Industrial Cellular Router

R10 R10A

Industrial cellular Router

R10 R10A

User Manual

Ver 1.0

Date updated: 2022-8-26

Shenzhen Beilai Technology Co.,Ltd

www.iot-solution.com

Preface

Thank you for using the industrial cellular router of Shenzhen Beilai Technology Co., LTD. Reading this product manual will enable you to quickly master the functions and usage of this product.

Copyright statement

Disclaimer

If the equipment can no longer be used due to the carrier's network upgrade, the company cannot provide free upgrade service. If the operator's network service is interrupted due to special reasons, the machine will not work normally, and the company will not bear the consequences.

This product is mainly used for data transmission based on 4G networks application, please provide the parameters according to the specifications and technical specifications used, at the same time please note especially 4G radio products should pay attention to when using the matters needing attention, the company does not undertake due to abnormal use or improper use or personal injury caused by the product property.

Revision History

Updated date	Version	Instructions	Author
2022.08.26	V1.0	The first edition	XJH

Models Selection Table

Model	SIM card	WiFi mode	RS 232	RS 485	GPS	Micro USB	Extend Function
R10	1	2	Multiplexing		optional	support	Modbus Slave/MQTT
R10A	1	2	Multiplexing		optional	support	Modbus Master /Slave /MQTT

Directory

1. Product introduction

1. 1. Brief Introduction

R10A is not only an industrial-grade router, but also has outstanding feature such as programmable logic control, cycle timer, edge computing and replaces PLC to a certain extent. it can be used as Modbus RTU/TCP Master for data acquisition, convert Modbus to MQTT protocol, or Transparently Transmit data (Pass-through). One-click directly connect to multiple cloud platforms such as AWS IoT, Thingsboard cloud, Huawei cloud etc. It is suitable for remote monitoring and remote control.

Router function:

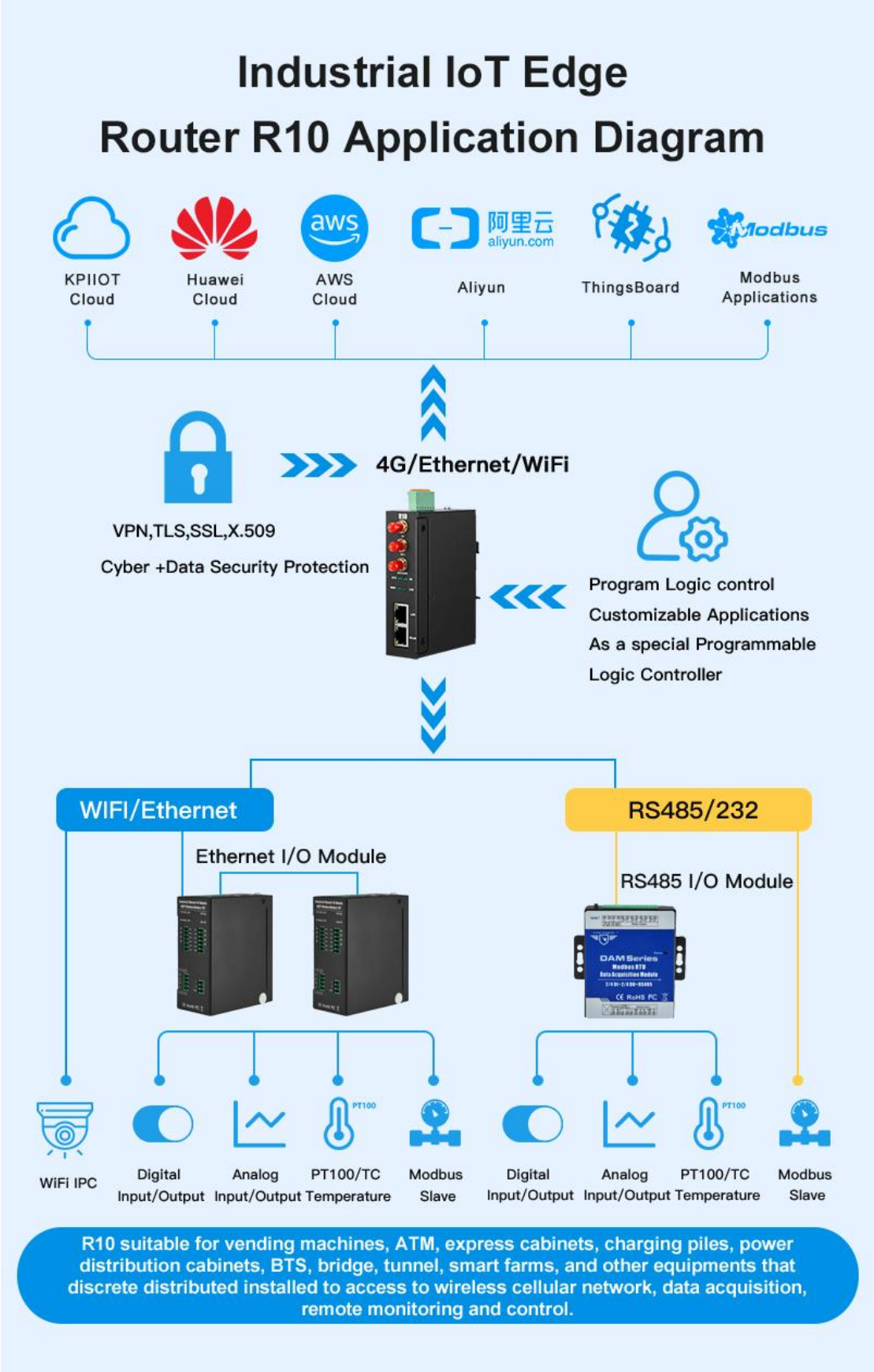
R10A support WiFi both AP mode and Client mode. It can provide Internet access for other networking devices, such as IP camera.

Data acquisition DAQ and cloud monitoring :

R10A can performs Modbus Master to poll data from meters/sensors , and then transmit data to cloud platform for remote monitoring

Extension function :

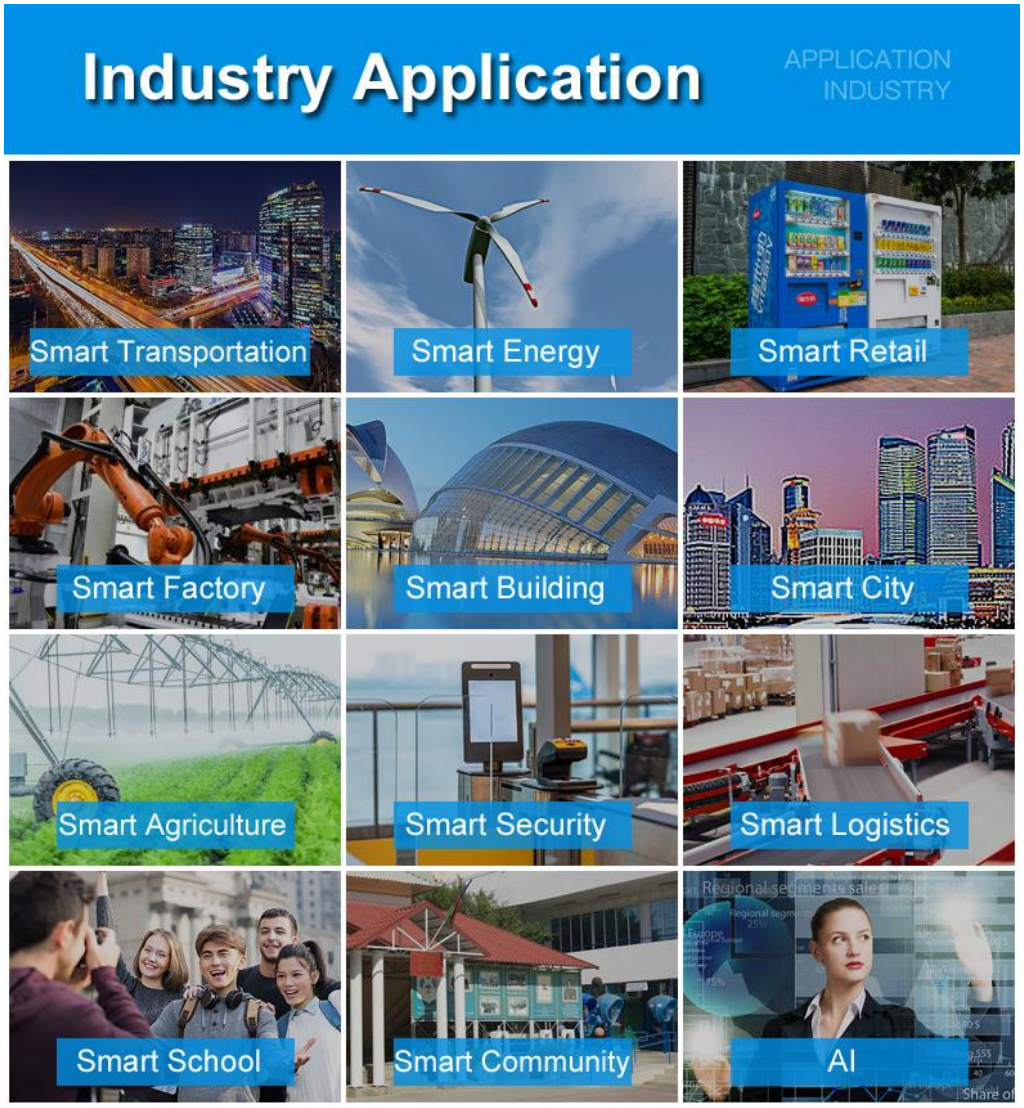
R10A can connect the I/O modules either by RS485/232 or Ethernet cable, so as to extend I/O .


Industrial IoT Edge
Router R10 Application Diagram
KPIIOT Cloud
Huawei Cloud
AWS Cloud
Aliyun
ThingsBoard
Modbus Applications
4G/Ethernet/WiFi
VPN,TLS,SSL,X.509
Cyber +Data Security Protection
Program Logic control
Customizable Applications
As a special Programmable
Logic Controller
WIFI/Ethernet
RS485/232
Ethernet I/O Module
RS485 I/O Module
WiFi IPC
Digital Input/Output
Analog Input/Output
PT100/TC Temperature
Modbus Slave
Digital Input/Output
Analog Input/Output
PT100/TC Temperature
Modbus Slave
R10 suitable for vending machines, ATM, express cabinets, charging piles, power distribution cabinets, BTS, bridge, tunnel, smart farms, and other equipments that discrete distributed installed to access to wireless cellular network, data acquisition, remote monitoring and control.

1. 2. Typically Applications

R10 router can be widely used in the M2M industry in the Internet of Things industry chain. Such as smart power grid, intelligent transportation, smart home, financial Internet of Things wireless communication router, mobile POS terminal, supply chain automation, industrial automation, intelligent building, fire protection, public safety, environmental protection, meteorology, digital medical, remote sensing survey, agriculture, forestry, water, coal, petrochemical and other fields.

BTS Monitoring, Security Alarm System applications, Supervision and monitoring alarm systems, Automatic monitoring system, Vending Machines security protection, Pumping Stations, Tanks, Oil or Water levels, Buildings and Real Estate, Weather Stations, River Monitoring and Flood Control, Oil and gas pipelines, Corrosion protection, Temperatures, water leakage applications, Wellheads, boat, vehicle, Energy saving, street lights control system, Valve controls, Transformer stations, Unmanned machine rooms, Control room application, Automation System, M2M, etc.



1. 3. Safety instructions

Safety instructions

Please do not use this product in places where mobile phones are prohibited!

Radio interference

This product uses GSM/GPRS/3G/4G wireless network, please pay attention to wireless interference

1. 4. Standard Packing List

Before installing and using the equipment, please check whether the following materials are available in the product packaging box. (pictures are for reference only)

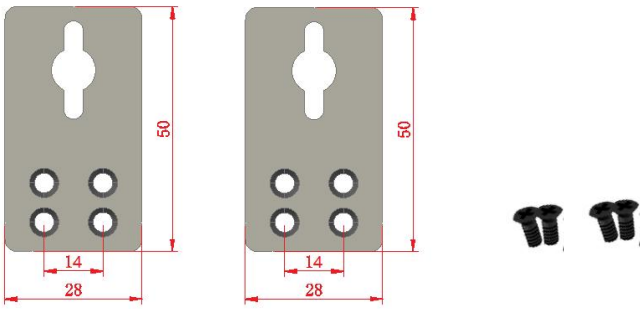
- 1 x Router device

- 1 x 7PIN 3.5mm Terminal

- 1 x antenna for 2G/3G/4G cellular

- 2 x antenna for WIFI 2.4G

- 2 x bracket kit for wall-mounted

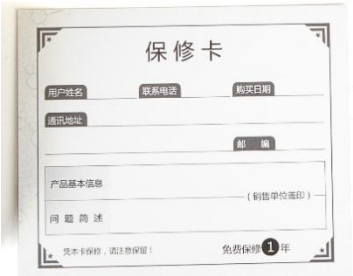


- 1 x bracket kit for DIN rail mounted

- 1 x Instruction Manual (PDF version)

  Note: Please scan the card QR code to download
- 1 x Certificate of QC pass

- 1 x Warranty card



Note: The package does not include any SIM card or Power Adapter

1. 5. Main Features

- Supports 4G wireless Internet access, and APN parameters can be set.
- Intelligent anti-drop line, support online detection, online maintenance, automatic redial, ensure that the device is always online；
- Cloud remote background management, remote upgrade and remote configuration；
- GPS is supported and location data can be published via MQTT；
- Supports VPN protocols such as L2TP, IPSEC, and OPENVPN；
- Support RS485 and RS232 serial port transparent transmission and MODBUS RTU to TCP；
- Complete and robust router function, support a variety of Internet access methods: automatic allocation, specified IP, PPPoE；

- Monitors the online status of network devices connected to the LAN port and reports the status through the platform；
- Support IPTABLES firewall, various network protocols；
- Support WAN port and 4G network connection switch, preferentially use WAN port wired network；
- Supports MODBUS and MQTT protocols, and MQTT supports SSL encryption；
- Alarms are sent by SMS or email；
- Supports one-time timers, periodic timers, and cyclic timers；
- Supports remote upgrade through web pages。
- Dynamic DDNS: Supports peanut shell, 88IP, and dynDNS；

1. 6. Technical parameters

Item	Parameters	Description
Power Supply	Input voltage	9~36VDC
	Input current	Normal: 130mA@12V. Maximum: 800mA@12V
	Connection	3.5mm wiring terminal
	Protection	Anti-reverse connection Protection
WAN	Qty	1
	Interface Spec	RJ45 interface, 10M/100Mbps, adaptive MDI/MDIX
	Protection	ESD ±30kV (contact), ±30kV (air) EFT 40A (5/50ns) Lightning 24A (8/20μs)
LAN (non-POE）	Qty	1
	Interface Spec	RJ45 interface, 10M/100Mbps, adaptive MDI/MDIX
	Protection	ESD ±30kV (contact), ±30kV (air) EFT 40A (5/50ns) Lightning 24A (8/20μs)
Serial Port	Qty	1
	Type	1 Channel RS485 or RS232
	Baud rate	1200，2400，4800，9600，14400，19200，38400，57600，115200，230400
	Data Bit	5，6，7，8
	Parity	None, Even, Odd
	Stop Bit	1,2
	Working mode	Transparent transmission, Modbus RTU to TCP, Modbus slave, Modbus master (R10A support but R10 can't)
	Protection	ESD contact: 8KV Surge: 4KV (8/20us) ESD ±8kV (contact), ±15kV (air) EFT 4KV, 40A (5/50ns)
WIFI	Antenna Port qty	2
	Antenna type	SMA hole type

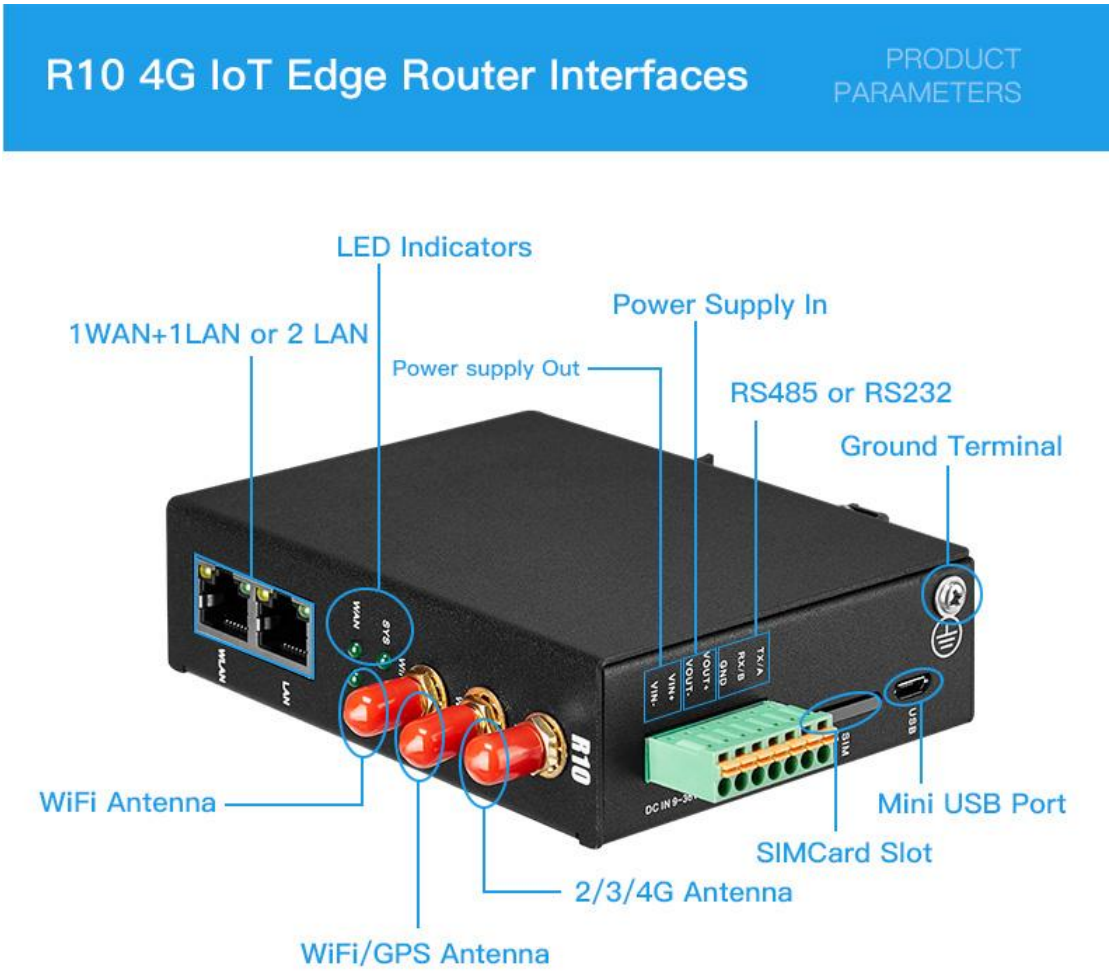
	Protocol	802.11a/b/g/n (mixed)
	Mode	AP mode, client mode
	Frequency	2.4G
	Channel	Channel 1 - 13
	Security	Open, WPA, WPA2
	Encryption	AES, TKIP, TKIPAES
	Connection number	16(Max)
	Speed	300Mbps(Max)
	Transmit Distance	Max. 20 meters in open space where there is no obstruction
	SSID Broadcast Switch	Support
Cellular Network	Antenna Port Qty	1
	Antenna Port Type	SMA hole type
	4G(L-E)	GSM/EDGE：900,1800MHz WCDMA：B1,B5,B8 FDD：B1,B3,B5,B7,B8,B20 TDD：B38,B40,B41
	4G(L- AU)	GSM/EDGE：850,900,1800MHz WCDMA：B1,B2,B5,B8 FDD：B1,B2,B3,B4,B5,B7,B8,B28 TDD：B40
	4G(L-A)	WCDMA：B2,B4,B5 FDD：B2,B4,B12
	4G(L-V)	FDD：B4,B13
	4G(L-J)	WCDMA：B1,B3,B8,B18,B19,B26 FDD：B2,B4,B12 TDD: B41
	4G(L-CE)	GSM/EDGE：900,1800MHz WCDMA：B1,B8 TD-SCDMA：B34,B39 FDD：B1,B3,B8 TDD：B38,B39,B40,B41
SIM	Qty	1
	Interface Spec	Drawer interface, support 1.8V/3V SIM/UIM card (NANO)
	Protection	Built-in 15KV ESD protection
GPS (optional)	Antenna qty	1
	Antenna type	SMA hole type
	Tracking Sensitivity	> -148 dBm
	Horizontal Accuracy	2.5m
	Protocol	NMEA-0183 V2.3
Indicator light	SYS	System running indicator (blinking for 2S and then off after normal operation)
	4G	4G cellular operating status indicator (when SIM registered

		successfully, this indicator always on)
	WAN	WAN status indicator
	LAN	LAN status indicator
System	CPU	MIPS CPU, main frequency 580Mhz
	Storage	128Mbits SPI Flash
	RAM	1024Mbits DDR2
Software	Network Protocol	PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, HTTP, HTTPs, DNS, ARP, NTP, SMTP, SSH2, DDNS
	VPN	IPsec, OpenVPN, L2TP
	Firewall	DMZ, DoS defense, IP packet, domain name and MAC address filtering, port mapping, access control
	Remote Management	Supports web remote configuration
	System Log	Support
	Firmware Update	Supports serial port local TFTP and Web upgrade
Certificate	EMI	EN 55022: 2006/A1: 2007
	EMS	IEC(EN)61000-4-2(ESD) IEC(EN)61000-4-3(RS) IEC(EN)61000-4-4(EFT) IEC(EN)61000-4-5(Surge) IEC(EN)61000-4-6(CS) IEC(EN)61000-4-8
	Others	CE, FCC, ROHS, 3C
Working Environment	Working temperature	-20～+65℃
	Storage temperature	-40～+85℃
	Humidity	5 ~ 95%RH (non-condensation)
Others	Enclosure	Metal material
	Size	Height 110mm * Length 83mm * Width 30mm
	IP level	IP30
	Net weight	300g
	Installation	Wall mounted, DIN rail

1. 7. Models Selection Table

Model	SIM card	WiFi mode	RS 232	RS 485	GPS	Micro USB	**Extend function**
R10	1	2	Multiplexing		optional	support	Modbus Slave/MQTT
R10A	1	2	Multiplexing		optiona	support	Modbus Master /Slave /MQTT

2. Hardware Description



2. 1. Device Size

2. 2. Indicator light

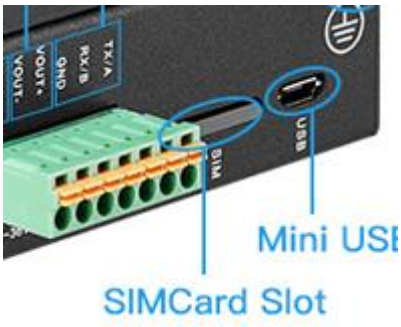
LED Indicator light			
Name		Status	Description
SYS	System running status indicator	Always on	Working normally
		Light off	Device fail
4G	4G cellular status indicator	Slow flash	Cellular network normal (registration successful)
		Light off	abnormal
WAN	WAN status indicator	Fast flash	WAN port normal
		Light off	abnormal
LAN	LAN status indicator	Always on	LAN port is normal
		Light off	abnormal

2. 3. Reset button

After the router runs normally, press and hold the Reset button for about 10 seconds with a pointed stick. Release the button when all the indicators are off until the WAN indicator blinks slowly. At this time, restart the router and restore the factory default Settings.

2. 4. SIM card

When inserting or removing a SIM card, ensure that the device is powered off, insert the card pin into the hole in the card slot, and press down to push the card slot out。



Drawer type Nano SIM card slot

2. 5. Connect the external antenna

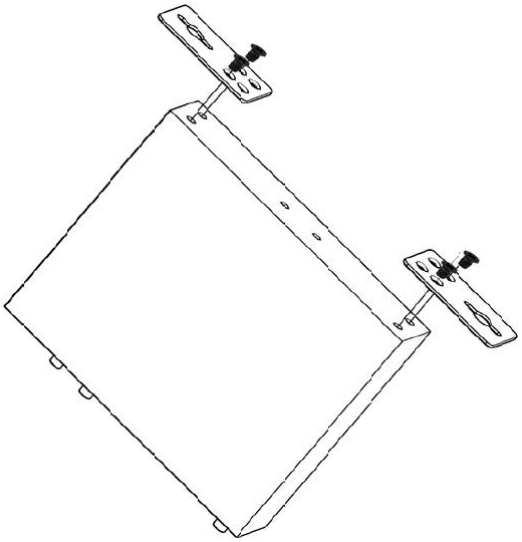
2. 6. Ground the Router

The router grounding cable helps protect against electromagnetic interference. Before connecting the device, ground the device by connecting the ground screw. Note: The product should be installed on a well grounded device surface, such as a metal plate.

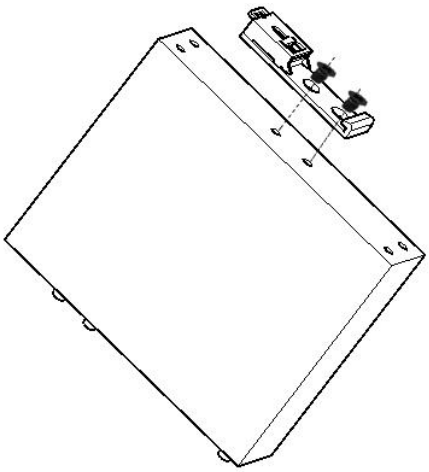
2. 7. Installation

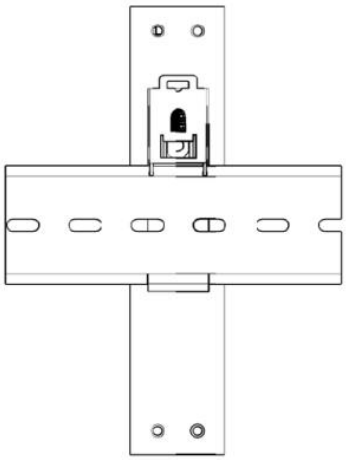
This device supports horizontal desktop placement, wall mounting and rail mounting.

2.7.1 Wall-mounted installation



2.7.2 Rail mounting



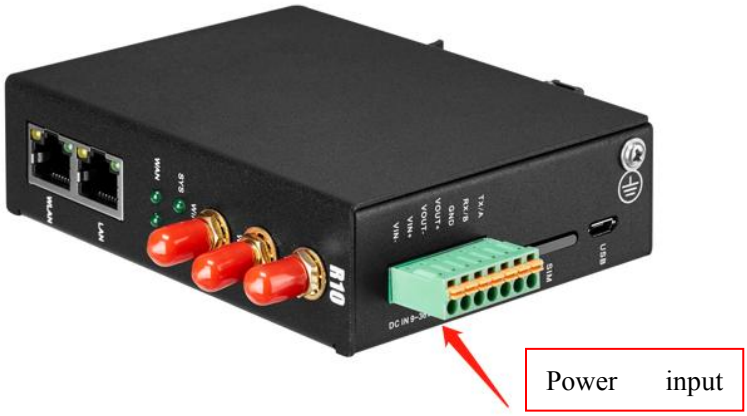


3. Router operation（basic operation)

3. 1. Start the Router device

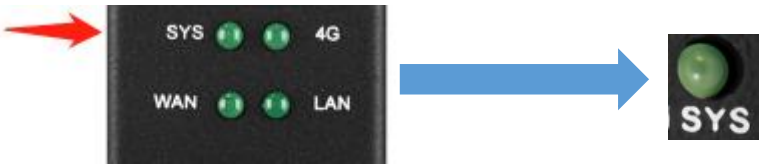
3. 1. 1. Power on the device

Power input port: the device adopts 9 to 36V dc power supply，



3. 1. 2. System running status

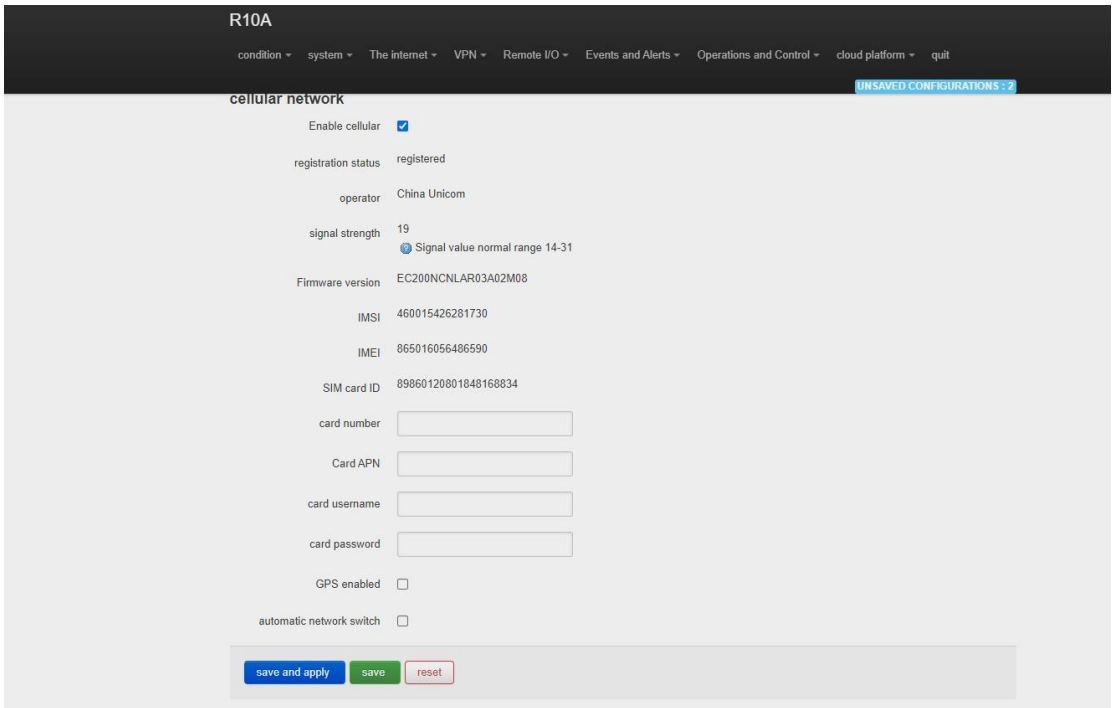
Observe the system running status indicator -SYS: The indicator is off when the device is powered on. Wait 1 to 2 minutes until the SYS indicator blinks slowly. If the light is not on, the device is faulty, please contact the agent, or email after the sale：technical@bliiot.com



3. 2. SIM Card operation instructions

The device supports dual SIM cards (only NANO SIM cards). When installing the card, disconnect the power supply of the device, remove the card holder with the card taking pin, install the NANO SIM card into the card holder according to the position, insert the card holder back into the card slot, and then power on the device again.

After the device is powered on and running properly, log in to the router configuration interface -- Network -- Cellular network（For login operations, see4.Log in to the Web page and configure 4G cellular dial-up networking by default SIM card For details, see5.3.1Network setting interfaceand 5.3.3.The cellular network



3. 3. Serial port operation

The device has a communication port 485/232. The default port is 485. It can be used for communication between Modbus master and Modbus slave, transparent transmission, and Modbus RTU to TCP.

Note: Only one function can be selected for a serial port at a time. If you cannot select the serial port on the configuration page, it indicates that the serial port has been configured on another configuration page.

3. 3. 1. Modbus Master

Modbus master function: The local PC functions as the Modbus master, and the serial port connects to the Modbus slave device 5.5.5.Modbus master After configuring slave machine parameters, the local computer will collect slave machine data through Modbus protocol and store slave machine data in the local mapping register. You can query slave machine data directly on the configuration page， Also available in 5.8.Cloud Platform Configure the Modbus or MQTT protocol to upload data from the slave computer to the server and convert the Modbus protocol to MQTT protocol。

If the slave port is set to RS485/RS232 or Ethernet, the device will continuously poll the slave device based on Modbus RTU (RS485 and RS232 are slave ports) or Modbus TCP (Ethernet is slave ports). To read the value of a register from a machine device into the device mapping area for storage. In this way, the register data in the machine will be mapped to the device. Reading and writing the mapped register of the device will be directly transmitted to the slave device through RS485 serial port, RS232 serial port or Ethernet. There is a one-to-one correspondence between the slave register address and the mapped register address in the device, which is the mapped register list.

Users can connect various slave computers through RS485 serial port, RS232 serial port, or Ethernet port to add I/O ports and read and write intelligent instruments and devices. For example, connect the remote I/O module of Mxxx series of our company to expand the number of INPUT ports of DIN, DO, AI, AO and PT100, or connect the power parameter monitoring module to read the current, voltage and power of three-phase power, or connect it to the UPS power supply for parameter monitoring, etc. Or a combination of the above intelligent devices, etc., can meet the functional requirements of most applications.

3. 3. 2. Modbus slave

Modbus slave function: The local PC serves as the Modbus slave, and the serial port is connected to the Modbus master device 5.5. Remote I/O and Serial Port setting. After serial port and server parameters are set, the master device can collect data from the local device using Modbus RTU

(RS485/RS232 interface) or Modbus TCP (Ethernet interface).

3. 3. 3. Transparent transmission

Transparent transmission: The local machine acts as a data transfer station between the server and slave device, through the configuration page 5.5. Remote I/O and Serial Port setting. After serial port parameters and server parameters are configured, the local PC transparently transmits data from the PC to the server and sends data from the server to the slave PC. Data content is not processed but only forwarded, realizing transparent data transmission.

3. 3. 4. Modbus RTU to TCP protocol convert

Transfer from Modbus RTU to TCP: The local host communicates with the slave host using Modbus RTU, and the local host communicates with the server using Modbus TCP, through the configuration page 5.5. Remote I/O and Serial Port setting. After setting serial port parameters and server parameters, the local computer automatically converts the Modbus TCP commands sent by the server into Modbus RTU commands and sends them to the slave computer, and then converts the Modbus RTU commands returned by the slave computer into Modbus TCP commands and replies to the server. Realize the communication between Modbus RTU slave and Modbus TCP server.

4. Prepare Configuration router by WEB

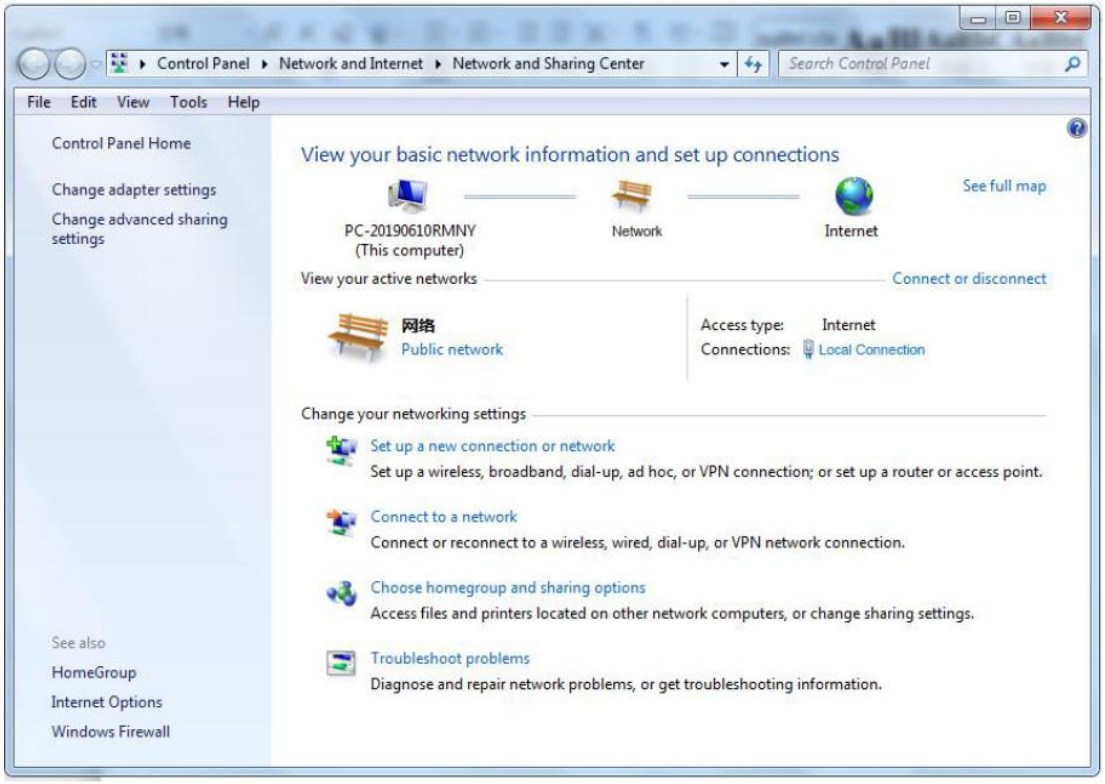
The router supports web page configuration. There are two ways to connect the router. One is to connect the computer to any LAN port of the router through cable connection. The other is to connect to a router via WIFI. The PC can automatically obtain an IP address through DHCP or set a static IP address on the same network segment as the router. After the connection is set up, enter the default login address 192.168.3.1 in the browser of the PC to access the Web login page of the router. The default login user name is admin and there is no password.

4. 1. Wired connection router

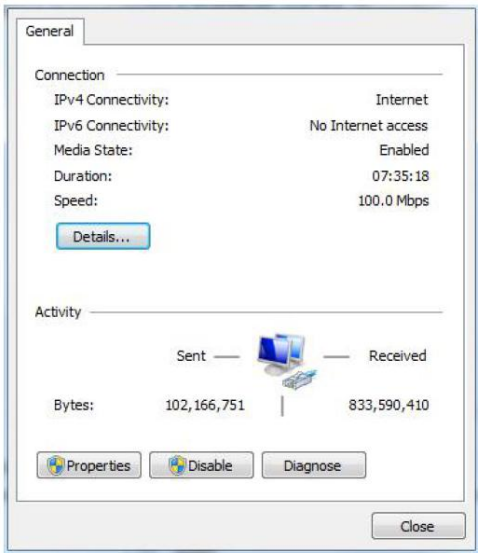
On the PC, you can configure its IP address in two ways. Enable automatic IP address acquisition on the local connection of the PC. Configure a static IP address on the local connection of the PC on the same subnet as the router.

The following uses Windows 7 as an example. The configuration of Windows is similar.

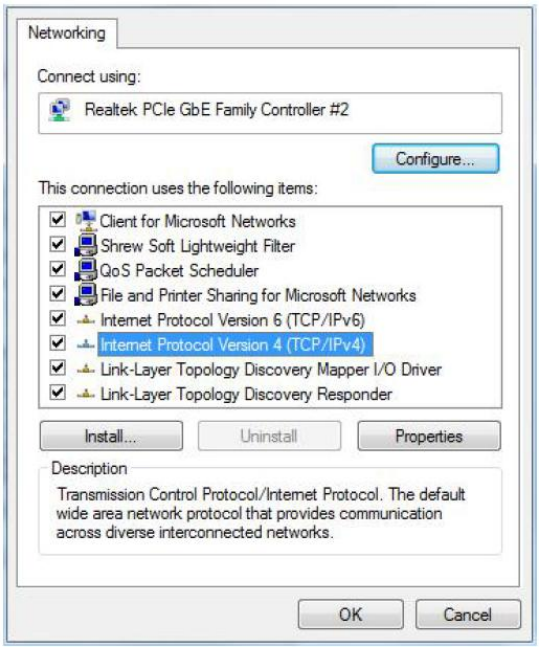
1. Click Start > Control panel & GT; Network and Sharing Center, double-click Local Connection in the window that opens”



2. In the Local Area Connection Status window, click Properties

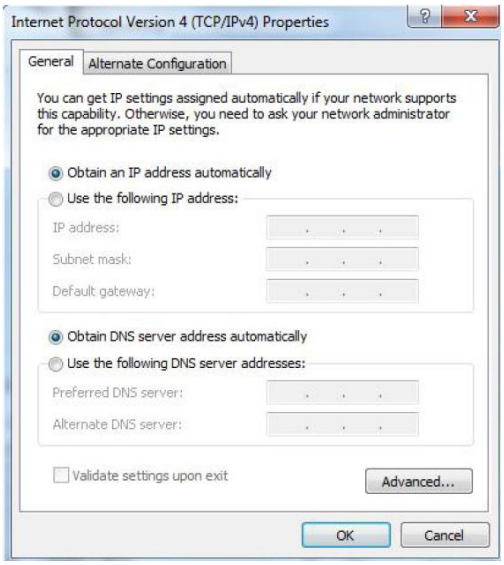


3. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties”

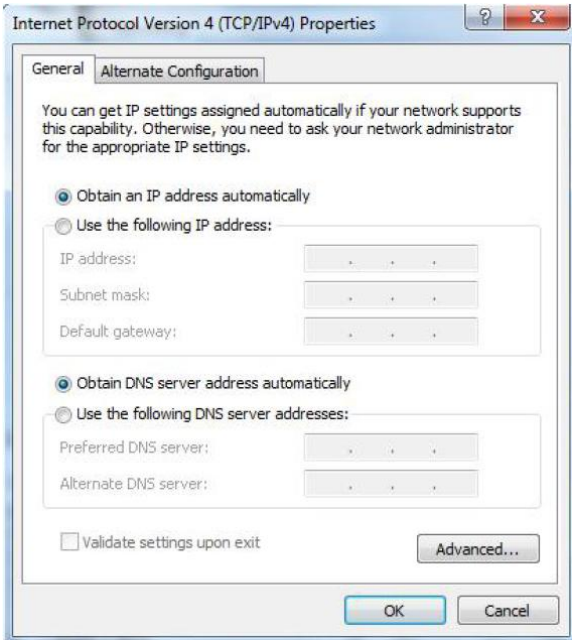


4. You can configure the IP address of the PC in either of the following ways：

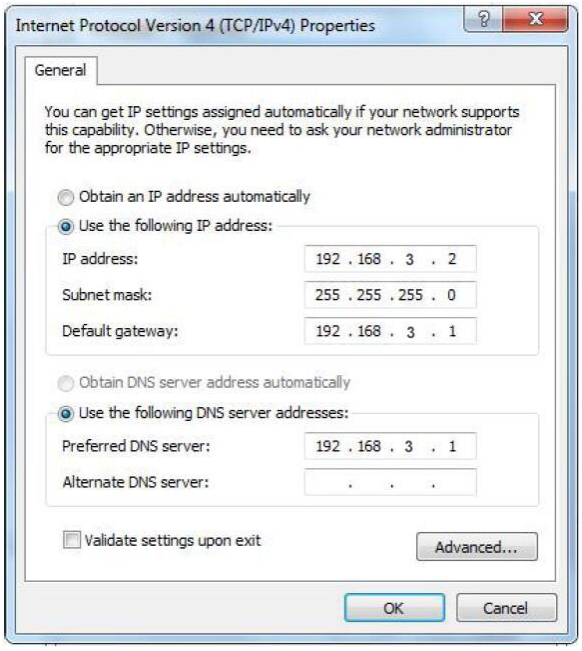
To automatically obtain an IP address from the DHCP server, click Automatically Obtain an IP address”；



Manually configure a static IP address for the PC on the same subnet as the IP address of the router. Click and configure Use the following IP address”



5. Click OK to complete the configuration



4. 2. WiFi Connection router

Search for wireless networks: The default WiFi network name is King-XXxxxx(XXXXXX is a 6-digit random number and letter combination) without password

1. Establish a connection: no encryption is required by default. Click "Connect"。

4. 3. Factory default Settings

Before logging in to the Web configuration page, it is necessary to understand the following default Settings.。

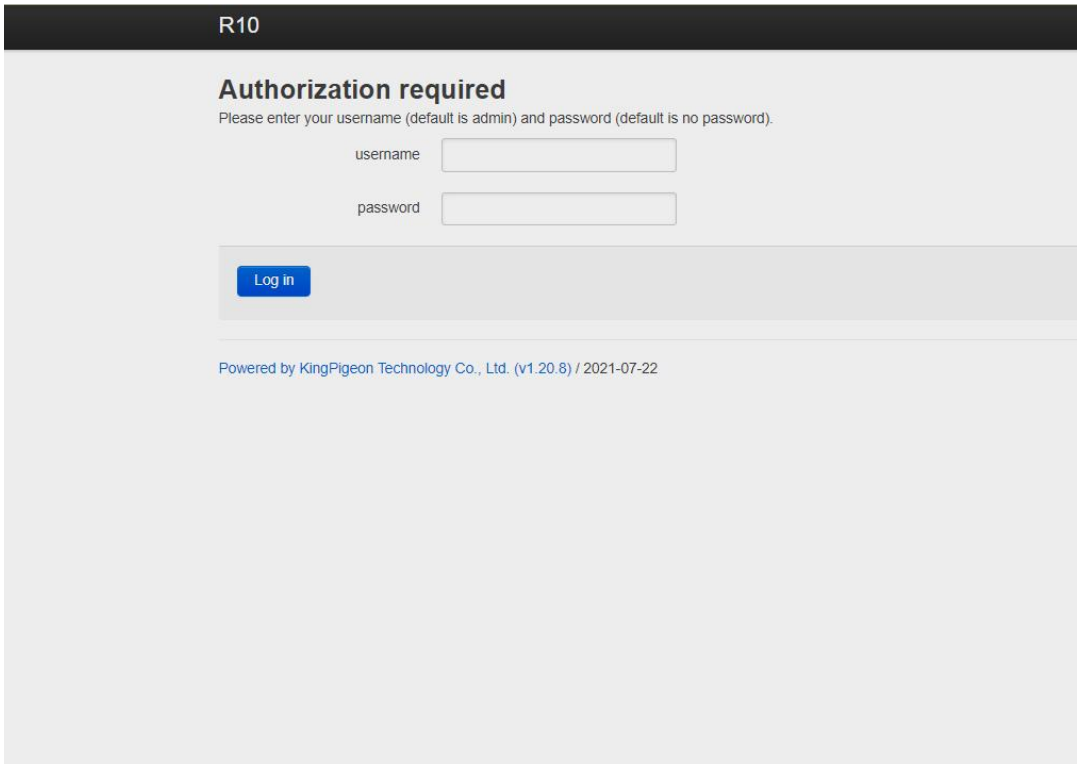
Project	**Describe**
Login IP Address	192.168.3.1
User name	admin
Password	There is no password
DHCP server	The default open
WIFI	SSID: KING-XXXXXX (XXXXXX is a 6-digit random number and letter combination) KEY: No encryption (open network)

4. 4. Login configuration page on WEB browser

1) After connecting the router with wired or wireless operation, open the browser, such as IE, Edge, Google, etc., on the PC;
2) Enter the IP address of the router in the address bar of your browser 192.168.3.1 The login page is displayed.

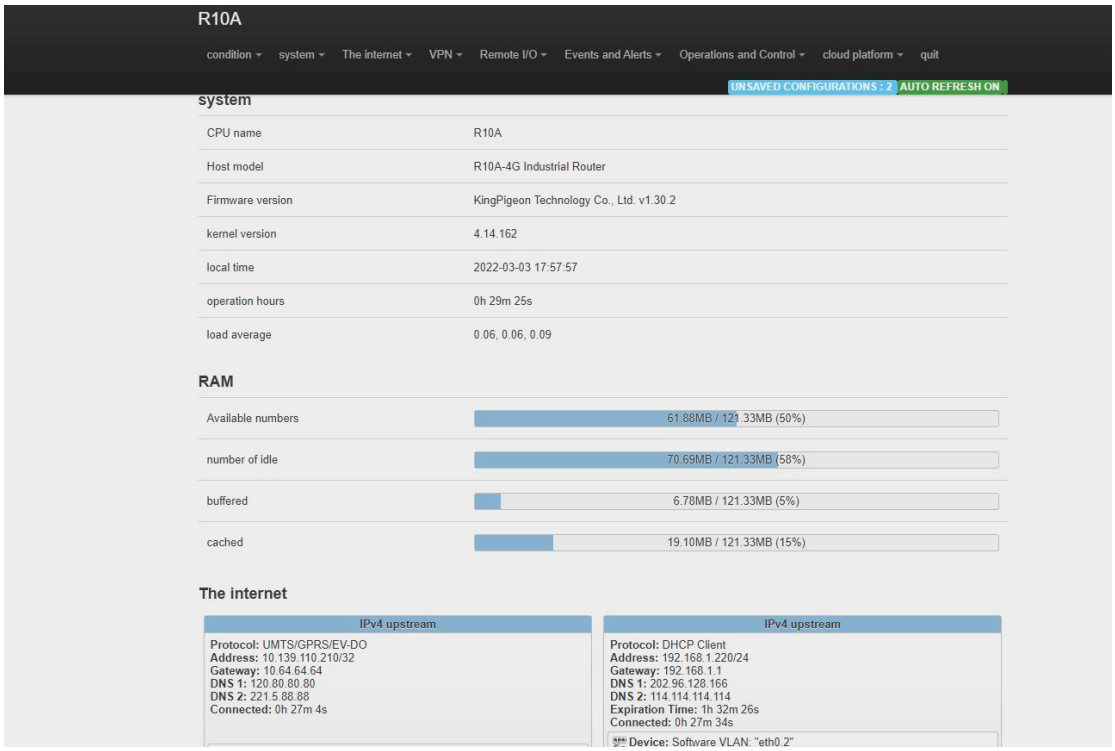
On the login page, enter the user name admin (default), leave the password blank (default), and click Login.

3) After you log in to the router, the status summary page is displayed
4) Notice After configuring the parameters, click Save and Apply" to take effect



5. Configure router

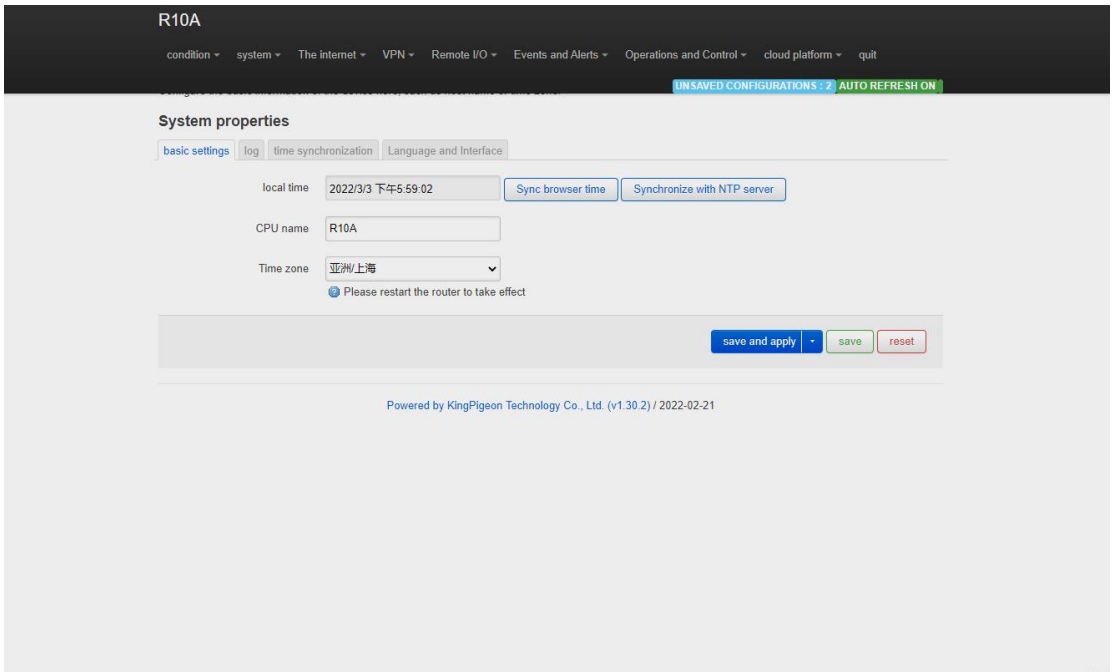
5.1. Status



Status provides the overview, firewall, routing table, system logs, kernel logs, and real-time information to view the running status of the router.

5.2. System

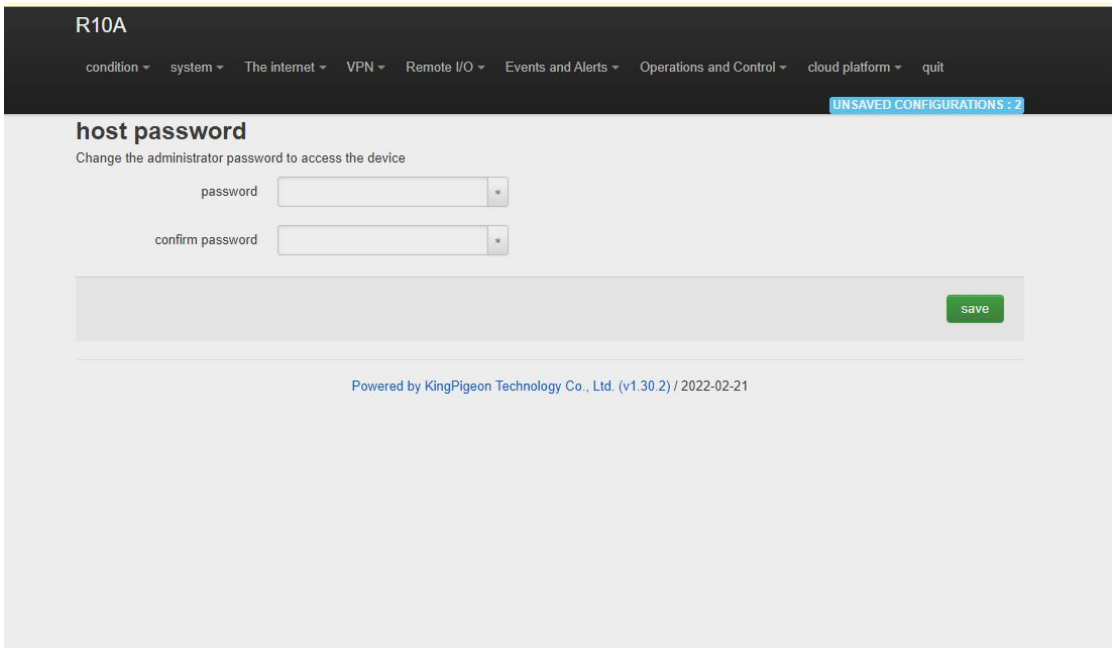
5. 2. 1. System Properties



Configure basic device information, such as the host name and time zone.

System property		
Project		Instructions
Basic setup	Local time	You can set the time of the router to synchronize the time of the browser or the NTP server
	Host name	Same as product type, modification is invalid
	Time zone	Select a region and restart the router for the Settings to take effect
Log		Log property, you can set the external system log server to save logs externally
Time synchronization		Configure the NTP server to synchronize time
Language and Interfaces		Language optional automatic (according to the browser language change, only Chinese and English), Chinese, English; The theme cannot be modified
Product type		That is, the product model, factory curing, modification is invalid

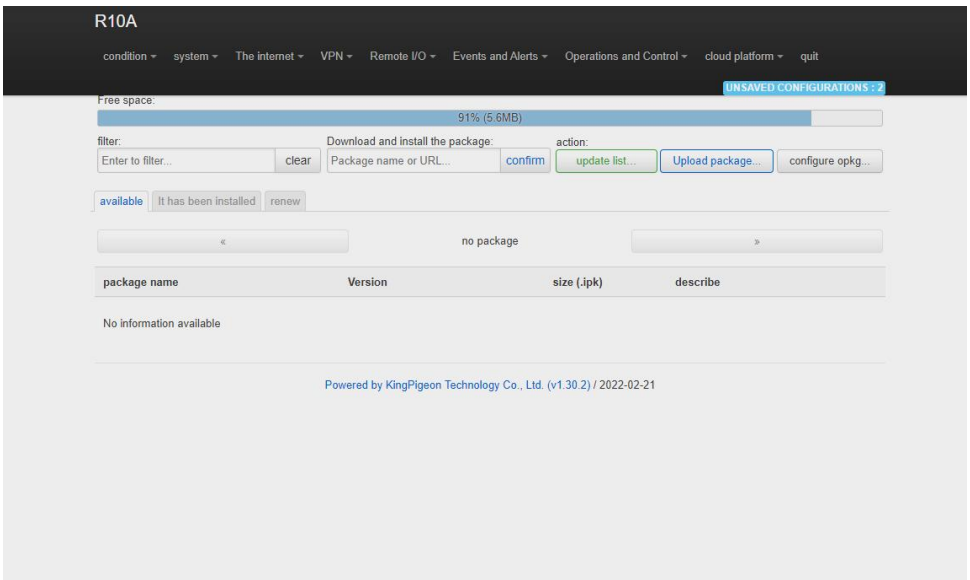
5. 2. 2. System Management Rights



System Management	
Project	Instructions
Password	Change the administrator password for accessing the device
SSH access	Provides SSH access and SCP services
SSH key	The public key allows password-less SSH login with greater security than using a common password. To upload the new key to the device, paste the OpenSSH compatible public key line or drag the.pub file into the input field.

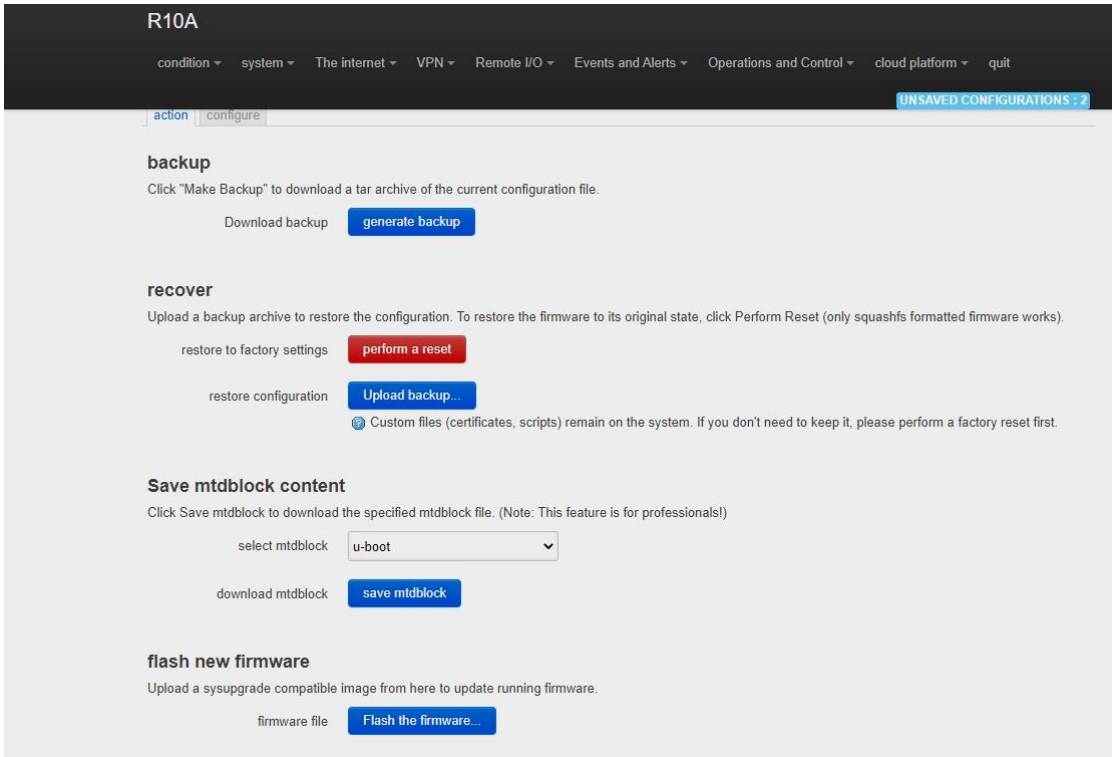
5. 2. 3. Software Package

This function provides software installation, removal, and upgrade.



(Note: This is advanced function for professionals!)

5. 2. 4. Backup/Upgrade

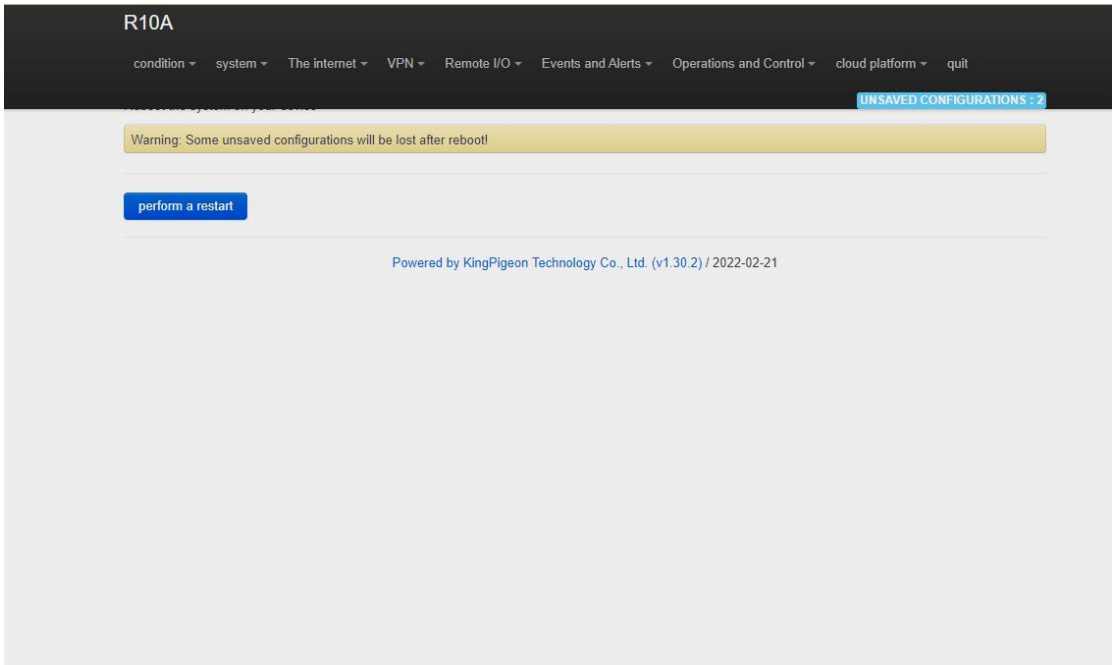


Backup/Upgrade	
Project	Instructions
Backup	Click Build Backup to download the tar archive of the current configuration file.

Restore	Upload the backup archive to restore the configuration. To restore the firmware to its initial state, click Perform Reset (valid only for squashFS format firmware).
Save the MTdblock content	Click Save MtdbLock to download the specified MTdblock file. (Note: This feature is for professionals!)
Brush new firmware	Upload a SysupGrade compatible image from here to update the running firmware

5. 2. 5. Reboot

Click Perform Reboot to restart the system on your device.

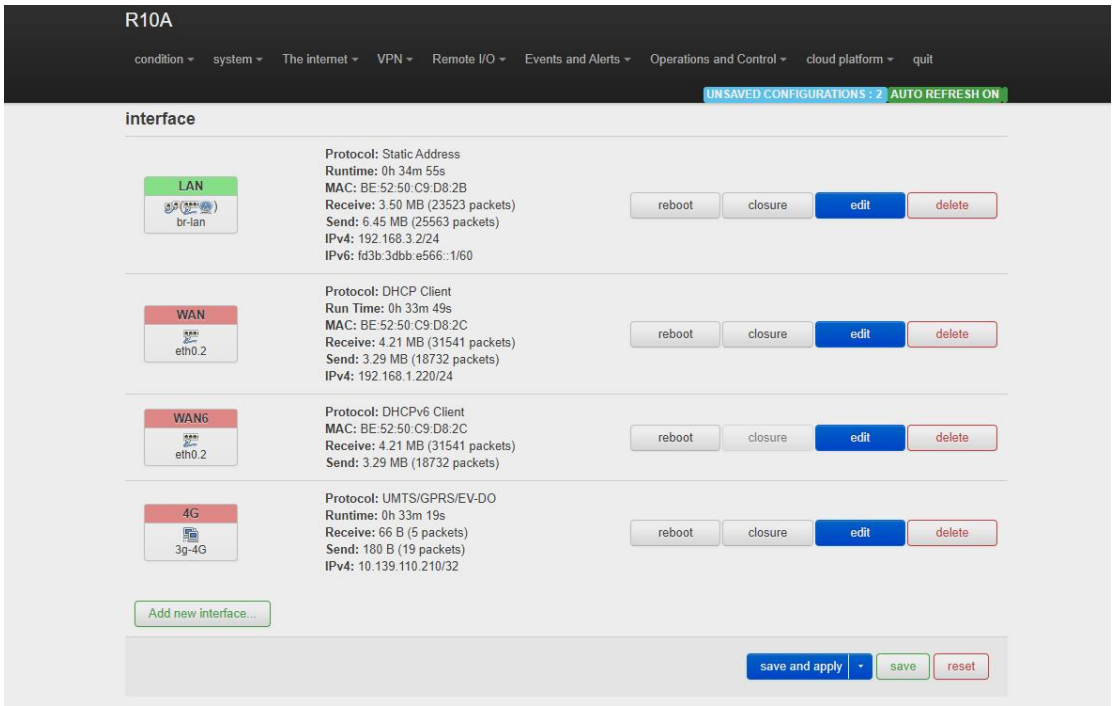


5.3. Network

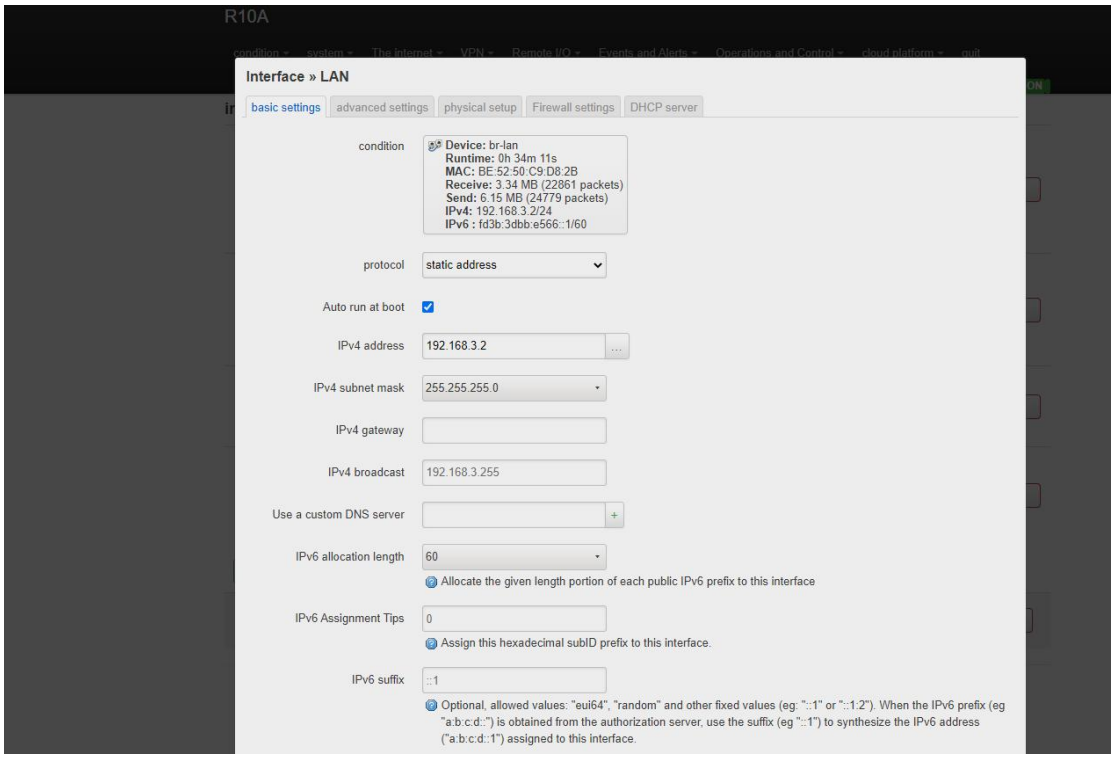
5.3.1 Network setting Interface (WAN/LAN switching, 4G, WAN6)

You can restart, close, edit, or delete an existing interface, or add a new interface.

By default, interfaces such as LAN, WAN, WAN6, and 4G are configured. You can click Edit to modify detailed configurations.



5.3.1.1 LAN port



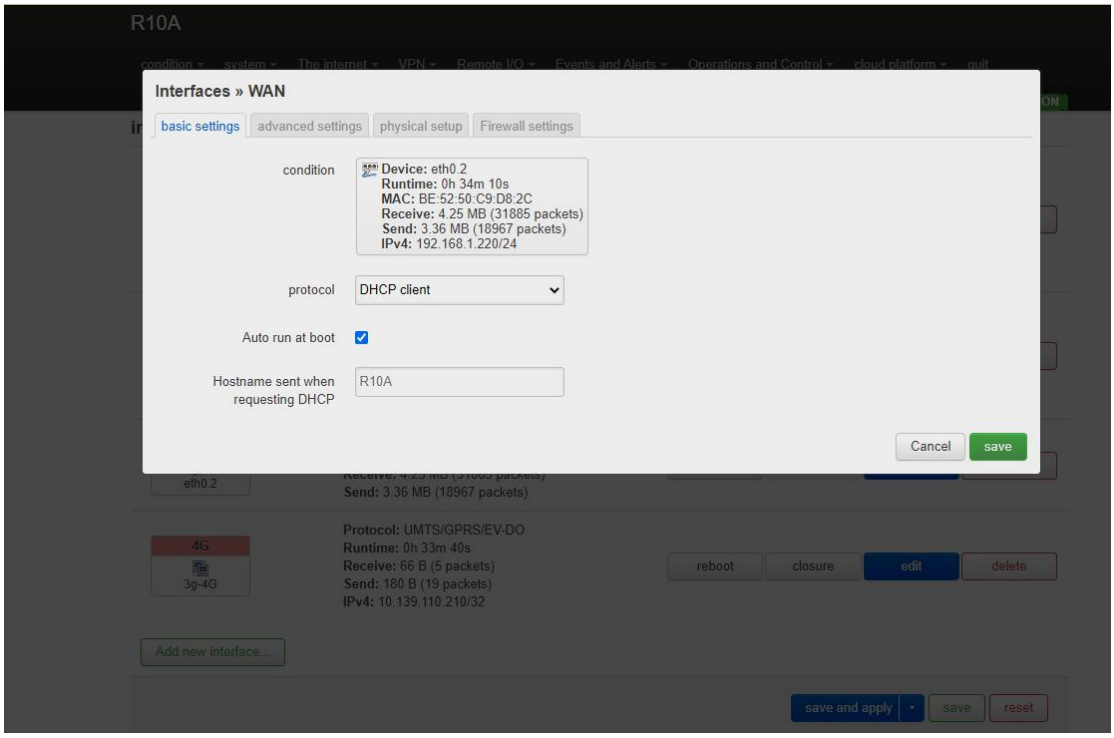
LAN		
Project		Instructions
Basic setup	state	Equipment: br - LAN Running time: 8h 57m 16s

		MAC: E2:2F:C4:54:93:BA Reception: 18.81 MB (149126 packets) Send: 99.87 MB (132321 packets) IPv4:192.168.3.1/24 IPv6: fdb2:428b:ddbe::1/60
	Agreement	Static address
	Automatic startup	Check the default
	IPv4 address	The default IP address is 192.168.3.1. Modifying this setting can change the network segment that DHCP assigns IP to the LAN port. This is also used as the login address of router. If the IP address is modified, select Force application when saving the application. After the modification is complete, please log in with the new IP address.
	IPv4 subnet mask	Default 255.255.255.0
	IPv4 gateway	This parameter is empty by default. If multiple IPv4 addresses are configured, you need to specify the gateway address
	IPv4 radio	Default 192.168.3.255
	Use a customized DNS server	Default empty
	IPv6 Allocation Length	Assigns a given length portion of each public IPv6 prefix to this interface, 60 by default
	IPv6 Assignment Prompt	Assign this hexadecimal subID prefix to this interface.
	IPv6 suffix	Optional. Allowed values: EUi64, Random, and other fixed values (for example ::1 or ::1:2). If an IPv6 prefix (such as A :b: C :d::) is obtained from the authorization server, a suffix (such as ::1) is used to synthesize an IPv6 address (A :b: C: D ::1) and assign it to the interface.
Advanced Settings	Use the built-in IPv6 management	Selected by default
	Mandatory link	Always use application Settings regardless of the link state of the interface (if selected, link state changes will no longer trigger hotPlug event handling). This parameter is selected by default.
	The MAC address was reset	Changing a MAC Address
	Reset the MTU	Default is 1500

	Use gateway hops		The default 0
physical setting	Bridge interfaces		Create a bridge for the specified interface. This parameter is selected by default.
	Open the STP		Enable spanning tree protocol on this bridge, not selected by default.
	Enable IGMP sniffing		Enable IGMP snooping on this bridge, not selected by default.
	Interface		VLAN: eth0.1 (LAN) for switches and Master king-xxxxxx (LAN) for wireless networks. You do not need to change the Settings of physical interfaces that use LAN interfaces
Firewall Settings	Create/assign firewall areas		Assign a firewall area to the interface, select unspecified to remove the interface from the associated area, or fill in the Create field to create a new area and associate the current interface with it.
DHCP server	Basic setup	Ignore this interface	The DHCP service is not provided on this interface. This parameter is not selected by default.
		start	The starting base address assigned to a network address. The default of 100.
		The customer number	Maximum number of addresses allocated. The default of 150.
		Lease	The minimum expiration time of the rented address is 2 minutes (2m). The default 12 h.
	Advanced Settings	Dynamic DHCP	Provides DHCP services for all clients. If disabled, only customers with static leases will be served. This parameter is selected by default.
		Mandatory	Force DHCP on this network even if another server is detected. This parameter is not selected by default.
		IPv4 subnet mask	Reset the subnet mask sent to the client.
		DHCP options	Set the DHCP additional options, such as setting "6192168 2.1, 192.168.2.2" said notice different DNS server to the client.
	IPv6 is set	Routing Advertisement service	Default Server mode
		DHCPv6 service	Default Server mode
		HDP agent	Disabled by default
		DHCPv6 mode	The default is stateless + stateful
		Always advertise	It advertises itself as the default route even if

		the default route	no public network prefix is available. This parameter is deselected by default.
		DNS server for notification	This parameter is not required based on actual Settings
		The advertised DNS domain name	This parameter is not required based on actual Settings

5.3.1.2 WAN port

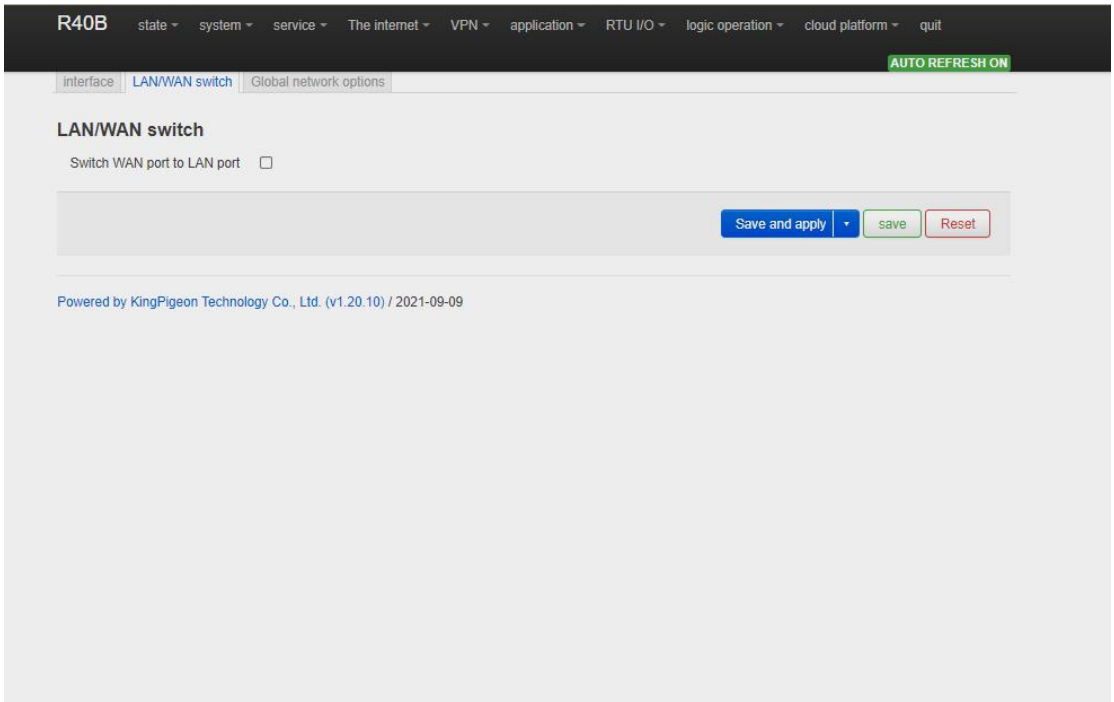


WAN		
Project		Instructions
Basic setup	State	Equipment: eth0.2 Running time: 9h 37m 16s MAC: E2:2F:C4:54:93:BB Reception: 113.65 MB (290226 packets) Send: 19.02 MB (137282 packets) IPv4:192.168.1.173/24
	Agreement	DHCP client by default. If the network connected to the WAN requires an account and password to log in, select PPPoE
	Automatic startup	Selected by default
	Host name sent when requesting DHCP	The default value is product model

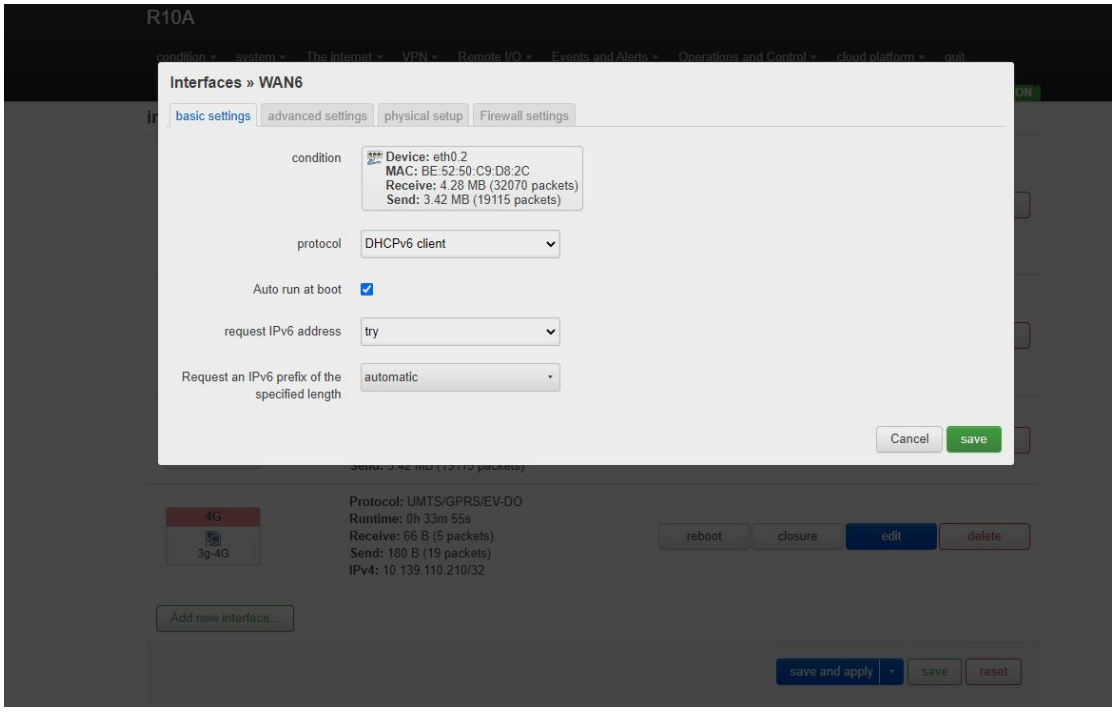
Advanced Settings	Use the built-in IPv6 management	Selected by default
	Mandatory link	Always use application Settings regardless of the link state of the interface (if checked, link state changes will no longer trigger hotPlug event handling). This parameter is NOT selected by default.
	Use broadcast tags	Some ISPs require DOCSIS 3 for coaxial network. This option is not selected by default.
	Using the Default Gateway	If the default route is left blank, it is selected by default.
	The DNS server is automatically obtained	If left blank, the advertised DNS server address is ignored. This parameter is selected by default.
	Use gateway hops	The default 0
	ID of the client sent when requesting DHCP	This parameter is not required based on actual Settings
	Vendor Class option sent when requesting DHCP	This parameter is not required based on actual Settings
	The MAC address was reset	Changing a MAC Address
	Reset the MTU	default is 1500
Physical setting	Bridge interfaces	Create a bridge for the specified interface. This parameter is not selected by default。
	Interface	Switch VLAN: eth0.2 (wan, WAN6). You do not need to change the value of this parameter
Firewall Settings	Create/assign firewall areas	Assign a firewall area to the interface, select unspecified to remove the interface from the associated area, or fill in the Create field to create a new area and associate the current interface with it.

5.3.1.3 WAN/LAN switching

When you do not need to use the WAN interface function, you can convert the WAN into the LAN function to use, save and apply.



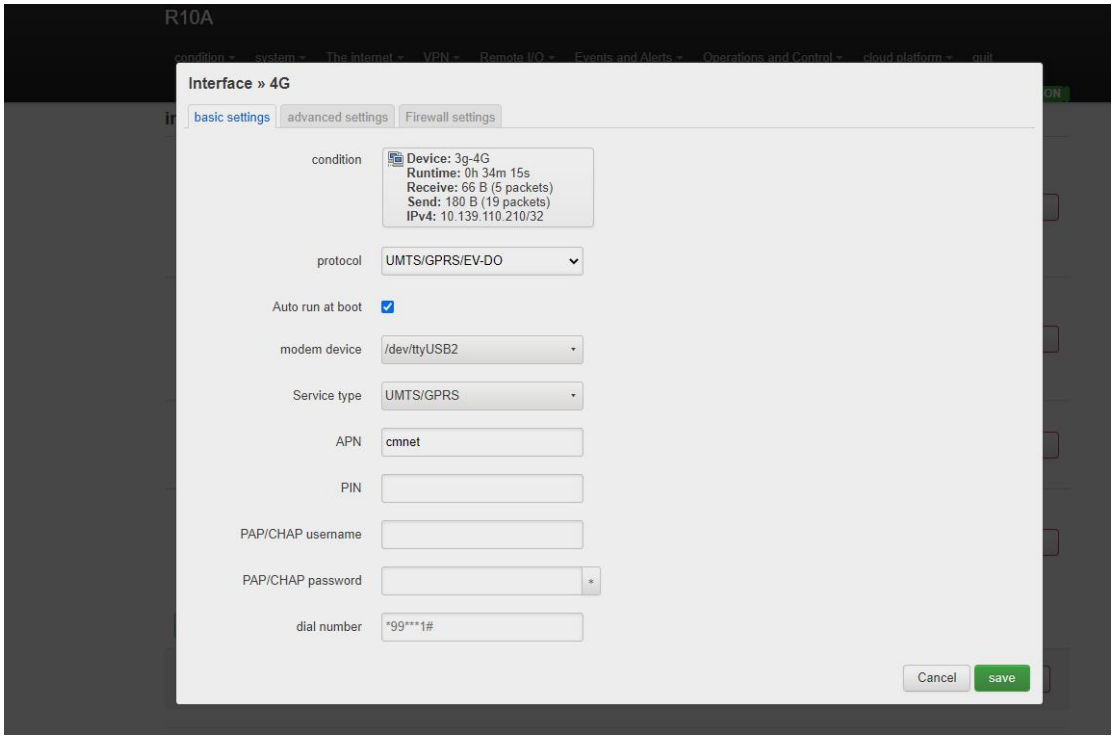
5.3.1.4 WAN6 Port



WAN6		
Project		Instructions
Basic setup	state	Equipment: eth0.2 MAC: E2:2F:C4:54:93:BB Reception: 115.31 MB (299495 packets)

		Send: 19.41 MB (140798 packets)
	Agreement	DHCPv6 client by default
	Automatic startup	Selected by default
	Requesting an IPv6 Address	Try by default
	Requests an IPv6 prefix of the specified length	Default automatic
Advanced Settings	Use the built-in IPv6 management	Selected by default
	Mandatory link	Always use application Settings regardless of the link state of the interface (if checked, link state changes will no longer trigger hotPlug event handling). This parameter is not selected by default.
	Using the Default Gateway	If this parameter is left blank, the default route is not configured
	User-defined assigned IPv6 prefix	This parameter is not required based on actual Settings
	The DNS server is automatically obtained	If left blank, the advertised DNS server address is ignored. This parameter is selected by default
	ID of the client sent when requesting DHCP	This parameter is not required based on actual Settings
	The MAC address was reset	Changing a MAC Address
	Reset the MTU	The default is 1500
The physical setting	Bridge interfaces	Create a bridge for the specified interface. This parameter is deselected by default。
	Interface	Switch VLAN: eth0.2 (wan, WAN6). You do not need to change the value of this parameter
Firewall Settings	Create/assign firewall areas	Assign a firewall area to the interface, select unspecified to remove the interface from the associated area, or fill in the Create field to create a new area and associate the current interface with it.

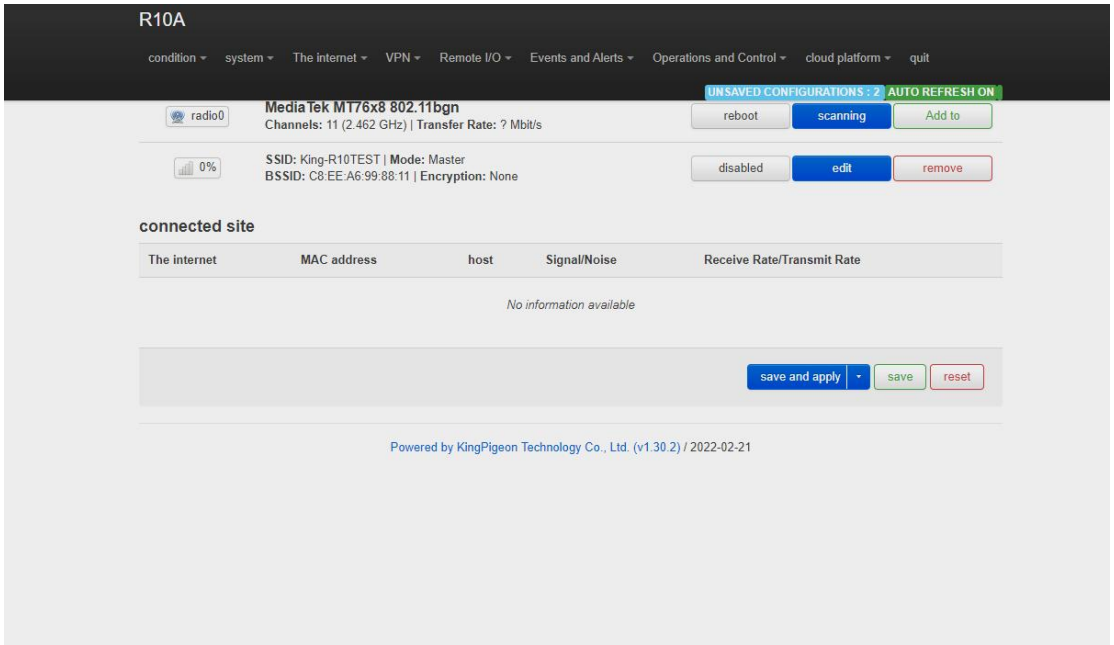
5.3.1.5 4G Port



4G		
Project		Instructions
Basic setup	State	Equipment: 3 g to 4 g Running time: 0h 11m 52s Reception: 1.06 KB (18 packets) Send: 8.50 KB (36 packets) IPv4:10.94.92.16/32
	Agreement	UMTS/GPRS/EV-DO
	Automatic startup	Selected by default
	Modem equipment	The default/dev/ttyUSB4
	Service type	The default UMTS/GPRS
	APN	SIM card Access point
	PIN	SIM card PIN code
	PAP/CHAP user name	User name used for PPP authentication
	PAP/CHAP password	Password used for PPP authentication
	Dial the number	SIM card Dial-up
Advanced Settings	Use the built-in IPv6 management	Selected by default
	Mandatory link	Always use application Settings regardless of the link state of the interface (if checked, link state changes will no longer trigger hotPlug event handling). Not selected by default。
	Obtaining an IPv6 Address	The default automatic
	Modem initialization timed out	Maximum wait time (seconds) for the modem to be ready. Default is 10.

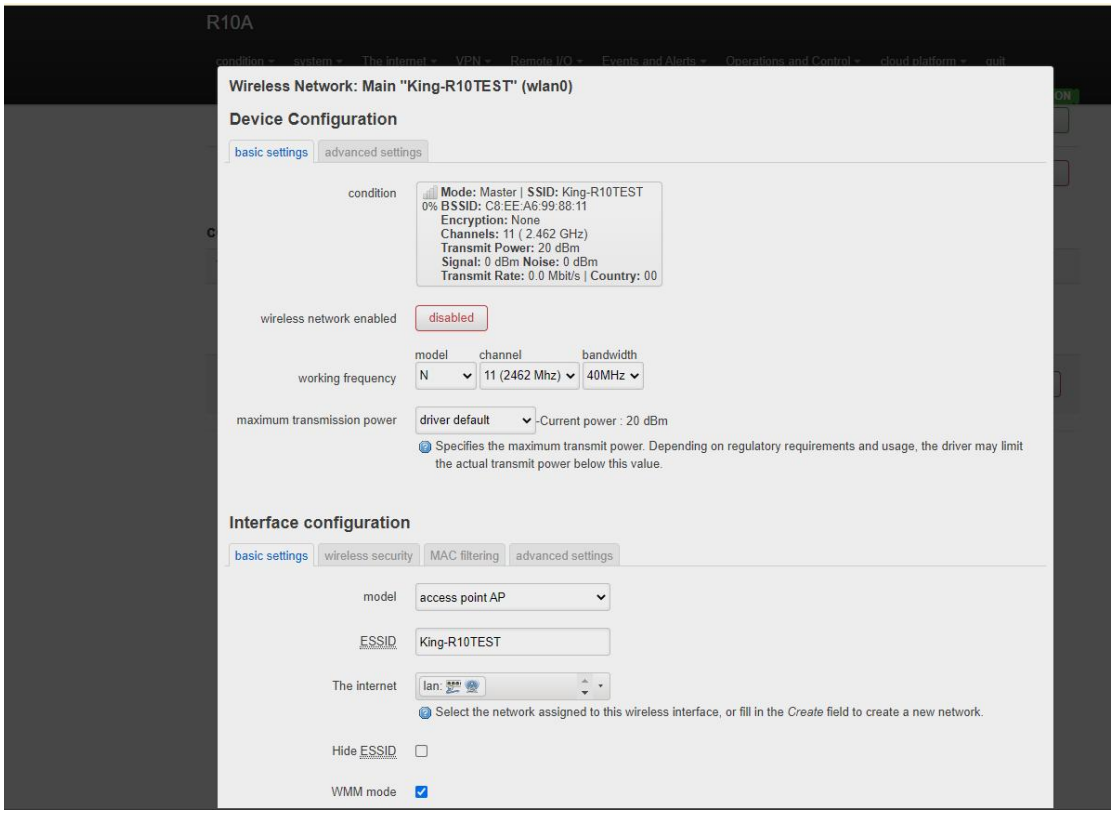
	Using the Default Gateway	If the default route is left blank, it is selected by default.
	Use gateway hops	If the default route is empty, the route is selected by default.
	The DNS server is automatically obtained	If left blank, the advertised DNS server address is ignored. This parameter is selected by default.
	LCP response fault threshold	If a specified number of LCPS respond to a fault, assume that the link is disconnected. 0 indicates that the fault is ignored. The default value is 0
	LCP response interval	LCP response is sent periodically (in seconds), valid only when combined with the fault threshold. The default is 5
	Activity timeout	Closes the inactive link after a given time (seconds). 0 remains the connection. Default: 0
Firewall Settings	Create/assign firewall areas	Assign a firewall area to the interface, select unspecified to remove the interface from the associated area, or fill in the Create field to create a new area and associate the current interface with it.

5.3.2 WIFI (AP mode or WLAN Client)

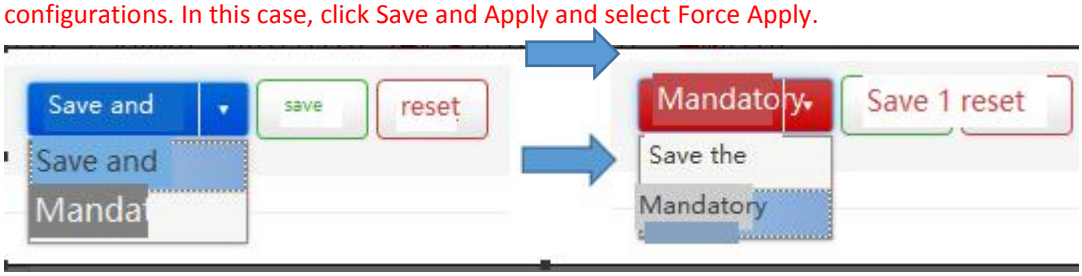


It can be used as both a WLAN hotspot (WiFi AP mode) and a WLAN client (WiFi client mode).
WiFi Settings display the current wireless status. You can click Edit to enter detailed configuration, or restart, scan, add, disable, remove and other operations.
Connected Site Displays connected wireless sites that you can disconnect.

5.3.2.1 WLAN Hotspot (WiFi AP mode)



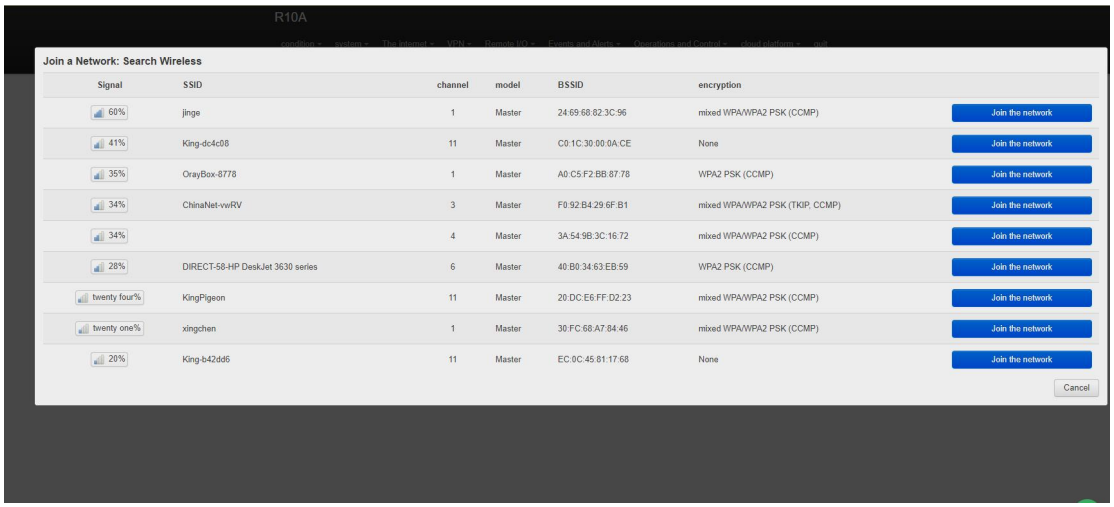
The default SSID is KING-XXXXXX (XXXXXX is a 6-digit random number and letter combination). The encryption mode does not exist. Other clients (such as mobile phones and computers) can directly search for wireless networks and connect to this hotspot.
Quick configuration: Select the wireless configuration in Master mode in WiFi Settings, click "Edit" to enter the configuration page, find "Interface Configuration" -- "Basic Settings" -- "ESSID" to modify the WiFi hotspot name, find "Interface Configuration" -- "Wireless Security" -- "Encryption" to modify the encryption mode and set the WiFi password.
Note: If you use WiFi to access router configurations, select Force Apply to modify WLAN hotspot configurations. In this case, click Save and Apply and select Force Apply.



Wireless AP hotspot device configuration		
Project		Instructions
Basic setup	State	97% Pattern: Master | SSID: King - ff4a8a BSSID: EE:0C:45:81:26:51 Encryption: None Channel: 6 (2.437 GHz) Transmission power: 20 dBm Noise signals: - 42 dBm | : 0 dBm Transfer rate: 58.5 Mbit/s | countries: 00
	Wireless network enabled	Enabled by default
	Working frequency	If the current frequency has too many devices in use, please change the frequency to reduce interference and optimize the signal
	Maximum transmission power	Specifies the maximum transmitted power. Depending on regulatory requirements and usage, the driver may limit the actual transmitted power below this value. The signal
Advanced Settings	Country code	Driven by default
	Allows traditional 802.11b rates	Check the default
	Distance optimization	Distance of the farthest network user (in meters). Default automatic, according to the distance to automatically adjust the transmission power
	Fragmentation threshold	When the data length exceeds the threshold, fragments are automatically sent. The default value is generally used
	The RTS/CTS threshold	Request send/Permit send protocol. When the data length exceeds the threshold, enable this protocol to avoid signal conflicts caused by multiple terminals sending data to the AP. The default value is generally used
	Mandatory 40MHz mode	The 40MHz channel is always used even when the auxiliary channels overlap. Using this option does not comply with IEEE 802.11N-2009! This parameter is not selected by default.
	Beacon interval	Indicates the interval at which a wireless route broadcasts its SSID periodically. The default value is generally used

Configure AP hotspot interfaces on wireless networks		
Project		Instructions
Basic setup	Model	Access point AP
	ESSID	Default king-xxxxxx (XXXXXX is a 6-digit random number and letter combination)
	network	Default LAN, select the network assigned to this wireless interface, or fill in the Create field to create a new network.
	Hide the ESSID	Not selected by default
	WMM mode	WiFi multimedia: Provides different priorities for different services to ensure service quality. This parameter is selected by default
Wireless security	Encryption	Default no encryption (open network)
MAC filtering	MAC Address Filtering	Disabled by default
Advanced Settings	Quarantine client	Disable communication between clients. This parameter is not selected by default
	The name of the interface	Reset the default interface name
	Short Preamble	Different rates require different preambles. This parameter is selected by default
	DTIMinterval	As a terminal node, periodically wakes up and sends traffic indication message intervals
	Time interval for re-encrypting GTK	The temporary secret key (GTK) uses the default value
	Disable inactive polling	Not selected by default
	Inactive site restrictions	The default 300 seconds
	Maximum listening interval allowed	Default maximum of 65535
	Disconnect on low Ack reply	Disconnect a wireless terminal in low ACK mode when AP mode is enabled. This parameter is selected by default

5.3.2.2 WLAN Client (WiFi Client Mode)



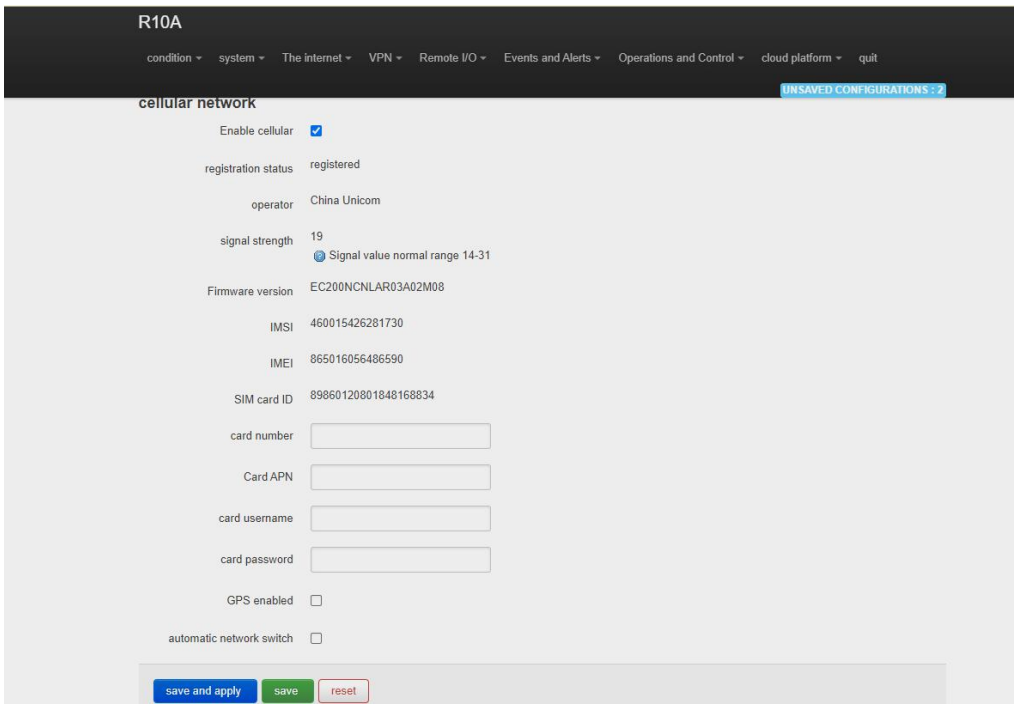
Please first click "Scan" to search for wireless network, and select "Join Network" to enter the quick configuration page. If you need a password, enter the WiFi password in "WPA Key", then click "Submit" to enter the detailed configuration page, and finally click "Save".

Wireless network client device configuration		
Project		Instructions
Basic setup	State	100% Pattern: Client | SSID: jingekeji BSSID: EC:0C:45:81:26:51 Encryption: WPA2 PSK (CCMP) Channel: 6 (2.437 GHz) Transmission power: 20 dBm Noise signals: - 38 dBm | : 0 dBm Transfer rate: 1.0 Mbit/s | countries: 00
	Wireless network enabled	Enabled by default
	Working frequency	If the current frequency has too many devices in use, please change the frequency to reduce interference and optimize the signal
	Maximum transmission power	Specifies the maximum transmitted power. Depending on regulatory requirements and usage, the driver may limit the actual transmitted power below this value.
Advanced Settings	Country code	Driven by default
	Allows traditional 802.11b rates	Selected by default
	Distance optimization	Distance of the farthest network user (in meters). By default, the transmission power is automatically adjusted according to the distance
	Fragmentation threshold	When the data length exceeds the threshold, fragments are automatically sent. The default value is generally used

	RTS/CTS The threshold value	Request send/Permit send protocol. When the data length exceeds the threshold, enable this protocol to avoid signal conflicts caused by multiple terminals sending data to the AP. The default value is generally used
	Mandatory 40MHz mode	The 40MHz channel is always used even when the auxiliary channels overlap. Using this option does not comply with IEEE 802.11N-2009! This parameter is deselected by default.
	Beacon interval	Indicates the interval at which a wireless route broadcasts its SSID periodically. The default value is generally used

Wireless network client interface configuration		
Project		Instructions
Basic setup	Mode	The Client Client
	ESSID	Name of the wireless network to be added
	BSSID	NO
	Network	Wwan, select the network assigned to this wireless interface, or fill in the Create field to create a new network. Generally do not modify.
Wireless security	Encryption	WPA2-PSK(Strong security)
	Algorithm	Automatic
	Password	Join the wireless network password
	802.11w Managing Frame Protection	Requires a full version of Wpad/HostAPd and WiFi driver support, disabled by default
	The name of the interface	Reset the default interface name
	Short Preamble	Different rates require different Preambl codes. This parameter is selected by default
	DTIMinterval	As a terminal node, periodically wakes up and sends traffic indication message intervals
	Time interval for re-encrypting GTK	The temporary secret key (GTK) uses the default value
	Disable inactive polling	Not selected by default
	Inactive site restrictions	The default 300 seconds
	Maximum listening interval allowed	Default maximum of 65535
	Disconnect on low Ack reply	Disconnect a wireless terminal in low ACK mode when AP mode is enabled. This parameter is selected by default

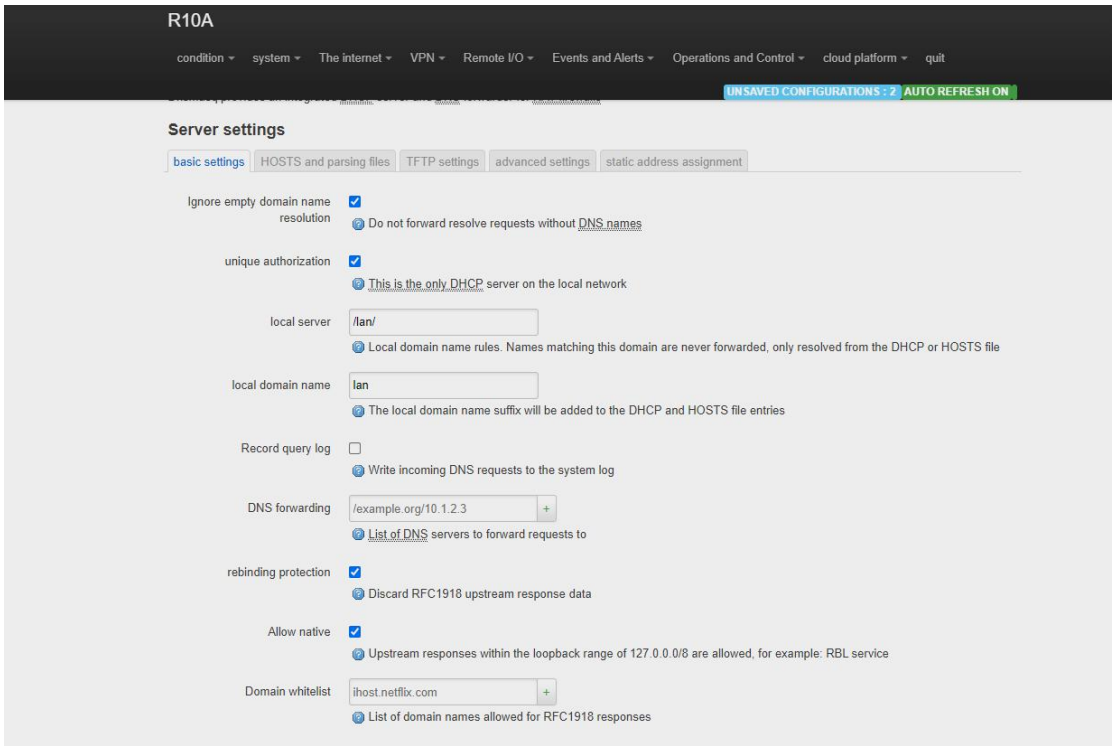
5.3.3 Cellular Network



The cellular network	
Project	Instructions
Registration status	Displays cellular registration status
Operator	The operator of the SIM card is displayed
Signal strength	Signal value normal range 14 to 31
Firmware version	Displays the module firmware version
IMSI	The IMSI code of the SIM card is displayed
IMEI	Displays the IMEI of the module
SIM card ID	The ICCID number of the SIM card is displayed
The card number	Enter card 1 number
Card APN	Enter the SIM card access point
The card user name	Enter SIM card Internet access account
Card password	Enter the SIM card Internet access password
Enable GPS	Default is disable, When the router you bought supports GPS function, please check this item to enable GPS function. GPS data will be uploaded through MQTT protocol; if the router does not have GPS function, please do not enable it. (The router does not support GPS function by

	factory default, if you need GPS function, please remark when purchase)

5.3.4 DHCP/DNS



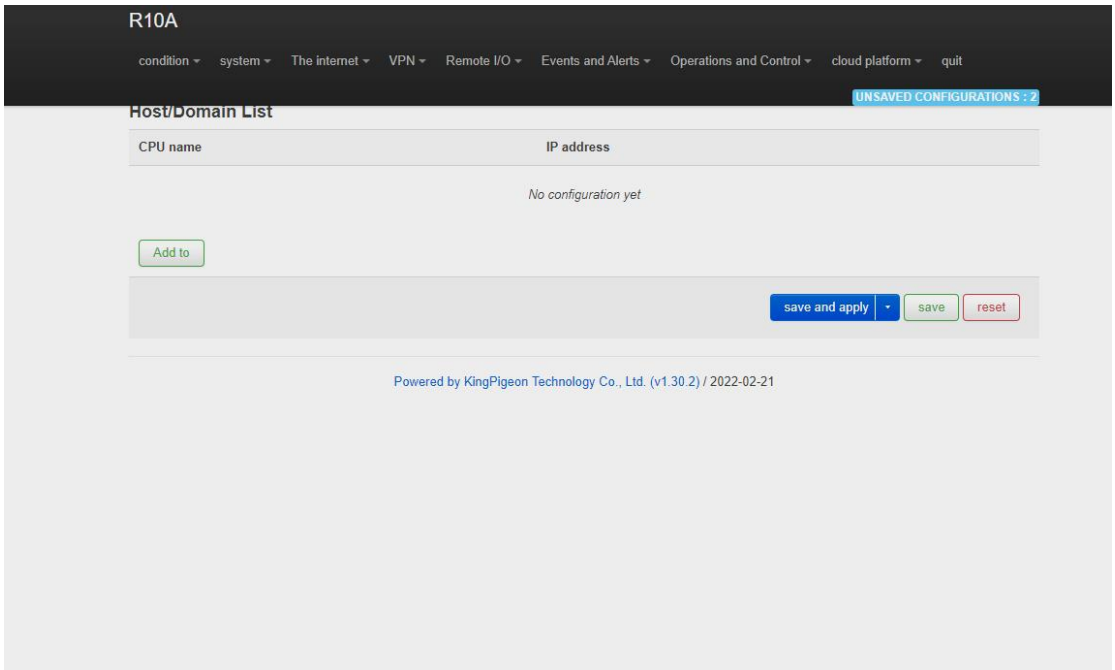
Dnsmasq Provides an integrated DHCP server and DNS forwarder for the NAT firewall。

Server Settings		
Project		Instructions
Basic setup	Ignore airspace name resolution	Do not forward resolution requests without DNS names. This parameter is selected by default
	The only authorized	This is the only DHCP server on the local network and is selected by default
	Local server	Local domain name rules. Names that match this domain are never forwarded and are resolved only from the DHCP or HOSTS file
	The local domain name	The local domain name suffix is added to the DHCP and HOSTS file entries
	Recording Query Logs	Write received DNS requests to system logs. This parameter is not selected by default
	DNS forwarding	List of DNS servers to which requests are forwarded

	Rebinding protection	Discard RFC1918 uplink response data. This parameter is selected by default
	Allow the machine	Allows uplink responses in the 127.0.0.0/8 loopback range, such as RBL service. This parameter is selected by default
	Domain name whitelist	List of domain names allowed to respond to RFC1918
	Local service only	The DNS service is available only on the subnet to which the NIC belongs. This parameter is selected by default
	Non-full address	Dynamically bound to an interface rather than a wildcard address (recommended as the Linux default), selected by default
	Listening to the interface	Listen only on these and loopback interfaces.
	Eliminate interface	Do not listen on these interfaces.
HOSTS and parse files	Use/etc/ethers configuration	Configure the DHCP server based on /etc/ethers. This parameter is selected by default
	The lease documents	Leases a file used to hold assigned DHCP leases. The default value is/TMP /dhcp.leases
	Ignoring parsing files	Not selected by default
	Ignore the/etc/hosts	Not selected by default
	Additional HOSTS files	The default empty
TFTP set	Enabling the TFTP Server	Not selected by default
Advanced Settings	Not logging	Do not record routine operation logs of these protocols. This parameter is not selected by default
	Sequential IP address assignment	IP addresses are assigned from the lowest available addresses in sequence. This parameter is not selected by default
	Filtering local Packets	This parameter is selected by default
	Filtering useless packets	Do not forward requests that the public domain name server cannot respond to. This parameter is not selected by default
	Localized query	If more than one IP is available, the host name is localized based on the subnet from which the request came, selected by default
	Extend the host suffix in the HOSTS file	Add the local domain name suffix to the domain name in the HOSTS file. This parameter is selected by default
	Disable invalid information caching	Do not cache useless responses, for example, non-existent domain names. This parameter is not selected by default
	Additional SERVERS file	This file may contain lines in formats such as

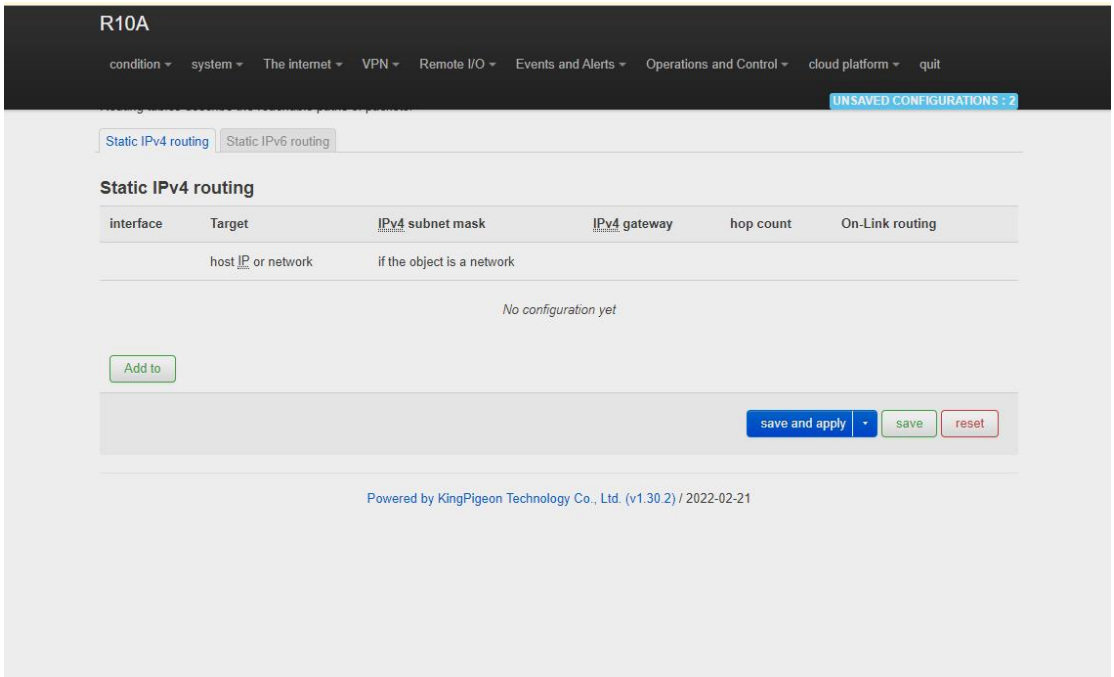
		"server=/domain/1.2.3.4" or "server=1.2.3.4". The former specifies a DNS server for a specific domain, while the latter does not limit the resolution scope of the server.
	Rigorous check sequence	Query DNS servers in the sequence in Parse File. This parameter is not selected by default
	All servers	Example Query all available upstream DNS servers. This parameter is not selected by default
	Ignore false airspace name resolution	List of servers that allow bogus airspace name responses
	DNS Server Port	Inbound DNS query port
	DNS Query port	Specifies the source port for DNS query
	Maximum number of DHCP leases	Maximum number of DHCP leases
	Maximum EDNS0 packet size	Maximum EDNS.0 UDP packet size allowed
	Maximum number of concurrent queries	Maximum number of concurrent DNS queries
	Size of DNS query cache	Number of DNS entries cached (Max. 10000,0 indicates no cache)
Static Address assignment		The static lease is used to assign fixed IP addresses and host IDS to DHCP clients. Only the specified host can be connected, and the interface must be non-dynamically configured. Use the Add button to add a new lease entry. The IPv4 address and host name fields are assigned to the hosts identified by the MAC address field. The LEASE period is an optional field. You can set the DHCP lease duration for each host, for example, 12H, 3D, and INFINITE, which indicate 12 hours, 3 days, and forever respectively.

5.3.5 Host names



After a host mapping is added, you can access a specified IP address by accessing the host name.

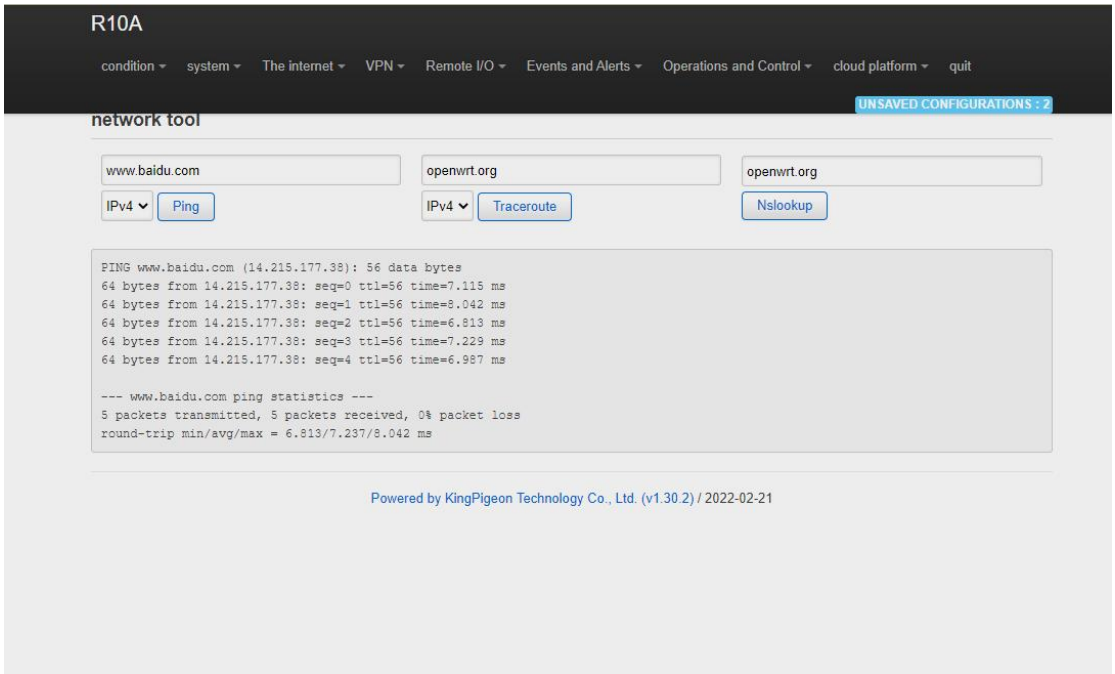
5.3.6 Static Routers



Routing tables describe the reachable paths of packets。

The routing table		
Project		Instructions
Basic setup	Interface	Select set interface
	The target	The host IP address or network must be valid
	IP Indicates the subnet mask	If the object is a network, a valid IP or network is required
	IP gateways	A valid IP or network is required
Advanced Settings	Jump points	0
	MTU	1500
	Routing type	unicast
	The routing table	main(254)
	Source address	automatic
	On cc-link routing	Not selected by default

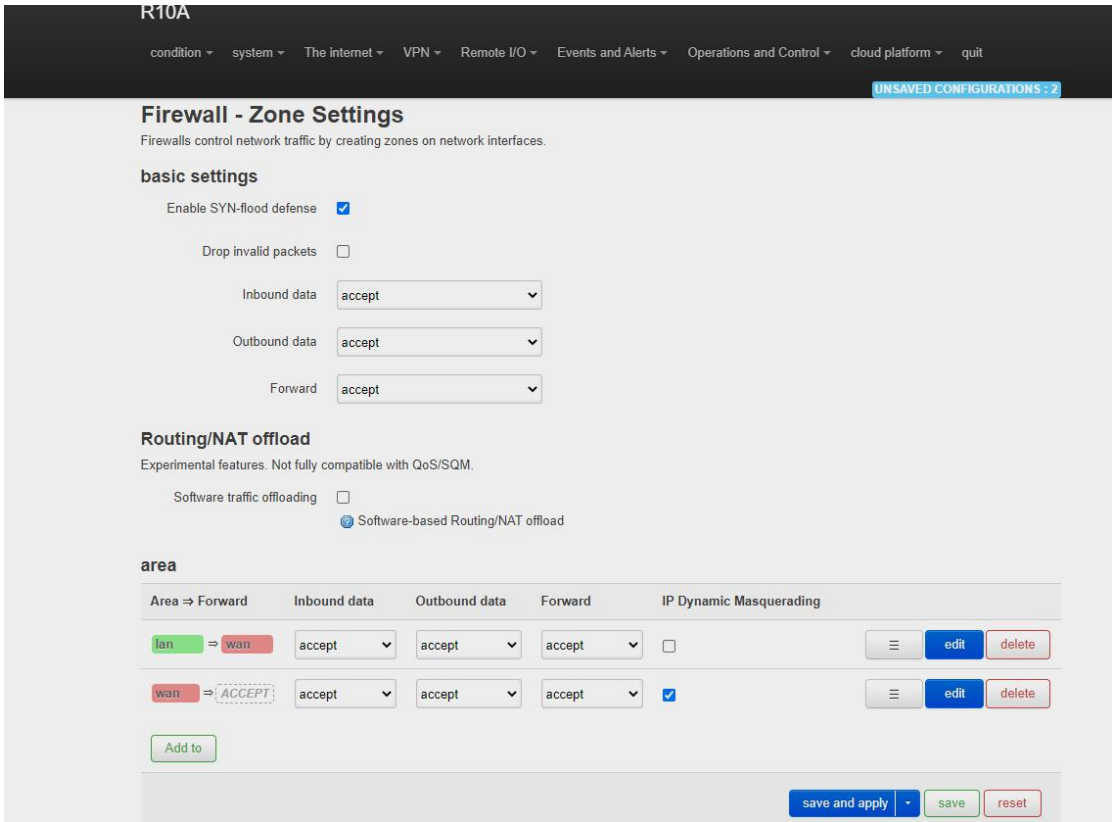
5.3.7 Diagnosis



The Ping, Traceroute, and Nslookup commands are provided to perform simple network diagnosis.

5.3.8 Firewall

5.3.8.1 Zone settings



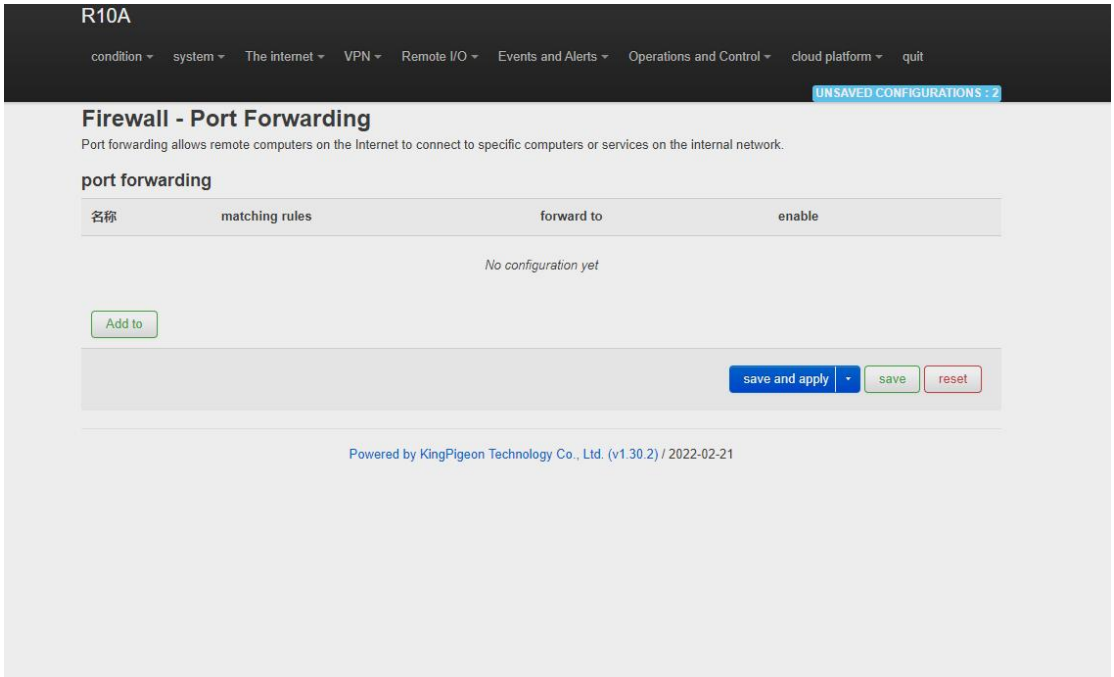
Firewalls control network traffic by creating zones on network interfaces。

Firewall - Area Settings		
Project		Instructions
Basic setup	This section defines generic attributes for "LAN". Inbound data and outbound data options Set the default policies for inbound and outbound traffic in the zone. The forwarding option describes the traffic forwarding policies between different networks in the zone. The covered networks specify the networks that are subordinate to this zone.	
	The name of the	lan
	Inbound data	The default accept
	The outbound data	The default accept
	Forwarding	The default accept
	IP dynamic camouflage	You do not need to set the IP address of the LAN interface. The IP address of the WAN interface may change during dynamic allocation. Therefore, you need to configure dynamic camouflage to connect to the Internet
	MSS muzzle	Automatically adjust MSS (maximum segment size) according to MTU (maximum transmission unit)

	Covered networks	lan
	Allows forwarding to the target zone	wan
	Allow forwarding from the source region	Is not specified
Advanced Settings	The following options control the forwarding policy between this LAN and other zones. The destination area receives the forwarding traffic from the LAN. Traffic matched by the source zone is forwarded from other zones whose destination is THE LAN. Forwarding rules are unidirectional. For example, forwarding traffic from the LAN to the WAN does not mean that traffic from the WAN to the LAN can be forwarded in reverse.	
	Equipment covered	This option classifies area traffic for raw, non-UCI-hosted network devices.
	Covered subnets	This option classifies area traffic for source or target subnets rather than networks or devices.
	Limit the address	IPv4 and IPv6
	Source subnets to restrict IP dynamic masquerade	Based on actual Settings
	Target subnets to restrict IP dynamic masquerade	Based on actual Settings
	Enable logging for this zone	Not selected by default
Conntrack set	Allow "invalid" traffic	Do not install additional rules to reject forward traffic whose Conntrack status is invalid. This may be a necessary setting for complex asymmetric routes. This parameter is not selected by default.
	Automatic assistant assignment	Automatically assign conntrack assistants based on traffic protocols and ports. This parameter is selected by default.
Additional iptables parameters	By passing iptables parameters to classification rules for source and target traffic, packets can be matched based on criteria other than interfaces or subnets. Care should be taken with these options because invalid values can break the firewall rule set and expose all services.	
	Additional source parameters	The iptables parameter is added to classify incoming traffic in an area. For example, -p TCP --sport 443 matches only inbound HTTPS traffic.

	Additional target parameters	The iptables parameter is added to classify area outgoing traffic. For example, -p TCP --dport 443 matches only outbound HTTPS traffic.

5.3.8.2 Port forwarding

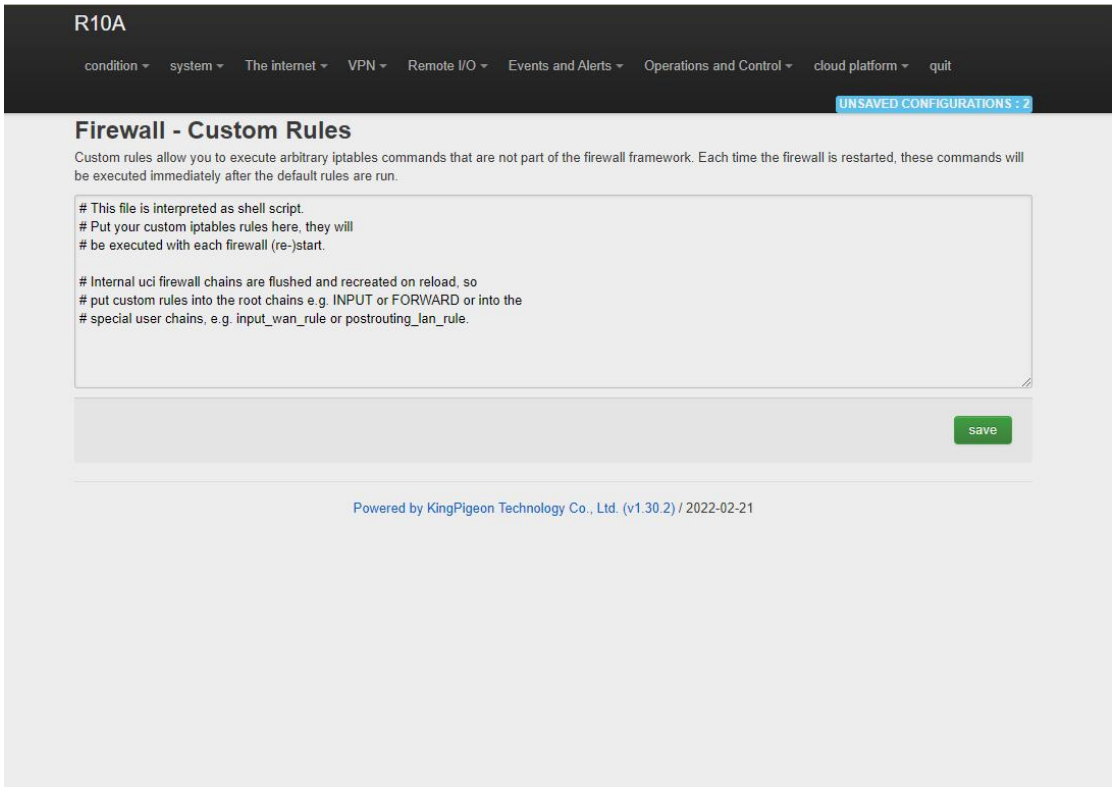


Port forwarding allows remote computers on the Internet to connect to specific computers or services on the internal network

Firewall - Port forwarding		
Project		Instructions
Basic setup	The name	Forward named
	Agreement	Optional TCP+UDP、TCP、UDP、ICMP
	The source area	wan
	External port	Matches inbound traffic that points to a specified destination port or range of destination ports on this host
	The target area	lan
	Internal IP address	Redirects matching inbound traffic to the specified internal host
	The internal port	Redirect the matched inbound traffic to the port of the internal host
Advanced Settings	The source MAC address	Only inbound traffic from these Macs is matched.

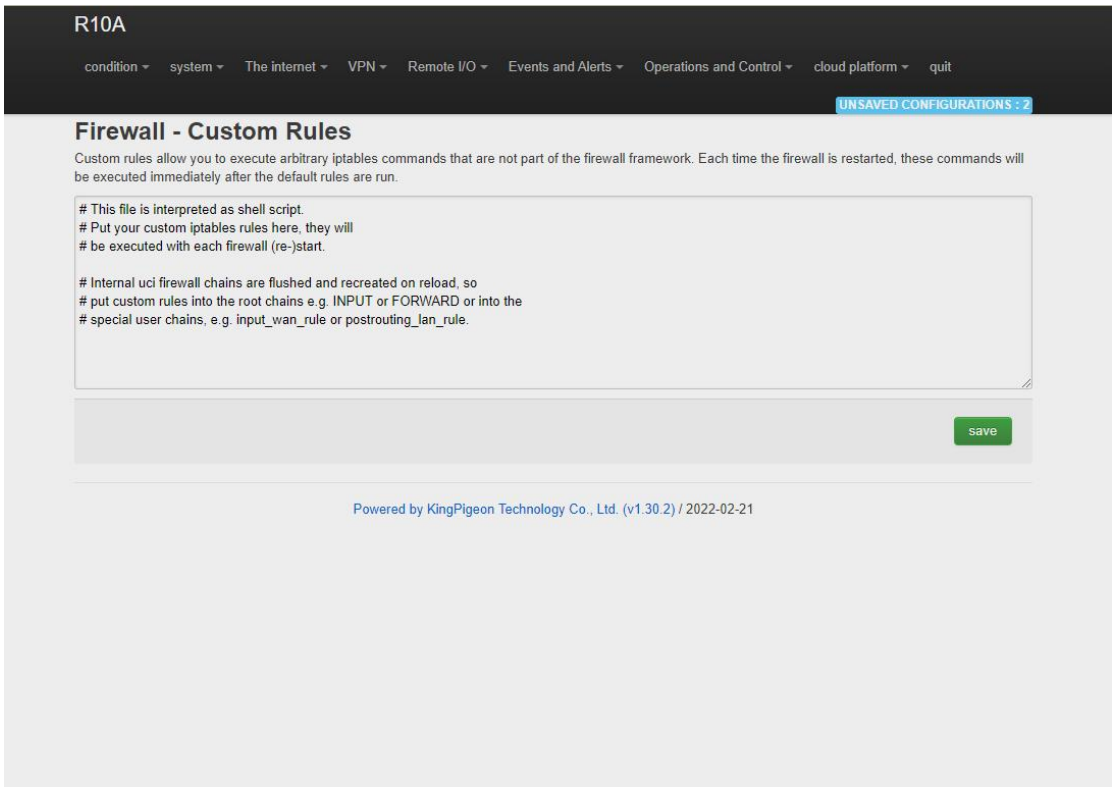
	The source IP address	Only inbound traffic from this IP address or IP range is match。
	Source port	Matches only inbound traffic originating from a given source port or range of source ports on the client host
	External IP address	Only inbound traffic from this IP address or IP range is match
	Enable NAT loop back	Selected by default
	Additional parameters	Additional arguments passed to iptables. Careful when use it

5.3.8.3 Traffic rules



Communication rules define packet transmission policies between different areas. For example, they deny communication between hosts and open ports on the ROUTER WAN.

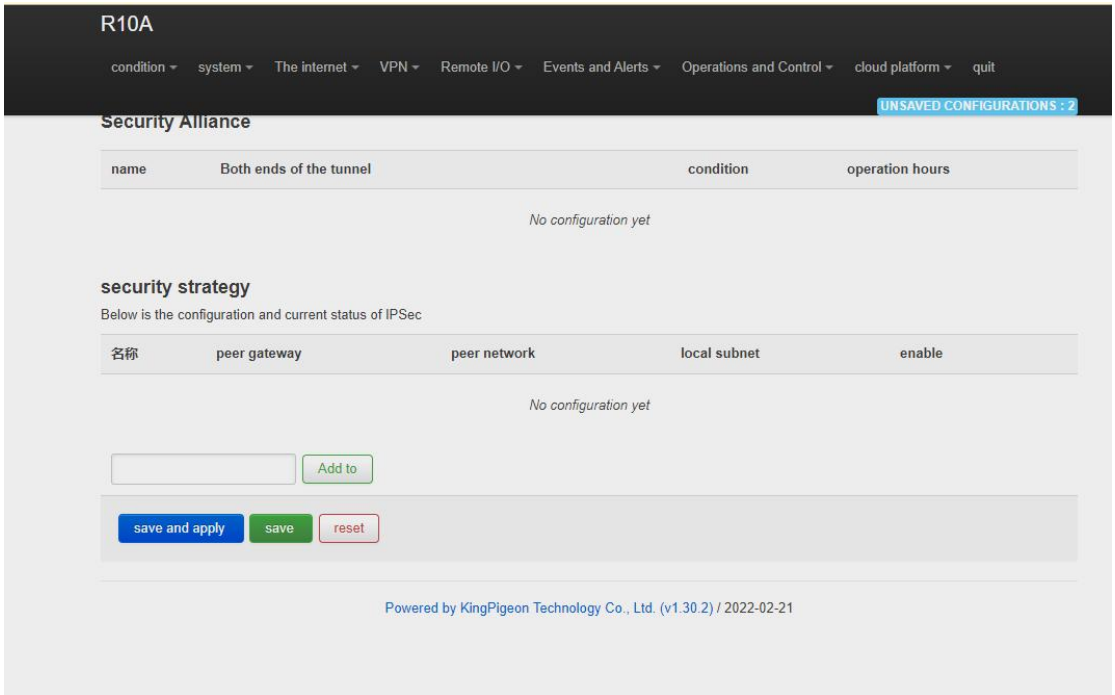
5.3.8.4 Custom rules



Custom rules allow you to execute arbitrary iptables commands that are not part of the firewall framework. Each time you restart the firewall, these commands will be executed immediately after the default rules run.

5.4. VPN

5.4.1 IPSec



IPSec is an open network layer security framework protocol developed by Internet Engineering Task Force (IETF). It is not a single protocol, but a collection of protocols and services that provide security for IP networks. IPSec includes Authentication Header (AH) and Encapsulating Security Payload (ESP). Internet Key Exchange (IKE) and some algorithms used for network authentication and encryption.

IPSec provides security services for IP packets through encryption and authentication. Security services provided by IPSec

Including：

(1) User data encryption: provide data privacy through user data encryption.

(2) Data integrity verification: ensure that data has not been tampered in the transmission path through data integrity verification.

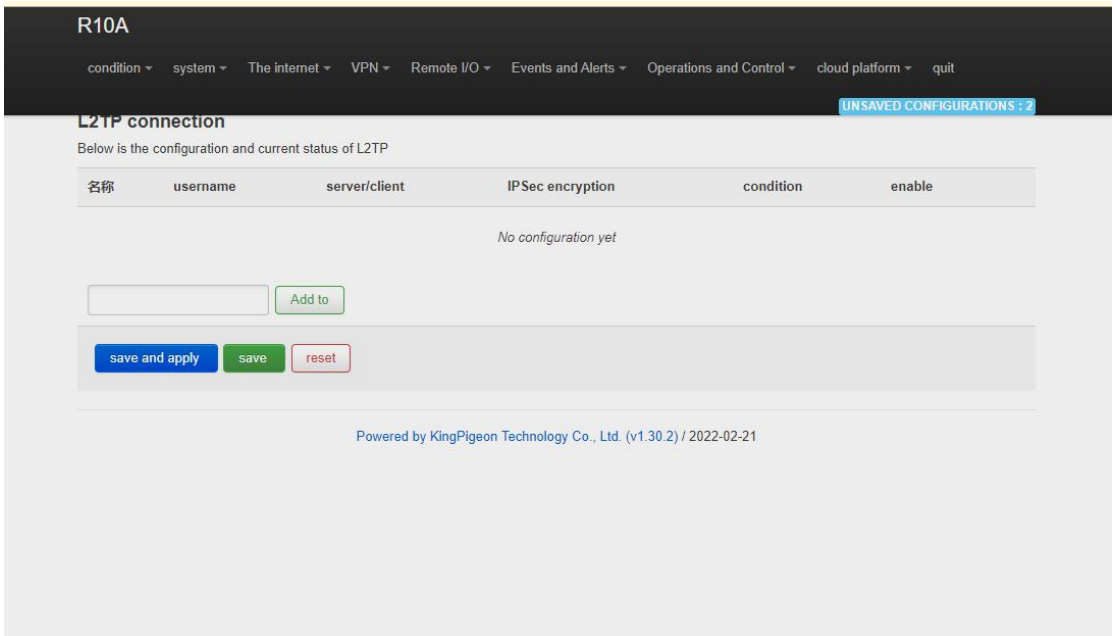
(3) Data source authentication: Ensure that the data comes from the real sender by authenticating the source that sends the data.

(4) Prevent data replay: prevent malicious users from repeatedly sending captured data packets to attack by rejecting repeated data packets at the receiver.

IPSec		
Project		Instructions
IPSec configuration	Enable	Check the enable
	Encapsulation type	Tunnel mode and transmission mode are optional. Tunnel mode Indicates host-to-host, host-to-subnet, or subnet-to-subnet tunnels. Transport Mode Indicates the host-to-host transmission mode.
	To end the gateway	Peer gateway with which the IPSec connection is established
	Local subnet IP address/mask	In tunnel mode, you need to specify the local end and peer terminal network range for the subnet-to-subnet tunnel
	IP/ mask of the terminal network	In tunnel mode, you need to specify the local end and peer terminal network range for the subnet-to-subnet tunnel
	Pre-shared key	Pre-shared keys are used for authentication by default
Stage 1 Setup		Phase 1 negotiates encryption parameters, exchanges key information, and authenticates device identities
IKE Encryption Algorithm		Specify the protocol message encryption algorithm in the IKE negotiation phase
Authentication algorithm		Specify the digital signature authentication algorithm for encrypted packets
DH group		Specifies the Diffie Hellman (DH) key group used for key exchange
IKE version		IKEv1or IKEv2
Exchange pattern		Main mode or Savage mode. The main mode is safer and faster than the aggressive mode. If the responder (server) cannot know the address of the initiator (end user) in advance or the address of the initiator always changes and both parties want to use the pre-shared key authentication method to create an IKE SA, the aggressive mode can be adopted
Negotiation model		Responder or originator, the originator is the end user and the responder is the server
Local ID		The value can be an IP address, standard domain name, email address, or distinguished name. The default value is a local IP address
The client ID		It can be an IP address, standard domain name, email address, or distinguished name. The default is the peer IP address

IKETime to live	The time to renegotiate the key
Stage 2 Setup	Phase 2 establishes an IPSec SA for data transmission
ESP encryption algorithm	Specifies the algorithm used for data encryption
The hash algorithm	Specifies the digital signature authentication algorithm for encrypted data
PFS group	Perfect Forward Secrecy (PFS) : When a key is decrypted, the security of other keys is not affected
Time to live	How long should it take from the negotiation success to the connection instance
DPD detection interval	Dead Peer detection (DPD) : When no traffic occurs within a period of time, the local end sends a DPD message to Detect the status of the Peer end before sending traffic

5.4.2 L2TP



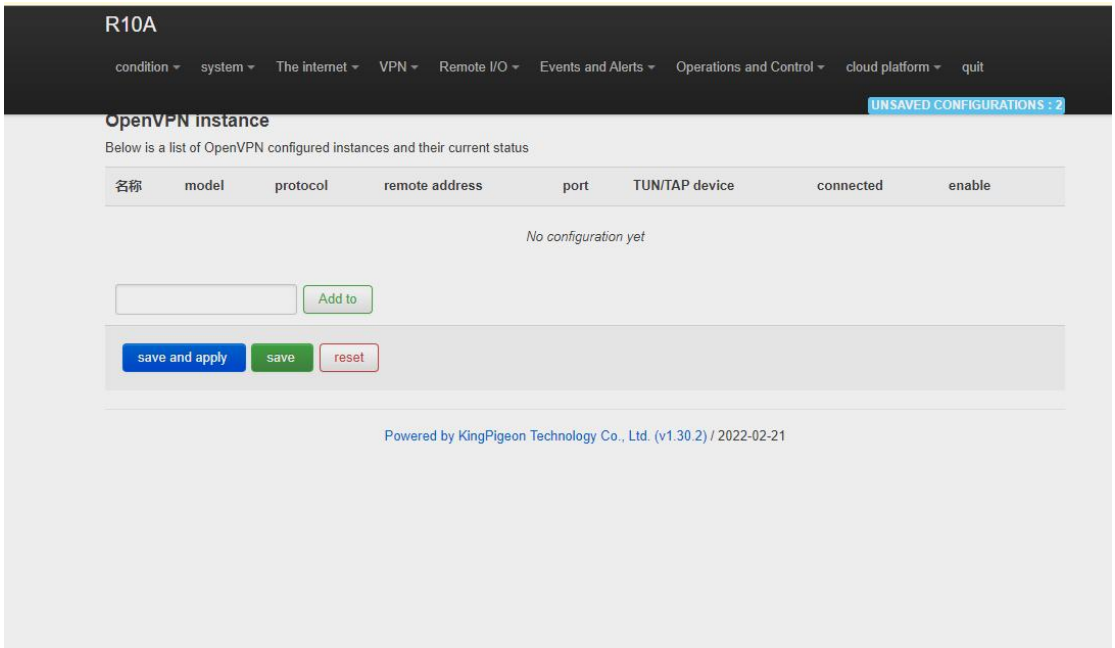
Layer 2 Tunneling Protocol (L2TP) is a Virtual Private Dial-up Network (VPDN) tunnel Protocol.。
The Virtual Private Dial Network (VPDN) uses the dial-up function and access Network of public networks (such as ISDN and PSTN) to implement the Virtual Private Network (VPDN) to provide access services for enterprises, small ISPs, and mobile office workers.
VPDN uses a dedicated network encryption communication protocol to establish secure virtual private networks for enterprises on public networks. An enterprise's overseas offices and

employees on business trips can remotely connect to the enterprise headquarters over the public network through a virtual encrypted tunnel. However, other users on the public network cannot access resources on the enterprise network through the virtual tunnel. The Layer Two Tunneling Protocol (L2TP) is the most widely used VPDN tunnel Protocol.l。

PPP defines an encapsulation technology that can transmit packets of various protocols on layer 2 point-to-point links. In this case, PPP runs between users and Network Access servers (NAS). L2TP supports Tunnel transmission of PACKETS at the PPP link layer, allows layer-2 link endpoints and PPP session points to reside on different devices, and uses packet switching technology to exchange information, thus extending the PPP model. L2TP function is to establish point-to-point PPP session connections on a non-point-to-point network. L2TP combines the advantages of Layer 2 Forwarding (L2F) and Point-to-point Tunneling Protocol (PPTP), becoming the industrial standard of IETF.

L2TP	
Project	Instructions
Enable	Check the enable
User name	User name used for PPP authentication
Password	Password used for PPP authentication
Server/client	The client and server are optional
Server address	Address of the L2TP Network Server (LNS)
IPSec encryption	Optional: Use the default IPSec policy when selecting IPSec encryption. Manual IPSec configuration is not required. Before using an IPSec policy, you need to configure an IPSec policy in advance
Pre-shared key	When selecting encryption, you need to set the pre-shared key of IPSec
The security policy	The IPSce security policy has been configured

5.4.3 OpenVPN



OpenVPN is an application-layer VPN implementation based on OpenSSL library. It uses virtual network cards to establish connections and transmit data, and uses SSL to encrypt and authenticate data.

Virtual network card is a driver software implemented by network programming technology. It can be configured like other network cards. If an application to access a remote virtual address (belong to virtual network card with the address of the series, different from the real address), the operating system will be through the routing mechanism packets (top) or data frames (TAP) sent to the virtual network adapter, service program receives the data and process accordingly, through the SOCKET send out from the Internet, The remote server program receives data from the Internet through the SOCKET, processes the data, and sends it to the virtual network card. Then the application software can receive the data, completing a one-way transmission process, and vice versa. OpenVPN provides two types of virtual network interfaces: the universal Tun/Tap driver, through which layer 3 IP tunnels can be established or virtual Layer 2 Ethernet can transmit any type of Layer 2 Ethernet data, which can be compressed by LZO algorithm.

The Secure Socket Layer (SSL) protocol uses the public key system and X.509 digital certificate technology to protect the confidentiality and integrity of information transmission. The SSL protocol includes server authentication, customer authentication (optional), data integrity on SSL links, and data confidentiality on SSL links. SSL is independent of application-layer protocols. High-level application-layer protocols (such as HTTP, FTP, and Telnet) can be transparently established on SSL. SSL completes encryption algorithm, communication key negotiation, and server authentication before communication with application-layer protocols. After this, data transmitted by application-layer protocols is encrypted to ensure communication privacy.

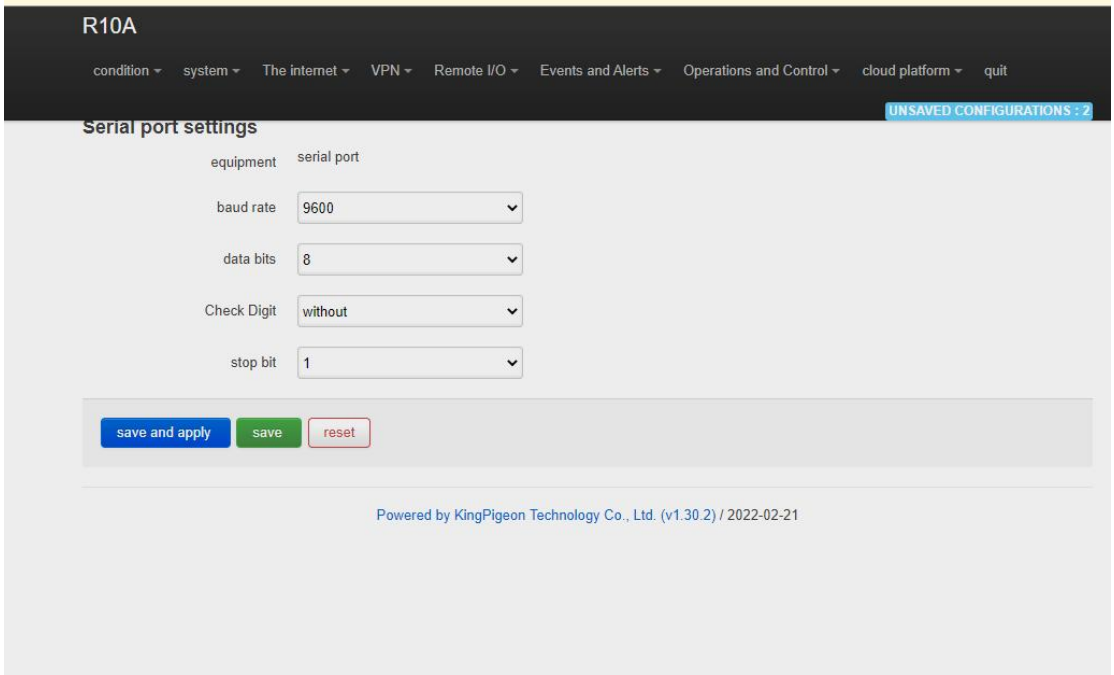
OpenVPN	
Project	Instructions

Enable	Check the enable
Configure the client mode	Select client mode
VPN Subnet IP address/mask	In TAP mode, the server can transfer data from a host to a subnet
Server address	IP address of the server with which the client establishes a VPN connection
Port	TCP/UDP port provided by the server for establishing connections. The default value is 1194
Use agreement	UDP, TCP-server, and TCP-client are used by default
TUN/TAPequipment	TUN mode Establishes layer 3 tunnels to implement point-to-point transmission. Layer 2 tunnels are established in TAP mode to implement transparent transmission of IP packets
User name/password	When security certificate authentication is not applicable, you can use the user name and password for authentication
Encryption algorithm	Select an encryption algorithm for data
Authentication and Authorization (Root Certificate)	Select the root certificate provided by the server for file upload
Local certificate	If file upload is selected, the client certificate is generated based on the root certificate
A local private key	Select the key corresponding to the client certificate for file upload
DH key exchange parameters	This command is used for key exchange and can be generated by openssl dhparam-out dh2048.pem 2048
Compression algorithm	LZO、LZ4
Keepalive interval time (seconds)	Interval at which the server sends probe packets to the client
Keepalive timeout time (s)	If the server does not receive any response from the probe packet at this time, the connection is restarted

Note: When uploading the certificate file, you need to find the directory where the file is saved after you click to select the file, and then select the file after the upload is complete.

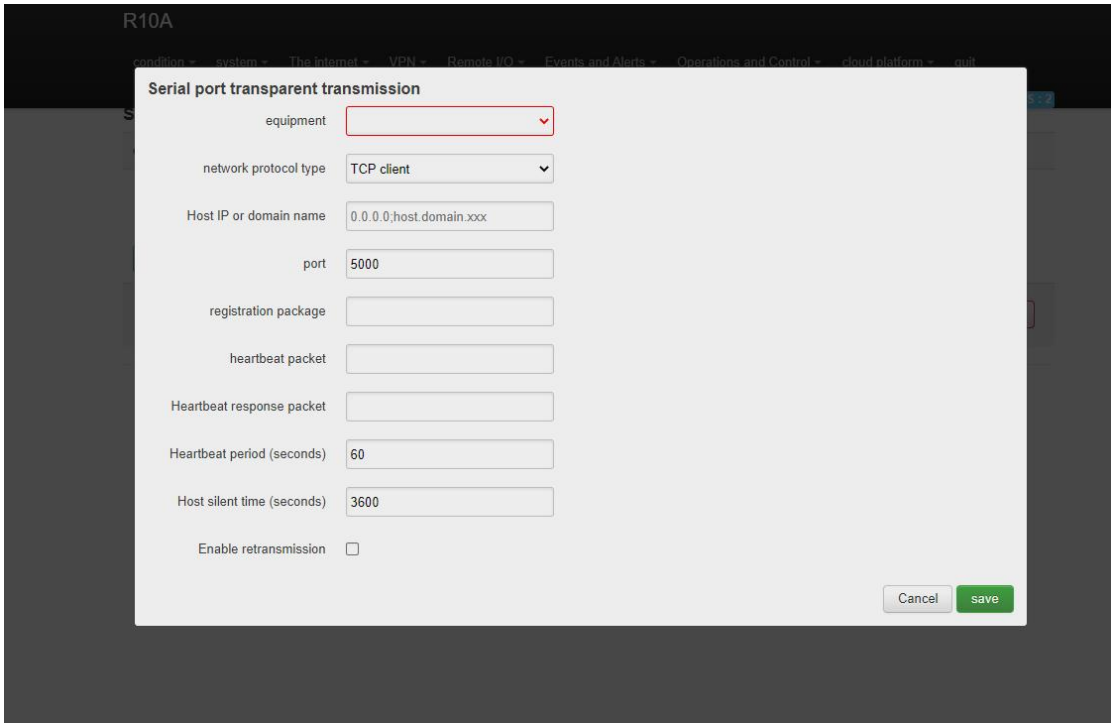
5.5. Remote I/O and Serial Port setting

5.5.1 Serial Port settings

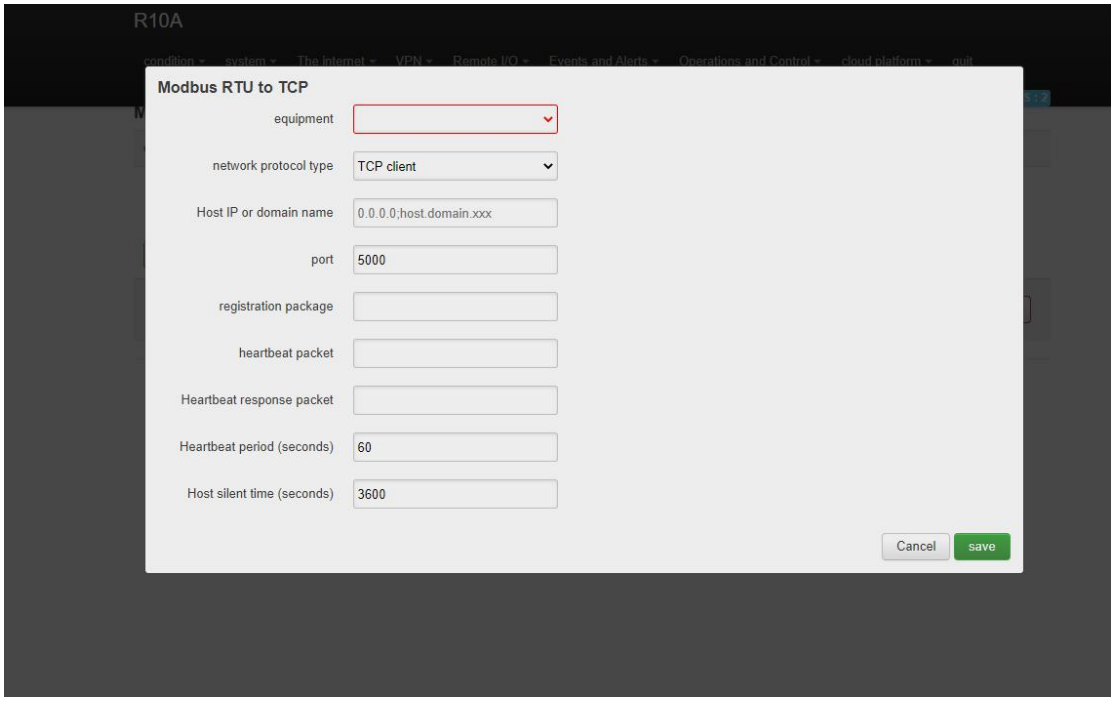


Serial port Settings		
Project		Instructions
ID of the local Modbus device		Modbus device ID Ranges from 1 to 247. The default value is 1
RS485 set	Baud rate	Optional 1200，2400，4800，9600，14400，19200，38400，57600，115200，230400
	Data bits	Optional 5，6，7，8
	Check digit	Optional None, parity check, even check
	Stop bit	Optional 1，2

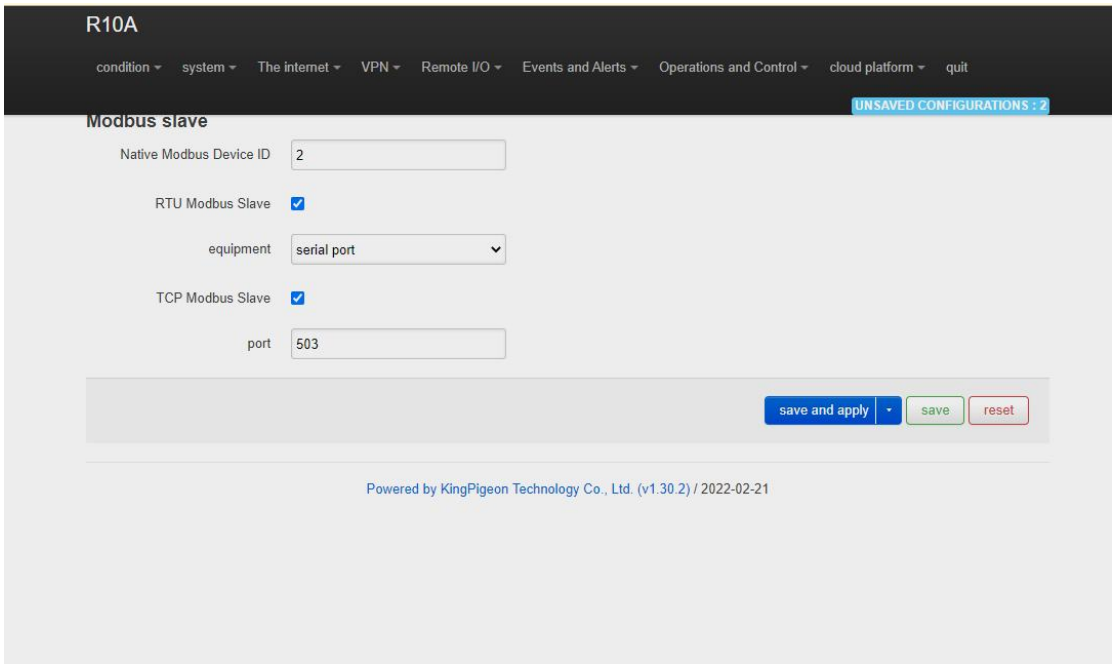
5.5.2 Transparent Transmission data



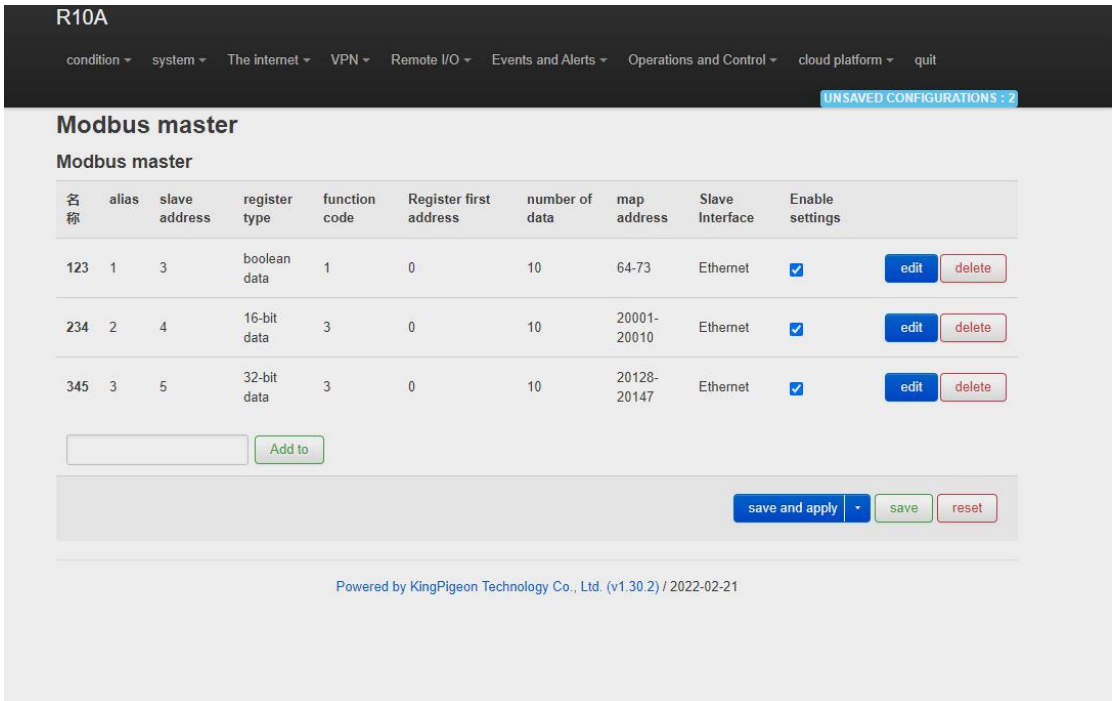
5.5.3 Modbus RTU to TCP



5.5.4 Modbus Slave

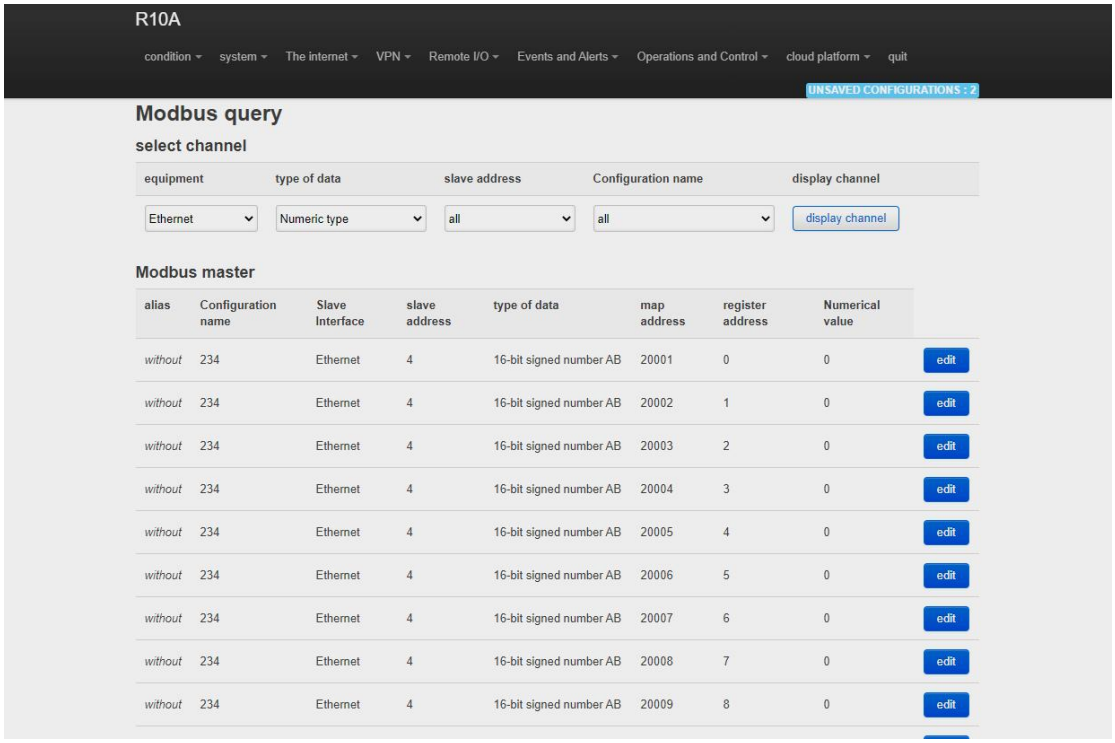


5.5.5 Modbus Master

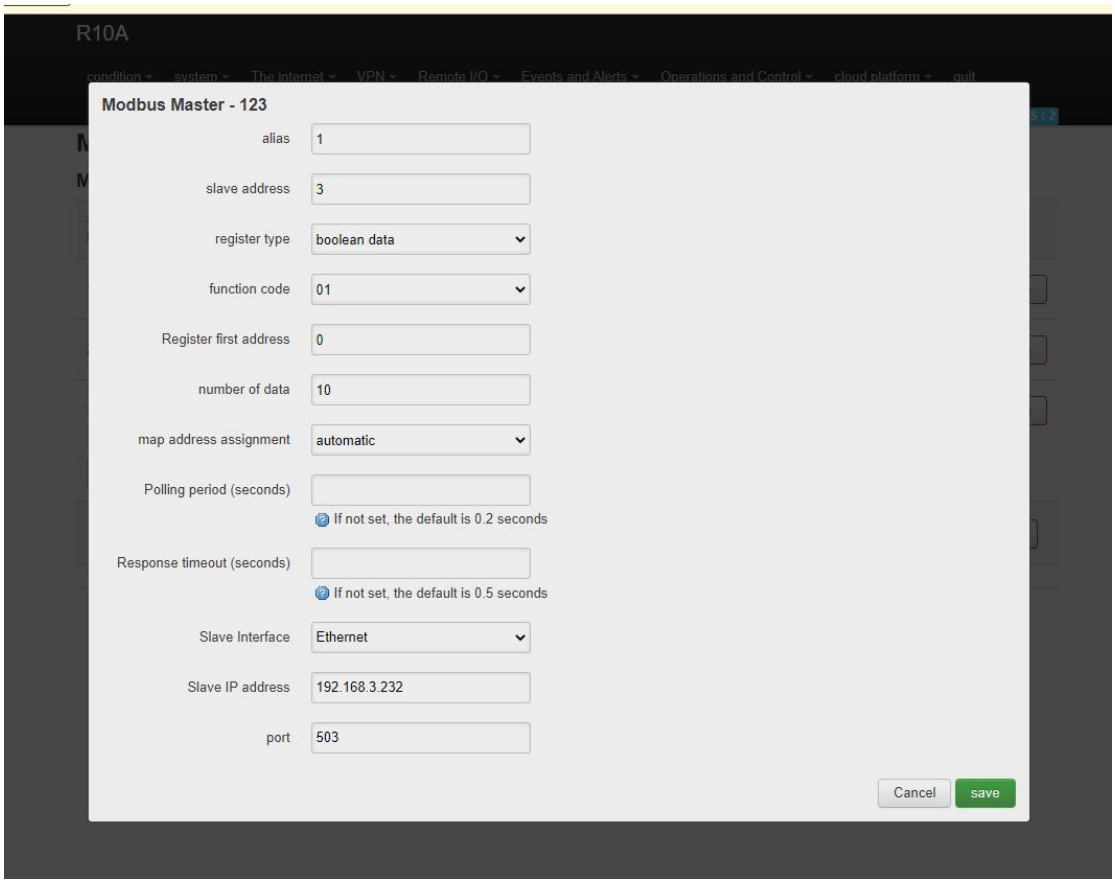


Note: The Modbus master is displayed only when the selected device model supports this function.

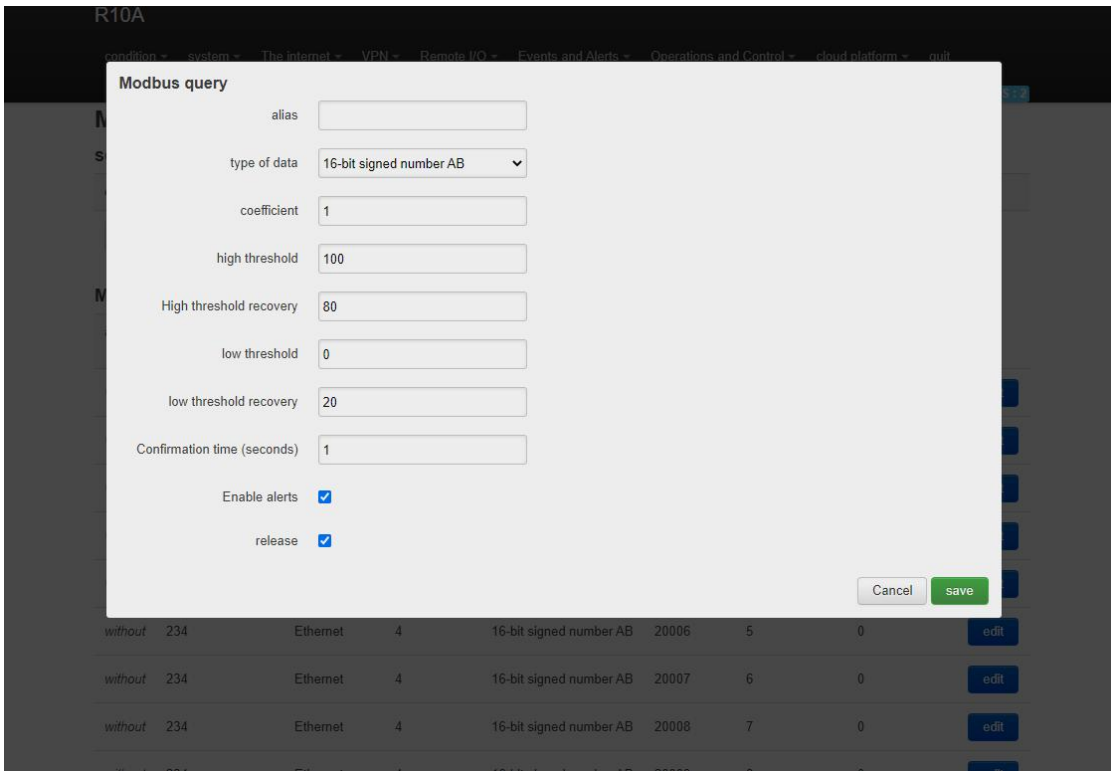
Before clicking "Add", you need to fill in the name; otherwise, the file cannot be saved.



Click "Edit" on the last edge to enter the interface for setting slave mapping parameters：



Click "Edit" under detailed configuration to enter the interface of setting slave data points:

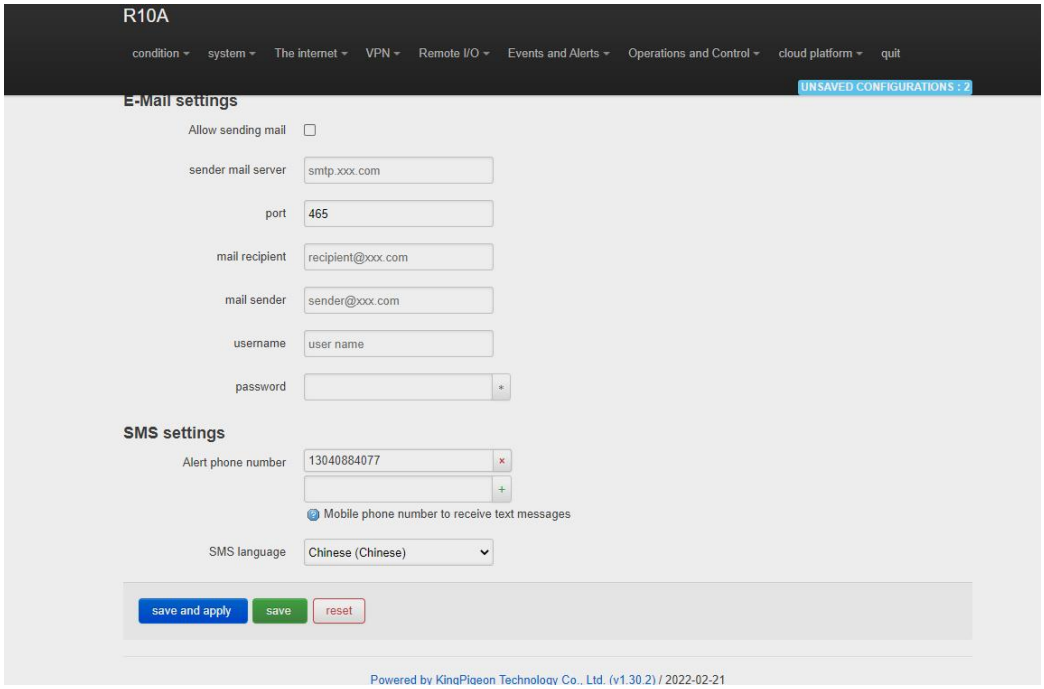


Modbus master	
Project	Instructions
Enable	Check the enable
Alias	Name the setting
Slave address	ID of a Modbus device on the slave
Register type	Boolean data, 16 bit data, 32 bit data
Function code	01, 02, 03, 04; 01/02 function code applies to Boolean data type, 03/04 function code applies to 16/32 bit data type; If 01 is selected, 05/15 is supported. If 03 is selected, 06/16 is supported.
Register start address	Set according to the slave register address
The number of data	Set according to the number of slave registers
Mapping address allocation	Automatic, manual
Mapping start address	Player movement distribution visible; Boolean type mapping register addresses 64~256, 16-bit data type mapping addresses 20001 to 20127, 32-bit data type mapping addresses 20128 to 20254
Slave interface	RS485/RS232, Ethernet If RS485 or RS232

		has been configured for serial port applications, this parameter is unavailable
IP address of the slave machine		Visible when Ethernet is selected from the machine interface
Port		Visible when Ethernet is selected from the machine interface
Detailed configuration	Mapping the address	Slave register address
	The alias	Name slave data points, for example, note usage; After the alias is set, the slave data point is displayed as the configured alias on other configuration pages. If no alias is set, the slave data point is displayed as the mapped address
	The data type	Slave register data type
	Input type	Boolean data type visible, open or closed
	The coefficient	The 16/32 bit data type is visible, and the true value is proportional to the register value
	High threshold	16/32 bit data type visible, greater than or equal to the high threshold will trigger an alarm
	High threshold recovery	16/32 bit data type visible, less than or equal to the high threshold recovery value will trigger alarm recovery
	The low threshold	16/32 bit data type visible, less than or equal to the low threshold will trigger an alarm
	Low threshold recovery	16/32 bit data type visible, greater than or equal to the low threshold recovery value will trigger alarm recovery
	Confirmation time (s)	Confirm trigger alarm time
	To enable the alarm	Select Enable Alarm
	Action	The machine can be linked to DO closed or disconnected
	Hold time (seconds)	DO action time
	Release	Check to publish data via MQTT

5.6. Event and Alarm (without RTU IO)

5.6.1 Alarm by E-mail & SMS

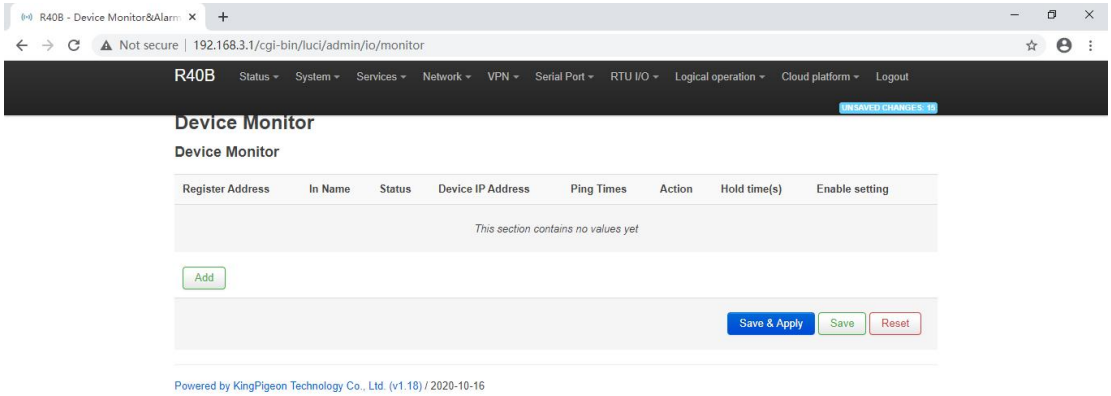


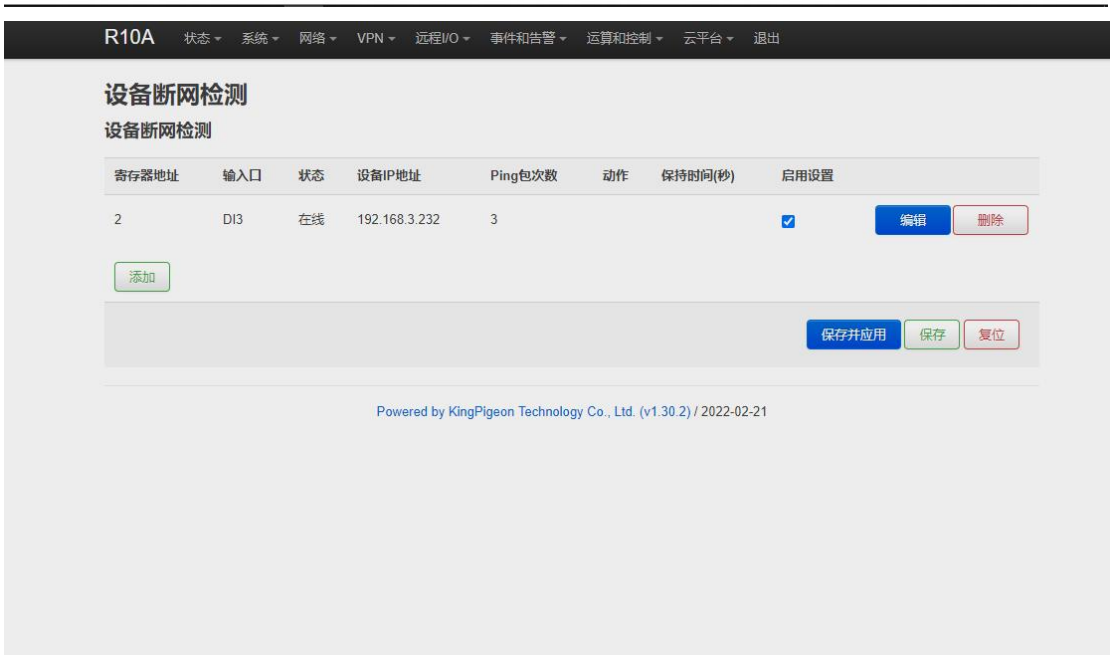
Email Settings	
Item	Description
Allow sending emails	Check allow mail to be sent
Mail server	Enter the SMTP mail server address smtp.qq.com
port	Port number of the SMTP mail server Port number: 465
Mail recipient	Enter the email receiving address
Mail sender	Enter the email sending account address
The user name	Enter the email sending account user name (User's email address Opens the SMTP server)
Password	Enter the third-party password for enabling the SMTP port
SMS Settings	
Project	Instructions
Alarm Phone Number	You can add multiple mobile phone numbers to receive SMS messages. After entering a mobile phone number, click + to save the number
Short message language	Optional English, Chinese (Chinese)

Note: The SMTP service must be enabled on the mail server. If the mail fails to be sent, ensure that the SMTP service is enabled on the email box and the account and password are correct.

5.6.2 Device monitor (device disconnection alarm)

This function allows the router device detect itself whether connect to internet properly. In case of network disconnection, router will enable alarm and trigger action.

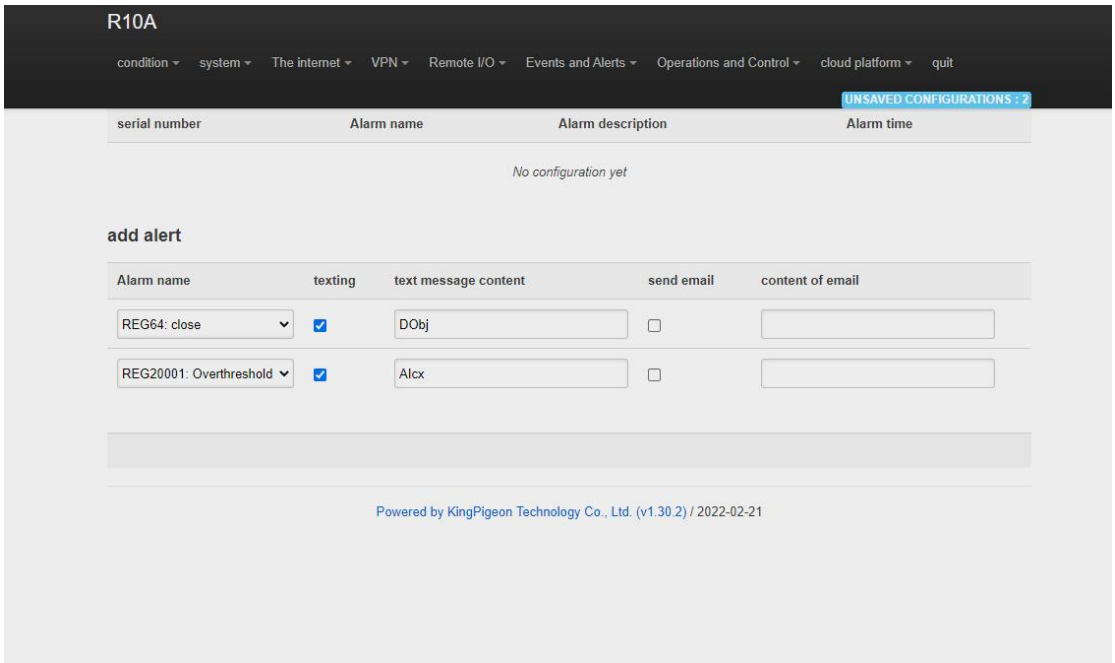




Device Monitor(router disconnection alarm)	
Item	Description
Register address	Range 2~63
Input	DI3~DI64，Automatically generated according to the register address, MQTT report data identifier
Device IP address	Detect IP address of device （ Max 20 IP

	addresses can be detected）
PING times	According to the set value PING how many times, if there is no PING, then the detection equipment is disconnected from the network
Action	Linkage DO close or open
Hold time (seconds)	DO action time
Enable	Tick to enable

5.6.3 Event and Alarm



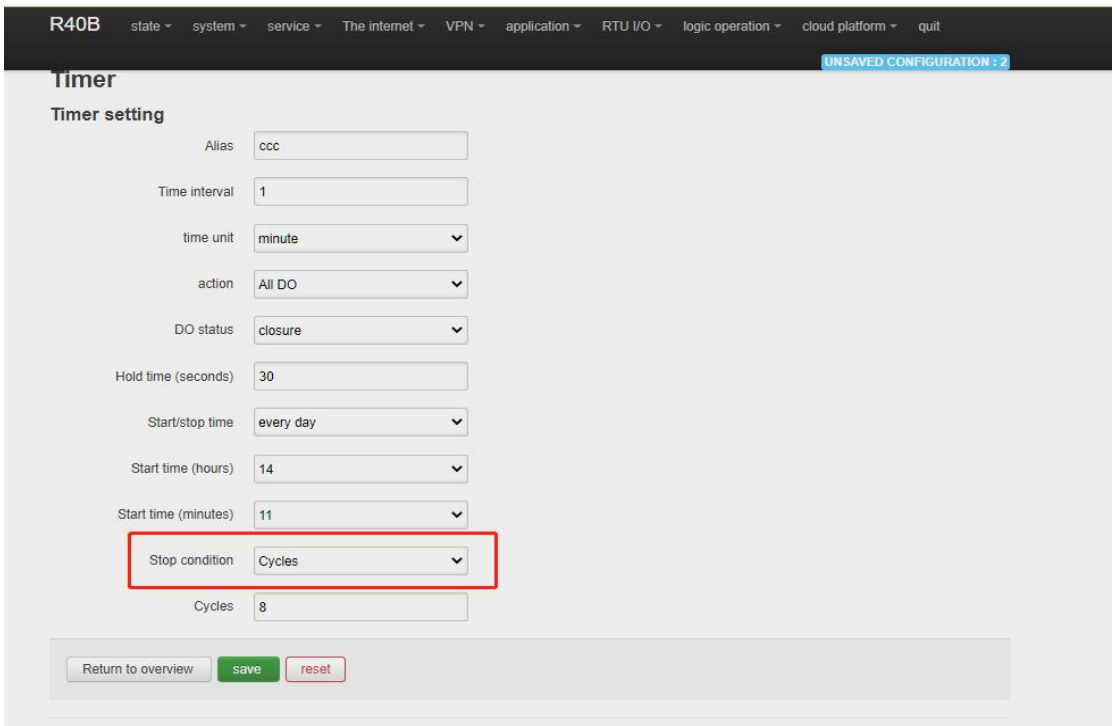
When the trigger conditions are set in the Modbus master , digital input and output, analog input, network disconnection detection and alarm related settings and the alarm is enabled, the related alarm events can be seen here. You can set related alarm messages and content of email.

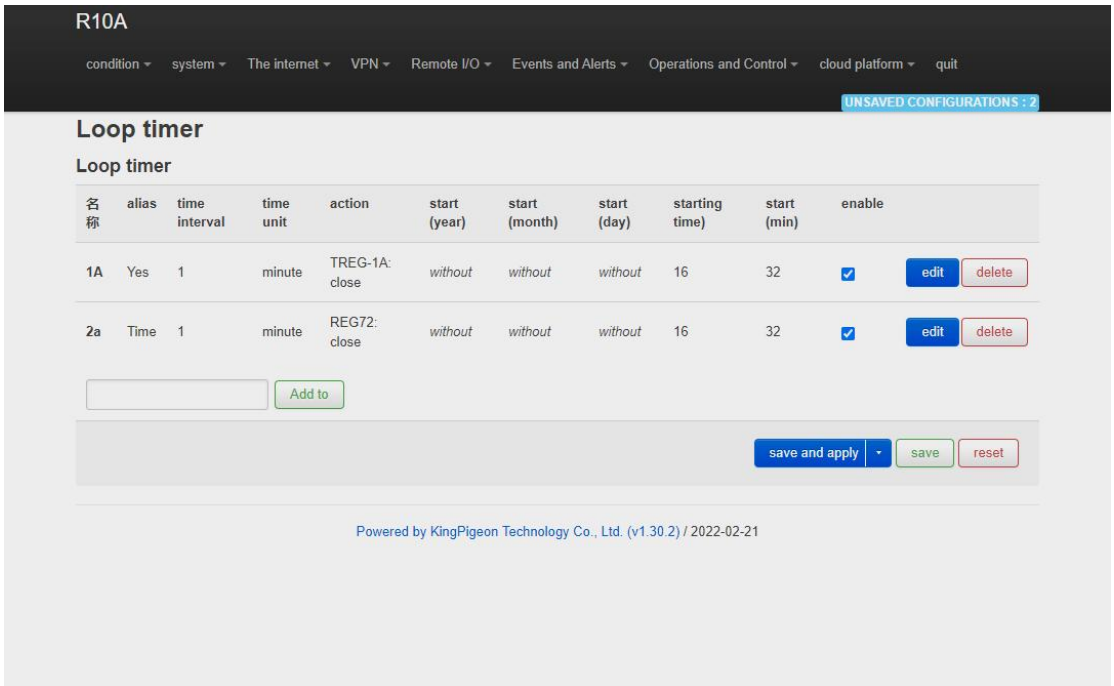
Note: SMTP service needs to be enabled to use the mail server.

If email is sent unsuccessfully, please check again to make sure the SMTP service is enabled in the mailbox settings, and the account password is entered correctly.

5.7 Edge computing and logical control

5.7.1 Timer





Timer execution actions are optional, such as trigger DO close or open, send mail, restart device etc

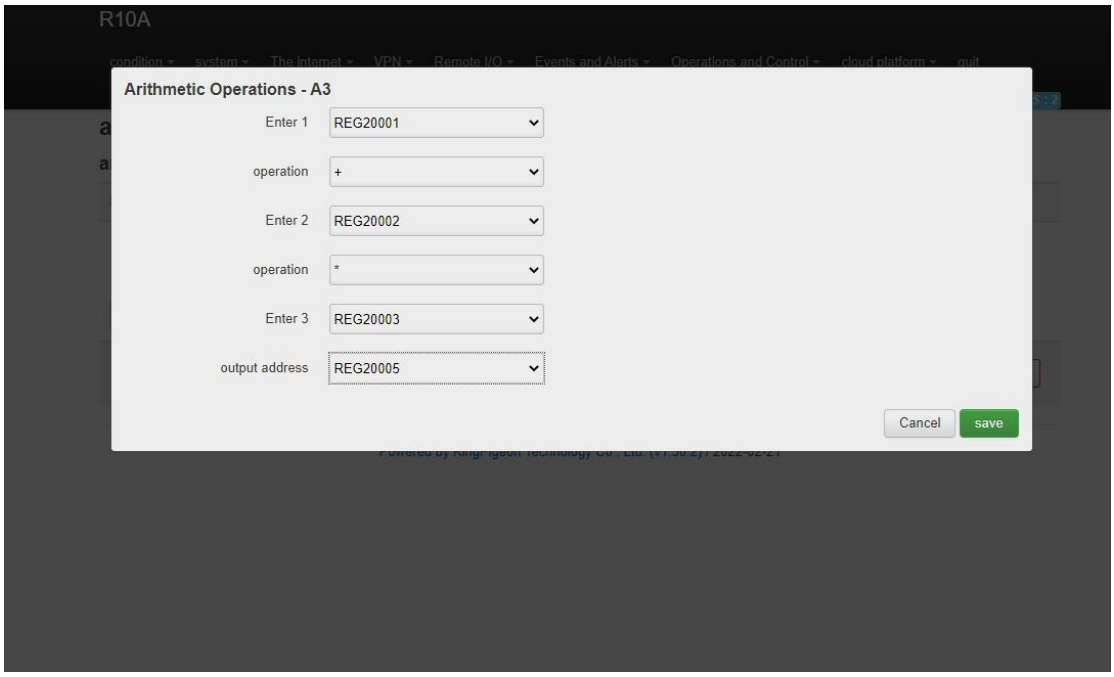
Regular timer: Execution at a certain regulation such as daily or weekly

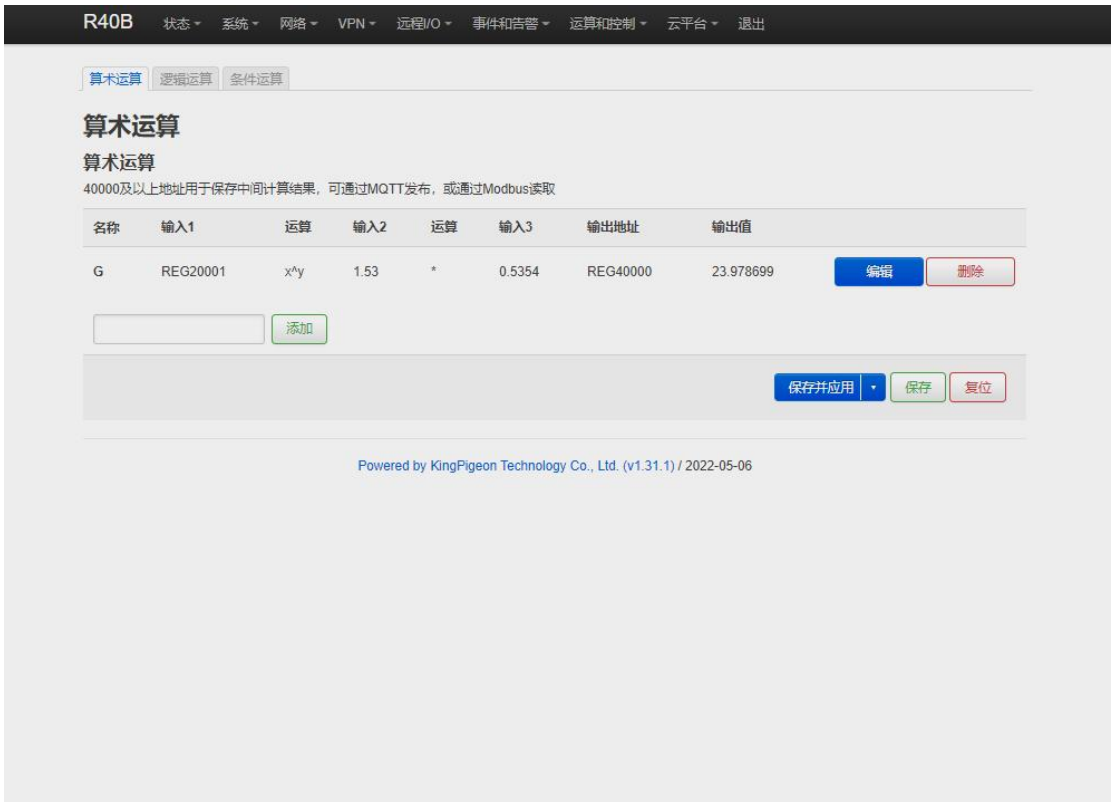
Once timer: Execution only one time at a certain appointed time, similar to Alarm clock

Cycle timer: Execution cycle at a certain time interval, such as every 5 seconds, every 1 hours

5.7.2 arithmetic operation & logical operation

5.7.2.1 Introduction of arithmetic operation



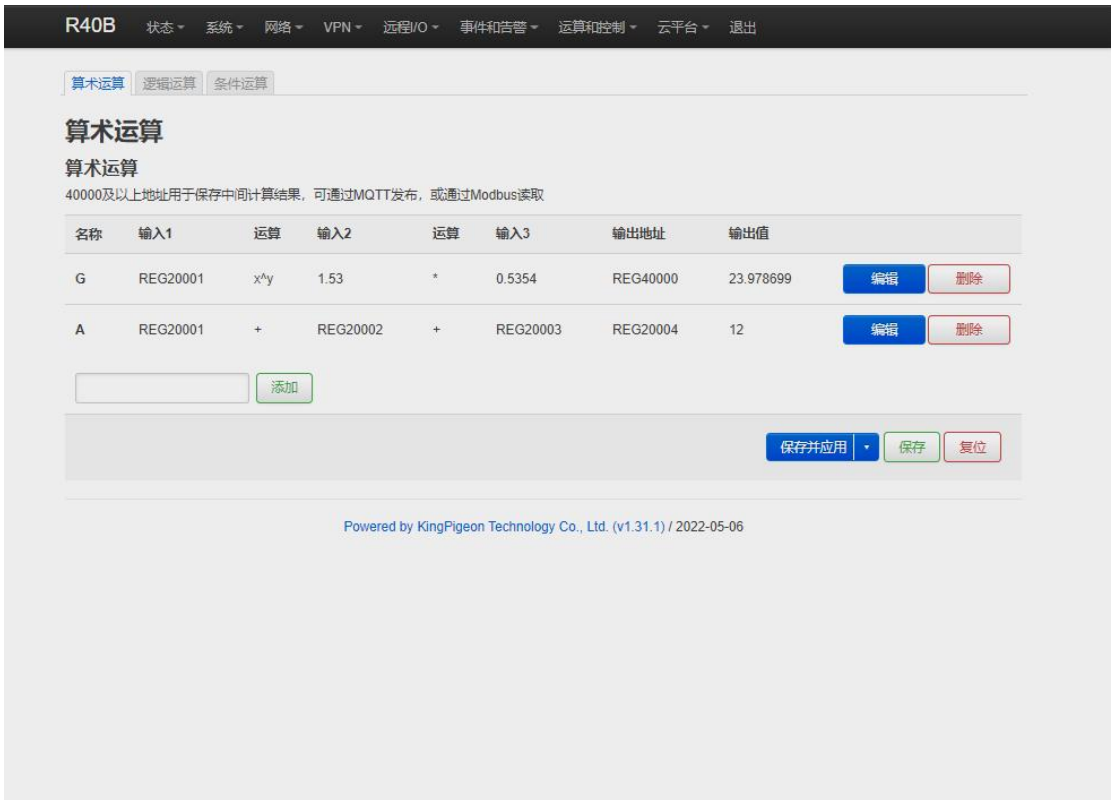


Arithmetic operation supports the "addition, subtraction, multiplication and division" operations between the value type registers of the local device (R40 router) and the Modbus slave device. You can adjust the order of operations at will, "addition, subtraction, multiplication and division" between registers value.

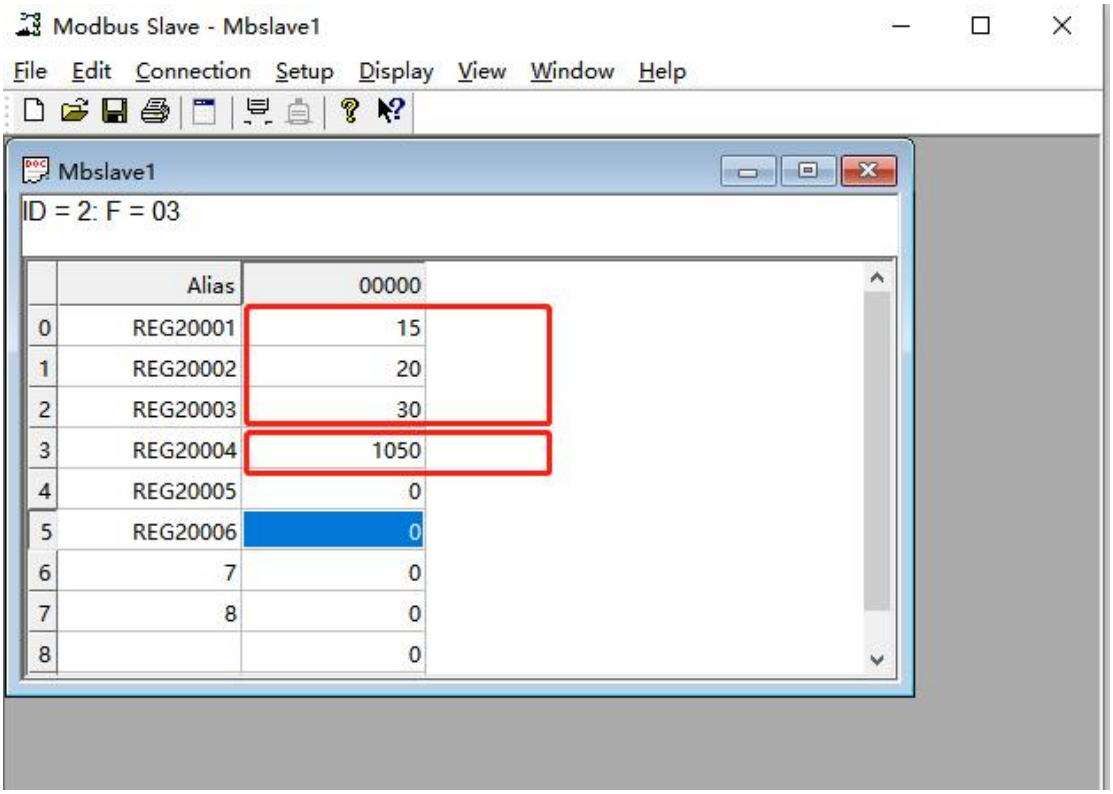
For example:

Slave 2 register REG20001 adds the value of REG20002 multiplied by REG20003, performs arithmetic operation, and outputs the result to REG20004

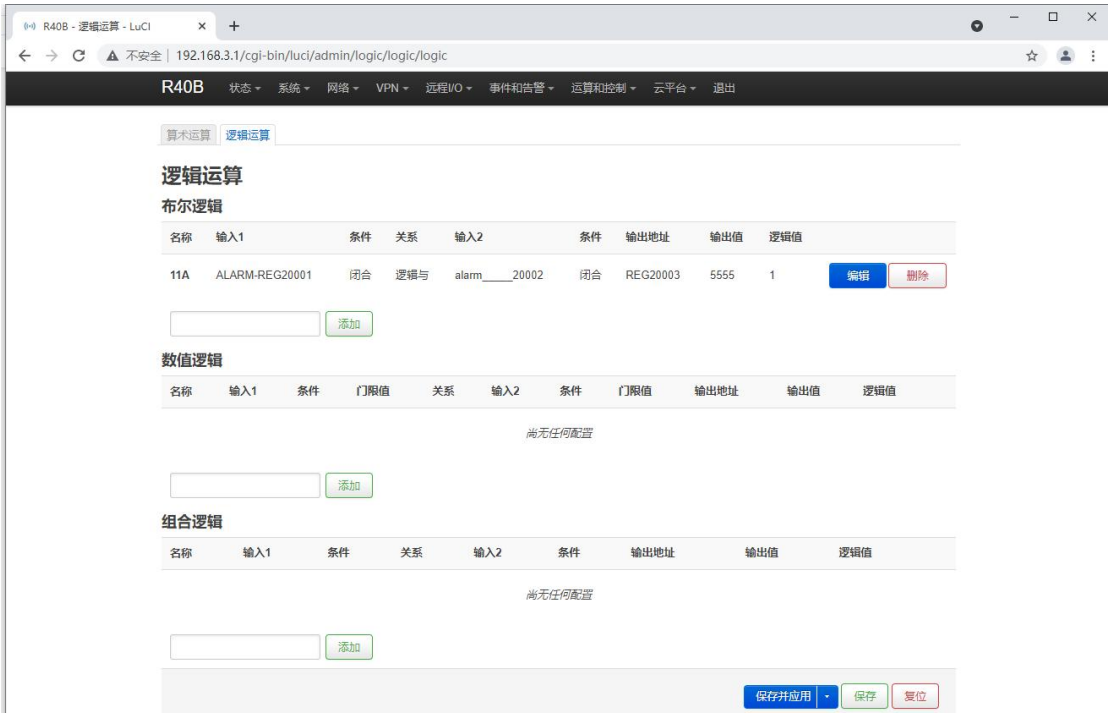
See below:



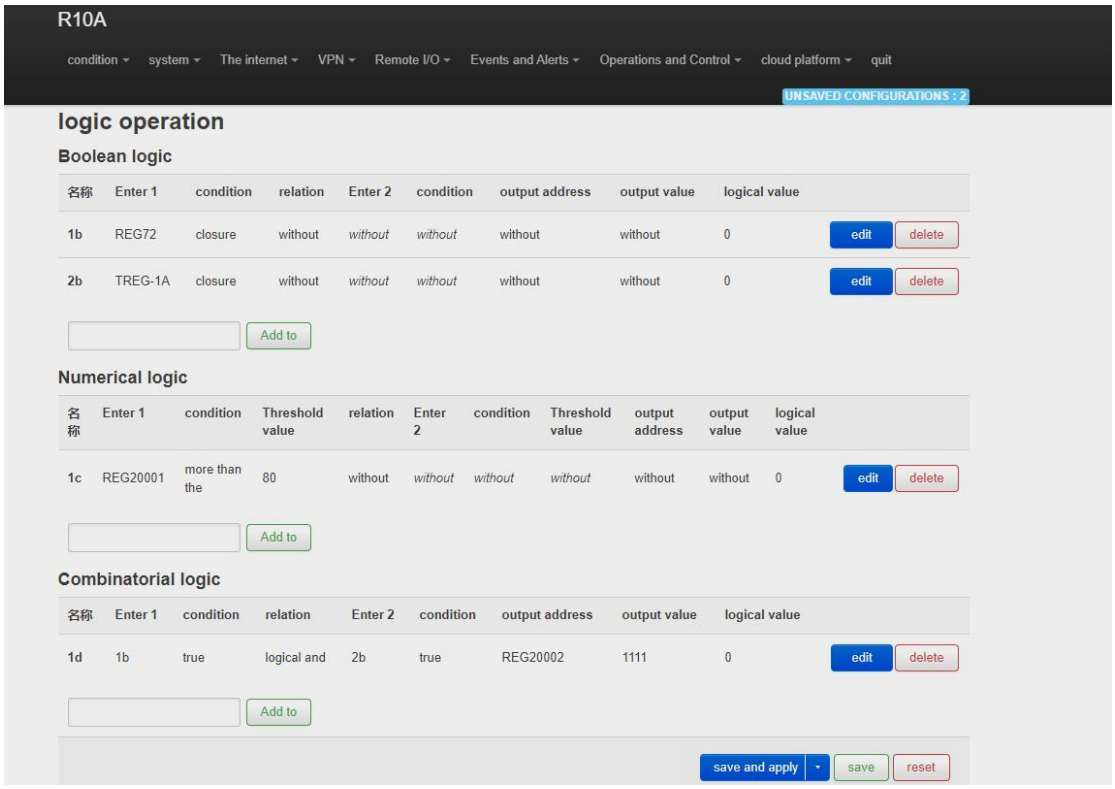
As shown in below, use the virtual serial port tool to simulate the slave 2 register, and the operation result is displayed in SLAVE as follows.

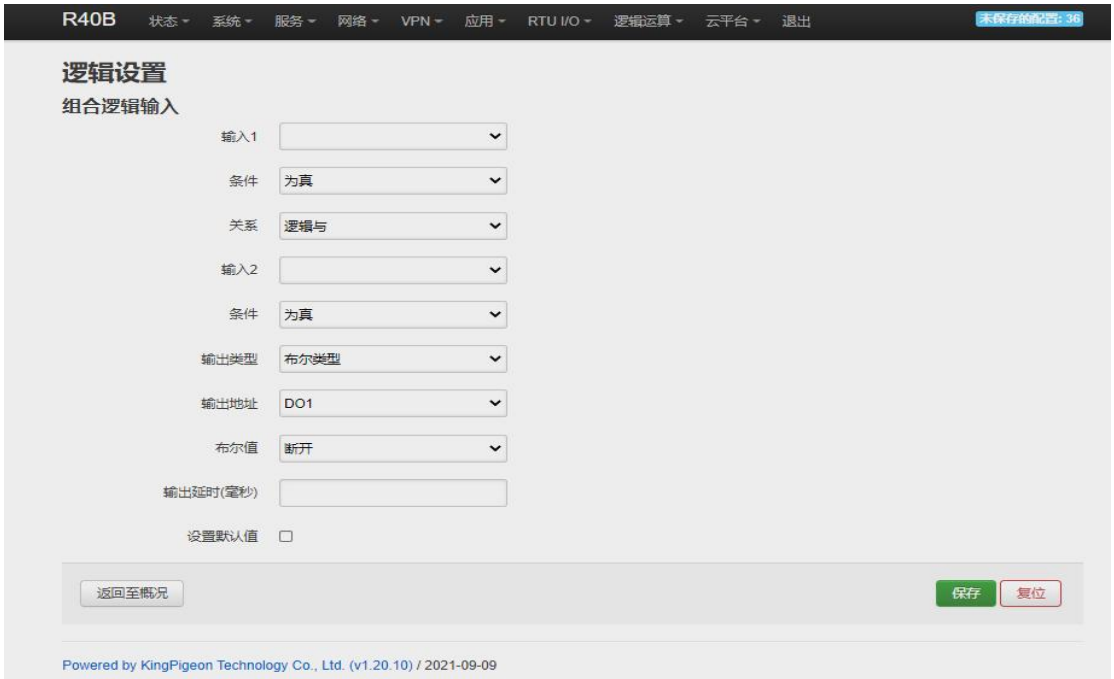


Note: If a 16-bit register address is used as the output result, the fractional part will be output as an integer.



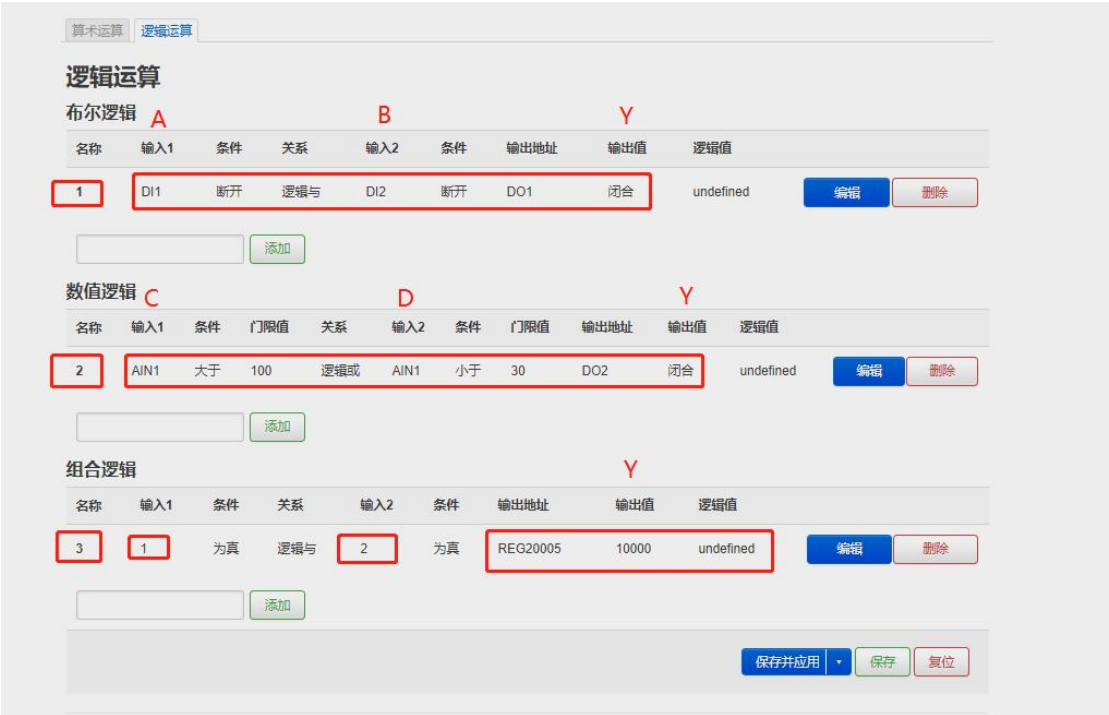
5.7.2.2 Introduction of logical operation





The logical operation function can link the local device I/O (digital input and output, analog input) with the Modbus slave I/O (slave device register), combine them at will as required.

See below picture examples:



Logical operation example (1)

Logic AND: When condition A and condition B are satisfied at the same time, the action is triggered, and then output result Y.

logical operation example (2)

Logical OR: either condition C or condition D is satisfied, the action is triggered and then output result Y.

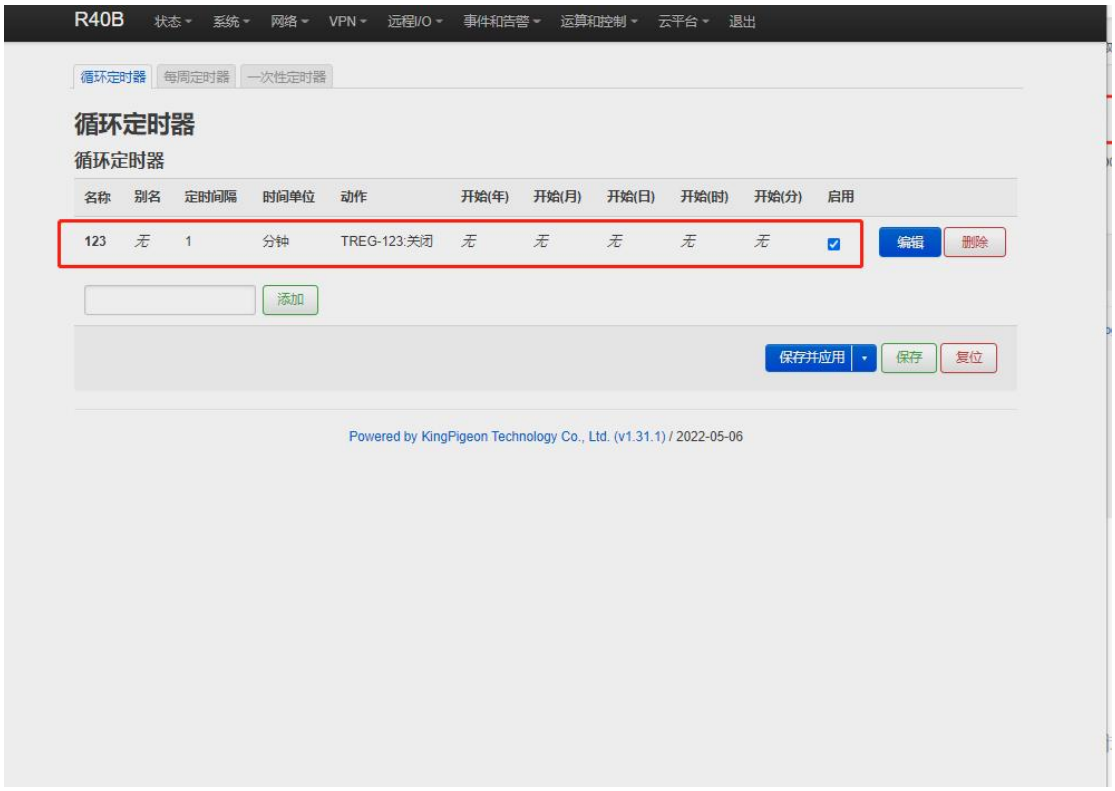
logical operation example (3)

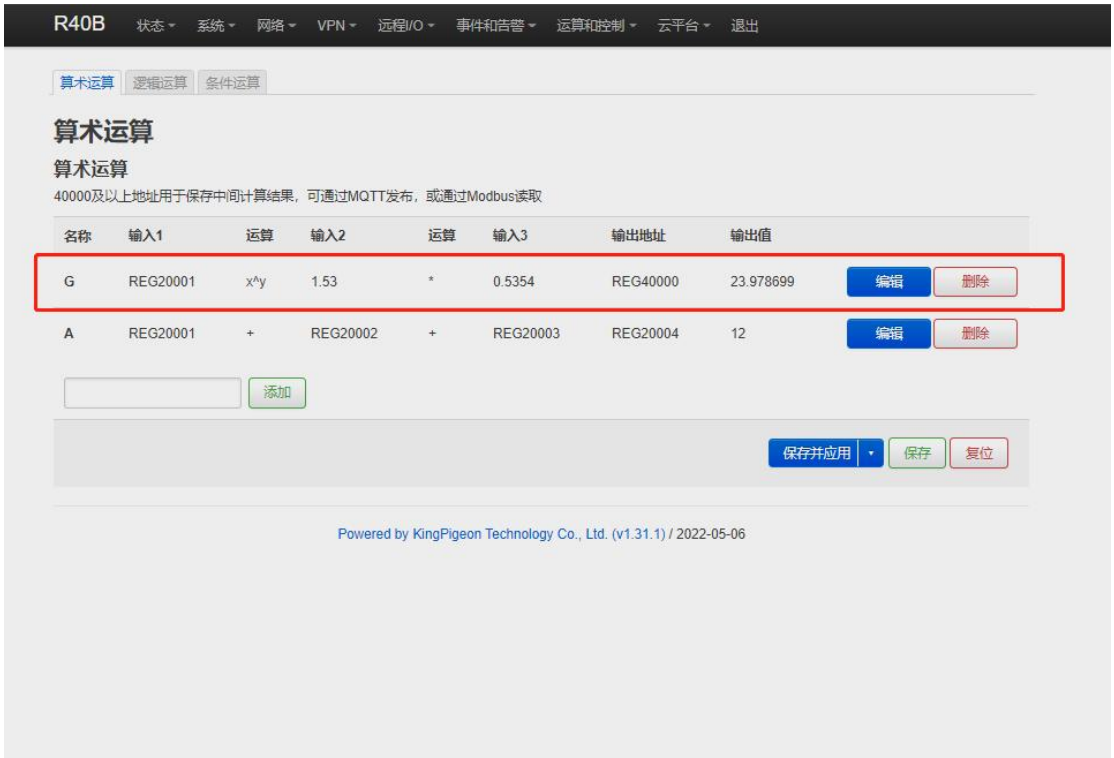
Combined logical operation: the result of the above said logic operation 1 is used as an input value, and the result of logical operation 2 is used as another input value, these two can be combined and comprise logical operation 3.

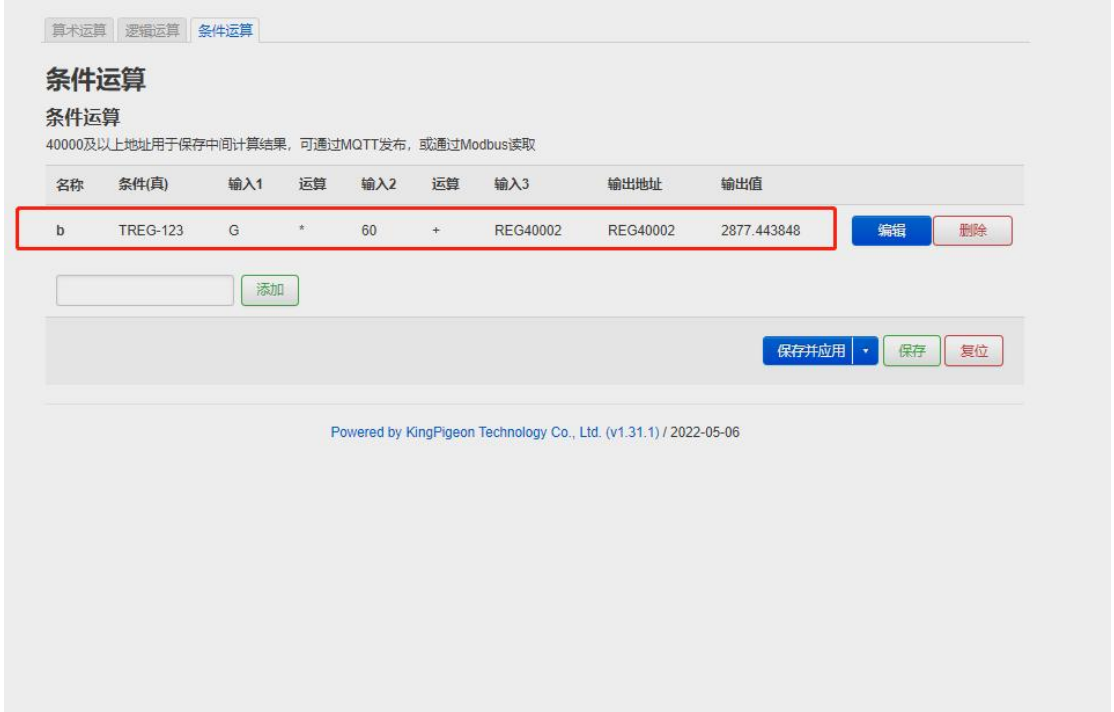
Similarly , you could create more combined logical operations.

5.7.3 Combined conditions operation

Combined conditions operation is an advanced function. It combines timer, arithmetic operation and conditional operation to realize logic control under multiple conditions. it is programmable. You can adjust the combination method, so as to achieve complex task of edge computing and logic control.







Combined conditions operation can perform exponential logarithmic operations. Take a cumulative water flow that is accumulated every 1 minute as an example to create the process as follows:

TREG123: Circular timer acts as an accumulation count trigger.

G: Create water flow per second for the formula

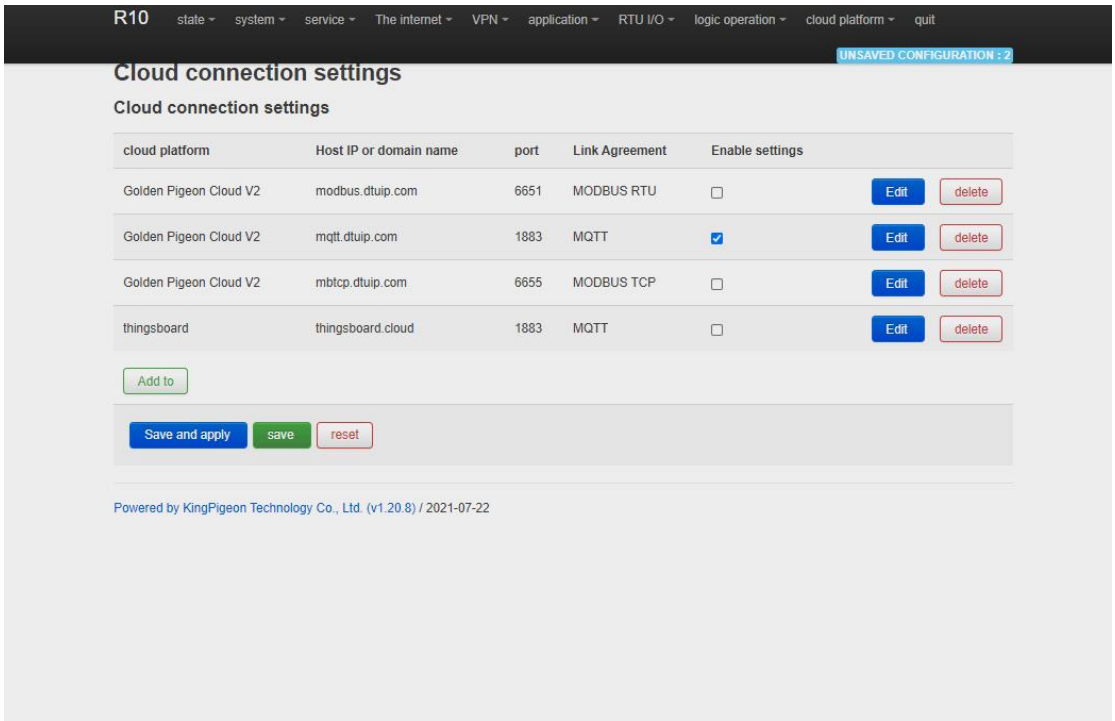
B: TREG123 (condition) and (G operation result per second * 60 seconds per minute) + continuous output result REGXXX

Equal to cumulative output value

5.8 Connection to Cloud Platform

5.8.1 Private cloud (KPIIOT or Custom MQTT cloud)

This router can connect to various private cloud platform, including KingPigeon Cloud Platform KPIIOT V2.0 and V3.0 or other private clouds, for example custom MQTT platform. The configuration is described below, and the setting interface is shown in screenshot.

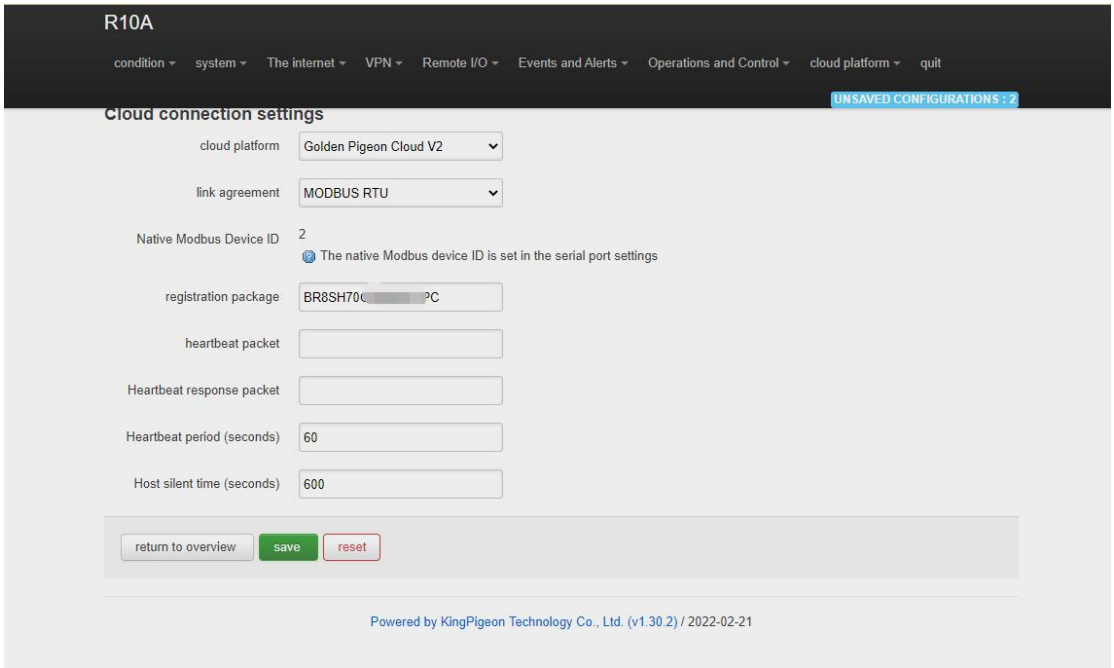


Cloud Connection Settings		
Item		Description
Enable setting		Select to enable
Cloud Platform		King Pigeon KPIIOT V2, KPIIOT V3, other private clouds
Host IP or domain name		Connect Server Port
Port		Connect to other cloud platform server ports
Link Protocol		Modbus RTU,Modbus TCP ,MQTT
Modbu Protocol Parameters	Modbus Device ID	Default is 1
	Register packet	Server register handshake protocol package, contact salesman if need
	Heartbeat packet	Heartbeat content to avoid network offline
	Heartbeat response packet	The server responds to the heartbeat packet
	Heartbeat period（s）	Network keep online heartbeat interval time
	Host Silence time（s）	The server sends silent time without data, and will reconnect if it times out

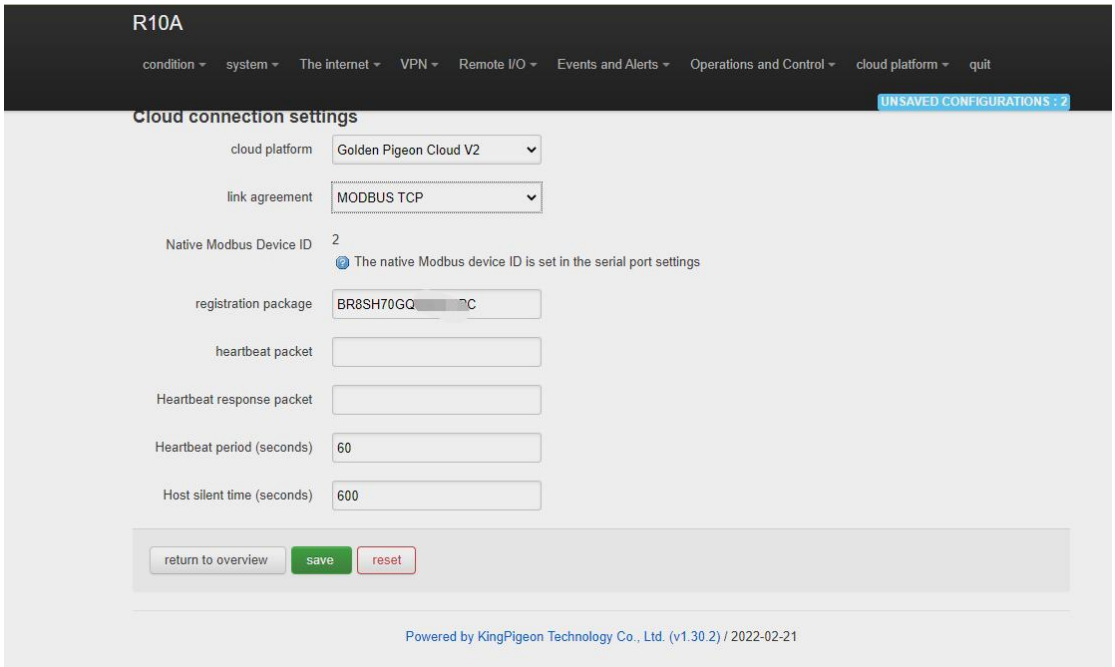
MQTT Protocol Parameters	MQTT Client ID	The client identifier used in the MQTT connection message, the server uses the client identifier to identify the client, and each client connected to the server has a unique client identifier.
	Username	The user name used in the MQTT connection message, which can be used by the server for authentication and authorization.
	Password	The password used in the MQTT connection message, which can be used by the server for authentication and authorization.
	Publish topic	The subject name used in the MQTT publish message. The subject name is used to identify the information channel to which the payload data should be published. The subject name in the publish message cannot contain wildcards.
	Subscribe topic	The topic name used in MQTT subscription messages. After the subscription, the server can send publish messages to the client to achieve control.
	Publish Period (seconds)	MQTT data timing publish interval
	Publisher QOS	Service quality level guarantee for application message distribution: 0-at most once, 1-at least once, 2-only once
	Encryption	Optional not encrypted, encrypted (root certificate), encrypted (self-signed)
	Authentication and authorization (root certificate)	Choose file upload
	Local certificate	Choose file upload
	Local private key	Choose file upload
	Enable data transfer	Enable to work
	Data packing	Send multiple data in one message

5.8.1.1 KingPigeon Cloud Platform (KPIIOT)

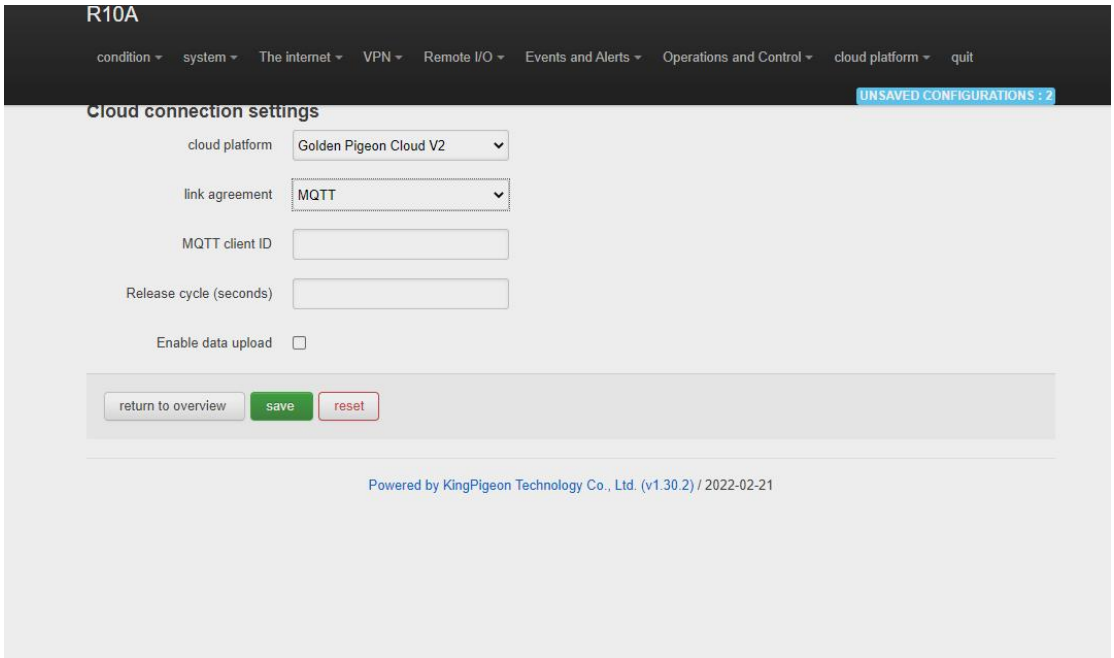
Connection to KingPigeon cloud KPIIOT V2.0 by Modbus RTU protocol, see below setting



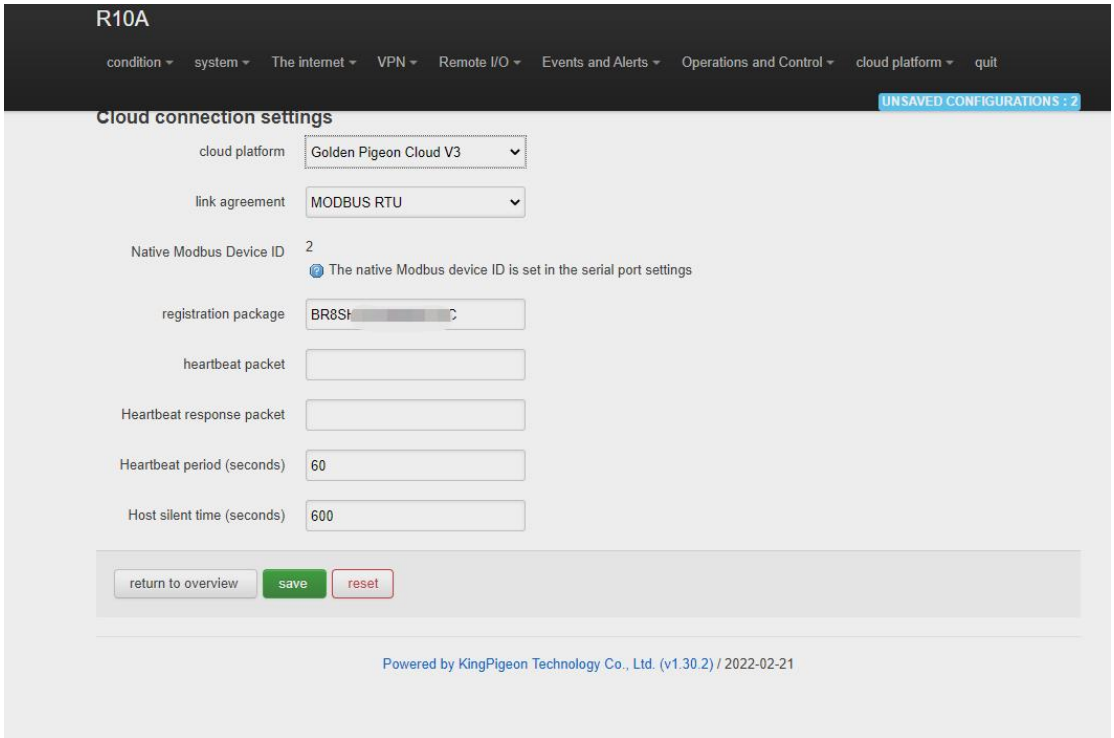
Connection to KingPigeon cloud KPIIOT V2.0 by Modbus TCP protocol, see below setting



Connection to KingPigeon cloud KPIIOT V2.0 by MQTT protocol, see below setting

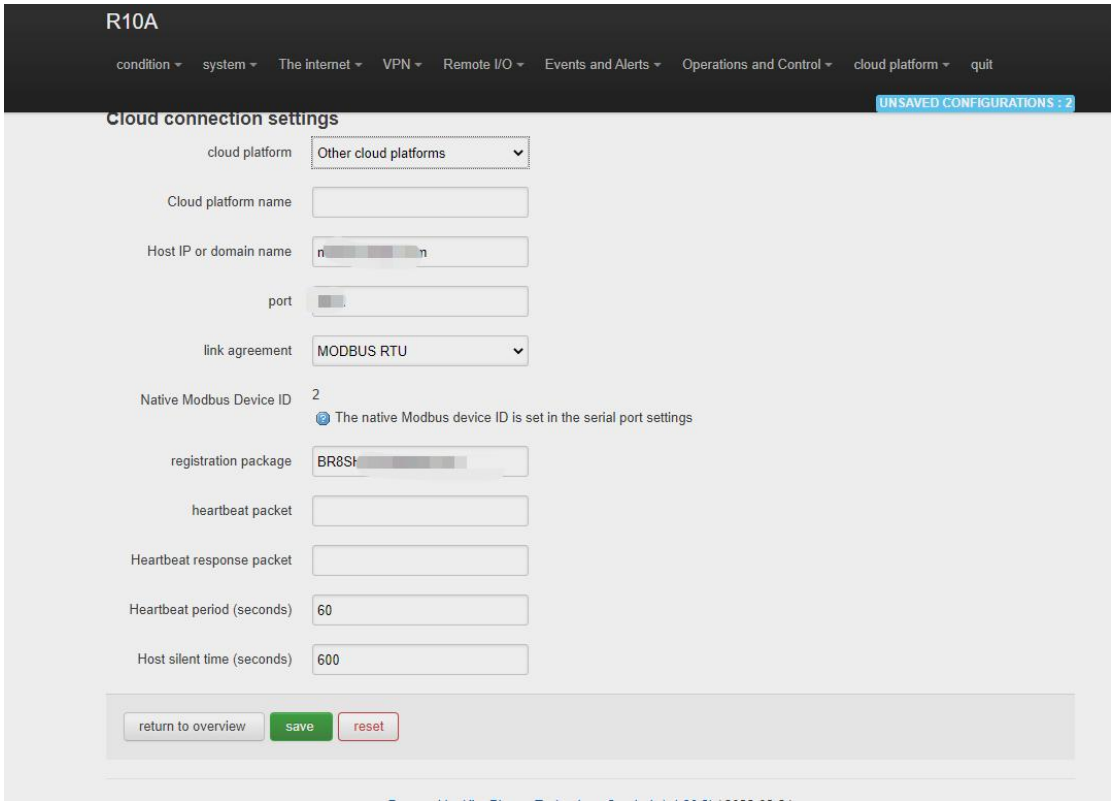


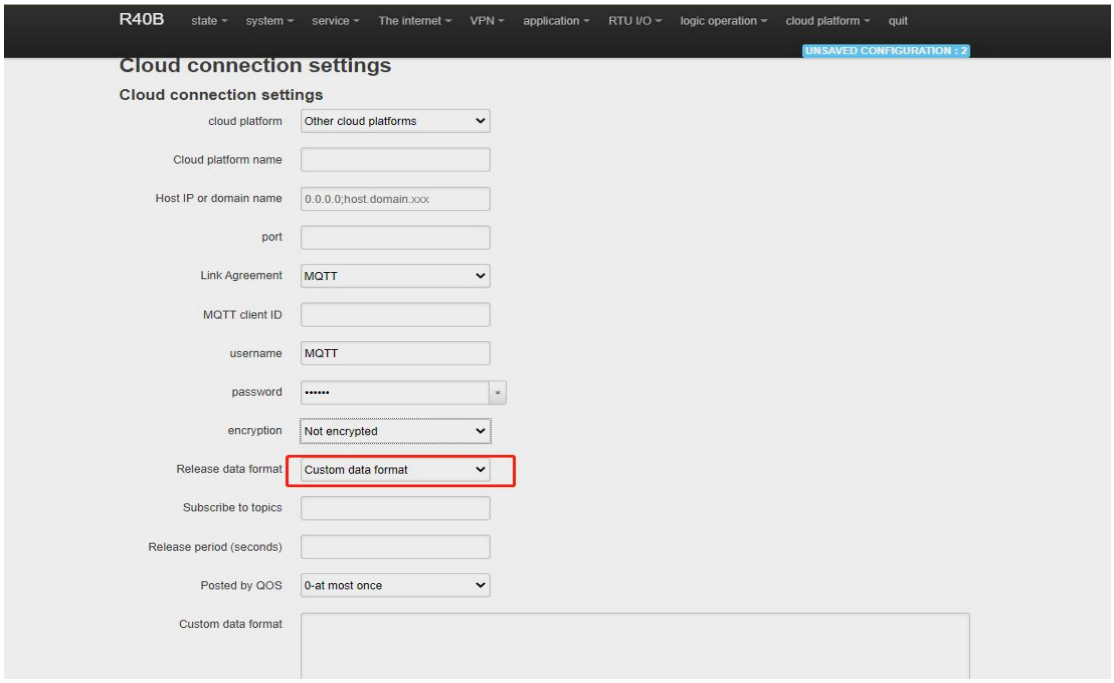
Connection to KingPigeon cloud KPIIOT V3.0 by Modbus RTU protocol, see below setting

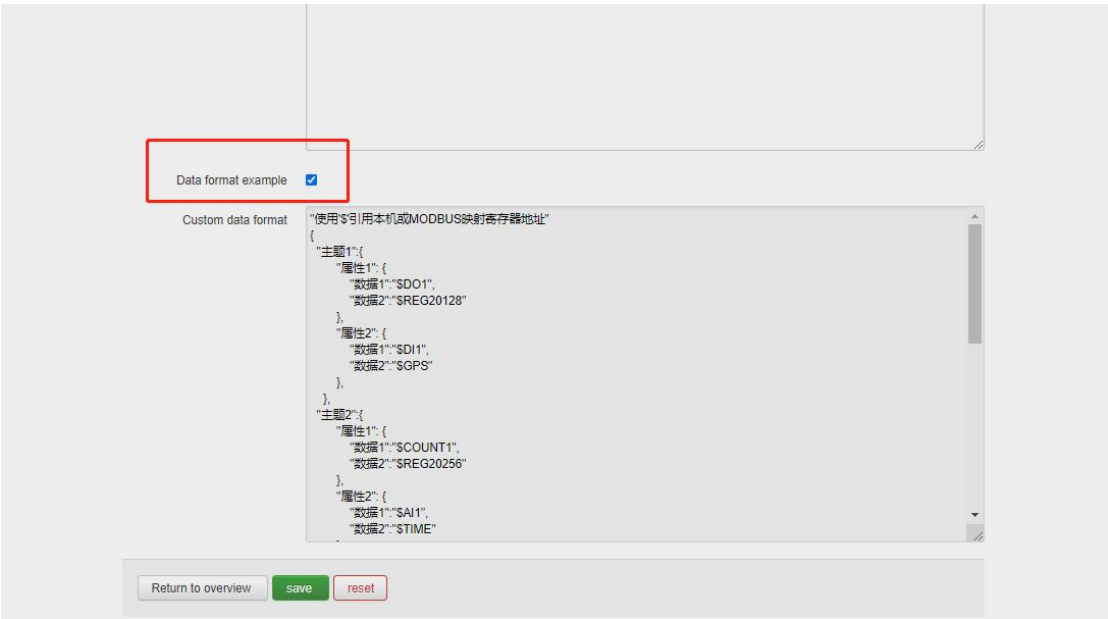


5.8.1.2 Other private cloud --- Custom MQTT

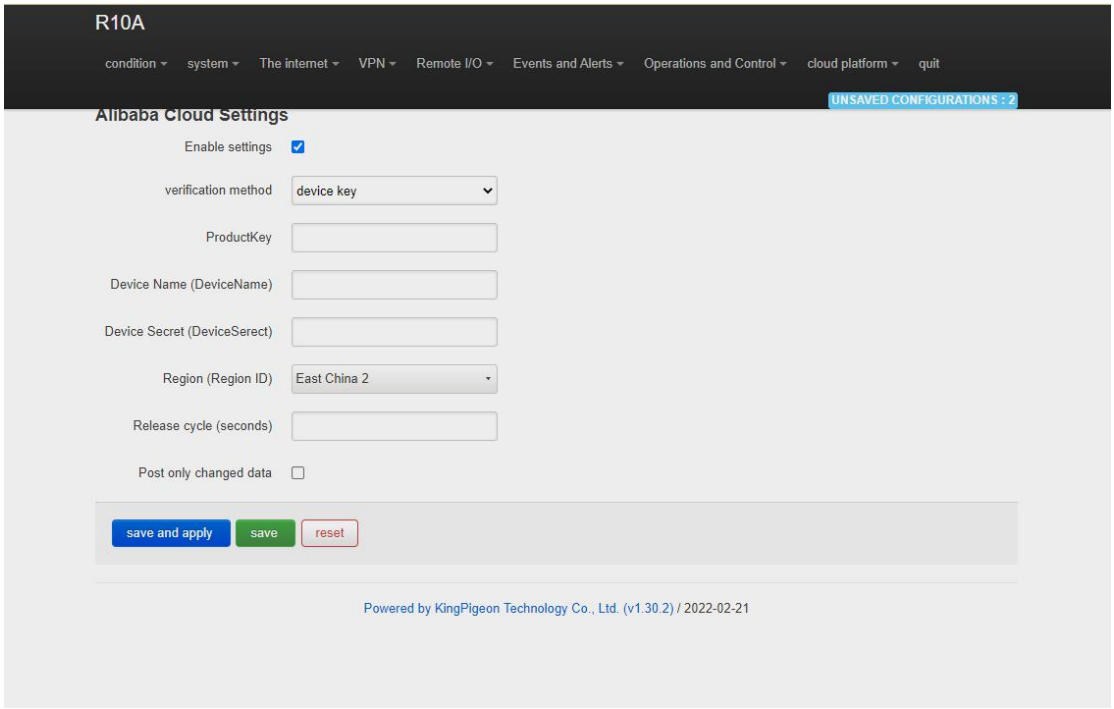
You could also connect to other private cloud platform by custom MQTT data format. See blow setting


R10A
condition
system
The internet
VPN
Remote I/O
Events and Alerts
Operations and Control
cloud platform
quit
UNSAVED CONFIGURATIONS : 2
Cloud connection settings
cloud platform
Other cloud platforms
Cloud platform name
Host IP or domain name
port
link agreement
MODBUS RTU
Native Modbus Device ID
2
The native Modbus device ID is set in the serial port settings
registration package
heartbeat packet
Heartbeat response packet
Heartbeat period (seconds)
60
Host silent time (seconds)
600
return to overview
save
reset


R40B
state
system
service
The internet
VPN
application
RTU I/O
logic operation
cloud platform
quit
UNSAVED CONFIGURATION : 2
Cloud connection settings
Cloud connection settings
cloud platform
Other cloud platforms
Cloud platform name
Host IP or domain name
0.0.0.0;host.domain.xxx
port
Link Agreement
MQTT
MQTT client ID
username
MQTT
password
encryption
Not encrypted
Release data format
Custom data format
Subscribe to topics
Release period (seconds)
Posted by QOS
0-at most once
Custom data format



5.8.2 Alibaba Cloud platform

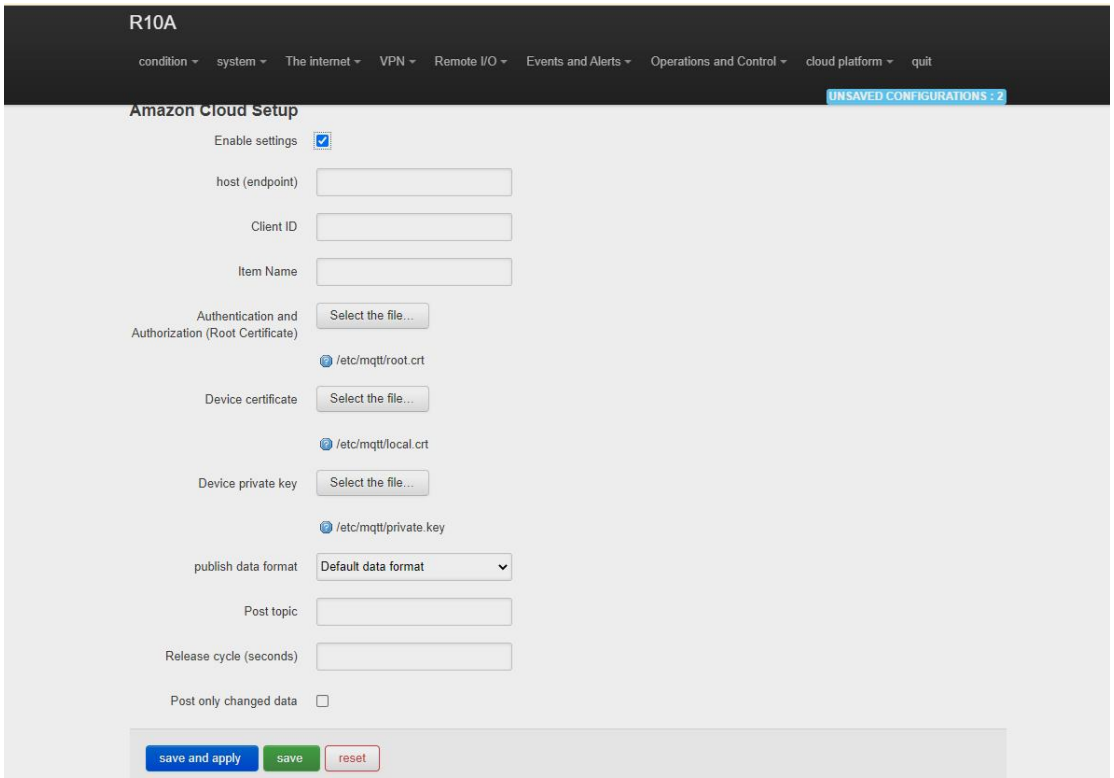


Ali Cloud Connection Settings	
Item	Description
Enable setting	Select to enable
Authentication method	Device secret key, X509 certificate
Product Key	Set the product key on Alibaba Cloud
Device Name	Set the device name on Alibaba Cloud
Device Secret	Set the device key on Alibaba Cloud
Region ID	Ali cloud region

Publish period (seconds)	>60
Certification authority (root certificate)	Choose file upload
Local certificate	Choose file upload
Local key	Choose file upload

Ali cloud device creation certificate creation and details reference Ali Cloud help documentation guide

5.8.3 AWS Cloud



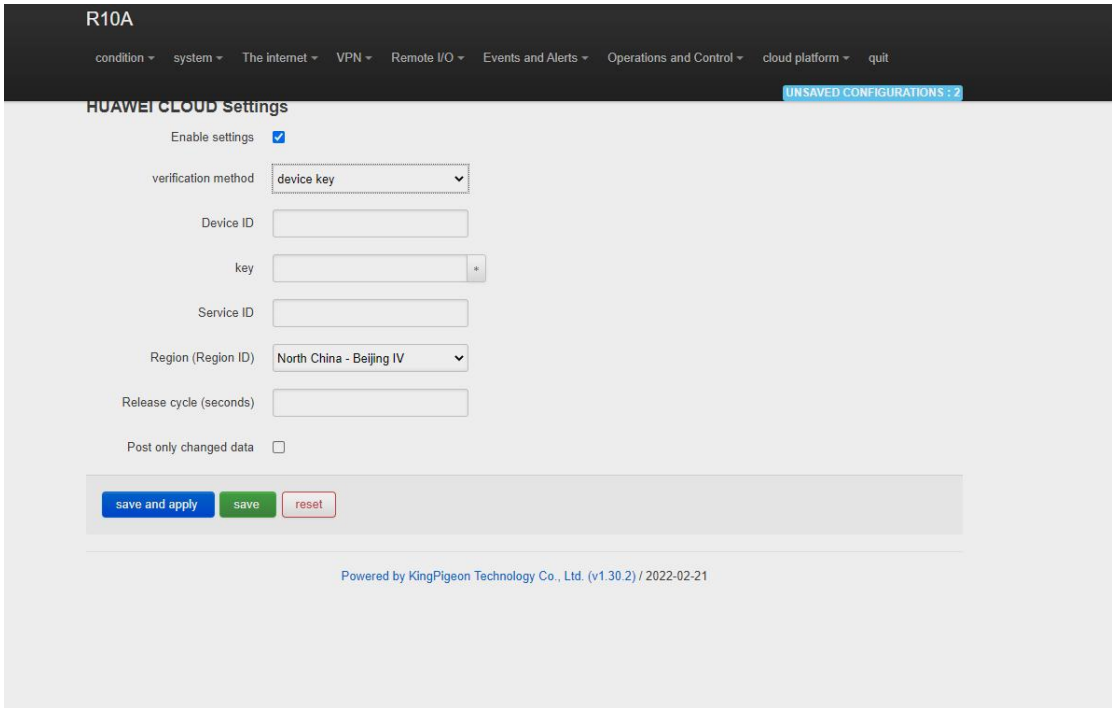
AWS Cloud Connection Settings	
Item	Description
Enable setting	Select to enable
Host（Endpoint）	Set End point
Clint ID	The client identifier used in the MQTT connection message, the server uses the client identifier to identify the client, and each client connected to the server has a unique client identifier.
Item name	Set Item name
Publish topic	The subject name used by MQTT to publish messages. The subject name is used to identify which information channel the payload data should be published to. The

	subject name in the published message cannot contain wildcards.
Publish period (seconds)	>60
Certification authority (root certificate)	Choose file upload
Local certificate	Choose file upload
Local key	Choose file upload

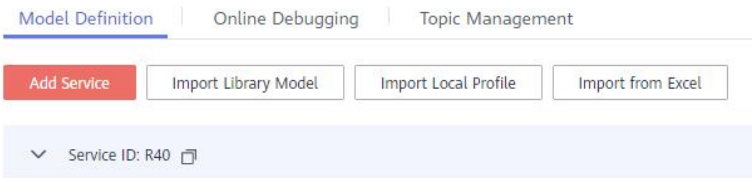
For details about how to create a certificate for an Amazon device, see：Amazon Getting Started documentation tutorial

5.8.4 Huawei cloud

HUAWEI CLOUD supports access to the cloud platform in two ways: device secret key and authentication certificate：

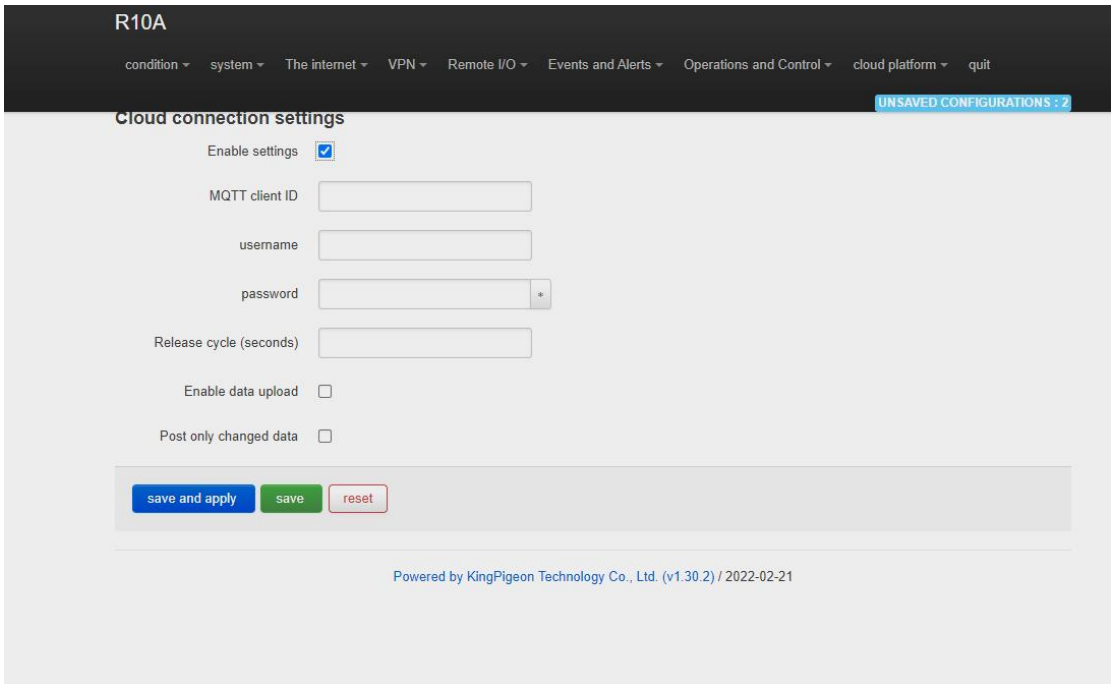


Huawei cloud connection settings	
Item	Description
Enable setting	Select to enable
Authentication method	The device secret key method and the authentication certificate method can be selected, and the authentication certificate method needs to upload the certificate
Device ID	The ID of the device when HUAWEI CLOUD creates the device,

	
Service ID	The product needs to create a service to report data. 
Region ID	The location of the device can be queried on the HUAWEI CLOUD platform
Publish Period（s）	Above 60s
Secret key	For the password entered when creating the device certificate, you can refer to the HUAWEI CLOUD help document to create a test certificate
Certification authority (root certificate)	Root certificate provided by Huawei:rootcert.pem，It's included in the release version, generally don't need to upload
Device certificate	Device certificate deviceCert.pem,Upload to the /etc/conf directory and select the file, you can refer to the HUAWEI CLOUD help document to create a test certificate
Device key	Device key/deviceCert.key,Upload to the /etc/conf directory and select the file, you can refer to the HUAWEI CLOUD help document to create a test certificate

For the steps of creating and registering devices on the platform, please refer to the help documents of Huawei Cloud.

5.8.5 Thingsboard cloud platform



Thingsboard Cloud Connection Settings	
Item	Description
Enable setting	Select to enable
Host（Endpoint）	Set End point
Clint ID	The client identifier used in the MQTT connection message, the server uses the client identifier to identify the client, and each client connected to the server has a unique client identifier.
Item name	Set Item name
Publish topic	The subject name used by MQTT to publish messages. The subject name is used to identify which information channel the payload data should be published to. The subject name in the published message cannot contain wildcards.
Publish period (seconds)	>60
Certification authority (root certificate)	Choose file upload
Local certificate	Choose file upload
Local key	Choose file upload
Enable data transfer	click to enable this function
Only release changed data	click to enable this function

For thingsboard cloud device user manual, please refer to the

Thingsboard Getting Started document

5.9 Logout

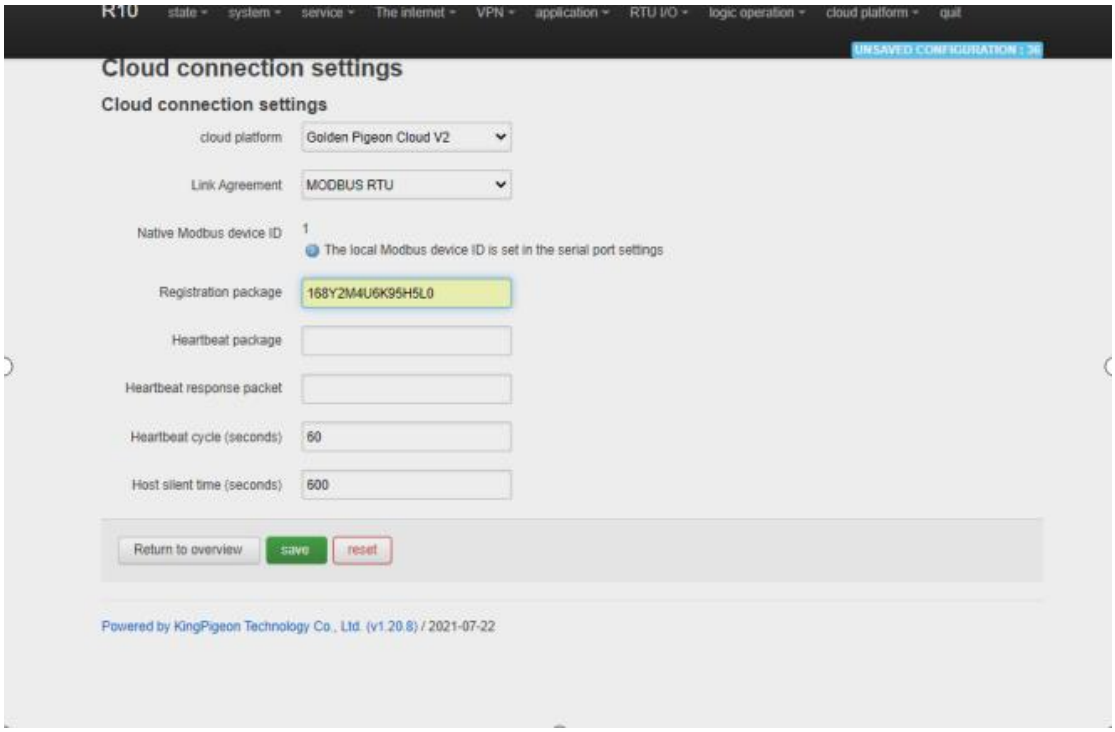
After the router parameter configuration is complete, click "Logout", the device will log out and return to the login web configuration page.

6. Communication Protocol

The device supports Modbus RTU protocol, Modbus TCP protocol and MQTT protocol. For specific communication protocol, please refer to relevant materials. The following introduces the application of Modbus RTU and MQTT protocol on the device.
Modbus TCP and RTU protocol are very similar, as long as an MBAP header is added to the RTU protocol, and the two byte CRC check code of the RTU protocol can be removed.

6.1 Modbus RTU Protocol

6.1.1 Platform connection setting



1. Set the platform server IP and port, select Modbus RTU protocol and set the local Modbus device ID (the effective range of Modbus device ID is 1~247)
2. Set relevant message information according to the platform to be connected (if not, you can not set it)

[Register Package]: The registration package sent by the device to the server when connected to the server. *This is required when you connect KPIIOT, please contact sales to get it if you need.
[Heartbeat Packet]: A heartbeat packet sent by the device to the server to maintain the connection.
[Heartbeat Response Packet]: The server responds to the heartbeat packet

[Heartbeat period]: The heartbeat packet sending period.
[Host Silent Time]: Silent time when no data is sent from server, timeout will reconnect.

6.1.2 Read Mapping Address

6.1.2.1 Mapping Register Address

1) Boolean Slave Mapping Register Address, holding coil type, input coil type (Function Code 01/02/05/15)

Modbus Register Address(Decimal)	PLC or configuration address (Decimal)	Data Name	Data Type	Description
64	00065 or 10065	Bool 64	Bool	Boolean type, Slave mapping address, can map the slave input coil and holding coil state, 193 addresses in total.
65	00066 or 10066	Bool 65	Bool	
66	00067 or 10067	Bool 66	Bool	
…	…	…	Bool	
…	…	…	Bool	
256	00257or 10257	Bool 256	Bool	

2) 16 Bit Slave Mapping Register Address, holding type, input type (Function Code 03/04/06/16)

Read and Write Holding Register (Function Code 03,04, 06, 16)				
Modbus Register Address(Decimal)	**PLC or configuration address (Decimal)**	**Data name**	**Data Type**	**Description**
20001	420002 or 320002	16 Bit data 20001	Data type according to slave mapping data type	Can map the slave input register and holding register, 64 addresses in total
20002	420003 or 320003	16 Bit data 20002	Same as above	Same as above

20003	420004 or 320004	16 Bit data 20003	Same as above	Same as above
…….	127 data similar as above	…….	Same as above	Same as above
20127	420128 or 320128	16 Bit data 20127	Same as above	Same as above

3) 32 Bit Slave Mapping Register Address, holding type, input type (Function Code 03/04/06/16)

Holding Register and input Register(Function Code 03,04, 06, 16)				
Modbus Register Address(Decimal)	**PLC or configuration address (Decimal)**	**Data name**	**Data Type**	**Description**
20128	420129 or 320129	32 Bit data 20128	Data type according to slave mapping data type	Can map the slave input register and holding register, 64 addresses in total
20130	420131 or 320131	32 Bit data 20130	Same as above	Same as above
20132	420133 or 320133	32 Bit data 20132	Same as above	Same as above
…….	64 data similar as above	…….	Same as above	Same as above
20254	420255 or 320255	32 Bit data 20254	Same as above	Same as above

6.1.2.2 Read Boolean Mapping Address Data

Master Send Data Format：

Content	Bytes	Data	Description
Device ID	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read holding coil type, function code 01
Boolean Register Starting Address	2	00 40H	Range: 0040H-0100H, address refer to [" Mapping Register Address”]
Read Register Qty	2	00 0AH	Range： 0001H-00C1H, 193 address total
16 CRC Verify	2	BD D9H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data	Description
Device ID	1	01H	01H Device, according to data sent by master

Function Code	1	01H	Read holding coil type
Return Data Length	1	02H	Return data length
Returning Data	2	73 01H	
16 CRC Verify	2	5D 0CH	CRC0 CRC1 low byte in front, high behind

Example: Start from address 64,read 10 Boolean mapping data value, then:

Server send: 01 01 00 40 00 0A BD D9

01= Device ID; 01 = Read holding coil; 00 40 = Read Boolean data start from address 64; 00 0A = Serial to read 10 Boolean status; BD D9 CRC Verify.

Device answer: 01 01 02 73 01 5D 0C

01= Device ID; 01 = Read holding coil; 02= Return Data byte; 73 01= Return 10 Boolean status. High byte stands for low address data, low address stands for high address. According to Modbus protocol, fix 73 01H real value to be 01 73H, converter to Binary as below:

Register mapping address	Invalid	Invalid	Invalid	Invalid	Invalid	Invalid	73	72
Value	0	0	0	0	0	0	0	1
Register mapping address	71	70	69	68	67	66	65	64
Value	0	1	1	1	0	0	1	1

The address value higher than 10 digits will be seen as invalid.

5D 0C CRC Verify.

6.1.2.3 Modify Boolean Mapping Address Data

If you want to control the holding coil state of the access slave, you must configure the add slave 01 function code instruction mapping. After the mapping address value is changed, the corresponding slave address data will be written.

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	05H	Write single holding coil, function code 05H
Boolean Mapping Register Address	2	00 40H	Range: 00 40H-0100FH, address refer to ["**Mapping Register Address**"]
Write value	2	FF 00H	This value: FF 00H or 00 00H, FF 00H stands for write 1; 00 00H stands for write 0
16 CRC Verify	2	8D EEH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	05H	Write single holding coil
Boolean Mapping Register Address	2	00 40H	Range: 00 40H-0100FH, address refer to ["**Mapping Register Address**"]
Write value	2	FF 00H	This value: FF 00H or 00 00H. FF 00H stands for write 1,00 00H stands for write 0.
16 CRC Verify	2	8D EEH	CRC0 CRC1 low byte in front, high behind

Example: Modify Boolean mapping address 64 status, modify to 1, then:

Server send: 01 05 00 40 FF 00 8D EE

01= Device address; 05= Write boolean value; 00 40=The mapping address which need to revise;

FF 00 = Write 1; 8D EE CRC Verify.

Device answer: 01 05 00 40 FF 00 8D EE

01= Device address; 05= Write boolean value; 00 40= The mapping address which need to write;

FF 00= Write 1; 8D EE CRC Verify.

If need multiple modify, please check function 15 of Modbus protocol.

6.1.2.4 Read Data Type Mapping Address Data

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	03H	Read holding register, function code 03
Mapping Register Starting Address	2	4E 20H	The starting address of the mapped data type, and the corresponding address refer to **["Slave Mapping Register Address"]**
Read Mapping Register Qty	2	00 0AH	Read input register qty.
16 CRC Verify	2	82 EFH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description

Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	03H	Read holding register
Range Data Bytes	1	14H	
Returning Data	20	00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2AH	Returning Data
16 CRC Verify	2	FB 34H	CRC0 CRC1 low byte in front, high behind

Example: Mapping address start from 20001, read 10 address data, then:

Server send: 01 03 4E 21 00 0A 82 EF

01= Device address; 03= Read holding register ; 4E 21=Mapping register starting address, current is Decimal data 20001; 00 0A = Read 10 register value; 82 EF=16 CRC Verify.

Device answer: 01 03 14 00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2A FB 34

01= Device address; 03= Read holding register; 14= Returning 20 byte; 00 14 00 1E 00 28 00 32 00 4B 00 41 00 0A 00 25 00 14 00 2A = Returning data.

Register Mapping Address	20010	20009	20008	20007	20006	20005	20004	20003	20002	20001
Value	00 2A	00 14	00 25	00 0A	00 41	00 4B	00 32	00 28	00 1E	00 14

FB 34=16 CRC Verify.

6.1.2.5 Modify Data Type Mapping Address Data

If you want to rewrite slave data, you must configure the add slave 03 function code instruction mapping. After the mapping address value is changed, the corresponding slave address data will be rewritten. If address 20001 mapping slave data type is Signed Int, sort AB.

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	06H	Write single holding register, function code 06
Mapping Register Address	2	4E 21H	Mapping data type address range, refer to **["Slave Mapping Register Address"]**
Write Data	2	00 64H	Data writing value is Decimal data 100
16 CRC Verify	2	CF 03H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	06H	Write single holding register

Mapping Register Address	2	4E 21H	Mapping data type
Write Data	2	00 64H	Write 100 successfully
16 CRC Verify	2	CF 03H	CRC0 CRC1 low byte in front, high behind

Example: If address 20001 mapping slave data type is Signed Int, sort AB, modify mapping address 20001 register to 100, then:

Server send: 01 06 4E 21 00 64 CF 03

01= Device address; 06= Modify single holding register value; 4E 20=Modify address 20001 register value; 00 64 = Write Decimal value 100; CF 03=16 CRC Verify.

Device answer: 01 06 4E 20 00 64 CF 03

01= Device address; 06= Modify single holding register value; 4E 20= R Modify address 20001 register value; 00 64= Modify to Decimal value 100, CE 03=16 CRC Verify.

If need to modify multiple data type mapping address, pls check function code 16 in Modbus protocol.

6.2 MQTT Protocol

MQTT is a client-server based message publish/subscribe transport protocol. The MQTT protocol is lightweight, simple, open, and easy to implement, and these features make it very versatile. In many cases, including restricted environments such as machine to machine (M2M) communication and the Internet of Things (IoT). It is widely used in satellite link communication sensors, occasionally dialed medical devices, smart homes, and some miniaturized devices. The MQTT protocol runs on TCP/IP or other network protocols, providing ordered, lossless, two-way connectivity.

6.2.1 MQTT Introduction

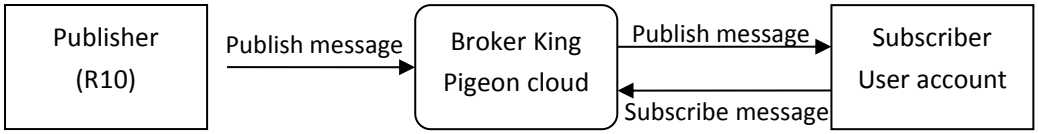
MQTT is a client-server based message publish/subscribe transport protocol. The MQTT protocol is lightweight, simple, open, and easy to implement, and these features make it very versatile. In many cases, including restricted environments such as machine to machine (M2M) communication and the Internet of Things (IoT). It is widely used in satellite link communication sensors, occasionally dialed medical devices, smart homes, and some miniaturized devices. The MQTT protocol runs on TCP/IP or other network protocols, providing ordered, lossless, two-way connectivity.

6.2.2 MQTT Principle

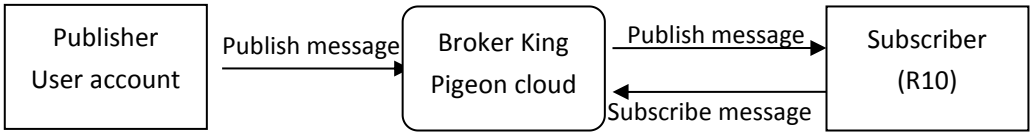
There are three identities in the MQTT protocol: Publisher (Publish), Broker (Server), Subscriber (Subscribe). Among them, the publisher and subscriber of the message are both clients, the message broker is the server, and the message publisher can be the subscriber at the same time.

Devices use MQTT communication through only two steps.
1.Devices publish the Topic through broker;

2. Users can create a account on broker to subscribe to the device to achieve monitoring



(uploads data to Broker)



(The R10 receives the downlink message from the Broker to implement control of the R10)

6.2.3 Device Communication Application

Client configuration

1. Connect Platform: KPIIOT cloud platform 2.0 or other cloud platform to enter the corresponding IP and port.
2. Connection protocol: MQTT protocol.
3. MQTT client ID: the unique identification of the device, which can be a serial number, device ID, or IMEI code; (King Pigeon 2.0 device ID defaults is the serial number).
4. MQTT account: the account where the device publishes the theme on the proxy server (King Pigeon 2.0 defaults is MQTT).
5. MQTT password: the device's account password for publishing the theme on the proxy server (King Pigeon 2.0 defaults is MQTTPW).
6. Publish topic: refers to the topic of the device publishing uplink data to the platform, King Pigeon Cloud 2.0 is the cloud service ID / +.
7. Subscription topic: refers to the topic that the device subscribes to when receiving downlink data, King Pigeon Cloud 2.0 is the cloud platform serial number/+.
8.Release cycle (seconds): MQTT data release interval, in seconds. The King Pigeon Cloud 2.0 cycle needs to be set to 10 seconds or more. If it is less than 10 seconds, the platform will disable the device.
9. Publisher QOS: The service quality level guarantee for application message distribution, 0-at most once, 1-at least once, 2-only once, you can choose according to your needs.
10. Encryption: You can use encryption to connect to the server according to your needs, and you can choose not to encrypt when you connect to King Pigeon Cloud 2.0. non-encrypted
11. Enable data re-transmission: Check enable, after enabling, when reconnecting to the

cloud platform, the data during the offline period will be re-transmitted.
12. Data packing: After checking, send multiple data in one message, when unchecked, one message corresponds to one I/O data point.

After the configuration is complete, the client will initiate a connection to the server:
CONNECT: The client sends a CONNECT connection message request to the server;
CONNACK: The server responds with a CONNACK confirmation connection message, indicating that the connection is successful;
After the client establishes a connection, it is a long connection, and the client can publish or subscribe to the message on the server;
For example the device and the client's mobile phone as the client:
After the device publishes the topic on the proxy server, customers can view the data through subscription. That is, the device is the publisher and the customer's mobile phone is the subscriber.

Users can also publish topics through the MQTT server to control the device. That is, the user is the publisher and the device is the subscriber.

6.2.4 Publish MQTT Format

If data packing is selected during configuration, multiple I/O data points will be sent in one message (when there are many data points, multiple messages will be sent separately, and each message contains multiple data points), if not selected, one message only corresponds to one I/O data point, please noted the two publishing formats are slightly different.

(1)Following is the device communication data format(Data packing):

Publish Topic Name：serial numbers // Corresponding configured topic options

```
{
"sensorDatas":
  [
      {
      // switch type,
      "switcher":"1",                    // Data type and value
      "flag":"DI1"                       //Read and write Flag
      },
      {
      // Slave switch type
      "switcher":"0",                    // Data type and value
      "flag":"REG64"                     //Read and write Flag
      },
      {
        //value
      "value":"10.00",
      "flag":"AI1"
      },
    {
```

```
        //Slave value
        "value":"217.5",
        "flag":"REG2001"
        },
      {
        //Positioning
        "lng":"116.3",                    // longitude data
        "lat":"39.9",                     // latitude data
        "spd":"0.0",                      // speed data
      "dir":"0.0",                        // direction data
        "flag":"GPS"
        }
    ],
  "time":"1602324850"          //Time , data release timestamp UTC format
        "retransmit":"enable"
    //Retransmission flag, indicating historical data (retransmission historical data only has this flag, real-time data does not have this flag)
  }
```

Note:

Each I/O point must contain three types of information when the device publish message: add Time, data type and value, read and write flag;

/ / Data type and value: according to the type is divided into the following:

1. The numeric character is "value" followed by: "data value".
2. The switch character is "switcher" followed by: "0"or"1" (0 is close,1 is open).
3. Positioning data :

   The GPS longitude character is "lng" and the value is: "data value".

   The GPS latitude character is "lat" and the value is: "data value".

   The GPS speed character is "spd" and the value is: "data value".

   The GPS direction character is "dir" and the value is: "data value".

Read and write Flag:

Each I/O port has a fixed flag when the device publish a message, The specific flags are as follows:

Device own I/O Port

Data name	Flag	Data type	Description
Digital output	DO1,DO2	Switcher	0 is open,1 is close
Digital input	DI1,DI2	Switcher	0 is open,1 is close
Analog input	AI1,AIN2,AIN3,AIN4	Value	The actual value = original value
Network failure	DI3~DI22	Switcher	0 is offline,1 is online
Pulse count	COUNT1,COUNT2	Value	

Extend I/O Port

Data name	Flag	Data type	Description
Boolean	REG64~256	Switcher	Defined according to slave data
16 Bit	REG20000~20127	Value	Defined according to slave data
32 Bit	REG20128~20254	Value	Defined according to slave data

Note:

//Time flag: the character is "time", followed by "specific reporting timestamp"

//Re-transmission flag: the character is "Re-transmit", followed by "enable"

The data collected during the network offline period will be temporarily stored in the device, and will be republished when the network is restored. It is identified by the "Re-transmit" field to indicate historical data. (Need to check the enable data transmission on the configuration interface)

(2) The payload data format in the device release message (data unpacking)

Publish Topic：serial numbers

```
{
        "switcher": "0",
        "flag": "DI1",
        "time": "1602324850"
}
```

Note: When the data is unpacking, there is a little difference except for the format. The others are exactly the same. This is an example of DI1. For other data types, please refer to the above description.

6.2.5 Device Subscribe MQTT Format

The payload data format in the device subscription message

Subscription format:serial number /+ (subscription topic needs to add the wildcard "/+" after the serial number)

```
{
    "sensorDatas":
   [
     {
        "sensorsId": 211267,          // cloud platform sensor ID
        "switcher":1,                  // switch type data, 0 is off, 1 is closed
        "flag":"DO1"                  //read write flag
      }
   ],
        "down":"down"                  // platform downlink message
}
```

Note:

The data sent by the device control must contain three types of information: sensor ID, data type,flag, and downlink message packet.

//Sensor ID: The character is "sensorsID", and the ID is automatically generated according to the platform definition.

/ / Data type and value: according to the type is divided into the following:

1. The switch character is " switcher " followed by: "0"or "1",0 is open,1 is close.
2. The numeric character is " value " followed by: "data value"

/ /Read write flag: the character is "flag" followed by "flag"

// "down" confirmation data sent to subscribers by the platform.

7. SMS Command List

This device supports remote query and control operations through SMS commands.The following are the precautions:

1. The default password is 1234, you can edit the SMS command to modify the password;
2. The "password" in the SMS command refers to the device password, such as 1234, just enter the password directly;
3. The "+" sign in the SMS command is not used as the content of the SMS, please do not add any spaces or other characters;
4. The SMS command must be CAPITAL LETTERS, such as "PWD" instead of "pwd";
5. If the password is correct but the command is incorrect, the device will return: SMS Format Error, Please check Caps Lock in Command! So please check the Command, or add the country code before the telephone number or check the input is in ENGLISH INPUT METHOD and CAPS LOCK. If password incorrect then will not any response SMS.
6. If the password is entered incorrectly, no information will be returned;
7. Once the Unit received the SMS Command, will return SMS to confirmation, if no SMS return, please check your command or resend again.

1) *Modify Password, 4 digits, default is 1234*

SMS Command	Return SMS Content
Old Password＋P＋New Password	Password reset complete

2) *Inquiry Current Status SMS Command*

SMS Command	Return SMS Content
password+EE	Model:xxx Version:xxx IMEI:xxx GSM Signal Value:xxx

8. Warranty

1) This device is warranted to be free of defects in material and workmanship for one year.
2) This warranty does not extend to any defect, malfunction or failure caused by abuse or misuse by the Operating Instructions. In no event shall the manufacturer be liable for any router altered by purchasers.

The End!
Any questions please feel free to contact us.
www.iot-solution.com