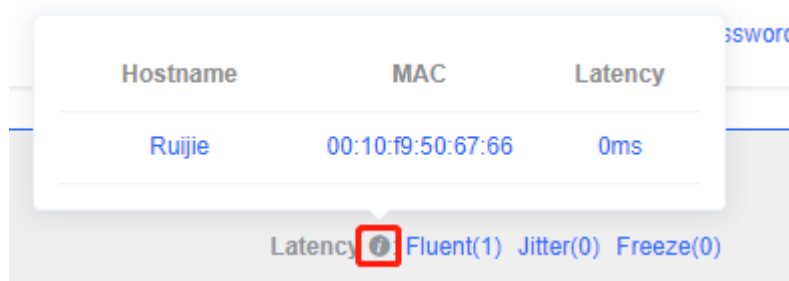
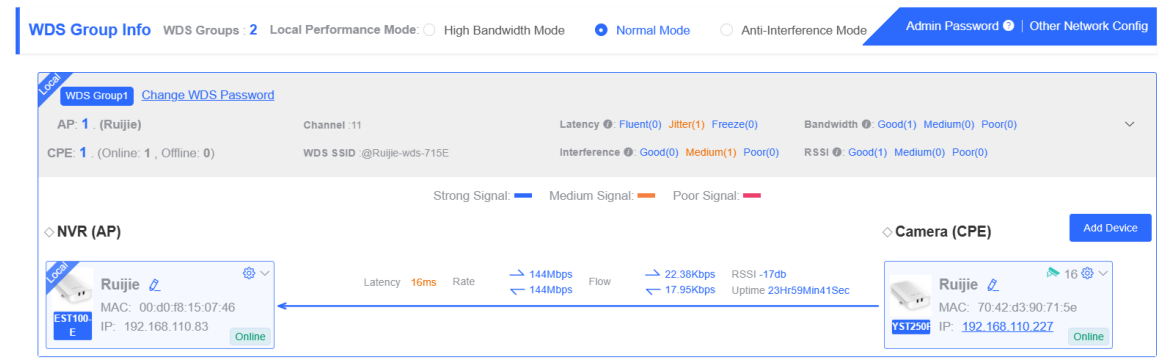
Note

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

4.11 Displaying WDS Group Information

Choose **Overview > WDS Group Info**.

Displayed WDS group information includes the number of APs 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.




Note

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

4.12 Displaying the Information About a Single Device

- Choose **Overview > WDS Group Info > NVR (AP)/Camera (CPE)**.



Click the  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.

The screenshot shows the Ruijie Rcycc dashboard. On the left is a navigation menu with categories: Overview, LAN, Wireless, Advanced, Diagnostics, and System. The main content area features an orange alarm banner with the message "Configuration is uninitialized." and details about hostname, password, and time zone. Below this is the "WDS Group Info" section, which includes a "WDS Group 1" summary with AP and CPE counts, and a table of NVR (AP) devices. One device is listed as "Ruijie" with MAC 00:d0:f8:15:07:46 and IP 192.168.110.83, marked as "Online".

This panel provides detailed settings for a selected device (Group 1 / AP / Ruijie). It is divided into three sections: "SYS" (System), "LAN", and "Wi-Fi". The "SYS" section includes fields for Hostname, Uptime, Net Status, Model, SN, Software Ver, Hardware Ver, and MAC, along with a QR code. The "LAN" section shows IP Address, Subnet Mask, and LAN port status (LAN0 and LAN1). The "Wi-Fi" section displays Noise Floor/Utilization, Distance, Channel, Transmit Power, Channel Width, RSSI, and Band.

This panel provides detailed settings for a selected device (Group 1 / AP / Ruijie). It is divided into three sections: "SYS" (System), "LAN", and "Wi-Fi". The "SYS" section includes fields for Hostname, Uptime, Net Status, Model, SN, Software Ver, Hardware Ver, and MAC, along with a QR code. The "LAN" section shows IP Address, Subnet Mask, and LAN port status (LAN0 and LAN1). The "Wi-Fi" section displays Noise Floor/Utilization, Distance, Channel, Transmit Power, Channel Width, RSSI, and Band.

Note

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

4.13 Configuring TDMA Mode

Note

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

4.13.1 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.

4.13.2 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.

TDMA--NVR (BaseStation)
Select the TDMA-based time slot allocation mode.

TDMA

TDMA

Mode ? Flexible Fix

Advanced ▾

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.

Save

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.

TDMA--NVR (Base Station)
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

Advanced >

Save

TDD Ratio

1:1

The time slot of downlink and uplink base on 1:1

- 1:1
- 1:2
- 1:3
- 2:1
- 3:1

ed >

TDD Time Slot

5ms

>

- 5ms
- 8ms
- 10ms

3. Expert mode

TDMA

TDMA

Advanced ▾

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 ms

Cpe/Ruijie
1234567891234 ms

[Save](#)

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.

4.14 Configuring One-Touch Pairing

Note

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

4.14.1 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.

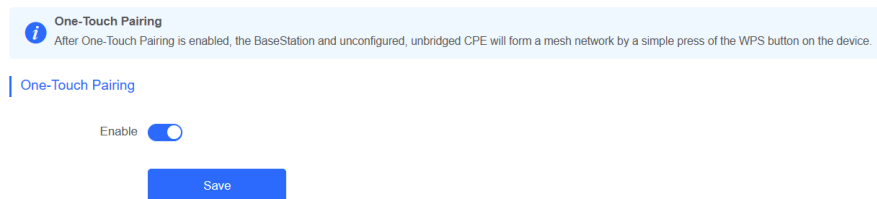
The One-Touch Pairing feature is designed to simplify the process of setting up a network bridge for users who have purchased a wireless bridge that supports this feature. By pressing a physical button on the wireless bridge, the wireless bridge will automatically search for and connect with a factory-configured 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.

4.14.2 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.

5 Network Settings

5.1 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.


5.1.1 Allocating IP Addresses to All Bridges in the Network

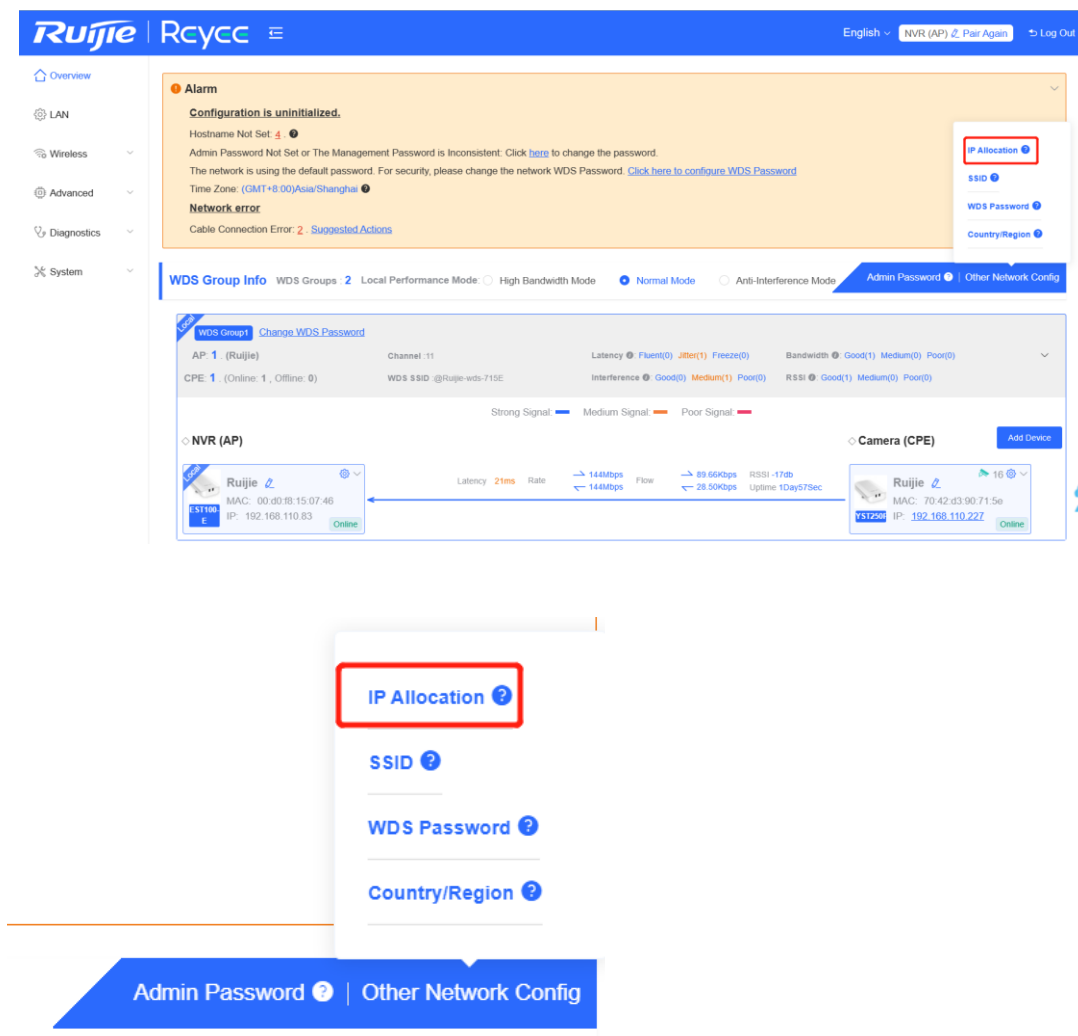
- Static IP address

Choose: **Overview > Other Network Config > IP Allocation**

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  to view the help information.



The screenshot shows the Ruijie Rcycc web interface. The top navigation bar includes the Ruijie logo, Rcycc, and a menu icon. The main content area is divided into several sections:

- Alarm:** Configuration is uninitialized. Hostname Not Set. Admin Password Not Set or The Management Password is Inconsistent. The network is using the default password. Time Zone: (GMT+8:00)Asia/Shanghai. Network error: Cable Connection Error.
- WDS Group Info:** WDS Groups: 2. Local Performance Mode: High Bandwidth Mode, Normal Mode, Anti-interference Mode. Admin Password, Other Network Config.
- WDS Group 1:** Change WDS Password. AP: 1 (Ruijie). Channel: 11. Latency: Fluent(0), Jitter(1), Freeze(0). Bandwidth: Good(1), Medium(0), Poor(0). CPE: 1 (Online: 1, Offline: 0). WDS SSID: @Ruijie-wds-715E. Interference: Good(0), Medium(1), Poor(0). RSSI: Good(1), Medium(0), Poor(0).
- NVR (AP):** Ruijie 2. MAC: 00:d3:18:15:07:46. IP: 192.168.110.83. Online.
- Camera (CPE):** Ruijie 2. MAC: 70:42:d3:90:71:5e. IP: 192.168.110.227. Online.

A red box highlights the **IP Allocation** link in the top right corner of the main content area. A blue callout box at the bottom of the page lists navigation options: **Admin Password** and **Other Network Config**.

IP Allocation

ⓘ Assign static IP addresses to conflicting devices.

Internet

* Start IP Address ⓘ

* Subnet Mask ⓘ

* Gateway ⓘ

* DNS Server

IP Count 253

OK

⚠ 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 [Configuring the IP Address of the Management Computer](#)) 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**.

IP Allocation

ⓘ Assign DHCP-assigned IP addresses to all devices.


Internet

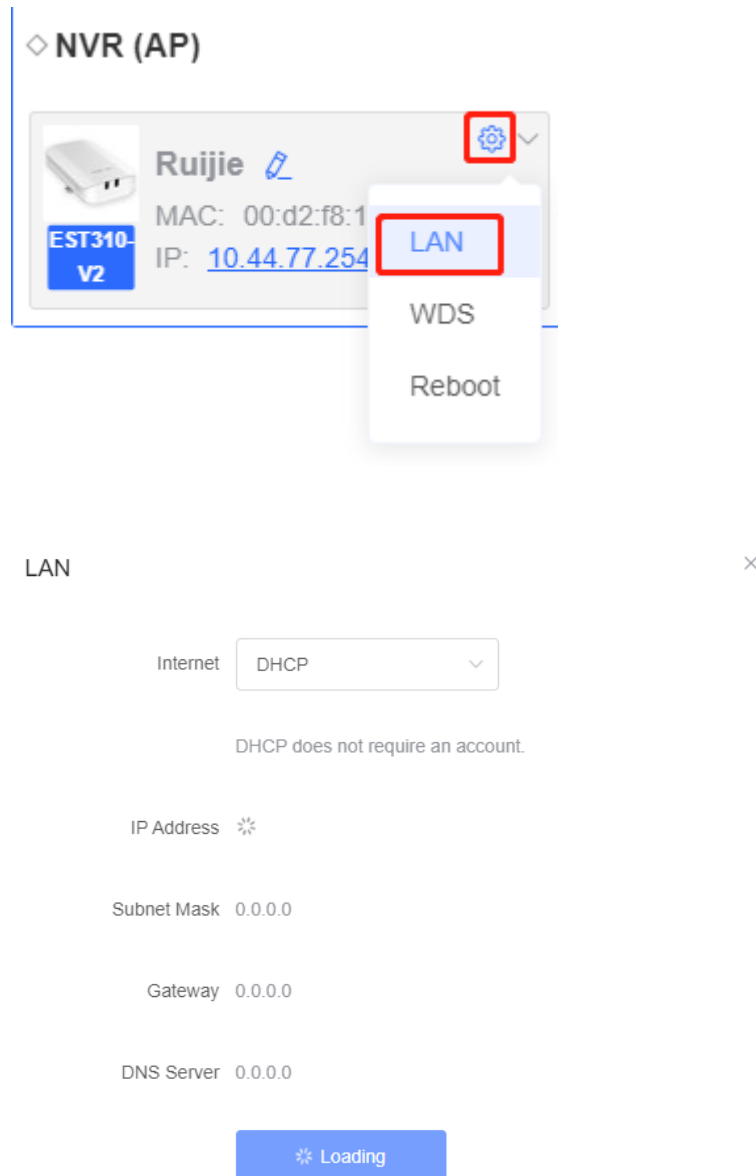
DHCP does not require an account.

OK




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

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

To set the IP address for a single device, click , and select LAN from the drop-down list. For the configuration method, see [Allocating IP Addresses to All Bridges in the Network](#).



◇ NVR (AP)

 Ruijie   ✓

MAC: 00:d2:f8:1
IP: 10.44.77.254

EST310-V2

LAN
WDS
Reboot

LAN ×

Internet

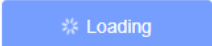
DHCP does not require an account.

IP Address *

Subnet Mask 0.0.0.0

Gateway 0.0.0.0

DNS Server 0.0.0.0



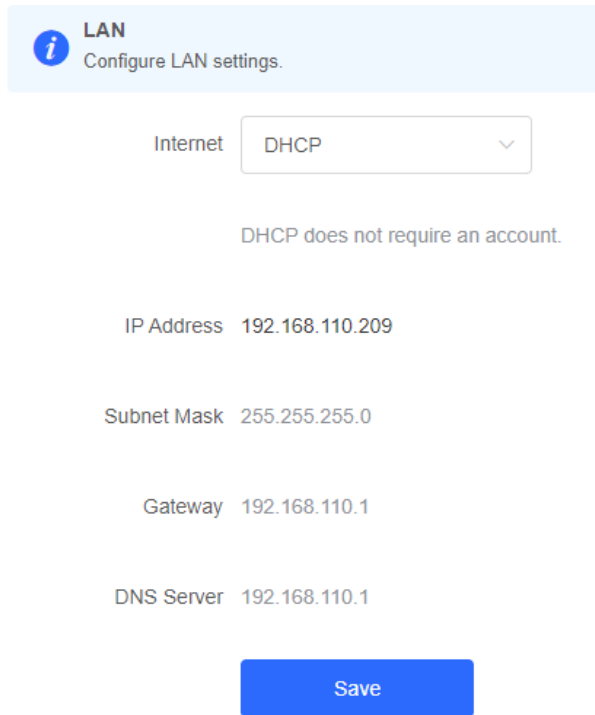
Caution

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 [Configuring the IP Address of the Management Computer](#)) Therefore, exercise caution when performing this operation.

5.1.3 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**.



The screenshot shows the LAN configuration interface. At the top, there is a header with an information icon and the text "LAN Configure LAN settings." Below this, the "Internet" setting is set to "DHCP" in a dropdown menu. A note states "DHCP does not require an account." The "IP Address" is set to "192.168.110.209", "Subnet Mask" is "255.255.255.0", "Gateway" is "192.168.110.1", and "DNS Server" is "192.168.110.1". A blue "Save" button is located at the bottom of the configuration area.

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 [Configuring the IP Address of the Management Computer](#)) Therefore, exercise caution when performing this operation.

5.2 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.



Flow Control

Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.

Flow Control

Save

5.3 Packet Rate Limiting

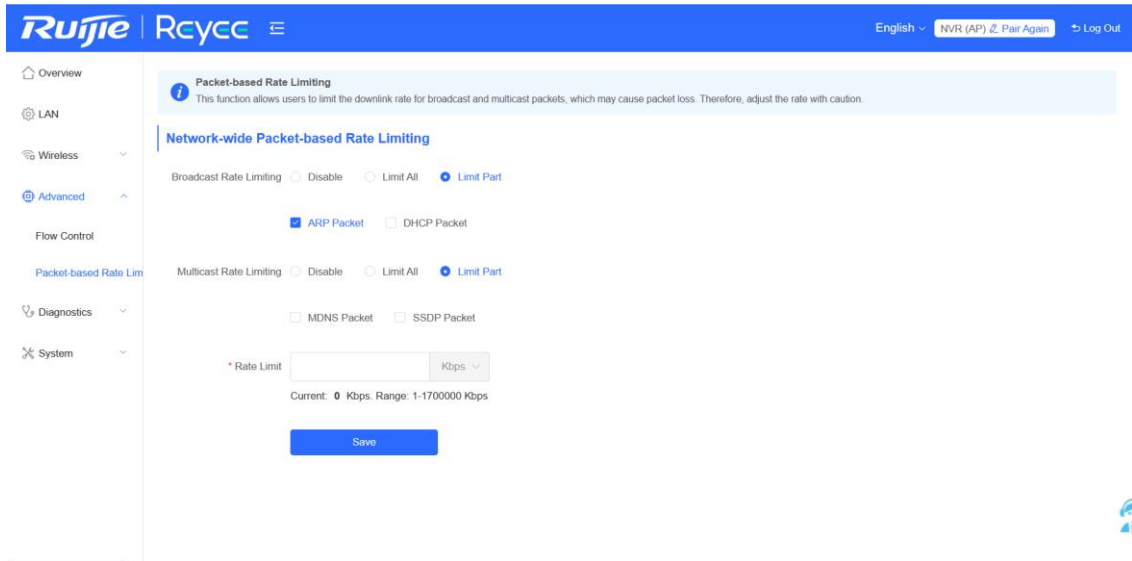
Enable rate limiting on broadcast or multicast packets to avoid congestion on the air interface.

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**.



The screenshot displays the Ruijie Rcycc web interface. The top navigation bar includes the Ruijie logo, the Rcycc name, and user information (English, NVR (AP) Pair Again, Log Out). The left sidebar shows a menu with options: Overview, LAN, Wireless, Advanced (selected), Flow Control, Packet-based Rate Lim, Diagnostics, and System. The main content area is titled "Packet-based Rate Limiting" and contains a warning message: "This function allows users to limit the downlink rate for broadcast and multicast packets, which may cause packet loss. Therefore, adjust the rate with caution." Below this, the "Network-wide Packet-based Rate Limiting" section is visible. It has two main sections: "Broadcast Rate Limiting" and "Multicast Rate Limiting". Under "Broadcast Rate Limiting", there are radio buttons for "Disable", "Limit All", and "Limit Part" (selected). Below these are checkboxes for "ARP Packet" (checked) and "DHCP Packet". Under "Multicast Rate Limiting", there are radio buttons for "Disable", "Limit All", and "Limit Part" (selected). Below these are checkboxes for "MDNS Packet" and "SSDP Packet". At the bottom, there is a "Rate Limit" input field set to "0 Kbps" with a dropdown menu for "Kbps". Below the input field, it says "Current: 0 Kbps. Range: 1-1700000 Kbps". A "Save" button is located at the bottom of the configuration area.

6 Alarm and Fault Diagnosis

6.1 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.

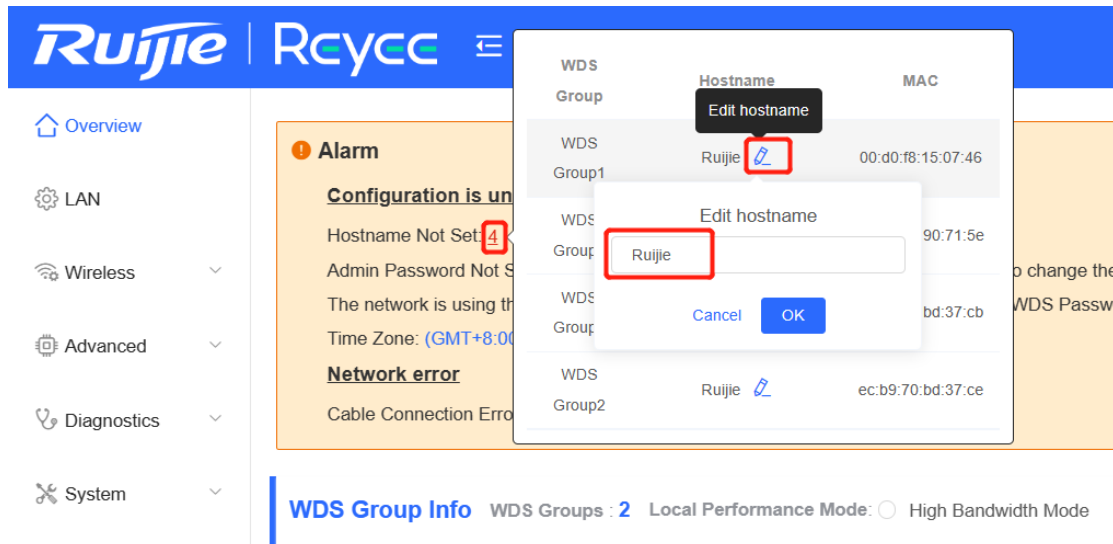
Choose **Overview** > **Alarm**.

The screenshot displays the Ruijie Rcycc management interface. At the top, there is a navigation menu with options like Overview, LAN, Wireless, Advanced, Diagnostics, and System. The main content area shows an 'Alarm' section with a red border, indicating a critical issue. The alarm message states 'Configuration is uninitialized' and lists several configuration errors: 'Hostname Not Set: 4', 'Admin Password Not Set or The Management Password is Inconsistent', and 'Time Zone: (GMT+8:00)Asia/Shanghai'. Below this, a 'Network error' section shows 'Cable Connection Error: 2' with a 'Suggested Actions' link. The interface also displays 'WDS Group Info' for 'WDS Group1', including details for APs and CPEs, channel, WDS SSID, and various performance metrics like Latency, Jitter, Freeze, Bandwidth, Interference, and RSSI. A legend for signal strength (Strong Signal, Medium Signal, Poor Signal) is also visible.

6.1.1 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.

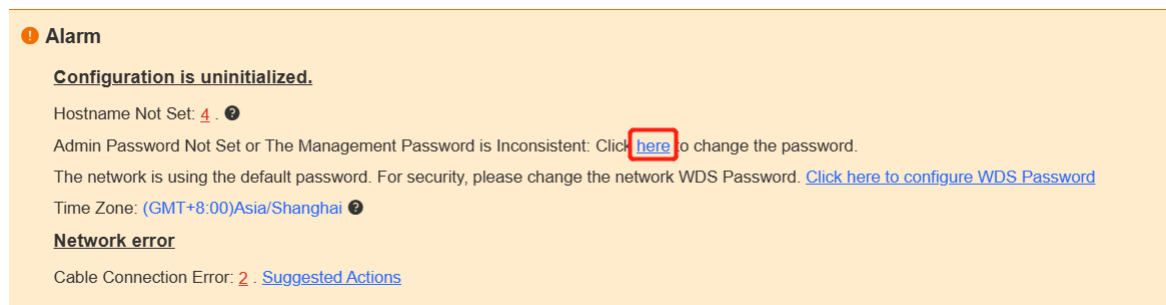
When viewing the alarm, hover the cursor over the orange number of the prompt and click  in the displayed dialog box to modify the name of each device. (The orange number, 2 in the figure, indicates the number of devices that still use the default name in the network.) Enter the new device name and click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



6.1.2 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 [Default Device Name Is Not Modified](#).



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 [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.

6.1.3 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.

1 Alarm

Configuration is uninitialized.

Hostname Not Set: 4

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.

6.1.4 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.

1 Alarm

Configuration is uninitialized.

Hostname Not Set: 4

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.

6.1.5 Latency Is High or Bandwidth Is Insufficient

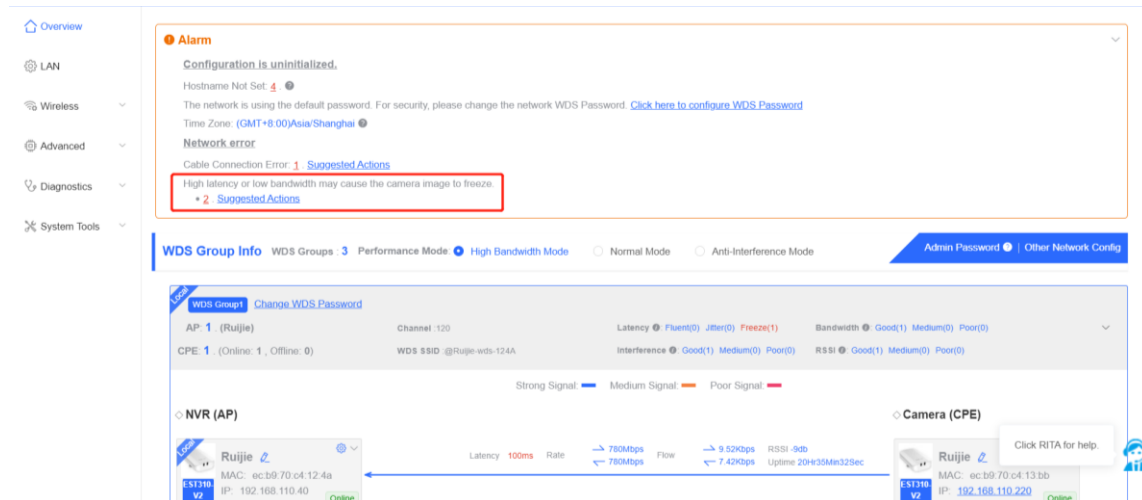
First, check whether the device latency is too high. If yes, the interference in the environment may be severe. Then, you are advised to change to a channel with smaller interference.

If not, increase the channel width. For channel settings, see [Channel settings](#). For channel width settings, see [Optimizing the Channel Width](#).

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

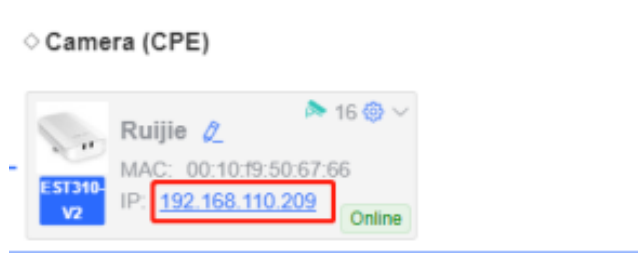
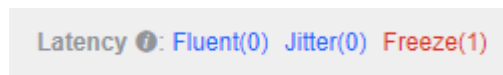
Hover the cursor over the orange number of the prompt to display all WDS groups, and click a group to display the details.

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



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

- [3 . Suggested Actions](#)

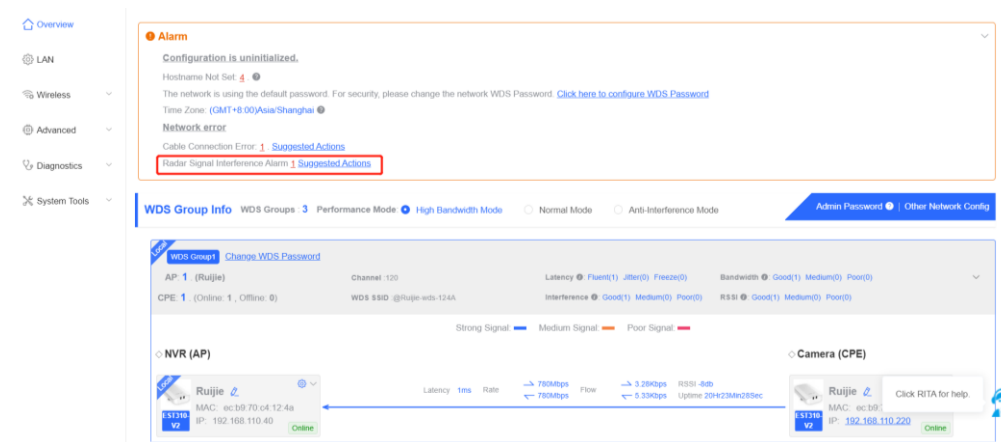


⚠ Caution

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.

6.1.6 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.



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: 2. [Suggested Actions](#)

Radar Signal Interference Alarm 1 [Suggested Actions](#)

WDS 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 [Displaying WDS Group Information](#).) If so, manually switch the channel to a non-dynamic frequency selection (DFS) channel. For the setting method, see [Channel settings](#).

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.

6.2 Network Diagnosis Tools

6.2.1 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 Network Tools

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* Ping Count

* Packet Size

Result

6.2.2 Collecting Fault Info

Choose **Diagnostics > Fault Collection**.

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

i Fault Collection
Compress the configuration into a file for engineers to identify fault.

6.3 Configuring Spectrum Scan

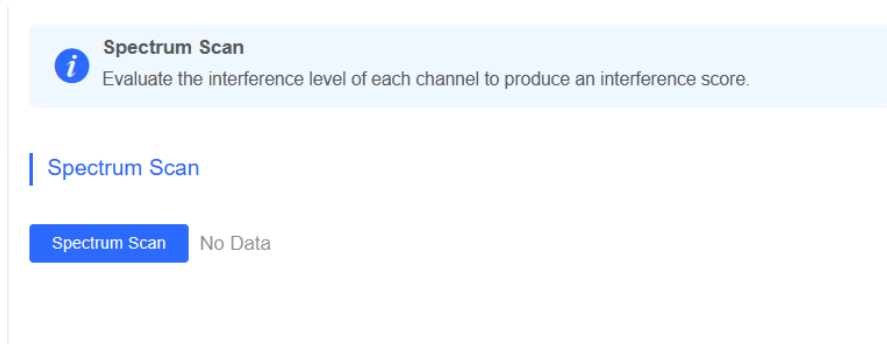
i Note

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.

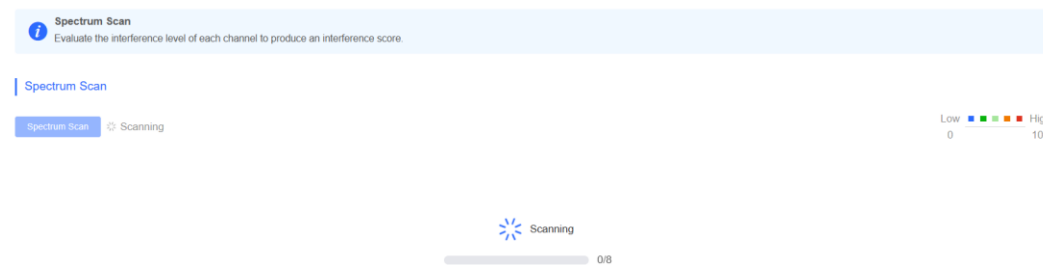
Click **Spectrum Scan**, and then click **OK** on the pop-up window. The **Spectrum Scan** page is displayed.



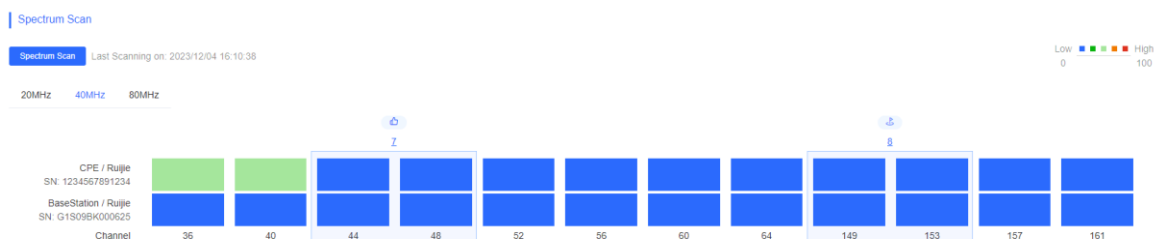
Tip



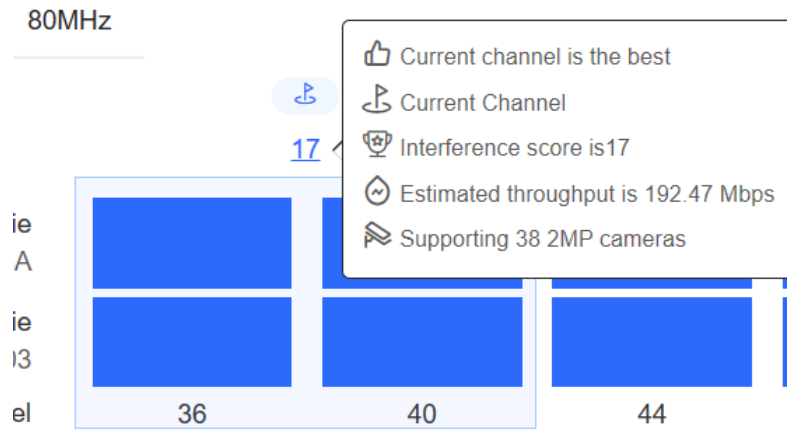
Switching the channel scan may take up to a few minutes, during which the device may experience a temporary disconnection. Continue?



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.



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**.



Tip



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

Cancel OK

7 Reyee FAQs

7.1 [Reyee Password FAQ](#)

7.2 [Reyee EST Bridge FAQ](#)

7.3 [Reyee Series Devices Parameters Tables](#)

7.4 [Reyee Parameter Consultation FAQ](#)

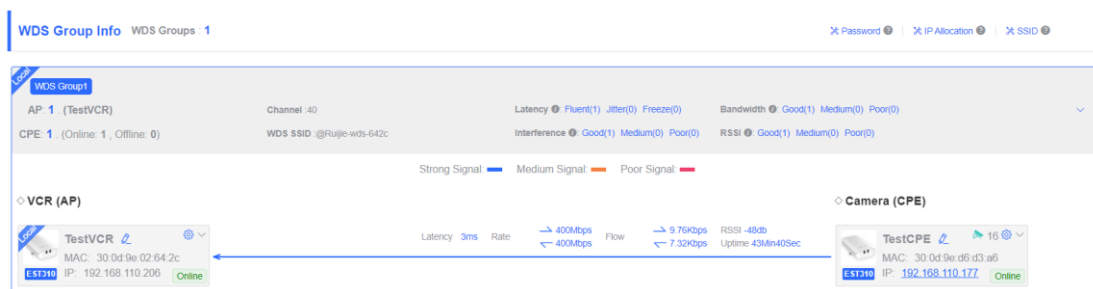
8 Appendix: Monitoring

8.1 WDS Group Information

Choose **Overview > WDS Group Info**. Displayed WDS group information includes the number of APs 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 the items to view details.

Note:

The AP is at the NVR end, while the CPE is at the camera end.



AP: indicates the number of ESTs in NVR mode in this group. There can be only one EST in this mode in a group.

CPE: indicates the number of ESTs in CPE mode in this group. The group allows one to five EST310 V2s or one to three EST350 V2s. Only one CPE can be bridged by the RG-EST100-E wireless bridge.

Channel: indicates the channel for the WDS SSID. Only the 5G channel is supported.

Latency: indicates the latency of bridges in this group, which can be **Fluent**, **Jitter**, or **Freeze**. You can click the icon to check the exact latency of all CPEs.

Hostname	MAC	Latency
TestCPE	30:0d:9e:d6:d3:a6	9ms

Latency **Fluent**(1) Jitter(0) Freeze(0)

Bandwidth: indicates the transmission rate of all bridges in this group, which can be **Good**, **Medium**, or **Poor**. You can click the icon to check the exact bandwidth of all CPEs.

Hostname	MAC	Bandwidth
TestCPE	30:0d:9e:d6:d3:a6	378Mbps

(0) Freeze(0) Bandwidth ⓘ: Good(1) Medium(0) Poor(0)

WDS SSID: indicates the name of the WDS SSID.

Interference: indicates the interference status of all bridges in this group, which can be **Good**, **Medium**, or **Poor**.

You can click the icon to check the exact air interface utilization of all CPEs.

Hostname	MAC	Air Interface Utilization
TestCPE	30:0d:9e:d6:d3:a6	1%

Interference ⓘ: Good(1) Medium(0) Poor(0)

RSSI: indicates the connected signal of all bridges in this group, which can be **Good**, **Medium**, or **Poor**. You can click the button to check the exact RSSI of all CPEs.

Hostname	MAC	RSSI
TestCPE	30:0d:9e:d6:d3:a6	-50bd

Medium(0) Poor(0) RSSI ⓘ: Good(1) Medium(0) Poor(0)

8.1.1 IP Allocation

- When a large number of devices on the network require static IP addresses, you can use **IP Allocation** to automatically allocate a static IP address to each device.

Choose **Overview > WDS Group Info**, click **IP Allocation** in the upper right corner of the **WDS Group Info** area, set **IP Assignment** to **Static IP Address**, set **Start IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server**, and click **OK**.

×

IP Allocation

ⓘ Assign static IP addresses to conflicting devices.

IP Assignment

* Start IP Address ⓘ ⓘ

* Subnet Mask ⓘ

* Gateway ⓘ

* DNS Server ⓘ

IP Count 253

 **Note**

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 will change, 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 on the same network segment. If they are on different network segments, reconfigure the IP address of the management computer.

- When a large number of devices on 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. Choose **Overview > WDS Group Info**, click **IP Allocation** in the upper right corner of the **WDS Group Info** area, set **IP Assignment** to **DHCP**, and click **OK**.

×

IP Allocation

ⓘ Assign DHCP-assigned IP addresses to all devices.

IP Assignment

DHCP does not require an account.

8.1.2 Configuring the SSID

You can configure the SSID for all EST devices on the network. The SSID is disabled by default and devices cannot be managed by accessing Wi-Fi. The default device management SSID is @Ruijie-bXXXX. XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with devices.

Choose **Overview > WDS Group Info**, click **SSID** in the upper right corner of the **WDS Group Info** area, set parameters on the **SSID Settings** page, and click **Save**.

SSID Settings ×

Enable WiFi

* SSID:

Security:

Hide SSID: (The SSID must be manually entered exactly.)

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

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

Security: The following encryption modes are available: **Open**, **WPA-PSK**, **WPA2-PSK**, and **WPA_WPA2-PSK**. You are advised to use **WPA_WPA2-PSK** and set the password to enhance security.

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

8.1.3 Displaying Information About a Single Device

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

Click the icon of a device to display 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.

The screenshot displays a network management interface with the following sections:

- WDS Group Info**: Shows 'WDS Groups - 1' and 'WDS Group1'. Key metrics include AP: 1 (TestVCR), Channel: 40, Latency: Fluent(1), Jitter(0), Freeze(0), CPE: 1 (Online: 1, Offline: 0), WDS SSID: @Ruaje-wds-642c, Interference: Good(1), Medium(0), Poor(0).
- VCR (AP)**: A list of devices with a red box highlighting 'TestVCR'. Below it, details for 'EST310' are shown: MAC: 30.0d.9e.02.64.2c, IP: 192.168.110.206, and Online status.
- Device Selection**: A dropdown menu is set to 'Group 1 / AP / TestVCR'.
- Setup**: Tabs for LAN, WDS, and Reboot. Lock Status is 'Locked'.
- System Information**: Includes WDS SSID (TestVCR), Uptime (01h:27m:39s), Net Status (Connected), Model (EST310), SN (CAN90TZ04553C), Software Ver (AP_3.0(1)B2P28.Release(07220919)), Hardware Ver (2.00), and MAC (30.0d.9e.02.64.2c).
- LAN Information**: Shows IP Address (192.168.110.206), Subnet Mask (255.255.255.0), and LAN type (100baseT/F-Full-Duplex).
- Wi-Fi Information**: Shows Noise Floor/Utilization (-103 dBm / 1%), Distance (1000M), Channel (40), Transmit Power (27dBm), Channel Width (--), RSSI (--), and Band (5.8G).