Outdoor 5G Industrial Router

NR230

User Manual

V1.0.0

* This manual is applicable to the following products:： NR230-00W6

Xiamen Yifan Communicaton Technology Co., Ltd.

Add：Floor 14th, A06 Building, No. 370, ChengYi Street,
Jimei District, XiaMen, China   Zip Code: 361000

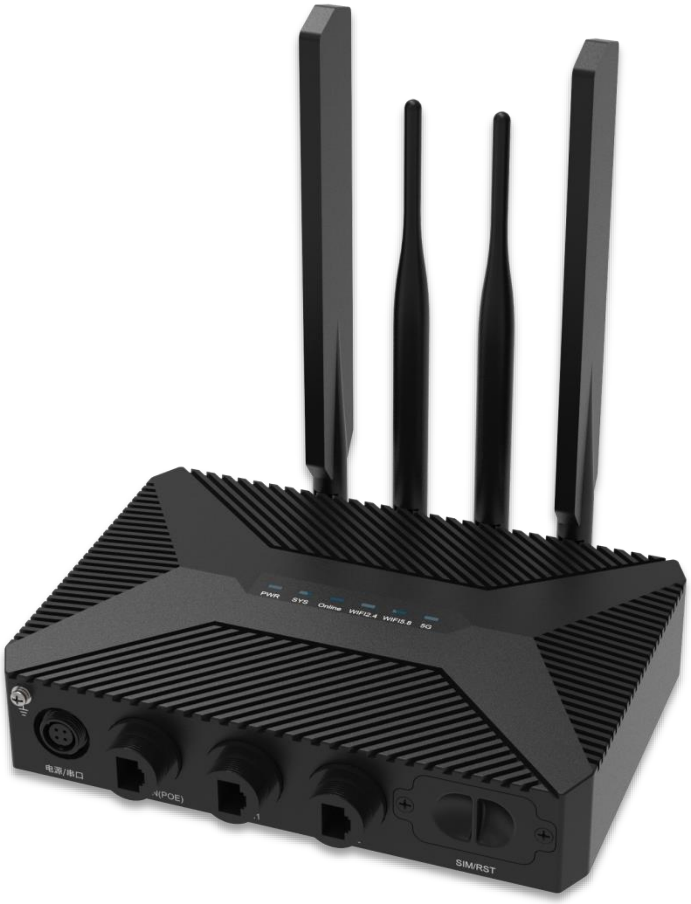
Tel：+86 592-6101492

Fax:+86 592-5222813

http://www.yifanwireless.com

Document Revision History

Date	Version	Note	Author
2024-11-06	V1.0.0	Initial Chinese Version	CHY
2024-12-23	V1.0.1	Initial English Version	Larry



Note: There may be differences between models of accessories and interfaces, actual products shall prevail.

Copyright Notice

All contents in the files are protected by copyright law, and all copyrights are reserved by Xiamen Yifan Communication Technology Co., Ltd. Without written permission, all commercial use of the files from Yifan are forbidden, such as copy, distribute, reproduce the files, etc., but non-commercial purpose, downloaded or printed by individual (all files shall be not revised, and the copyright and other proprietorship notice shall be reserved) are welcome

Trademark Notice

Yifan and Yeacomm are all registered trademarks of Xiamen Yifan Communication Technology Co., Ltd., illegal use of the name of Yifan, trademarks and other marks of Yifan is forbidden, unless written permission is authorized in advance

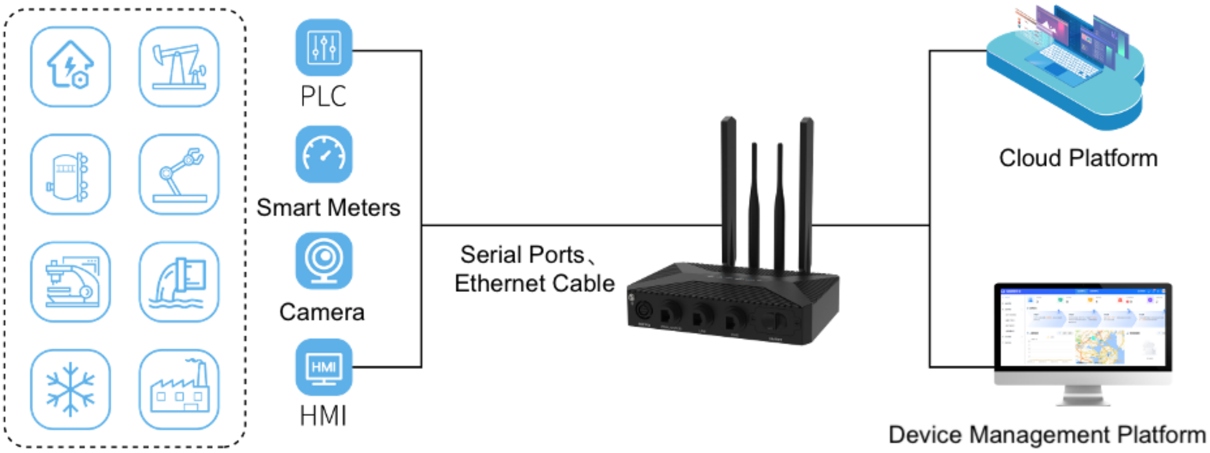
Contents

Chapter 1 Product Introduction

1.1 Product Overview

NR230 is a wireless communication router for the Internet of Things, which uses public 4G/5G networks to provide users with wireless long-distance big data transmission functions.

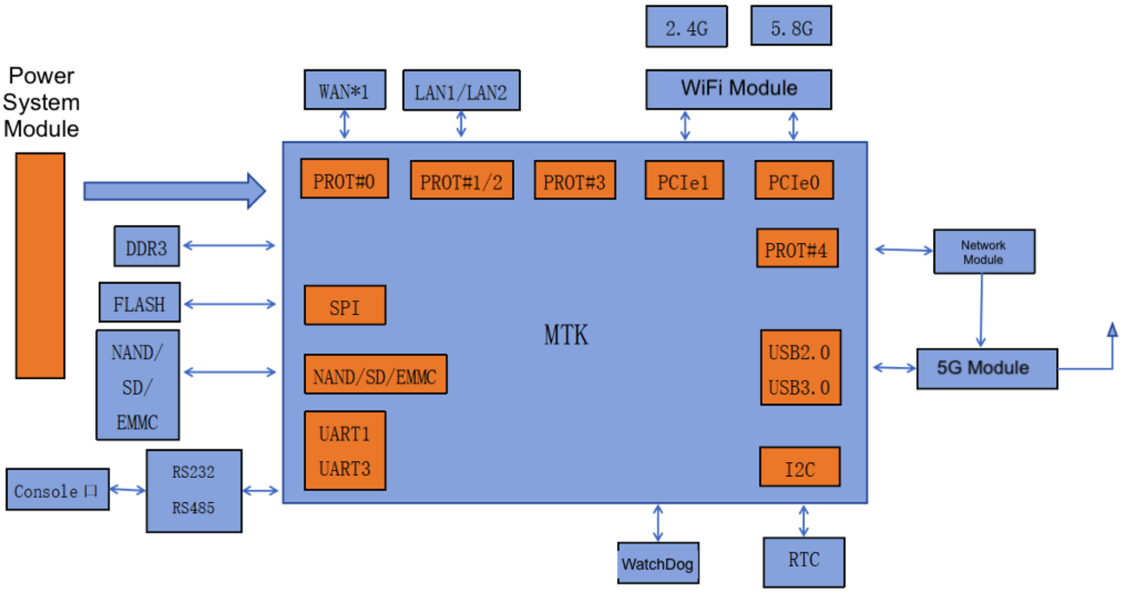
The product adopts high-performance industrial-grade 32-bit communication processor and industrial-grade wireless module, with embedded real-time operating system as the software support platform, and provides 1 RS232 and 1 RS485 + 3 Gigabit Ethernet LAN + 1 Ethernet, which can connect serial devices, Ethernet devices and WIFI devices at the same time to realize data transparent transmission and WiFi 6 routing functions.



This product has been widely used in the M2M industry on the Internet of Things industry chain, such as smart grid, smart transportation, smart home, finance, mobile POS terminals, supply chain automation, industrial automation, smart buildings, fire protection, public safety, environmental protection, meteorology, Digital medical treatment, remote sensing survey, military, space exploration, agriculture, forestry, water affairs, coal mine, petrochemical and other fields.

1.2 Block Diagram of Working Principle & Key Feature

5G Router Block Diagram as follow:



The main functions of the product are as follows:

- Support 5G LAN function
- Support input power failure alarm
- Support alarm for abnormal device temperature
- Support FRP intranet penetration
- Support POE+ power receiving
- Support network port on-off detection, rate reporting, delay reporting, etc
- Support 4G/5G and wired WAN dual-link intelligent handover and backup function
- Support VPN PPTP/L2TP/GRE/IPSEC/OPENVPN
- Support remote management, SYSLOG, SNMP, TELNET, SSHD, HTTPS
- Support SPI firewall, VPN traversal, access control, URL filtering
- WiFi supports WEP, WPA, WPA2 and other encryption methods, MAC address filtering
- SIM/UIM card interface with built-in 15KV ESD protection
- Support frequency locking, cell locking, EOIP, bridge mode, VXLAN, virtual IP, GRETAP and other functions
- Support multi-channel DHCP server and DHCP bundle MAC address, DDNS, firewall, NAT, DMZ host and other functions
- Support VLAN, MAC address cloning, PPPOE server
- Support Yifan Cloud Docking, making O&M more convenient
- Support a variety of online and offline trigger modes, serial port data, network data trigger online and offline mode

Chapter 2 Installation

2.1 Overview

5G routers must be installed correctly to achieve the designed functions. Usually the installation of the equipment must be carried out under the guidance of qualified engineers approved by the company.

Notes: Please do not install a 5G router with power.

2.2 Packing List

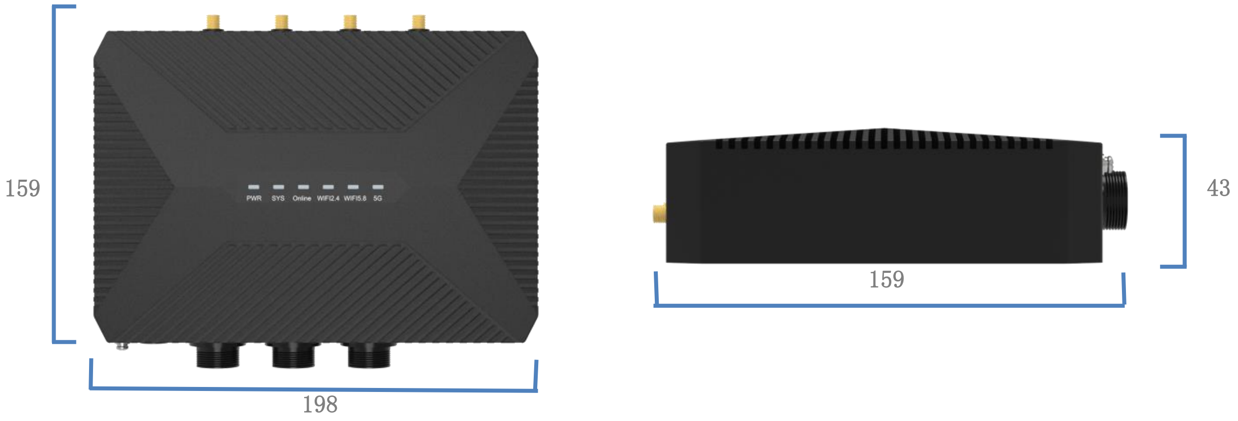
When you open the box, please keep the packing materials, so that you can use it when you need to transfer in the future.

The list is as follows:

- 1 x 5G router host
- 4 x 5G wireless cellular antennas (SMA male) / 2 x 5G wireless cellular antennas (Redcap Version)
- 2 x WIFI antenna (SMA female)
- 1 x Matching power supply
- 1 x Ethernet direct connection
- 1 serial port wiring for 1-in-3 power supply
- 3 IP68 Ethernet Ports Protective Covers
- Easy Operation Guide for the Product
- 1 x Warranty card

2.3 Installation and Cable Connection

Dimensions(mm):



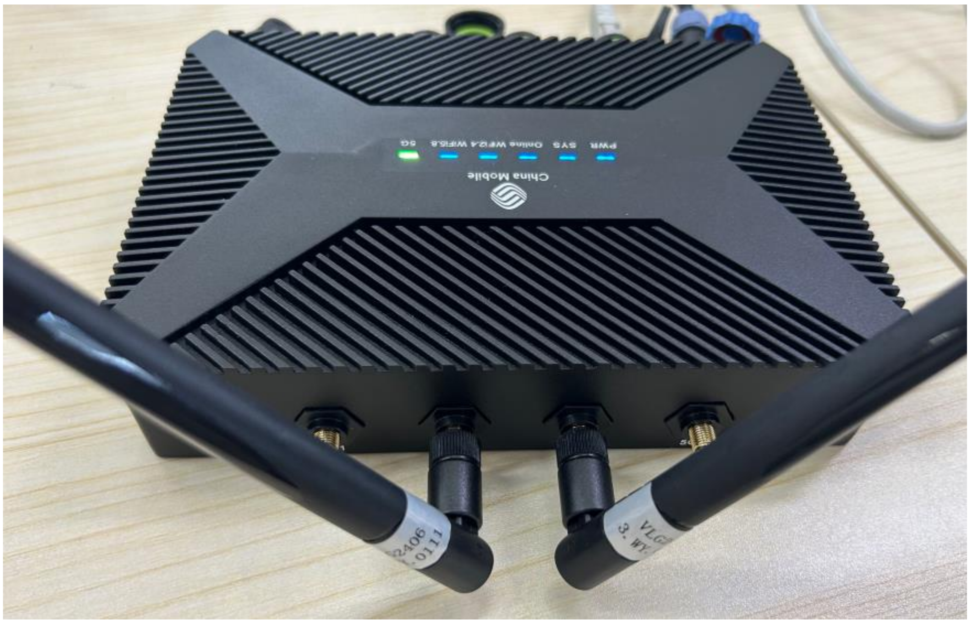
5G Router Size

Antenna Installation:

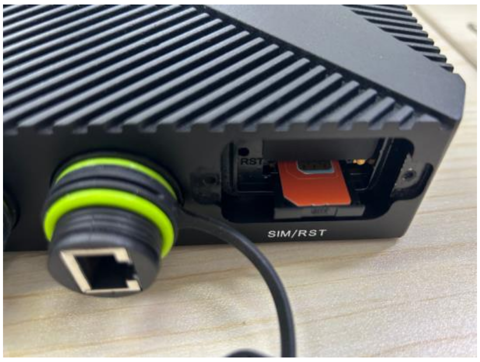
The 5G antenna interface is an SMA female socket（Identifier“5GX”，where X is "1-4"). Screw the SMA male of the matching wireless cellular antenna to the antenna interface and make sure to tighten it. To increase the isolation of the 5G antenna, try to keep the antenna at an angle of 30 degrees to enhance signal quality. As Follow.

The WIFI antenna interface is an SMA male socket(Identify as “WIFI1”，“WIFI 2”). Screw the SMA female of the matching WIFI antenna to the antenna interface and make sure to tighten it. In addition, to increase the isolation of the

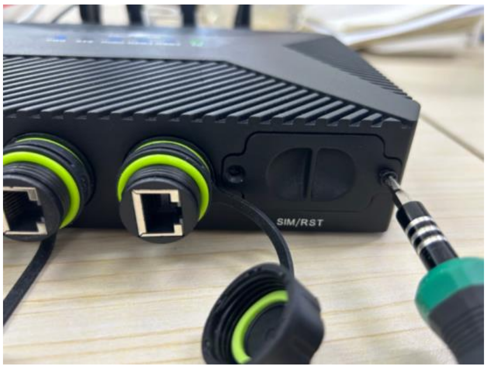
Wi-Fi antenna, it is recommended that the two Wi-Fi are placed at a 90-degree angle.



SIM/UIM Card Installation



Install SIM Card



Install Cover

When installing or removing the SIM/UIM card, first use a pointed object to gently hold the eject button, and the SIM/UIM card sleeve will pop out. Put the SIM/UIM card into the card holder first, and make sure that the metal contact surface of the SIM/UIM card is facing outward, then insert the SIM/UIM card holder into the drawer.

Install the card sleeve and lock the screws on both sides of the card sleeve with a screwdriver to achieve the waterproof and anti-theft effect.

Connecting Ethernet Cables:

Plug one end of the network direct cable into any port of LAN1~LAN3 of the 5G router, and plug the other end into the Ethernet interface of the user device. The network direct connection signal connection is as follows: Connecting

Ethernet Cables: Plug one end of the network direct cable into any port of LAN1~LAN3 of the 5G router, and plug the other end into the Ethernet interface of the user device. The network direct connection signal connection is as follows::

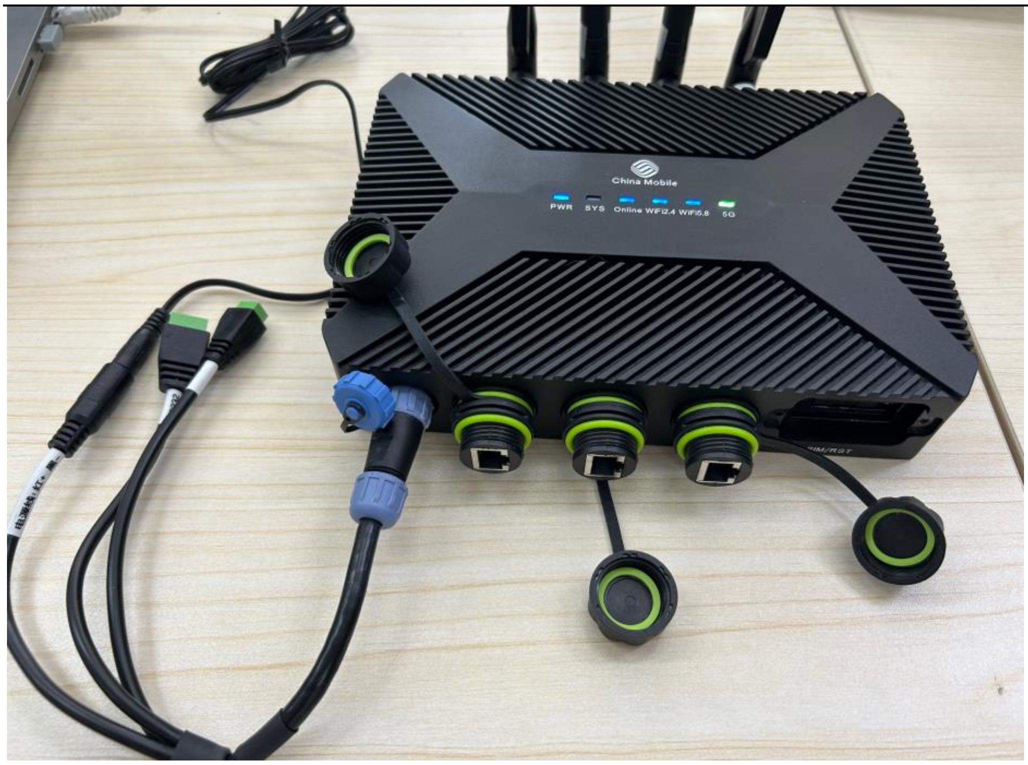
RJ45-1	RJ45-2	Wire Color
1	1	White/ Orange
2	2	Orange
3	3	White/ Green
4	4	Blue
5	5	White/ Blue
6	6	Green
7	7	White/ Brown
8	8	Brown

Definition of power supply and serial cables:

It adopts a one-to-three power serial port line, and one end is a round end connected to the "power/serial port" interface, including power supply, RS232, RS485 functions, which are defined as follows:

No.		Definition	Signal Recognition	Note
1	Power Cable（Round head）	VCC	The positive pole of the power supply end of the device	Red+
2		GND	The negative pole of the power supply end of the device	Black-
3	RS232 Cable （Green Terminal）	TX	RS232 Send	Wire identification “1”
4		RX	RS232 Receive	Wire identification “2”
5		GND	RS232 Ground	Wire identification “3”
6	RS485 Cable （Green Terminal）	A	RS485 A	Wire identification “+”
7		B	RS485 B	Wire identification “-”

The wire styles are as follows:



Connect the console cable (connect when using the serial port):

Connect the stripped end of the terminal serial port cable to the green terminal interface (GND RX TX) of the Router, and plug the DB9 end into the RS232 serial port interface of the user device. The signal connection of the terminal serial port cable is as follows:

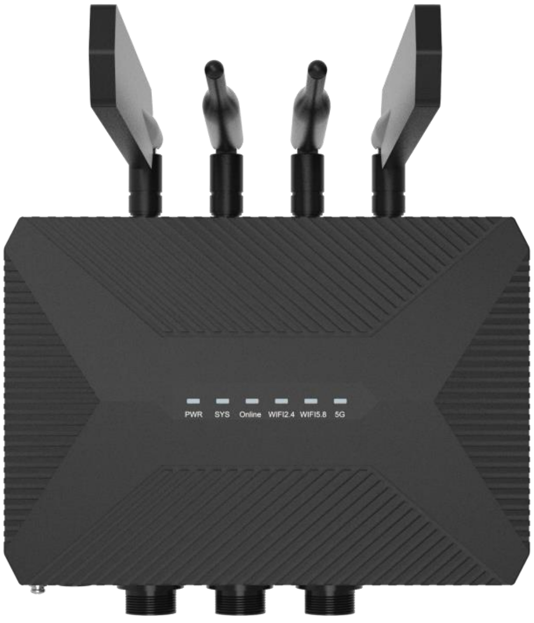
Terminal serial line signal definition(RS232)				
No.	Wire Color	Signal Definition	DB9 F	Signal Definition
1	Black	GND	5	Ground
2	Blue	RX	3	Receive Data
3	Brown	TX	2	Send Data

2.4 Power Supply

5G routers are usually used in complex external environments. To adapt to the complex application environment and improve the stability of the system, the router adopts advanced power supply technology. Users can use the standard 12VDC/1.5A power adapter to power the 5G router, or directly use the DC 9~36V power supply to power the router. When the user uses an external power supply to power the router, the stability of the power supply must be ensured (the ripple is less than 300mV, and the instantaneousvoltage does not exceed 36V), and the power supply must be greater than 8W.

A standard 12VDC/1.5A power supply is recommended

2.5 Indicator Specification



5G Router provide indicators as below: "Power", "System", "WiFi", "ONLINE", "5G":

Indicator Lights	Status	Definition
PWR	On	Device Power Normal
	Off	The device is not powered on
SYS	Blink	System is Running Normally
	Off	System is Running Abnormally
WiFi	On	WiFi On (2.4G or 5.8G or Both is Turn On)

	Off	WiFi Off（2.4G and 5.8G are Both Off）
Online	On	Device SIM1 is Logged in to the Network
	Off	Device SIM1 is Not Logged in to the Network
5G（Tri-color Light）	Green	The signal strength is excellent （Greater than -90dbm）
	Yellow	The signal strength is moderate （-90dbm~-105dbm）
	Red	The signal strength is Week（Less Than-105dbm）

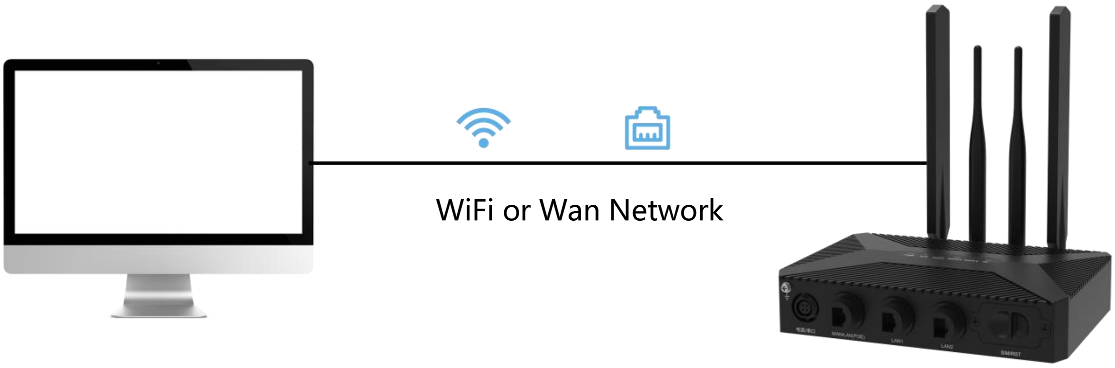
2.6 Reset Button Specification

5G routers have a reset button that is identified as "RST". What this button does is to restore the parameter configuration of the 5G router to factory values. Here's how to do it: Insert the "RST" hole with a sharp object, and gently press and hold the reset button for about 15 seconds before letting go, at this time, the 5G router will automatically restore the parameter configuration to the factory value, and after about 10 seconds, the 5G router will automatically restart (the auto-restart phenomenon is as follows: the "SYS" indicator turns off for about 10 seconds, and then works normally again).

Chapter 3 Parameter Configuration

3.1 Configuration Connection

Before configuring a 5G router, the 5G router and the PC used for configuration need to be connected via a factory-configured network cable or WiFi. When connected with a network cable, one end of the network cable is connected to one of the Ethernet ports of the 5G router's "Local Network" (hereinafter referred to as the LAN port), and the other end is connected to the Ethernet port of the PC. When connected with WiFi, the default SSID of the 5G router is "Yifan" or "Yifan-5G", and the password is "admin" for verification.

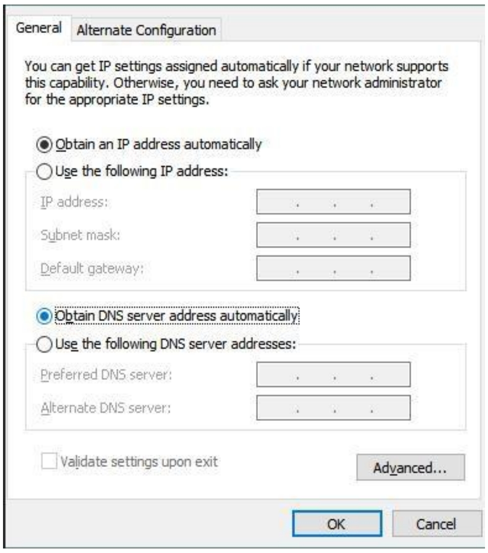


3.2 Access the Configuration Web Page

3.2.1 PC IP Address Settings(Two Methods)

The first way:

Get an IP address automatically



General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

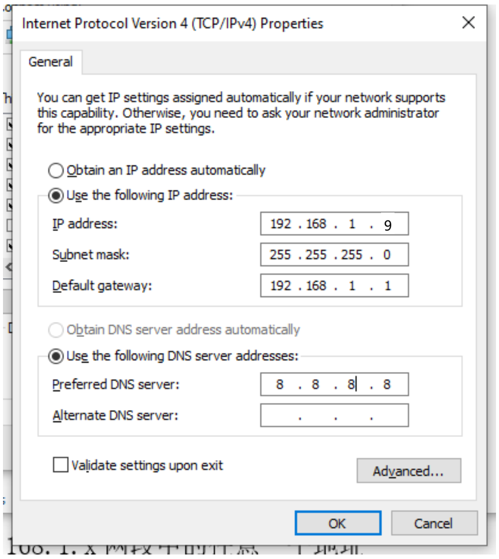
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

The second way:

Specify the IP address Set the IP address of the PC to 192.168.1.9 (or the IP address of another 192.168.1 network segment), and set the subnet mask to: 255.255.255.0, the default router is set to 192.168.1.1. DNS is set to the router address or a locally available DNS server Utensil.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

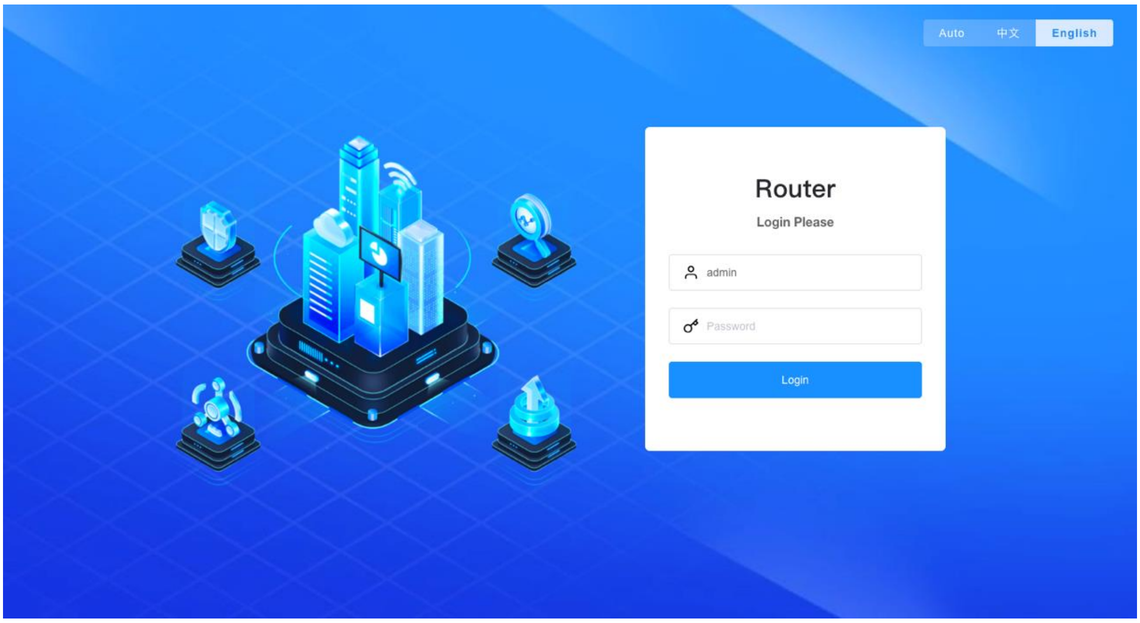
Alternate DNS server: . . .

□ Validate settings upon exit

3.2.2 Login to Configuration Page

The chapter is to present main functions of each page. Users visit page tool via web browser after connecting users' PC to the Router. There are eleven main pages: Home, Network, Data Acquisition, Application, Maintenance, Cloud Management, System. Users enable to browse slave pages by click one main page.

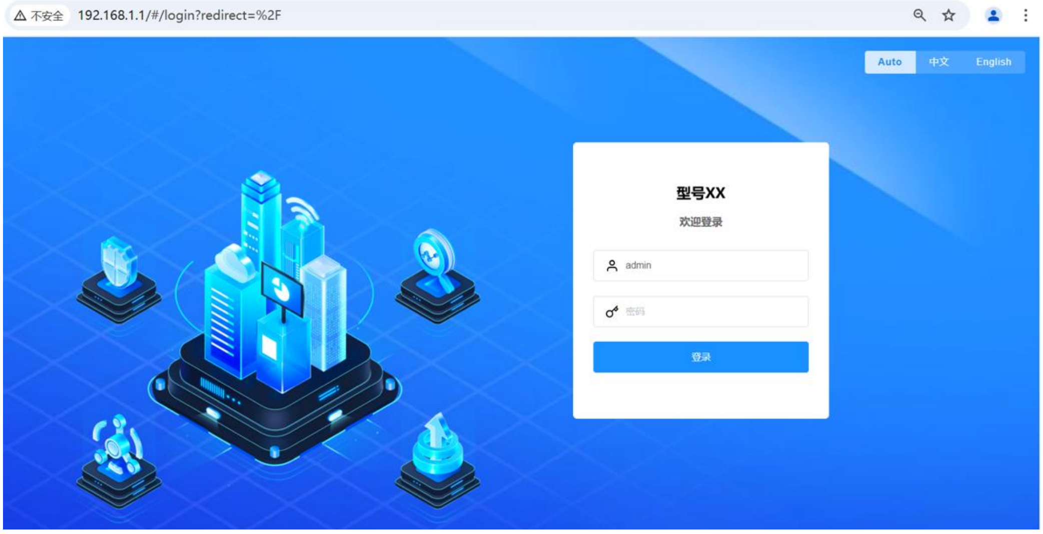
Users can open IE or other explorers and enter the Router's default IP address of 192.168.1.1 on address bar, then press the button of Enter to visit page Web management tool of the Router. The user’ s login in the web page at the first name, there will display a page shows as blow to tip users to modify the default username and password of the Router. Users must click "change password" to make it work if they modify username and password.



After access to the information main page

3.3 Boot Guide

(1) The default address of the router is 192.168.1.1, before that, please set your computer to the same network segment corresponding to it, or set the computer to automatically obtain the IP mode, as shown in the figure for the first time to configure the boot guide page of the router, the default account and password for the first login are admin



⚠ 不安全 192.168.1.1/#/login?redirect=%2F

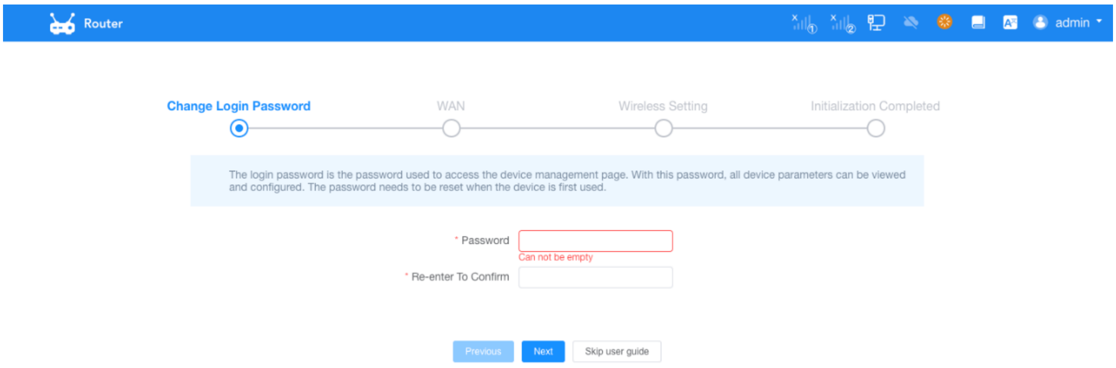
型号XX

欢迎登录

admin

密码

(2) Users can change the login password as needed



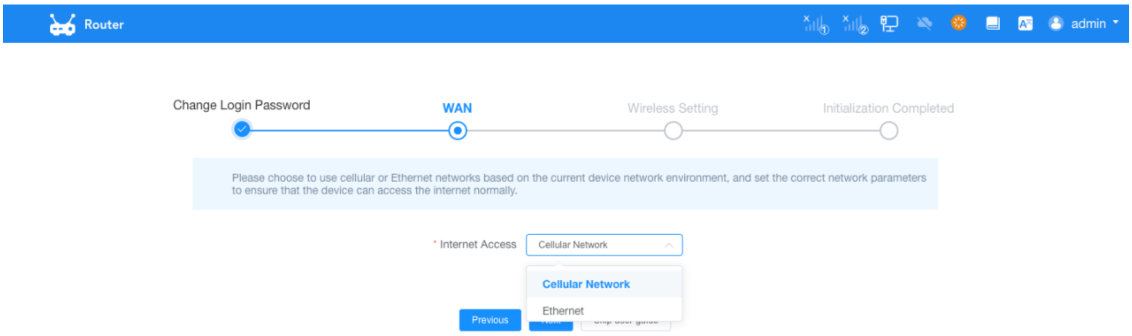
The login password is the password used to access the device management page. With this password, all device parameters can be viewed and configured. The password needs to be reset when the device is first used.

* Password

Can not be empty

* Re-enter To Confirm

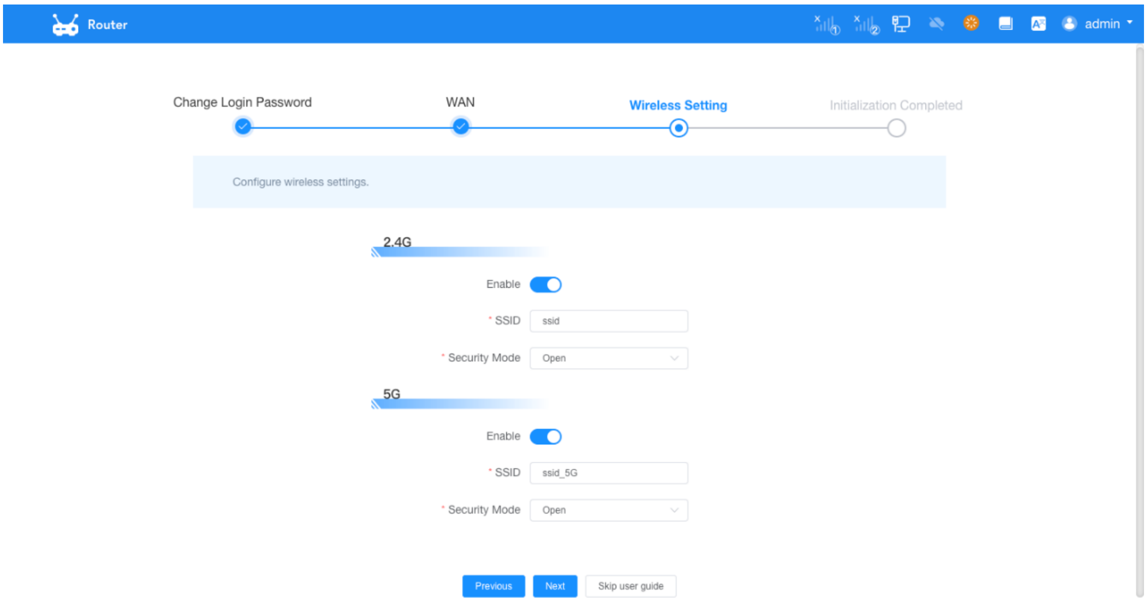
(3) Initialize the configuration according to the network environment, if the router uses the mobile phone card to access the Internet, select Cellular Network, if the router uses wired Internet access, select Ethernet, and if you select Ethernet, you can access the Internet after the correct configuration is carried out according to the corresponding IP field.



Please choose to use cellular or Ethernet networks based on the current device network environment, and set the correct network parameters to ensure that the device can access the internet normally.

* Internet Access: Cellular Network

(4) Users can choose whether to enable the WiFi hotspot and password according to their needs



Configure wireless settings.

2.4G

Enable: ●

* SSID: ssid

* Security Mode: Open

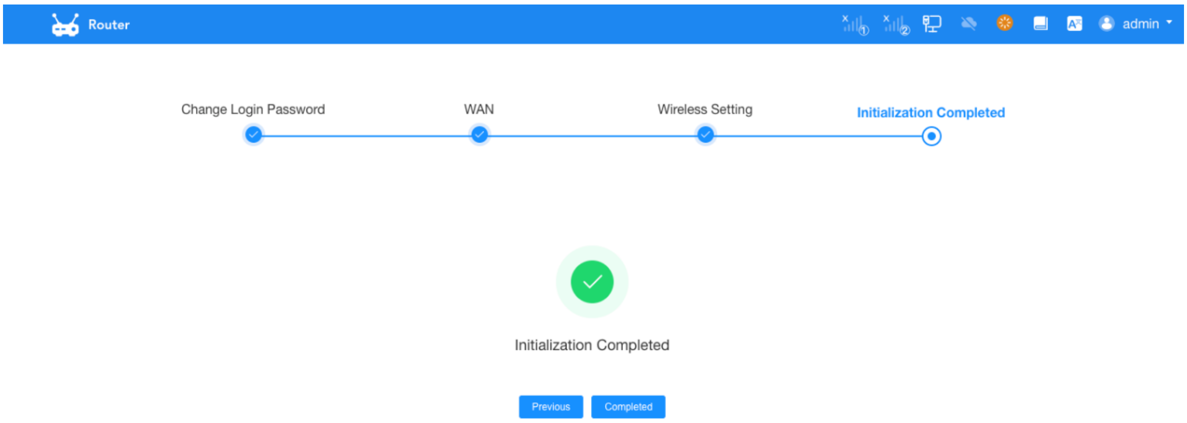
5G

Enable: ●

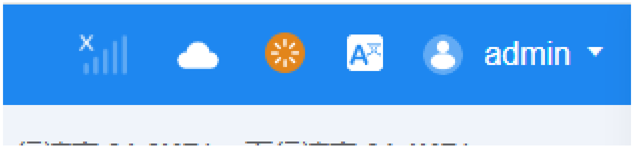
* SSID: ssid_5G

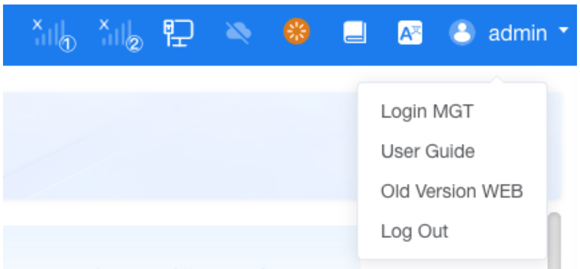
* Security Mode: Open

(5) After the initialization is completed, the device already has the basic network function, and more refined configurations need to be set in different sections.



3.4 Navigation Bar

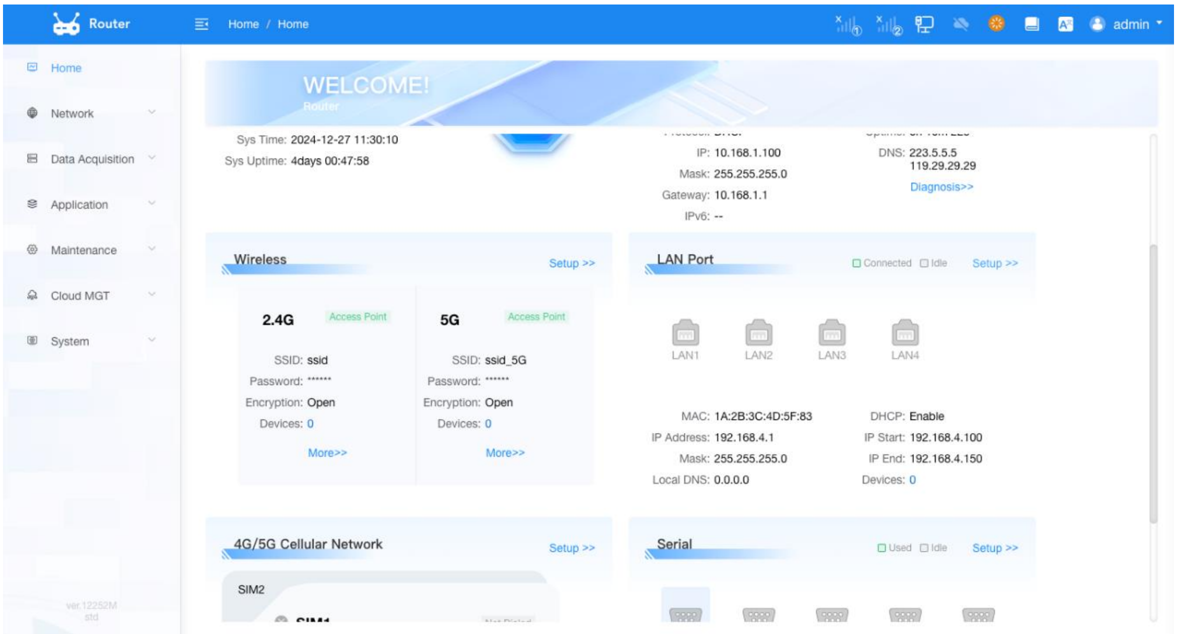




From left to right, there are cellular signals, cloud platform connection flags, restart buttons, language options, and a jump button to return to the legacy routing page

3.5 Home(Operation Status)

The home page is the running status of the router, on this page, you can see the status parameters of all modules in an integrated manner, and the following is an introduction to each module.



Sys Time: 2024-12-27 11:30:10
Sys Uptime: 4days 00:47:58

IP: 10.168.1.100
Mask: 255.255.255.0
Gateway: 10.168.1.1
IPv6: --

DNS: 223.5.5.5
119.29.29.29
Diagnosis>>

Wireless Setup >>

2.4G Access Point
SSID: ssid
Password: ******
Encryption: Open
Devices: 0
More>>

5G Access Point
SSID: ssid_5G
Password: ******
Encryption: Open
Devices: 0
More>>

LAN Port □ Connected □ Idle Setup >>

LAN1 LAN2 LAN3 LAN4

MAC: 1A:2B:3C:4D:5F:83
IP Address: 192.168.4.1
Mask: 255.255.255.0
Local DNS: 0.0.0.0

DHCP: Enable
IP Start: 192.168.4.100
IP End: 192.168.4.150
Devices: 0

4G/5G Cellular Network Setup >>

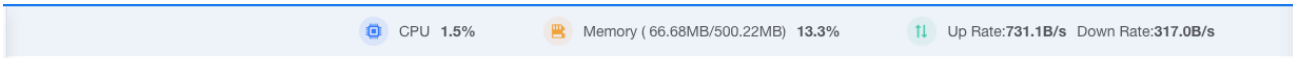
SIM2

SIM1

Serial □ Used □ Idle Setup >>

Real-time operating parameters:

In the top bar, you can see the CPU usage, memory usage, and real-time uplink and downlink rate of Internet access, which are displayed with the dynamic changes of the device.



CPU 1.5%   Memory (66.68MB/500.22MB) 13.3%   Up Rate:731.1B/s Down Rate:317.0B/s

Device Information:

Name: The name of the device, which can be changed in System Management - System Settings

Model: displayed according to the specific device model

SN: the SN of the router, which uniquely identifies the router

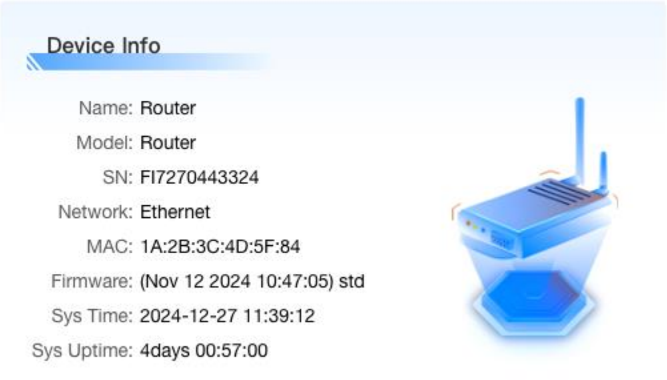
Network: The link that is currently connected to the Internet, if it is wired, Ethernet is displayed

MAC: the MAC address of the device

Firmware: The current firmware version

System Time: The current system time

System Uptime: How long has the Device being running



Device Info

Name: Router
Model: Router
SN: FI7270443324
Network: Ethernet
MAC: 1A:2B:3C:4D:5F:84
Firmware: (Nov 12 2024 10:47:05) std
Sys Time: 2024-12-27 11:39:12
Sys Uptime: 4days 00:57:00

Internet Networking

This module is the WAN port networking information

Main link: If it is green, it is connected normally, and if it is gray, it is not connected

Protocol: The type of device connected to the WAN port

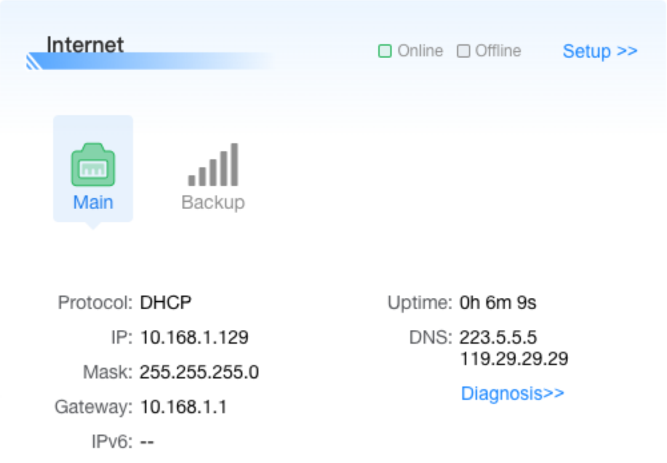
IP: WAN IP address

Subnet mask: The subnet mask of the device that goes online

Router: The IP address of the router configured on the device

DNS: the DNS address configured by the device

On-line time: the duration of the WAN dial-up Internet connection

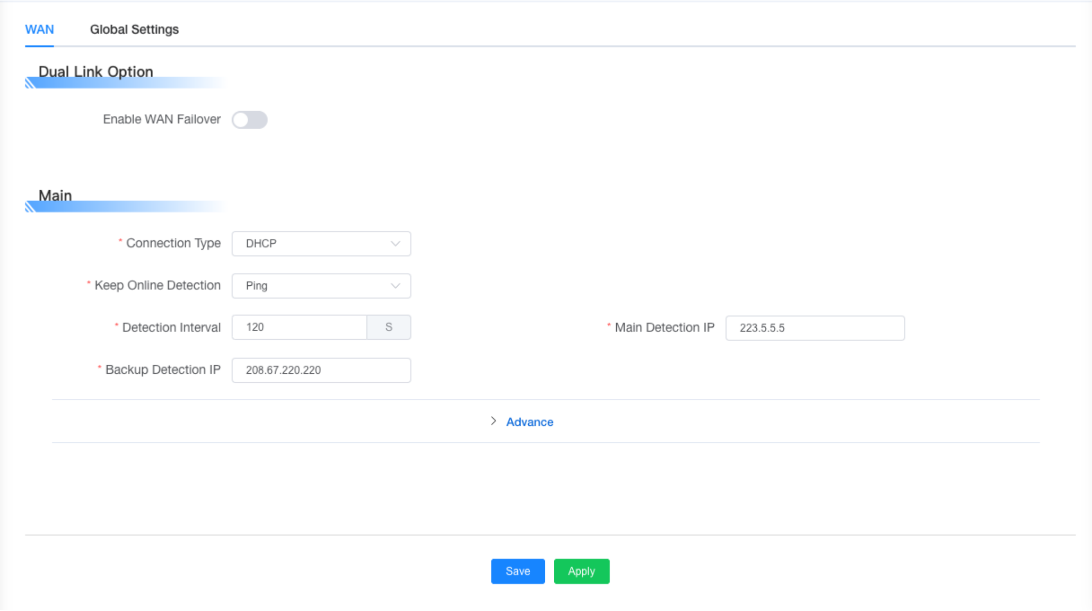


Internet

Protocol: DHCP
IP: 10.168.1.129
Mask: 255.255.255.0
Gateway: 10.168.1.1
IPv6: --

Uptime: 0h 6m 9s
DNS: 223.5.5.5
119.29.29.29

Click Settings to set the Internet link, as shown in the figure



Dual Link Option

Enable WAN Failover ○

Main

* Connection Type: DHCP

* Keep Online Detection: Ping

* Detection Interval: 120 S

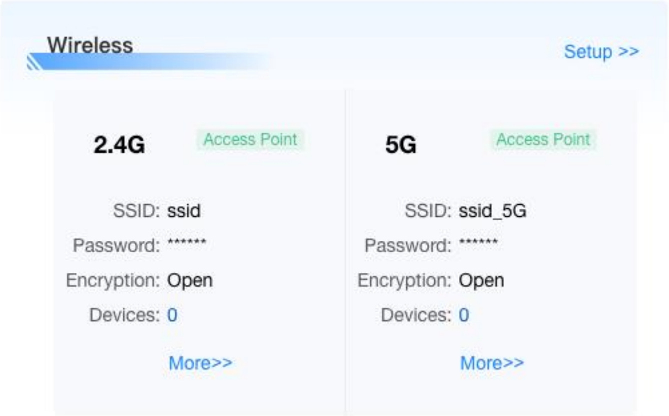
* Main Detection IP: 223.5.5.5

* Backup Detection IP: 208.67.220.220

Click Network Diagnostics to perform detailed network analysis.

Wireless

Display the relevant information of dual-band WiFi, click Settings, you can enter more detailed wireless (WiFi) settings, WiFi support AP and client relay bridging mode, etc., you can also view the information of sub-devices connected to WiFi

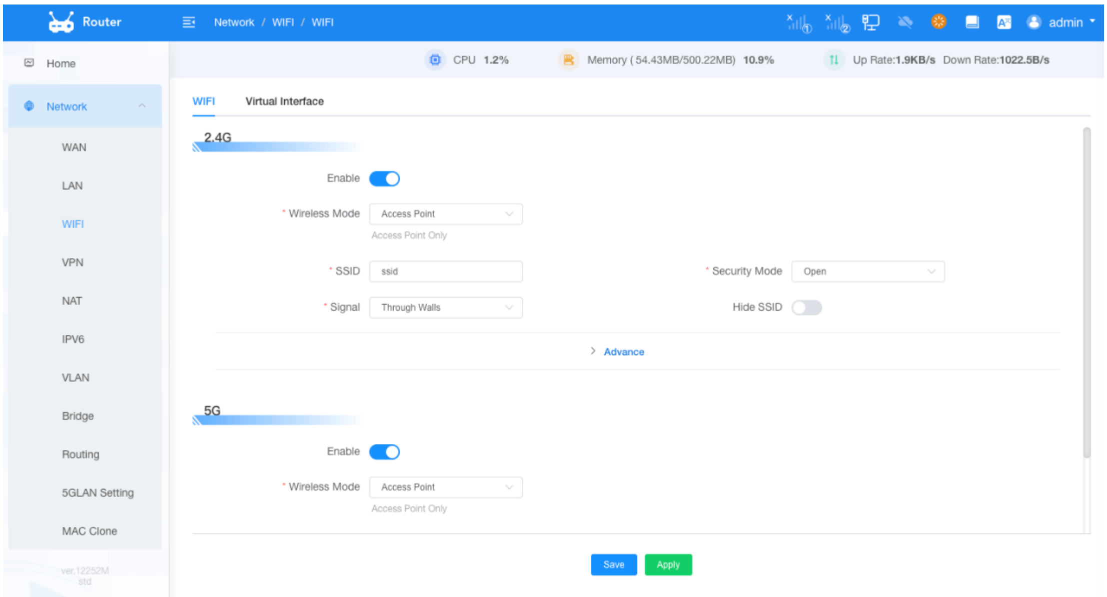


2.4G Access Point

SSID: ssid
Password: ******
Encryption: Open
Devices: 0

5G Access Point

SSID: ssid_5G
Password: ******
Encryption: Open
Devices: 0



CPU 1.2% Memory (54.43MB/500.22MB) 10.9% Up Rate:1.9KB/s Down Rate:1022.5B/s

2.4G

Enable

* Wireless Mode: Access Point

Access Point Only

* SSID: ssid

* Security Mode: Open

* Signal: Through Walls

Hide SSID

5G

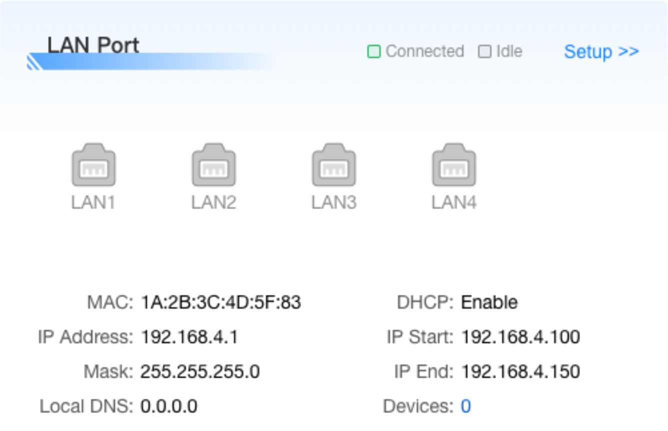
Enable

* Wireless Mode: Access Point

Access Point Only

LAN Port

If the port is green, it means that there are devices accessing the LAN port, and if it is gray, there is no device access MAC address: the MAC address of the LAN port IP Address: The IP address of the router itself in the LAN Subnet Mask: The subnet mask of the router Client: Tap to view information about connected devices Settings: Click Setup to enter the detailed LAN port parameter settings



MAC: 1A:2B:3C:4D:5F:83

IP Address: 192.168.4.1

Mask: 255.255.255.0

Local DNS: 0.0.0.0

DHCP: Enable

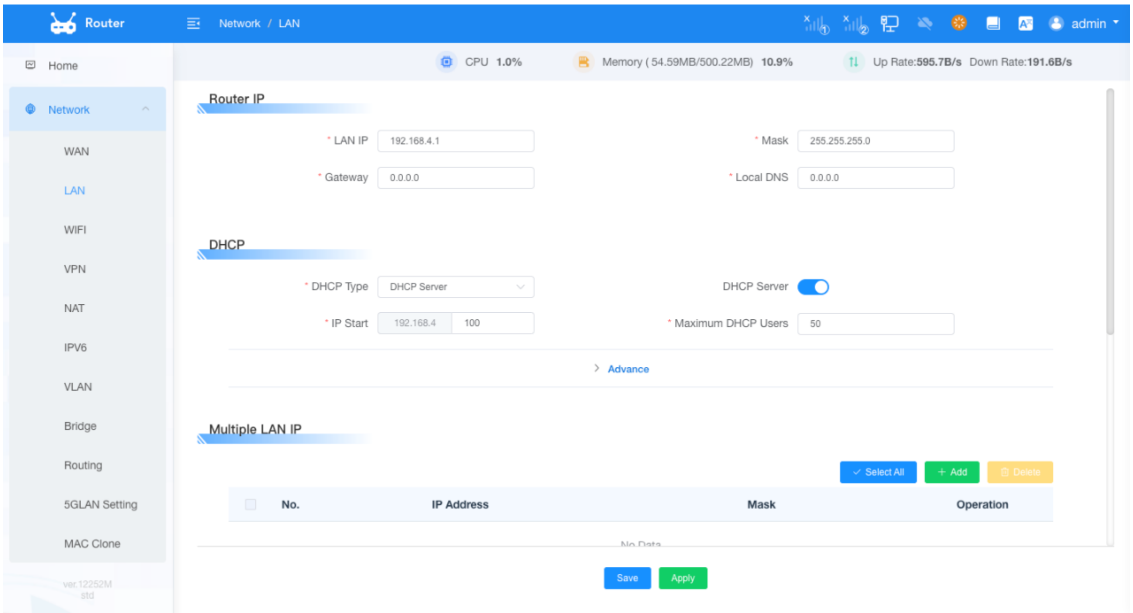
IP Start: 192.168.4.100

IP End: 192.168.4.150

Devices: 0

Click to view the device

Click Setup to view the configuration:



CPU 1.0% Memory (54.59MB/500.22MB) 10.9% Up Rate:595.7B/s Down Rate:191.6B/s

Router IP

* LAN IP 192.168.4.1 * Mask 255.255.255.0

* Gateway 0.0.0.0 * Local DNS 0.0.0.0

DHCP

* DHCP Type DHCP Server DHCP Server ●

* IP Start 192.168.4 100 * Maximum DHCP Users 50

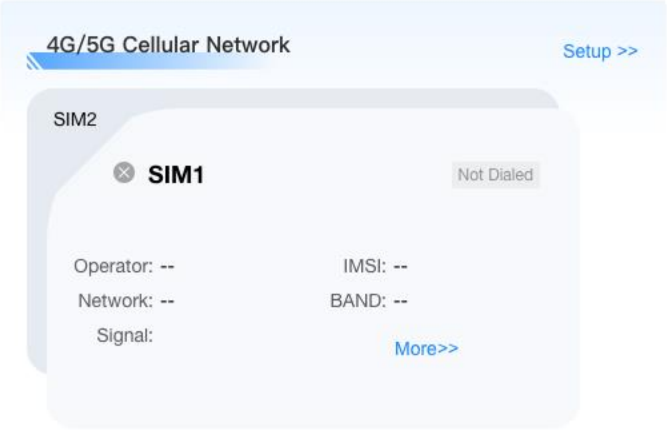
Multiple LAN IP

□	No.	IP Address	Mask	Operation

No Data

4G/5G Cellular:

When the main link is set to cellular, if the dial is successful, the relevant cellular information will be displayed, click more to view the detailed cellular information, if the main link is set to wired mode, then there is no dial there and no relevant cellular information can be seen



4G/5G Cellular Network

SIM2

SIM1 Not Dialed

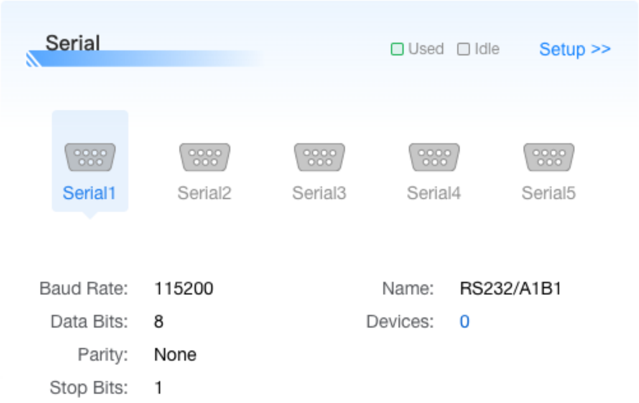
Operator: -- IMSI: --

Network: -- BAND: --

Signal:

Serial Ports

When there is a connected device on the serial port and a sub-device is successfully added, the color of the serial port is green, otherwise it is gray. The parameters of each serial port are displayed at the bottom, as well as the number of connected devices, click to view the details



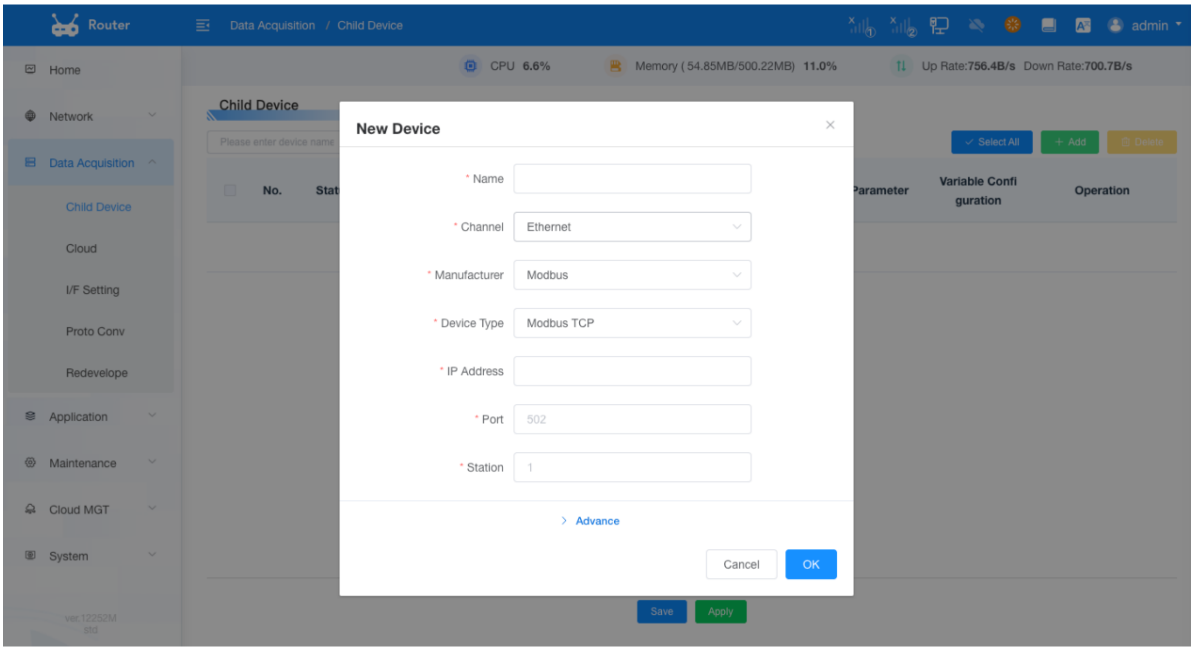
Baud Rate: 115200
Data Bits: 8
Parity: None
Stop Bits: 1
Name: RS232/A1B1
Devices: 0

3.6 Data Acquisition

3.6.1 Child Device

On this page, you need to add a device, for example, the device is connected to a temperature and humidity sensor, and the device with a temperature and humidity sensor is added here, and the device is added to the MODBUS RTU-based sensor docking.

(1) Add the device, the device name is recommended in English, because it needs to be transmitted to the MQTT server later, as shown in the figure

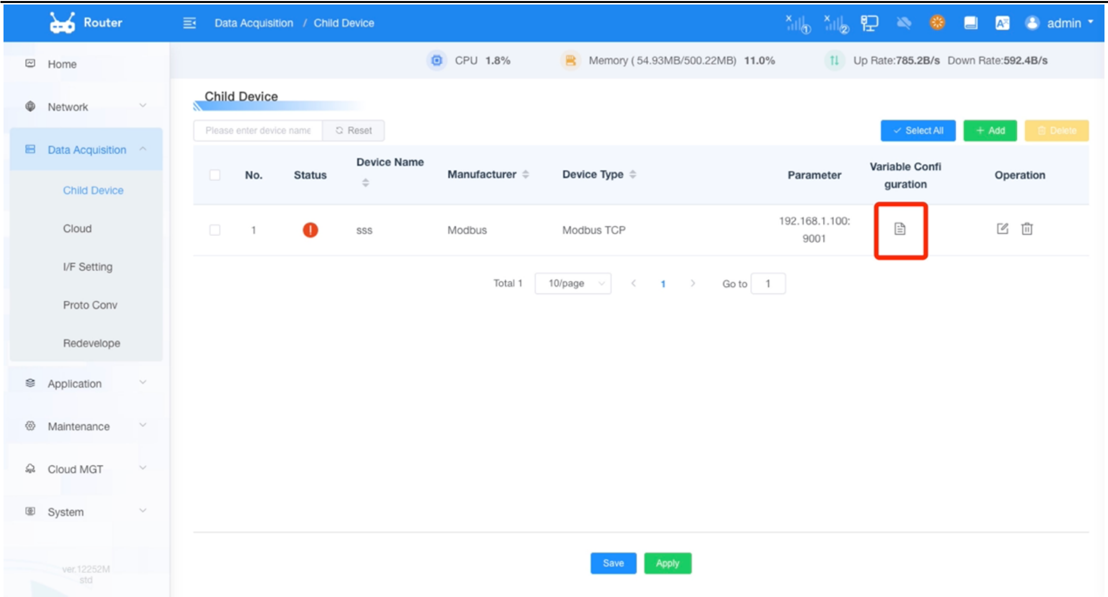


CPU 6.6%
Memory (54.85MB/500.22MB) 11.0%
Up Rate:756.4B/s Down Rate:700.7B/s

New Device

* Name:
* Channel: Ethernet
* Manufacturer: Modbus
* Device Type: Modbus TCP
* IP Address:
* Port: 502
* Station: 1

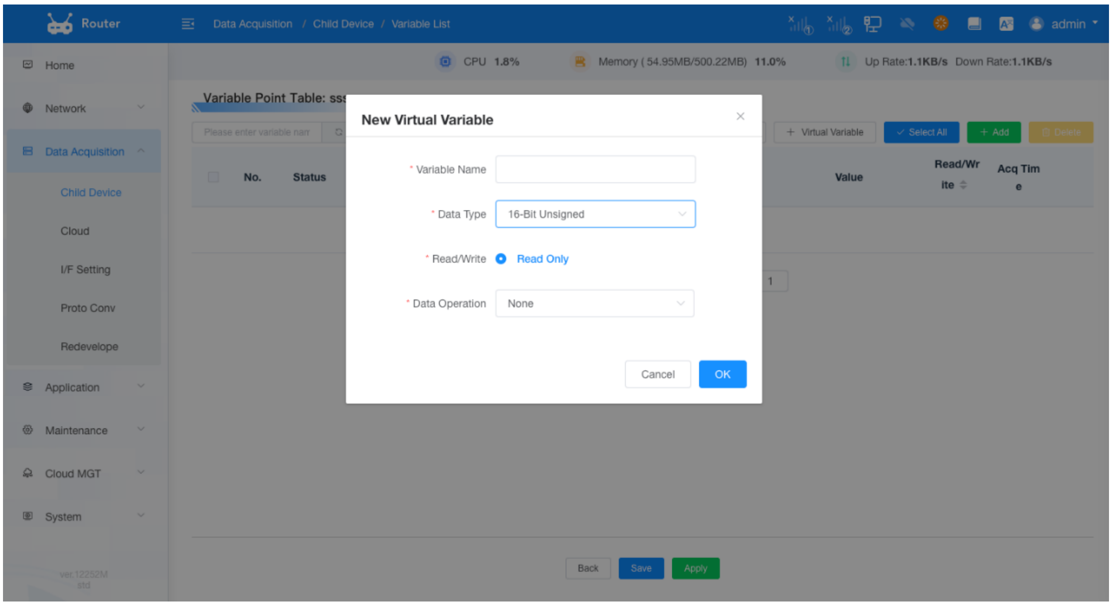
(2) Add variables to the device, because there are many variables that need to be reported under a sensor or a certain device, as shown in the figure



CPU 1.8% Memory (54.93MB/500.22MB) 11.0% Up Rate:785.2B/s Down Rate:592.4B/s

Child Device

□	No.	Status	Device Name	Manufacturer	Device Type	Parameter	Variable Configuration	Operation
□	1	!	sss	Modbus	Modbus TCP	192.168.1.100:9001		



CPU 1.8% Memory (54.95MB/500.22MB) 11.0% Up Rate:1.1KB/s Down Rate:1.1KB/s

Variable Point Table: sss

New Virtual Variable

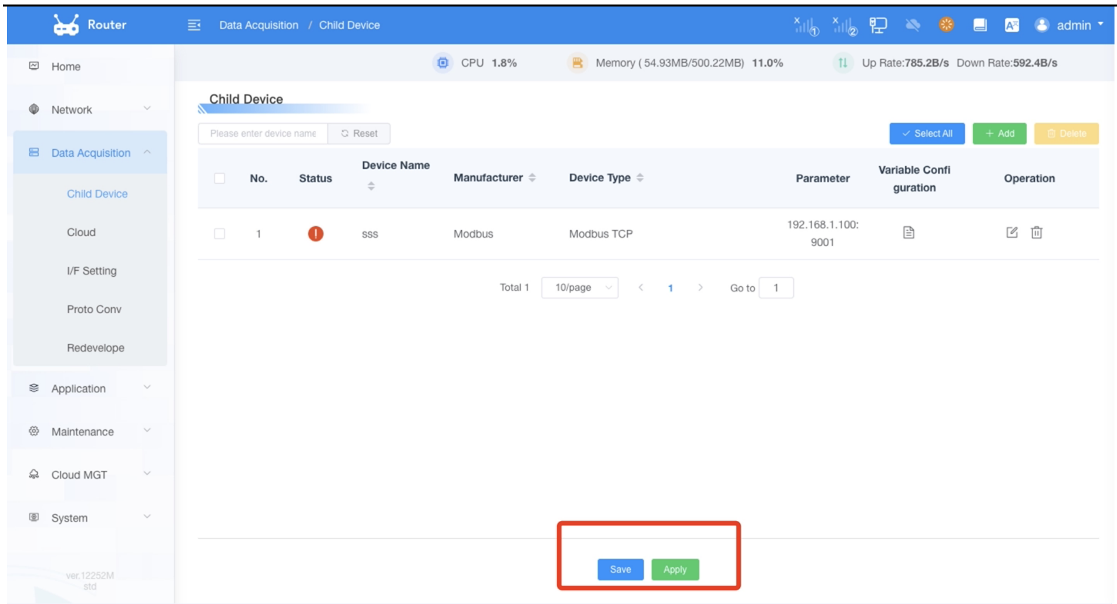
* Variable Name

* Data Type 16-Bit Unsigned

* Read/Write ● Read Only

* Data Operation None

Cancel OK

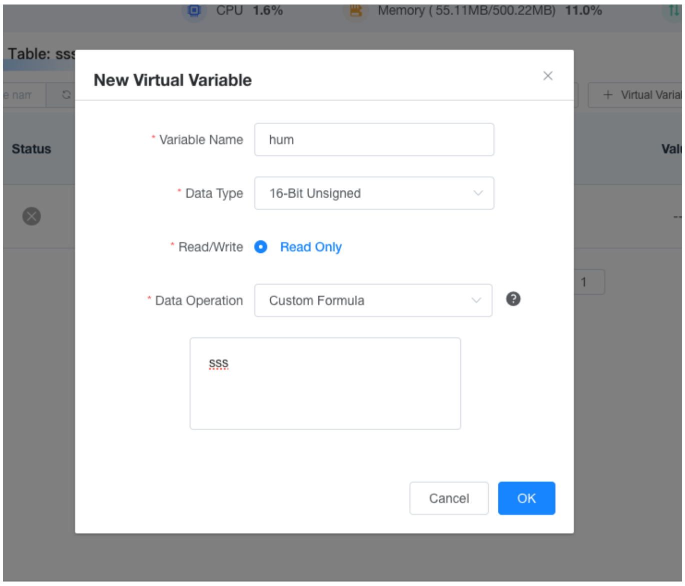


	No.	Status	Device Name	Manufacturer	Device Type	Parameter	Variable Configuration	Operation
□	1	!	sss	Modbus	Modbus TCP	192.168.1.100: 9001		

Remember to use the name of the variable in English, because the name here needs to be reported to the MQTT server, and other parameters can be set according to the MODBUS RTU parameters of the device.

(3) After adding the device and adding the variables, you can send MQTT data, please see the cloud service section for MQTT.

(4) When you click Edit Variable, you can convert the data collected by the variable to the following operations: Select a custom formula to convert the data through the variable * magnification ± offset value, as shown in the figure (click Help for more details)



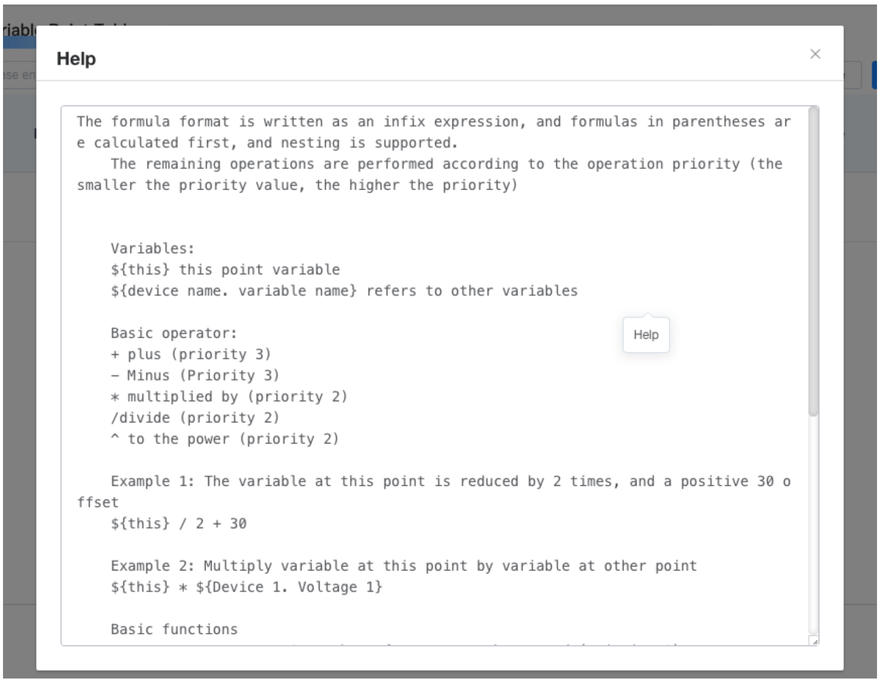
* Variable Name: hum

* Data Type: 16-Bit Unsigned

* Read/Write: ● Read Only

* Data Operation: Custom Formula

sss



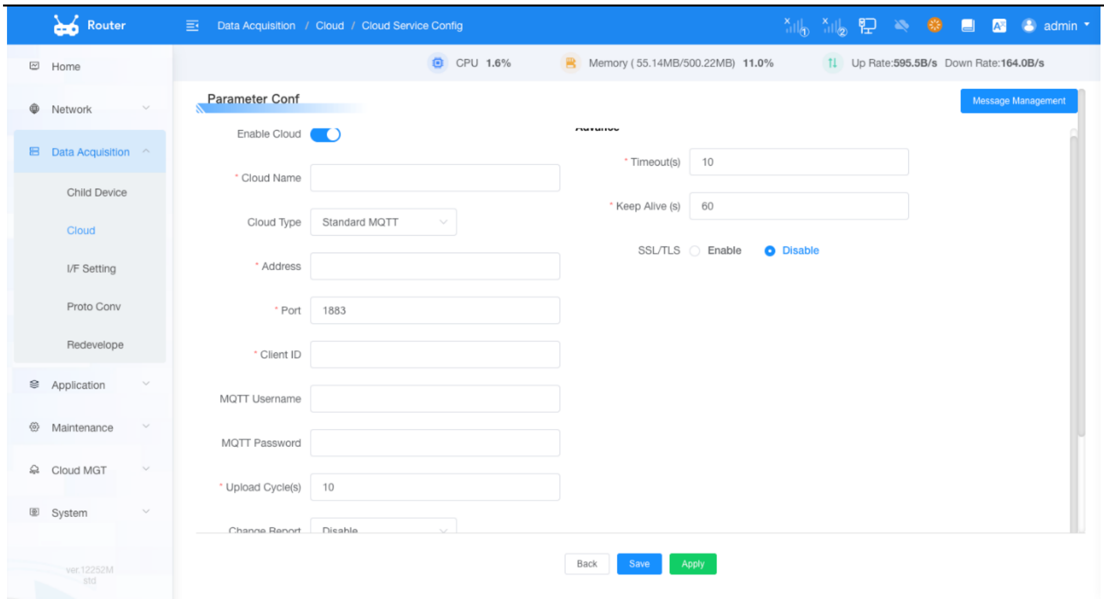
```
The formula format is written as an infix expression, and formulas in parentheses ar
e calculated first, and nesting is supported.
    The remaining operations are performed according to the operation priority (the
smaller the priority value, the higher the priority)


    Variables:
    ${this} this point variable
    ${device name. variable name} refers to other variables

    Basic operator:
    + plus (priority 3)
    - Minus (Priority 3)
    * multiplied by (priority 2)
    /divide (priority 2)
    ^ to the power (priority 2)

    Example 1: The variable at this point is reduced by 2 times, and a positive 30 o
ffset
    ${this} / 2 + 30

    Example 2: Multiply variable at this point by variable at other point
    ${this} * ${Device 1. Voltage 1}

    Basic functions
```

3.6.2 Cloud Service

This page adds MQTT server forwarding to the device, and forwards the variable data of the variable monitoring module to the MQTT server so that the platform can subscribe to it. There are 2 steps in total about this module

1. Add an MQTT Server

Add an MQTT server, fill in the server parameters, such as server address, port, account and password (if necessary), select the topic you want to subscribe to or publish (the topic is set in the message management in the upper right corner), and then click Apply, as shown in the figure



CPU 1.6%   Memory (55.14MB/500.22MB) 11.0%   Up Rate:595.5B/s Down Rate:164.0B/s

Parameter Conf

Enable Cloud: on

* Cloud Name:

Cloud Type: Standard MQTT

* Address:

* Port: 1883

* Client ID:

MQTT Username:

MQTT Password:

* Upload Cycle(s): 10

Change Report: Disable

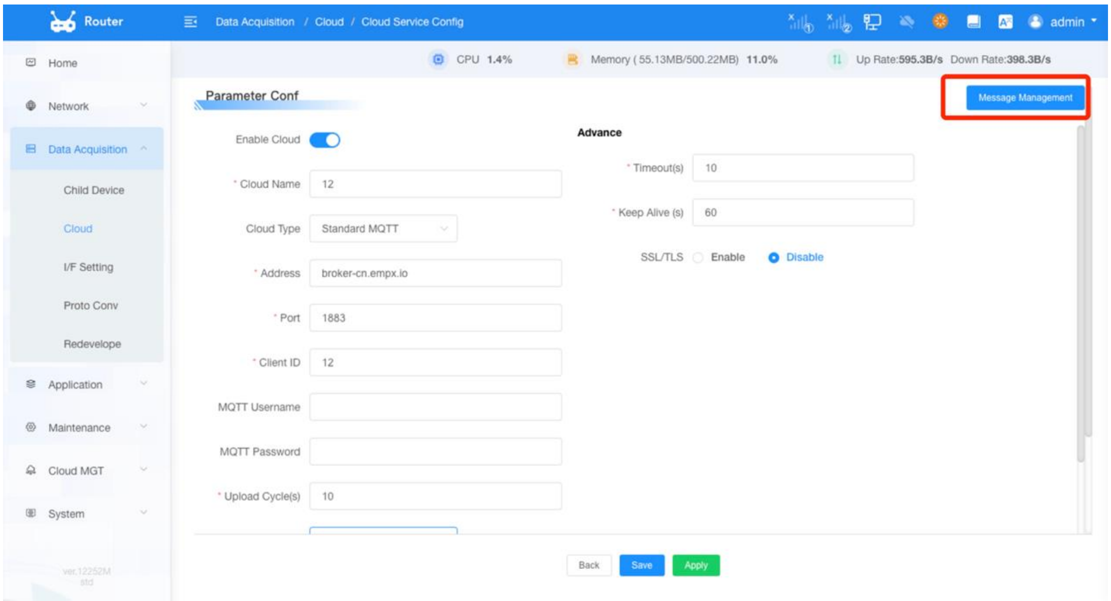
Advance

* Timeout(s): 10

* Keep Alive (s): 60

SSL/TLS: ○ Enable ● Disable

When selecting a cloud platform type, you can use standard MQTT as normal, and use the rest to interconnect with Ali Cloud and HUAWEI Cloud.



CPU 1.4%   Memory (55.13MB/500.22MB) 11.0%   Up Rate:595.3B/s Down Rate:398.3B/s

Parameter Conf

Enable Cloud: on

* Cloud Name: 12

Cloud Type: Standard MQTT

* Address: broker-cn.empx.io

* Port: 1883

* Client ID: 12

MQTT Username:

MQTT Password:

* Upload Cycle(s): 10

Advance

* Timeout(s): 10

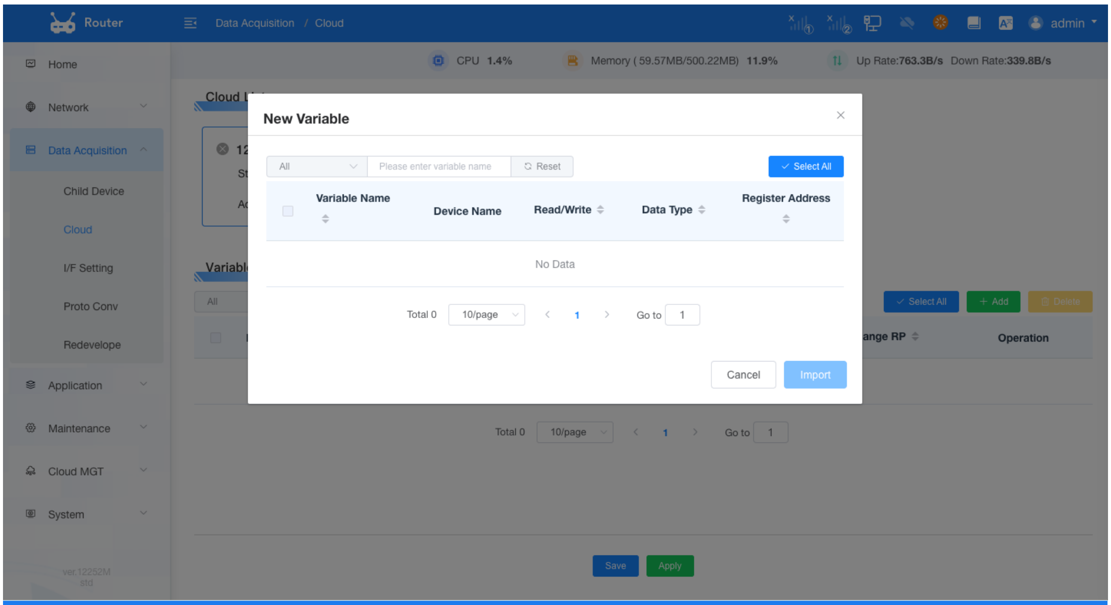
* Keep Alive (s): 60

SSL/TLS: ○ Enable ● Disable

1. The data cache in the page means that when the device is offline, the collected point data will be stored in the memory first, and the offline content will be sent when the device is online
2. Clear reported data: This indicates that if necessary, disable the cache clear function, and the data that can be downloaded from the device to the cache database.

2. Import Variables

After adding the MQTT server, you need to import variables to report data to the MQTT server, as shown in the figure.



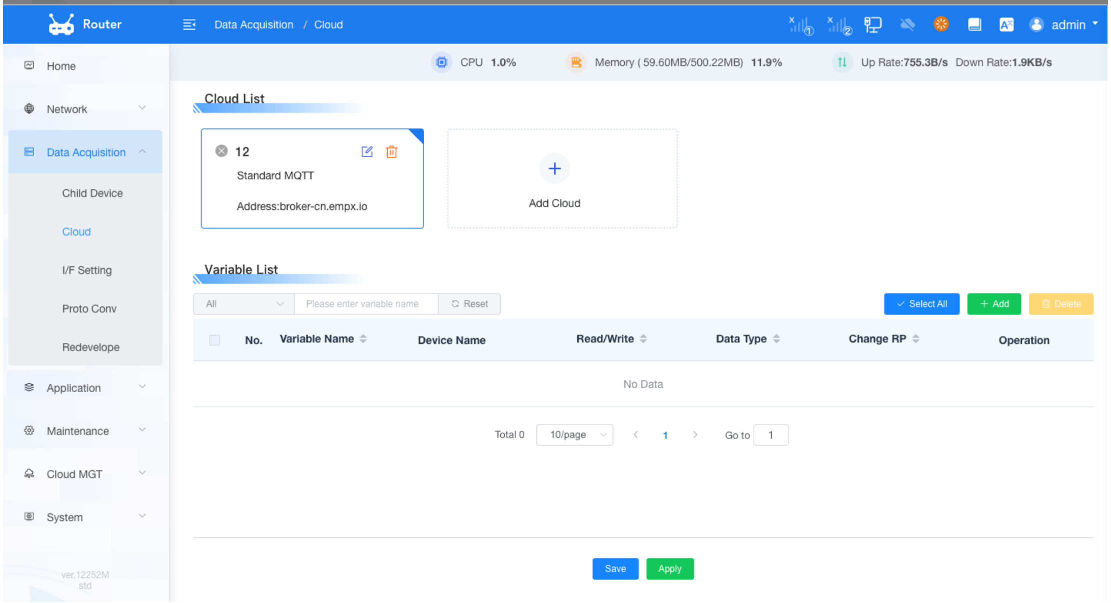
New Variable

All | Please enter variable name | Reset | ✓ Select All

□	Variable Name	Device Name	Read/Write	Data Type	Register Address
No Data					

Total 0 10/page < 1 > Go to 1

Cancel Import



Cloud List

12
Standard MQTT
Address:broker-cn.empx.io

+ Add Cloud

Variable List

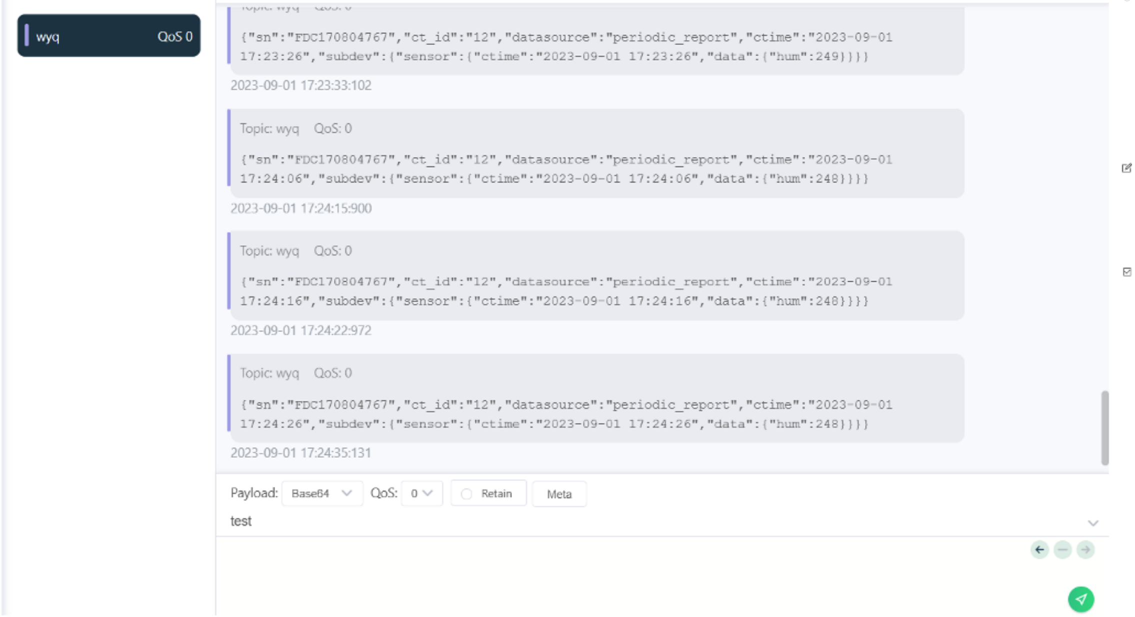
All | Please enter variable name | Reset | ✓ Select All | + Add | Delete

□	No.	Variable Name	Device Name	Read/Write	Data Type	Change RP	Operation
No Data							

Total 0 10/page < 1 > Go to 1

Save Apply

Finally, you can go to the MQTT server to subscribe to the device data, as shown in the figure



```
Topic: wyq QoS: 0
{"sn":"FDC170804767","ct_id":"12","datasource":"periodic_report","ctime":"2023-09-01
17:23:26","subdev":{"sensor":{"ctime":"2023-09-01 17:23:26","data":{"hum":249}}}}
2023-09-01 17:23:33:102

Topic: wyq QoS: 0
{"sn":"FDC170804767","ct_id":"12","datasource":"periodic_report","ctime":"2023-09-01
17:24:06","subdev":{"sensor":{"ctime":"2023-09-01 17:24:06","data":{"hum":248}}}}
2023-09-01 17:24:15:900

Topic: wyq QoS: 0
{"sn":"FDC170804767","ct_id":"12","datasource":"periodic_report","ctime":"2023-09-01
17:24:16","subdev":{"sensor":{"ctime":"2023-09-01 17:24:16","data":{"hum":248}}}}
2023-09-01 17:24:22:972

Topic: wyq QoS: 0
{"sn":"FDC170804767","ct_id":"12","datasource":"periodic_report","ctime":"2023-09-01
17:24:26","subdev":{"sensor":{"ctime":"2023-09-01 17:24:26","data":{"hum":248}}}}
2023-09-01 17:24:35:131
```

Payload: Base64 QoS: 0 ○ Retain Meta

test

MQTT format

{"sn":"FDC170804767","ct_id":"12","datasource":"periodic_report","ctime":"2023-09-01 17:26:16","subdev":{"sensor":{"ctime":"2023-09-01 17:26:16","data":{"hum":248}}}}

The above is the format of publishing data to an MQTT server through a cloud service

The fields have the following meanings:

SN: SN of the router

ctime: the collection time

Sensor: The sensor here is the device name, if the name is other, the other will be displayed, so it is recommended to use the English name when adding the device

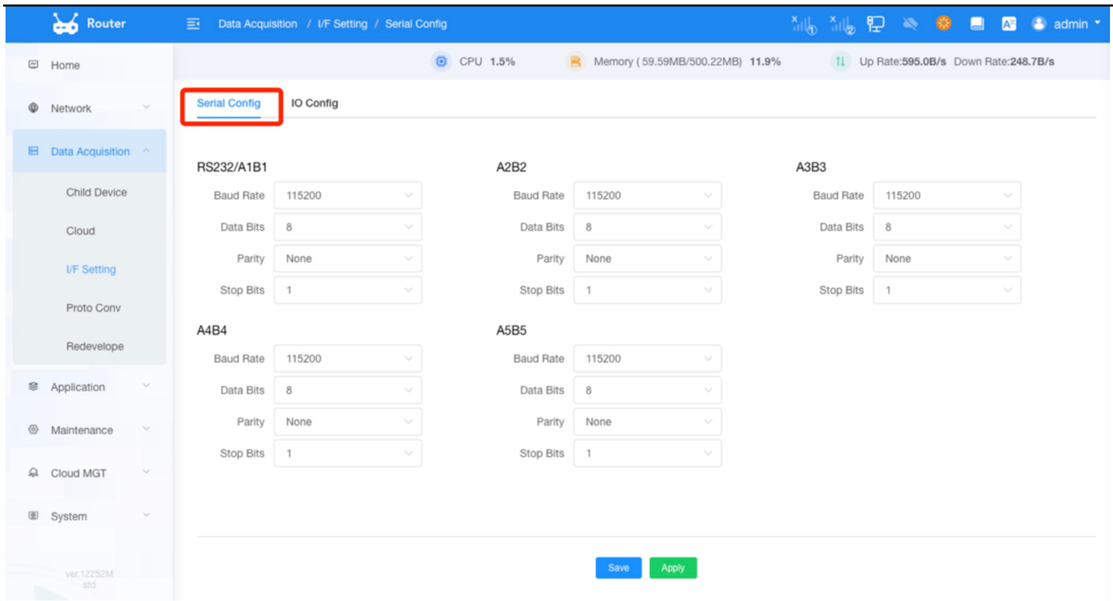
data: the nest of collected data

hum: This is the variable, and the variable name is different here

3.6.3 Interface Setting

3.6.3.1 Serial Ports Parameter

When the device is connected to the sub-device through the serial port, you need to set the serial port parameters, remember that you need to set the same serial port parameters as the connected sub-device to send and receive serial port data, and remember to click Apply after the parameters are set.



CPU 1.5% Memory (59.59MB/500.22MB) 11.9% Up Rate:595.0B/s Down Rate:248.7B/s

RS232/A1B1

Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1

A2B2

Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1

A3B3

Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1

A4B4

Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1

A5B5

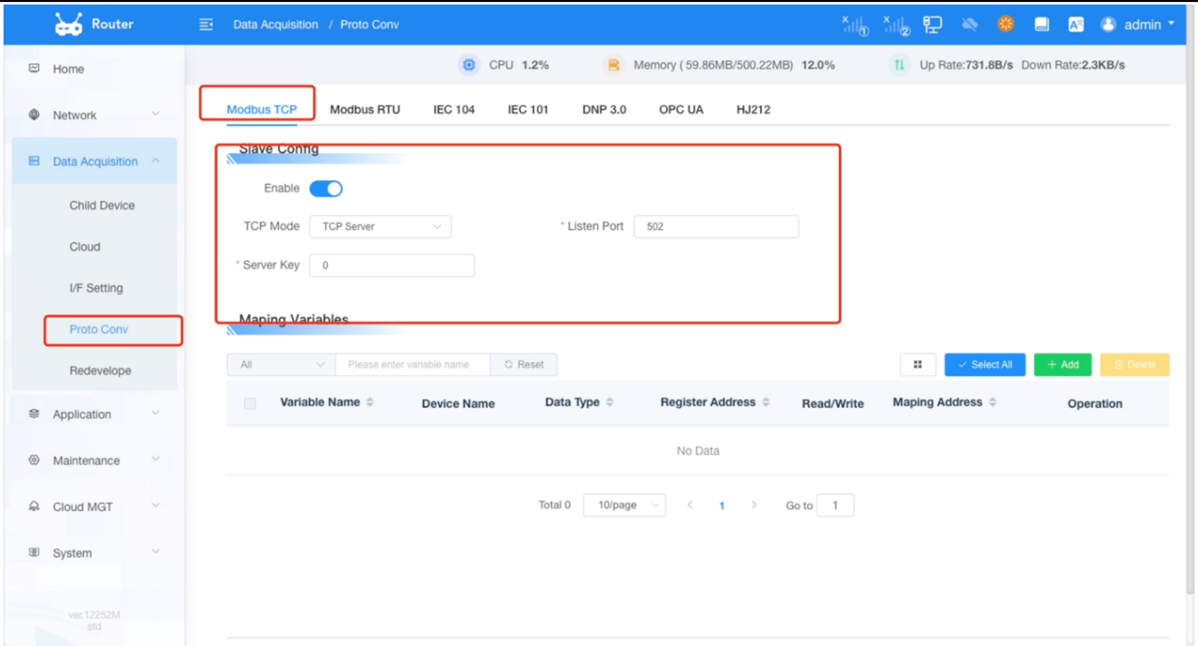
Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1

If you do not know the detailed parameters of the docking sub-device, you can perform the following tests, in most serial port equipment, the basic use of 8N1 mode, that is, 8 data bits, 1 stop bit, no verification.

3.6.4 Protocol Conversion

The main function of the protocol conversion is to convert the device data collected as the master into slave data, and then connect to other devices for transmission, here is also the sensor data collected based on modbus RTU mentioned above as an example, the sensor data has been collected as the master station, and it needs to be sent as a slave here, and the operation is as follows

(1) Select modbus TCP and set the port and station number, that is, the slave address. The IP address of modbus TCP is the local IP address, as shown in the figure



Enable: on

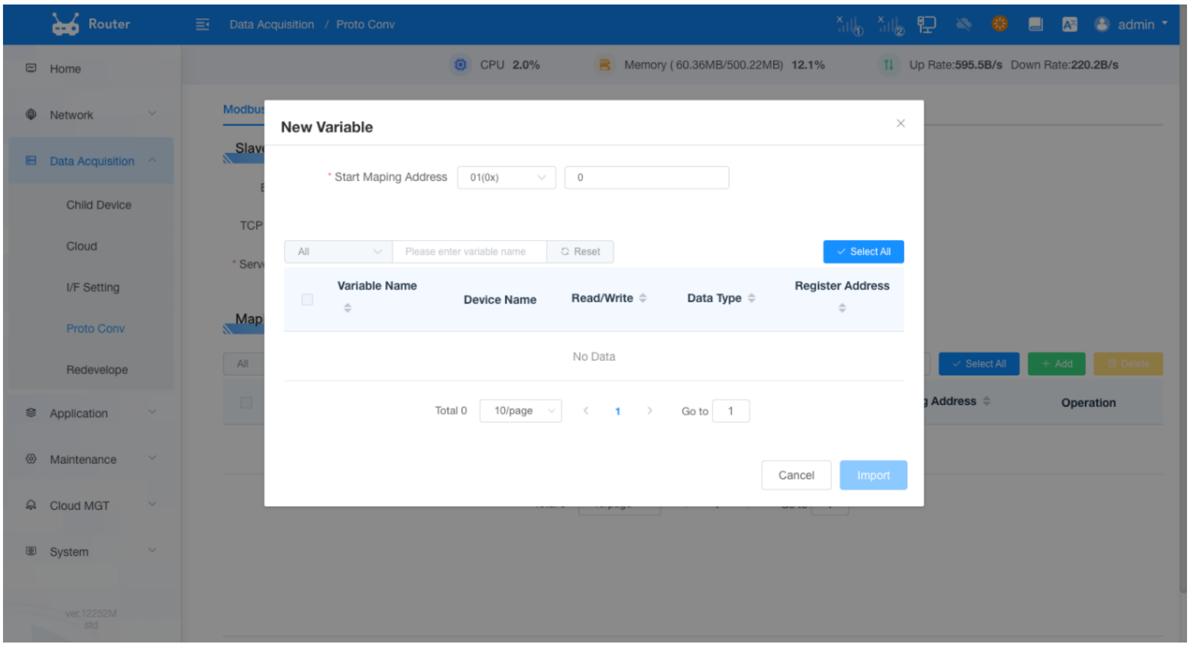
TCP Mode: TCP Server

* Listen Port: 502

* Server Key: 0

	Variable Name	Device Name	Data Type	Register Address	Read/Write	Maping Address	Operation

(2) The map point table, if used as the master station to collect data based on modbusRTU, is shown in the figure



* Start Maping Address: 01(0x) 0

	Variable Name	Device Name	Read/Write	Data Type	Register Address

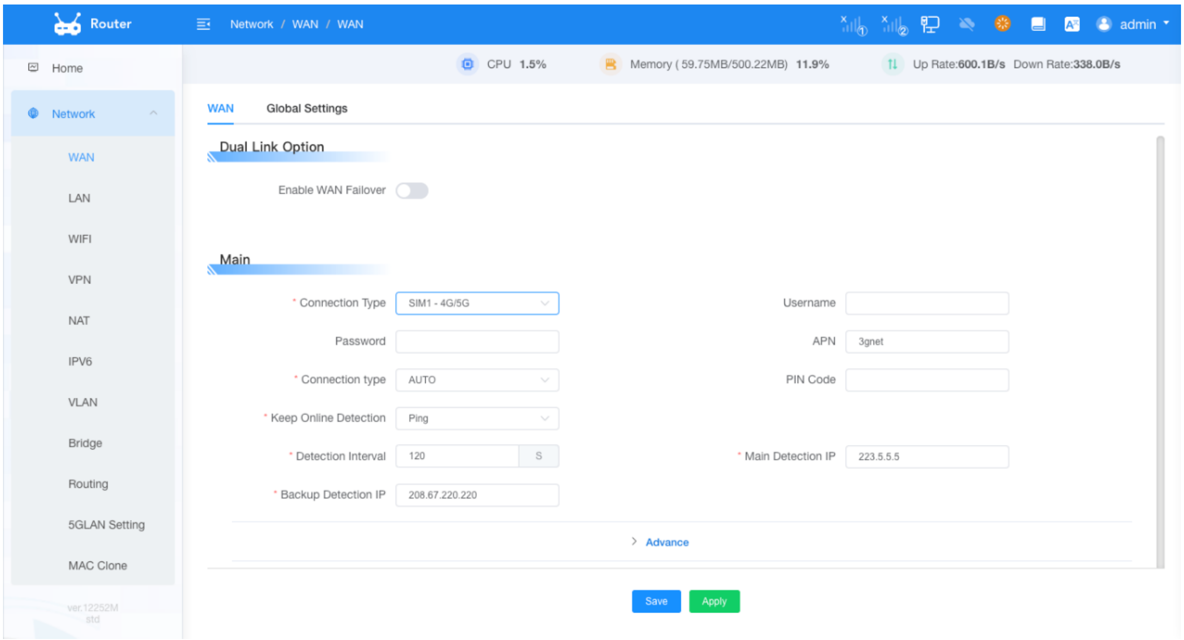
Import the device and click Apply.

1. If modbusRTU is used as a master, modbusTCP is required as a slave, and modbusRTU is required as a slave if modbusTCP is used as a master.
2. The rest of IEC104, IEC01, DNP3.0, OPCUA, etc. are the same, the basic principle of the setting is to report the sensor data collected in the southbound direction as the data converted into a standard protocol field by the slave station to other devices, and it is still used as the southbound interface of the connected equipment in the original sense.

3.7 Network

3.7.1 WAN

3.7.1.1 WAN



CPU 1.5%   Memory (59.75MB/500.22MB) 11.9%   Up Rate:600.1B/s Down Rate:338.0B/s

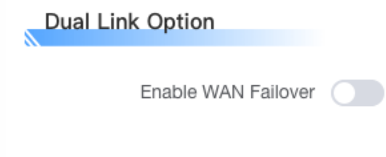
Dual Link Option

Enable WAN Failover ○

Main

* Connection Type: SIM1 - 4G/5G
Username:
Password:
APN: 3gnet
* Connection type: AUTO
PIN Code:
* Keep Online Detection: Ping
* Detection Interval: 120 S
* Main Detection IP: 223.5.5.5
* Backup Detection IP: 208.67.220.220

Dual Link Option


Dual Link Option

Enable WAN Failover ○

Enable the dual-link backup function, that is, whether to enable two links, so that the route has the dual-link function, and if it is disabled, only one link, that is, the primary link, is enabled, and the backup link does not work. If you click Enable to display the Dual-Link Simultaneous Online configuration option, this option means as follows:

Enabled: When the primary link goes online, all default data is sent to the Internet network through the primary link. If the primary link goes offline, the backup link is online, and the default data is sent to the Internet network through the backup link, and the primary link tries to connect continuously, and if the primary link is connected again, it switches to the primary link again. In general, it is the function of primary link priority and backup link backup.

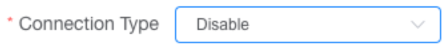
Note: If the load balancing and load distribution functions are enabled online at the same time, please refer to the load balancing menu for detailed data direction description.

Note: When the dual-link backup function is enabled, if the connection type in the "Primary Link Connection Type" and "Backup Link Connection Type" is set to "Static IP" or "DHCP", you must configure the corresponding online keep-alive function. The Primary Link Connection Type and Backup Link Connection Type cannot be the same, and the same physical WAN egress cannot be selected.

Main/Backup

Select the Internet connection type from the drop-down menu, the WAN connection type includes 8 ways: Disable, Static IP, Auto-Provision-DHCP, PPPOE, SIM1-4G/5G, SIM2-4G/5G, SIM1-3G/UMTS/4G/LTE, SIM2-3G/UMTS/4G/LTE.

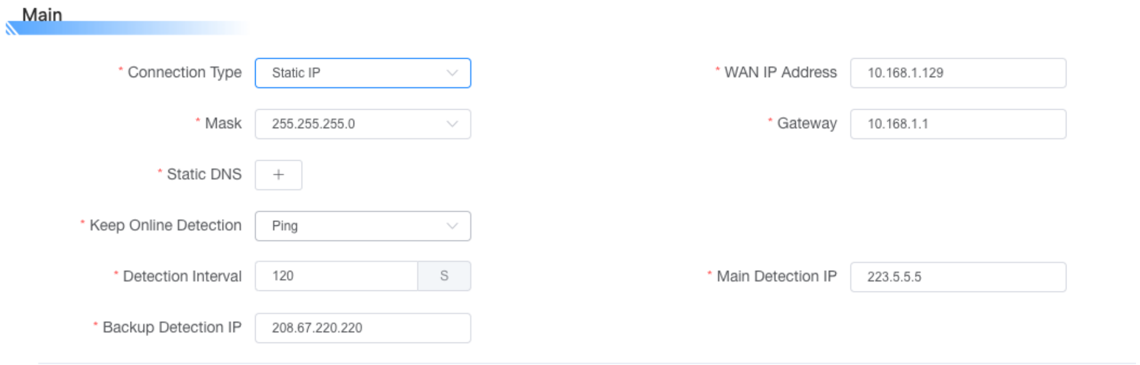
Method 1: Disable



* Connection Type: Disable

Disables connection type setting for WAN ports

Method 2: Static IP



Main

* Connection Type: Static IP
* WAN IP Address: 10.168.1.129
* Mask: 255.255.255.0
* Gateway: 10.168.1.1
* Static DNS: +
* Keep Online Detection: Ping
* Detection Interval: 120 S
* Main Detection IP: 223.5.5.5
* Backup Detection IP: 208.67.220.220

This type of connection is usually used for private line access, such as business fiber. The broadband service provider will provide you with detailed parameters such as IP address, subnet mask, router and DNS, which you will need to set on your 5G router.

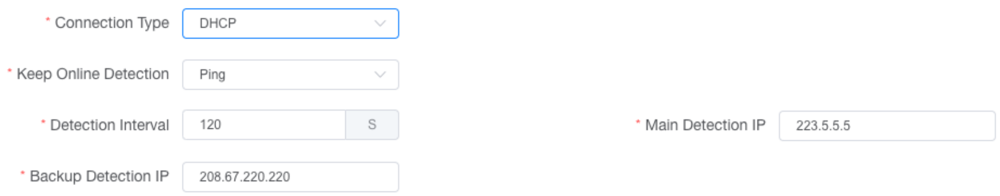
WAN IP address: The IP address that the user sets based on their own or ISP assignments

Subnet Mask: The subnet mask set by the user based on their own or ISP assignment

Gateway: The gateway set by the user based on their own or ISP assignment

Static DNS: A static DNS that users set up based on their own or ISP assignments

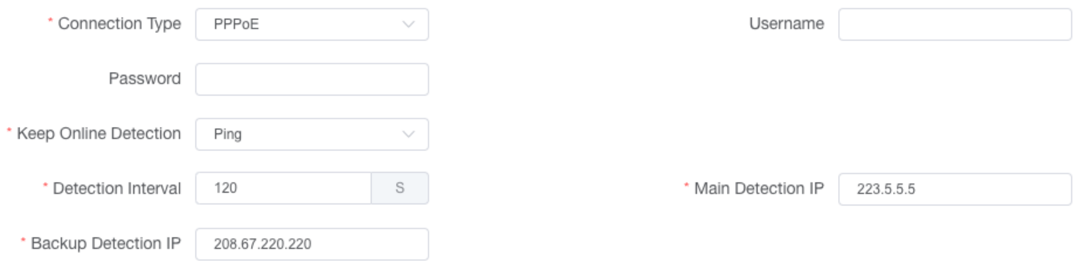
Method 3: DHCP



* Connection Type	DHCP		
* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

Cable television (Cable) and some cell broadband use this connection. The IP address of the WAN port is obtained by DHCP

Method 4: PPPOE



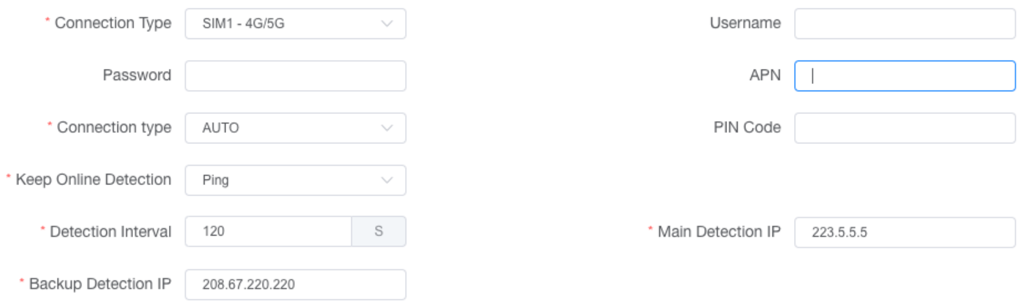
* Connection Type	PPPoE	Username	
Password			
* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

This type of connection is typically used by China Telecom and China Netcom ADSL broadband services, as well as by some other broadband service providers. The PPPoE connection type requires your ISP to provide you with a username and password, which needs to be set up on the 5G router.

Username: The username used to log in to the Internet.

Password: The password used to log in to the Internet.

Method 5: 4G/5G



* Connection Type	SIM1 - 4G/5G	Username	
Password		APN	|
* Connection type	AUTO	PIN Code	
* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

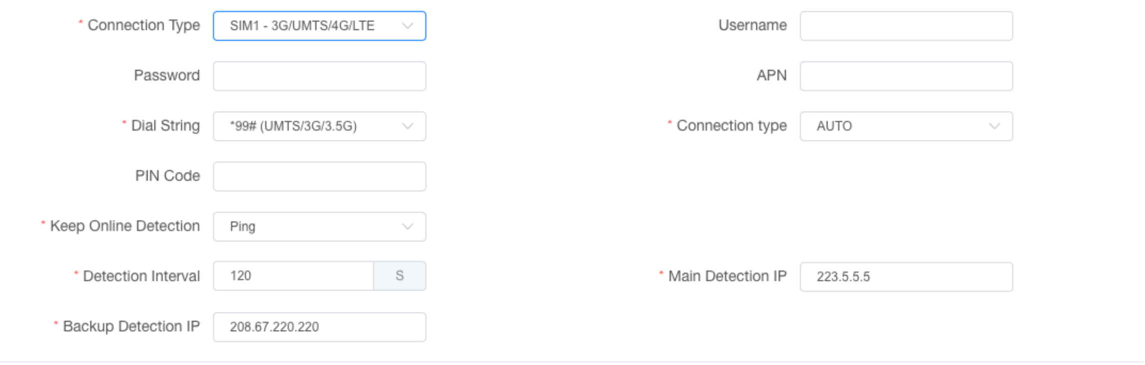
Username: The username used to log in to the Internet

Password: The password used to log in to the Internet

APN: The name of the access point

PIN: The PIN code provided by the SIM card

Method 6: 3G/UMTS/4G/LTE



* Connection Type	SIM1 - 3G/UMTS/4G/LTE	Username	
Password		APN	
* Dial String	*99# (UMTS/3G/3.5G)	* Connection type	AUTO
PIN Code			
* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

Username: The username used to log in to the Internet.

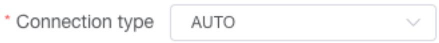
Password: The password used to log in to the Internet.

Call Center Number: The calling number to the carrier.

APN : Access Point Name.

PIN: The PIN code provided by the SIM card

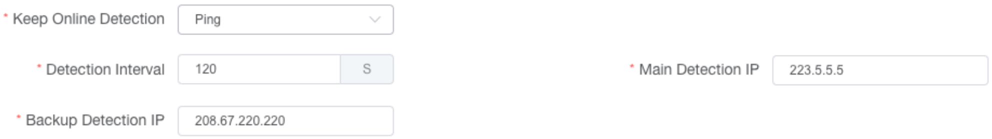
Connection Type



* Connection type: AUTO

Network selection: including automatic mode, force to 3G, force to 2G, 3G priority, 2G priority and other methods, if used 5G modules, the corresponding 5G network options will be added, and they can be selected according to user needs and different module types

Keep Online



* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

The online hold feature is used to detect if the Internet link is active. If this is set, the 5G router will automatically detect the Internet link, and once it detects that the link is disconnected or invalid, the system will automatically reconnect and re-establish a valid link. If the network environment is poor, or in the case of a private network, it is recommended to use the 5G route mode.

Keep Online Detection:

None: Does not use the online hold feature.

Ping: Sends a ping packet to detect the link. If this is set, the Hold Online Detection Interval, Hold Detect Primary IP, and Hold Detect Secondary Server IP must also be configured correctly.

Route: If you use route mode to detect links, you must also correctly configure the Online Hold Detection Interval, Online Hold Detection Primary Server IP, and Online

Hold Detect Secondary Server IP Addresses.

TCP: If you use TCP mode to detect links, if you set this mode, you must also correctly configure the "Online Hold Detection Interval", "Online Hold Detect Primary Server IP", "Online Hold Detect Secondary Server IP" configuration items, and "Check times" configuration items.

Detection Interval:

The time interval between two online hold detections, in seconds.

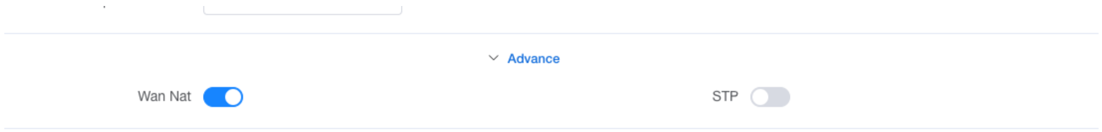
Main Detection IP:

The IP address of the primary server that responds to the 5G router inspecting packets online. Only if the "Online Hold Mode" is set to This configuration item is valid only when Ping or Route is used.

Backup Detection IP:

The IP address of the secondary server that responds to the 5G router's online detection packet. Only if the "Online Hold Mode" is set to This configuration item is valid only when Ping or Route is used.

Advance



Advance

Wan Nat ●

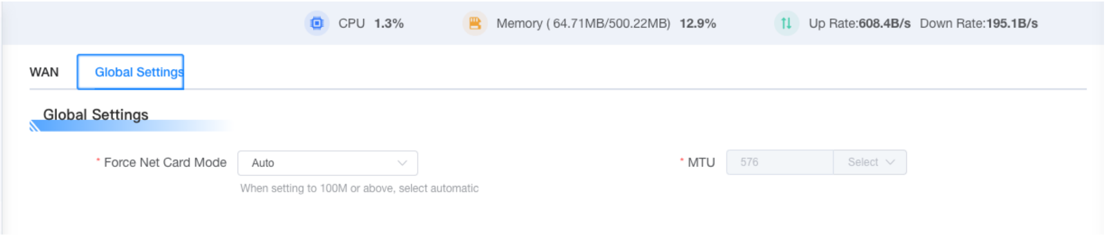
STP ○

Manually set up WAN IP/Gateway:

If enabled, you can manually set the IP address and gateway address of the WAN port.

STP (Spanning Tree Protocol) is an abbreviation for Spanning Tree Protocol. This protocol can be applied to the loop network, and the path redundancy is realized through a certain algorithm, and the loop network is pruned into a loop-free tree network, so as to avoid the proliferation and infinite loop of packets in the loop network.

3.7.1.2 Global Setting



CPU 1.3% Memory (64.71MB/500.22MB) 12.9% Up Rate:608.4B/s Down Rate:195.1B/s

WAN | Global Settings

Global Settings

* Force Net Card Mode: Auto

When setting to 100M or above, select automatic

* MTU: 576 Select

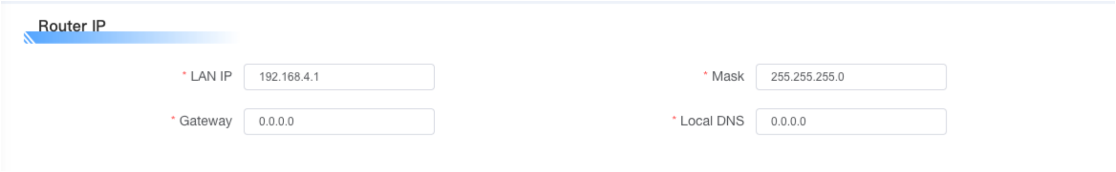
Forced Net Card Mode:

The default is automatic, which can be set to 10M and 100M;

Assign the WAN port as the switching port:

This configuration allows you to set the device's WAN to a LAN

3.7.2 LAN



Router IP

* LAN IP 192.168.4.1

* Mask 255.255.255.0

* Gateway 0.0.0.0

* Local DNS 0.0.0.0

Router IP

LAN IP:

Represents the 5G router IP address that can be seen by your local area network

Subnet Mask:

Represents a 5G router IP address subnet mask that can be seen by your local area network.

Gateway:

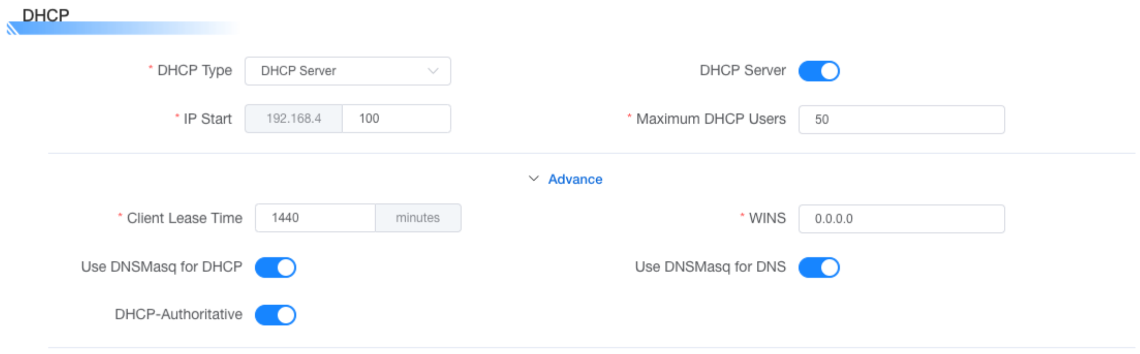
Set the router inside the 5G router, if the default setting, the internal router is the address of the 5G router itself

Local DNS:

DNS servers are automatically assigned by the carrier access server, and you can choose to use these reliable DNS servers if you have your own DNS servers or other stable and reliable DNS servers. Otherwise, the default setting

DHCP

These settings are used to configure the Dynamic Host Configuration Protocol (DHCP) server functionality of the 5G router. A 5G router can act as a DHCP server for the network. The DHCP server automatically assigns an IP address to each computer in the network. If you choose to enable the DHCP server option for your 5G router, you can set up all computers on your LAN to automatically get IP addresses and DNS, and ensure that there are no other DHCP services on your network



DHCP

* DHCP Type: DHCP Server

DHCP Server: ●

* IP Start: 192.168.4 | 100

* Maximum DHCP Users: 50

Advance

* Client Lease Time: 1440 minutes

* WINS: 0.0.0.0

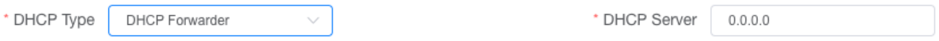
Use DNSMasq for DHCP: ●

Use DNSMasq for DNS: ●

DHCP-Authoritative: ●

DHCP type: There are two types: DHCP server and DHCP forwarder

If you set it to a DHCP forwarder, enter the DHCP server address as follows



* DHCP Type: DHCP Forwarder

* DHCP Server: 0.0.0.0

DHCP Server:

DHCP is enabled by default at the factory. If you already have a DHCP server in your network, or if you don't want a DHCP server, click Disable. If you select a DHCP forwarder, fill in the corresponding DHCP server IP.

IP Start:

Input Range 1-254 Enter a numeric value that is used as the starting value when the DHCP server assigns an IP address. Because the default IP address of this 5G router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater but smaller than 192.168.1.254. The default starting IP address is 192.168.1.100.

Maximum DHCP Users:

Enter the maximum number of computers that you want the DHCP server to assign IP addresses. This number cannot exceed 253, and the number of IP addresses plus users cannot be greater than 255, and the default value is 50.

Client lease time:

Refers to the lease period for which a network user with a dynamic IP address occupies an IP address. Enter the time in minutes, and in this way, the user "leases" the dynamic IP address. When a dynamic IP address expires, it's automatically assigned to a new dynamic IP address for the user. The default setting is 1440 minutes, which represents 1 day. The range can be set from 0-99999

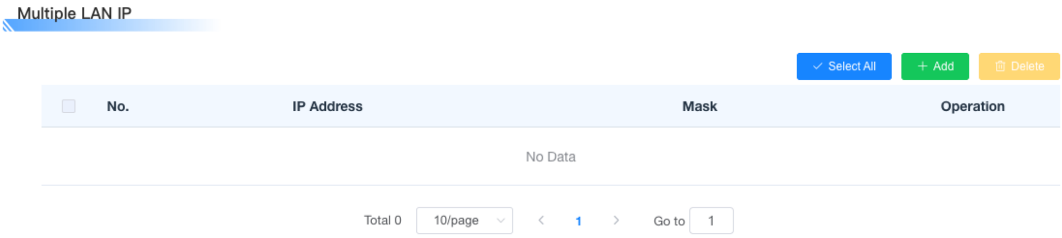
WINS：

The Windows System Internet Naming Service (WINS) manages every computer that interacts with the Internet. If you're using a WINS server, you'll enter the IP address of that server here. Otherwise, no address is filled.

DNSMasq：

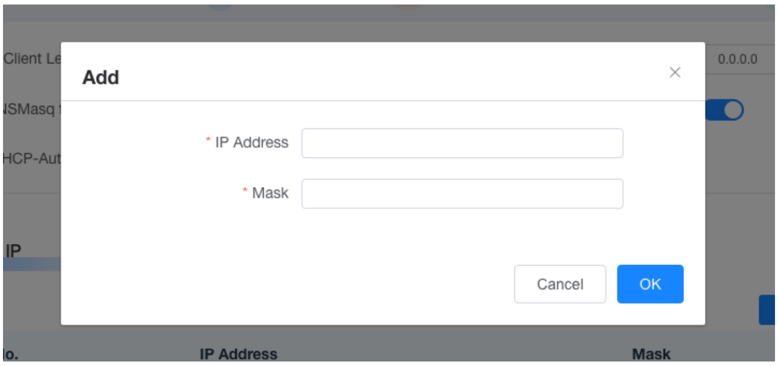
Add your domain name to the local search realm, add extended hosting options, use DNSMasq to assign IP addresses and DNS to subnets, and use the dhcpd service to provide IP addresses and DNS to subnets if you don't choose DNSMasq.

Multiple LAN IP


Multiple LAN IP

□	No.	IP Address	Mask	Operation
		No Data		

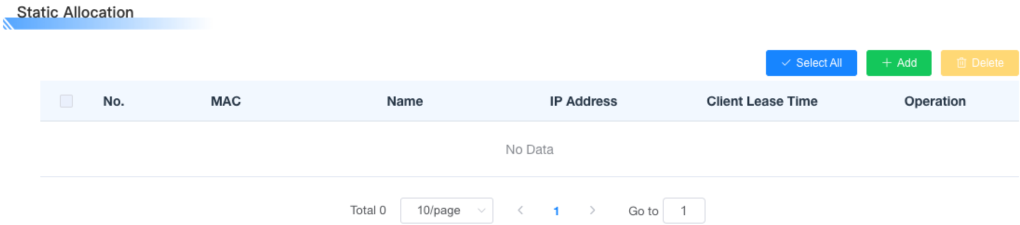
You can use the Add button to enter the corresponding IP address and subnet mask to divide multiple network segments of LAN ports, or you can choose to delete the configuration.


Add

* IP Address

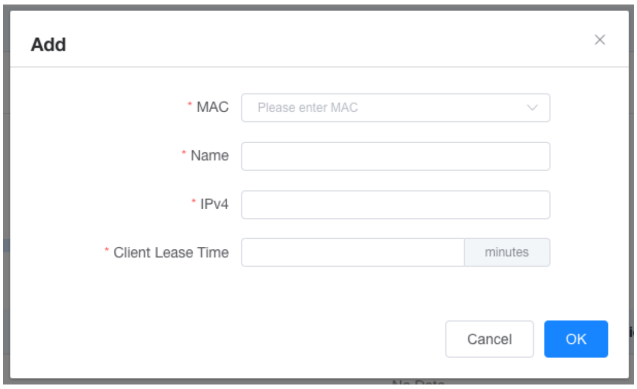
* Mask

Static Allocation


Static Allocation

□	No.	MAC	Name	IP Address	Client Lease Time	Operation
			No Data			

You can add a new device, select the MAC address of the corresponding device, set the name and IPV4 address, specify the device as a fixed IP address, and set the lease time, which will be automatically renewed by default after the terminal lease time expires.


Add

* MAC Please enter MAC

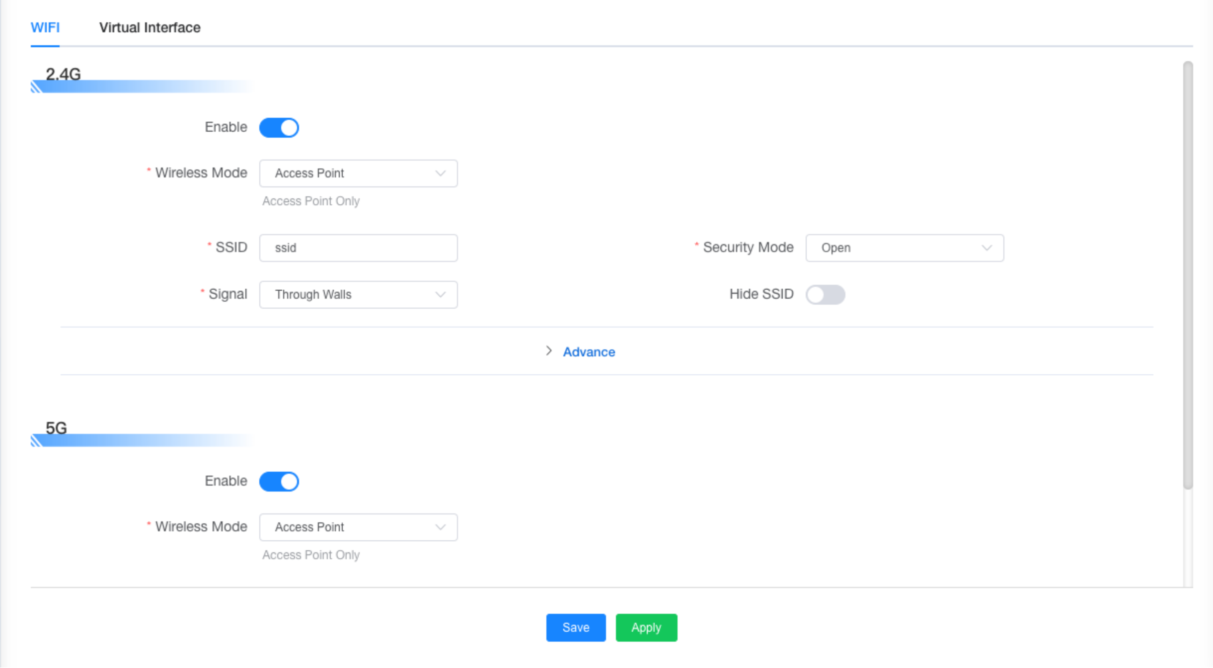
* Name

* IPv4

* Client Lease Time minutes

3.7.3 WiFi

3.7.3.1 WiFi



WIFI | Virtual Interface

2.4G

Enable: on

* Wireless Mode: Access Point
Access Point Only

* SSID: ssid

* Security Mode: Open

* Signal: Through Walls

Hide SSID: off

5G

Enable: on

* Wireless Mode: Access Point
Access Point Only

Enabled: Turn on WiFi.

Disable: Turn off WiFi.

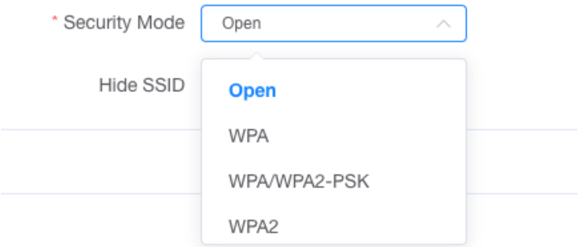
Wireless Mode:

There are four modes to choose from: access point, client, trunk, and trunk bridging.

SSID:

You can set the access point name of the wireless AP, the network name shared by all devices in the wireless network, and the SSID of all devices is the same. SSIDs are made up of numbers and letters, are case-sensitive, and must not exceed 32 characters.

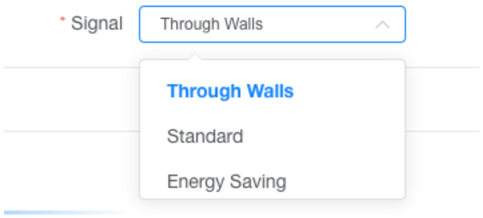
Security modes: Open, WPA, WPA/WPA2-PSK, WPA2, WPA3



* Security Mode: Open

Hide SSID

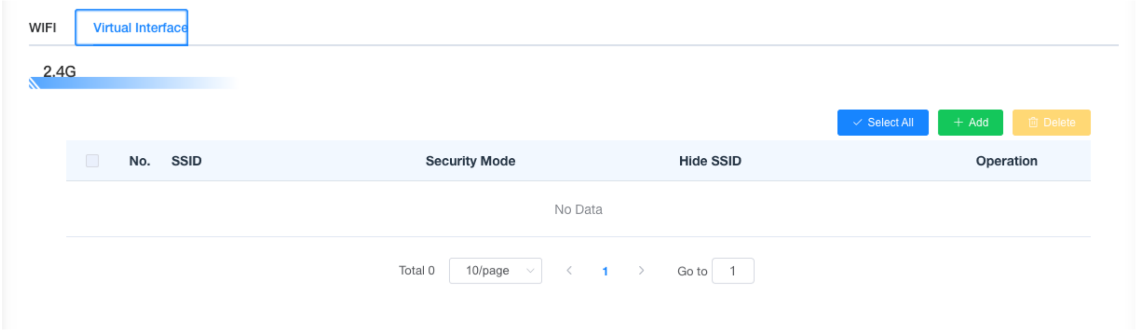
Signal strength: Through Walls, Standard, Energy Saving can be selected



* Signal: Through Walls

3.7.3.2 Virtual Interface

Click Add to add a Virtual Interface. After the Virtual Interface is added, click Remove to remove the Virtual Interface.

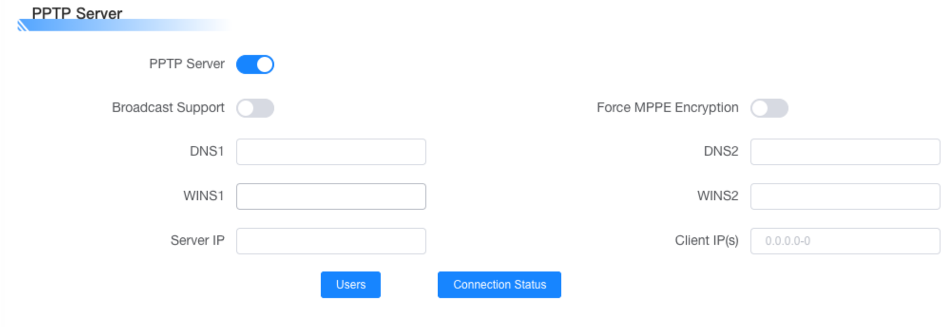


☐	No.	SSID	Security Mode	Hide SSID	Operation
			No Data		

Total 0 10/page < 1 > Go to 1

3.7.4 VPN

3.7.4.1 PPTP



PPTP Server: on
Broadcast Support: off
Force MPPE Encryption: off
DNS1:
DNS2:
WINS1:
WINS2:
Server IP:
Client IP(s): 0.0.0.0-0

Broadcast Support:

Enable or disable the PPTP server support broadcast function

Force MPPE Encryption:

Whether you want to enforce MPPE encryption for PPTP data

DNS1，DNS2，WINS1，WINS2：

Set up your 1st DNS, 2nd DNS, 1st WINS, 2nd WINS

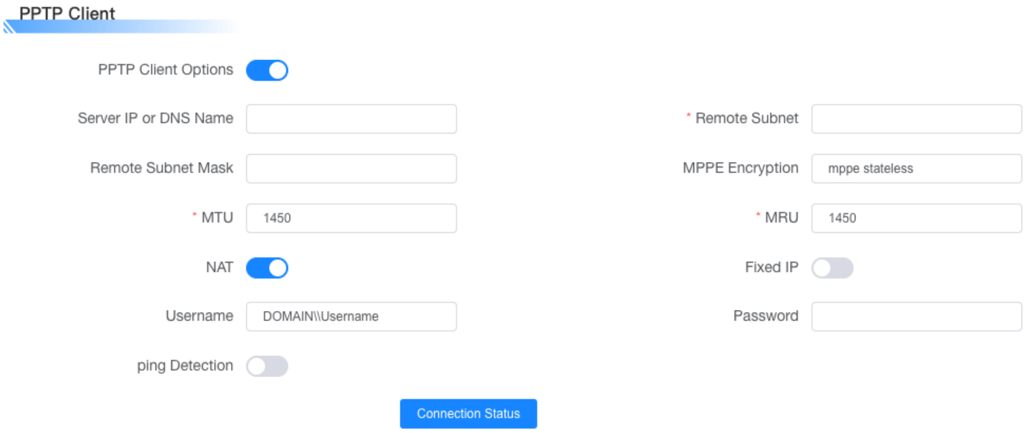
Server IP:

Enter the IP address of the 5G router as the PPTP server, which should not be the same as the LAN address.

Client IP(s):

The IP address assigned to the client in the format xxx.xxx.xxx.xxx-xxx

Note: The client IP cannot be the same as the IP assigned by the DHCP of the 5G router, as long as it is outside this range.



PPTP Client

PPTP Client Options: ●

Server IP or DNS Name:

* Remote Subnet:

Remote Subnet Mask:

MPPE Encryption: mppe stateless

* MTU: 1450

* MRU: 1450

NAT: ●

Fixed IP: ○

Username: DOMAIN\\Username

Password:

ping Detection: ○

Server IP or DNS Name:

PPTP server’ s IP Address or DNS Name

Remote Subnet:

The network of the remote PPTP server

Remote Subnet Mask:

Subnet mask of remote PPTP server

MPPE Encryption:

Enable or disable Microsoft Point-to-Point Encryption。

MTU:

Maximum Transmission Unit 0-1500

MRU:

Maximum Receive Unit 0-1500

NAT:

Network Address Translation

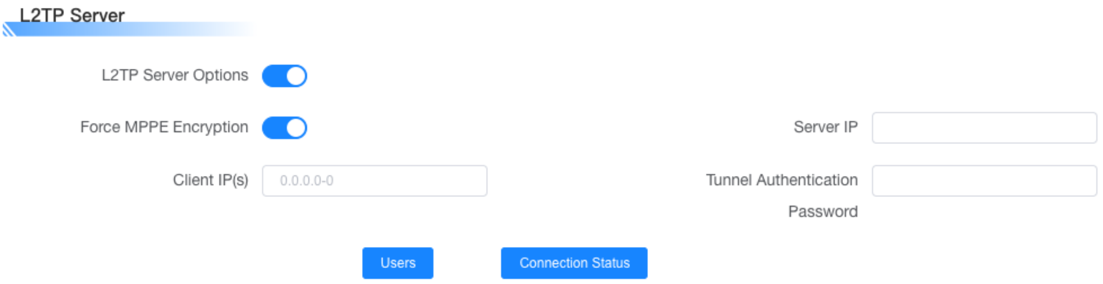
Username:

User name to login PPTP Server.

Password:

Password to log into PPTP Server.

3.7.4.2 L2TP



L2TP Server

L2TP Server Options: ●

Force MPPE Encryption: ●

Server IP:

Client IP(s): 0.0.0.0-0

Tunnel Authentication Password:

Force MPPE Encryption:

Enable or disable force MPPE encryption of L2TP data

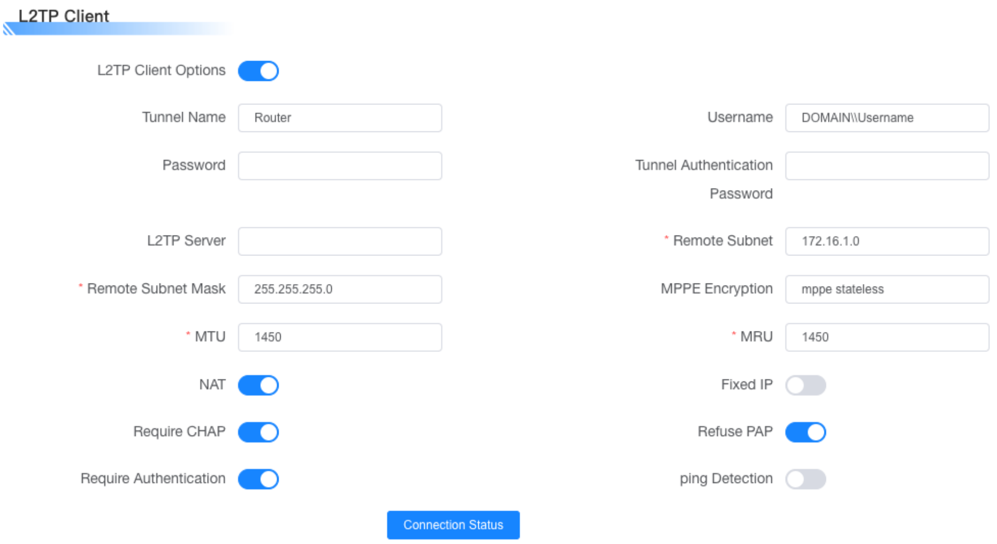
Server IP:

Input IP address of the 5G Router as PPTP server, differ from LAN address

Client IP(s):

IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx

Note: Client IP must be different with IP assigned by 5G Router DHCP.



L2TP Client

L2TP Client Options: ●

Tunnel Name: Router

Username: DOMAIN\\Username

Password:

Tunnel Authentication Password:

L2TP Server:

* Remote Subnet: 172.16.1.0

* Remote Subnet Mask: 255.255.255.0

MPPE Encryption: mppe stateless

* MTU: 1450

* MRU: 1450

NAT: ●

Fixed IP: ○

Require CHAP: ●

Refuse PAP: ●

Require Authentication: ●

ping Detection: ○

L2TP Server:

L2TP server’ s IP Address or DNS Name

Remote Subnet:

The network of remote PPTP server

Remote Subnet Mask:

Subnet mask of remote PPTP server

MPPE Encryption:

Enable or disable Microsoft Point-to-Point Encryption

MTU:

Maximum transmission unit 0-1500

MRU:

Maximum receive unit 0-1500

NAT:

Network address translation

Username:

Username to login L2TP Server

Password:

Password to login L2TP Server

Require CHAP:

Enable or disable support chap authentication protocol

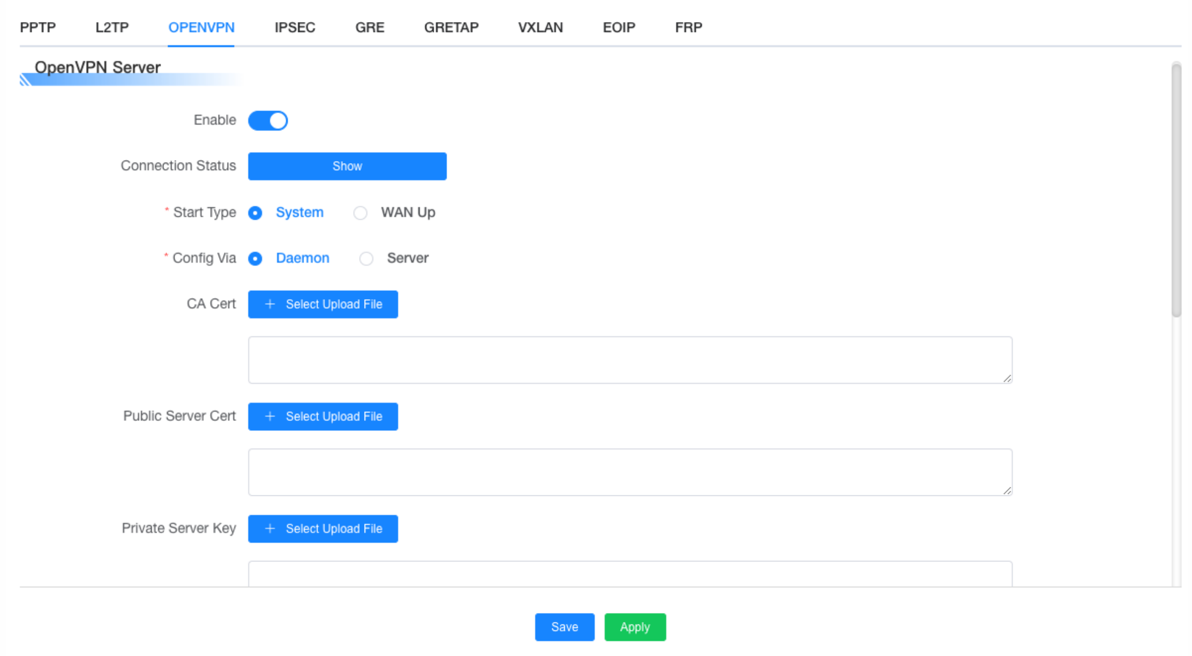
Refuse PAP:

Enable or disable refuse to support the pap authentication

Require Authentication:

Enable or disable support authentication protocol

3.7.4.3 OPENVPN



Enable: on

Connection Status

* Start Type ● System ○ WAN Up

* Config Via ● Daemon ○ Server

CA Cert

Public Server Cert

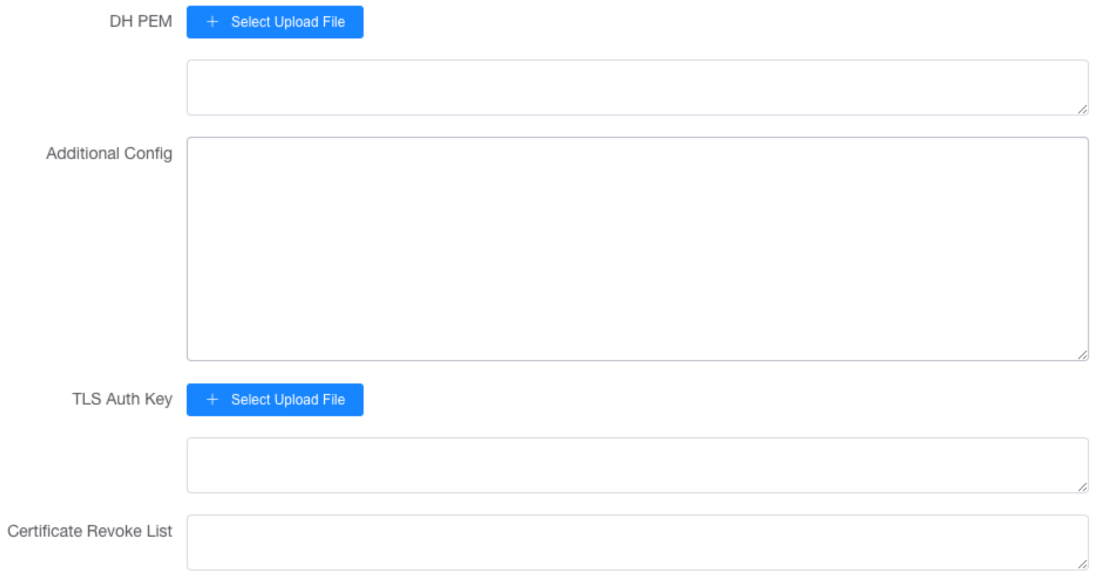
Private Server Key

CA Cert: CA certificate that is common to both the server and the client

Public Server Cert: The server-side certificate

Private Server Key:

The key set on the server side



DH PEM:

The PEM certificate on the server side

Additional Config:

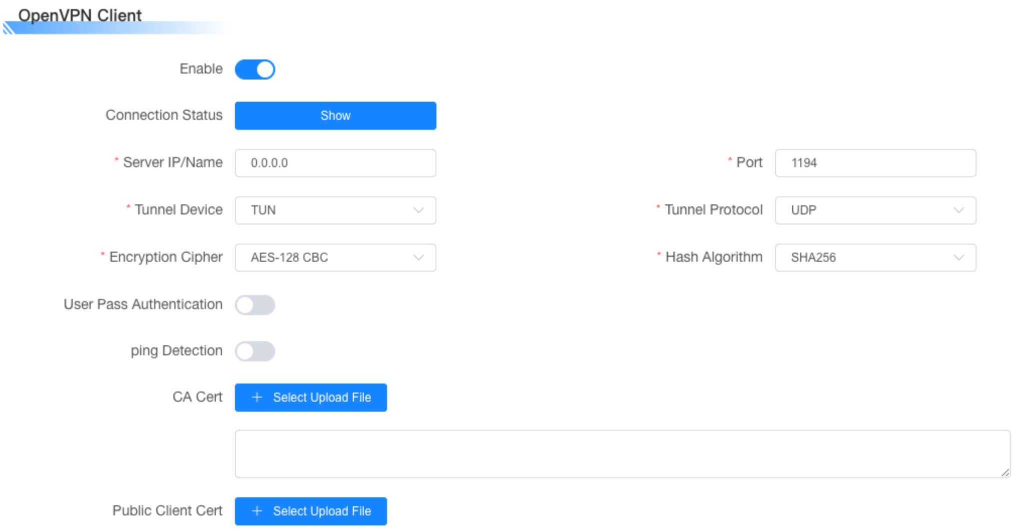
Other additional configurations of the server

TLS Auth Key:

Authentication key for Transport Layer Security

Certificate Revoke List:

Configure a list of some revocation certificates


OpenVPN Client

Enable: on

Connection Status: Show

* Server IP/Name: 0.0.0.0

* Port: 1194

* Tunnel Device: TUN

* Tunnel Protocol: UDP

* Encryption Cipher: AES-128 CBC

* Hash Algorithm: SHA256

User Pass Authentication: off

ping Detection: off

Server IP Name:

The IP Address or Domain Name of the OPENVPN Server

Port:

The Listening Port of the OPENVPN Client

Channel Equipment:

TUN --- route mode, TAP --- bridge mode

Channel Protocol:

UDP and TCP protocols Encryption Standards: The encryption standards of the channel include: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, and AES-512 CBC

Hash Algorithm:

The Hash algorithm provides a fast way to access data, including SHA1, SHA256, SHA512, and MD5

CA Cert:

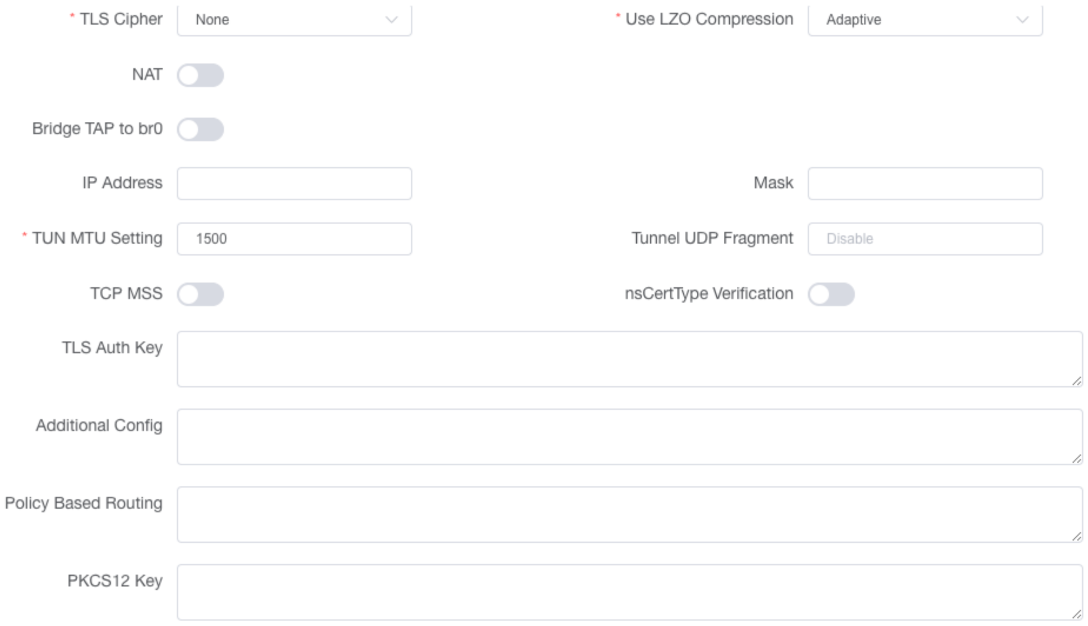
CA certificate that is common to both the server and the client

Public Client Cert:

Client certificate

Private Client Key:

The client's key



* TLS Cipher: None
* Use LZO Compression: Adaptive
NAT: ○
Bridge TAP to br0: ○
IP Address:
Mask:
* TUN MTU Setting: 1500
Tunnel UDP Fragment: Disable
TCP MSS: ○
nsCertType Verification: ○
TLS Auth Key:
Additional Config:
Policy Based Routing:
PKCS12 Key:

Use LZO Compression: Enables or disables the use of LZO compression for transferred data

NAT: Enables or disables NAT traversal

Bridge TAP to br0: Enables or disables TAP binding to br0 bridge

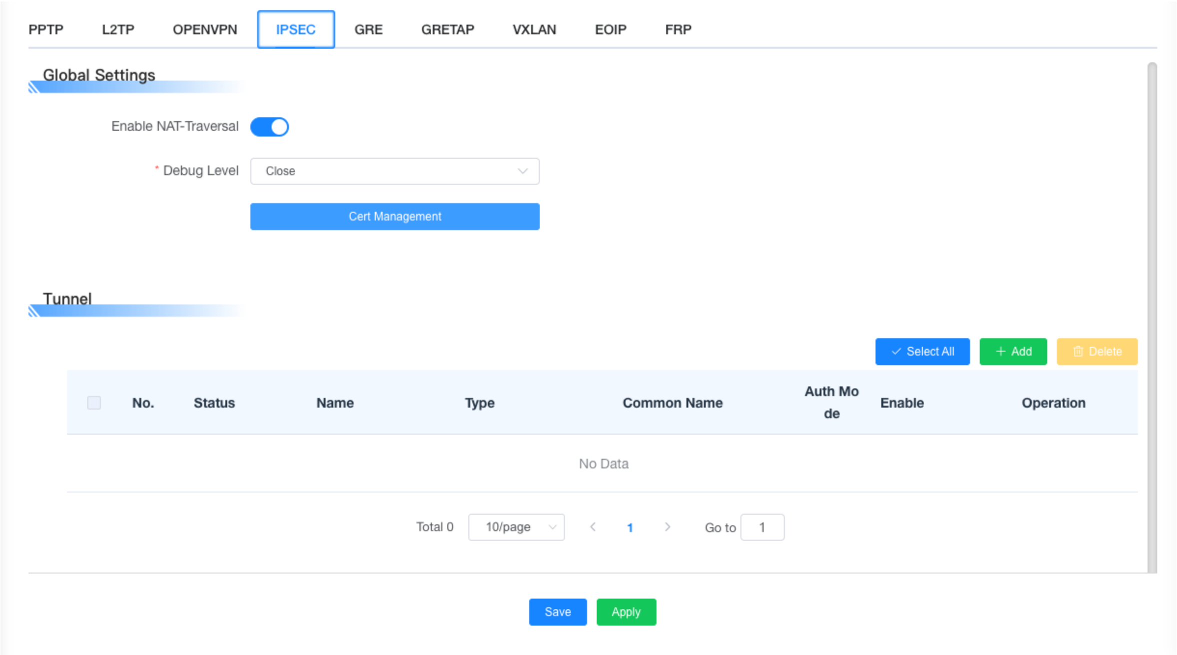
IP Address: Set the IP Address of THE LOCAL OPENVN CLIENT

TUN MTU Settings: Sets the MTU value for the channel

TCP MSS: THE MAXIMUM FRAGMENT SIZE OF TCP DATA

TLS encryption standard: The TLS (Transport Layer Secure) encryption standard supports AES-128 SHA and AES-256 SHA

TLS Authentication Key: The authentication key for the Transport Secure layer
Additional Configurations: Other Additional Configurations of OPENVPN Servers
Policy Based Routing : Enter some custom routing policies



Global Settings

Enable NAT-Traversal ●

* Debug Level: Close

Tunnel

□	No.	Status	Name	Type	Common Name	Auth Mode	Enable	Operation

No Data

Total 0 10/page < 1 > Go to 1

3.7.4.4 IPSEC

On the IPSEC Page, The IPSEC Connection that the current device has and their status are displayed.

Debug Level:

There are two Debug Levels in which the connection is located: Close and Basic.

Close: The connection does not request a connection to the peer.

Negotiating: The connection has been requested to the peer and is in the process of negotiation, but the connection has not yet been established.

Established: The connection has been established and the channel is ready to be used.

Operate:

Currently, there are four operations that can be performed on the connection: Delete, Edit, Reconnect, and Enable.

Delete: this operation will delete the connection, and if the ipsec channel has been established, it will also be removed;

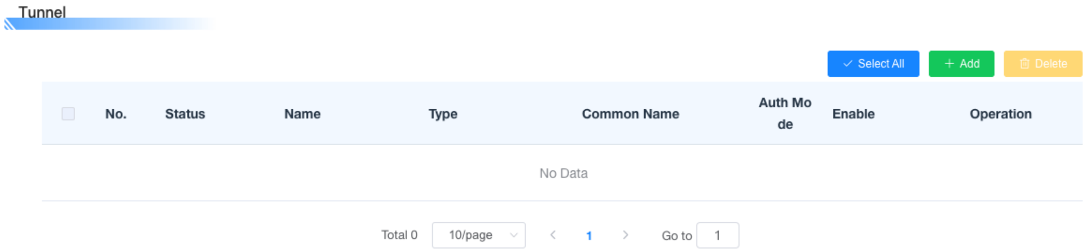
Edit: Modify the configuration information of the connection, and reload the connection if you want the configuration to take effect.

Reconnection: This operation will remove the current channel and re-initiate the channel establishment request.

Enabled: When the system restarts or reconnects when the connection is enabled, the connection initiates a channel establishment request. On the contrary, no request will be made.

Add: this feature is used to add a new ipsec connection.

Delete: this feature is used to delete an ipsec connection



Tunnel

□	No.	Status	Name	Type	Common Name	Auth Mode	Enable	Operation
No Data								

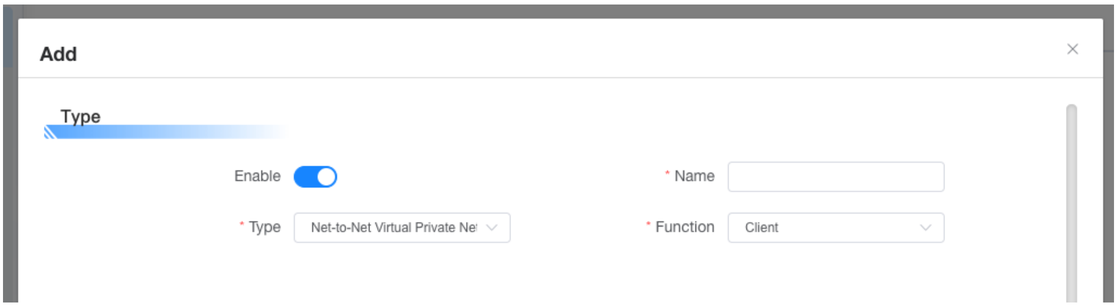
Name:

The name of the IPSEC Connection;

Type:

The Type and function of the current IPSEC connection;

Function: In this column, you can select the IPSEC mode and the corresponding functions, and currently support the client and server functions in tunnel mode.



Add

Type

Enable ●

* Name

* Type Net-to-Net Virtual Private Ne

* Function Client

Connection Config: This column contains the basic address information of the channel.

Local WAN interfaces:

The local address of the channel.

Local subnet:

IPSec local protection subnet and subnet mask, e.g. 192.168.1.0/24;

Local ID:

The local identifier of the channel, which can be IP and domain name;

Peer WAN address:

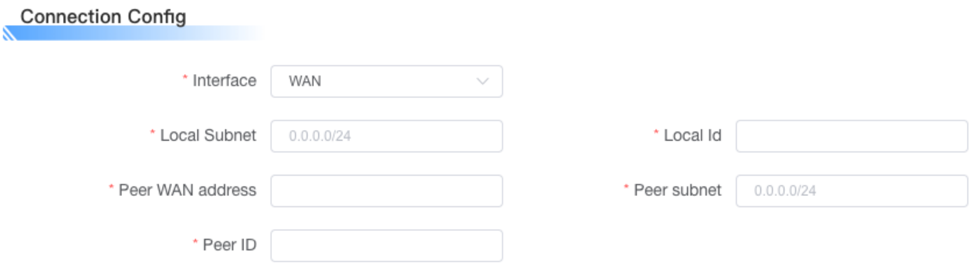
The peer's IP/domain name. If the server-side function in tunnel mode is used, this option cannot be specified.

Peer subnet:

IPSec peer protection subnet and subnet mask, for example: 192.168.7.0/24;

Peer ID:

The peer identifier of the channel, which can be an IP address and a domain name.



Connection Config

* Interface	WAN		
* Local Subnet	0.0.0.0/24	* Local Id	
* Peer WAN address		* Peer subnet	0.0.0.0/24
* Peer ID			

Detection

This section contains configuration information for Connection Detection (DPD).

Enable DPD Detection:

Whether to enable this function, tick to indicate that it is enabled;

Time Interval:

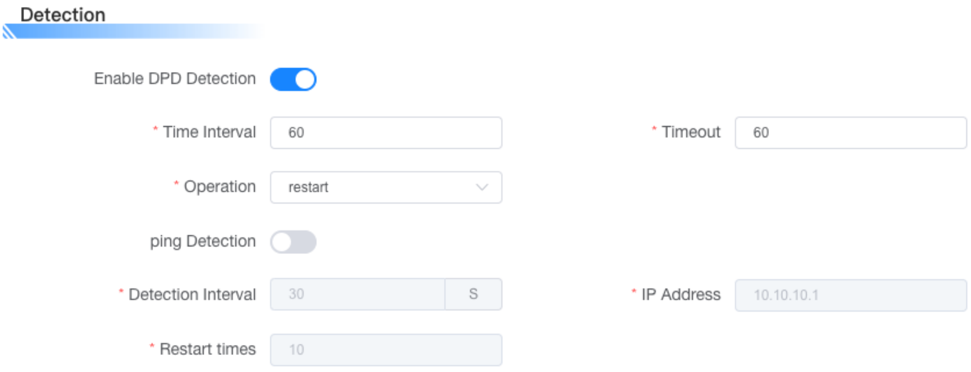
Set the time interval for connection detection (DPD);

Timeout:

Set the connection detection (DPD) timeout period;

Operation:

Set the action for connection detection.

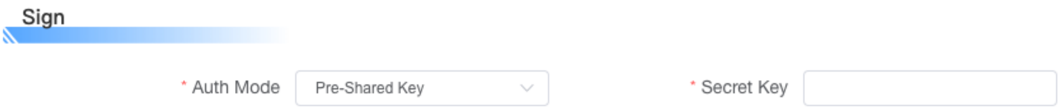


Detection

Enable DPD Detection	●		
* Time Interval	60	* Timeout	60
* Operation	restart		
ping Detection	○		
* Detection Interval	30 S	* IP Address	10.10.10.1
* Restart times	10		

Sign

You can select a shared key or certificate authentication based on your needs, but you can only select the shared key mode.

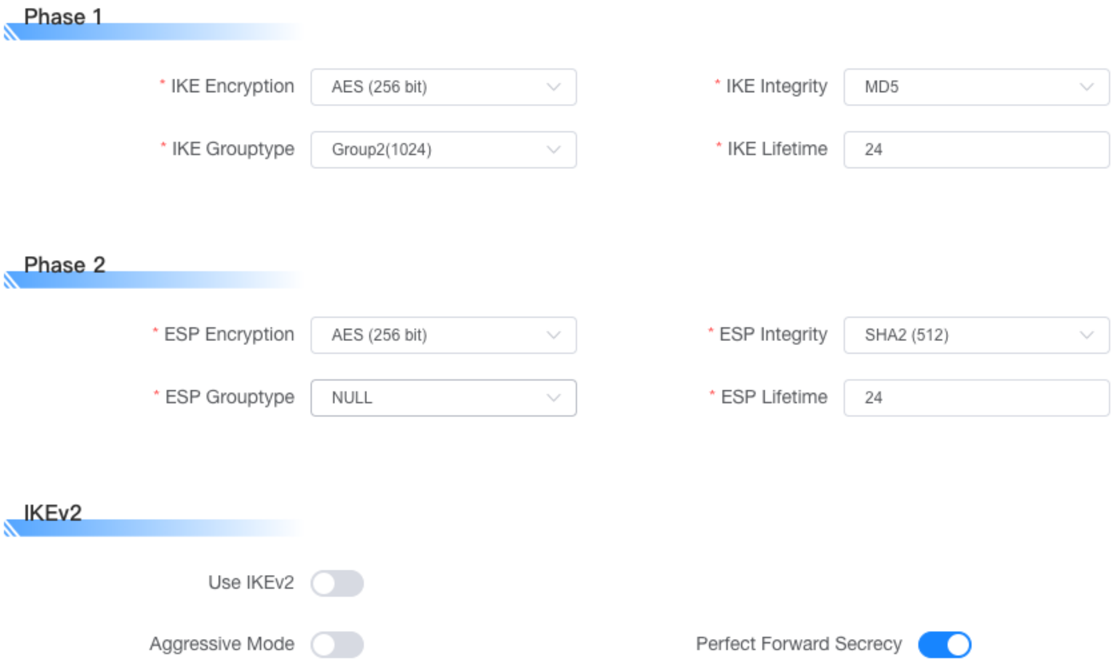


Sign

* Auth Mode	Pre-Shared Key	* Secret Key	

Advance

This section contains configurations such as IKE, ESP, and Aggressive Mode.



Phase 1

* IKE Encryption	AES (256 bit)	* IKE Integrity	MD5
* IKE Grouptype	Group2(1024)	* IKE Lifetime	24

Phase 2

* ESP Encryption	AES (256 bit)	* ESP Integrity	SHA2 (512)
* ESP Grouptype	NULL	* ESP Lifetime	24

IKEv2

Use IKEv2 ○

Aggressive Mode ○ Perfect Forward Secrecy ●

To enable advanced configuration:

If it is enabled, you can configure the information of the first and second phases, otherwise, it will be automatically negotiated according to the peer.

IKE encryption: the encryption method of the IKE stage;

IKE Integrity: An integrity protocol for the IKE phase;

IKE Group type: DH Swap Algorithm;

IKE Lifetime: Set the lifecycle of the IKE, which is currently measured in hours and defaults to 0;

ESP Encryption: the encryption method of ESP;

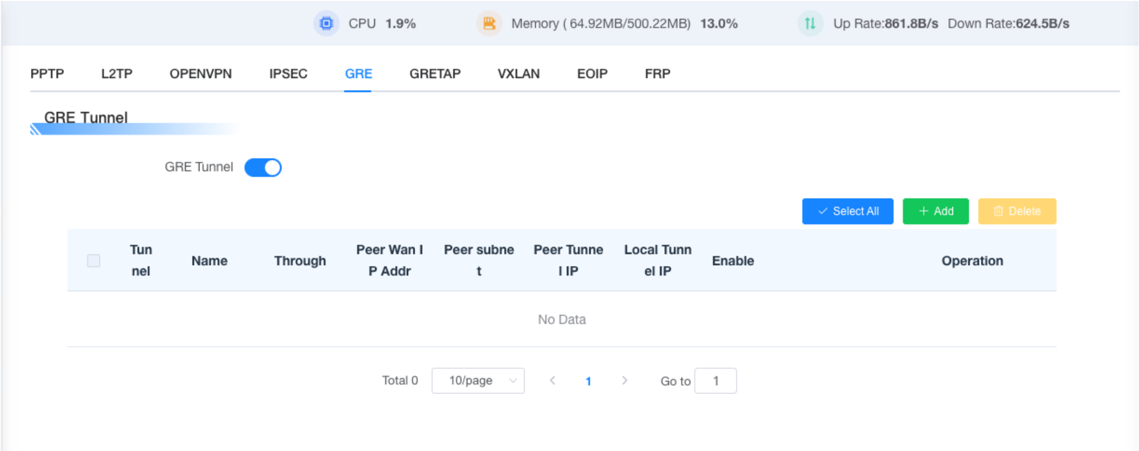
ESP Integrity: ESP Integrity Scheme;

ESP Lifetime: Set the lifecycle of ESP, which is currently measured in hours and defaults to 0;

Aggressive Mode: If the check is checked, the negotiation mode will adopt the savage mode, otherwise the main mode;

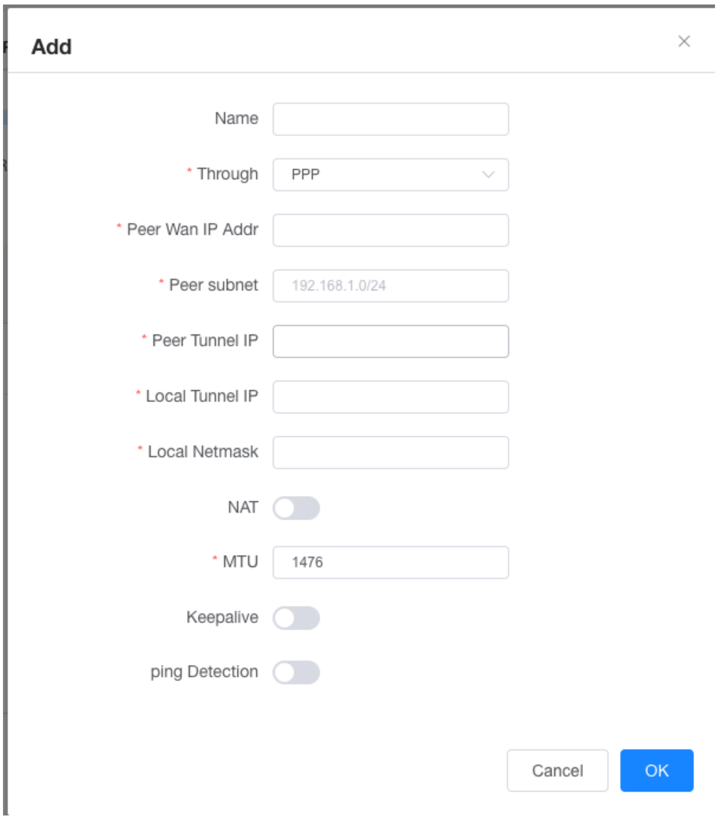
Perfect Forward Secrecy: PFS is enabled if checked, not otherwise;

3.7.4.5 GRE



GRE Tunnel ●

☐	Tunnel	Name	Through	Peer Wan IP Addr	Peer subnet	Peer Tunnel IP	Local Tunnel IP	Enable	Operation
No Data									



Name:
* Through: PPP
* Peer Wan IP Addr:
* Peer subnet: 192.168.1.0/24
* Peer Tunnel IP:
* Local Tunnel IP:
* Local Netmask:
NAT: ○
* MTU: 1476
Keepalive: ○
ping Detection: ○

The GRE (Generic Routing Encapsulation) protocol encapsulates data packets from certain network-layer protocols (such as IP and IPX) so that they can be transmitted in another network-layer protocol (such as IP). GRE uses Tunnel technology, which is the Layer 3 tunneling protocol of Virtual Private Network (VPN).

GRE Tunnel: Enables or disables the GRE feature
Channels: Configurable channels, currently up to 12 GRE tunnels can be set up
Status: Enabled means that the currently configured GRE tunnel is enabled, otherwise it

means that the current GRE tunnel is closed

Name: The name of the tunnel is up to 30 characters long

Through: GRE transceiver interface, currently has LAN port, and PPP dial port

Peer WAN IP Address: Enter the WAN port IP address of the peer GRE

Peer Subnet: The IP address of the peer subnet of the GRE, for example, 192.168.1.0/24

Peer Tunnel IP: The GRE tunnel IP of the peer Tunnel IP of this segment: The IP address of the local GRE tunnel

Local Netmask: the local subnet mask

Keep Alive:

Turn GRE keep-alive on/off

Number of re-pulls:

Maximum number of GRE keep-alive failures

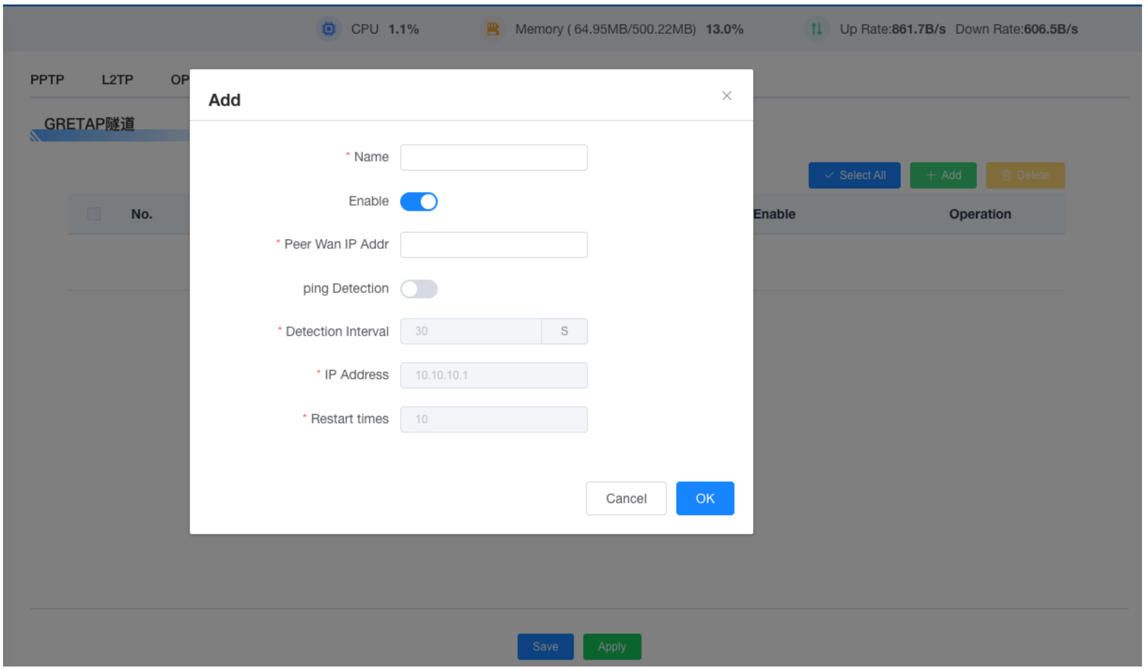
Re-Pull Interval:

GRE keepalive packet sending interval

Failure Strategy:

Keep-alive failure strategy

3.7.4.6 GRETAP



CPU 1.1% Memory (64.95MB/500.22MB) 13.0% Up Rate:861.7B/s Down Rate:606.5B/s

Add

* Name

Enable: on

* Peer Wan IP Addr

ping Detection: off

* Detection Interval: 30 S

* IP Address: 10.10.10.1

* Restart times: 10

Name: The name of the GRETAP port, up to 32 characters.

Enable: Specifies whether to enable the current GRETAP.

PEER WAN IP Addr: THE WAN IP ADDRESS OF THE PEER GRETAP.

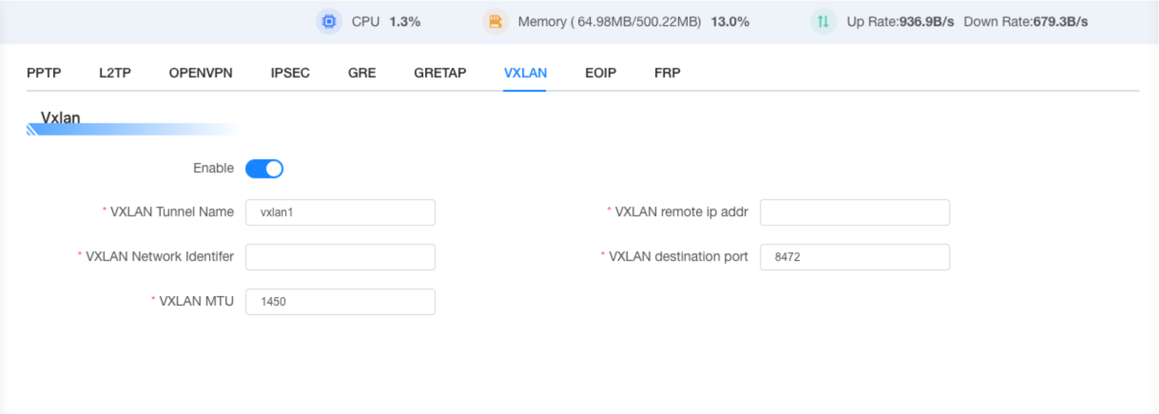
Ping Detection: Specifies whether to enable GRETAP link detection.

Detection Interval: The interval between GRETAP link detections.

IP Address: GRETAP detects the IP address of the peer.

Restart Times: the number of times that GRETAP fails to detect and re-initiates GRETAP.

3.7.4.7 VXLAN


CPU 1.3%
Memory (64.98MB/500.22MB) 13.0%
Up Rate:936.9B/s Down Rate:679.3B/s
PPTP
L2TP
OPENVPN
IPSEC
GRE
GRETAP
VXLAN
EOIP
FRP
Vxlan

Enable

* VXLAN Tunnel Name: vxlan1

* VXLAN remote ip addr:

* VXLAN Network Identifer:

* VXLAN destination port: 8472

* VXLAN MTU: 1450

Enable: Enables or disables the Vxlan feature.

VXLAN Tunnel Name: the name of the NIC of the VXLAN.

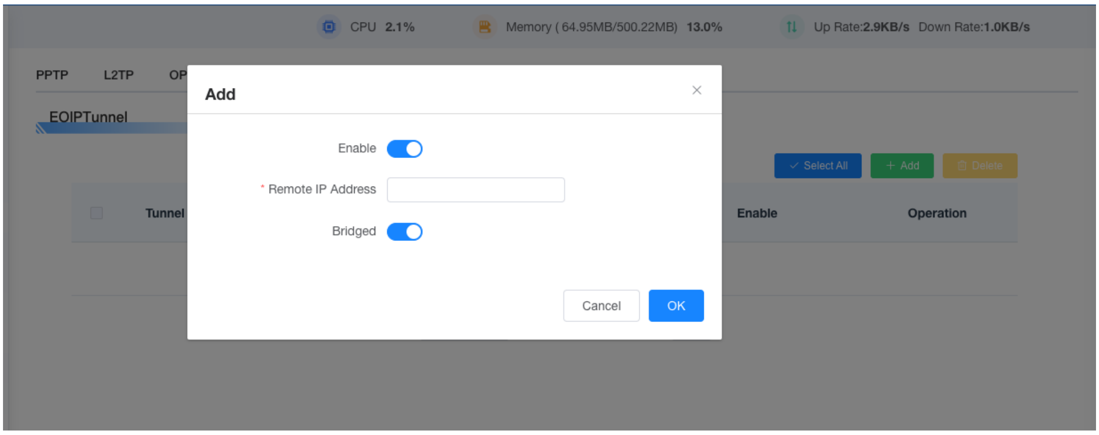
VXLAN Remote IP Address: the WAN IP address of the VXLAN peer.

VXLAN Network Identifer: The network ID of the VXLAN must be the same as that of the local end.

VXLAN Destination Port: The destination port of the VXLAN, default 8472.

VXLAN MTU: the MTU size of the VXLAN transmit and receive, which is 1450 by default.

3.7.4.8 EOIP



Enable

* Remote IP Address:

Bridged

Enable: Enable: Enables or disables the current EOIP feature.

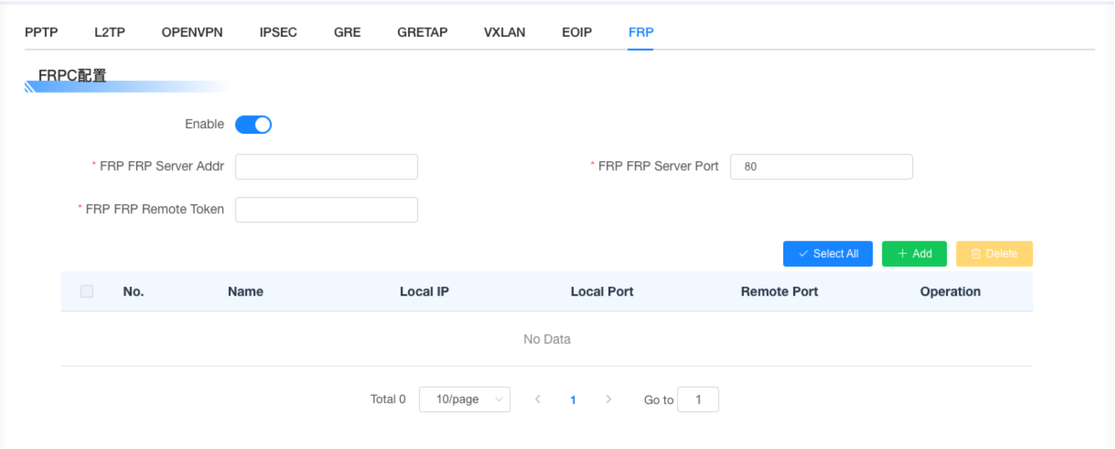
Remote IP Address: The WAN IP address of the peer EOIP.

Bridged: Whether to enable bridging, if it is not enabled, the EOIP CIDR blocks on both sides are different, and if it is enabled, the EOIP CIDR blocks on both sides of the bridge are the same.

IP Address: The tunnel IP address of the EOIP.

Subnet Mask: The tunnel subnet mask of the EOIP.

3.7.4.9 FRP



FRPC配置

Enable ●

* FRP FRP Server Addr

* FRP FRP Server Port 80

* FRP FRP Remote Token

□	No.	Name	Local IP	Local Port	Remote Port	Operation
			No Data			

Total 0 10/page 1 Go to 1

Enable: Enable or disable the FRP function.

FRP Server Address: The FRP server address of the public network.

FRP Server Port: The FRP server port of the public network.

FRP Remote Token: The FRP server key of the public network.

Local IP: The destination IP that FRP wants to access the mapping.

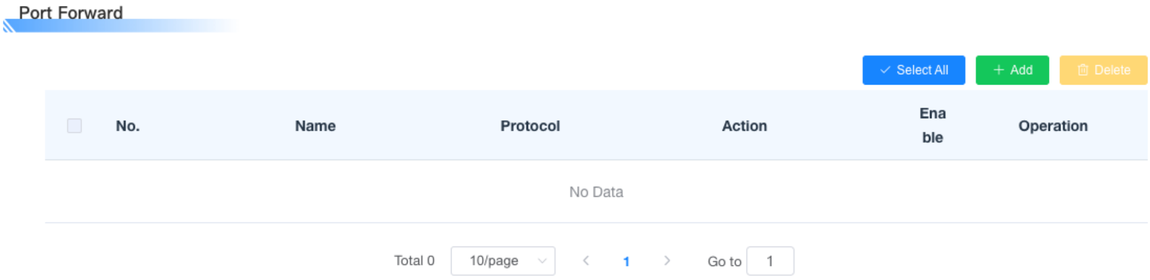
Local Port: The destination port that FRP wants to access the mapping.

Remote Port: The port that FRP uses to access the device through the public network.

3.7.5 NAT

3.7.5.1 Port Forward

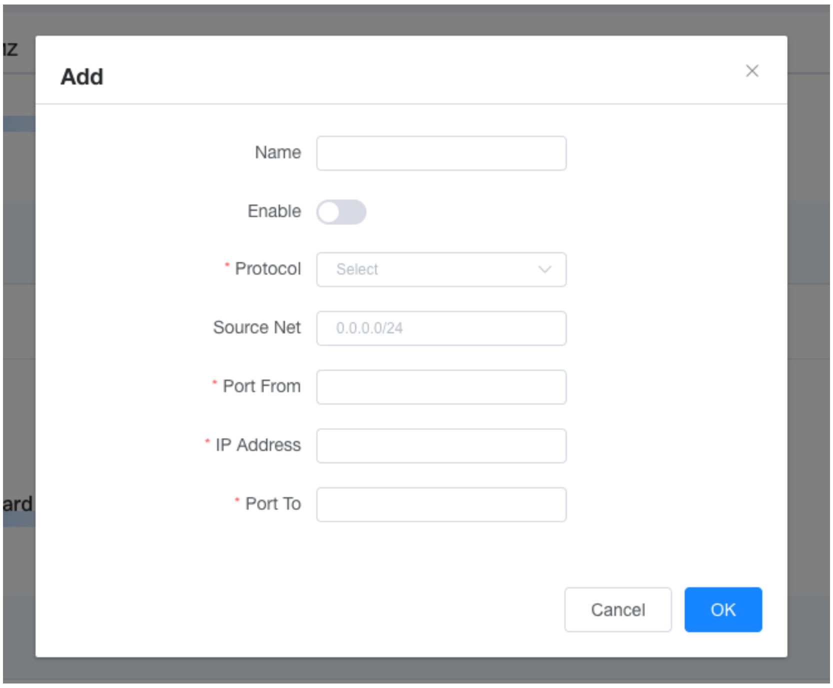
Port Forwarding is used to set up public services on the network, such as web servers, FTP servers, or other private Internet applications (a private Internet application is any application that uses Internet access to use functionality).



Port Forward

□	No.	Name	Protocol	Action	Enable	Operation
No Data						

Total 0 10/page < 1 > Go to 1



Add

Name
Enable
* Protocol Select
Source Net 0.0.0.0/24
* Port From
* IP Address
* Port To

Name: Enter the name of the application in the fields provided by the application.

Protocol: Choose either UDP or TCP for each application, and both at the same time.

Allowed source IP ranges:

Fill in the field with the IP address of the Internet user.

Source Port:

Enter the number of the external port used by the service in this field.

IP Address:

Enter the private IP address of the server that you want internet users to access.

Destination Port:

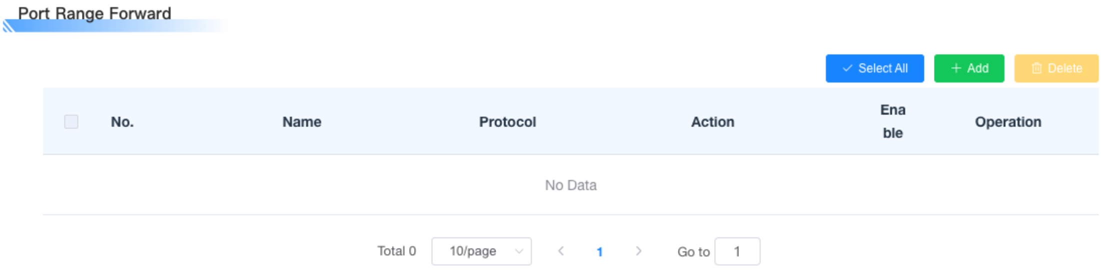
Enter the number of the internal port used by the service in this field.

Enable:

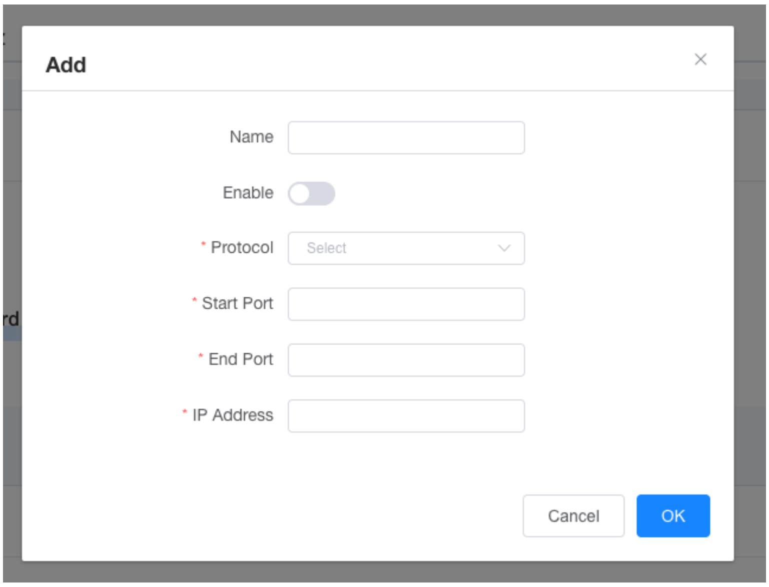
Select the Enable box to enable the multiport forwarding service that you define. The default configuration is Disabled (not selected).

When you're done modifying the page, click the "Save Settings" button to save your changes, or click the "Cancel Changes" button to cancel the changes, the help information is located on the right, and for more information, click "More".

Port Range Forward



□	No.	Name	Protocol	Action	Enable	Operation
No Data						



Some applications may require forwarding of a specific port range in order to function properly, and when a request to a port range is made from the Internet, the 5G router sends this data to the specified computer. For security reasons, you may want to limit port forwarding to only those ports that are in use, and if you no longer use it, we recommend that you remove the Enable check box to temporarily disable that port forwarding.

Name:
Enter the name of the application in the fields provided by the application;
Enable:
Select the Enable box to enable the multiport forwarding service that you define. The default configuration is Disabled (not selected).
Protocol:
Choose UDP or TCP protocol for each application, and choose both protocols at the same time;

Start Port:

Enter the start port number of the port forwarding range;

End Port:

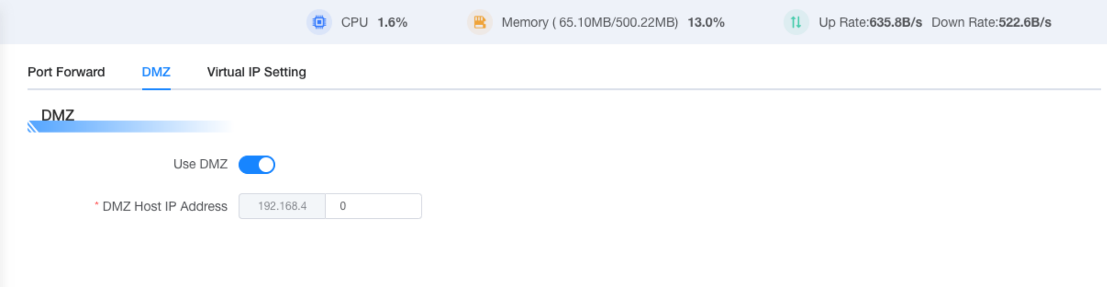
Enter the end port number of the port forwarding range;

Destination IP address:

Enter the private IP address of the server that you want Internet users to access.

When you are done modifying the page, click the Save Settings button to save your changes, or click the Apply key to make the configuration option work.

3.7.5.2 DMZ



CPU 1.6% Memory (65.10MB/500.22MB) 13.0% Up Rate:635.8B/s Down Rate:522.6B/s

DMZ

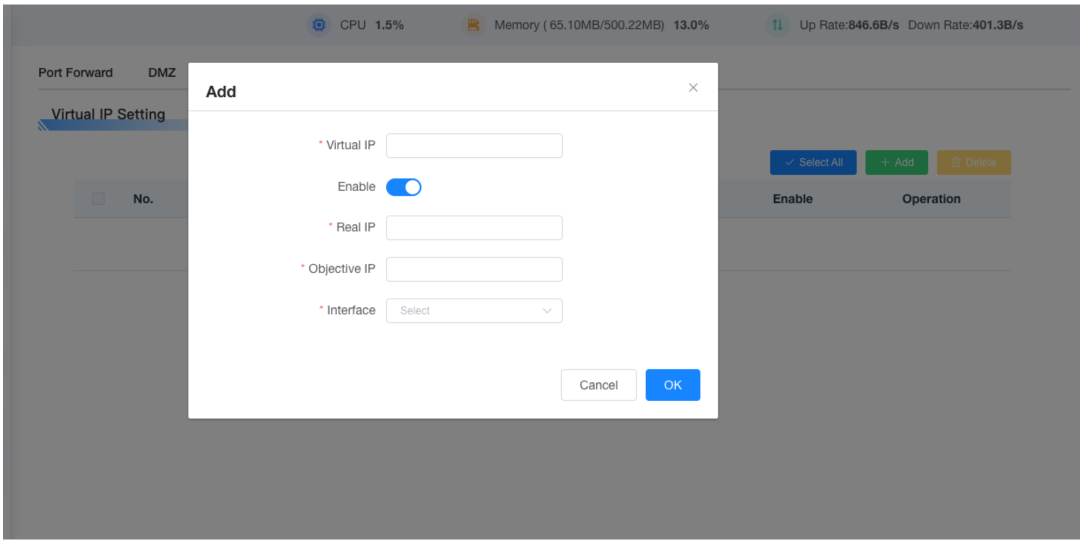
Use DMZ

* DMZ Host IP Address 192.168.4 0

The DMZ feature allows a network user to be exposed to the Internet and thus use a particular service. The DMZ host forwards all the ports to a computer at the same time, making port forwarding more secure because only the ports you want are open, while the DMZ host opens all the ports, exposing the computer to the Internet.

To enable the DMZ feature, select Enable, and then enter the IP address of your computer in the DMZ Host IP Address field.

3.7.5.3 Virtual IP Setting



CPU 1.5% Memory (65.10MB/500.22MB) 13.0% Up Rate:846.6B/s Down Rate:401.3B/s

Add

* Virtual IP

Enable

* Real IP

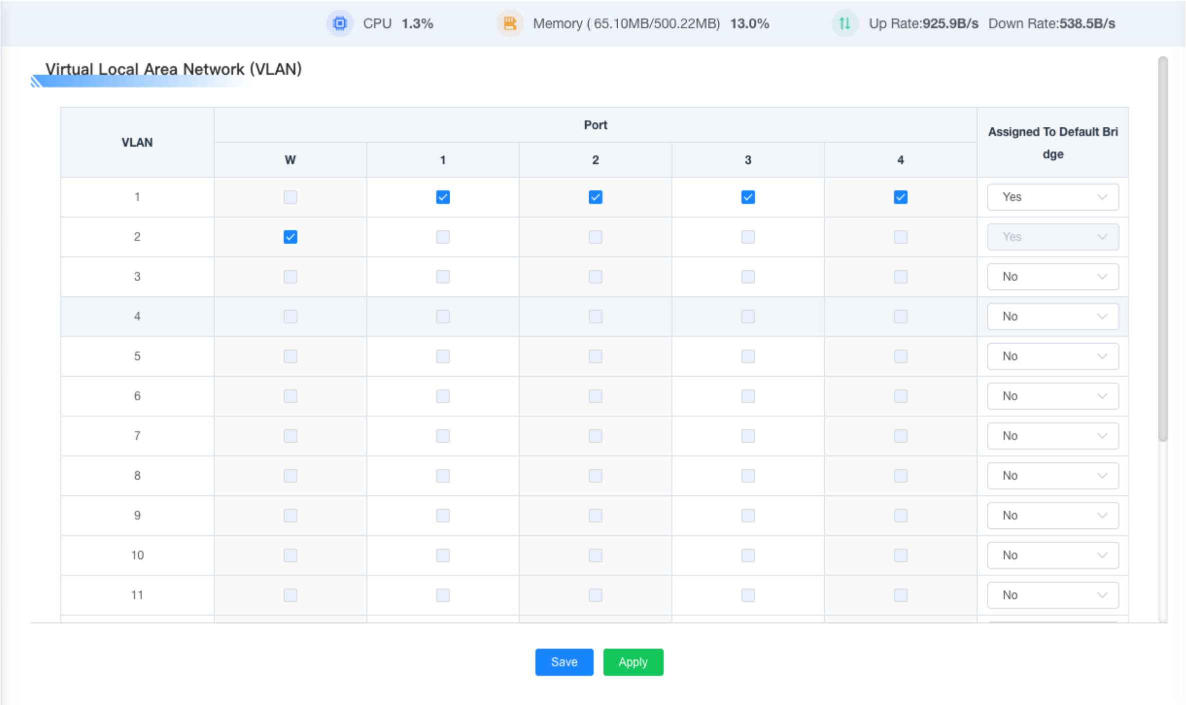
* Objective IP

* Interface Select

Virtual IP: The virtual IP address.

Real IP: the IP address to be accessed, for example, the IP address (192.168.1.100) under the route.
Objective IP: the subnet address and gateway of the peer end, which is not set by default (0.0.0.0/0).
Interface: the interface of virtual IP forwarding.

3.7.6 VLAN

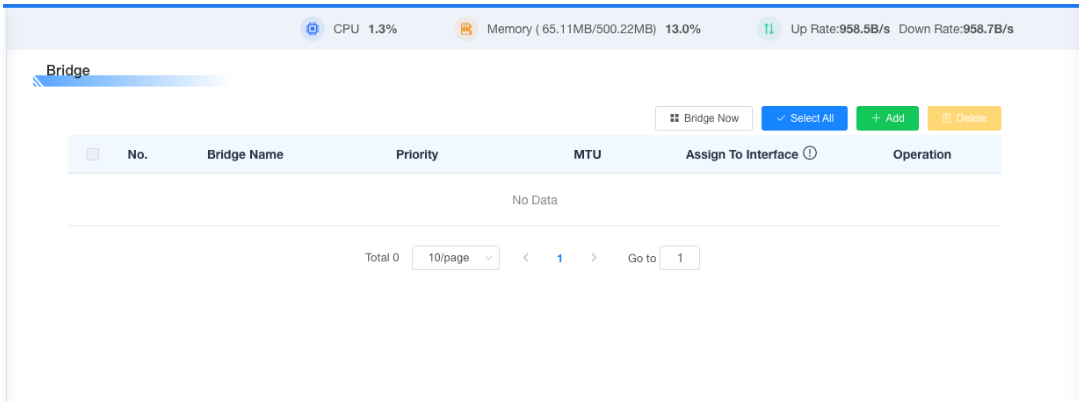

CPU 1.3%
Memory (65.10MB/500.22MB) 13.0%
Up Rate:925.9B/s Down Rate:538.5B/s

Virtual Local Area Network (VLAN)

VLAN	Port					Assigned To Default Bridge
	W	1	2	3	4	
1	☐	☑	☑	☑	☑	Yes
2	☑	☐	☐	☐	☐	Yes
3	☐	☐	☐	☐	☐	No
4	☐	☐	☐	☐	☐	No
5	☐	☐	☐	☐	☐	No
6	☐	☐	☐	☐	☐	No
7	☐	☐	☐	☐	☐	No
8	☐	☐	☐	☐	☐	No
9	☐	☐	☐	☐	☐	No
10	☐	☐	☐	☐	☐	No
11	☐	☐	☐	☐	☐	No

The VLANs function can be divided into different VALN ports according to the user's own wishes, and the system supports VLAN1-VLAN15 which have 15 VLAN ports, but there are only 5 ports at the time, including one WAN port and 4 LAN ports, which can be divided according to their own needs, and the LAN port and WAN port cannot be divided into the same VLAN port.

3.7.7 Bridge


CPU 1.3%
Memory (65.11MB/500.22MB) 13.0%
Up Rate:958.5B/s Down Rate:958.7B/s
Bridge
Bridge Now
Select All
+ Add
Delete

☐	No.	Bridge Name	Priority	MTU	Assign To Interface ⓘ	Operation
			No Data			

Total 0
10/page
1
Go to 1

To create a bridge:

Create a new bridge to use. STP stands for Spanning Tree Protocol, and you can set the priority of the bridge. The lowest number, with the highest priority.

Assign to Bridge:

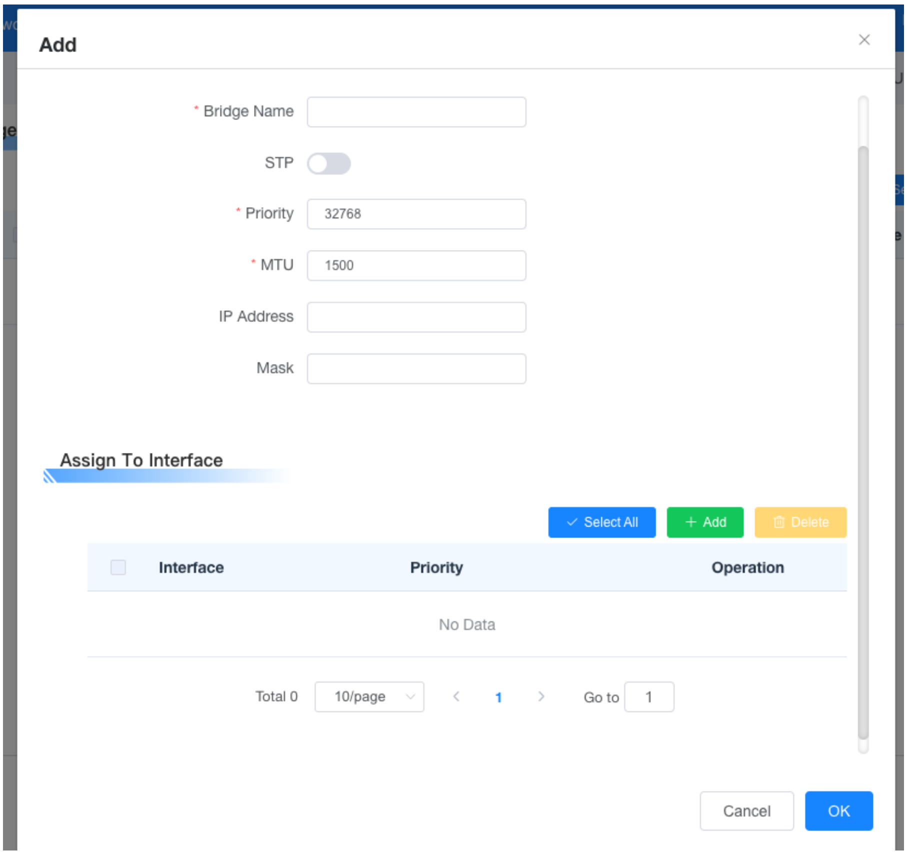
Allows you to specify any valid interface to an already established bridge.

Current list of bridgings: Displays a list of current bridges

The steps to create one are as follows:

In Create Bridge, click the Add button, and the following configuration will appear

The first br0 represents the name of the bridge, STP represents whether the spanning tree protocol is enabled, Prio represents the priority of the spanning tree protocol, the lower the number represents the higher level, and the MTU represents the maximum transmission unit. The default value is 1500, if you don't need it, delete it, and then click Save or Apply, the bridge property configuration will appear as follows:



Add

* Bridge Name

STP

* Priority: 32768

* MTU: 1500

IP Address

Mask

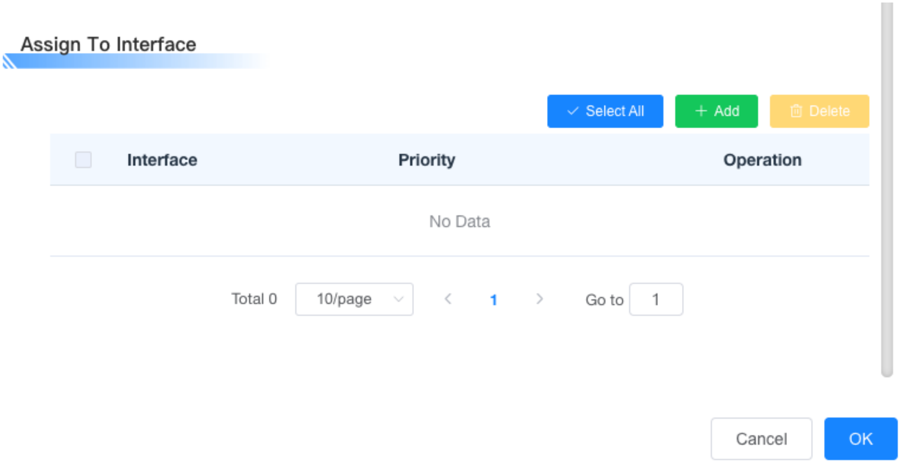
Assign To Interface

□	Interface	Priority	Operation
		No Data	

Enter the IP address and subnet mask of the corresponding bridge, and click the OK button to generate the bridge.

Note: Bridges can only be applied after they have been generated

This assignment to bridge allows you to assign different interfaces to an already created bridge, such as the interface RA0 (i.e., the wireless interface) assigned in the BR1 bridge, as shown below



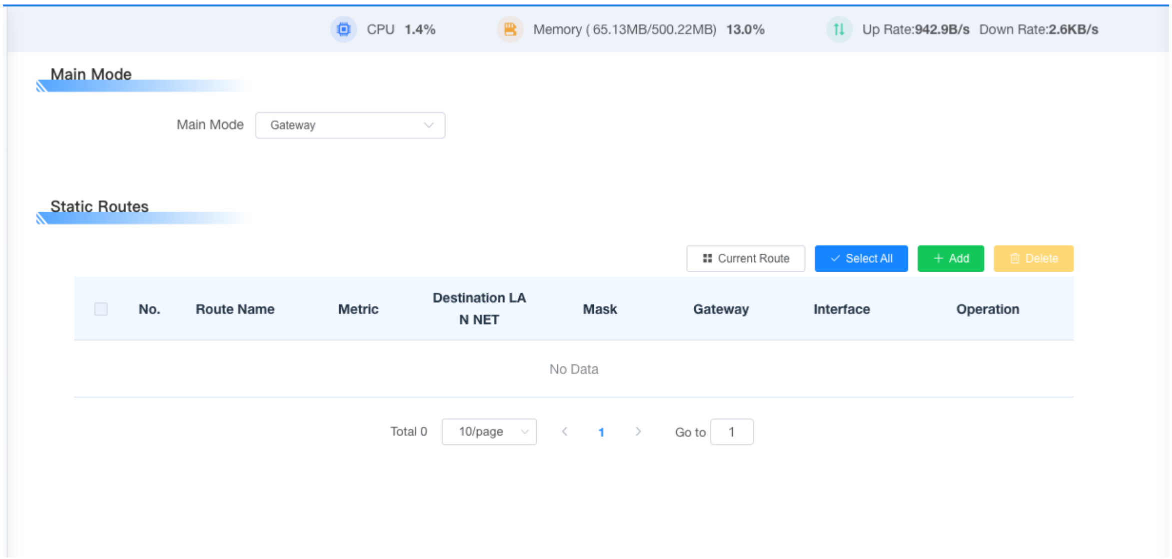
□	Interface	Priority	Operation
	No Data		

Total 0 10/page < 1 > Go to 1

Prio stands for priority, which is useful when there are multiple interfaces bound to the same bridge, and the lower the value, the higher the level. Click Apply to make it work.

Note: Some WAN interfaces that appear in the corresponding interfaces should not be bound, and this bridge function is basically used on the LAN port side, and should not be bound to the WAN port.

3.7.8 Advanced Routing



CPU 1.4% Memory (65.13MB/500.22MB) 13.0% Up Rate:942.9B/s Down Rate:2.6KB/s

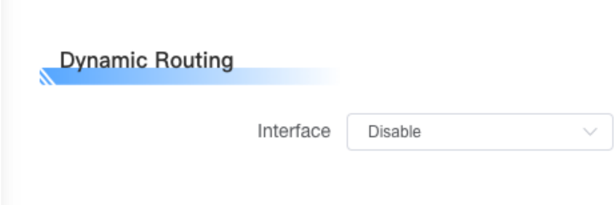
Main Mode: Gateway

□	No.	Route Name	Metric	Destination LAN NET	Mask	Gateway	Interface	Operation
				No Data				

Total 0 10/page < 1 > Go to 1

On the Advanced Routing page, you can set up the run mode and static routes. For most users, gateway mode is recommended.

Operating Modes: Choose the right mode of operation. If your 5G router shares an Internet broadband connection, keep the default gateway settings (gateway mode is recommended for most users). If you want to use only the routing capabilities of a 5G router on your network, choose a 5G router.



Dynamic Routing

Interface: Disable

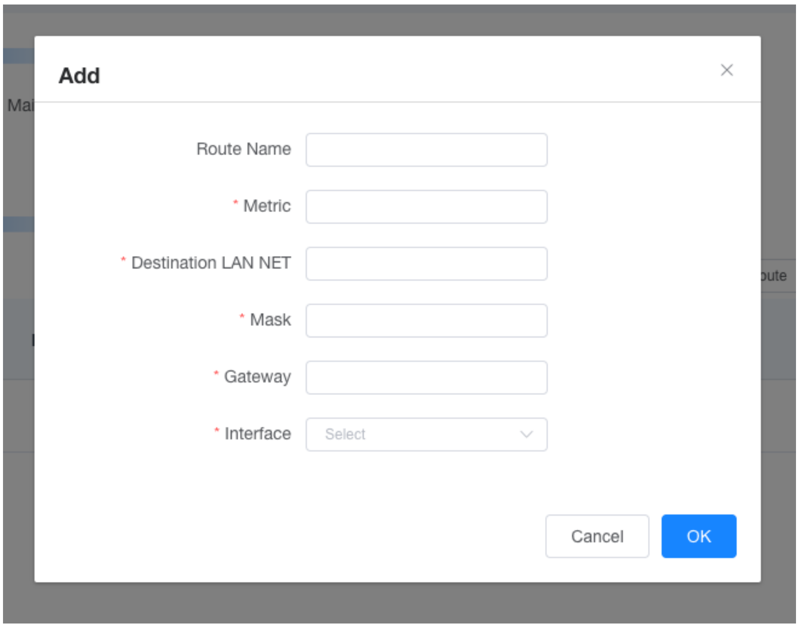
Dynamic Routing

The feature is not available in router mode. The dynamic routing feature enables 5G routers to automatically adjust to physical changes in the network layout and exchange routing tables with other 5G routers. 5G routers determine the routing of network packets based on the minimum number of hops between the source and destination.

To enable dynamic routing on the WAN side, select WAN. To enable the feature for both LAN and radio, select LAN &WLAN. To enable the feature for both WAN and LAN, select Both. To disable the dynamic routing feature for all data transfers, leave the default setting disabled.

Static routes

To set up a static route between a 5G router and another network, select a number from the Static Route drop-down list to set it up. (A static route is a predetermined path through which network information must be transmitted to a specific host or network.)



Add

Route Name

* Metric

* Destination LAN NET

* Mask

* Gateway

* Interface: Select

Route Name: A user-defined route name, which can be up to 25 characters long

Number of hops:

The unit of measurement for routing from source to destination addresses. Range 0-9999

Destination LAN IP:

The destination IP address is the address of the destination network or host of a static route.

Subnet Mask:

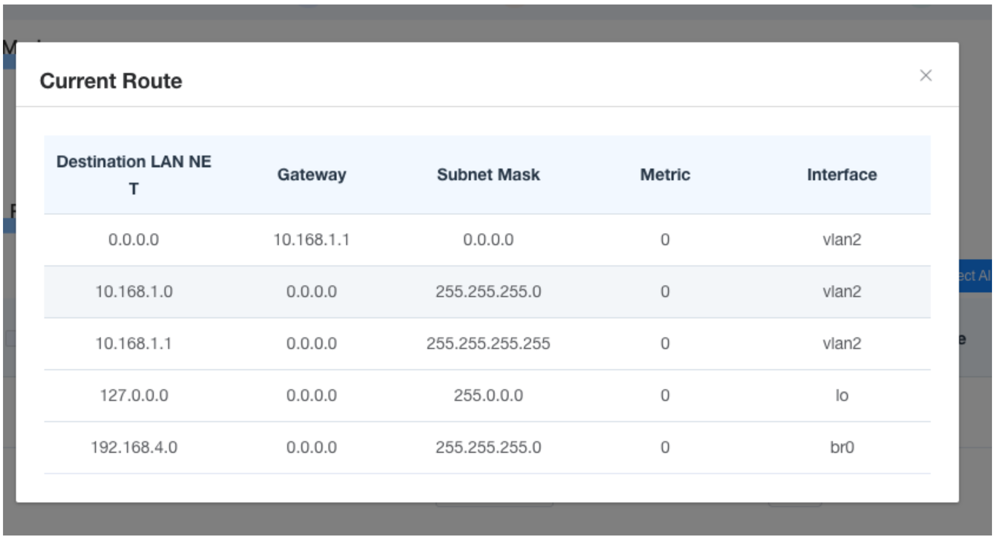
The subnet mask determines which part of the destination IP address is the network part and which part is the host part.

Gateway:

This is the IP address of the router device that allows communication between the 5G router and the destination network or host.

Interface:

Depending on where the destination IP address is located, you can select several ports, such as LAN and wireless or WAN (Internet). To delete a static route that has been configured, select the corresponding route table number and click Delete. To view the current one For detailed routing information of the 5G router, click the "Current Route" button.

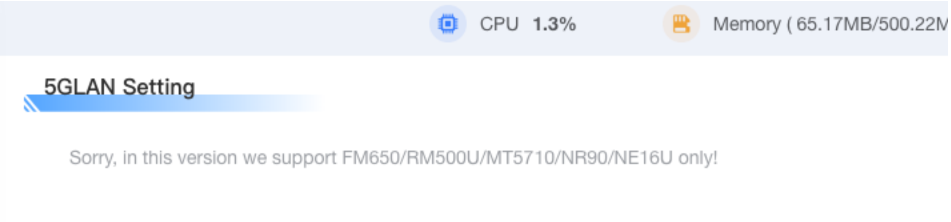


Current Route

Destination LAN NE T	Gateway	Subnet Mask	Metric	Interface
0.0.0.0	10.168.1.1	0.0.0.0	0	vlan2
10.168.1.0	0.0.0.0	255.255.255.0	0	vlan2
10.168.1.1	0.0.0.0	255.255.255.255	0	vlan2
127.0.0.0	0.0.0.0	255.0.0.0	0	lo
192.168.4.0	0.0.0.0	255.255.255.0	0	br0

When you're done modifying, click the Save Settings button to make the changes but they don't take effect, and click the Apply button to make the changes take effect.

3.7.9 5G LAN Setting



CPU 1.3%   Memory (65.17MB/500.22M

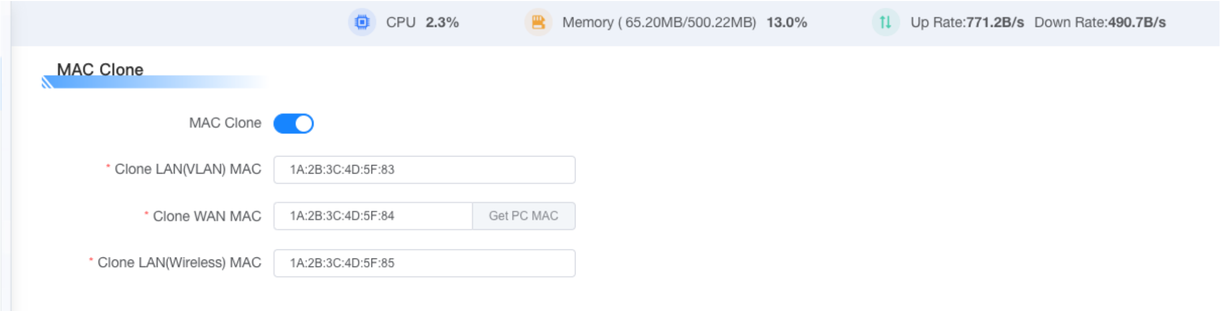
5GLAN Setting

Sorry, in this version we support FM650/RM500U/MT5710/NR90/NE16U only!

5G LAN is related to 5G modules, and only the corresponding 5G modules can support this function.

3.7.10 MAC Clone

Some ISPs may require you to register your MAC address. If you do not want to re-register your MAC address, you can clone the MAC address of the 5G router to the MAC address you registered with your ISP.



CPU 2.3%   Memory (65.20MB/500.22MB) 13.0%   Up Rate:771.2B/s Down Rate:490.7B/s

MAC Clone

MAC Clone ●

* Clone LAN(VLAN) MAC: 1A:2B:3C:4D:5F:83

* Clone WAN MAC: 1A:2B:3C:4D:5F:84 Get PC MAC

* Clone LAN(Wireless) MAC: 1A:2B:3C:4D:5F:85

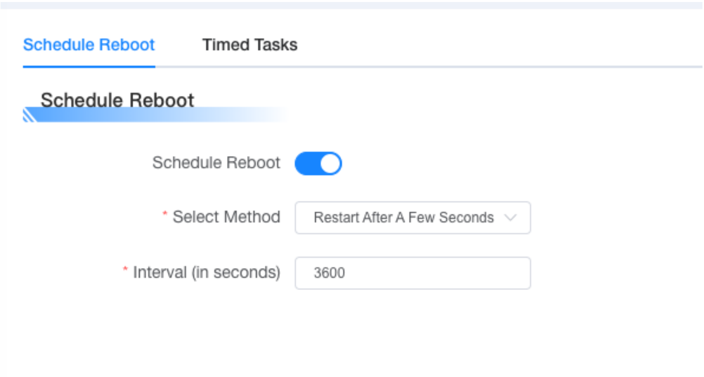
Mac address cloning can clone 3 parts, one is the clone of the LAN port, one is the clone of the WAN port, and the other is the clone of the wireless MAC address, there are two points to note, first, the MAC address is 48 bits, which cannot be set to a multicast address, that is, the first byte should be an even number. Second, since the wireless and LAN ports are connected together by bridge br0, the MAC address of bridge br0 is determined by the smaller of the MAC address of the LAN and the wireless MAC address.

3.8 Application

3.8.1 Active Policy

On the Activity Policy page, you can set Schedule Reboot and Timed Tasks

Schedule Reboot



Schedule Reboot | Timed Tasks

Schedule Reboot

Schedule Reboot: on

* Select Method: Restart After A Few Seconds

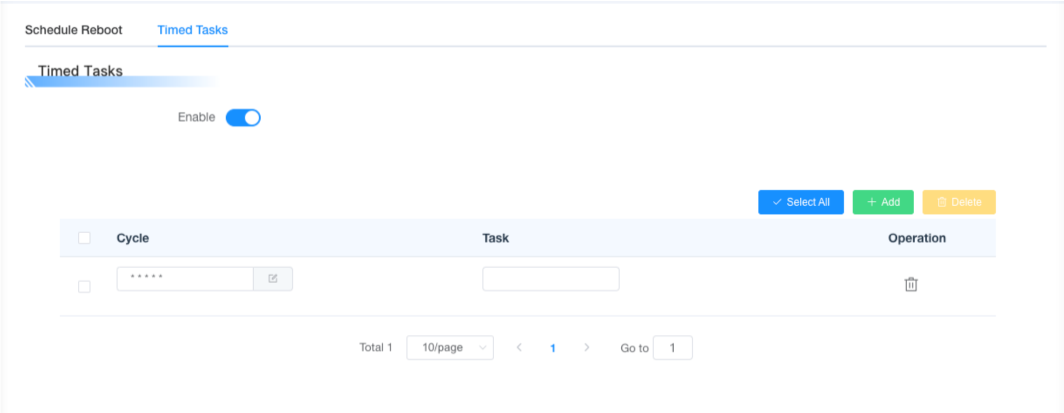
* Interval (in seconds): 3600

You can set a Schedule Reboot route:

Reboot after a scheduled time of xxx seconds

Reboot at a specific date, time, week, or day.

Timed Tasks



Schedule Reboot | Timed Tasks

Timed Tasks

Enable: on

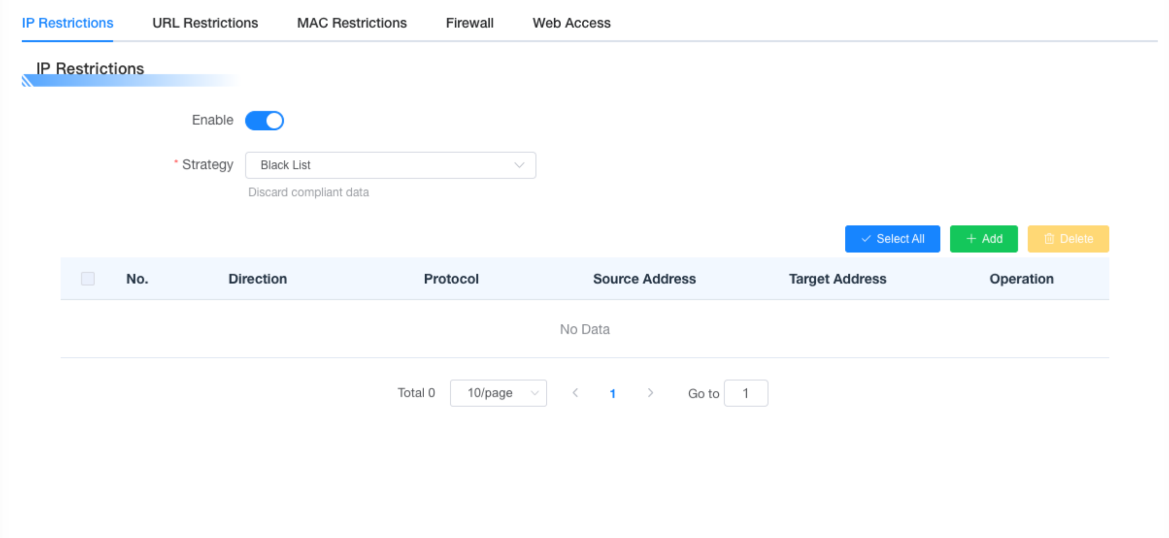
□	Cycle	Task	Operation
□	·····		

Total 1 | 10/page | 1 | Go to 1

3.8.2 Security

3.8.2.1 IP Restrictions

You can set a blacklist or whitelist to restrict the source or destination addresses of import/export, including the protocol of communication.



IP Restrictions

Enable: on

* Strategy: Black List

Discard compliant data

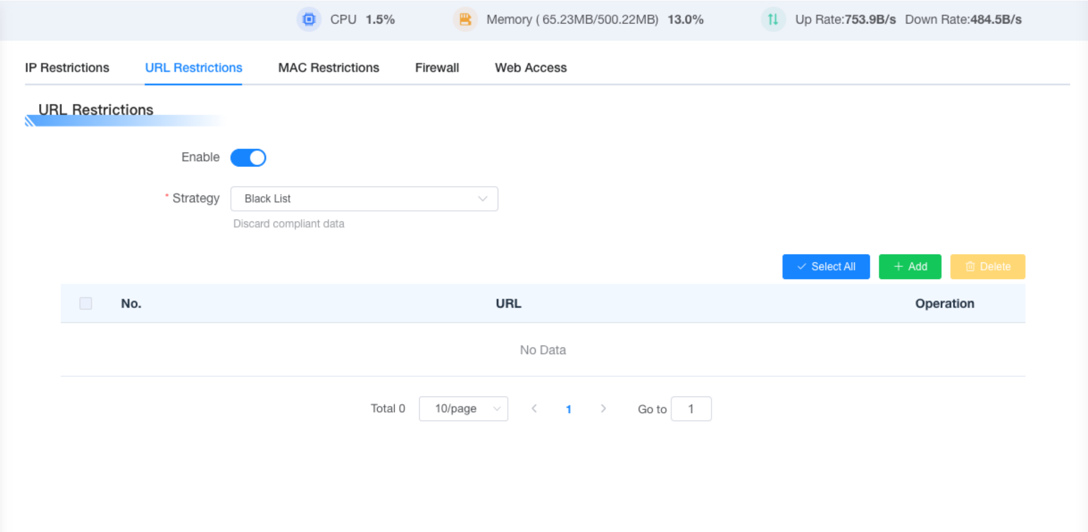
□	No.	Direction	Protocol	Source Address	Target Address	Operation

No Data

Total 0 10/page < 1 > Go to 1

3.8.2.2 URL Restrictions

You can set the URL address of the blacklist and whitelist through this column, that is, the data that meets the rules will be received, and all data that does not meet the rules will be discarded.



URL Restrictions

Enable: on

* Strategy: Black List

Discard compliant data

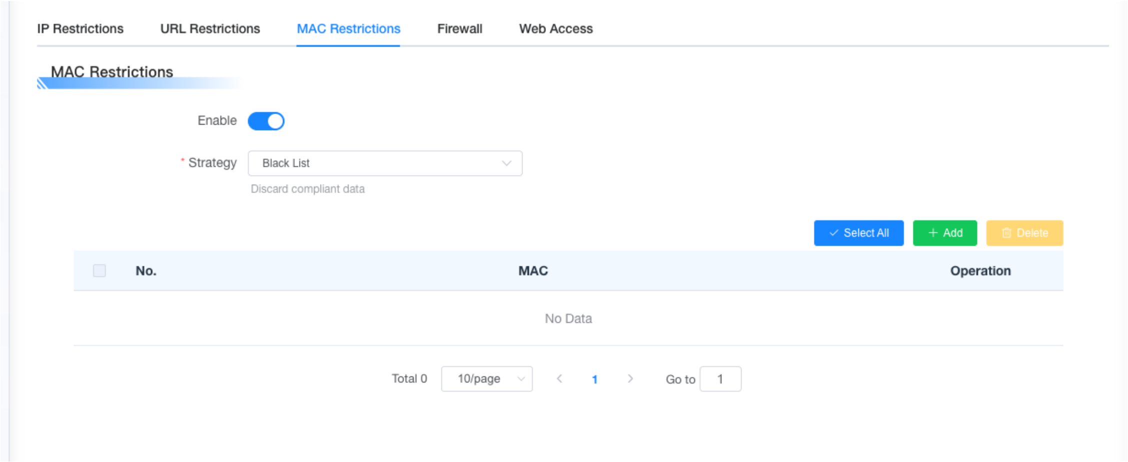
□	No.	URL	Operation

No Data

Total 0 10/page < 1 > Go to 1

3.8.2.3 MAC Restrictions

You can use this column to set the MAC address of the blacklist and whitelist, that is, to receive data that meets the rules and discard all data that does not meet the rules.



MAC Restrictions

Enable: on

* Strategy: Black List

Discard compliant data

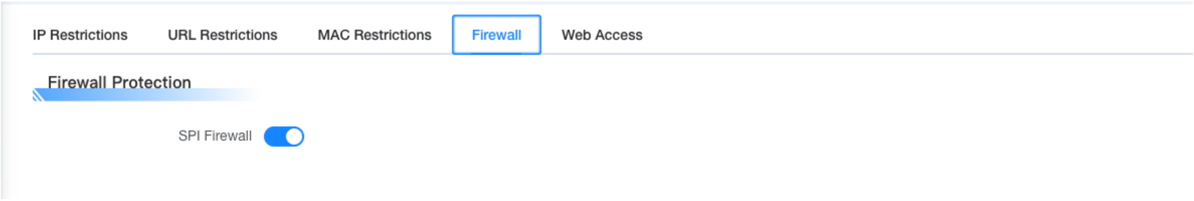
☐	No.	MAC	Operation
		No Data	

Total 0 10/page < 1 > Go to 1

3.8.2.4 Firewall

You can enable or disable firewalls, choose to filter specific Internet data types, and block anonymous Internet request, through which the security of the network is enhanced.

Firewall

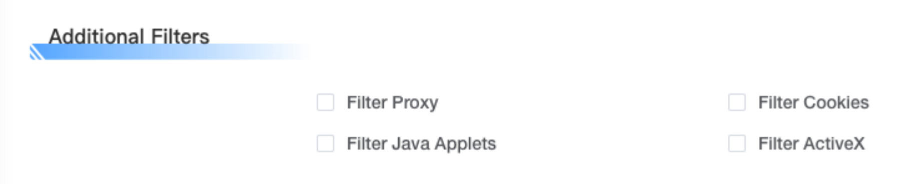


Firewall Protection

SPI Firewall: on

Firewalls enhance network security and inspect packets entering the network using Condition Monitoring (SPI), which are protected by firewalls, opt-in, or disabled. You must have the SPI firewall enabled to use other firewall features: filtering proxies, blocking WAN requests, and so on.

Additional Filters



Additional Filters

☐ Filter Proxy ☐ Filter Cookies

☐ Filter Java Applets ☐ Filter ActiveX

Filter Proxy:

Using a WAN proxy server can reduce the security of the router, and filtering proxies will reject any-to-any WAN Proxy server access, click the checkbox to enable proxy filtering or invert the check to disable the feature.

Filter Cookies:

Cookies are pieces of data that are stored on your computer by a website and used when you interact with an Internet site. Click the checkbox to enable cookie filtering or invert the check box to disable the feature.

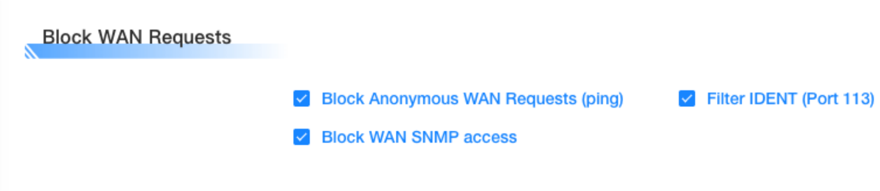
Filter Java applets:

If you reject Java, you may not be able to open a web page programmed with Java tools, click the checkbox to enable Java applet filtering or invert the check box to disable the feature.

Filter ActiveX:

If you reject ActiveX, you may not be able to open web pages programmed with ActiveX tools, click the checkbox to enable ActiveX filtering or invert the check to disable the feature.

Block WAN Requests



Block WAN Requests

☑ Block Anonymous WAN Requests (ping) ☑ Filter IDENT (Port 113)

☑ Block WAN SNMP access

Block Anonymous WAN Requests (ping):

Enable this feature to prevent your network from being pinged or probed by other Internet users, making it more difficult for external users to hack into your network by checking the box next to the "Block Anonymous Internet" request, which is enabled by default and allows anonymous Internet requests by selecting Disable.

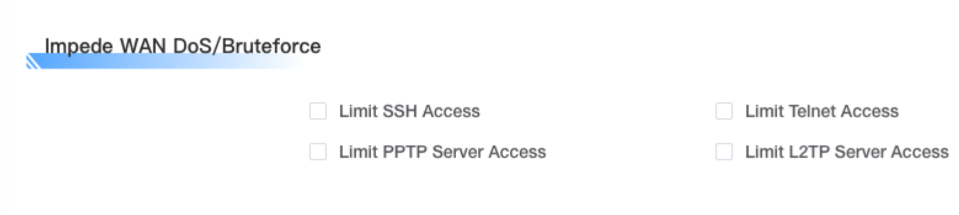
Filter IDENT (port 113):

This feature saves port 113 from being scanned by devices outside of your local network. Select Enable to filter port 113 or disable it.

Block WAN SNMP access:

This feature blocks SNMP connection requests from the WAN.

Impede WAN Dos/Bruteforce



Impede WAN DoS/Bruteforce

□ Limit SSH Access □ Limit Telnet Access

□ Limit PPTP Server Access □ Limit L2TP Server Access

Restrict SSH Access:

This feature restricts SSH access requests from the WAN to a maximum of 2 SSH connection requests per minute for the same IP.

Restrict Telnet Access:

This feature restricts Telnet access requests from the WAN to a maximum of 2 Telnet connection requests per minute for the same IP.

Restrict PPTP Server Access:

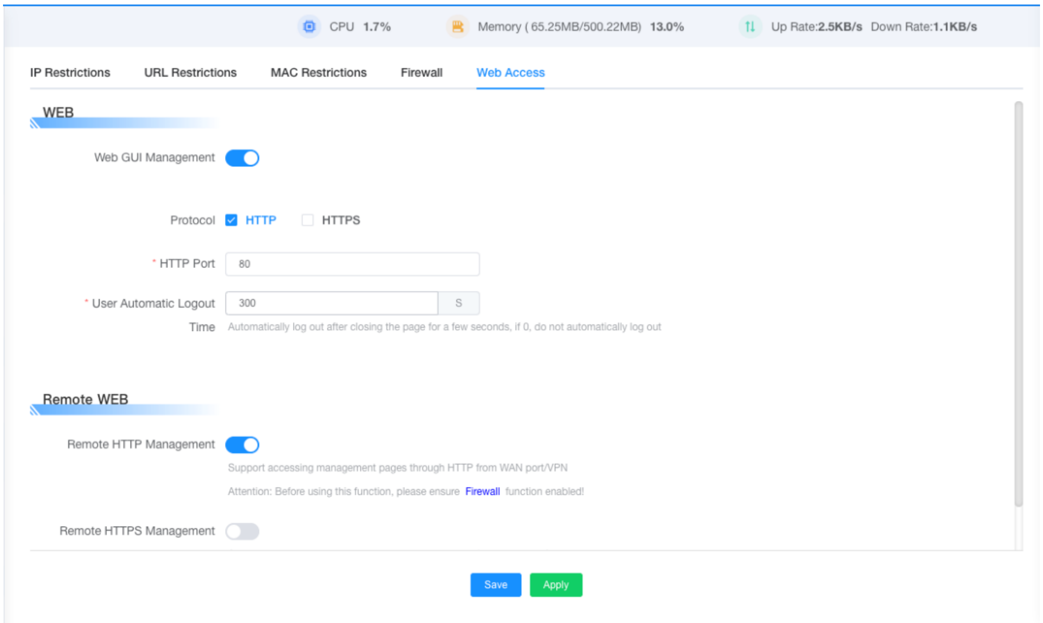
When a PPTP server is established on the device, this feature restricts PPTP from the WAN Access requests, up to 2 PPTP connection requests per minute for the same IP.

Restrict L2TP Server Access:

When a device establishes an L2TP server, this feature restricts L2TP from the WAN Access requests, up to 2 L2TP connection requests per minute for the same IP.

3.8.2.5 WEB Access

You can set the local web access protocol, port, and user logout time; and how remote web access is managed.



Web GUI Management ●

Protocol ☑ HTTP □ HTTPS

* HTTP Port 80

* User Automatic Logout Time 300 S

Automatically log out after closing the page for a few seconds, if 0, do not automatically log out

Remote HTTP Management ●

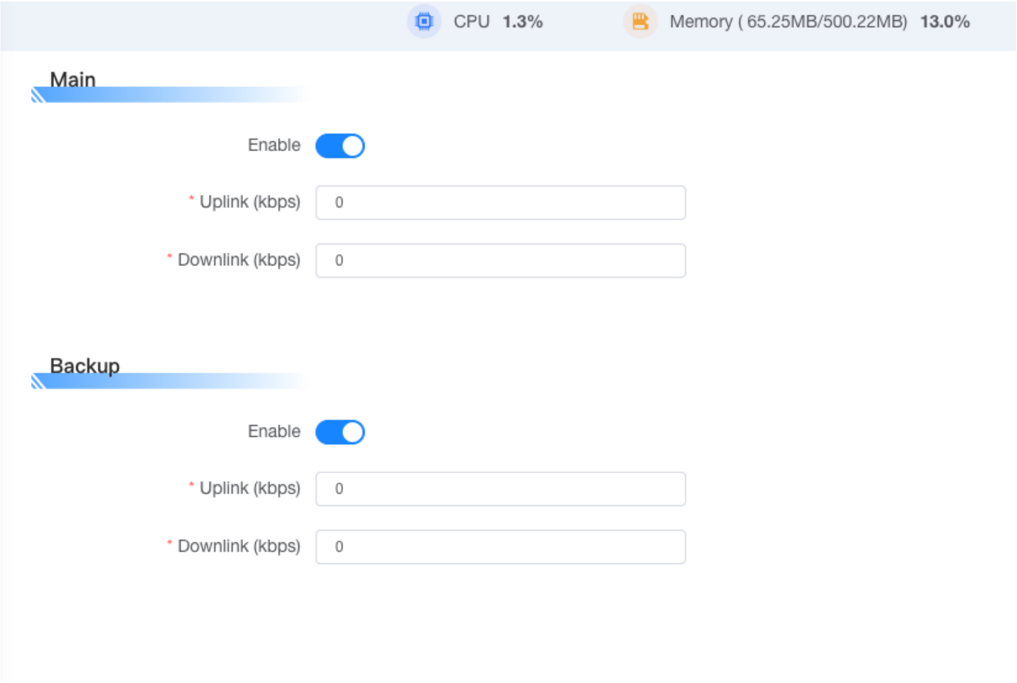
Support accessing management pages through HTTP from WAN port/VPN

Attention: Before using this function, please ensure Firewall function enabled!

Remote HTTPS Management ○

3.8.3 QOS

Use the QOS feature to limit the traffic for uploads and downloads separately, and you can set the maximum upload and download rates for the primary and secondary links separately.



CPU 1.3%   Memory (65.25MB/500.22MB) 13.0%

Main

Enable ●

* Uplink (kbps) 0

* Downlink (kbps) 0

Backup

Enable ●

* Uplink (kbps) 0

* Downlink (kbps) 0

Upload (kbps):

This field is filled in with the bandwidth you allocate to upload, which is typically 80% to 90% of the maximum bandwidth you have in actual use.

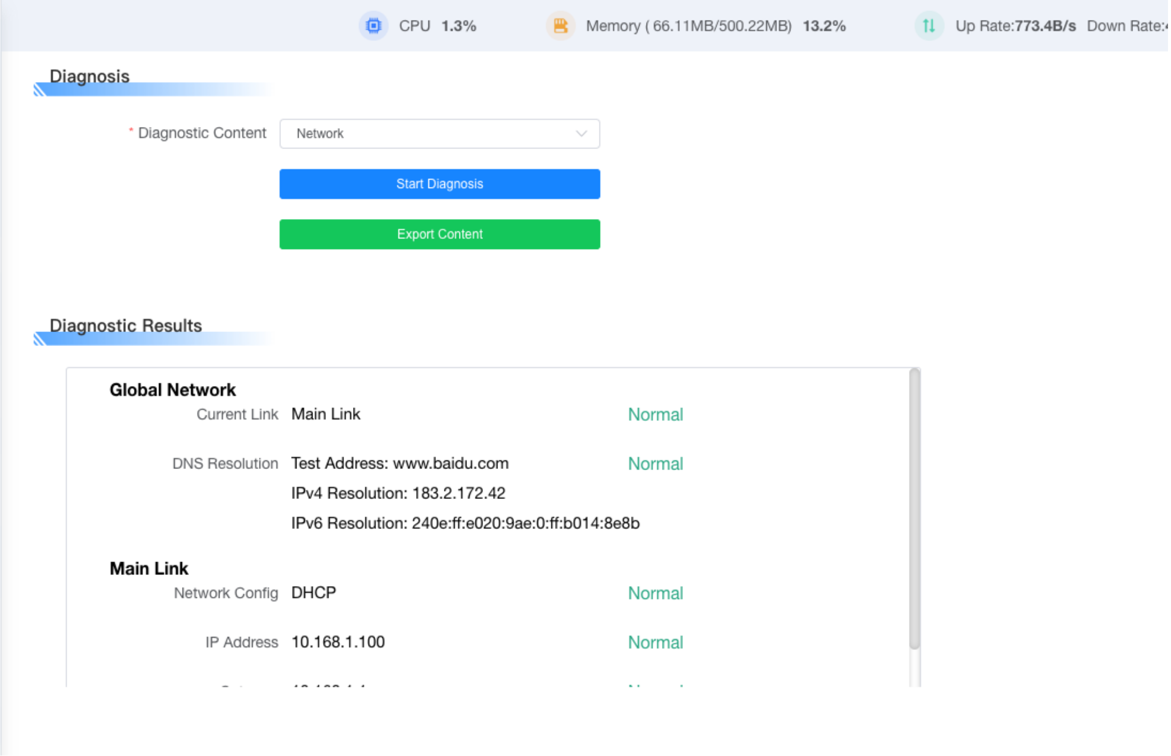
Download (kbps):

This field is filled in with the bandwidth you allocate to the download, which is generally the maximum bandwidth you have in actual use

3.9 Maintenance

3.9.1 Diagnosis

You can click Start Diagnosis, and the device will diagnose the current active and standby links, prompt you if there is an abnormality, or you can choose to export the current diagnostic content.



* Diagnostic Content: Network

Global Network

Current Link: Main Link — Normal

DNS Resolution: Test Address: www.baidu.com — Normal
IPv4 Resolution: 183.2.172.42
IPv6 Resolution: 240e:ff:e020:9ae:0:ff:b014:8e8b

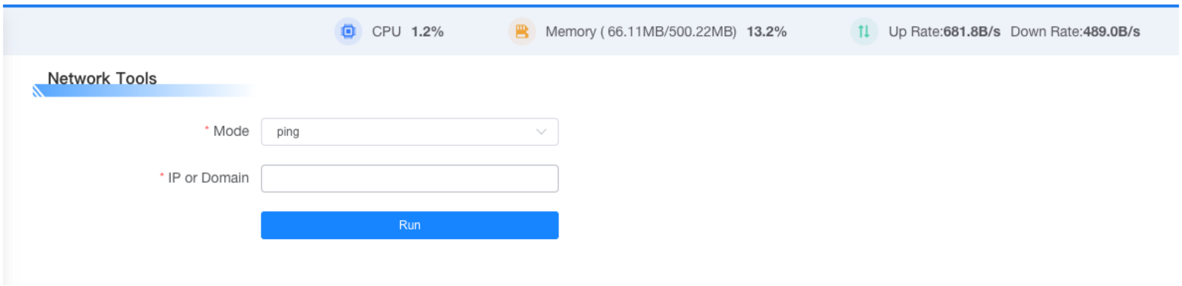
Main Link

Network Config: DHCP — Normal

IP Address: 10.168.1.100 — Normal

3.9.2 Network Tools

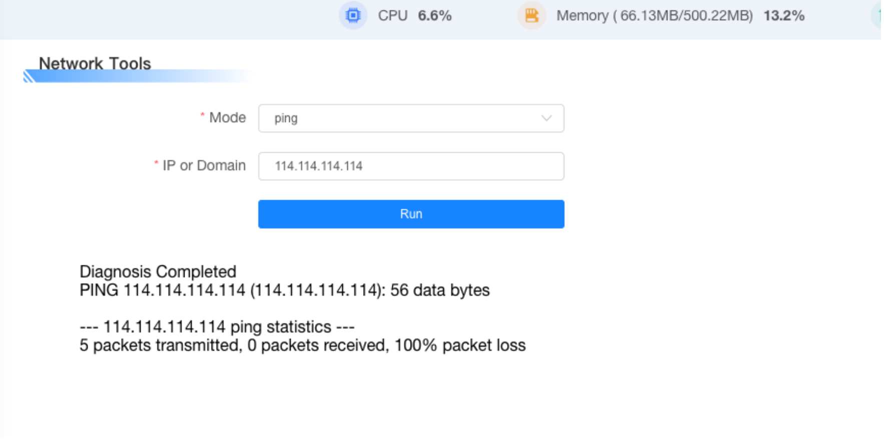
There are three modes in the network tool: ping, traceroute, and nslookup, which can be used to analyze the device.


CPU 1.2%
Memory (66.11MB/500.22MB) 13.2%
Up Rate:681.8B/s Down Rate:489.0B/s
Network Tools
Run

* Mode: ping

* IP or Domain:

For reference, please refer to the following:



* Mode: ping

* IP or Domain: 114.114.114.114

```
Diagnosis Completed
PING 114.114.114.114 (114.114.114.114): 56 data bytes

--- 114.114.114.114 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

3.9.3 Commands

You can run the command line through the command window.

Startup Command:

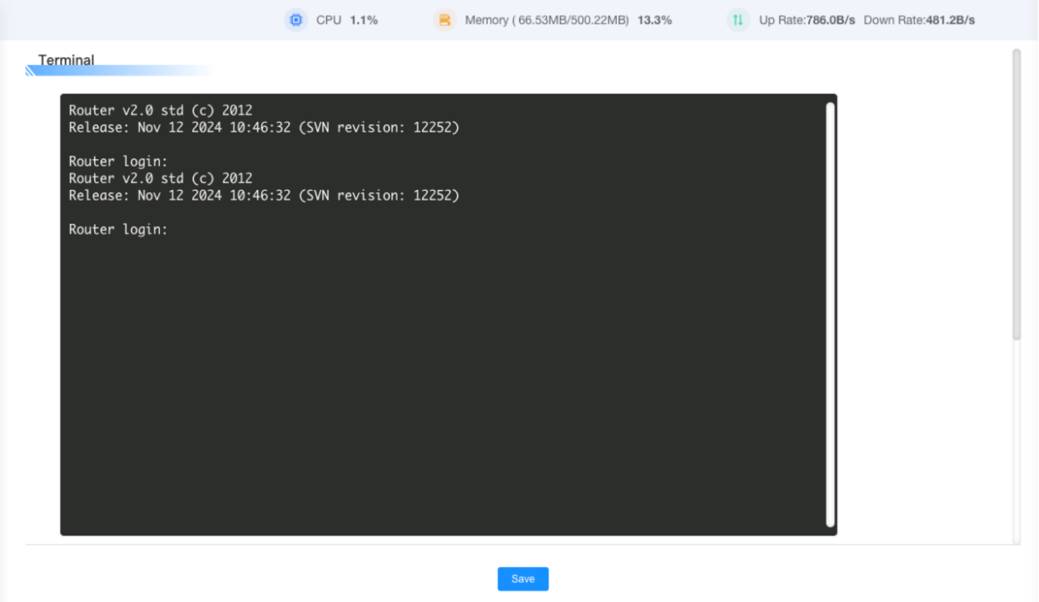
A command line that is self-executing when a 5G router boots up.

Shutdown Command:

A 5G router that executes itself on the command line when powered off.

Firewall Directives:

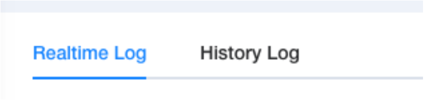
Every time the firewall is started, it can run some custom iptables directives.


CPU 1.1%
Memory (66.53MB/500.22MB) 13.3%
Up Rate:786.0B/s Down Rate:481.2B/s
Terminal
Save

```
Router v2.0 std (c) 2012
Release: Nov 12 2024 10:46:32 (SVN revision: 12252)

Router login:
Router v2.0 std (c) 2012
Release: Nov 12 2024 10:46:32 (SVN revision: 12252)

Router login:
```

This window is the device terminal, which can be logged in to the device through the device's username and password, and the corresponding command operation can be performed on the device and inquiry, etc.

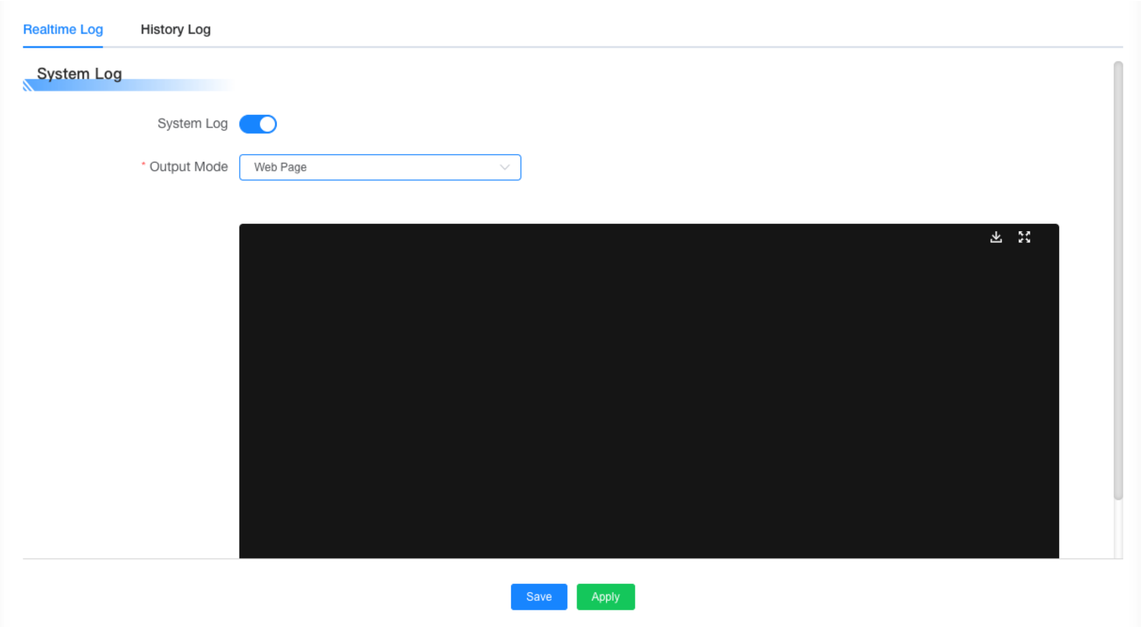
3.9.4 Log



You can choose to view Realtime Log or set up History Log

Realtime Log

Realtime Log can be viewed in real time on the local web to analyze problems, or they can be output through serial ports. Send via network.

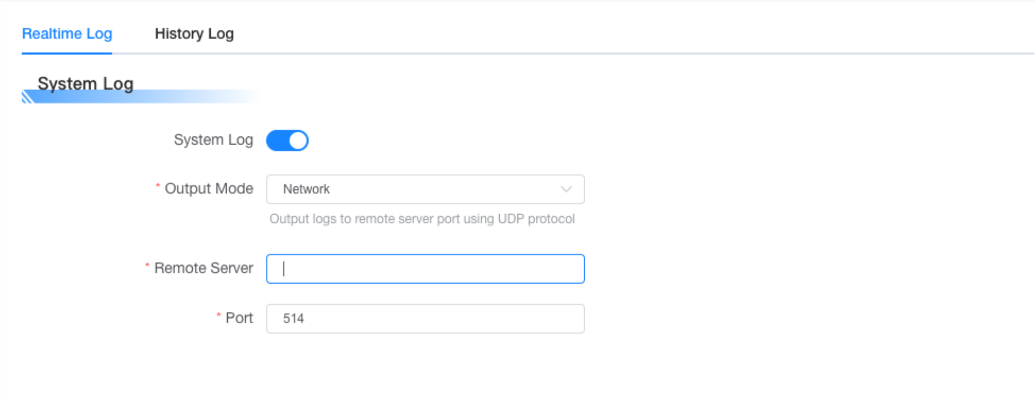


System Log

System Log: on

* Output Mode: Web Page

In the Network mode, UDP mode is used by default, and the corresponding remote server address and port need to be configured to receive log messages Please note that when the network mode is turned on for transmission, the traffic of the device will be occupied, and if the data card service package is small, you need to pay attention.



System Log

System Log: on

* Output Mode: Network

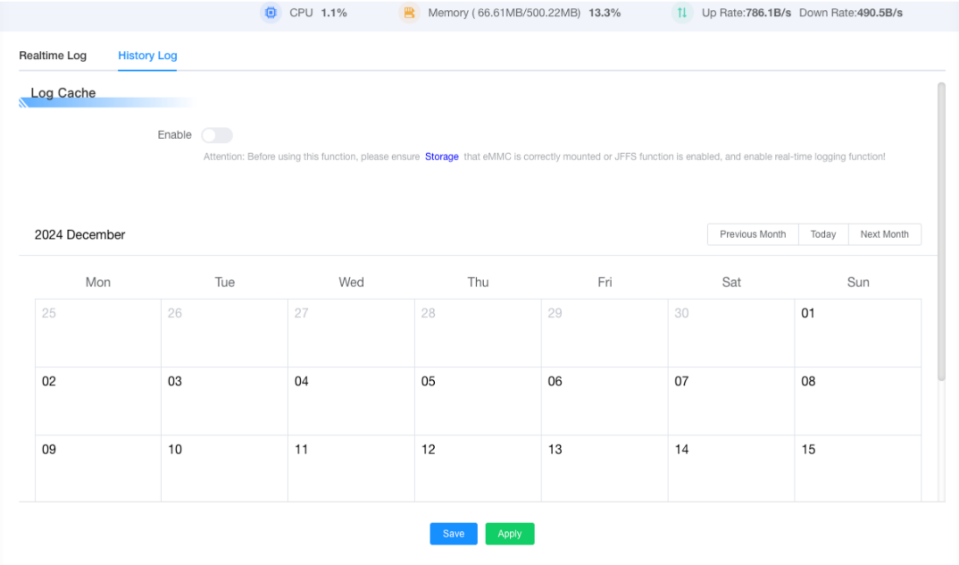
Output logs to remote server port using UDP protocol

* Remote Server:

* Port: 514

History Log

Log caching requires that your device has eMMC or a larger JFFS function, if it cannot be enabled, it means that the device does not have this function.



CPU 1.1% Memory (66.61MB/500.22MB) 13.3% Up Rate:786.1B/s Down Rate:490.5B/s

Log Cache

Enable

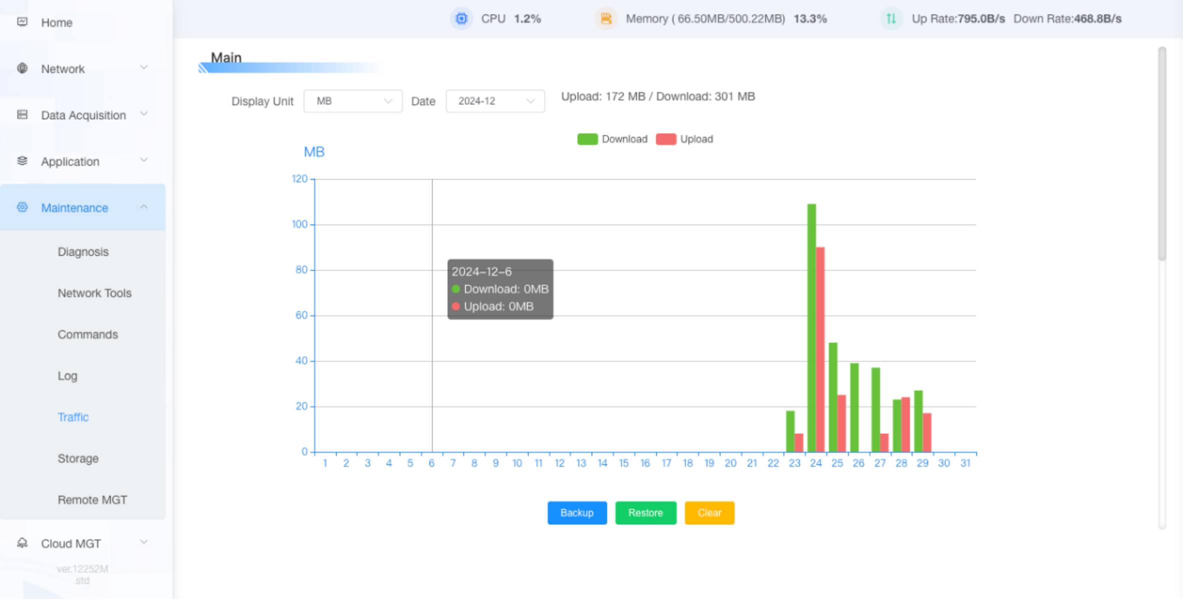
Attention: Before using this function, please ensure Storage that eMMC is correctly mounted or JFFS function is enabled, and enable real-time logging function!

2024 December

Mon	Tue	Wed	Thu	Fri	Sat	Sun
25	26	27	28	29	30	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15

3.9.5 Traffic

This page is used to count the traffic that the device runs in the current month



CPU 1.2% Memory (66.50MB/500.22MB) 13.3% Up Rate:795.0B/s Down Rate:468.8B/s

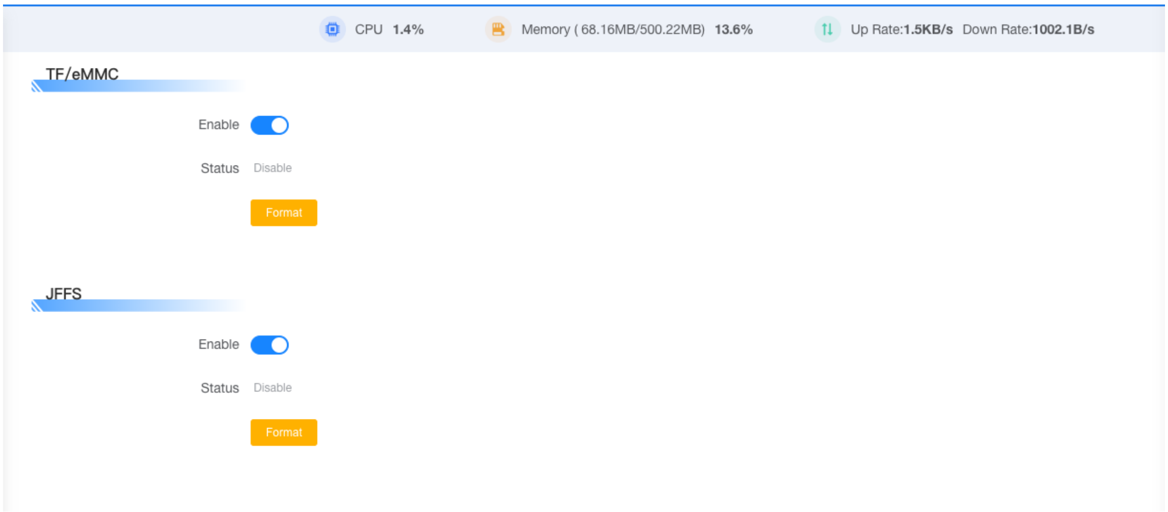
Main

Display Unit MB Date 2024-12 Upload: 172 MB / Download: 301 MB

Collect statistics on the traffic information of WAN ports, and record and display the total daily uplink and downlink traffic of the month.

3.9.6 Storage

The default is disabled, and you can format it first when you enable it for the first time (you don't need to do it when you are not enabled for the first time to prevent accidental deletion) Once enabled, you can see the size of the JFFS or eMMC. If you enable historical log caching or other storage needs, you need to use this function first After enabling it.



CPU 1.4% Memory (68.16MB/500.22MB) 13.6% Up Rate:1.5KB/s Down Rate:1002.1B/s

TF/eMMC

Enable ●

Status Disable

JFFS

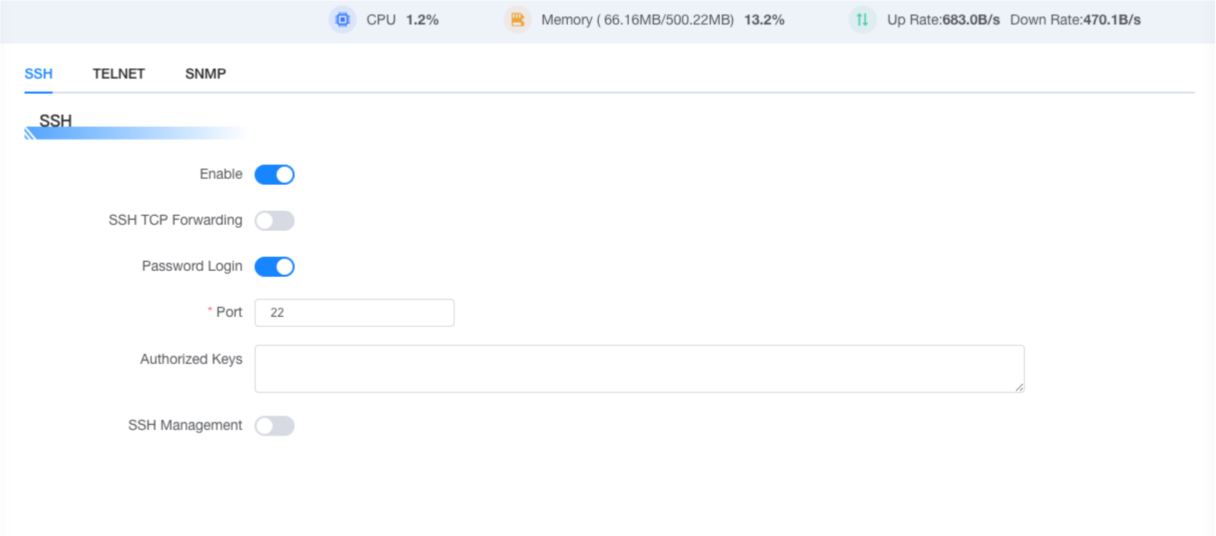
Enable ●

Status Disable

3.9.7 Remote Management

3.9.7.1 SSH

Once the SSHD service is enabled, remote access to your 5G router's operating system is allowed through an SSH client



CPU 1.2% Memory (66.16MB/500.22MB) 13.2% Up Rate:683.0B/s Down Rate:470.1B/s

SSH

Enable ●

SSH TCP Forwarding ○

Password Login ●

* Port 22

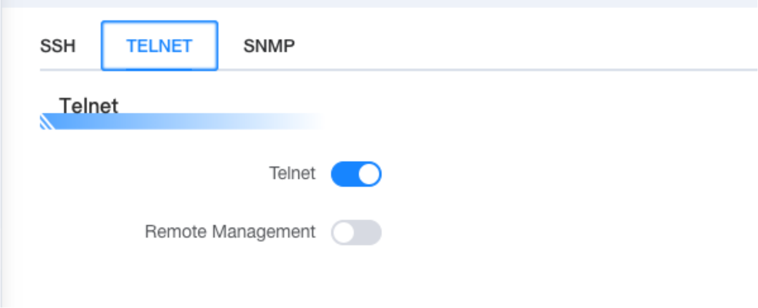
Authorized Keys

SSH Management ○

SSH TCP Forwarding: Whether TCP forwarding is supported
Password Login: Whether a password is required to log in
Port: Set the port of SSHD, the default system is set to 22 ports
Authorized Keys: Set as needed, and use the system login password and user name by default

3.9.7.2 Telnet

Enable or disable the Telnet feature



Telnet

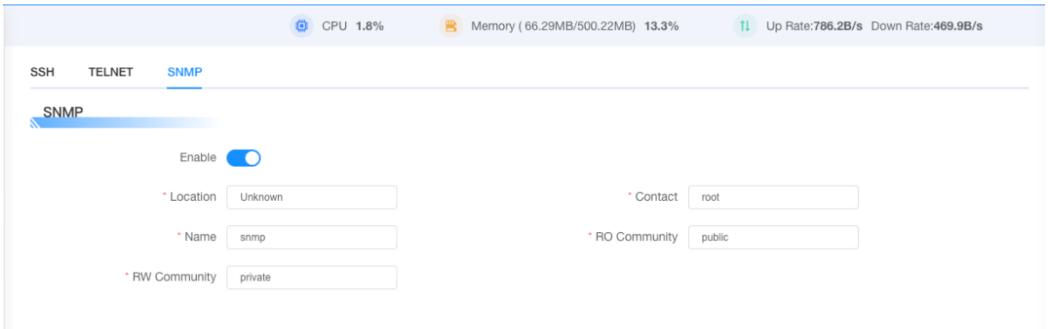
Telnet ●

Remote Management ○

The local Telnet function is enabled by default, and Telnet remote management is disabled by default.

3.9.7.3 SNMP

You can set parameters such as Location, Contact, Name, Read-Only Community, and Read-Write Community.


CPU 1.8%
Memory (66.29MB/500.22MB) 13.3%
Up Rate:786.2B/s Down Rate:469.9B/s
SSH
TELNET
SNMP

SNMP

Enable ●

* Location: Unknown

* Contact: root

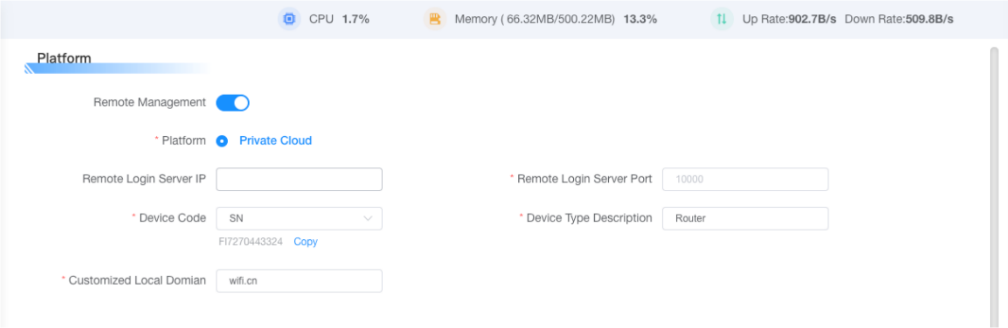
* Name: snmp

* RO Community: public

* RW Community: private

Enabled: Enables or disables SNMP.
Location: Describes the physical location where the SNMP device is located.
Contact: The name of the SNMP administration.
Name: The name of the SNMP.
Read-Only Community: SNMP read-only string that allows SNMP clients to read device information.
Read-Write Community: SNMP reads and writes strings that allow SNMP clients to read and modify device information.

3.10 Cloud Management



CPU 1.7% Memory (66.32MB/500.22MB) 13.3% Up Rate:902.7B/s Down Rate:509.8B/s

Platform

Remote Management: on

* Platform: ● Private Cloud

Remote Login Server IP:

* Remote Login Server Port: 10000

* Device Code: SN

FI7270443324 Copy

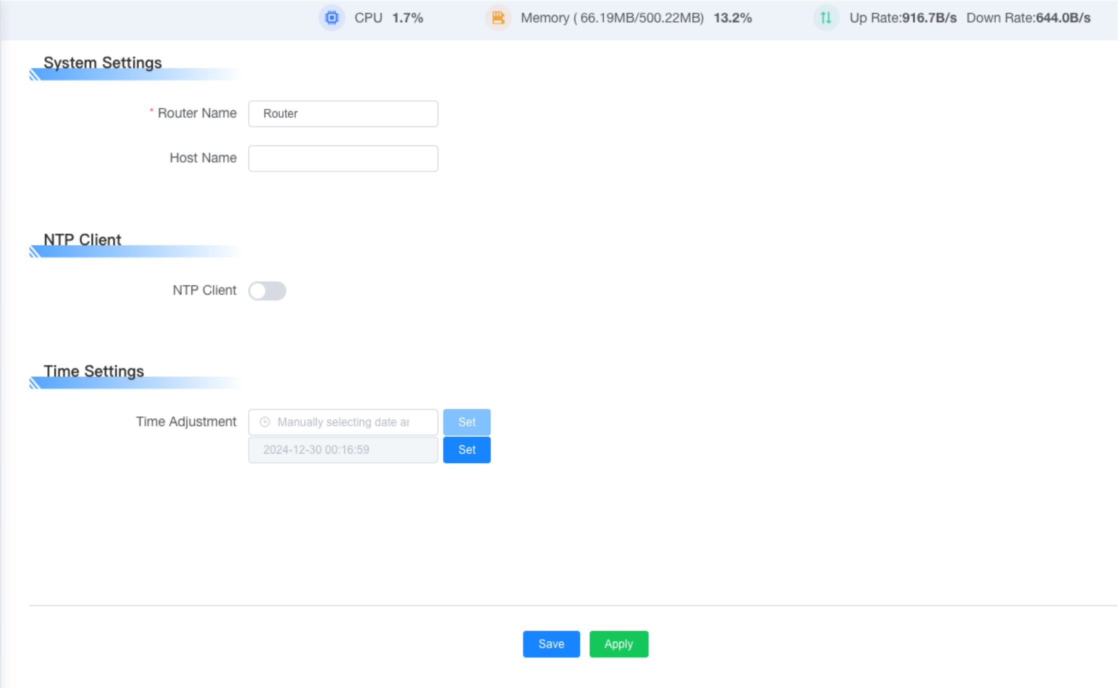
* Device Type Description: Router

* Customized Local Domian: wifi.cn

If you have the corresponding device management platform account, you can set the management address of our cloud platform, or if you have subscribed for a private cloud platform deployment, you can set the corresponding cloud platform address and port, and the device code is the SN and unique of the device by default.

3.11 System

3.11.1 System Settings



CPU 1.7% Memory (66.19MB/500.22MB) 13.2% Up Rate:916.7B/s Down Rate:644.0B/s

System Settings

* Router Name: Router

Host Name:

NTP Client

NTP Client: off

Time Settings

Time Adjustment: Manually selecting date ar [Set]

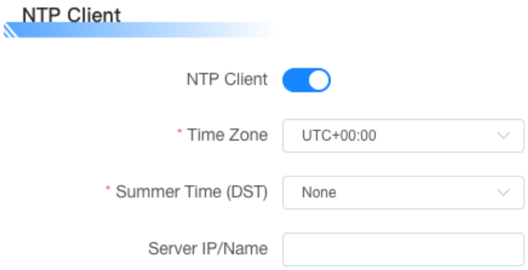
2024-12-30 00:16:59 [Set]

System Settings

In the System Settings bar, you can set the router name and host name, and the configuration option has a default value, or you can choose to customize.

NTP client

The NTP client is disabled by default, and when enabled, you can set the corresponding server address, and the 5G router can perform NTP timing calibration on the basis of this NTP server.



NTP Client

NTP Client ●

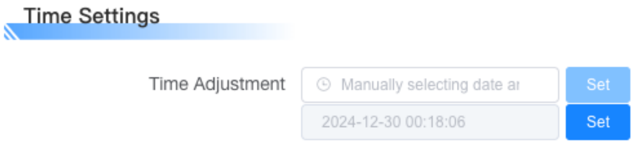
* Time Zone: UTC+00:00

* Summer Time (DST): None

Server IP/Name:

Time Settings

If you need to change the time of the current device, you can set it here.



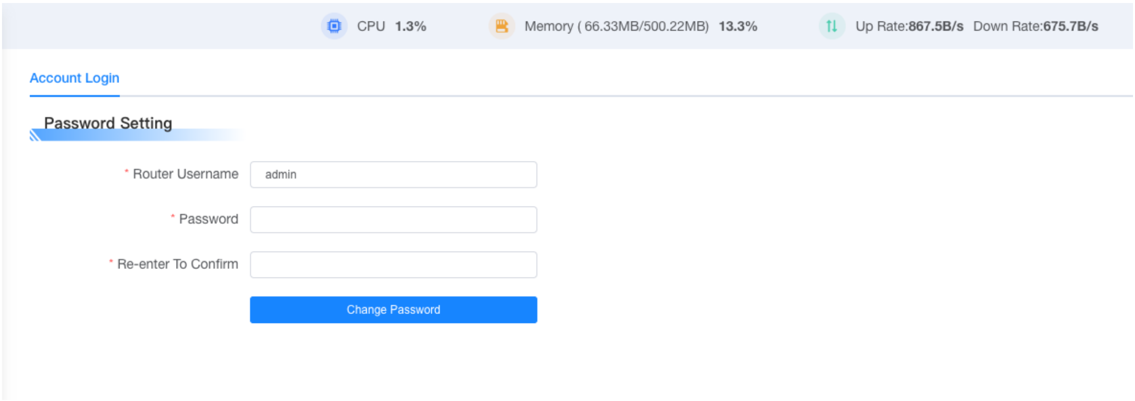
Time Settings

Time Adjustment: Manually selecting date ar | Set

2024-12-30 00:18:06 | Set

3.11.2 Login Management

This page can be used to change the login and password of the device.



CPU 1.3% Memory (66.33MB/500.22MB) 13.3% Up Rate:867.5B/s Down Rate:675.7B/s

Account Login

Password Setting

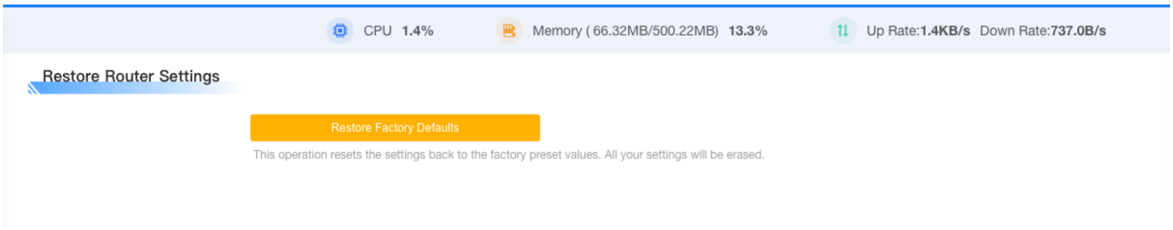
* Router Username: admin

* Password:

* Re-enter To Confirm:

Change Password

3.11.3 Restore



CPU 1.4% Memory (66.32MB/500.22MB) 13.3% Up Rate:1.4KB/s Down Rate:737.0B/s

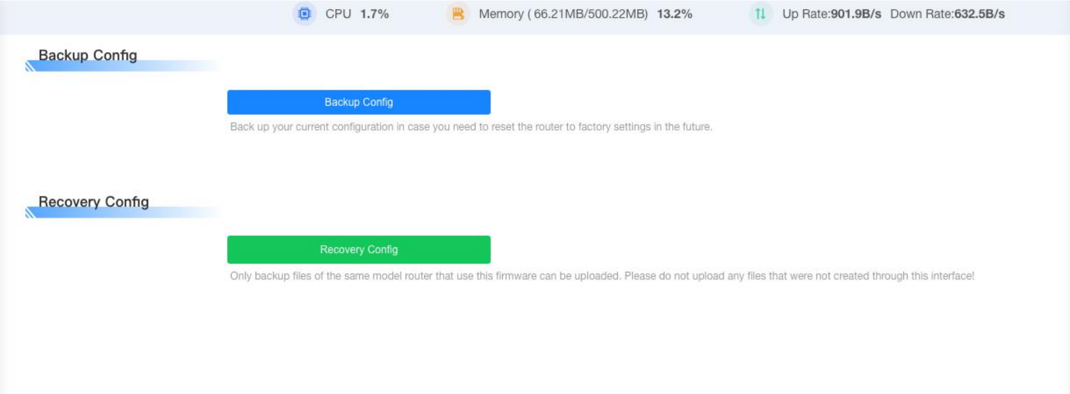
Restore Router Settings

Restore Factory Defaults

This operation resets the settings back to the factory preset values. All your settings will be erased.

Please note that if your parameters are not saved, you can configure and back up the parameters first, and then click Restore Factory Default, otherwise the device will be restored to the factory state, and the original configuration parameters will be cleared.

3.11.4 Backup


CPU 1.7%
Memory (66.21MB/500.22MB) 13.2%
Up Rate:901.9B/s Down Rate:632.5B/s
Backup Config
Backup Config
Recovery Config
Recovery Config

Back up your current configuration in case you need to reset the router to factory settings in the future.

Only backup files of the same model router that use this firmware can be uploaded. Please do not upload any files that were not created through this interface!

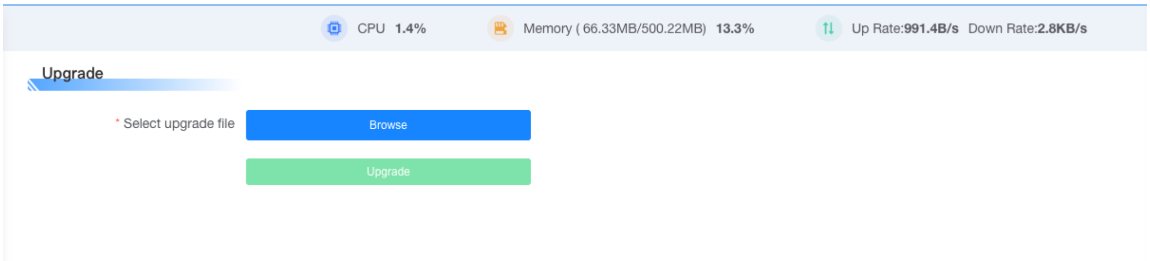
Backup the Config

Select the Backup Configuration button to download the configuration parameters of the current device and use it to save or import it to other devices for configuration Resume the replication of configuration parameters.

Recovery Config

You can import the backup file of the same model router into the device by selecting the corresponding file through the Restore Configuration button, Note: Do not upload any files that are not created through this interface!

3.11.5 Upgrade


CPU 1.4%
Memory (66.33MB/500.22MB) 13.3%
Up Rate:991.4B/s Down Rate:2.8KB/s
Upgrade
* Select upgrade file
Browse
Upgrade

New firmware can be loaded onto the 5G gateway. If there are no issues with the 5G gateway, you don't need to download an updated firmware version unless the new version includes the new features you want to use.

Click Browse, select the firmware file you want to upgrade, and then click the Upgrade button to start the firmware upgrade. It will take a few minutes to upgrade the firmware, please do not turn off the power or press the reset button.

Note: When you upgrade the firmware of your 5G gateway, you may lose its configuration settings, so make sure you back up your 5G gateway's settings before upgrading the firmware.