Industrial 4G Edge Router

R40 User Manual

Version 1.6

Date: 2023-2-17

Shenzhen Beilai Technology

https://www.bliiot.com

Preface

Thanks for choosing BLIIoT Industrial 4G Edge Router R40. These operating instructions contain all the information you need for operation of a device in the R40 family.

Copyright

Disclaimer

This document is designed for assisting user to better understand the device. As the described device is under continuous improvement, this manual may be updated or revised from time to time without prior notice. Please follow the instructions in the manual. Any damages caused by wrong operation will be beyond warranty.

Revision History

DATE	FIRMWARE VERSION	HARDWARE VERSION	DESCRIPTION
2020.03.13	*V 1.0*	*V 1.0*	***First edition***
2020.09.30	*V1.1*	*V1.0*	***Modify some configuration instructions***
2021.2.25	*V1.2*	*V1.0*	***Added link to Huawei Cloud IO platform***
2021.03.18	*V1.3*	*V1.0*	**Add device mapping register address from 64-127 to 64-256**
2021-9-30	*V1.4*	*V1.0*	***(1) MQTT: Add a new mode that*** only release changed data ***(2) Cellular network: Add an enable switch to power on/ off the cellular modem*** ***(3) Support custom MQTT data format*** ***(4) Modbus master: Increase the setting of acquisition cycle and response timeout time*** ***(5) Cycle timer: Increase the settings of start, end time and cycle times*** ***(6) Network settings: Add WAN/LAN switching function*** ***(7) USB interface can load external storage for network sharing functions***
2022-5-17	*V1.5*	*V1.0*	***Add conditional operation function, logarithm, exponential operation***
2023-2-17	*V1.6*	*V1.0*	***Support SNMP, add new function named BLRMS: remote configuration, remote upgrade firmware etc.***

Table of contents

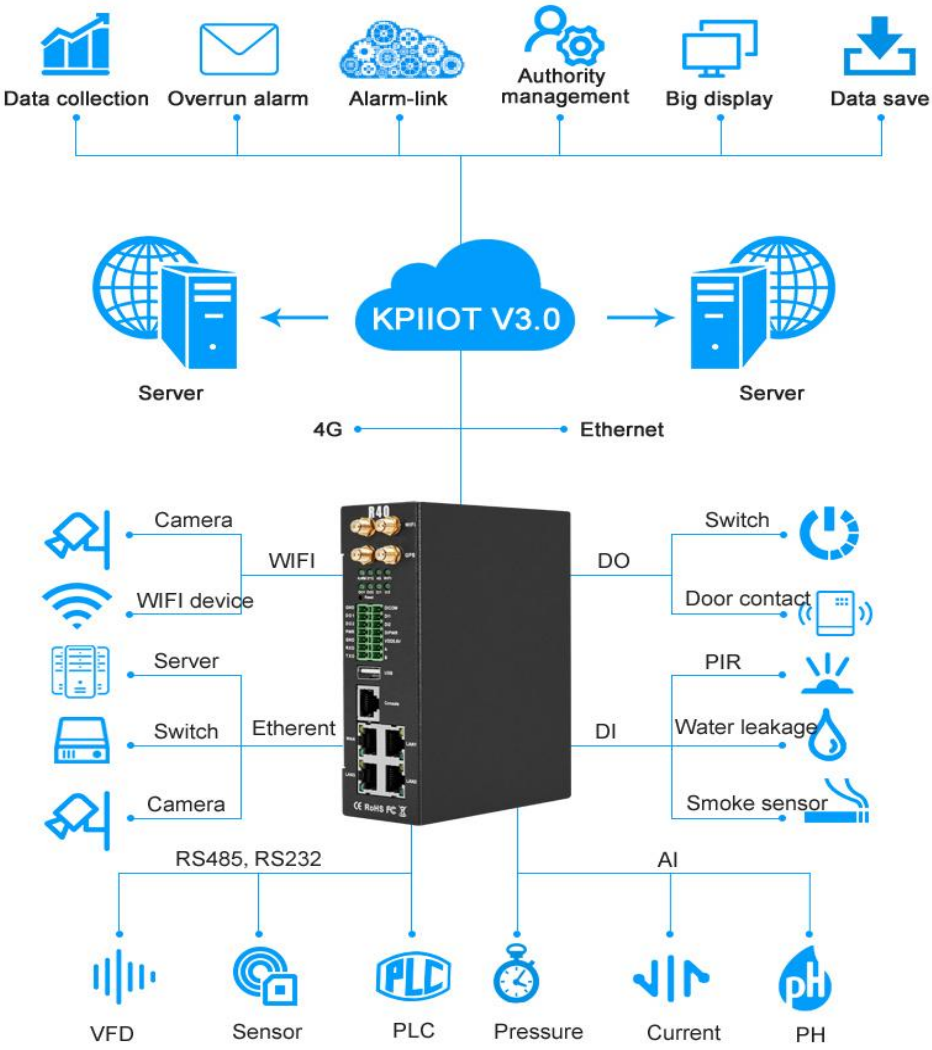
1. Product Description

1. 1 Brief Introduction

R40 is an industrial edge router, compatible with 4G/3.5G/3G/2.5G network, flagship configuration, VPN link, industrial protection, wide temperature, wide voltage design, easy to set up high speed, stable. The wireless transmission network uses the public LTE network to provide users with wireless long-distance data transmission, can be used in multiple industrial applications.

It is an industrial-grade multifunctional Internet of Things terminal device that supports POE power supply, comes with IO input and output, with 2 serial ports, supports transparent transmission, Modbus Master protocol for expanding IO and connecting PLC and other devices. It adopts dual SIM card redundancy design to ensure stable and reliable data transmission, supports MQTT protocol and Modbus protocol, SNMP protocol and is compatible with most PLC protocols, greatly simplifying on-site wiring construction costs and reducing operation and maintenance costs.

High-performance industrial-grade edge router adopts 32-bit processor, developed based on Linux system, supports GSM/2G/3G/4G/GPRS/EDGE/WCDMA/HSPA+/LTE network, provides high-speed wireless network bandwidth for the device through wireless connection, and has automatic detection of network disconnection, automatic restart of dial-up failure, and scheduled restart to ensure network stable connection.

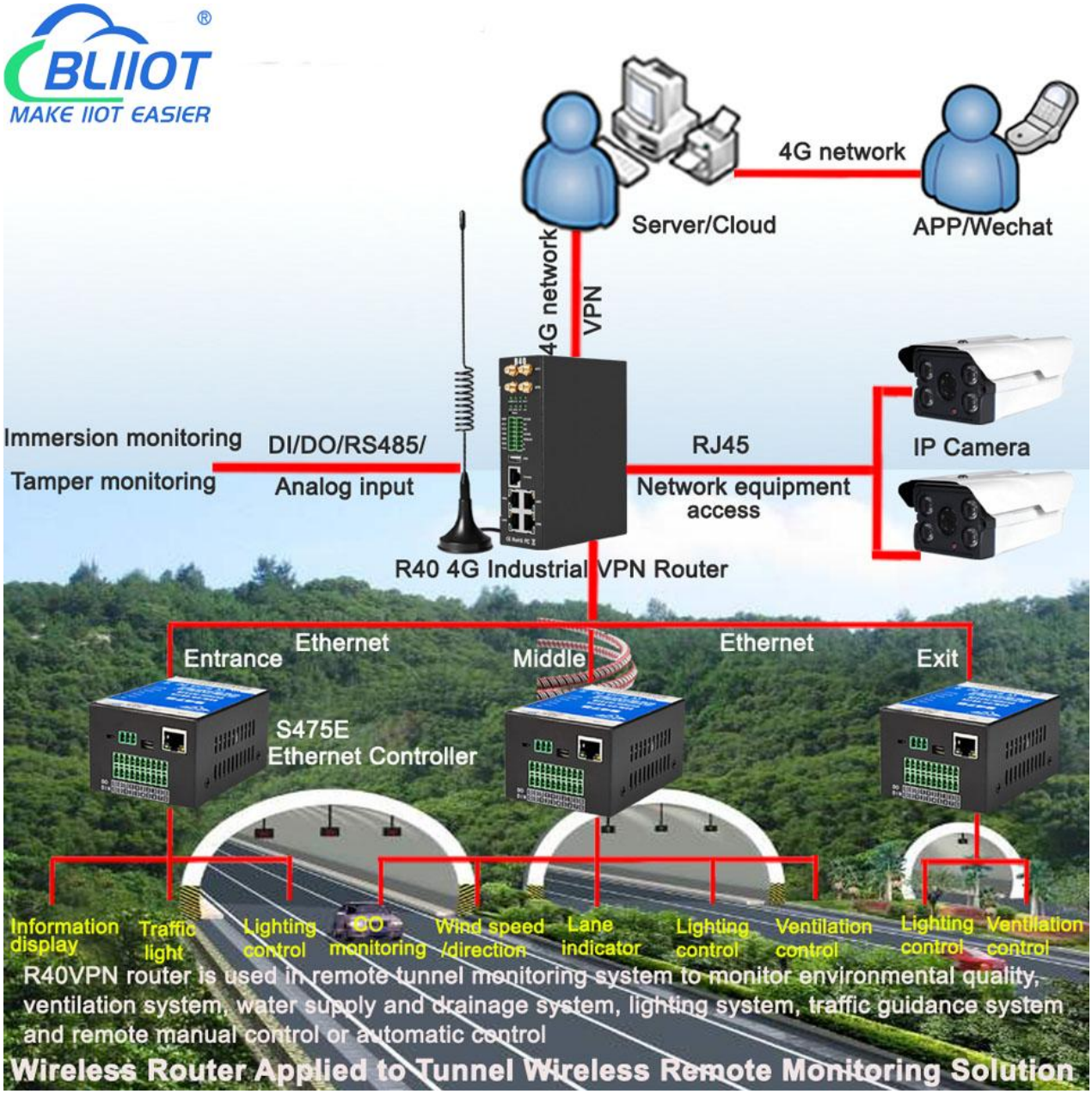


1.2 Typically Applications

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.

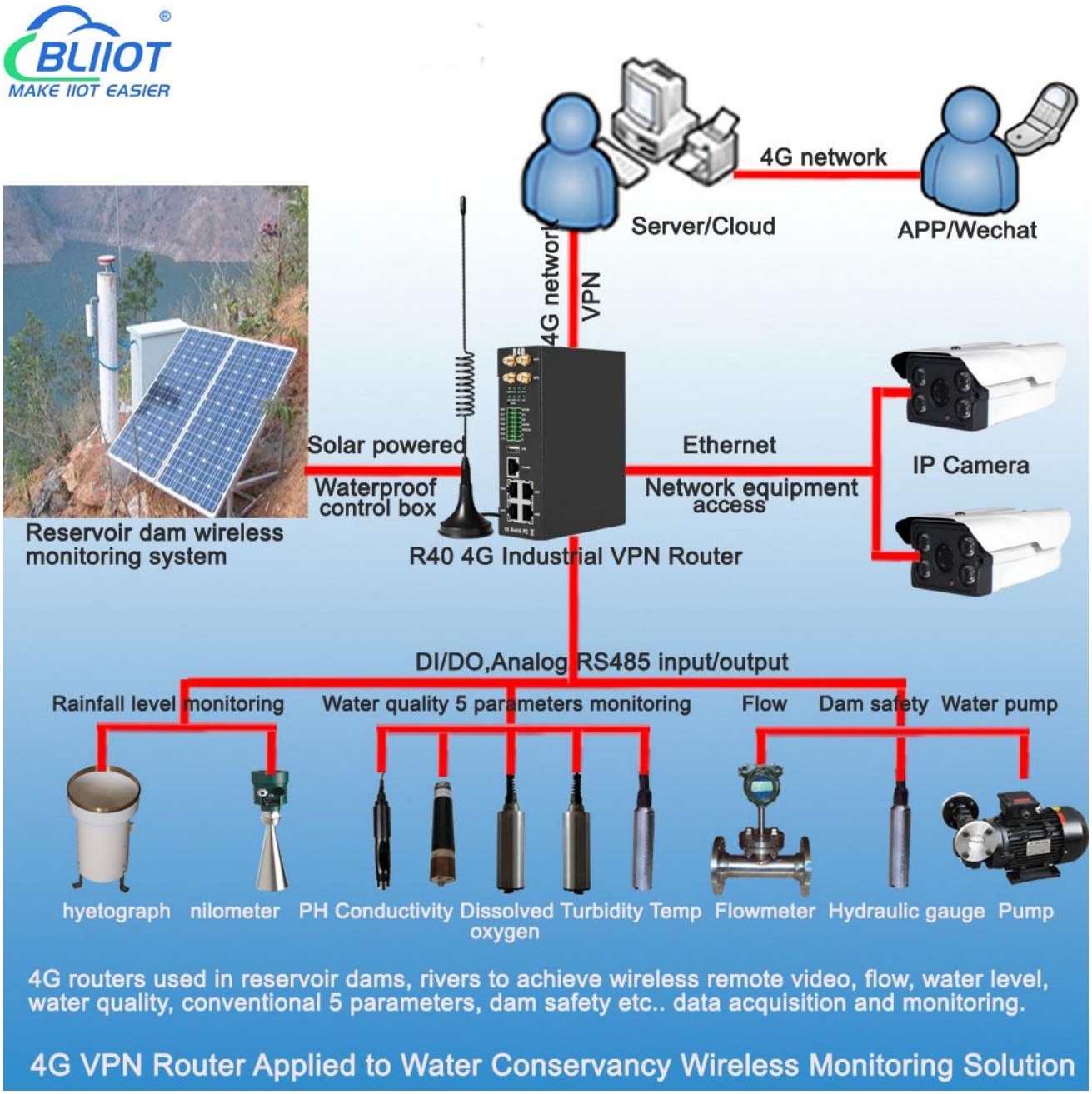
1.2.1 Tunnel Wireless Remote Monitoring

R40 4G industrial edge router is used in tunnel remote monitoring system to monitor environmental quality, ventilation system, water supply and drainage fire protection system, lighting system, traffic guidance system monitoring and remote manual control or automatic control.



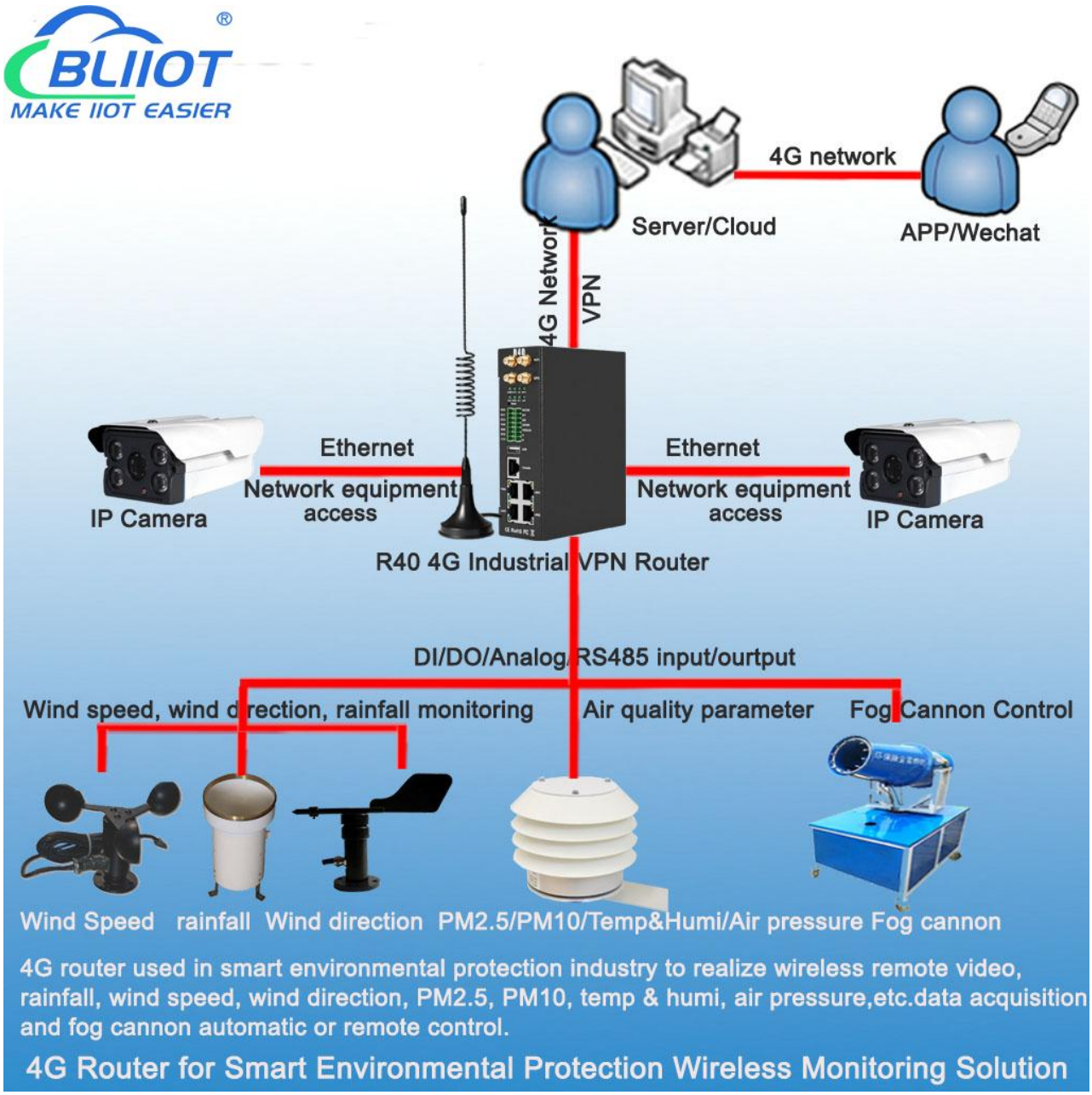
1.2.2 Water Conservancy Wireless Monitoring

R40 4G industrial edge router is used in reservoir dams, canals, rivers to achieve wireless remote video, flow, rainfall, water level, water quality routine 5 parameters, dam safety, water pumps and other data collection and control.



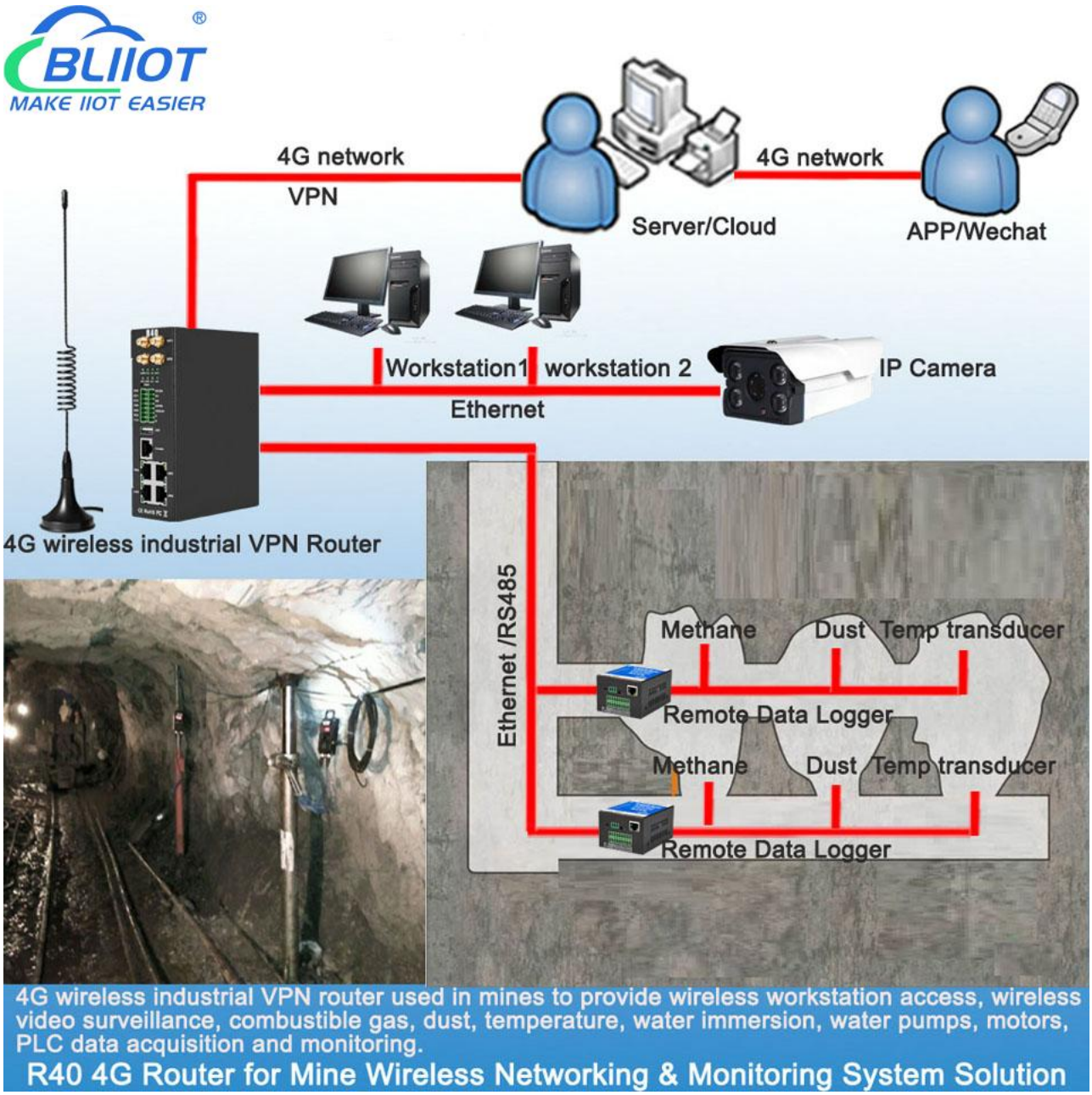
1.2.3 Smart Environmental Protection Wireless Monitoring

R40 4G industrial edge router is used in the smart environmental protection industry to realize wireless remote video, rainfall, wind speed, wind direction, PM2.5, PM10, temperature and humidity, air pressure and other data collection and automatic or remote control fog cannon.



1.2.4 Mine Wireless Networking & Monitoring System Solution

R40 4G industrial edge router is used in mines to provide data collection and control of wireless workstation network access, wireless video surveillance, combustible gases, dust, temperature, water immersion, water pumps, motors, electrical machinery, PLC, etc.



1.3 Safety Directions

Safe Notice

Please do not use this product in places where the use of mobile phones is prohibited

Interference

Do not use the unit when using GSM/3G/4G equipment is prohibited or might bring disturbance or danger.

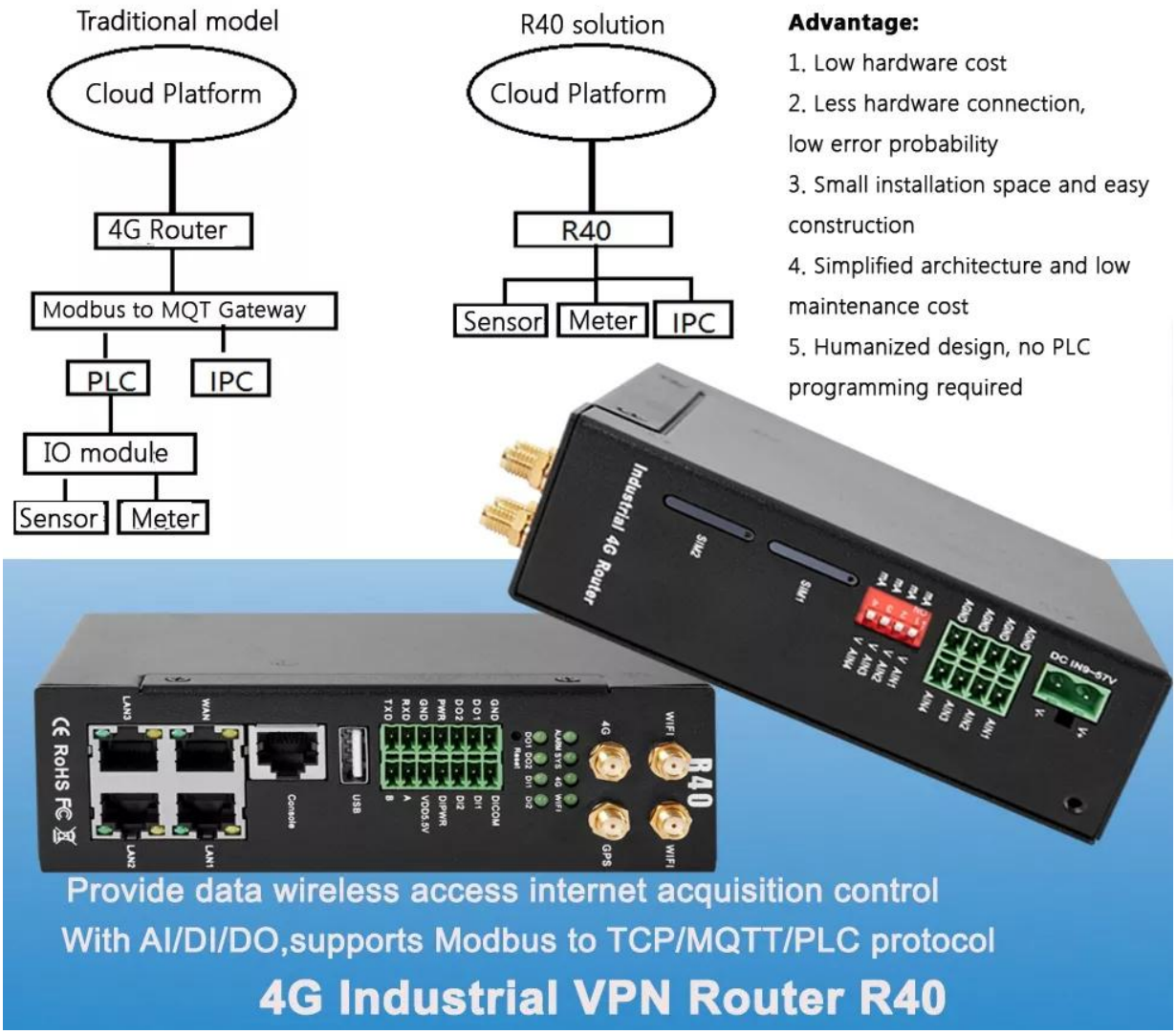
1.4 Standard Packing List

Router R40 X1, GSM/3G/4G Antenna X1, 2.4G WIFI Antenna X2
User Manual, Wall-mounted snap kit, 35mm Standard DIN rail fixed Bracket, Wiring terminal
Optional accessories: Power adaptor, GPS antenna, POE board

Note: The standard package does not include SIM card, Power adaptor, GPS antenna, POE board.

1.5 Main Features

- DIN(2 channel) :Support NO/NC/counting input, frequency <100, can set counting threshold, support alarm trigger.
- DO(2 channel): Can be set according to the trigger condition.
- AIN(4 channel): Support 0-5V, 0-20mA, 4-20mA, can set threshold value, support alarm trigger.
- Support SMS to query DI/DO/AI status and value, and set DO status;
- Support 4G wireless Internet access function, can set APN and other parameters;
- Two SIM card slots, support dual card switching;
- Support GPS, positioning data can be released through MQTT;
- VPN: Support L2TP, IPSEC, OPENVPN and other VPN protocols.
- Interface: Support RS485 and RS232 serial port transparent transmission and MODBUS RTU to TCP, Support MODBUS master, can regularly read MODBUS slave node data through RS485, RS232 and Ethernet.
- Support address mapping, mapping RS485, RS232 and Ethernet access device addresses to router local addresses.
- Support monitoring the online status of network devices connected to the LAN port, which can be reported to the platform through MODBUS or MQTT.
- Link switching: Support WAN port and 4G network connection switching, preferentially use WAN port wired network.
- Network management: Supports SNMPV1 / V2C.
- Platform connection: Support MODBUS and MQTT protocols, MQTT supports SSL encryption.
- Alarm: Supports SMS and e-mail alarm.
- Timer: Support one-time timer and period timer.
- Logic operations: Support Boolean and numeric logic operation, also support conditions and arithmetic logic operations;
- Upgrade: Support remote upgrade through web page



1.6 Technical Parameters

Item	Parameters	Description
Power Supply	Input voltage	9~57VDC
	Input current	Normal: 240mA@12V, max: 800mA@12V
	Connection	5.08mm terminals
	Protection	Anti-reverse connection Protection
WAN	Qty	1
	Interface Spec	RJ45,10/100Mbps, Automatically adapted to MDI/MDIX
	Protection	ESD ±30kV(contact), ±30kV(air) EFT 40A(5/50ns) Lightning strike 24A(8/20μs)
LAN(POE)	Qty	3
	Interface Spec	RJ45,10/100Mbps, Automatically adapted to MDI/MDIX
	POE(optional)	Supports 3 POE power output

		compatible IEEE802.3at/af Single POE maximum output power 30W With power management function Voltage range 48～57V
	Protection	ESD ±30kV(contact), ±30kV(air) EFT 40A(5/50ns) Lightning strike 24A(8/20μs)
Serial Port	Qty	2
	Type	1 RS485, 1 RS232
	Baud rate	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200, 230400
	Data Bit	5, 6, 7, 8
	Parity Bit	None, Even, Odd
	Stop Bit	1, 2
	Working mode	Data transparent transmit, Modbus RTU to TCP, Modbus master, Modbus slave
	Protection	ESD(contact): 8KV Surge: 4KV(8/20us) ESD ±8kV(contact), ±15kV(air) EFT 4KV, 40A(5/50ns)
Console	Qty	1
	Type	CONSOLE
	Interface Spec	RJ45
	Protection	ESD：±8kV(contact), ±15kV(air)
USB (Reserved)	Qty	1
	Type	USB2.0(HOST)
	Protection	ESD ±8kV(contact), ±15kV(air)
WIFI	Antenna qty	2
	Antenna type	SMA
	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	Outdoor non-blocking/opening, covering up to 20 meters
	SSID Broadcast Switch	Support
Cellular Network	Antenna Port Qty	1
	Antenna Port Type	SMA
	4G(L-E)	GSM/EDGE：900,1800MHz WCDMA：B1,B5,B8 FDD：B1,B3,B5,B7,B8,B20 TDD：B38,B40,B41

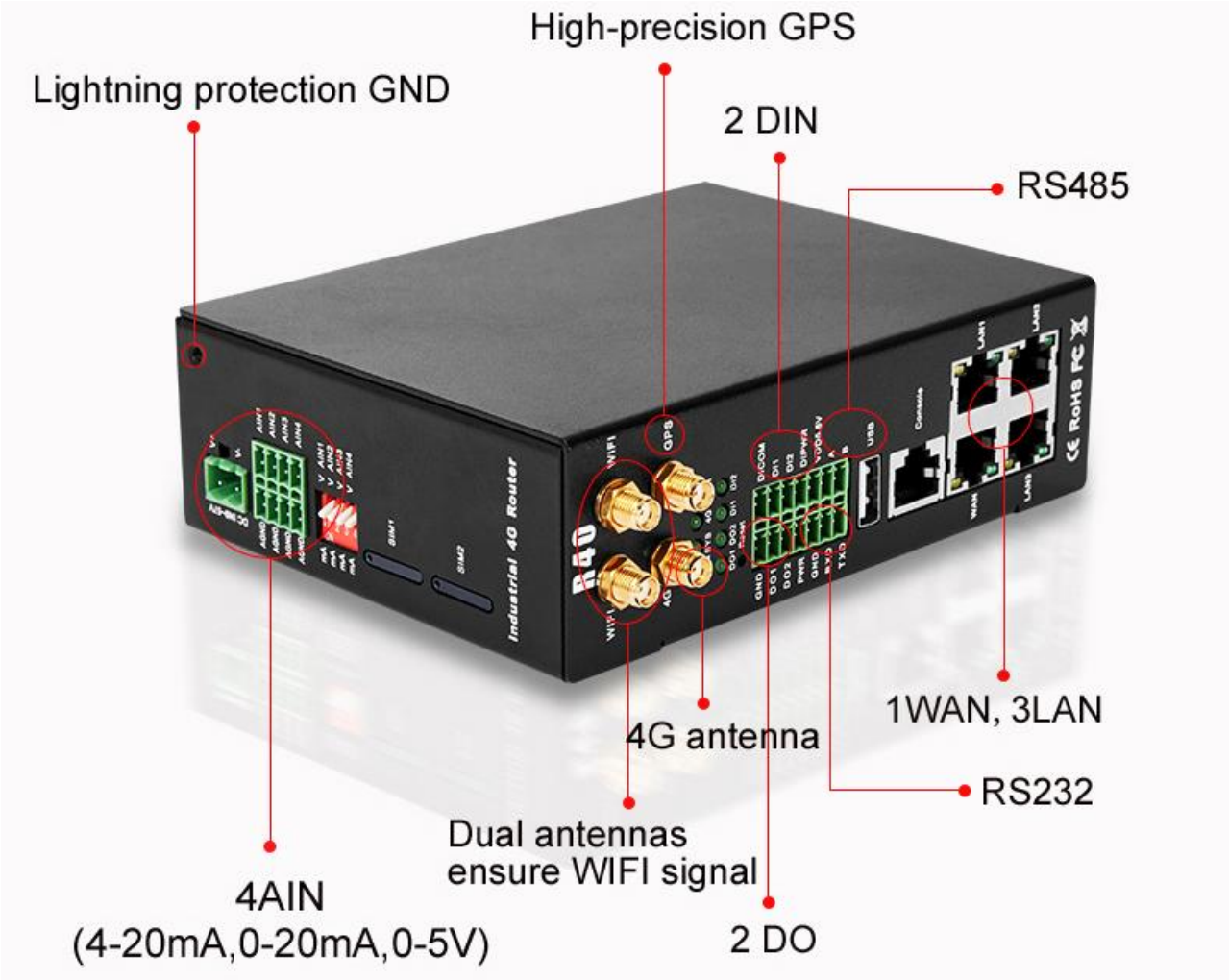
	4G(L- AU)	GSM/EDGE：850,900,1800MHz WCDMA：B1,B2,B5,B8 FDD：B1,B2,B3,B4,B5,B7,B8,B28 TDD：B40
	4G(L-A)	WCDMA：B2,B4,B5 FDD：B2,B4,B12
	4G(L-V)	FDD：B4,B13
	4G(L-J)	WCDMA：B1,B3,B8,B18,B19,B26 FDD：B2,B4,B12 TDD: B41
	4G(L-CE)	GSM/EDGE：900,1800MHz WCDMA：B1,B8 TD-SCDMA：B34,B39 FDD：B1,B3,B8 TDD：B38,B39,B40,B41
SIM	Qty	2
	Interface Spec	Drawer interface, supports 1.8V/3V SIM/UIM (NANO)
	Protection	In-built 15KV ESD Protection
GPS (optional)	Antenna qty	1
	Antenna type	SMA
	Tracking Sensitivity	> -148 dBm
	Horizontal Accuracy	2.5m
	Protocol	NMEA-0183 V2.3
Digital input	Qty	2
	Type	Switch contact signal (dry node) or level signal (wet node)
	Range	1: High level, 5~30VDC, close signal 0: low level 0~1VDC open signal
	Pulse frequency	Max 100Hz
	Protection	Isolation voltage 3750Vrms
Digital output	Qty	2
	Type	SINK output
	Load voltage	Max 50VDC
	Load current	500mA(single), 625mW
	Protection	EFT: 40A(5/50ns)
Analog input	Qty	4
	Type	0~5V，4~20mA，0~20mA
	ADC Resolution	16bit
	Protection	EFT: 40A(5/50ns)
Indicator light	ALARM	Alarm indicator light
	SYS	System running status indicator
	4G	4G status indicator
	WiFi	WiFi status indicator
	DO1, DO2	Digital output indicator light

	DI1, DI2	Digital input indicator light
System	CPU	MIPS CPU, Clock Speed 580Mhz
	Storage	16MB (Scalable to 32MB)
	RAM	128MB (Scalable to 256MB)
Software	Network Protocol	PPP, PPPoE, TCP, UDP,DHCP, ICMP, NAT, HTTP, HTTPs, DNS, ARP, NTP, SMTP, SSH2, DDNS,SNMP etc.
	VPN	Ipsec, OpenVPN, L2TP
	Firewall	DMZ, DoS defense, IP packet, Domain name and MAC address filtering, port mapping, access control
	Remote Management	Support web remote configuration
	System Log	Support
	Firmware Upgrade	Support serial port local TFTP/web firmware 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
	MTBF	100,000 hours
	Others	CE, FCC, ROHS, 3C
Working Environment	Working temperature	-40～85℃
	Storage temperature	-40～105℃
	Humidity	5～95%RH
Others	Enclosure	Metal
	Size	H145mm * L110mm * W45mm
	IP level	IP30
	Net weight	790g
	Installation	Wall-amount/Rail-amount

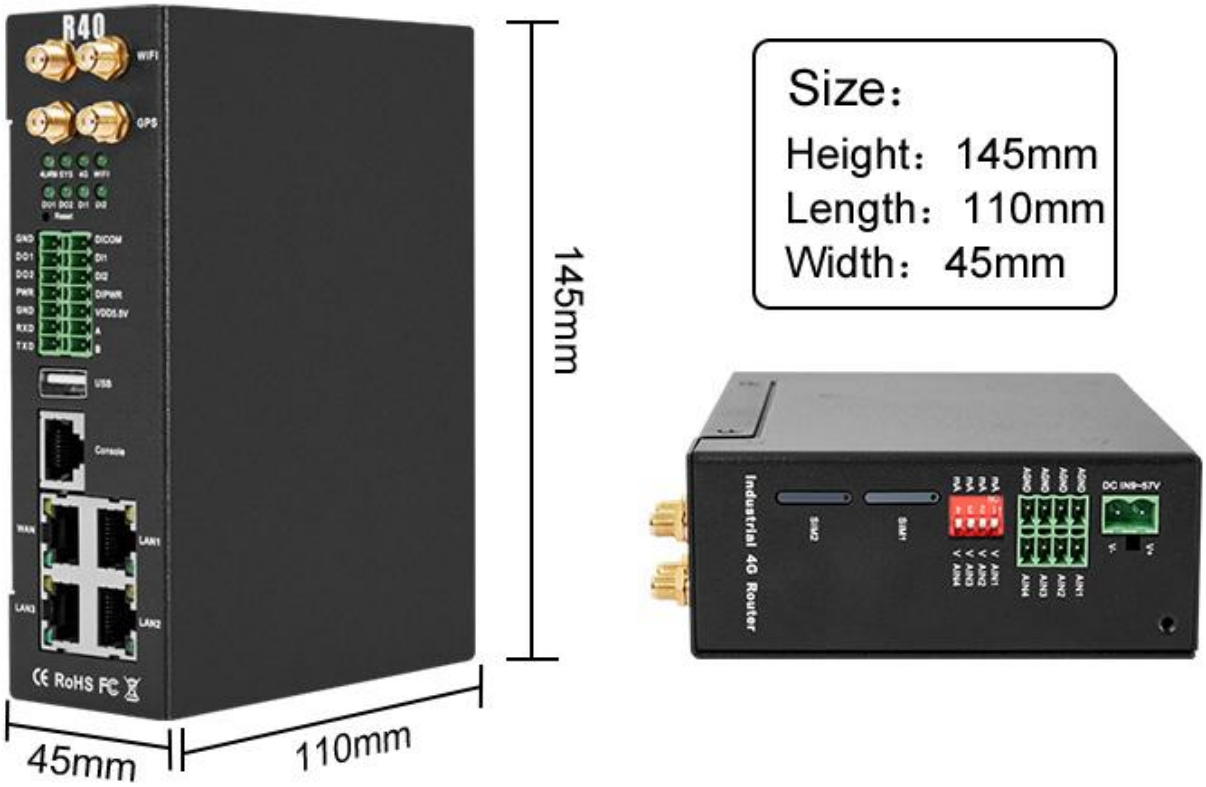
1.7 Model Selection

Model	Serial Port	WAN	LAN	WIFI	Digital input	Digital output	Analog input	Extend function
R40	1RS485,1RS232	1	3	√	2	2	x	Modbus slave/MQTT
R40A	1RS485,1RS232	1	3	√	2	2	x	Modbus master/slave/MQTT
R40B	1RS485,1RS232	1	3	√	2	2	4	Modbus master/slave/MQTT

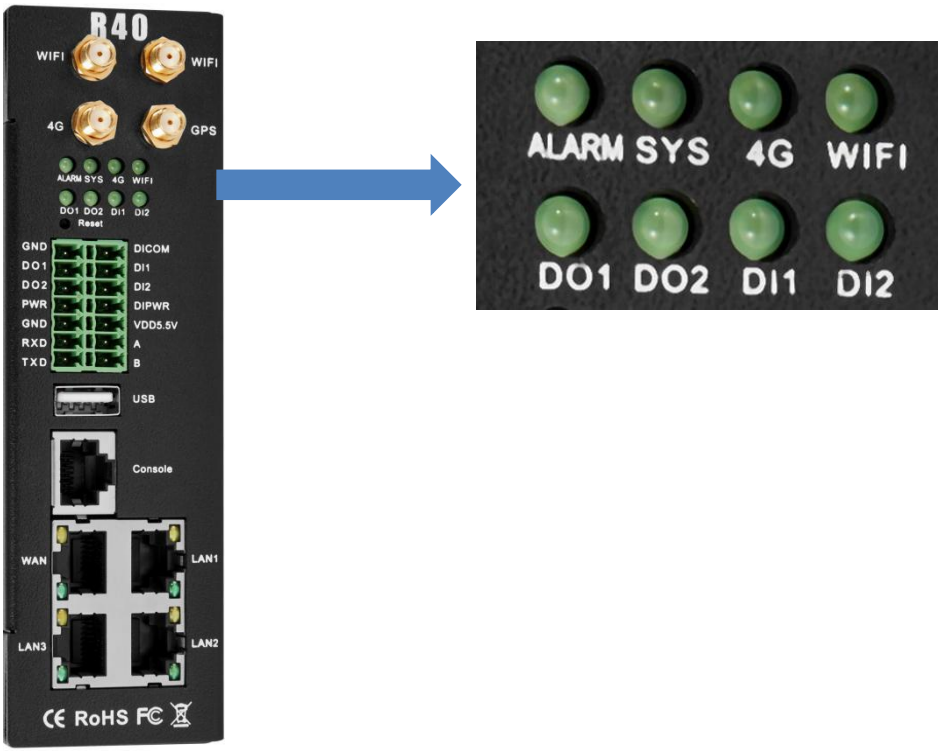
2. Hardware


High-precision GPS
Lightning protection GND
2 DIN
RS485
1WAN, 3LAN
4G antenna
RS232
Dual antennas
ensure WIFI signal
4AIN
(4-20mA,0-20mA,0-5V)
2 DO

2.1 Size



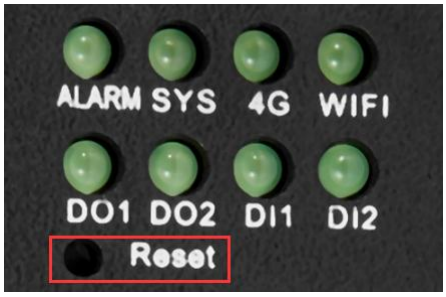
2.2 Indicator Light



LED Indicator light			
Name		Status	Description
ALARM	Alarm indicator light	ON	DI or AI trigger alarm
		OFF	Normal
SYS	System running status indicator	Flicks slowly	Normal
		OFF	Abnormal
4G	4G status indicator	Flicks fast	Signal normal
		OFF	Abnormal
WiFi	WiFi status indicator	ON	WiFi normal
		OFF	Abnormal
DO1	Digital output 1 indicator light	ON	DO1 Close
		OFF	DO1 Open
DO2	Digital output 2 indicator light	ON	DO2 Close
		OFF	DO2 Open
DI1	Digital input 1 indicator light	ON	DI1 Close
		OFF	DI1 Open
DI2	Digital input 2 indicator light	ON	DI2 Close
		OFF	DI2 Open

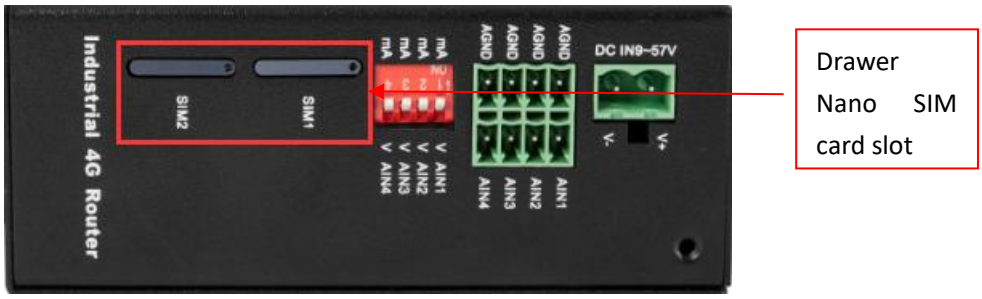
2.3 Reset

After the router runs normally, use a pointed stick to continue to hold down the Reset button for about 10 seconds until the WAN port indicator flashes slowly. At this time, restart the router to restore the factory default settings.

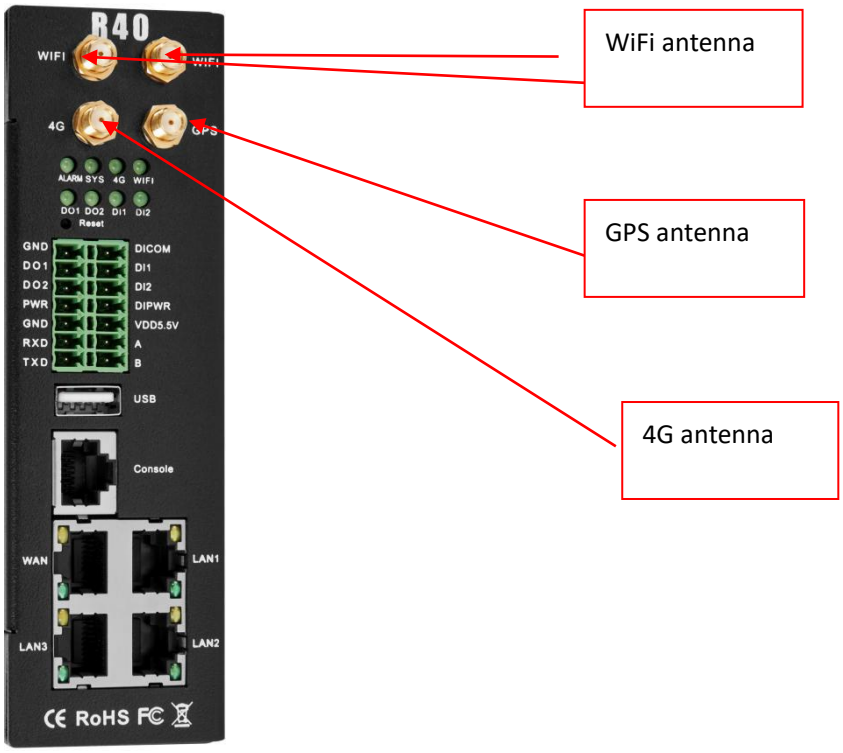


2.4 SIM Card

When inserting/removing the SIM card, first make sure that the device is turned off, insert the card take-out pin into the small hole of the card slot, press it slightly to push the card slot out.



2.5 Connect External Antenna



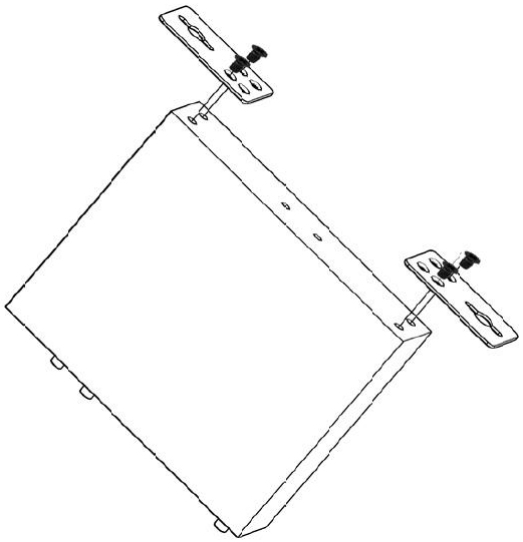
2.6 Router GND

The router ground wire helps prevent the effects of electromagnetic interference. Before connecting the device, ground the device through the ground screw connection. Note: This product should be installed on a well-grounded device surface, such as a metal plate.

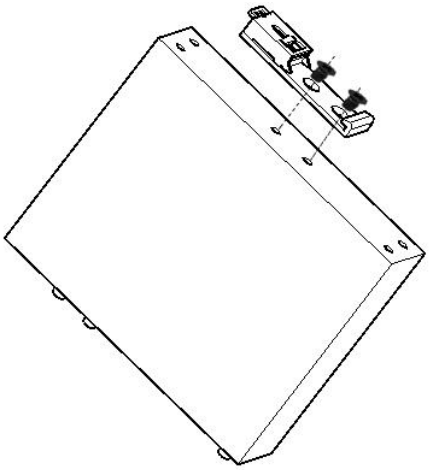
2.7 Installation

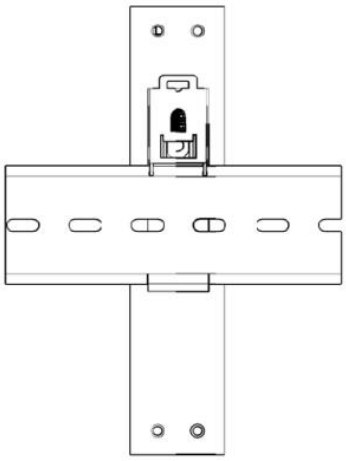
This device supports horizontal desktop placement, wall mounting and rail mounting.

2.7.1 Wall-mounted Installation



2.7.2 Rail Mounting





3. Router Operation (Start up)

3.1 Switch on Router Device

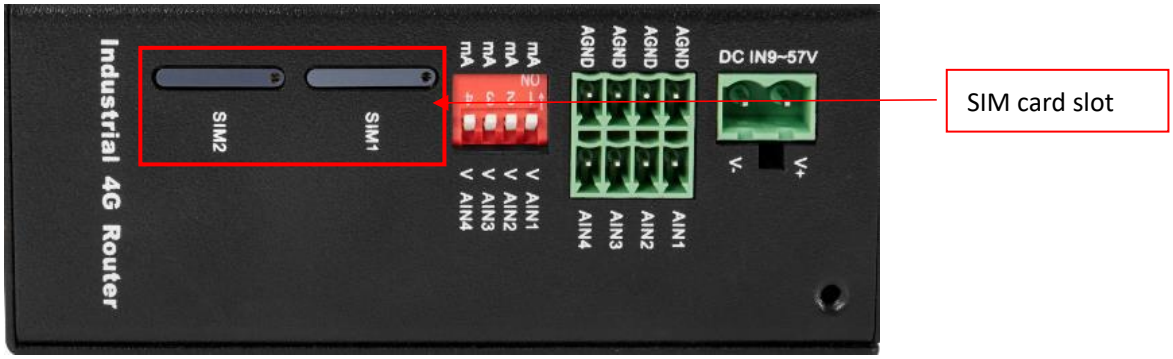
Power input port: R40 uses 9 ~ 57V DC voltage for power supply. If you need POE power supply then power supply must meet 44V ~ 57V DC voltage power supply (recommend 48V / 2A).

System running status

Observe the system running status indicator -SYS, slow blinking indicates that the device starts normally.

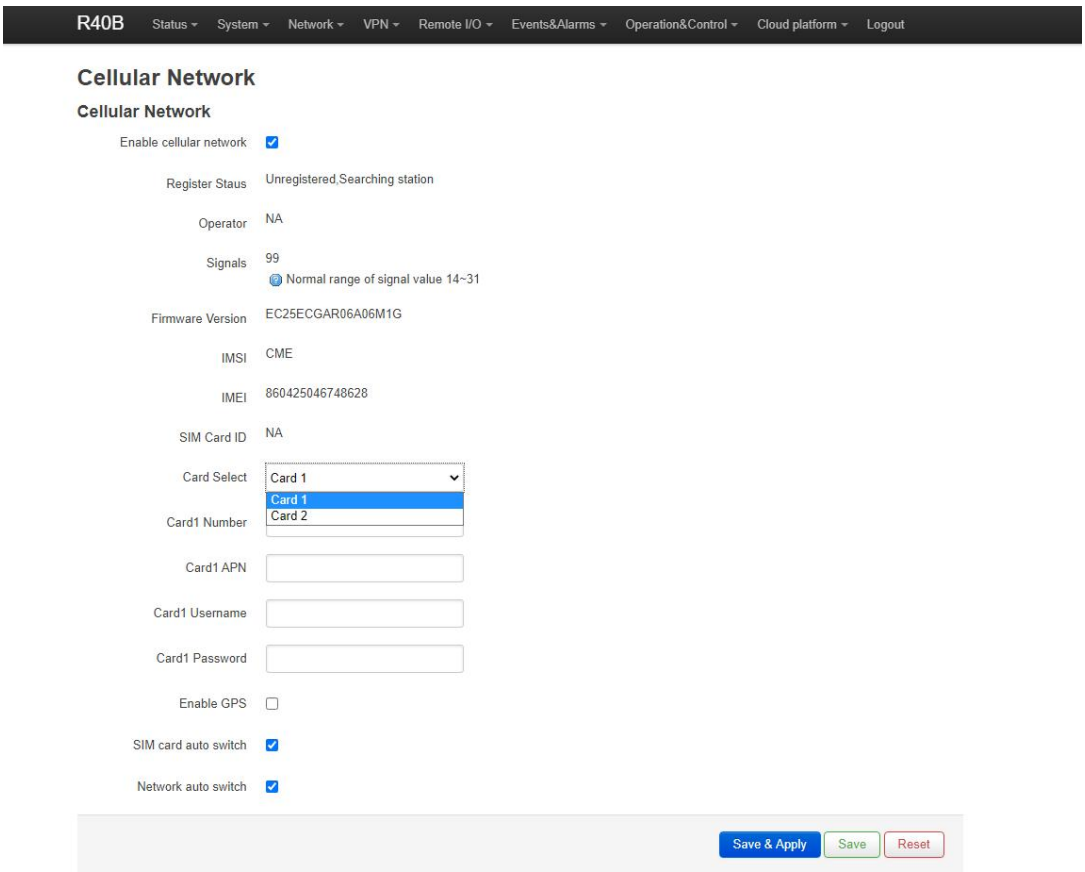
3.2 SIM Card Operation

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



After the device is powered on, enter the router configuration interface-network-cellular network, you can view the cellular network registration status.

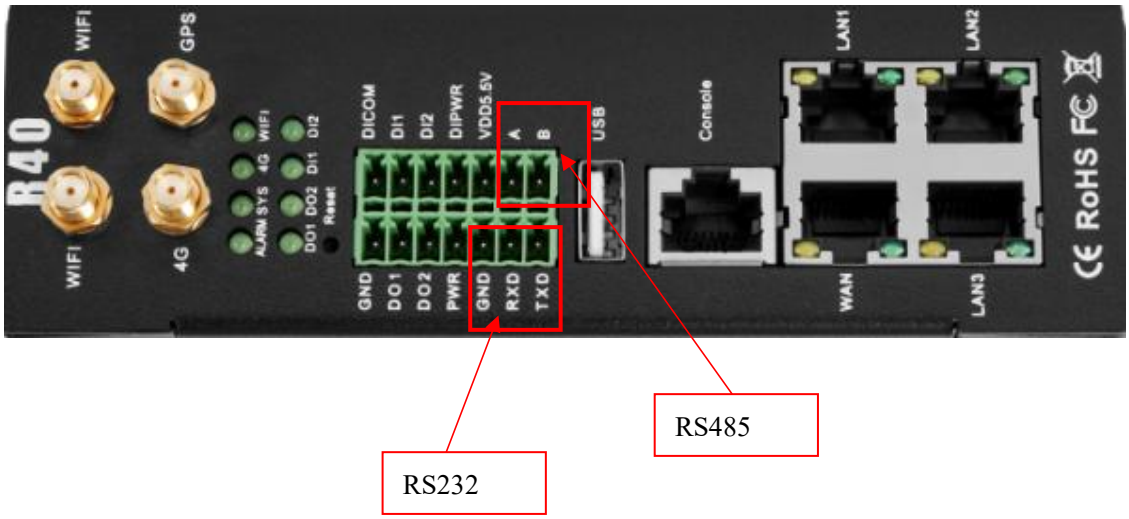
4G cellular network dial-up networking defaults to use SIM card 1, if you need to use SIM card 2, you need to enter the cellular network configuration interface, select card 2 in the column of selecting a phone card, save and apply to switch.
The dual card redundancy design of R40 can automatically switch to another SIM card for communication when the current SIM card network communication is abnormal (two minutes).
For detailed configuration, please refer to 5.4.1.5.4G port and 5.3.3 cellular network.



3.3 Serial Port Operation

This router device has RS485 and RS232 interface, which can be used for Modbus master function, Modbus slave function, transparent transmission function, Modbus RTU to TCP protocol conversion. Modbus master function is available in particular model only, please refer to selection table.

Note: At a certain moment, a serial port can only be selected for one function and cannot be used for other purposes. If it is found that the serial port cannot be selected on the configuration page, it means that the serial port has been set on other function configuration pages; different serial ports do not affect each other.



3.3.1 Modbus Master

Modbus master : Used as Modbus master, the serial port connected to Modbus slave equipment, through configuration Page 5.5.3. Modbus master configures slave register and serial port parameters, the host collect slaves data through Modbus RTU protocol, and store the slave data in the local mapping register, can query the slave data directly on the configuration page, or you can 5.8. Cloud connection settings: Configure Modbus protocol or MQTT protocol to upload slave data to the server to realize Modbus RTU protocol to MQTT protocol.

When the RS485 or RS232 selected as the "Modbus RTU master", or the corresponding slave IP is set on the Ethernet, the device will actively poll the slave device in accordance with the Modbus RTU or Modbus TCP protocol, and put the slave device in The value of the register is read into the device's mapping area for storage. In this way, the registers in the slave are mapped to the device, and reading and writing the mapped registers of the device will be directly transmitted to the slave device through the RS485 serial port, RS232 serial port or network port. There is a one-to-one correspondence between the slave register address and the mapped register address in this device. This is the mapping register list.

Users can connect various slaves through RS485 serial port, RS232 serial port or Ethernet port, supporting up to 48 slave devices, so as to realize the function of adding I/O ports and reading and writing smart meters and smart devices. For example, connect to the remote I/O modules of the Mxxx series to expand the number of DIN, DO, AIN, AO, PT100 input ports, or connect the power parameter monitoring module to read the current, voltage, power of the three-phase electricity, or connect to the UPS power supply for Parameter monitoring, etc. Or the combination of the above various smart devices, etc., can meet the functional requirements of most applications.

3.3.2 Modbus Slave

Modbus slave function: When used as Modbus slave , the serial port will be connected to the Modbus master device. Configure the serial port parameters through the configuration page 5.5.4. Modbus slave, the master device will be able to collect the local I/O data through Modbus RTU or TCP protocol.

3.3.3 Transparent Transmission

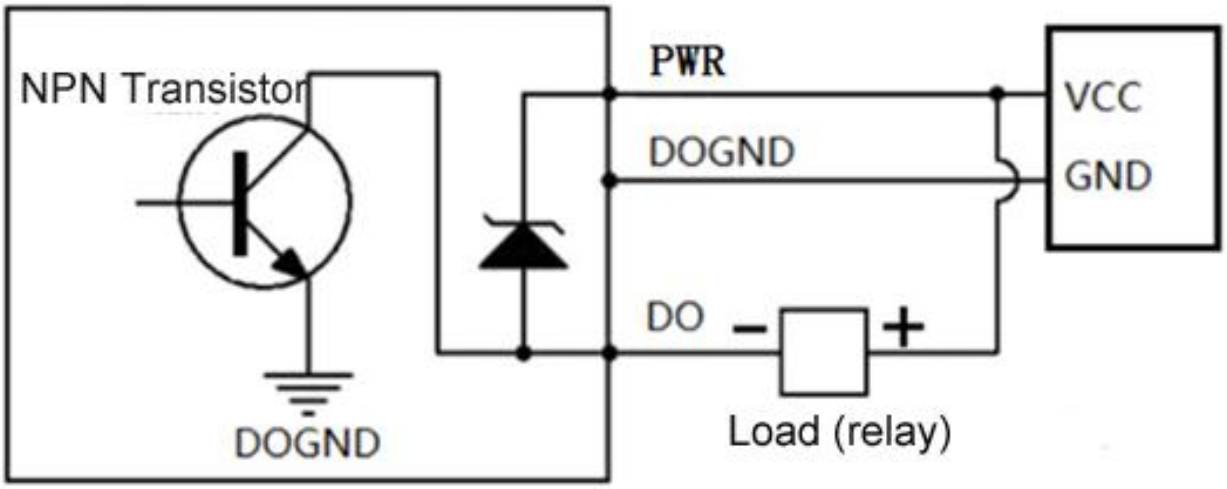
The device used as a data transfer station between the server and the slave device, through the configuration page 5.5.6. It transparently transmits the data uploaded from the slave to the server, and sends the data to the server Transparent transmission to the slave, without processing the data content, only forwarding data, to achieve data transparent transmission function.

3.3.4 Modbus RTU to TCP Protocol Conversion

Master communicate with slave via Modbus RTU protocol,master communicate with slave via Modbus TCP protocol,through the configuration page 5.5.5.
The device automatically converts Modbus TCP commands issued by the server into Modbus RTU commands and sends them to the slave, and then converts the Modbus RTU commands returned from the slave into Modbus TCP commands and replies to the server, so that the Modbus RTU slave device and the Modbus TCP server can be realized communication.

3.4 Digital Output DO Port Operation

3.4.1 Wiring



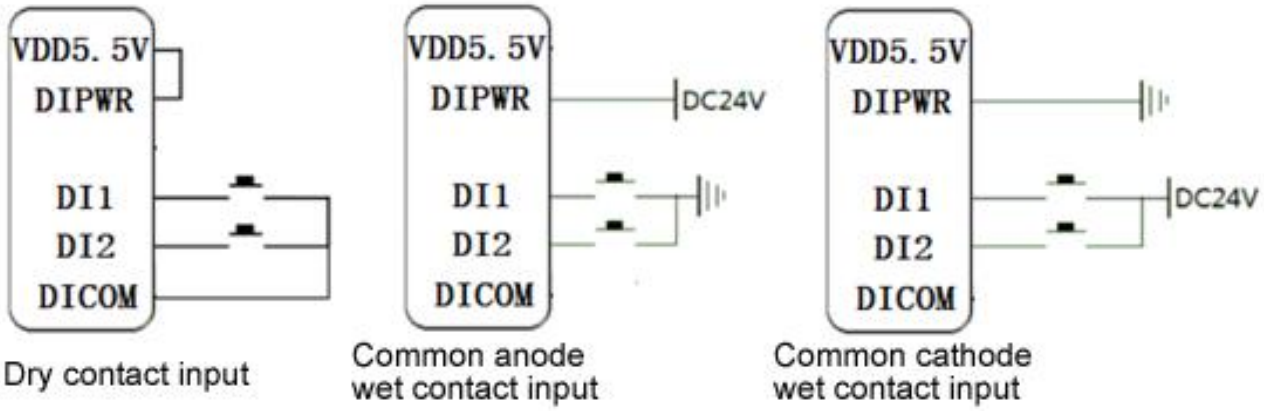
3.4.2 DO Ports

Digital output	QTY	2
	Type	SINK output
	Load voltage	Max 50VDC
	Load current	500mA（single）, 625mW
	Protection	EFT: 40A（5/50ns）

1. DO1~DO2 are two-way NPN transistor open-collector output, and PWR is the clamp protection for the external power supply of the common terminal.
2. Digital output setting: Enter the router configuration interface -RTU I/O-Digital input and output, and you can enable/disable or query and set the digital output status at the digital output port.
3. Trigger setting: According to the state of DI digital input or AIN analog input, you can set the trigger condition and control the DO digital output operation (the confirmation time is X seconds after the trigger condition is reached).
4. For detailed configuration, please refer to 5.6.2. Digital input and output.

3.5 Digital Input DI Port Operation

3.5.1 Wiring



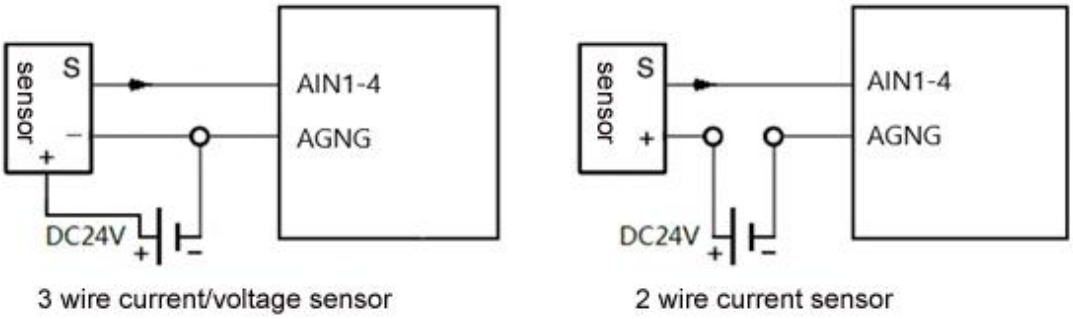
3.5.2 DI Ports

Digital input	QTY	2
	Type	Dry contact, Wet contact
	Range	High level (digital 1) 5~30VDC, low level (digital 0) 0~1VDC
	Pulse frequency	<100Hz
	Protection	Isolation voltage 3750Vrms

1. DI1~DI2 are two digital inputs. The default is wet contact input. Short-circuit VDD5.5V and DIPWR to switch to dry contact input.
2. Digital input setting: enter the router configuration interface -RTU I/O-Digital input and output, and you can enable/disable or query the digital input status and pulse count value at the digital input port.
3. Trigger setting: The trigger condition can be set according to the DI digital input state to control DO digital output, restart and other operations (the confirmation time is X seconds after the trigger condition is reached).
4. For detailed configuration, please refer to 5.6.2. Digital input and output.

3.6 Analog Input AI Port Operation

3.6.1 Wiring



3 wire current/voltage sensor　　2 wire current sensor

3.6.2 AI Ports

Analog input	QTY	4
	Type	0~5V, 4~20mA, 0~20mA
	ADC resolution	16 bit
	Pulse frequency	<100Hz
	Protection	EFT: 40A（5/50ns）

1. AI-AI4 is a four-way analog input, the default is 0~5V voltage type analog input, you can switch to current type analog input by turning the dial switch to mA. The four-way dial switch AI1~AI4 is Four analog inputs correspond one to one, V corresponds to voltage type, and mA corresponds to current type.
2. Analog input setting: enter the router configuration interface -RTU I/O-Analog input, in the mode you can select voltage 0~5V, current 4~20mA, current 0~20mA (note that the DIP switch should also be selected Corresponding mode), set the range in the minimum and maximum values, you can see the actual measured value in the current value.
3. Trigger settings: The trigger conditions can be set according to the AIN status to control DO digital output, restart and other operations (the confirmation time is X seconds after the trigger condition is reached).
4. For detailed configuration, please refer to 5.6.3. Analog input

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 a wired connection; the other is to connect to the router through WIFI. The computer can automatically obtain IP through DHCP, or you can set a static IP on the same network segment as the router. After the connection is established, enter the router's default login address 192.168.3.1 on the computer browser to enter the router's WEB login interface. The default login The user name is admin and there is no password.

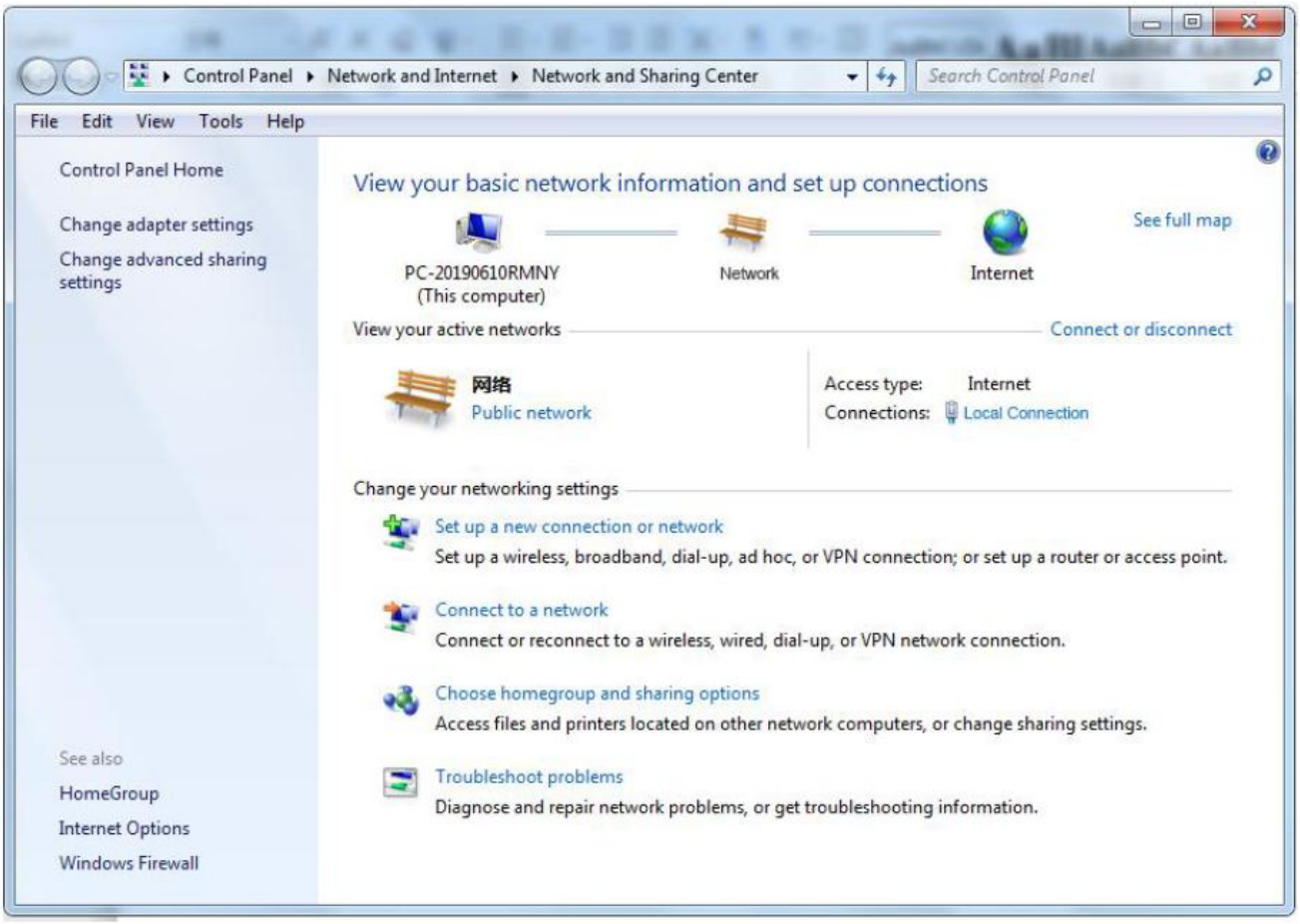
4.1 Wired Connection Router

There are two ways to configure its IP address on PC, one is to enable automatic IP address acquisition on the local connection of the PC, and the other is to configure a static IP address on the

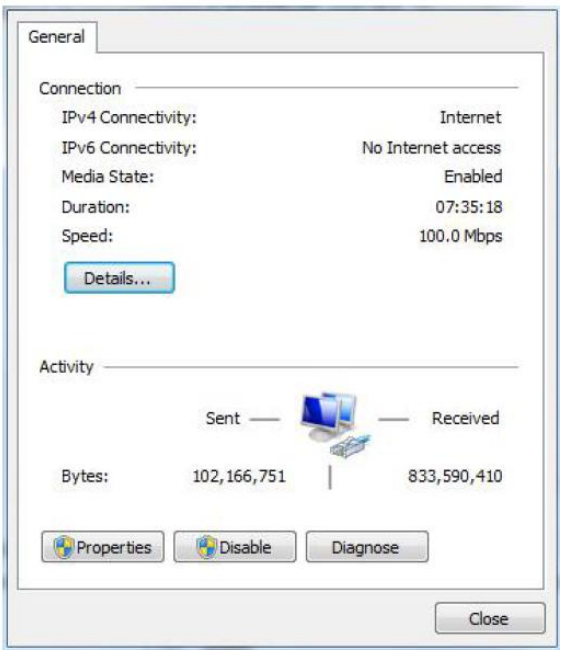
same subnet as the router on the local connection of the PC.

Setting on Windows 7 as an example:

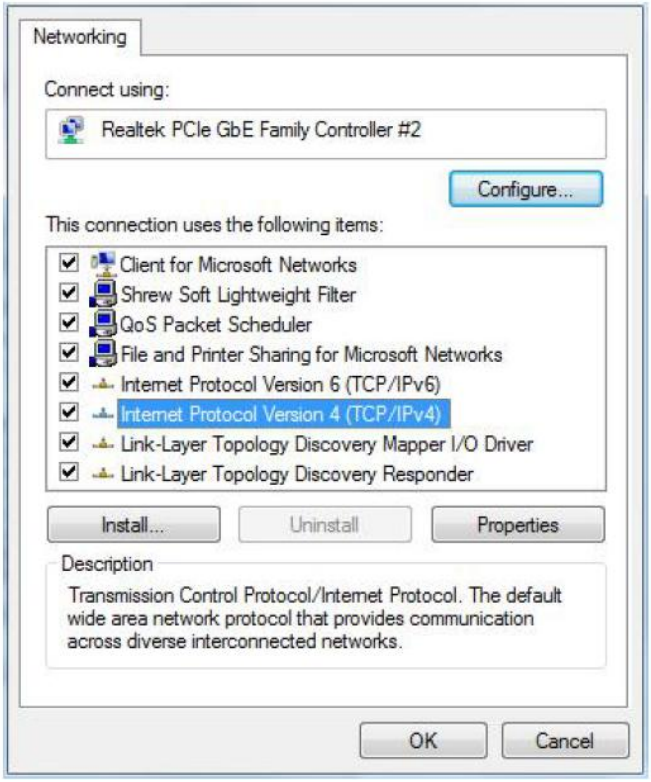
1. Click "Start> Control Panel> Network and Sharing Center", double-click "Local Area Connection" in the window.



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

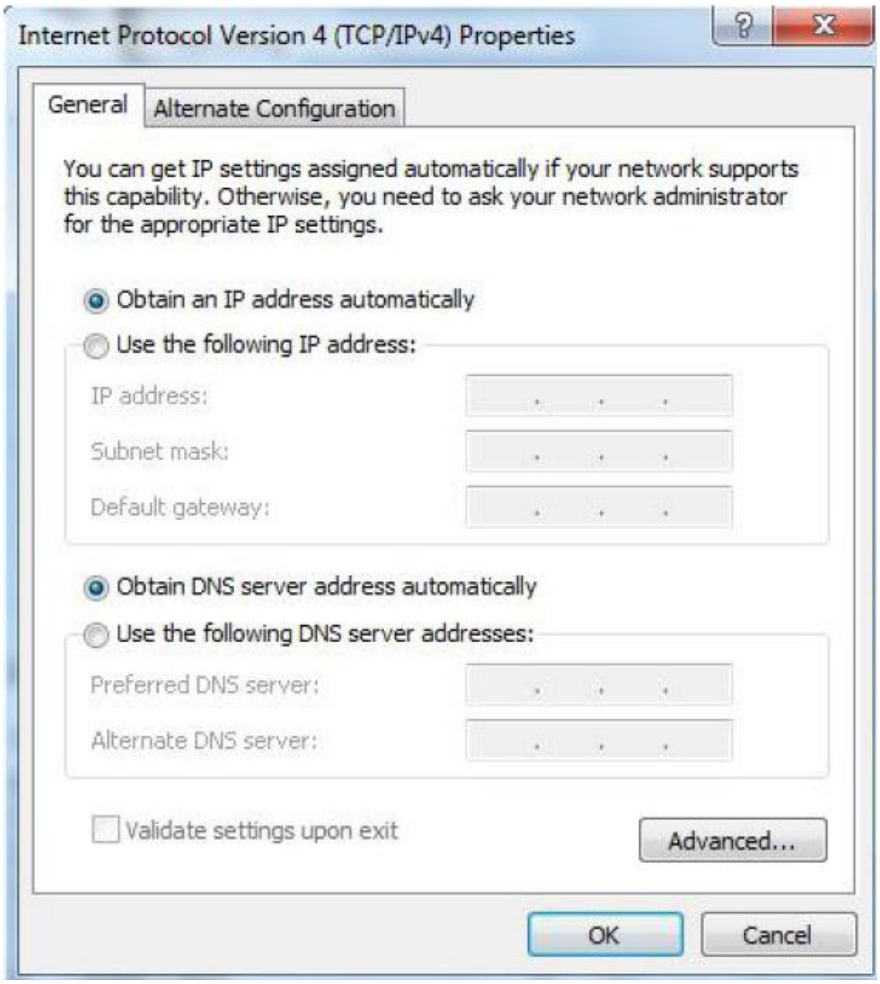


3. Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".

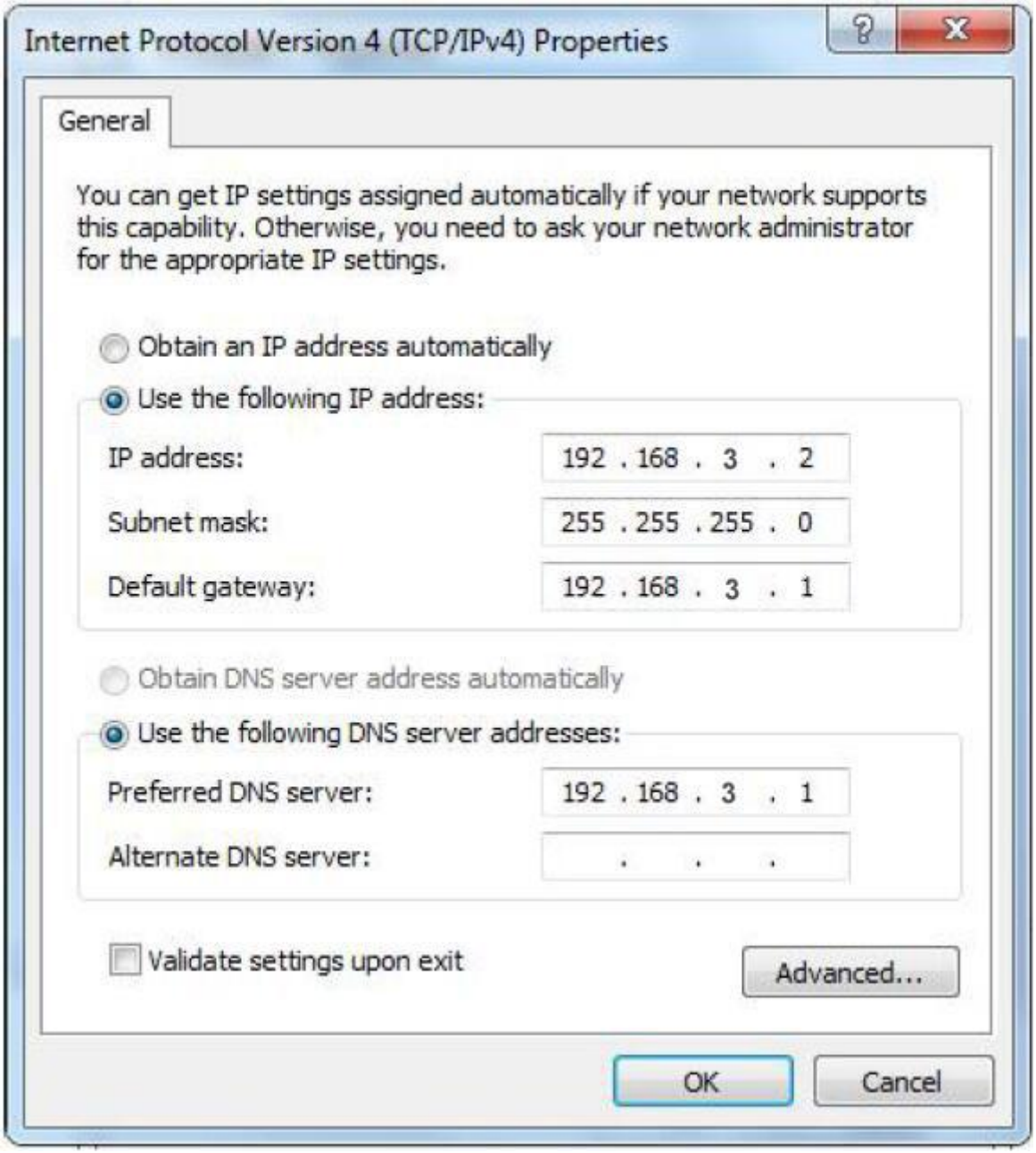


4. Two ways to configure the IP address:

Obtain an IP address automatically from the DHCP server and click "Obtain an IP address automatically";



Manually configure the PC with a static IP address on the same subnet as the router address, click and configure"Use the following IP address".



5. Click "OK" to complete the configuration.

4.2 Connect Router by WiFi

Step1: Search wireless network: The network name default is King-xxxxxx, no password.

Step2: Click “connect” to establish a connection.

4.3. Factory Default Settings

Before logging the configuration page, please check the default settings as below:

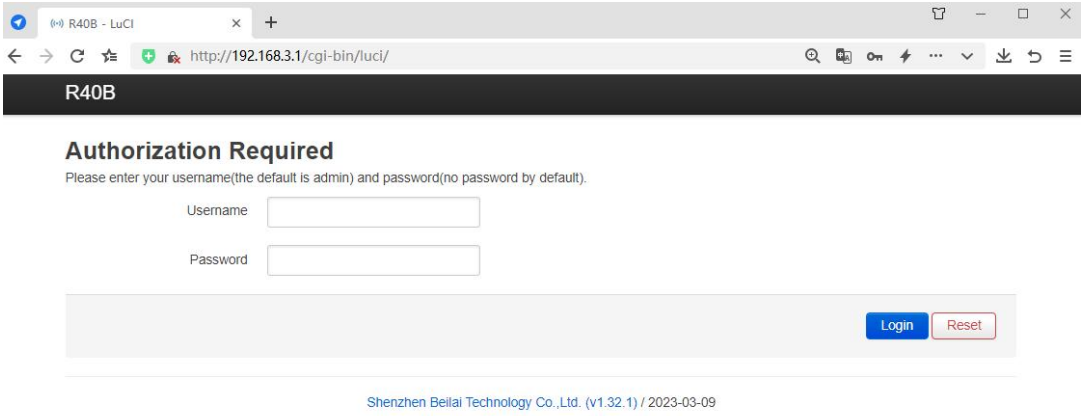
Item	Description
Login IP address	192.168.3.1
User name	admin
Password	none
DHCPserver	open
WIFI	SSID：King-xxxxxx KEY : No encryption (open network)

4.4. Login configuration page on WEB browser

1) After connecting to the router by wired or wireless operation, open a browser on the PC, such as IE, Edge, Google and other browsers;

2) Enter the router's IP address 192.168.3.1 on the address bar of the browser to enter the login page;

3) On the login page, enter the user name admin (default), no password (default), and then click the "Login" button.

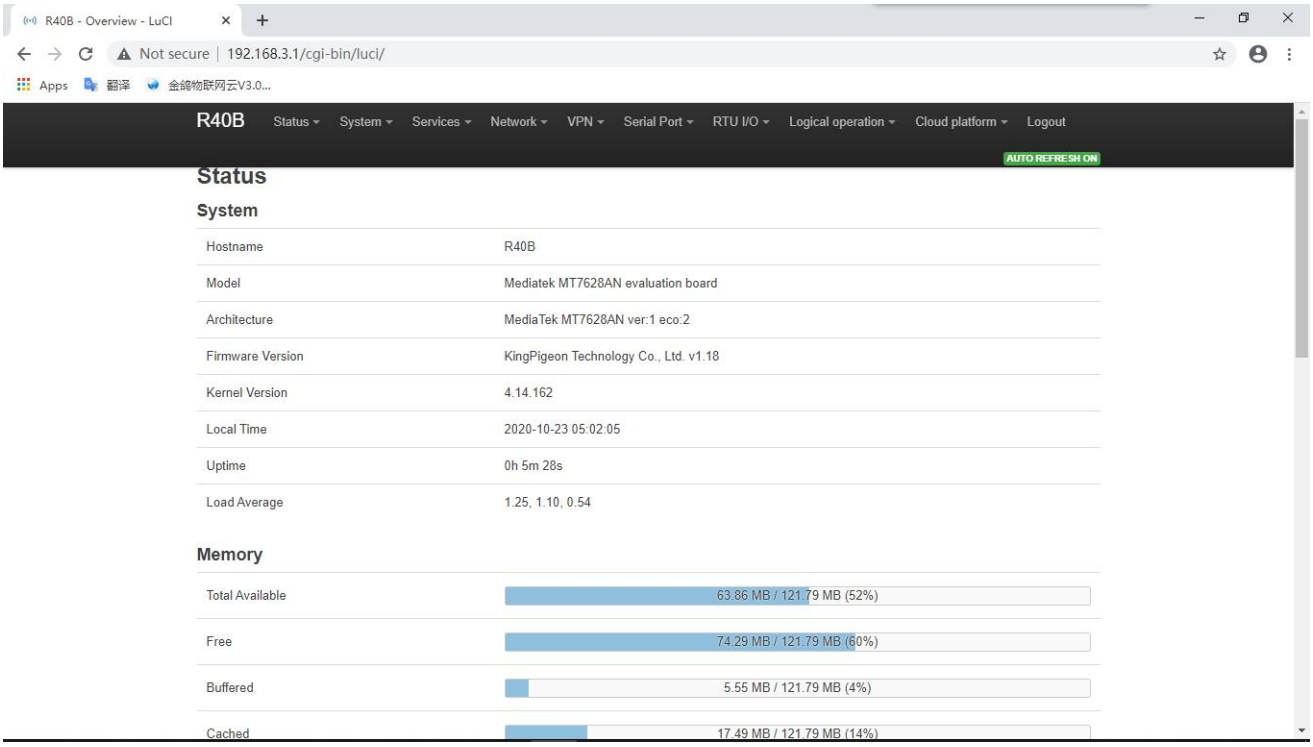


4) After successfully logging in to the router, you will enter the status overview page.

5) Note that after configuring the parameters, you need to click "Save and Apply" on the interface to take effect.

5. Configue Router Settings

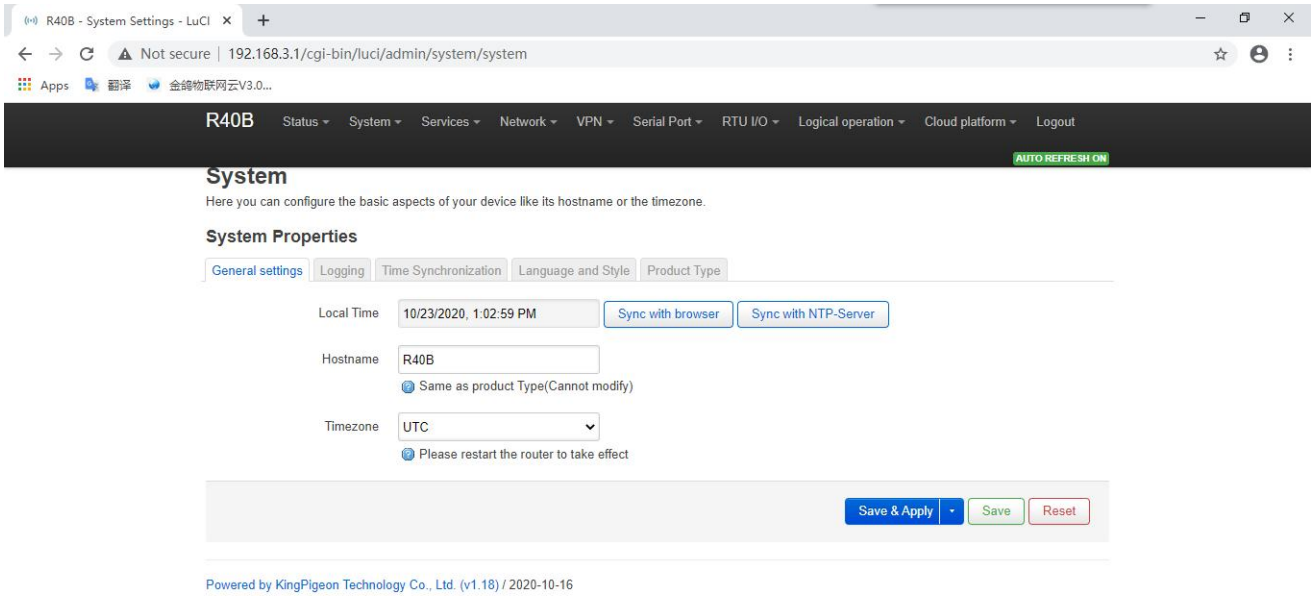
5.1 Status



In the status, it provides an overview, firewall, routing table, system log, kernel log, real-time information, etc., which is convenient for viewing the running status information of the router.

5.2. System

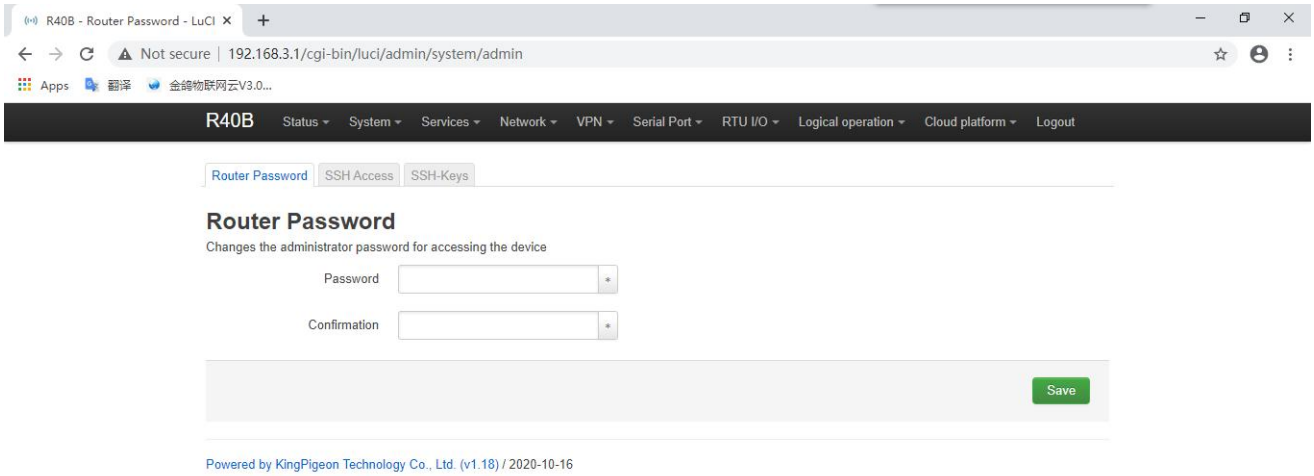
5.2.1 System Properties



Configure basic information , such as host name or time zone

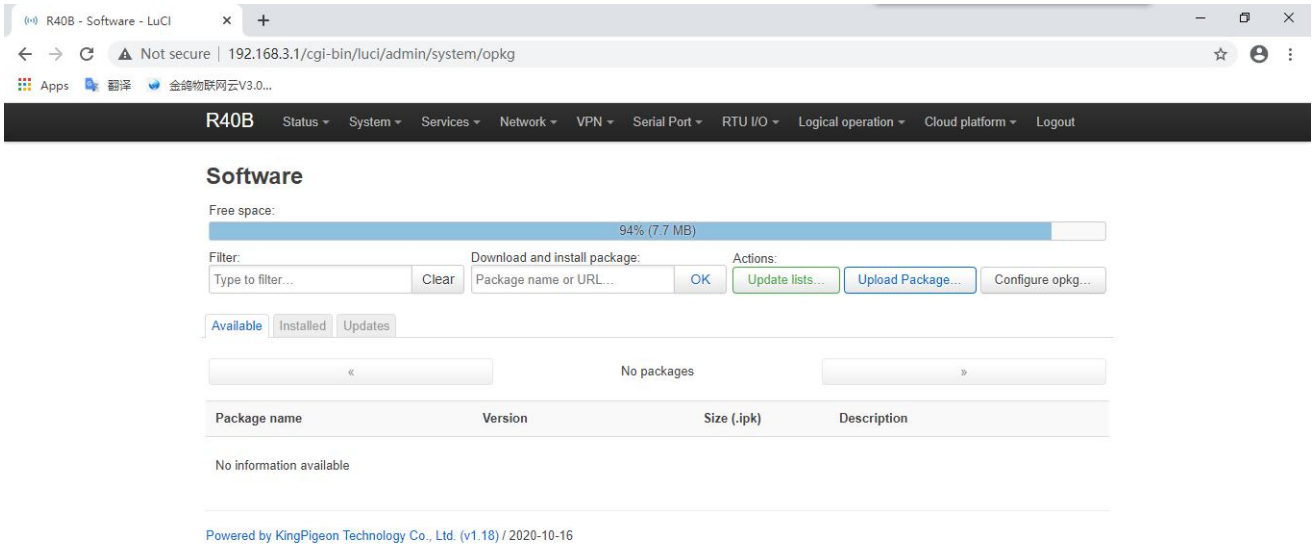
System Properties		
Item		**Description**
General setting	Local time	Set router time, can synchronize browser time or synchronize NTP server time
	Host name	Default is the router model, cannot be modified
	Time zone	Please select your region
Logging		Log properties, it is not recommended to modify
Time synchronization		Set NTP server for time synchronization
Language and style		Language optional automatic (according to browser language changes, only recognize Chinese and English), Chinese, English; The theme cannot be modified.
Product type		Product model, factory cured, cannot be modified

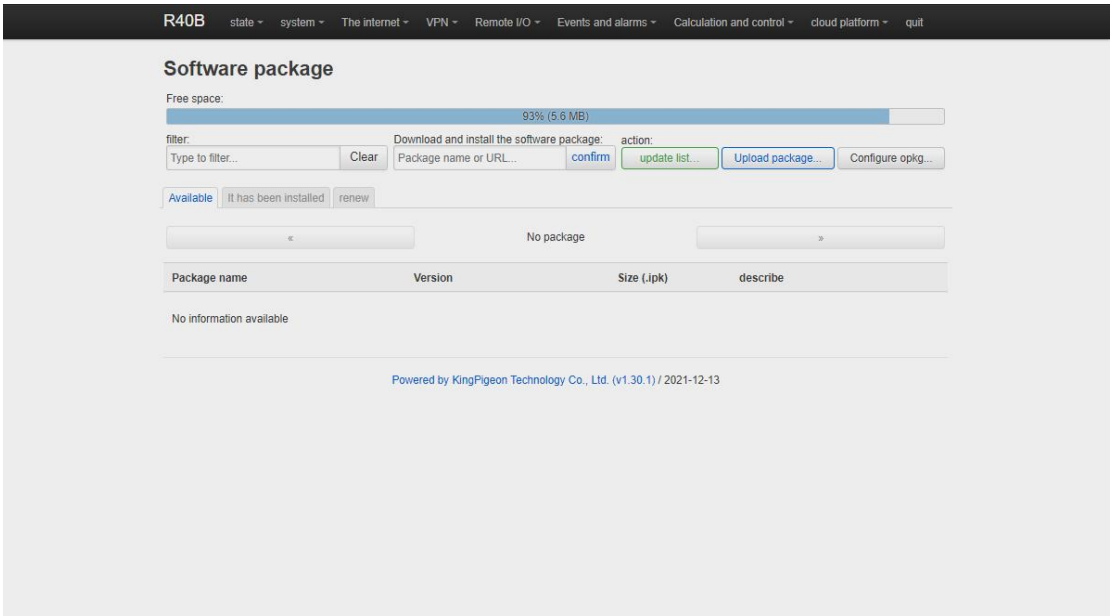
5.2.2 Management Rights



Management Rights	
Item	**Description**
Password	Change the administrator password to access the device
SSH access	Provides SSH access and SCP services
SSH keys	Compared with the use of ordinary passwords, the public key allows passwordless SSH login with higher security. 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

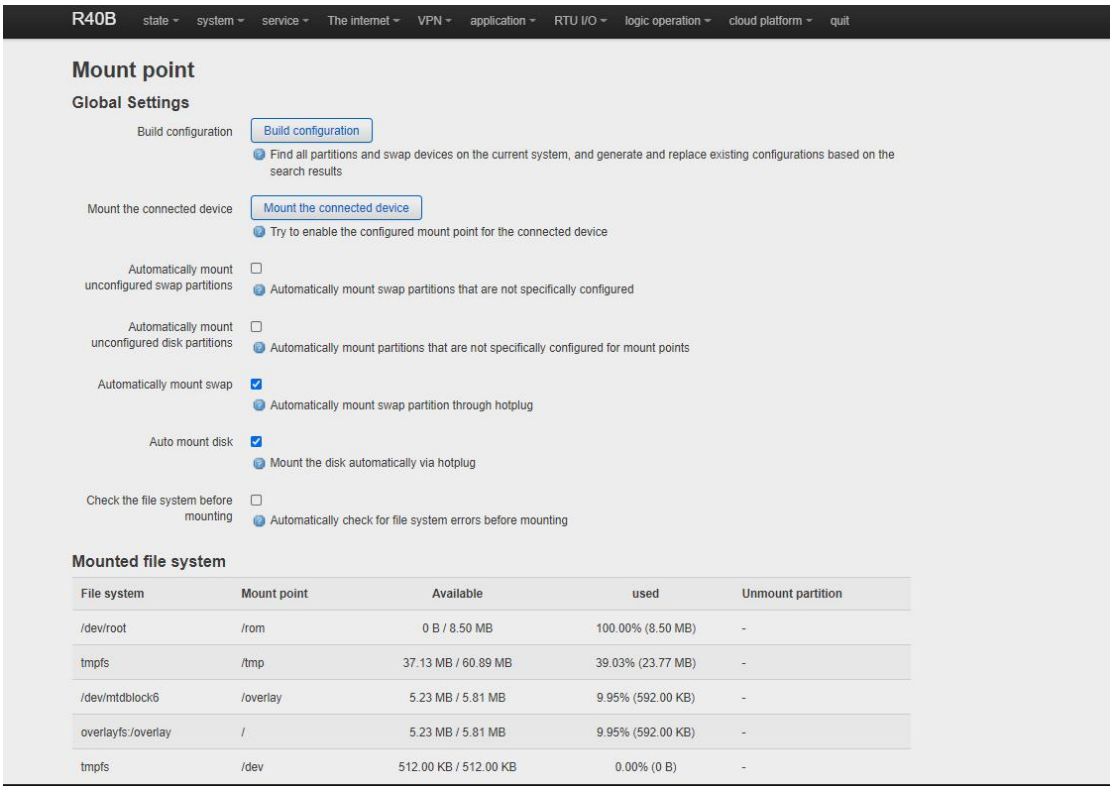


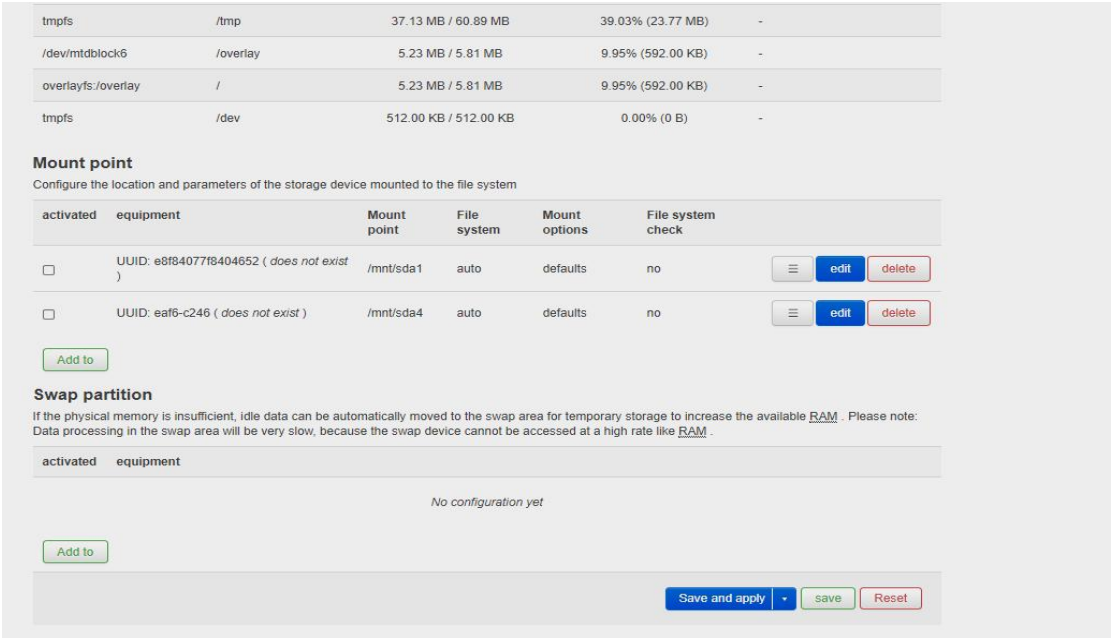


Software installation, clear, and upgrade. (Note: This function is for professionals!)

5.2.4 Support external storage

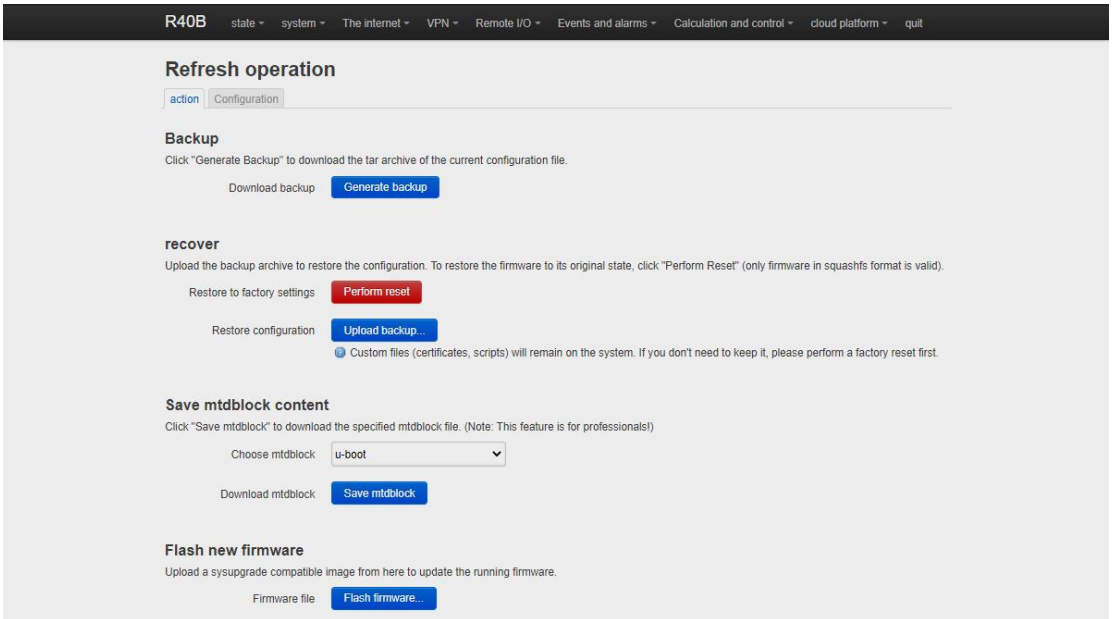
The mount point is used to support external storage devices, such as U disk, mobile hard disk, etc., click Generate configuration and mount the connected device, the partition of the storage device can be mounted in the system /mnt directory by default. For example, the U disk has two partitions sda1 and sda2. After mounting, the contents of the two partitions appear in the /mnt/sda1 and /mnt/sda2 directories under the system, which can be accessed by setting the shared directory through Services -> Network Sharing. The file system of the storage device supports NTFS, EXT4, FAT32 and other formats, and it needs to be partitioned and formatted before use.





Provide secondary development . (Note: This is for professionals)

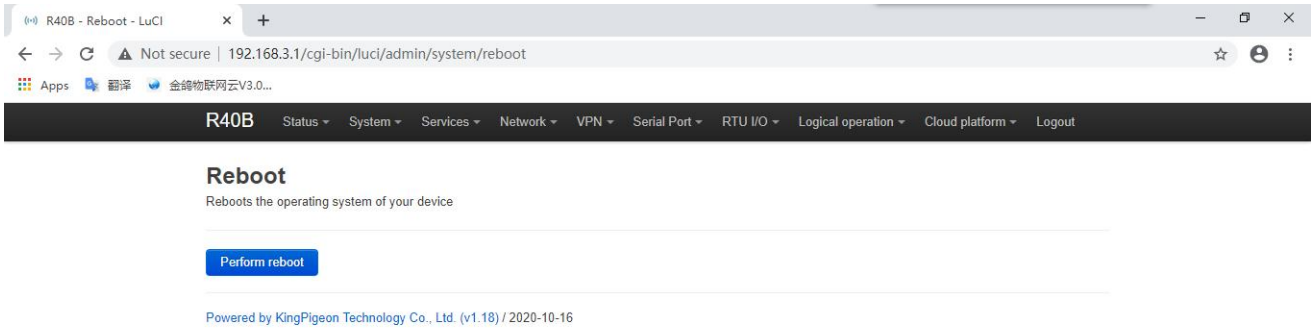
5.2.5 Backup/Upgrade



Backup/Upgrade	
Item	**Description**
Backup	Click "Generate Backup" to download the tar archive of the current configuration file.
Restore	Upload a backup archive to restore the configuration. To

	restore the firmware to its initial state, click "Perform Reset" (only squashfs format firmware is valid)
Save mtdblock content	Click "Save mtdblock" to download the specified mtdblock file. (Note: This function is for professionals!)
Flash new firmware	Upload a sysupgrade compatible image from here to update the running firmware

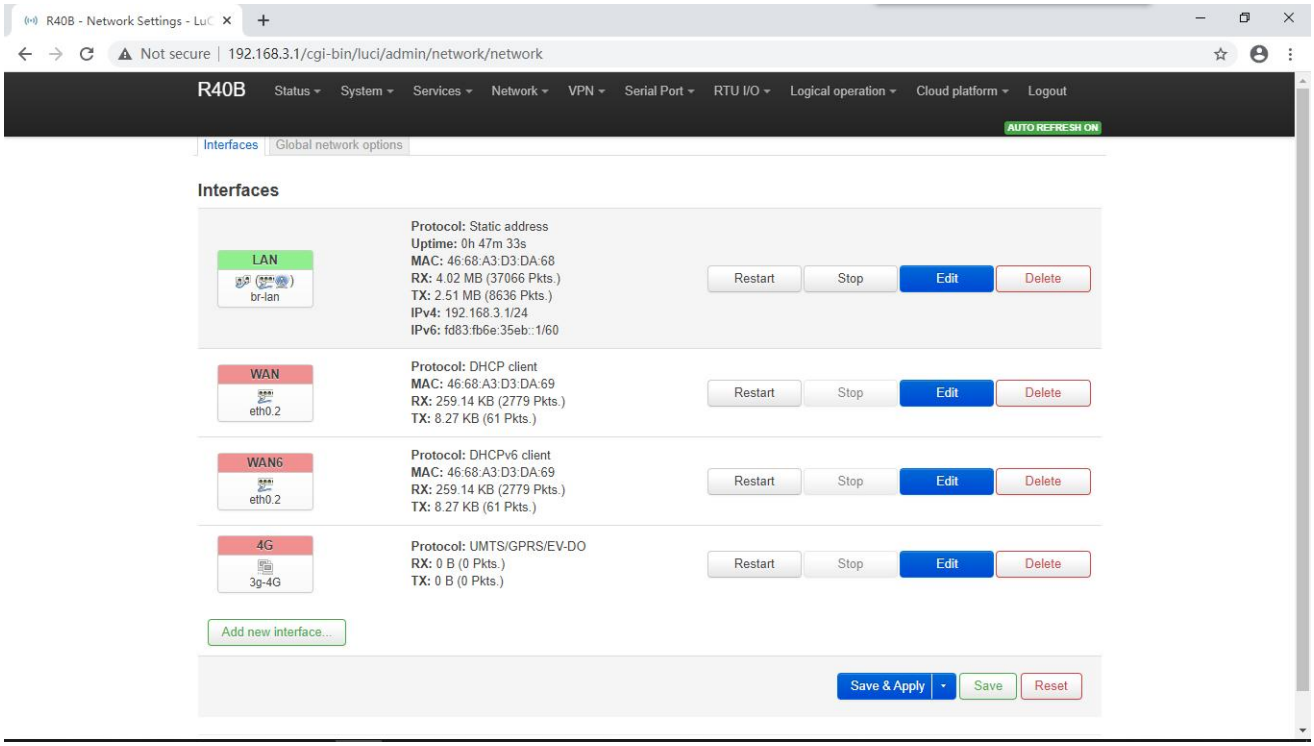
5.2.6 Reboot



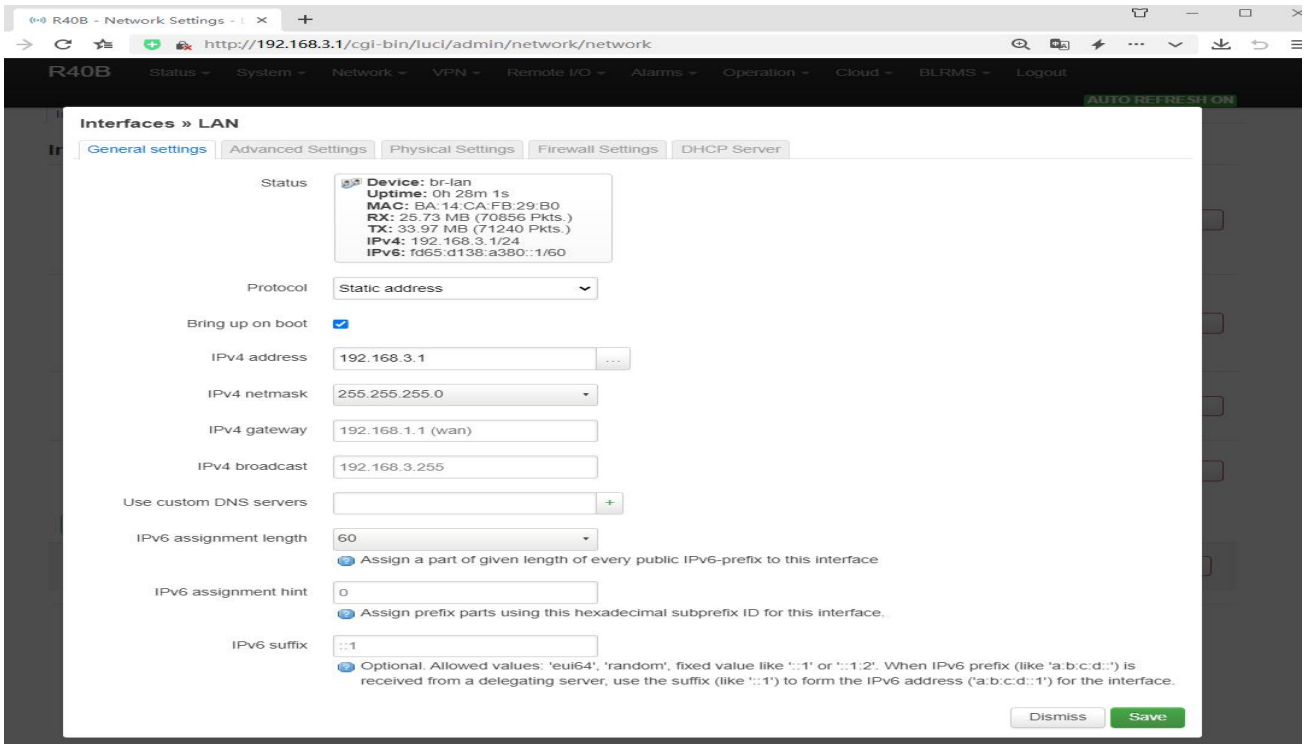
5.3 Network

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

You can restart, close, edit, and delete existing interfaces, or add new interfaces. Default has LAN, WAN, WAN6, 4G and other interface configurations . Click "Edit" to enter the detailed configuration modification.



5.3.1.1 LAN port

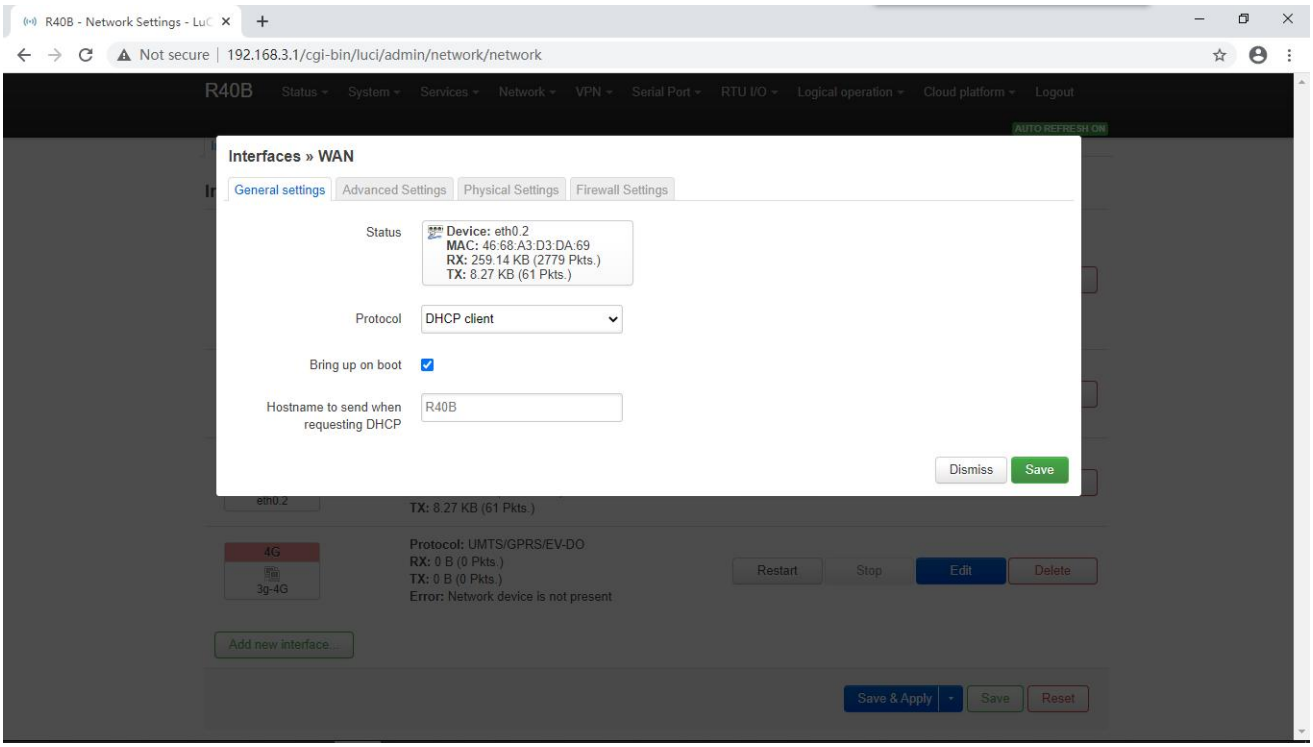


LAN Port		
Item		**Description**
Basic Setting	Status	Device: br-lan Running time: 8h 57m 16s MAC: E2:2F:C4:54:93:BA

		Receive: 18.81 MB (149126 data pack) Send: 99.87 MB (132321 data pack) IPv4: 192.168.3.1/24 IPv6: fdb2:428b:ddbe::1/60
	Protocol	Static address
	Bring up on boot	Default enable
	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 netmask	Default 255.255.255.0
	IPv4 gateway	Default is empty, when multiple IPv4 addresses are set, the gateway address needs to be specified
	IPv4 broadcast	Default 192.168.3.255
	Use custom DNS server	Default is empty
	IPv6 allocation length	Assign a given length part of each public IPv6 prefix to this interface, default 60
	IPv6 assignment tips	Assign this hexadecimal sub-ID prefix to this interface
	IPv6 suffix	Optional, allowed values: "eui64", "random" and other fixed values (for example: "::1" or "::1:2"). When the IPv6 prefix (such as "a:b:c:d::") is obtained from the authorization server, use the suffix (such as "::1") to synthesize an IPv6 address ("a:b:c:d::1") Assigned to this interface.
Advanced settings	Use built-in IPv6 management	Default enable
	Mandatory link	Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing). default is enable.
	Reset MAC address	Modify MAC address
	Reset MTU	Default 1500
	Use Gateway Hop	Default 0
Physical settings	Bridge interface	Create a bridge for the specified interface, default is enable.
	Enable STP	Enable spanning tree protocol on this bridge, default is disable.

	Enable IGMP sniffing		Enable IGMP snooping on this bridge, default is disable
	Interface		Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified
Firewall settings	Create/Assign firewall zone		Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it.
DHCP server	Basic Setting	Ignore this interface	DHCP service is not provided on this interface, default is disable
		Start	Start network address, default is 100.
		Customers	Maximum number of address assignments. The default is 150.
		Lease term	The expiration time of the leased address is at least 2 minutes (2m). The default is 12h.
	Advanced settings	DHCP	Provide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.
		Forcibly	Even if another server is detected, it is mandatory to use DHCP on this network,default is disable.
		IPv4 Subnet mask	Reset the subnet mask sent to the client.
		DHCP Options	Set additional options for DHCP, for example, setting "6,192.168.2.1,192.168.2.2" means to announce different DNS servers to clients.
	IPv6 setting	Route Advertisement Service	Default server mode
		DHCPv6 server	Default server mode
		HDP proxy	Default disable
		DHCPv6 mode	The default is stateless + stateful
		Always advertise the default route	Even if there is no public network prefix available, it still advertises itself as the default route,default is disable
		Advertised DNS server	Default is empty
		Advertised DNS domain name	Default is empty

5.3.1.2 WAN port

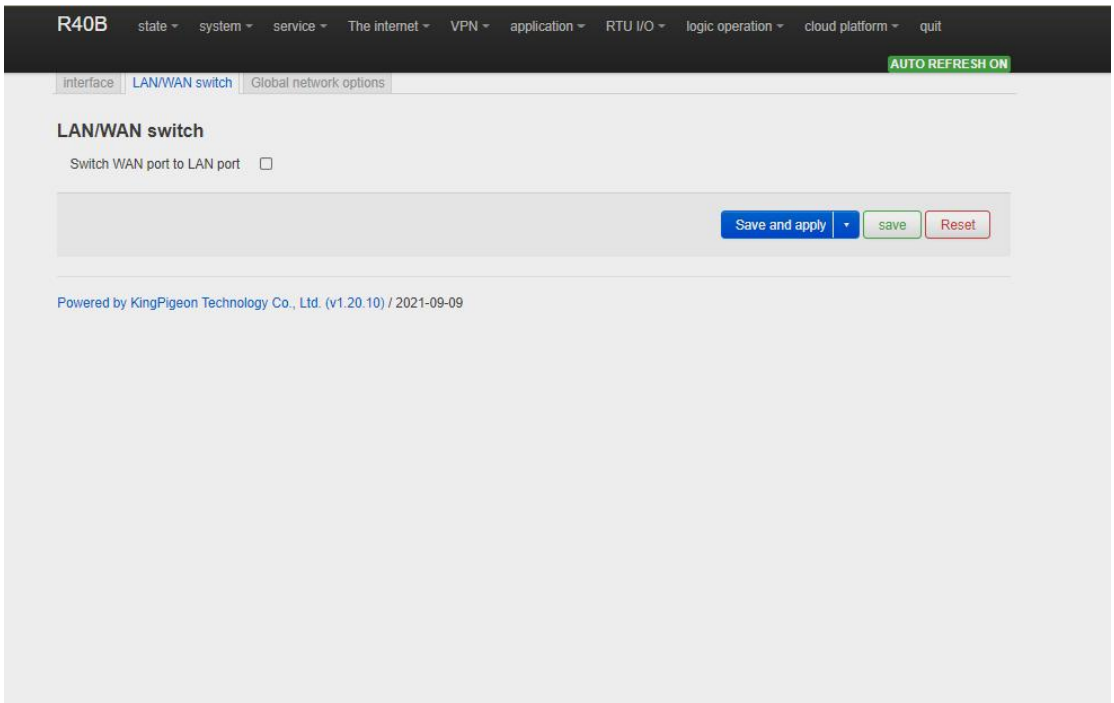


WAN Port		
Item		**Description**
General Setting	Status	Device: eth0.2 Running time: 9h 37m 16s MAC: E2:2F:C4:54:93:BB Receive: 113.65 MB (290226 data pack) Send: 19.02 MB (137282 data pack) IPv4: 192.168.1.173/24
	Protocol	Default DHCP client; If the WAN port connected newwork requires an account and password to log in, please select the PPPoE protocol
	Bring up on boot	Default is enable
	Hostname sent when requesting DHCP	Default is product model
Advanced settings	Use built-in IPv6 management	Default is enable
	Mandatory link	Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing). Default is disable.
	Use broadcast tags	Needed by some ISPs, for example: coaxial network DOCSIS 3, default is disable.
	Default gateway	Leave blank to not configure the default route,

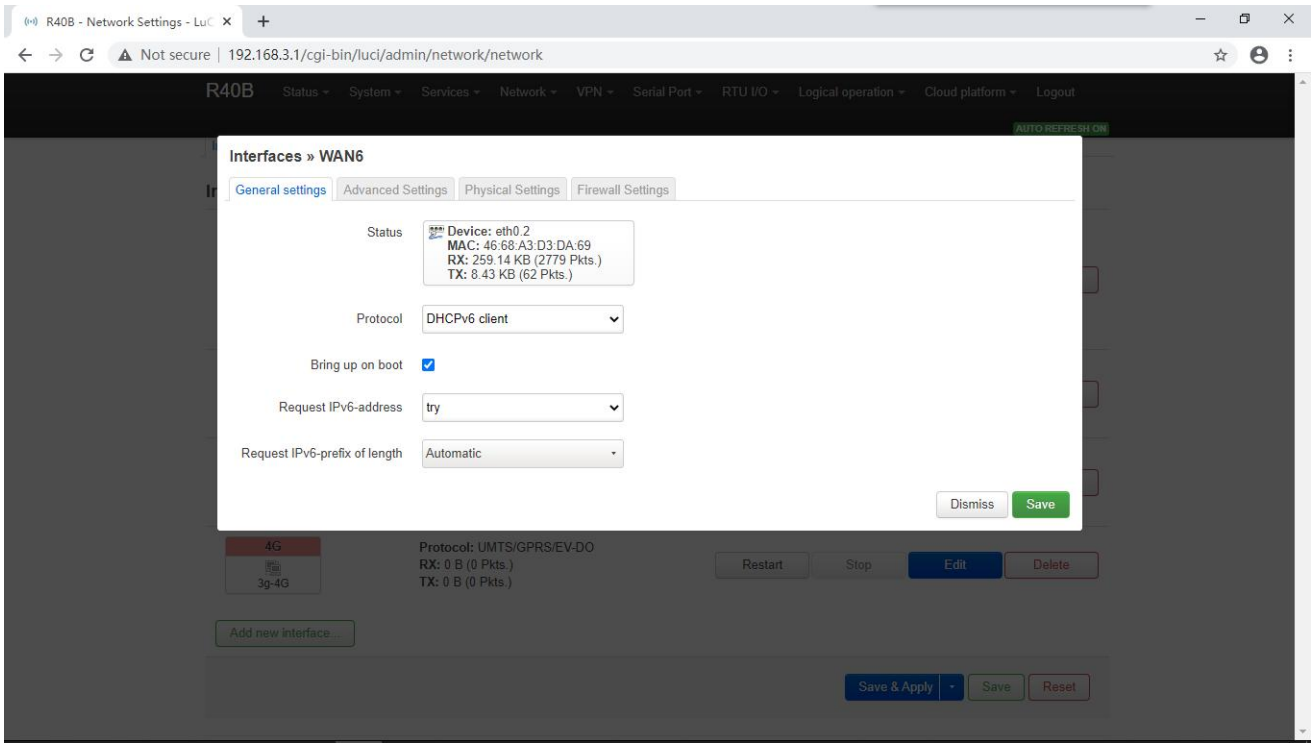
		default is enable.
	Obtain DNS server automatically	Leave blank to ignore the advertised DNS server address,default is enable.
	Use Gateway Hop	Default is empty
	Client ID sent when requesting DHCP	Default is empty
	Vendor Class option sent when requesting DHCP	Default is empty
	Reset MAC address	Modify MAC address
	Reset MTU	Default is 1500
Physical settings	Bridge interface	Create a bridge for the specified interface,default is disable
	Interface	Switch VLAN: "eth0.2" (wan, wan6), set which physical interface to use, generally do not need to be modified
Firewall settings	Create/Assign firewall zone	Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation 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.



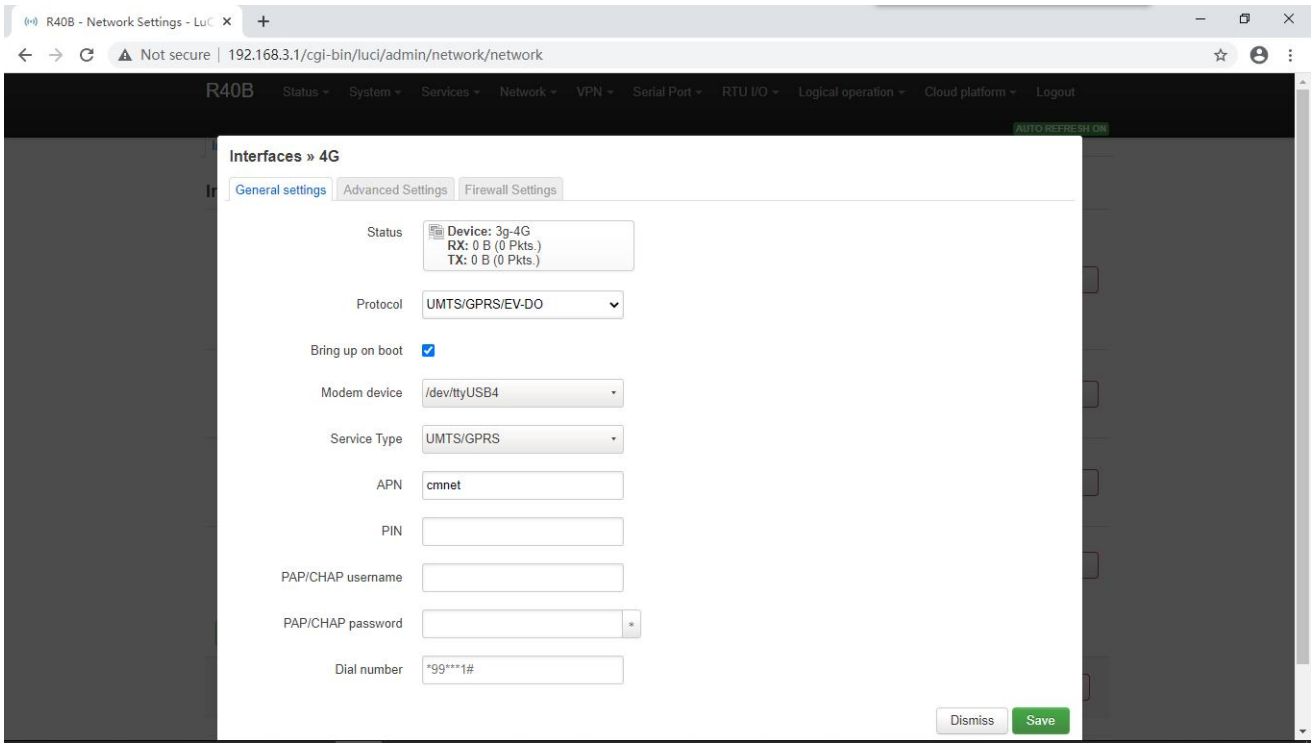
5.3.1.4 WAN6 Port



WAN6		
Item		Description
Basic Setting	Status	Device: eth0.2 MAC: E2:2F:C4:54:93:BB Receive: 115.31 MB (299495 data pack) Send: 19.41 MB (140798 data pack)
	Protocol	Default DHCPv6 client
	Bring up on boot	Default is enable
	Request IPv6 address	Default is try
	Request IPv6 prefix of length	Default automatic
Advanced settings	Use built-in IPv6 management	Default enable
	Mandatory link	Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing). Default is disable.
	Use default gateway	Leave blank to not configure the default route
	Custom assigned IPv6 prefix	Default is empty
	Obtain DNS server automatically	Leave blank to ignore the advertised DNS server address, default is enable.
	Client ID sent when requesting DHCP	Default is empty

	Reset MAC address	Modify MAC address
	Reset MTU	Default 1500
Physical settings	Bridge interface	Create a bridge for the specified interface, default is disable.
	Interface	Switch VLAN:"eth0.2"(wan,wan6)
Firewall settings	Create/Assign firewall zone	Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it.

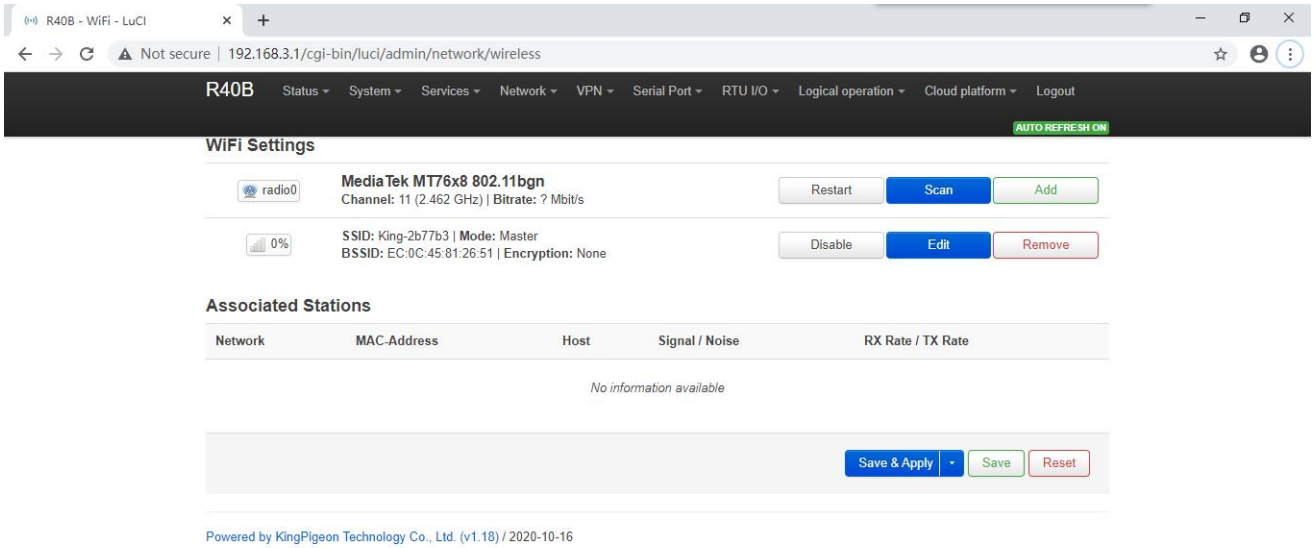
5.3.1.5 4G Port



4G		
Item		**Description**
Basic Setting	Status	Device: 3g-4G Running time: 0h 11m 52s Receive: 1.06 KB (18 data pack) Transmit: 8.50 KB (36 data pack) IPv4: 10.94.92.16/32
	Protocol	UMTS/GPRS/EV-DO
	Bring up on boot	Default is enable
	Modem equipment	Default/dev/ttyUSB4
	Service type	Default UMTS/GPRS
	APN	SIM Card Internet access point
	PIN	SIM card PIN code

	PAP/CHAP uernamе	User name for PPP authentication
	PAP/CHAP password	Password for PPP authentication
	Dial number	SIM Card Internet dialing
Advanced settings	Use built-in IPv6 management	Default is enable
	Mandatory link	Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing), Default is disable.
	Obtain IPv6 address	Default auto
	Modem initialization timeout	The maximum waiting time for the modem to be ready (seconds), default 10
	Use default gateway	Leave blank to not configure the default route, default is enable.
	Use Gateway Hop	Default is empty
	Obtain DNS server automatically	Leave blank to ignore the advertised DNS server address,default is enable.
	LCP Response failure threshold	After the specified number of LCPs respond to the fault, it is assumed that the link has been disconnected. 0 means ignore the fault, and the default is 0.
	LCP Response interval	LCP response is sent regularly (seconds), which is only valid when the fault threshold is combined, the default is 5
	Activity timeout	Close the inactive link after a given time (seconds), 0 is to keep the connection, the default is 0
Firewall settings	Create/Assign firewall zone	Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it.

5.3.2 WiFi (AP mode or WLAN Client)

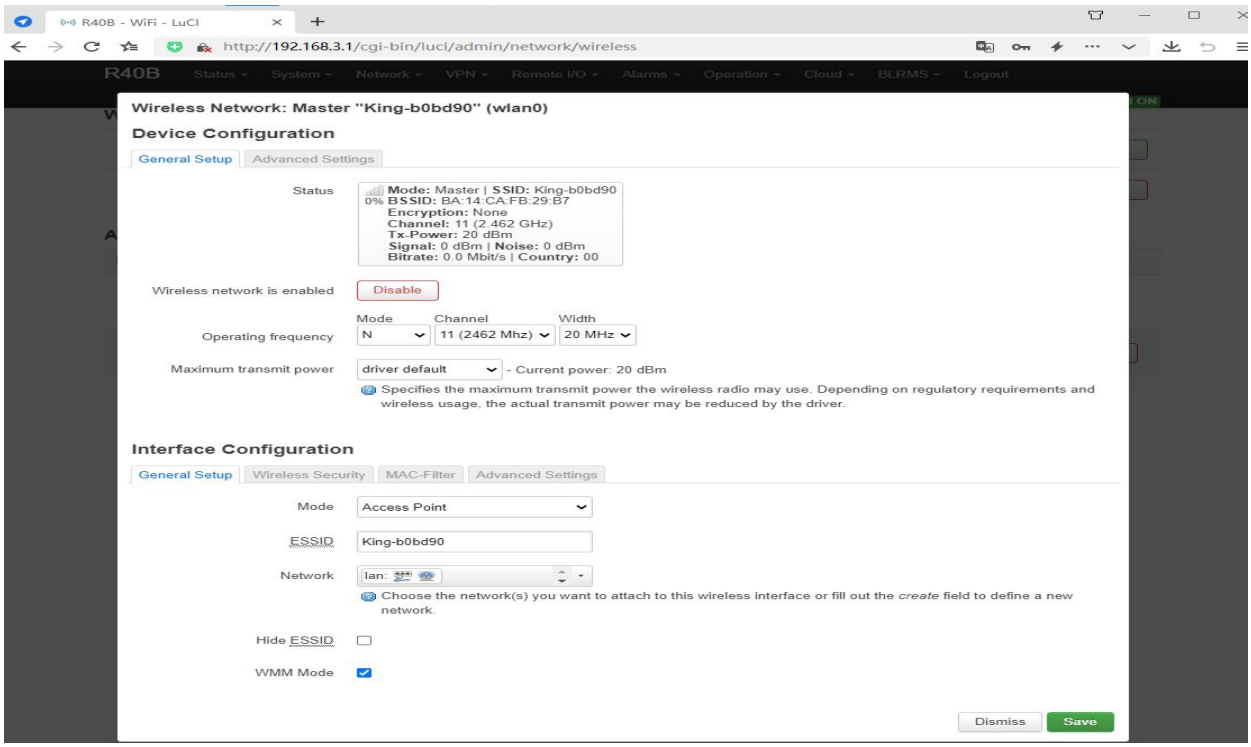


Supports both WLAN hotspot and WLAN client.

The wireless overview shows the current wireless status, you can click Edit to enter the detailed configuration, or restart, scan, add, disable, remove, etc.

Connected stations shows the currently connected wireless stations, which can be disconnected.

5.3.2.1 WLAN Hotspot (WiFi AP mode)



The default SSID is King-xxxxxx, no encryption method, other clients can directly search the wireless network to connect to this hotspot.
Quick configuration: Select the wireless configuration in Master mode in the wireless profile, 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" can modify the encryption method to set the WiFi password.

Note: When using the WiFi connection to enter the router configuration, you need to select "Force Application" to modify the WLAN hotspot configuration. Please click the drop-down button next to "Save and Apply" and select "Force Apply".

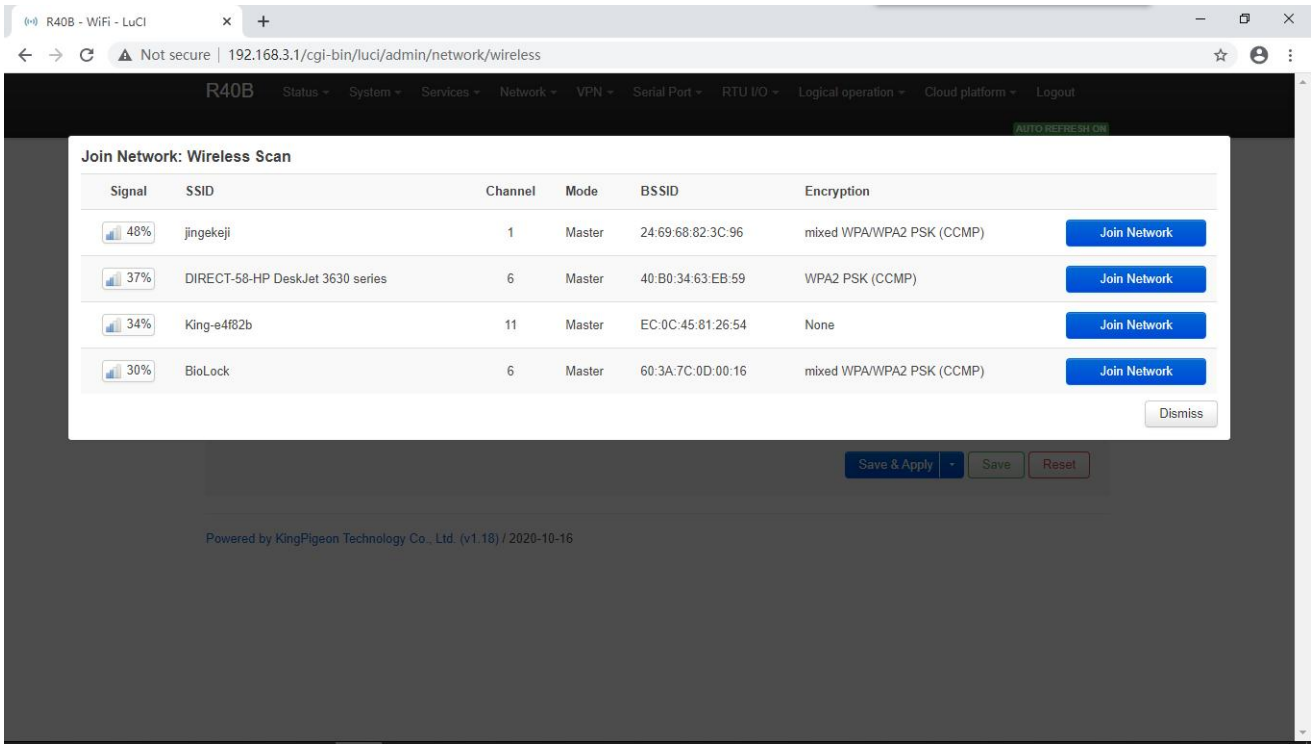
Wireless network AP hotspot device configuration		
Item		**Description**
General Setup	Status	97% Mode: Master | SSID: King-ff4a8a BSSID: EE:0C:45:81:26:51 Encryption: None Channel: 6 (2.437 GHz) Transmission power: 20 dBm Signal: -42 dBm | Noise: 0 dBm Transmission rate: 58.5 Mbit/s | Country: 00
	Wireless network	Default is enable

	is enabled	
	Operating frequency	If there are too many devices in use at the current frequency, please change one
	Maximum transmit power	Specify the maximum transmit power. Depending on regulatory requirements and usage, the driver may limit the actual transmit power below this value.
Advanced settings	Country code	Driver default
	Allow traditional 802.11b rate	Default is enable
	Distance optimization	The distance (meter) of the furthest network user. Automatic by default, automatically adjust the transmission power according to the distance
	Fragmentation threshold	Automatically send data when the data length exceeds the threshold, generally use the default value
	RTS/CTS Threshold	Request to send/allow sending protocol. When the data length exceeds the threshold, start the protocol to avoid signal conflicts caused by multiple terminals sending data to the AP. Usually use default value
	Force 40MHz mode	Even if the auxiliary channels overlap, the 40MHz channel is always used. Using this option is not compliant with IEEE 802.11n-2009! Default is disable.
	Beacon interval	Indicates the interval at which the wireless router periodically broadcasts its SSID. Usually use default value.

Wireless network AP hotspot interface configuration		
Item		**Description**
Basic Setting	Mode	Access Point
	ESSID	Default King-xxxxxx（xxxxxx is Random numbers or letters）
	Network	lan
	Hide ESSID	Default is disable
	WMM mode	Wi-Fi Multimedia,providing different priorities for different services to ensure service quality,default is enable
Wireless security	Encryption	No encryption by default (open network)
MAC filter	MAC address filter	Default is disable
Advanced settings	Isolate the client	Forbid communication between clients, default is disable
	Interface name	Reset the default interface name
	Short Preamble	Different rates need to use different Preamble (preamble),default is enable
	DTIM interval	As a terminal node, periodically wake up to send traffic indication message interval
	Interval for re-encrypting GTK	Temporary key (GTK), Use default

	Disable inactive polling	Default is disable
	Inactive site restrictions	Default 300 seconds
	Max allowed listening interval	Default Max 65535
	Disconnect on low Ack response	Allow AP mode to disconnect wireless terminal under low ACK,default is enable.

5.3.2.2 WLAN Client



Please click "Scan" to search the wireless network, select "Join Network" to enter the quick configuration page, if a password is required, enter the WiFi password in "WPA Key", then click "Submit" to enter the detailed configuration page, and finally click "Save" .

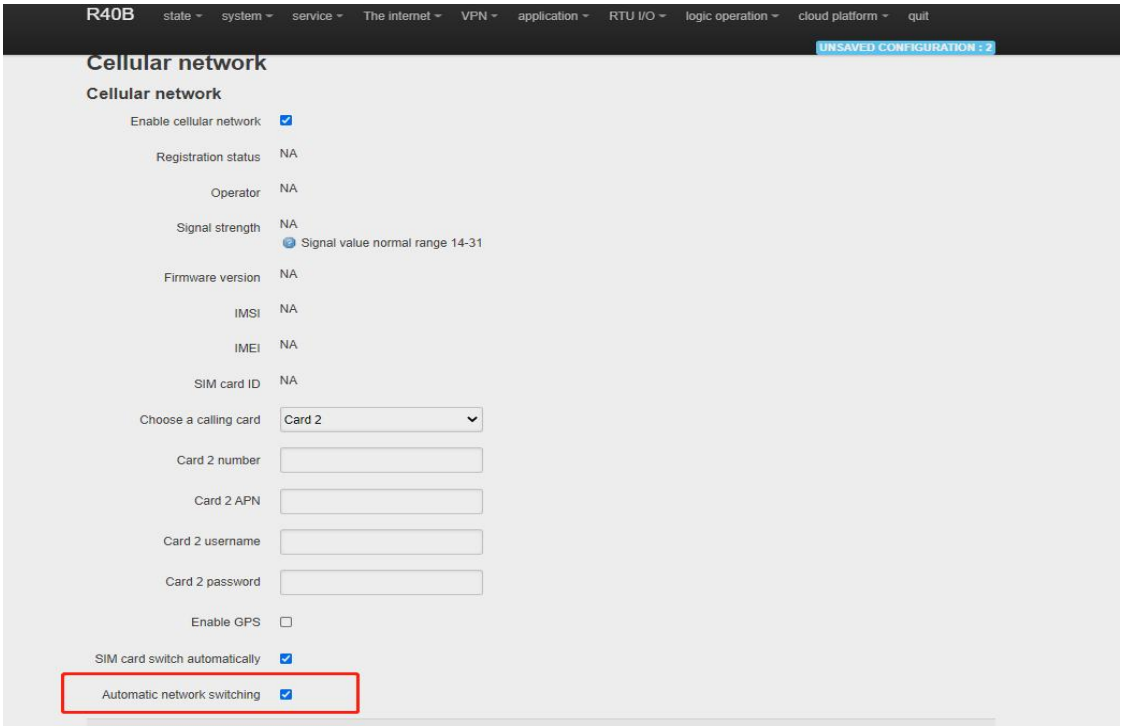
Device Configuration		
Item		Description
Basic Setting	Status	100% Mode: Client | SSID: jingekeji BSSID: EC:0C:45:81:26:51 Encryption: WPA2 PSK (CCMP) Channel: 6 (2.437 GHz) Transmission power: 20 dBm Signal: -38 dBm | Noise: 0 dBm Transmission rate: 1.0 Mbit/s | Country: 00
	Wireless network is enabled	Default is enable

	Working frequency	If there are too many devices in use at the current frequency, please change one
	Max transmission power	Specify the maximum transmit power. Depending on regulatory requirements and usage, the driver may limit the actual transmit power below this value.
Advanced settings	Country code	Driver default
	Allow traditional 802.11b rate	Default is enable
	Distance optimization	The distance (meter) of the furthest network user. By default, the transmission power is automatically adjusted according to the distance
	Fragmentation threshold	Automatically send data when the data length exceeds the threshold,usually use default value.
	RTS/CTS Threshold	Request to send/allow to send protocol. When the data length exceeds the threshold, start the protocol to avoid signal collision caused by multiple terminals sending data to the AP, usually use default value.
	Force 40MHz mode	Even if the auxiliary channels overlap, the 40MHz channel is always used. Using this option is not compliant with IEEE 802.11n-2009! default is disable.
	Beacon interval	Indicates the interval at which the wireless router periodically broadcasts its SSID, usually use default value.

Interface configuration		
Item		**Description**
Basic Setting	Mode	Client
	ESSID	Wireless network name
	BSSID	none
	Network	Wwan, no need modify it
Wireless security	Encryption	WPA2-PSK（Strong security）
	Algorithm	auto
	Password	Wireless network password
	802.11w Management Frame Protection	Requires the full version of wpad/hostapd, and WiFi driver support, default is disabled
	Interface name	Reset the default interface name
	Short Preamble	Different rates require different Preambl (preamble), default is enable
	DTIM interval	As a terminal node, periodically wake up to send traffic indication message interval
	Re-encrypt GTK time interval	Temporary key (GTK) Use default value
	Disable inactive polling	Default is disable
	Inactive site restrictions	Default 300 seconds
	Maximum allowed	Default max 65535

	listening interval	
	Disconnect on low Ack response	Allow AP mode to disconnect wireless terminal under low ACK,default is enable

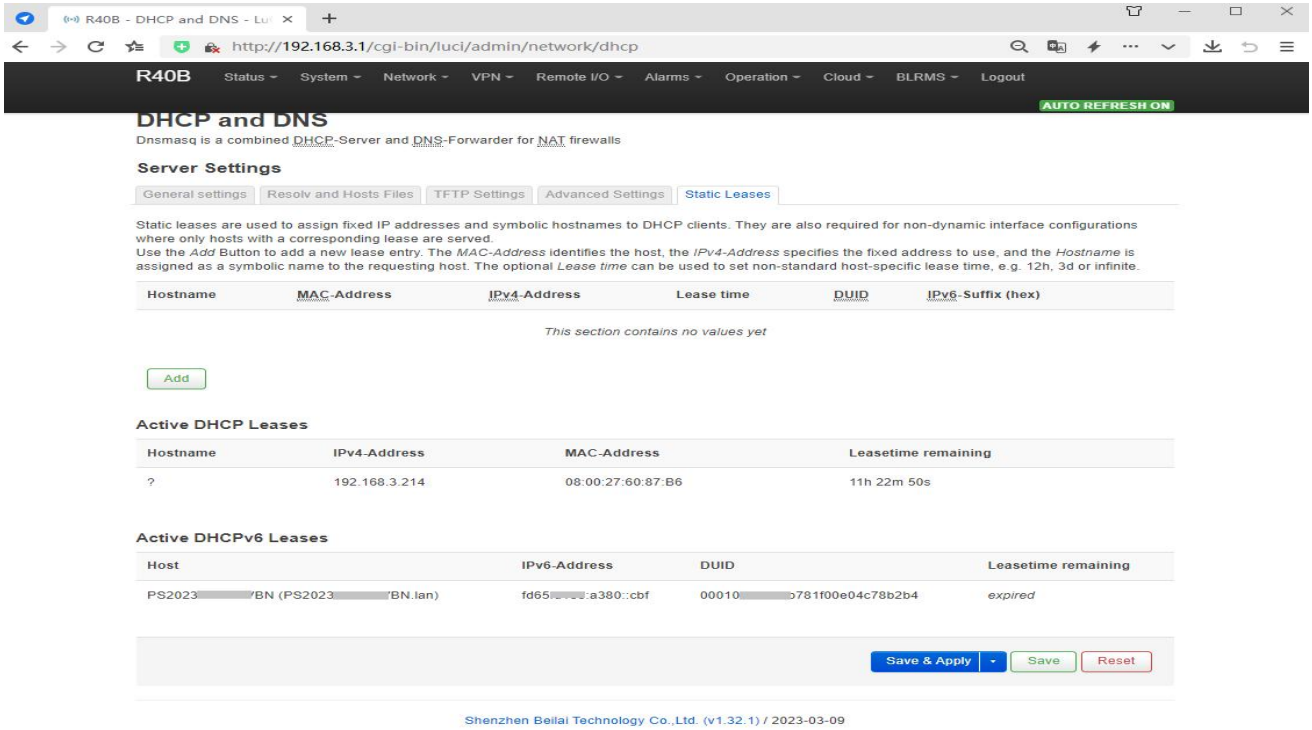
5.3.3 Cellular Network



Cellular Network	
Item	Description
Register status	Registered
Operator	N/A
Signal	Normally is 14-31
Firmware version	EC25AUGCR06A02M1G
IMSI	SIM card IMSI number
IMEI	Device IMEI number
SIM card ID	SIM card ICCID number
Card select	Card 1, Card 2, this selection as the preferred SIM card, When the preferred SIM card cannot be connected to the network, it will automatically switch to another card to try to connect to the network
Card 1 /2 number	Enter sim card 1 number
SIM card 1/2 APN	Enter APN
SIM card 1/2 username	Enter username
SIM card 1/2 password	Enter password

Enable GPS	Default is disable When the router 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



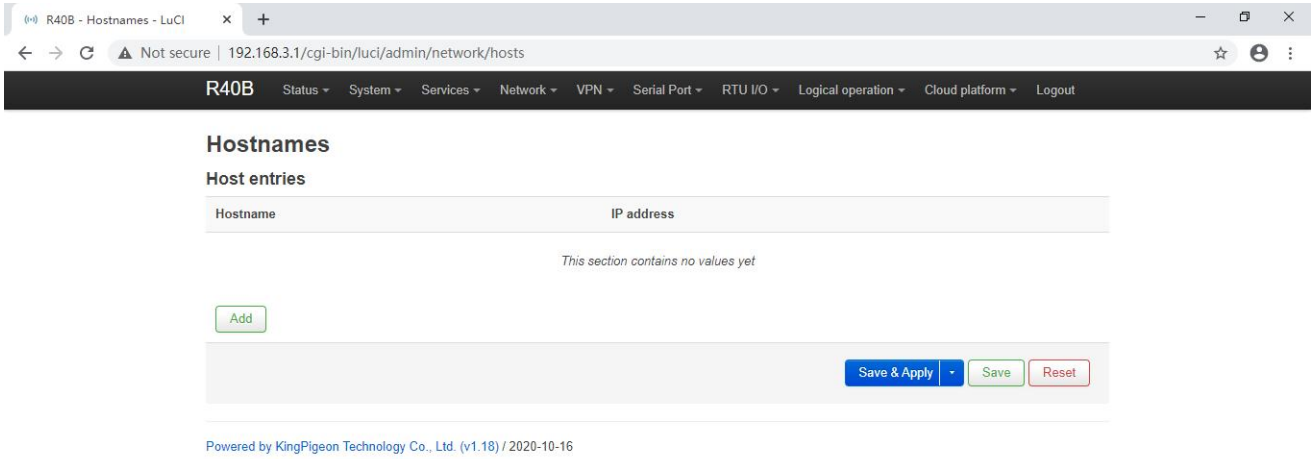
Dnsmasq provides an integrated DHCP server and DNS forwarder for the NAT firewall

Server Settings		
Item		Description
General Setting	Ignore empty domain name resolution	Do not forward resolution requests without DNS names, checked by default
	Unique authorization	This is the only DHCP server in the local network,default is enable
	Local server	Local domain rules. Names matching this domain are never forwarded, only resolved from DHCP or HOSTS files
	Local domain name	The local domain name suffix will be added to the DHCP and HOSTS file entries
	Record query log	Write received DNS request to system log,defaule is disable

	DNS forward	List of DNS servers to which requests are forwarded
	Rebinding protection	Discard RFC1918 upstream response data, default is enable
	Allow local	Allow upstream response within 127.0.0.0/8 loopback range, for example: RBL service, default is enable.
	Domain name whitelist	List of domain names that allow RFC1918 to respond
	Local service only	DNS service is only provided in the subnet to which the network card belongs,default is enable.
	Not all addresses	Dynamically bind to interface instead of wildcard address (recommended as linux default),default is enable
	Listening interface	Only listen to these interfaces and loopback interfaces.
	Exclude interface	Do not listen to these interfaces.
HOSTS& parse the file	Use etc/ethers Configuration	Configure DHCP server according to /etc/ethers,default is enable.
	Lease documents	The file used to store the assigned DHCP lease,default is :/tmp/dhcp.leases
	Ignore parsing file	Default is disable
	Ignore /etc/hosts	Default is disable
	Additional HOSTS file	Default is empty
TFTP setting	Enable TFTP server	Default is disable
Advanced settings	No log	Does not record general operation logs of these protocols,default is disable.
	Sequential allocation IP	IP addresses are assigned sequentially starting from the lowest available address, default is disable.
	Filter local packages	Reverse queries without forwarding the local network,default is enable.
	Filter useless packets	Do not forward requests that the public domain name server cannot respond,default is disable
	Localized query	If multiple IPs are available, the host name is localized according to the subnet from which the request originated,default is enable
	Expand the host suffix in the HOSTS file	Add the local domain name suffix to the domain name in the HOSTS file, default is enable
	Disable invalid information cache	Do not cache useless responses, for example: domain names that do not exist, default is disable
	Additional SERVERS file	This file may contain 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 range of the server.
	Strict order checking	Query DNS server in the order of "parse file",default is disable.
	All server	Query all available upstream DNS servers,default is disable.

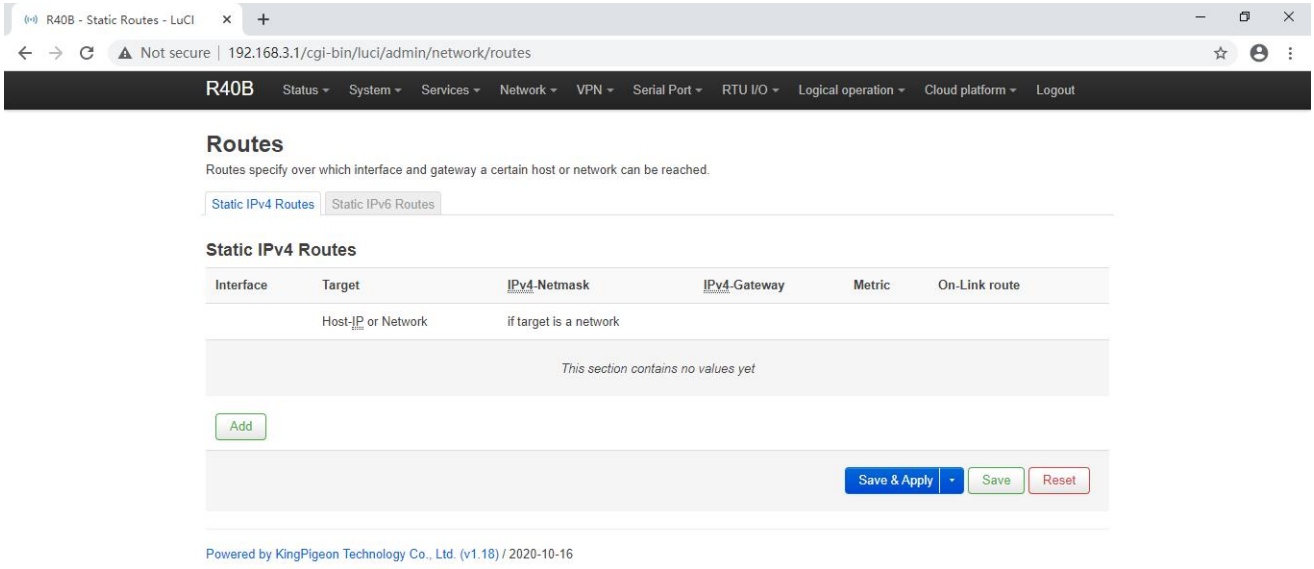
	Ignore fake empty domain name resolution	List of servers allowed to respond with fake empty domain names
	DNS server port	Inbound DNS query port
	DNS query port	Specified DNS query source port
	Max DHCP leases No.	Maximum number of DHCP leases allowed
	Max EDNS0 data pack size	Allowed max EDNS.0 UDP data pack size
	Maximum concurrent queries number	Maximum number of concurrent DNS queries allowed
	DNS Query cache size	Cached DNS entries numbers (maximum 10000, 0 means no cache)
Static address assignment		Static leases are 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 values of the IPv4 address and host name fields will be fixedly assigned to the hosts identified by the MAC address field. The lease period is an optional field, and the length of the DHCP lease period can be set separately for each host, for example: 12h, 3d, infinite, Respectively 12 hours, 3 days, permanent.

5.3.5 Host Names



After adding the host mapping, you can access the specified IP address by accessing the host name

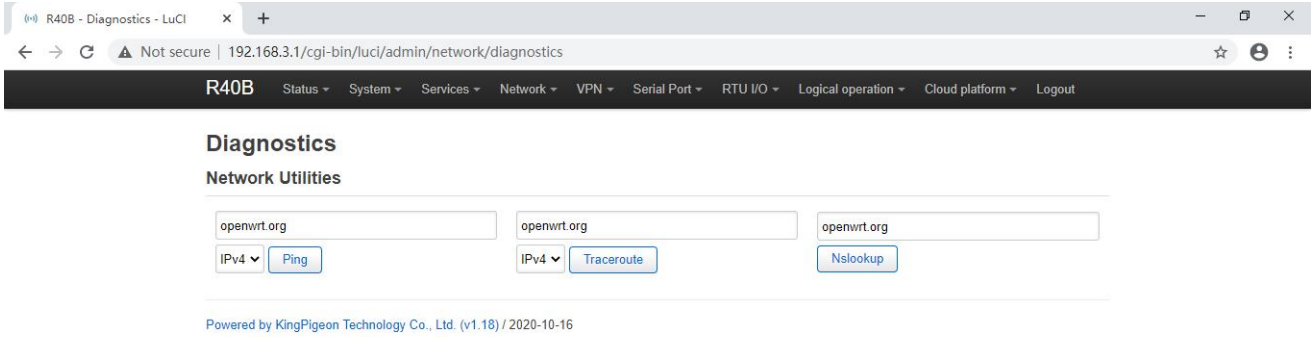
5.3.6 Static Routes



The routing table describes the reachable path of the packet

Routes		
Item		**Description**
Basic Setting	interface	Select setting interface
	Target	Host IP or network, requires valid IP or network
	IP Subnet mask	If the object is a network, a valid IP or network is required
	IP gateway	Need valid IP or network
Advanced settings	Hops	0
	MTU	1500
	Type	unicast
	Routing table	main(254)
	Source address	Auto
	On-Link Routing	Default is disable

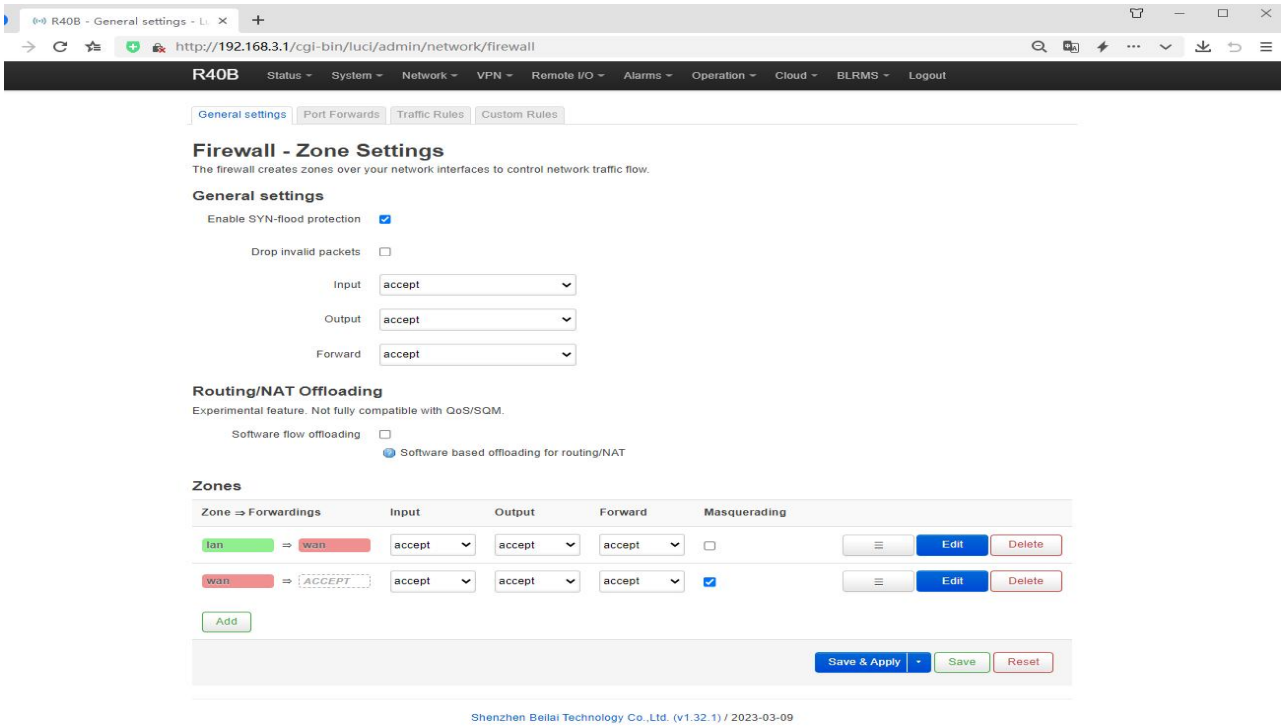
5.3.7 Diagnosis



Three commands are provided here: Ping, Traceroute, and Nslookup, which can perform simple diagnosis on the network.

5.3.8 Firewall

5.3.8.1 Zone Settings

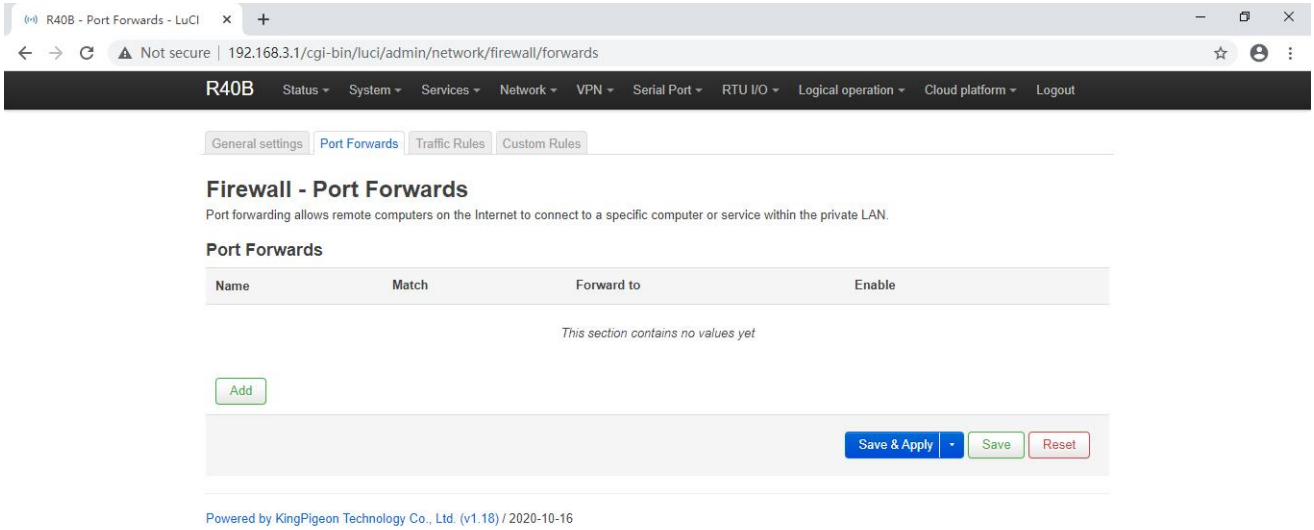


The firewall controls network traffic by creating zones on network interfaces.

Firewall-Zone Settings		
Item		Description
General Setting	This section defines the general properties of "lan". The inbound data and outbound data options are used to set the default strategy for inbound and outbound traffic in this area, and the forwarding options describe the traffic forwarding strategy between different networks in the area. The covered network designates the networks belonging to this area.	
	Name	lan
	Input	Default is accept
	Output	Default is accept
	Forward	Default is accept
	IP Dynamic camouflage	The LAN port does not need to be set, and the WAN port address may change during dynamic allocation. You need to set up dynamic disguise to connect to the external network
	MSS Clamp	Automatically adjust MSS according to MTU
	Covered networks	lan
	Allow forwarding to target area	wan
	Allow forwarding from source area	unspecified
Advanced	The following options control the forwarding strategy between this area (lan) and	

settings	other areas. The target area receives the forwarded traffic from lan. The forwarding traffic matching the source area comes from other areas whose destination is lan. The role of forwarding rules is one-way. For example, forwarding traffic from lan to wan does not mean allowing reverse forwarding of traffic from wan to lan.	
	Covered equipment	This option can classify regional traffic on original, non-UCI-hosted network devices.
	Subnets covered	This option can classify regional traffic by source or destination subnet instead of network or device.
	Restricted address	IPv4,IPv6
	To restrict the source subnet of IP dynamic masquerading	According to actual condition
	Target subnets to restrict IP dynamic masquerading	According to actual condition
	Enable logging in this area	Default is disable
Conntrack setting	Allow "invalid traffic"	Do not install additional rules to deny forwarded traffic with conntrack status invalid. This may be a necessary setting for complex asymmetric routing,default is disable
	Automatic assistant assignment	Automatically assign conntrack assistant according to traffic protocol and port,default is enable.
Additional iptables parameter	By passing the iptables parameter to the source and destination traffic classification rules, you can match packets based on other conditions than the interface or subnet. Use these options with extreme caution, as invalid values may break the firewall rule set and expose all services to the outside world.	
	Additional source parameters	Additional iptables parameters are used to classify regional inflows. For example: -p tcp --sport 443 only matches inbound HTTPS traffic.
	Additional target parameters	Additional iptables parameters are used to classify regional outgoing traffic. For example: -p tcp --dport 443 only matches outbound HTTPS traffic.

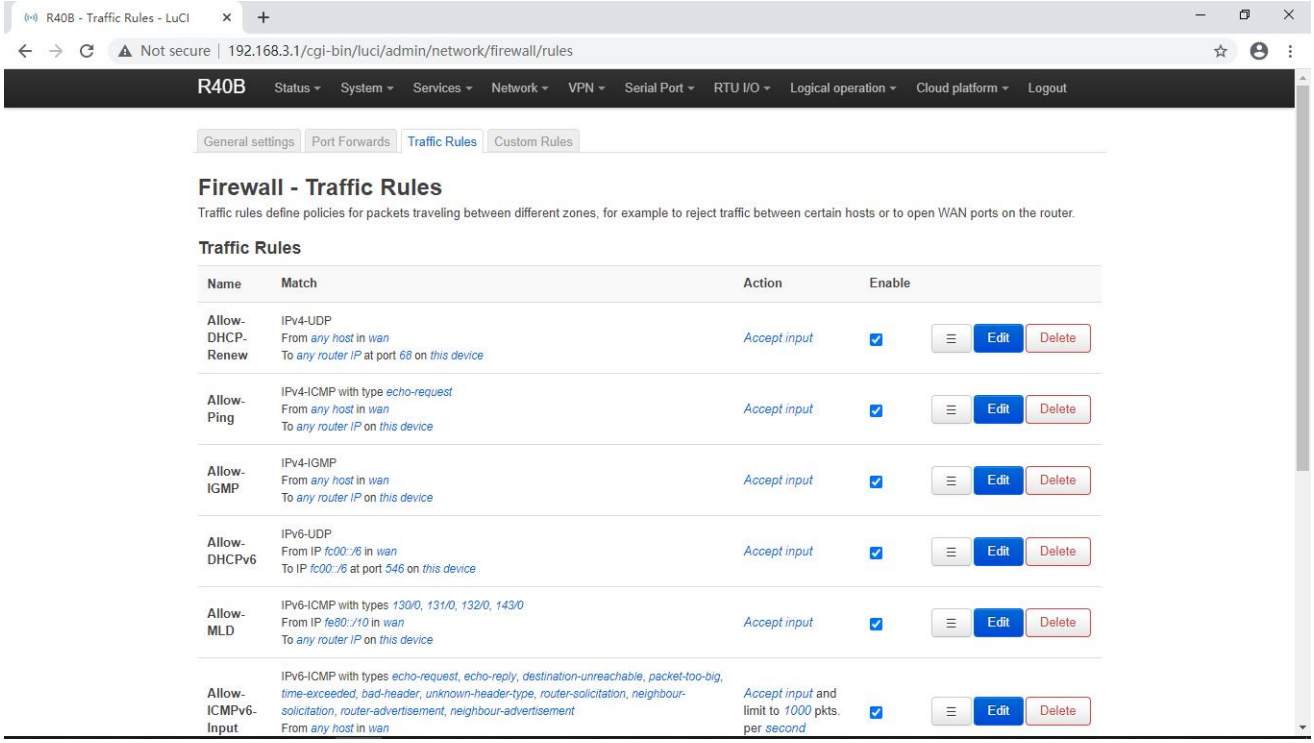
5.3.8.2 Port Forwards



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

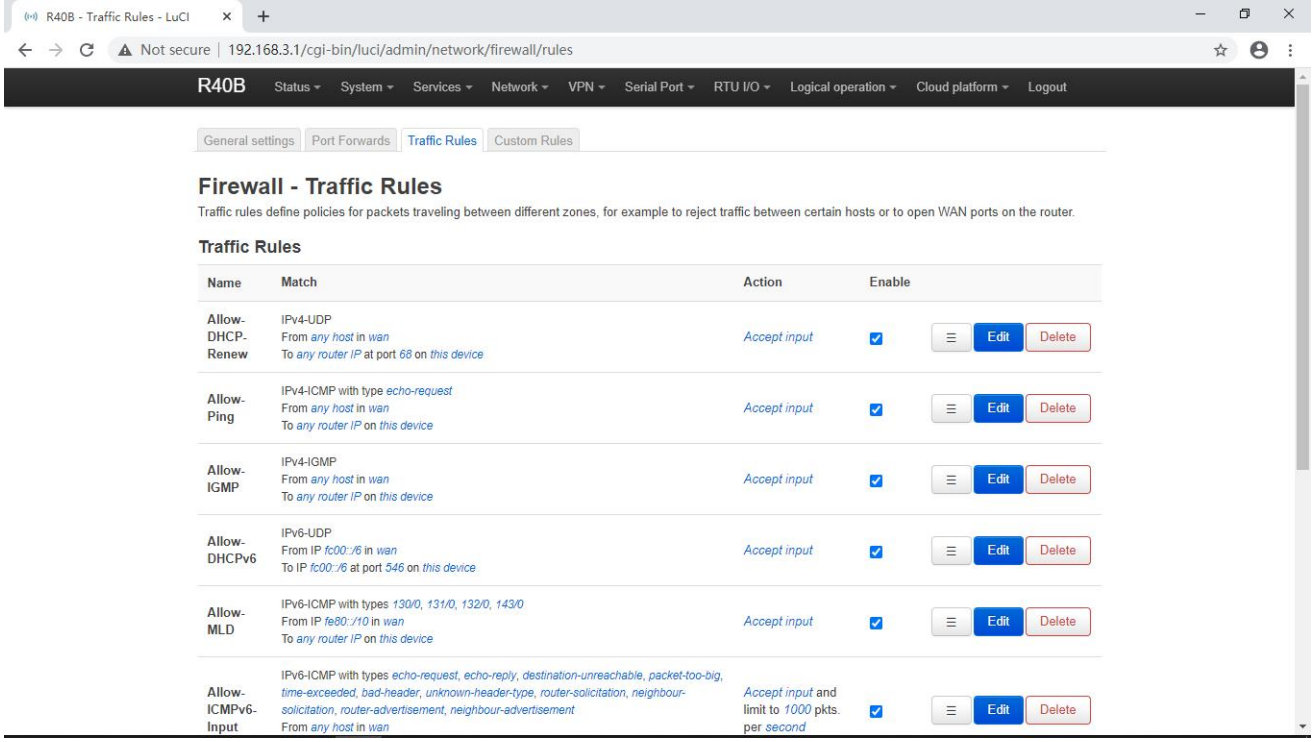
Firewall-Port Forwarding		
Item		**Description**
General Setting	Name	Forward naming
	Protocol	TCP+UDP,TCP,UDP,ICMP optional
	Source area	wan
	External port	Match inbound traffic to the specified target port or target port range on this host
	Target area	lan
	Internal IP address	Redirect matching inbound traffic to the specified internal host
	Internal port	Redirect matching inbound traffic to the port of the internal host
Advanced settings	Source MAC address	Match only inbound traffic from these MACs
	Source IP address	Only match inbound traffic from this IP or IP range
	Source port	Only match inbound traffic originating from a given source port or source port range on the client host
	External IP address	Only match inbound traffic for the specified destination IP address
	Enable NAT loopback	Default is enable
	Additional parameters	Extra parameters passed to iptables. Be caution!

5.3.8.3 Traffic Rules



Traffic rules define policies for packets traceling between different zones,for example to reject traffic between certain hosts or to open WAN ports on the router.

5.3.8.4 Custom Rules

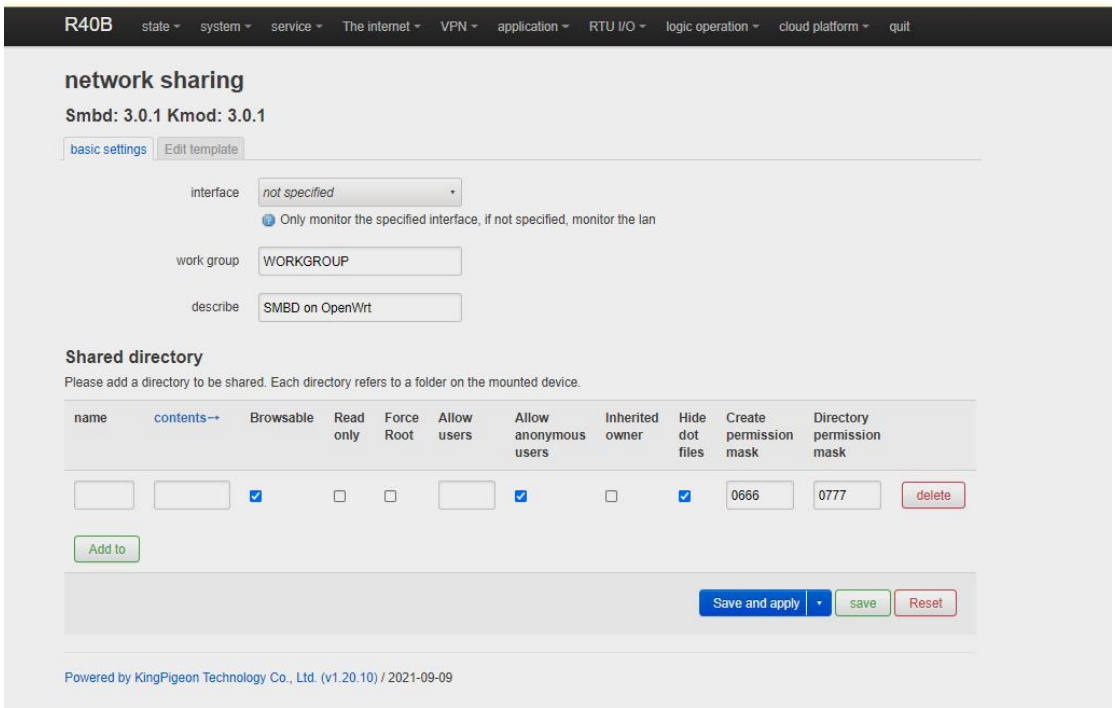


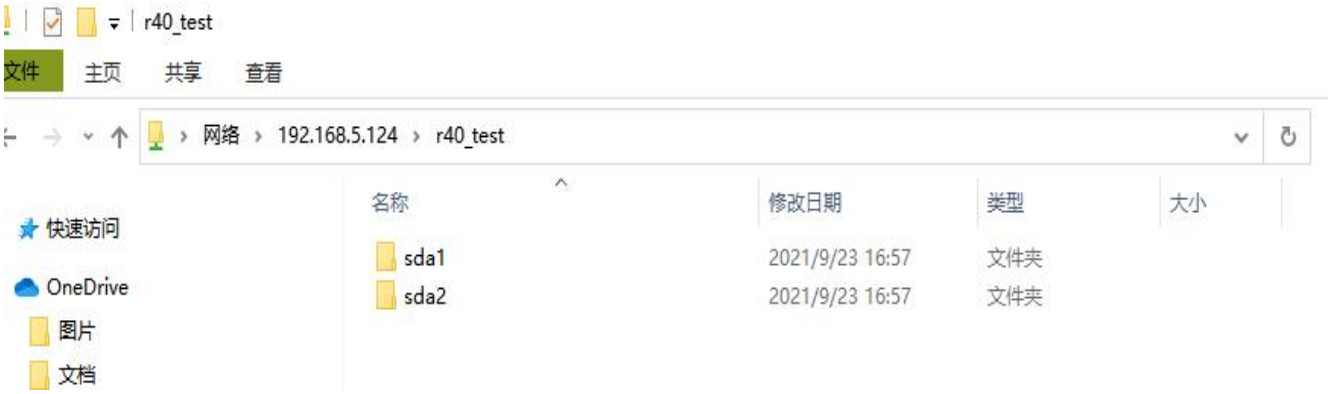
Custom rules allow you to execute any iptables command that is not part of the firewall framework. Each time the firewall is restarted, these commands will be executed immediately after the default rules are run.

5.3.9 Network Sharing

When an external storage device is connected to the USB port of the router, the networked computer can access the storage device by accessing the network shared directory. "Interface" needs to choose whether to access the router through WAN port or LAN. The "Directory" in the setting interface is the /mnt directory in the System->Mount Point Settings, and the "Name" is the shared directory accessible by the computer.

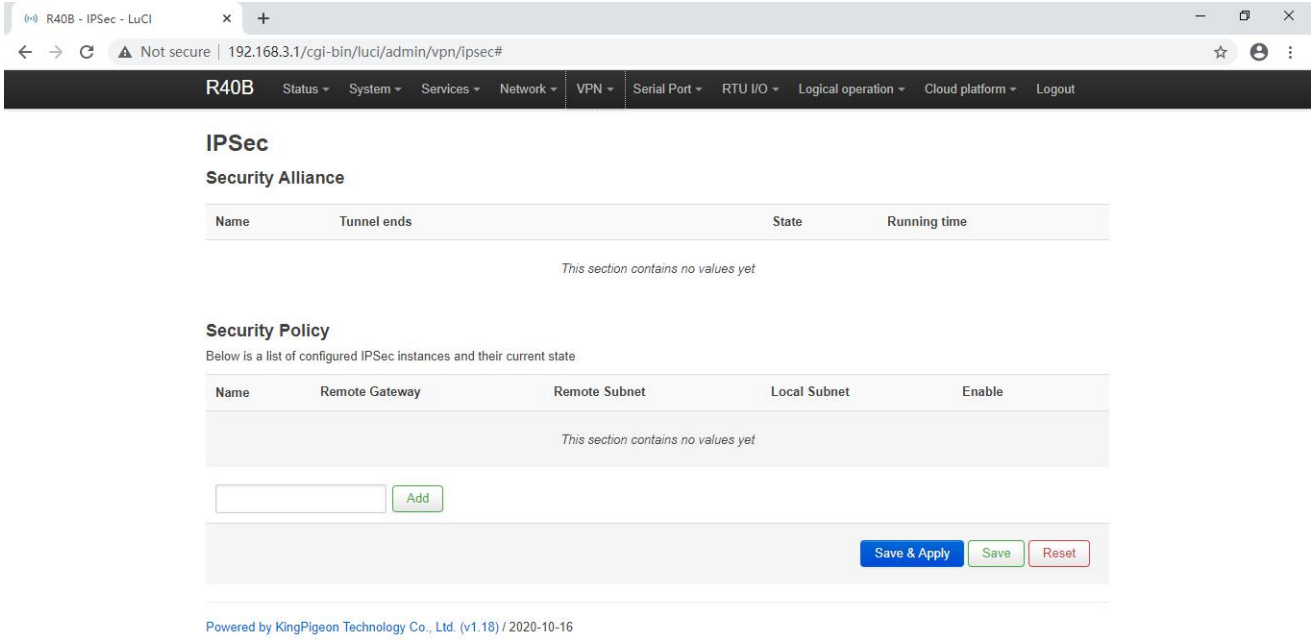
English interface diagram:


R40B
state
system
service
The internet
VPN
application
RTU I/O
logic operation
cloud platform
quit
network sharing
Smbd: 3.0.1 Kmod: 3.0.1
basic settings
Edit template
interface
not specified
Only monitor the specified interface, if not specified, monitor the lan
work group
WORKGROUP
describe
SMBD on OpenWrt
Shared directory
Please add a directory to be shared. Each directory refers to a folder on the mounted device.
name
contents→
Browsable
Read only
Force Root
Allow users
Allow anonymous users
Inherited owner
Hide dot files
Create permission mask
Directory permission mask
0666
0777
delete
Add to
Save and apply
save
Reset
Powered by KingPigeon Technology Co., Ltd. (v1.20.10) / 2021-09-09


r40_test
文件
主页
共享
查看
网络 › 192.168.5.124 › r40_test
快速访问
OneDrive
图片
文档
名称
修改日期
类型
大小
sda1
2021/9/23 16:57
文件夹
sda2
2021/9/23 16:57
文件夹

5.4 VPN

5.4.1 IPSec



IPSec is an open network layer security framework protocol formulated by the 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 mainly includes security protocols AH (Authentication Header) and ESP (Encapsulating Security Payload), key management exchange protocol IKE (Internet Key Exchange) and some algorithms used for network authentication and encryption.

IPSec mainly provides security services for IP data packets through encryption and authentication. The security services that IPSec can provide include:

(1) User data encryption provides data privacy through user data encryption.

(2) Data integrity verification Through data integrity verification to ensure that data has not been tampered with on the transmission path.

(3) Data source verification By authenticating the source of the sent data, the data is guaranteed to come from the real sender.

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

IPSec		
Item		Description
IPSec Configuration	Enable	Tick to enable
	Package type	Optional tunnel mode, transmission mode. Tunnel mode means host-to-host, host-to-subnet or subnet-to-subnet tunnel. The transmission mode indicates the transmission method from the host to the host.
	Peer gateway	Peer gateway which connect with IPSEC

	Local subnet IP/mask	In the tunnel mode, the tunnel from the subnet to the subnet needs to specify the local and opposite terminal network ranges
	Peer Subnet IP/Mask	In the tunnel mode, the tunnel from the subnet to the subnet needs to specify the local and opposite terminal network ranges
	Pre-shared key	Default authenticate using pre-shared key
Phase 1 settings		Phase 1 mainly negotiates encryption parameters, exchanges key information, and verifies device identity
IKE Encryption Algorithm		Specify IKE (Internet Key Exchange) negotiation message encryption algorithm
Authentication algorithm		Specify the digital signature authentication algorithm for encrypted messages
DH group		Specify which key group to use for DH (DiffieHellman) key exchange
IKE version		IKEv1 or IKEv2
Exchange mode		Main mode or brutal mode. The main mode is more secure than the brutal mode, and the brutal mode is faster. If the responder (server) cannot know the address of the initiator (end user) in advance, or the address of the initiator is always changing, and both parties want to use the pre-shared key authentication method to create an IKE SA, Brutal mode can be used at this time
Negotiation mode		Responder or initiator, the initiator is equivalent to the end user, and the responder is equivalent to the server
Local ID		Can be IP address, standard domain name, email address or proper name, default is local IP
Peer ID		Can be IP address, standard domain name, email address or proper name, default is peer IP
IKE live time		Re-negotiate the key time
Phase 2 setting		The purpose of Phase 2 is to establish an IPSec security association for data transmission
ESP Encryption Algorithm		Specify the algorithm used for data encryption
Authentication algorithm		Specify digital signature authentication algorithm for encrypted data
PFS group		PFS (Perfect Forward Secrecy), which means that a key is cracked and does not affect the security of other keys
Survive time		How long should it take from the negotiation to the connection instance
DPD detection cycle		DPD（Dead Peer Detect）,When no traffic occurs for a period of time, the local end sends a DPD message to check the status of the peer before sending traffic

5.4.2 L2TP

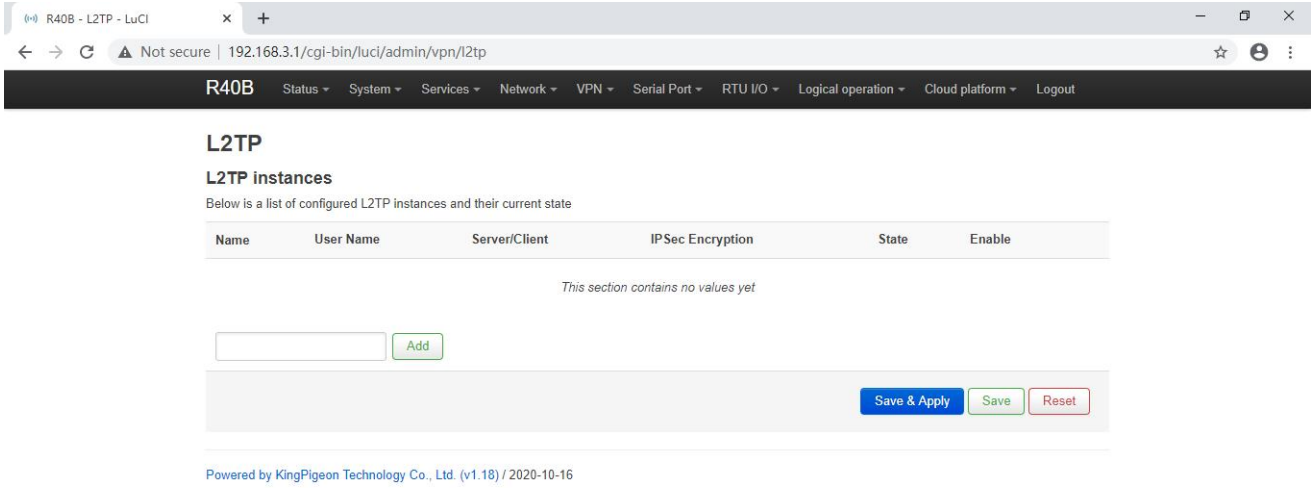
L2TP (Layer 2 Tunneling Protocol, Layer 2 Tunneling Protocol) is a type of VPDN (Virtual Private Dial-up Network, Virtual Private Dial-up Network) tunneling protocol.
VPDN (Virtual Private Dial Network) refers to the use of public network (such as ISDN and PSTN) dial-up

function and access network to achieve a virtual private network, providing access services for enterprises, small ISPs, and mobile office personnel.

VPDN uses a dedicated network encryption communication protocol to establish a secure virtual private network for enterprises on public networks. Enterprises abroad and business personnel can remotely connect to the corporate headquarters through a virtual encrypted tunnel through a public network, while other users on the public network cannot access resources inside the corporate network through the virtual tunnel. There are many VPDN tunneling protocols, and the most widely used is L2TP (Layer Two Tunneling Protocol).

The PPP protocol defines a encapsulation technology that can transmit multiple protocol data packets on a layer-2 point-to-point link. At this time, PPP runs between the user and the NAS (Network Access Server) network access server. The L2TP protocol provides tunnel transmission support for PPP link layer data packets, allows Layer 2 link endpoints and PPP session points to reside on different devices, and uses packet exchange technology for information exchange, thereby expanding the PPP model .

The L2TP function can be simply described as establishing a point-to-point PPP session connection on a non-point-to-point network. The L2TP protocol combines the advantages of the L2F (Layer 2 Forwarding) protocol and the PPTP (Point-to-Point Tunneling protocol) protocol, and has become the IETF industry standard for Layer 2 tunneling protocols.



L2TP	
Item	**Description**
Enable	Tick to enable
Username	User name for PPP authentication
Password	Password for PPP authentication
Server/client	Server,client optional
Server address	LNS（L2TP Network Server，L2TP network server）address
IPSec encryption	You can choose whether to use IPSec encryption or not, and choose to use the default IPSec security policy during encryption. You do not need to manually configure IPSec. When you choose to use a security policy, you need to configure the

	IPSec policy in advance
Pre-shared key	When selecting encryption, you need to set the IPSec pre-shared key
Security strategy	Configured IPSce security policy

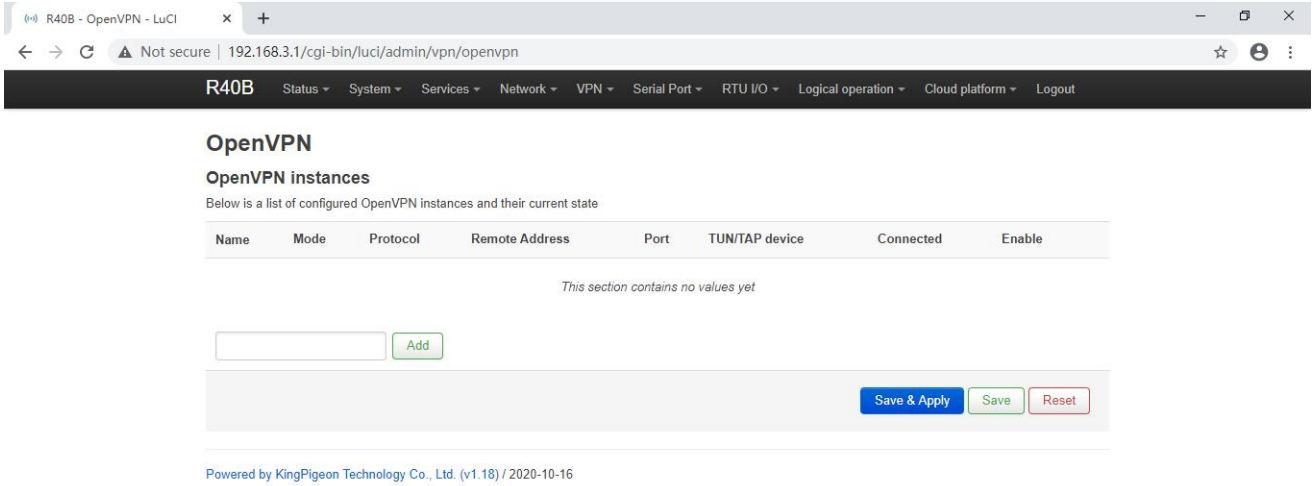
5.4.3 OpenVPN

OpenVPN is an application layer VPN implementation based on the OpenSSL library. It is a type of SSL VPN. It uses a virtual network card to establish a connection to transmit data, and uses SSL to encrypt and verify.

The virtual network card is a driver software implemented using the underlying network programming technology, and can be configured like other network cards. If the application accesses a remote virtual address (belongs to the address series used by the virtual network card, which is different from the real address), the operating system will send data packets (TUN mode) or data frames (TAP mode) to the virtual network card through the routing mechanism. After the service program receives the data and performs corresponding processing, it is sent from the external network through SOCKET, and the remote service program receives the data from the external network through SOCKET, and after corresponding processing, it is sent to the virtual network card, and the application software can receive At this point, a one-way transmission process is completed, and vice versa. OpenVPN provides two virtual network interfaces: universal Tun/Tap driver, through which you can establish a layer 3 IP tunnel or a virtual layer 2 Ethernet. The latter can transmit any type of layer 2 Ethernet data, and the transmitted data can be passed through the LZO algorithm compression.

The SSL protocol (Secure Socket Layer) mainly uses the public key system and X.509 digital certificate technology to protect the confidentiality and integrity of information transmission. It includes: server authentication, client authentication (optional), SSL chain Data integrity on the road and data confidentiality on the SSL link. The SSL protocol is independent of the application layer protocol.

High-level application layer protocols (such as HTTP, FTP, Telnet, etc.) can be transparently built on the SSL protocol. The SSL protocol has completed the encryption algorithm, communication key negotiation and server authentication before the application layer protocol communication. After that, the data transmitted by the application layer protocol will be encrypted to ensure the privacy of the communication.



OpenVPN	
Item	Description
Enable	Tick to enable
Configure client mode	Tick to client mode
VPN Subnet IP address/mask	TAP mode, as a server, it can transmit from host to subnet
Server address	Server address which establish VPN connect with client
Port	The TCP/UDP port provided by the server for establishing a connection, default is 1194
Protocol	UDP, TCP-Server, TCP-Client, default is UDP.
TUN/TAP device	TUN mode establishes a three-layer tunnel to achieve point-to-point transmission. TAP mode establishes a Layer 2 tunnel, which can realize the transparent transmission of IP packets
Username/password	When security certificate authentication is not applicable, user name/password authentication can be used
Encryption Algorithm	Choose data encryption algorithm
Authentication and authorization (root certificate)	Select file upload, root certificate provided by server
Local certificate	Select file upload, the client certificate generated by the user based on the root certificate
Local private key	Select the file upload, the key corresponding to the client certificate
DH Key exchange parameters	Used for key exchange, can be generated by openssl dhparam -out dh2048.pem 2048
Compression algorithm	LZO,LZ4
Keepalive interval (seconds)	The interval at which the server sends a probe message to the client
Keepalive timeout (seconds)	If the server does not receive a response to the probe message at this time, it restarts the connection

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.

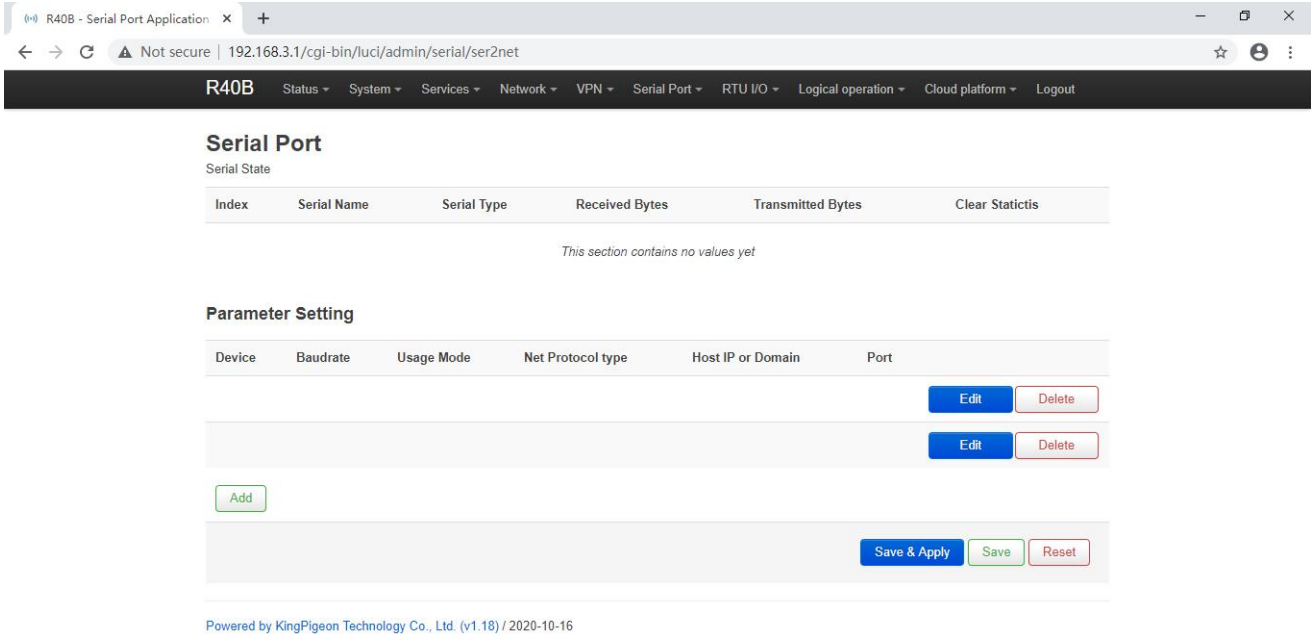
5.5 Remote I/O and Serial Port Setting

5.5.1 Serial Port Settings

The remote IO refers to the I/O of the Modbus slave
When the R40 router is connected with the Modbus slave device through the serial port, the router acts as the Modbus master station,

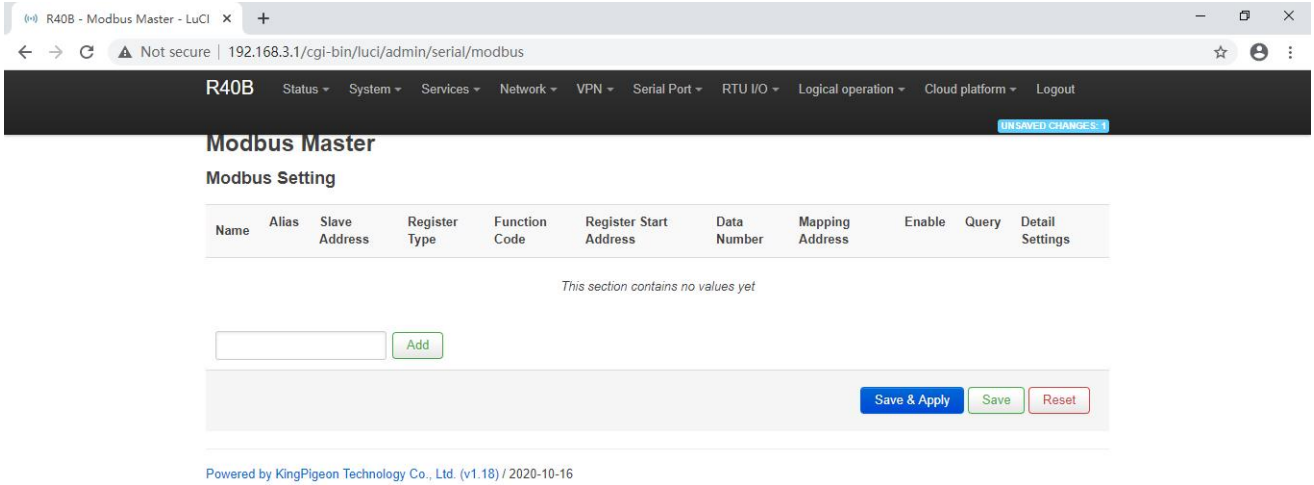
Serial Port Settings		
Item		Description
Modbus Device ID		Range 1~247,default is 1
RS485	Baud rate	1200,2400,4800,9600,14400,19200,38400,57600,115200,230400 optional
	Data bit	5,6,7,8
	Parity	None, Even and Odd optional
	Stop Bit	1,2 optional
RS232	Baud rate	1200,2400,4800,9600,14400,19200,38400,57600,115200 optional
	Data bit	5,6,7,8 optional
	Parity	None, Even and Odd optional
	Stop Bit	1,2 optional

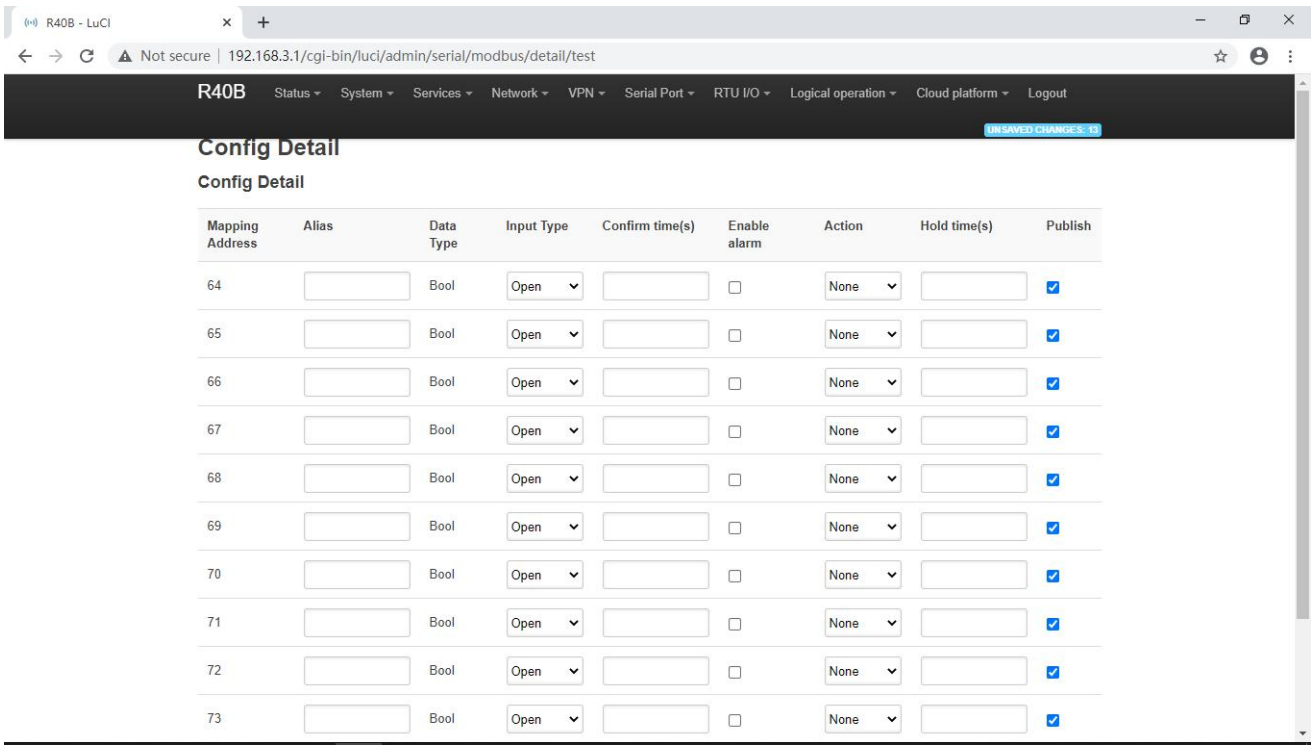
5.5.2 Serial Port Application



Serial Port Application	
Item	**Description**
Enable	Tick to enable
Device	RS485 or RS232
Mode	Transparent transmission, Modbus RTU to TCP, Modbus slave
Modbus Device ID	Set when mode is modbus slave, default is 1, please modify in the serial port settings
Network Protocol	TCP server, TCP client, UDP server, UDP client
Host IP or domain name	Select the client to be visible, set the connection server address here
Port	Set the connection server port when the client is selected, and set the local listening port when the server is selected
Login Message	Server register handshake protocol package
Heartbeat Message	Heartbeat content to avoid network offline
Heartbeat ACK Message	The server responds to the heartbeat packet
Heartbeat Interval(s)	Network keep online heartbeat interval time,default is 60s
Retransmission Times(s)	If server no response, the times which server will send data

5.5.3 Modbus Master



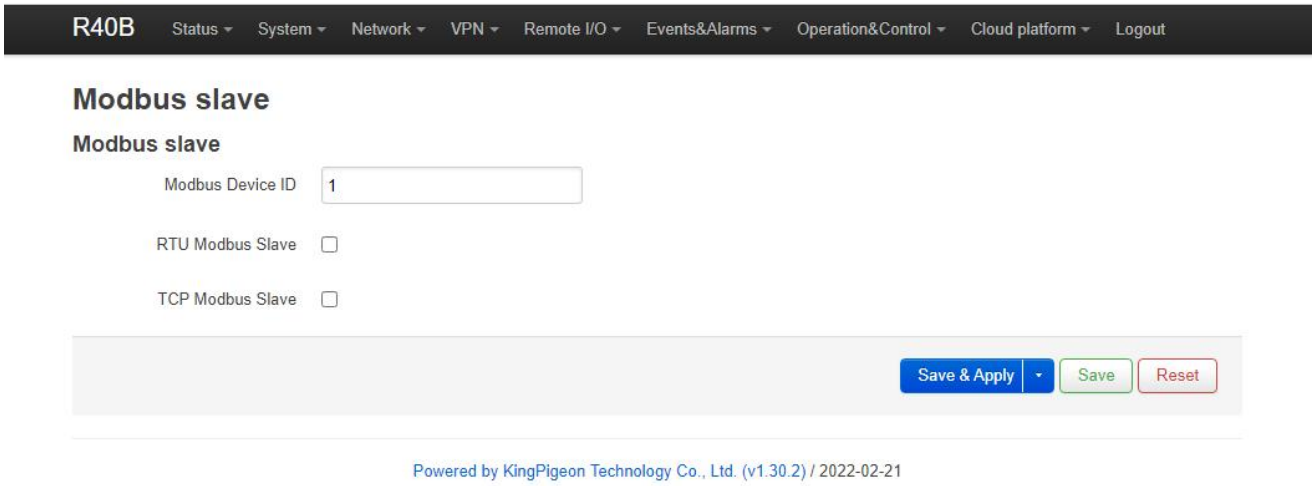


Note: Modbus master settings need to be selected device model to support this function will be displayed.

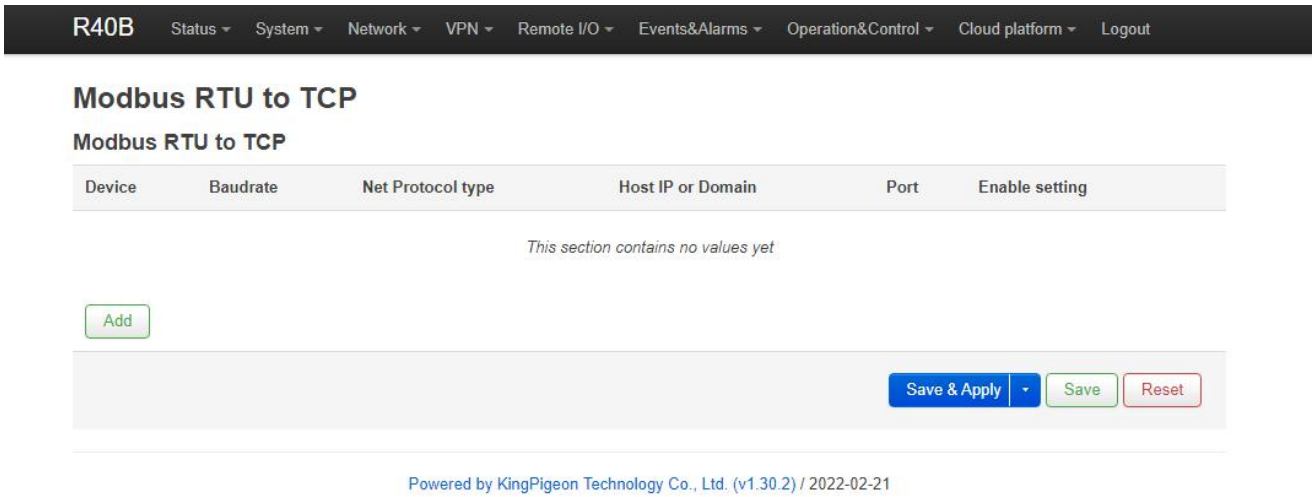
Modbus Master	
Item	Description
Enable	Tick to enable
Slave address	Slave Modbus device ID
Register type	Boolean,16-bit, 32-bit
Function code	01,02,03,04; 01/02 Function codes apply to Boolean data types

		03/04 Function codes apply to 16/32/64 bit data type； 01 function code supports 05/15 function code at the same time, 03 function code supports 06/16 function code at the same time.
Register start address		Set according to slave register address
Data number		Set according to the number of slave registers
Mapping address assignment		Automatic / Manual
Mapping start address		Select Manual Assignment Visible； Boolean type mapping register address 64~256， 16 bit type mapping register address 20000~20127， 32 bit type mapping register address 20128~20254，
Slave interface		RS485,RS232,Ethernet If RS485 or RS232 is already connected as a serial device, this is not visible here
Slave IP address		Visible when selecting Ethernet
Port		Visible when selecting Ethernet
Detailed configuration	Mapping address	Slave register address
	Alias	Name the slave data points, such as the purpose of remarks; After the alias is set, the slave data point will be directly displayed as the set alias on other configuration pages, or as the mapped address if no alias is set
	Data type	Slave register data type
	Input type	Boolean data type is visible, open or close
	Coefficient	16/32 bit data type is visible, ratio coefficient between register value and real value
	High threshold	16/32 bit data type is visible. Greater than or equal to the high threshold will trigger an alarm
	High threshold recovery	16/32 bit data type is visible. Less than or equal to the high threshold recovery value will trigger an alarm recovery
	Low threshold	16/32 bit data type is visible. Less than or equal to the low threshold will trigger an alarm
	Low threshold recovery	16/32 bit data type is visible. Greater than or equal to the low threshold recovery value will trigger an alarm recovery
	Confirmation time (second)	Confirm the trigger time of the alarm
	Enable alerts	Click to enable
	Action	Linkage local DO close or open
	Hold time	Do action time
	Publish	Tick to publish data via MQTT

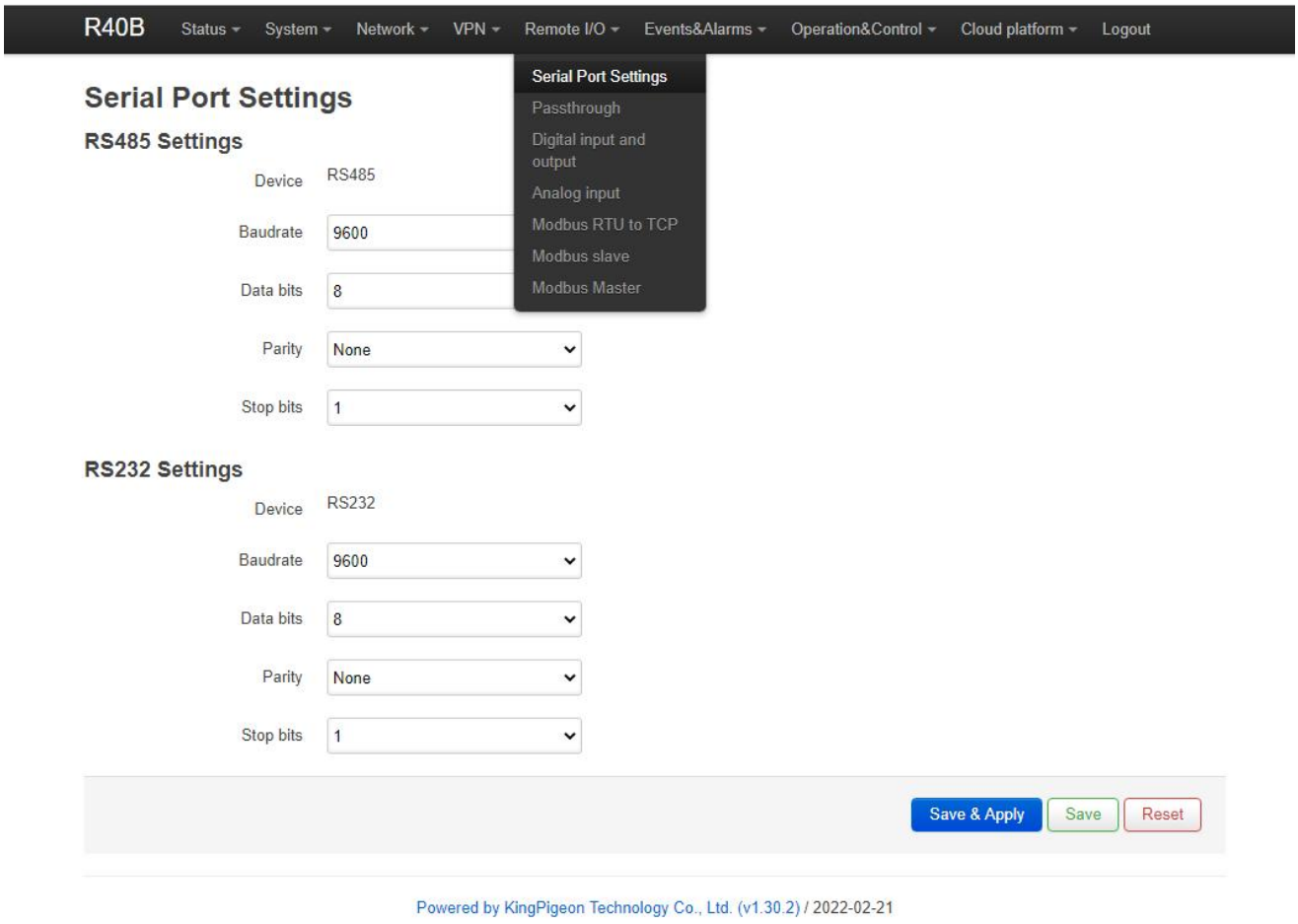
5.5.4 Modbus Slave

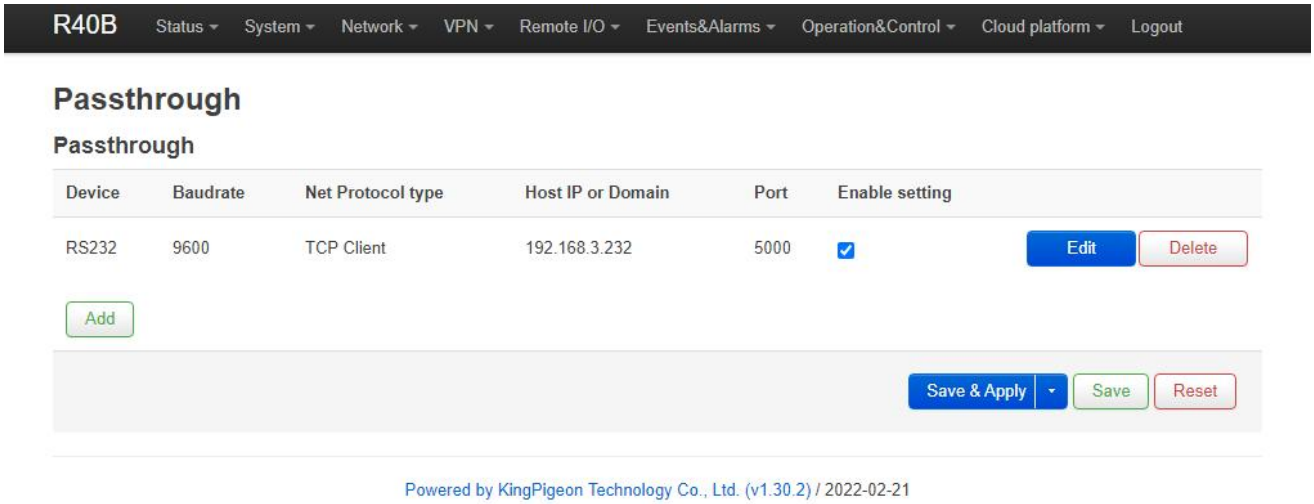


5.5.5 Modbus RTU to TCP



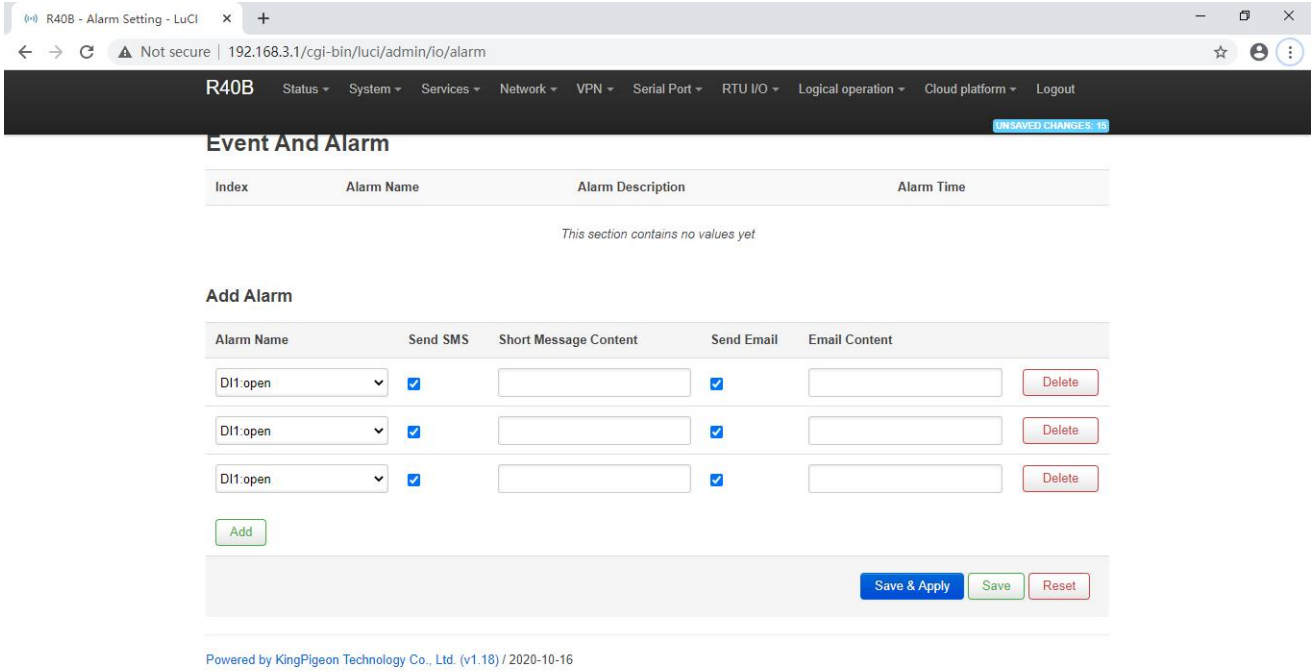
5.5.6 Transparent Transmission


R40B
Status
System
Network
VPN
Remote I/O
Events&Alarms
Operation&Control
Cloud platform
Logout
Serial Port Settings
Passthrough
Digital input and output
Analog input
Modbus RTU to TCP
Modbus slave
Modbus Master
Serial Port Settings
RS485 Settings
Device RS485
Baudrate 9600
Data bits 8
Parity None
Stop bits 1
RS232 Settings
Device RS232
Baudrate 9600
Data bits 8
Parity None
Stop bits 1
Save & Apply
Save
Reset
Powered by KingPigeon Technology Co., Ltd. (v1.30.2) / 2022-02-21


R40B
Status
System
Network
VPN
Remote I/O
Events&Alarms
Operation&Control
Cloud platform
Logout
Passthrough
Passthrough
Device
Baudrate
Net Protocol type
Host IP or Domain
Port
Enable setting
RS232
9600
TCP Client
192.168.3.232
5000
Edit
Delete
Add
Save & Apply
Save
Reset
Powered by KingPigeon Technology Co., Ltd. (v1.30.2) / 2022-02-21

5.6 Event and Alarm (RTU IO)

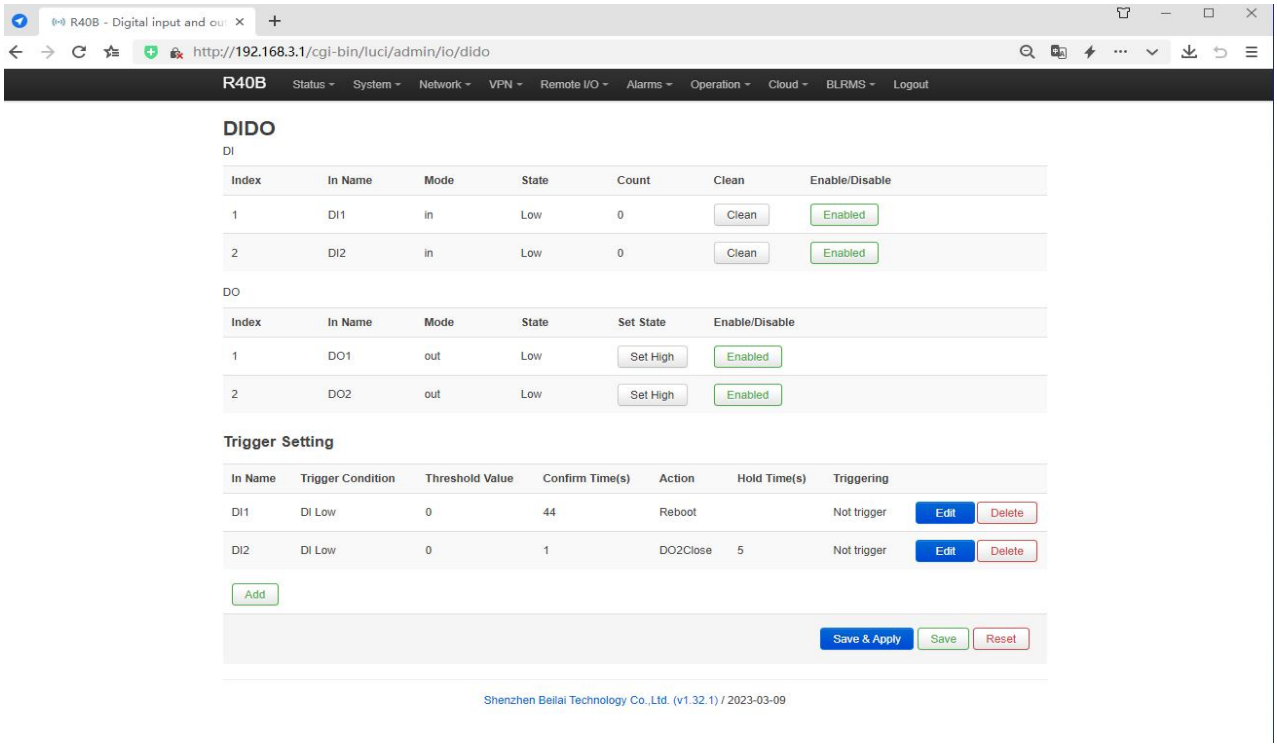
5.6.1 Event and Alarm



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.

5.6.2 Digital Input/Output

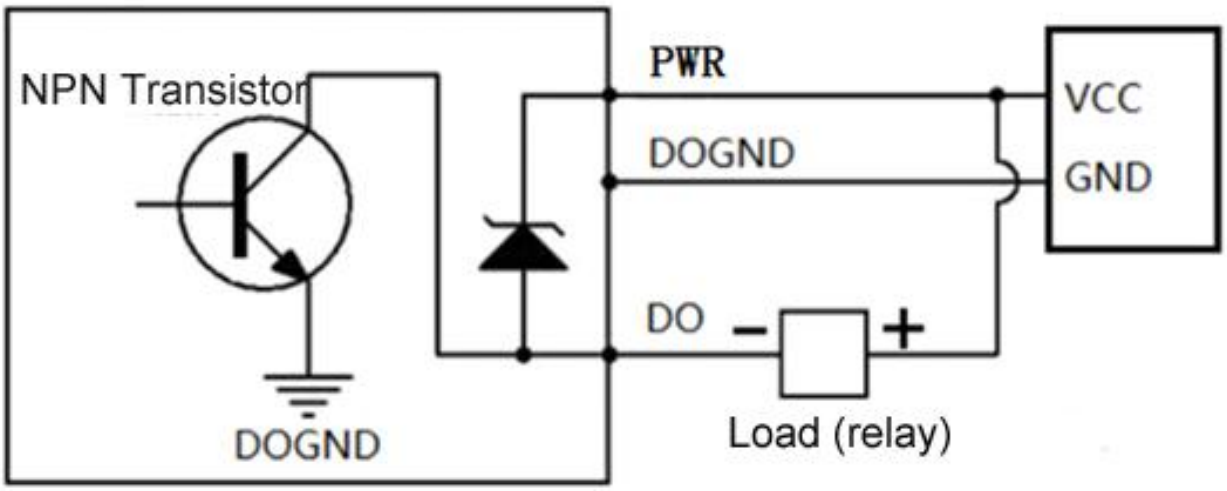


You can view the current status of DI and DO, the DI count value, set the type of DO normally open and normally closed, enable and disable the operation of DI and DO, and trigger settings can add DI trigger conditions.

Trigger Setting	
Item	Description
Input	DI1, DI2
Trigger conditions	NO,NC,Counting over threshold, Recovery
Threshold value	The threshold value should be entered when the condition selection count exceeds the threshold
Confirmation time (seconds)	The condition will reach the set time will confirm the trigger
Action	Linkage action：No,DO1,DO2,all DO, Reboot
DO status	Open,close,When the action selects DO, the execution state should be selected
Hold time (seconds)	DO action time
Trriggering	Tick to enable alarm

Digital output Instructions

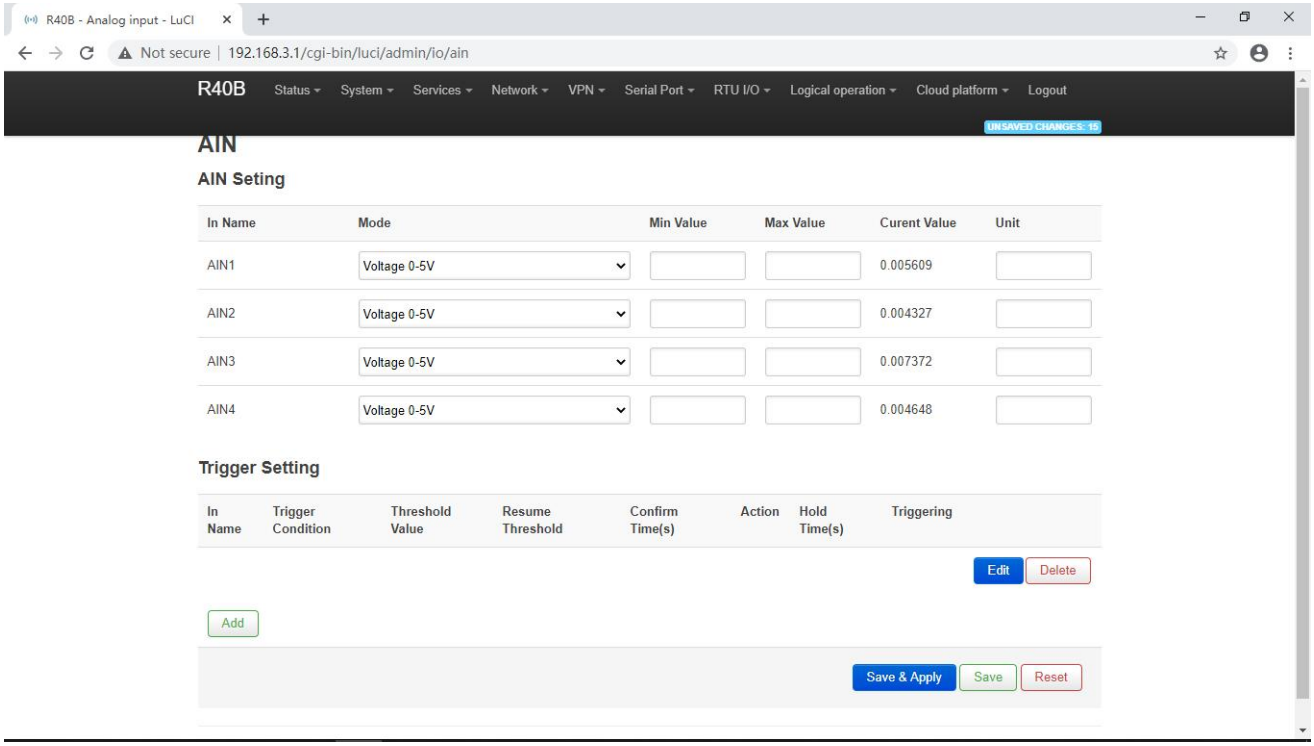
Wiring



Instruction:

Digital output	QTY	2
	type	SINK output
	Load voltage	Max 50VDC
	Load current	500mA（single）,625mW
	protection	EFT: 40A（5/50ns）

5.6.3 Analog Input

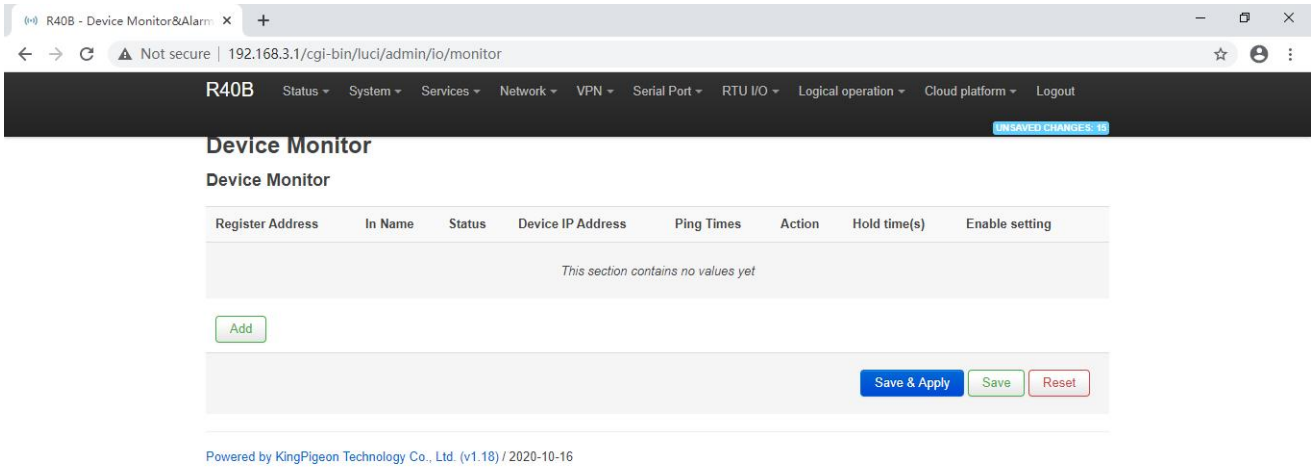


Note: When the device model supports analog input，this function will be displayed.

You can view the current AI value and set the mode: voltage 0~5V, current 4~20mA. Current 0~20mA, set the minimum value and unit of the range, trigger setting can add AI trigger condition.

Trigger	
Item	Description
Input	AIN1,AIN2,AIN3,AIN4
Trigger condition	Analog input is greater than the threshold, analog input is less than the threshold
Threshold value	The condition will be triggered when the set value is reached
Resume threshold	When the set value is reached, it will be regarded as recovery
Confirm time (seconds)	Confirm the trigger when condition reach the set time
Action	Linkage action：No,DO1,DO2,all DO, Reboot
DO status	Open,close,When the action selects DO, the execution state should be selected
Hold time (seconds)	DO action time
Trriggering	Tick to enable alarm

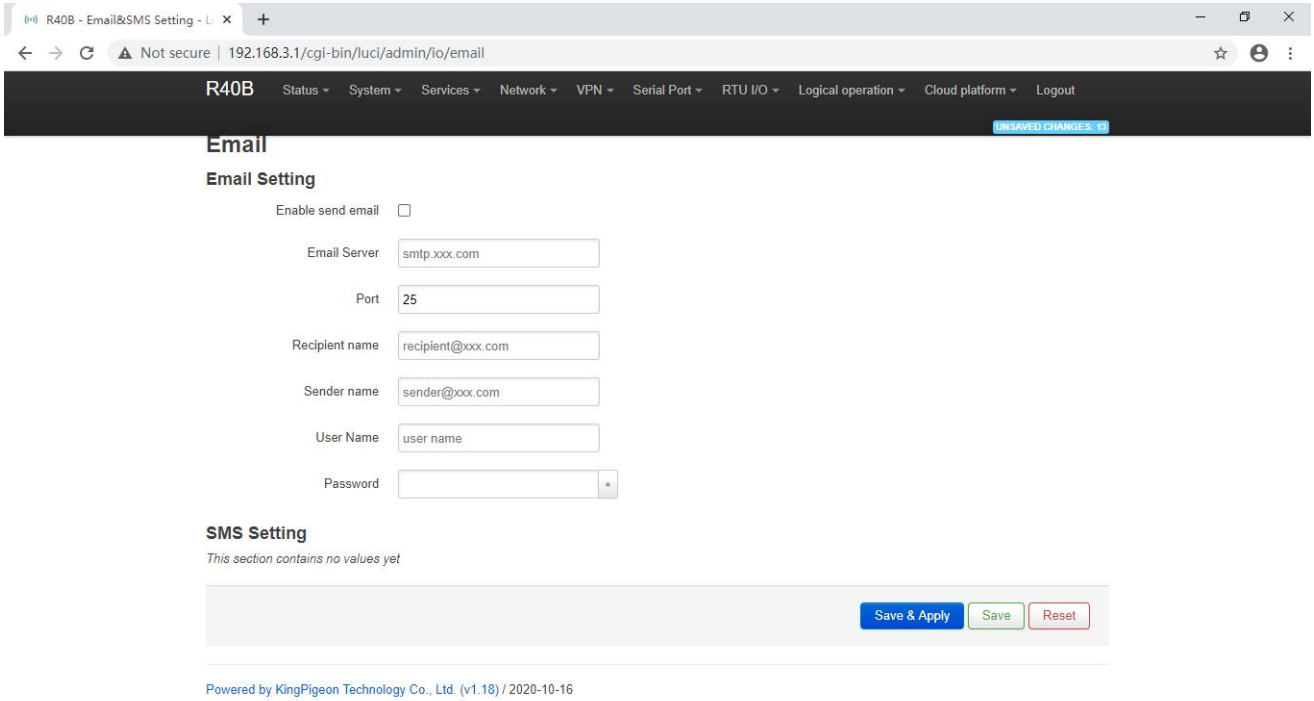
5.6.4 Device Monitor



Device Monitor	
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
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
Trriggering	Tick to enable alarm

5.6.5 E-mail & SMS



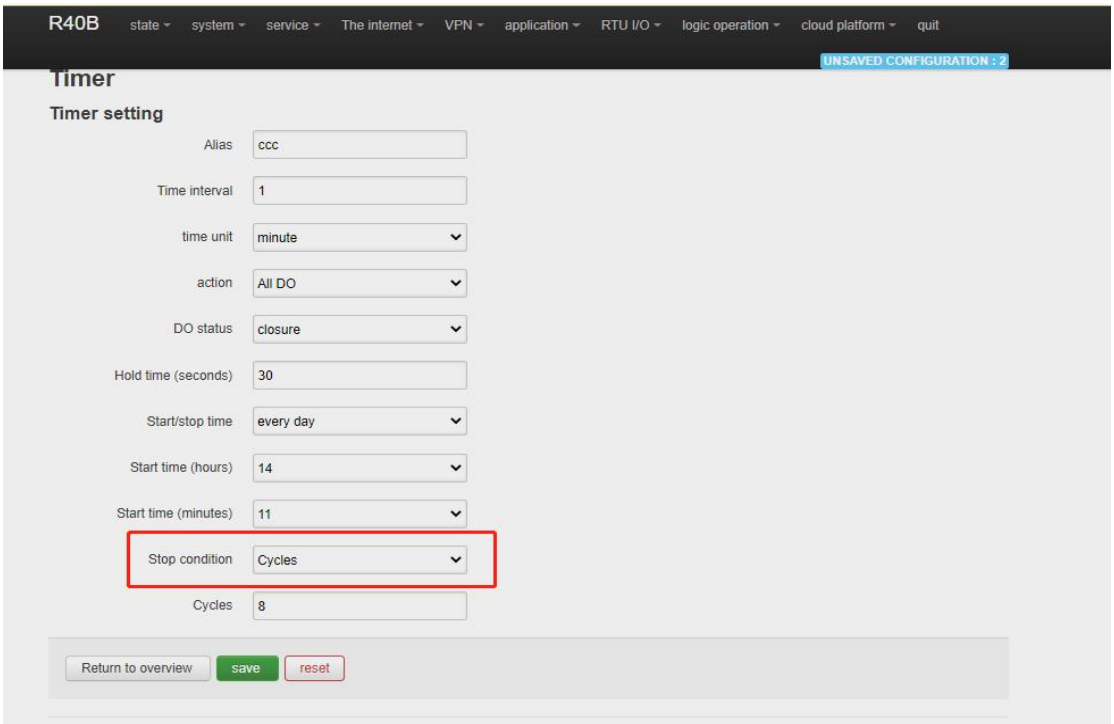
E-mail setting	
Item	Description
Enable send mail	Tick to allow send e-mail
Mail Server	Enter the SMTP mail server address
Port	Enter the SMTP mail server port number Port: 465
Recipient	Fill in the email recipient address
Sender	Enter the email sender address
User name	Enter the email sending account username(User mailbox opens smtp server)
Password	Fill in the third-party password to open the smtp port in the email

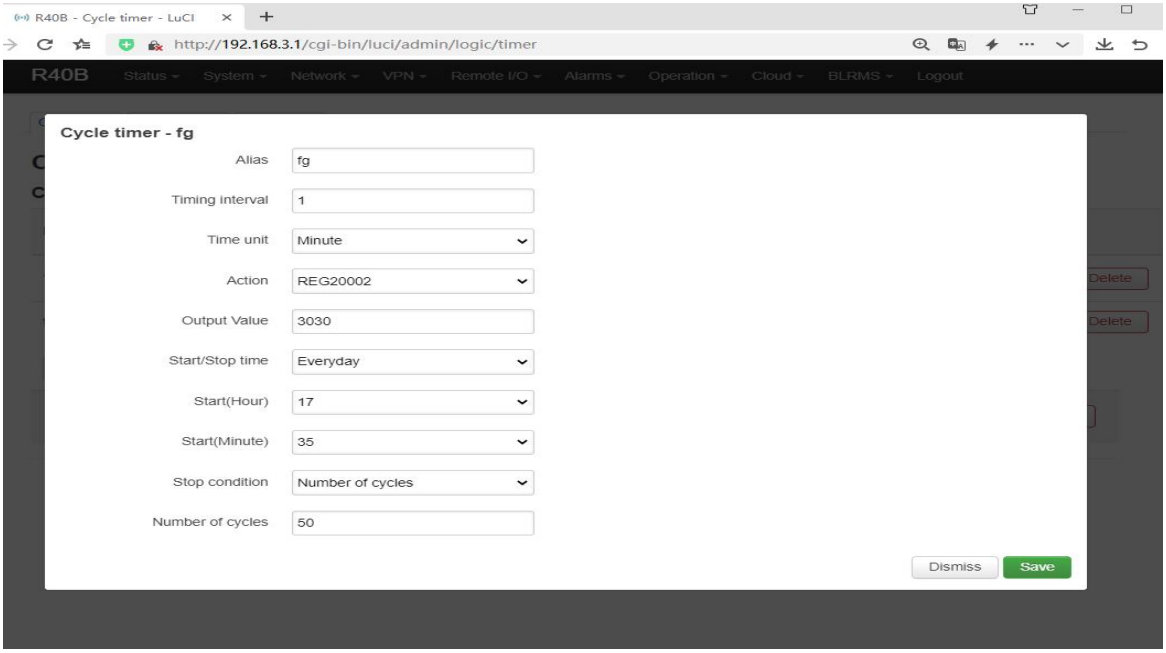
Note: The mail server needs to be enabled with the SMTP service. If the mail is not sent successfully, please make sure that the SMTP service is enabled in the mailbox settings and the account password is entered correctly.

SMS settings	
Item	Description
Phone Number	Multiple mobile phone numbers to receive SMS messages can be added. After entering a number, please click the "+" at the back to save
Language	English or Chinese

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

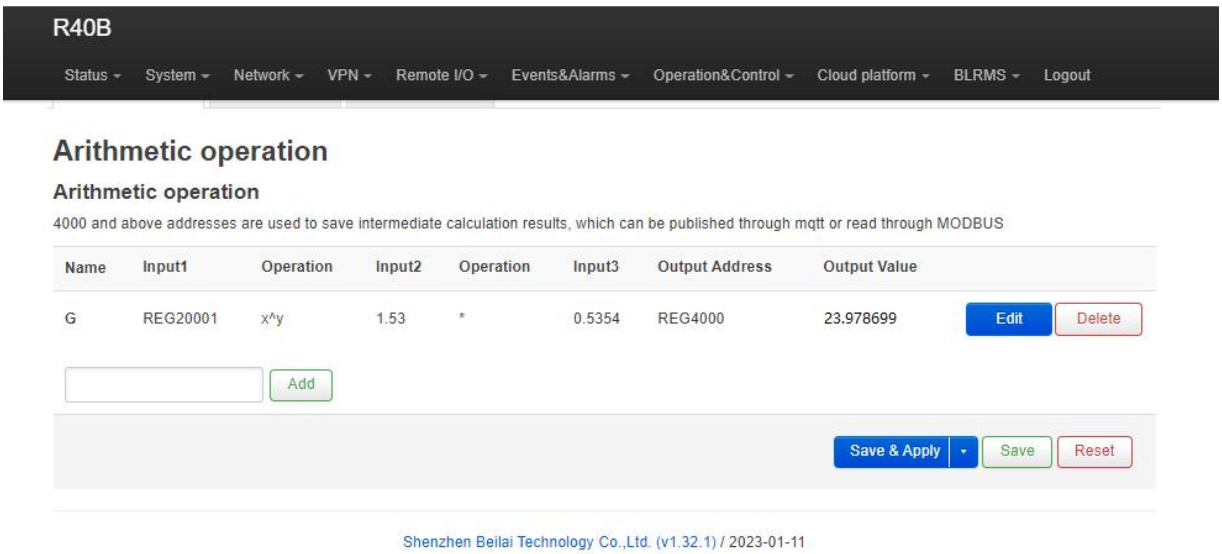
Regular timer: Execution at a certain regulation such as daily or weekly

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

Cycle timer: execution cyclely 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

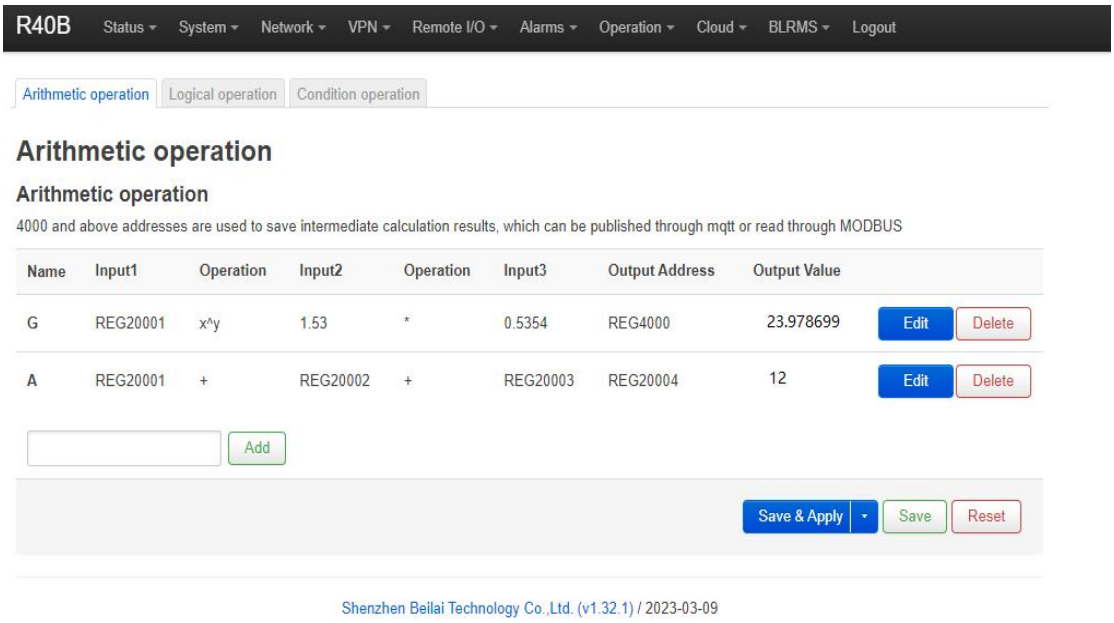


Arithmetic operation supports the "addition, subtraction, multiplication and division" operations between the value type registers of the local device (R40 router) and the Modbus slave device. You can adjust the order of operations at will, "addition, subtraction, multiplication and division" between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

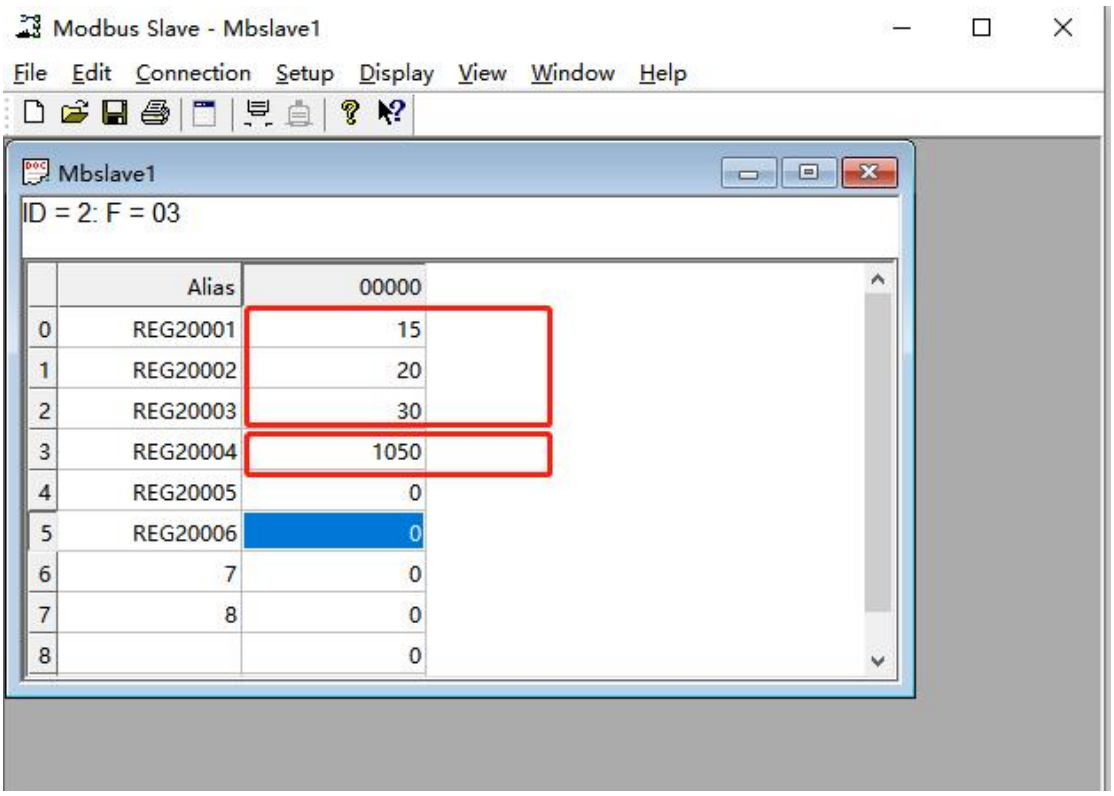
For example:

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

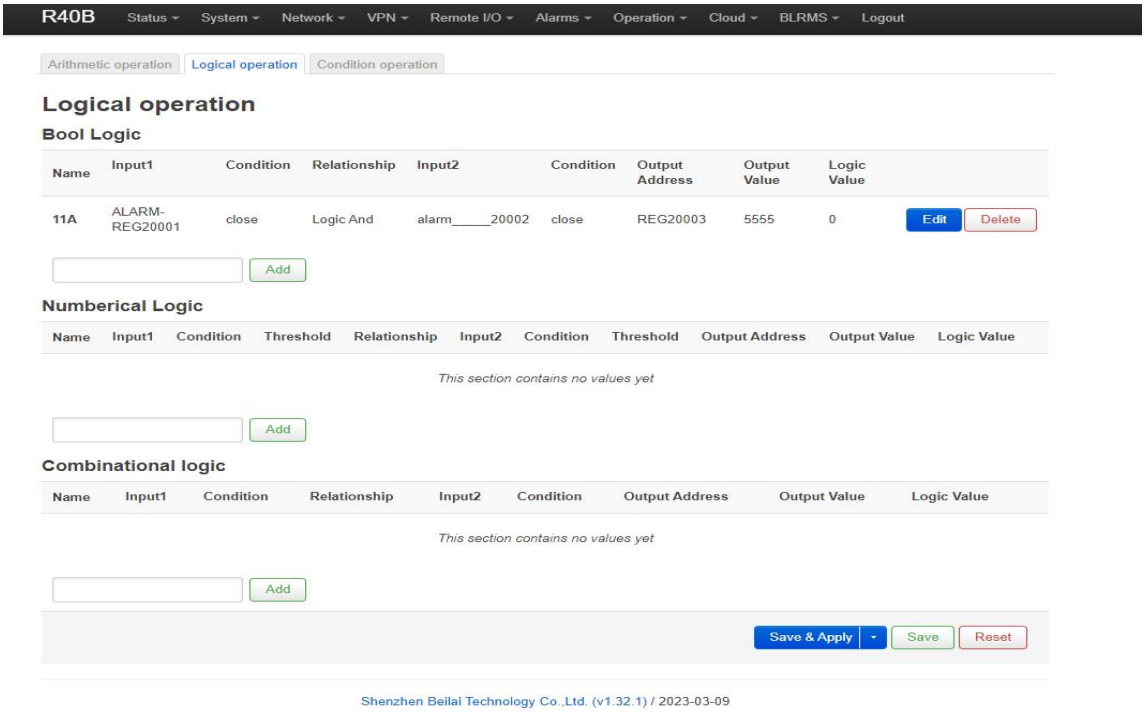
See below:



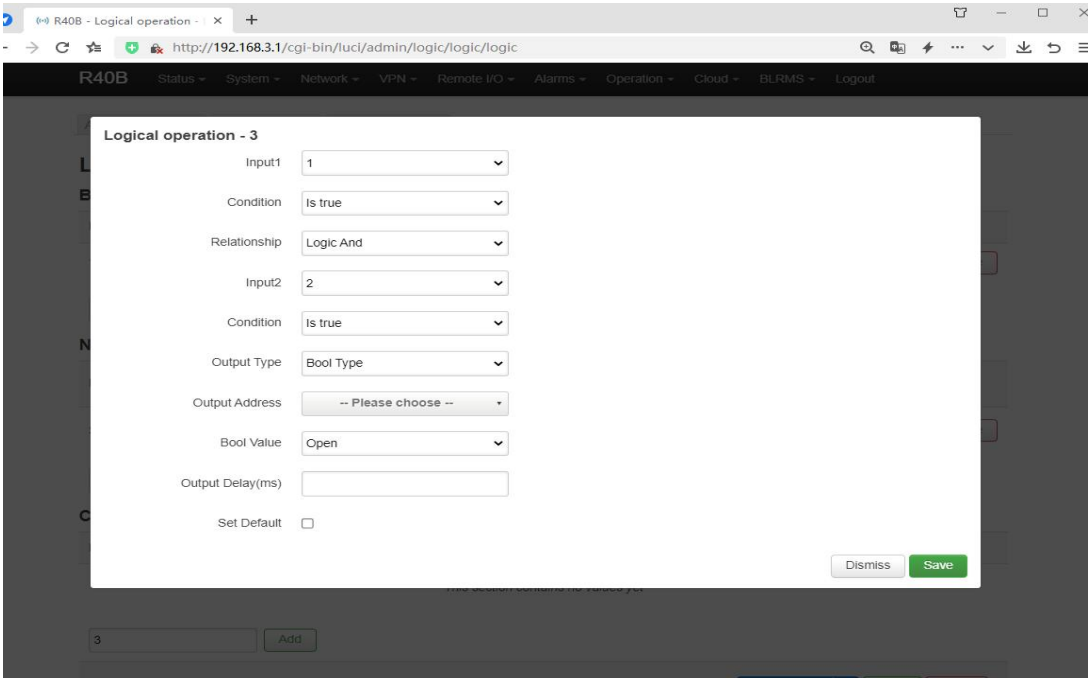
As shown in below, use the virtual serial port tool to simulate the slave 2 register, and the operation result is displayed in SLAVE as follows.



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

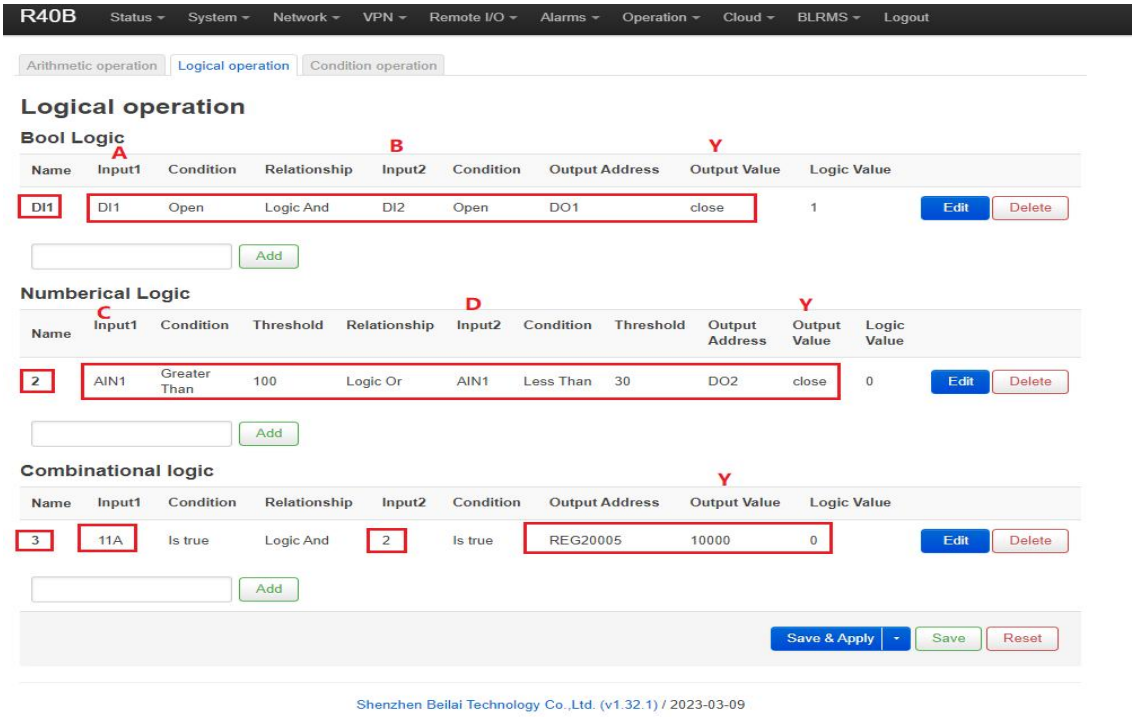


5.7.2.2 Introduction of Logical Operation



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.

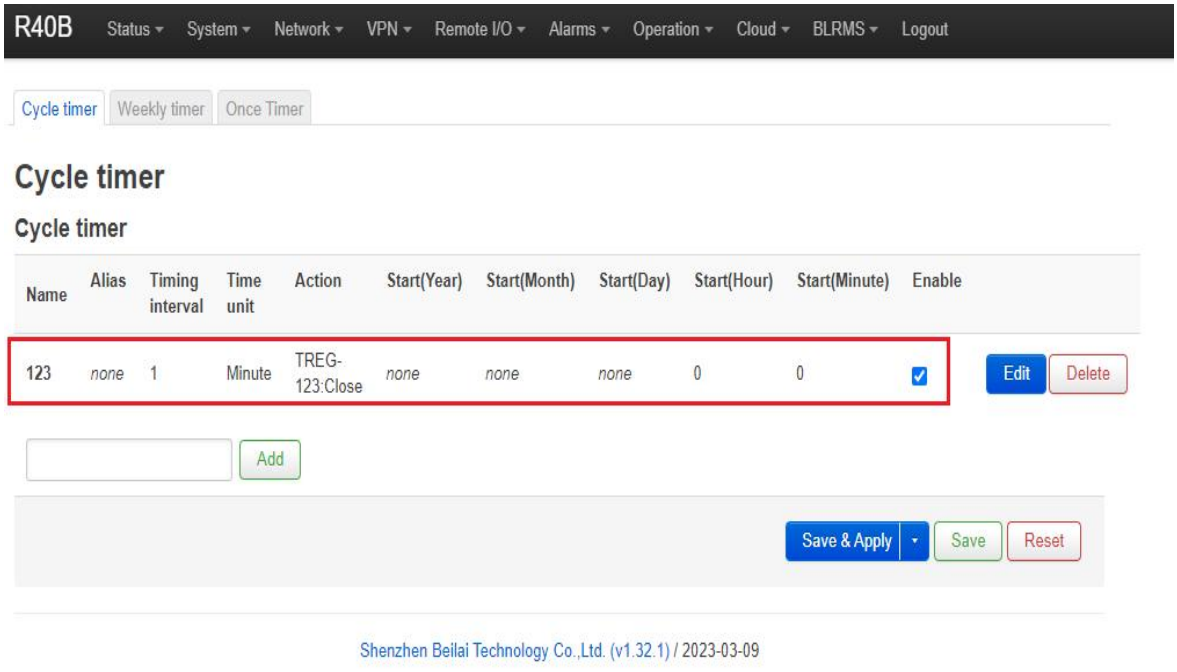
Logical operation example (3)

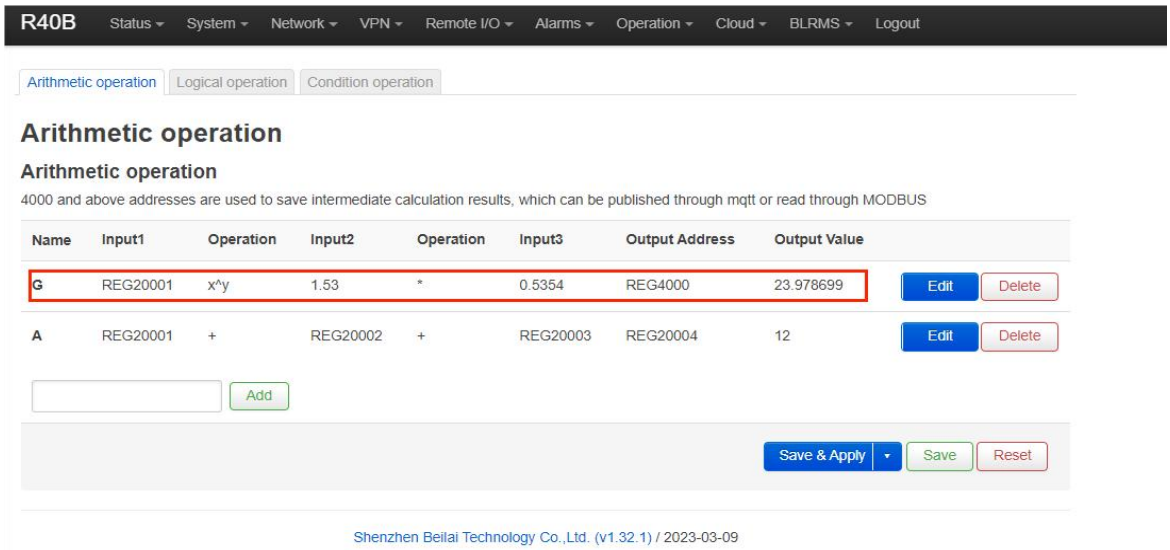
Combined logical operation: the result of the above said logic operation 1 is used as an input value, and the result of logical operation 2 is used as another input value, these two can be combined and comprise logical operation 3.

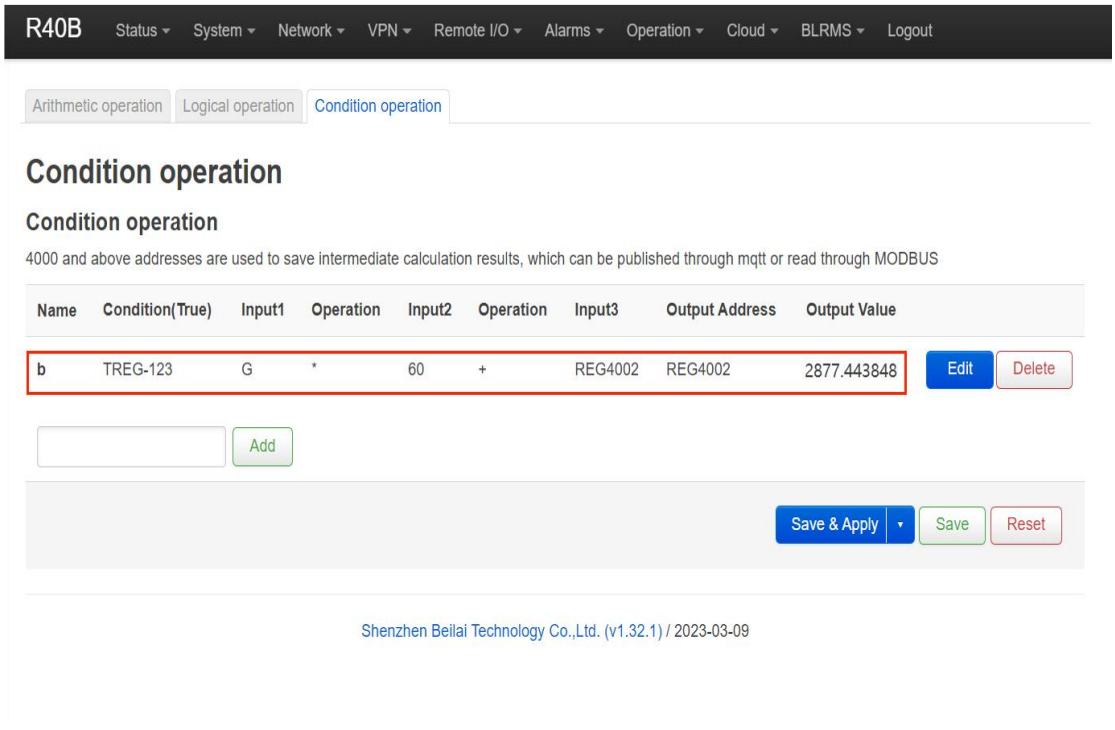
Similary , you could create more combined logical operations.

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.


R40B
Status System Network VPN Remote I/O Alarms Operation Cloud BLRMS Logout
Cycle timer
Weekly timer
Once Timer
Cycle timer
Cycle timer
Name Alias Timing interval Time unit Action Start(Year) Start(Month) Start(Day) Start(Hour) Start(Minute) Enable
123 none 1 Minute TREG-123:Close none none none 0 0
Edit
Delete
Add
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-03-09


R40B
Status System Network VPN Remote I/O Alarms Operation Cloud BLRMS Logout
Arithmetic operation
Logical operation
Condition operation
Arithmetic operation
Arithmetic operation
4000 and above addresses are used to save intermediate calculation results, which can be published through mqtt or read through MODBUS
Name Input1 Operation Input2 Operation Input3 Output Address Output Value
G REG20001 x^y 1.53 * 0.5354 REG4000 23.978699
Edit
Delete
A REG20001 + REG20002 + REG20003 REG20004 12
Edit
Delete
Add
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-03-09



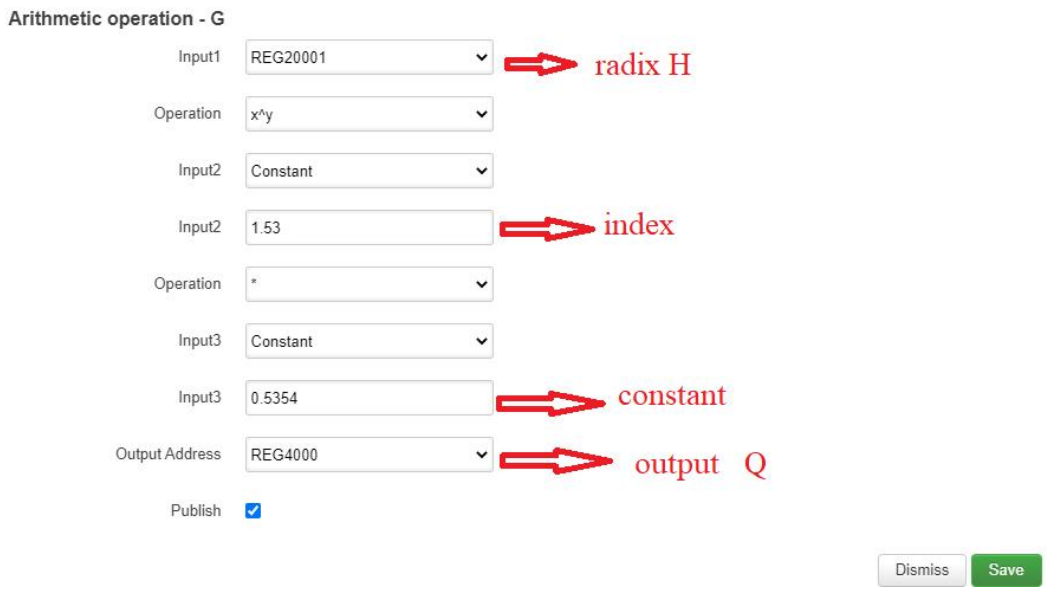
Combined conditions operation can perform exponential logarithmic operations. Take a cumulative water flow that is accumulated every 1 minute as an example to create the process as follows:

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

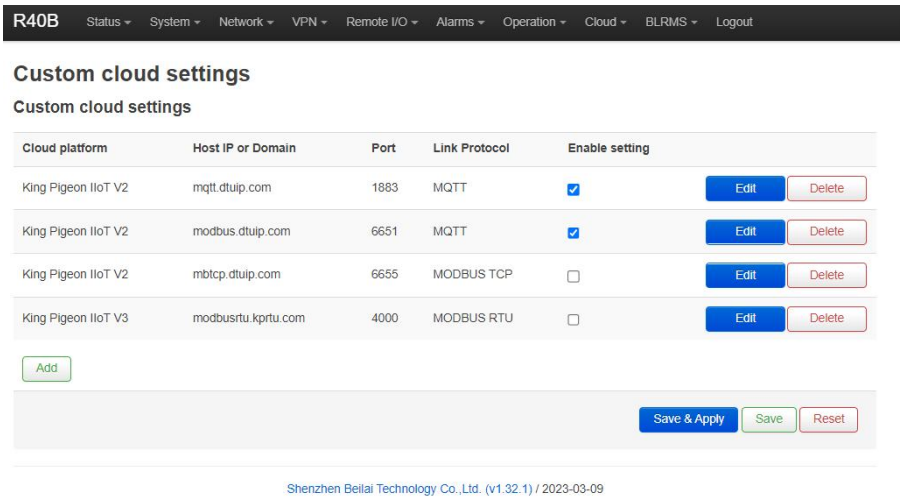
Equal to cumulative output value



5.8 Connection to Cloud Platform

5.8.1 Private Cloud (KPIIOT or Custom MQTT cloud)

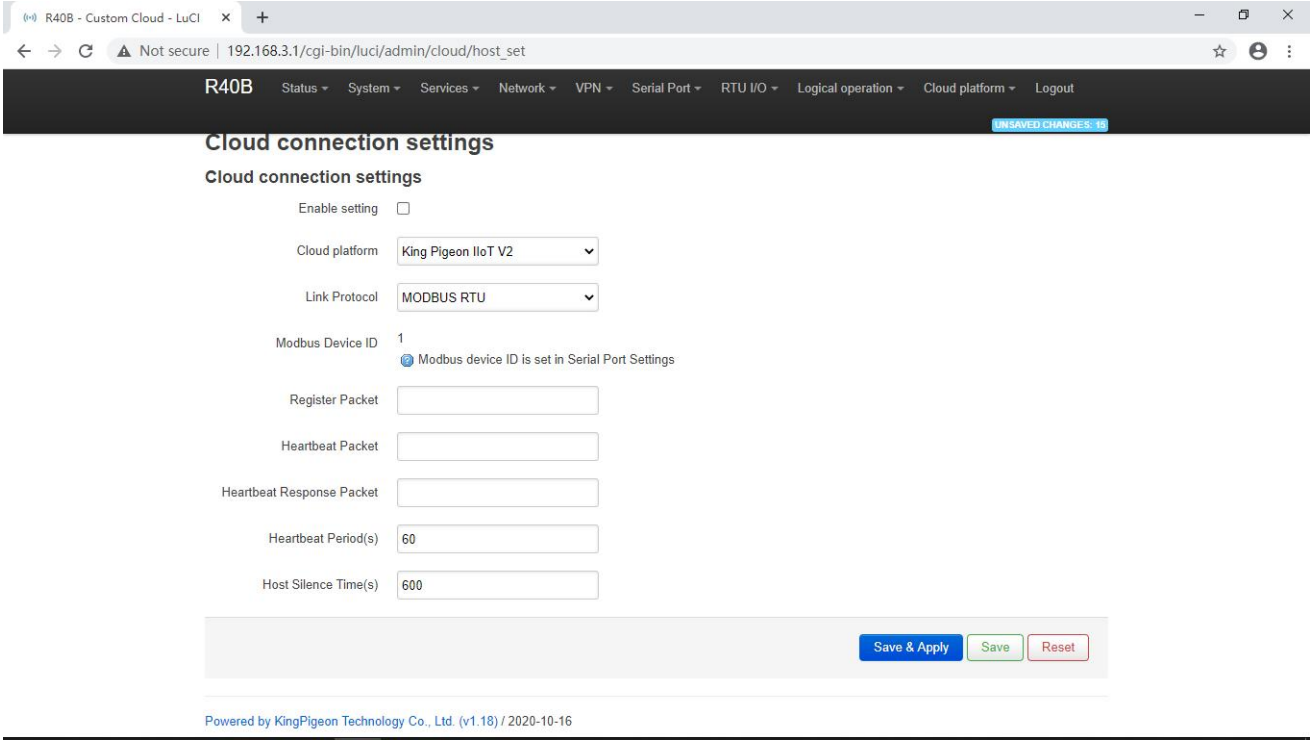
This router can connect to various private cloud platform, including KingPigeon Cloud Platform KPIIOT V2.0 and V3.0 or other private clouds, for example custom MQTT platform. The configuration is described below, and the setting interface is shown in screenshot.



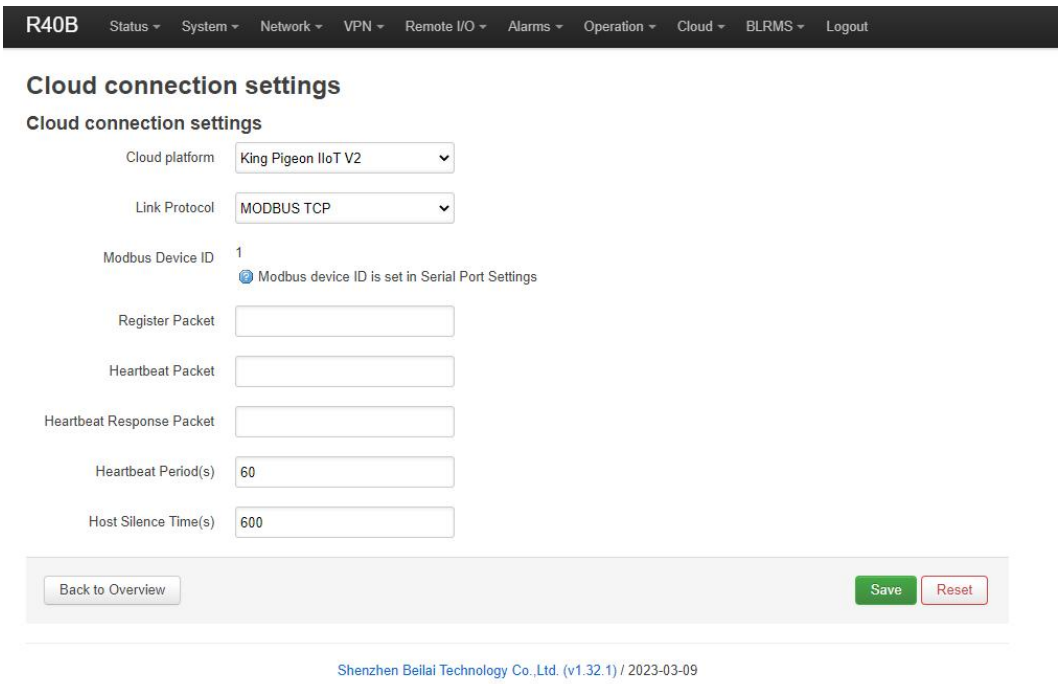
Cloud Connection Settings		
Item		Description
Enable setting		Tick to enable
Cloud Platform		King Pigeon KPIIOT V2, KPIIOT V3, other private clouds
Host domain name and port		2.0Modbus RTU ：modbus.dtuip.com， Port 6651； 2.0Modbus TCP ：mbtcp.dtuip.com， Port 6655； 2.0MQTT：mqtt.dtuip.com， Port 1883 3.0Modbus RTU：modbusrtu.kpiiot.com Port 4000
Link Protocol		Modbus RTU,Modbus TCP ,MQTT
Modbu Protocol Parameters	Modbus Device ID	Default is 1, device ID set in the serial port settings
	Register packet	Server register handshake protocol package, if need contact salesman
	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. If you want to use King Pigeon MQTT, you need to contact the sales to provide the client ID serial number. Just enter the serial number and no other settings are required.
	Publish Period (seconds)	MQTT data timing publish interval
	Enable data retransmission	Click to enable
Custom cloud parameters	Cloud platform name	Customize
	Host IP or domain name	Customize
	Port	Customize
	Link agreement	Modbus RTU, Modbus TCP, MQTT
	Modbus Device ID	Default 1, device ID set in the serial port settings
	Register packet	Customize
	Heartbeat packet, heartbeat response packet, heartbeat cycle, host silent time (as defined above)	

5.8.1.1 KingPigeon Cloud Platform (KPIIOT)

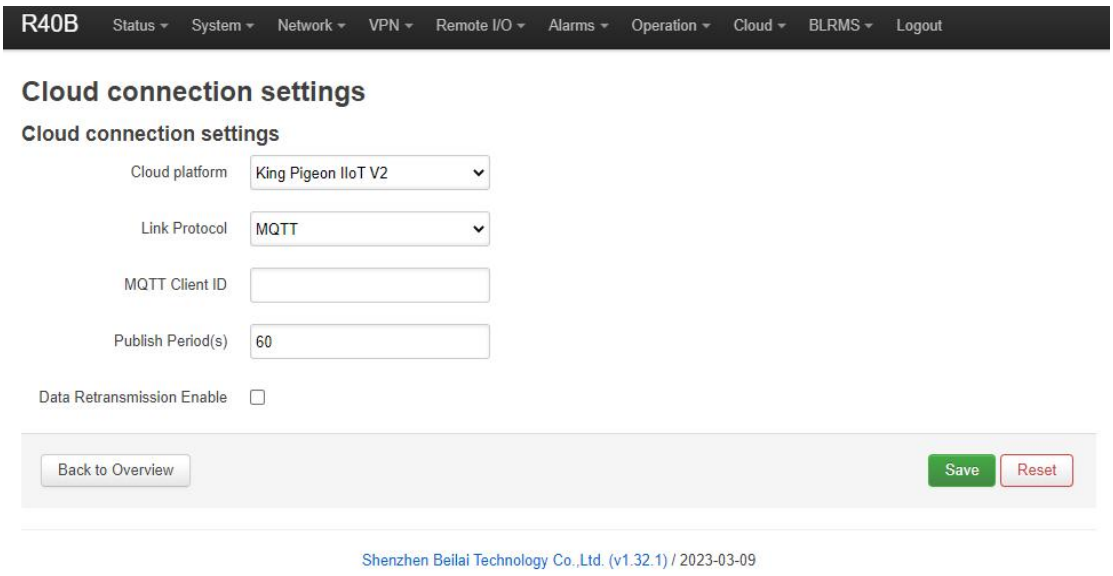
Connection to KingPigeon cloud KPIIOT V2.0 by Modbus RTU protocal, see below setting



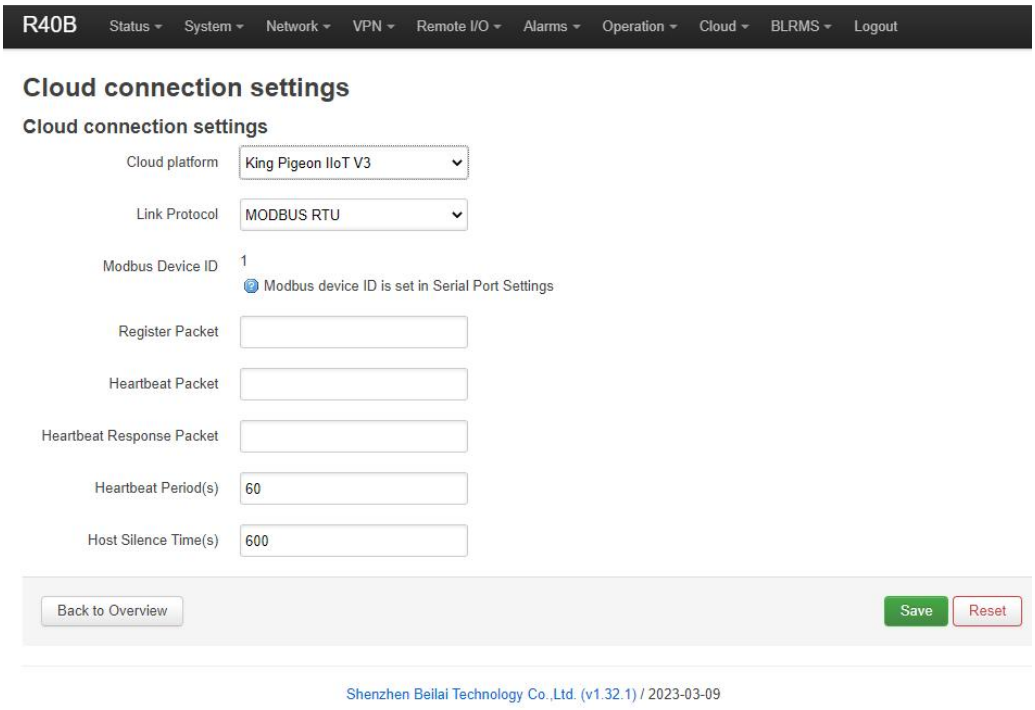
Connection to KingPigeon cloud KPIIOT V2.0 by Modbus TCP protocal, see below setting



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

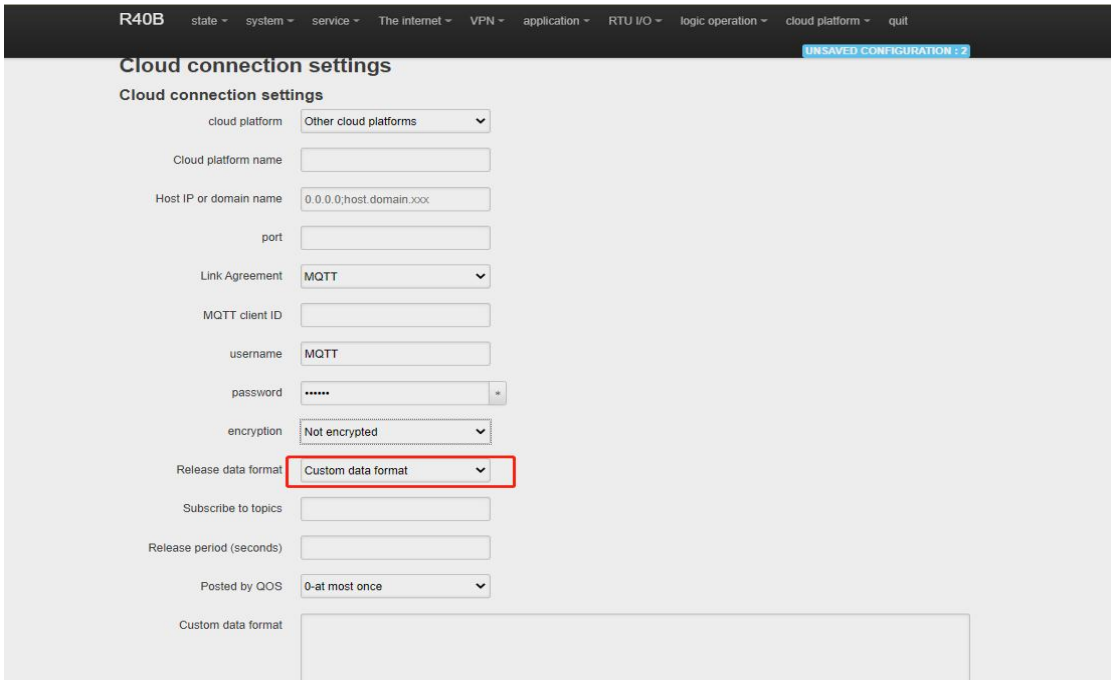


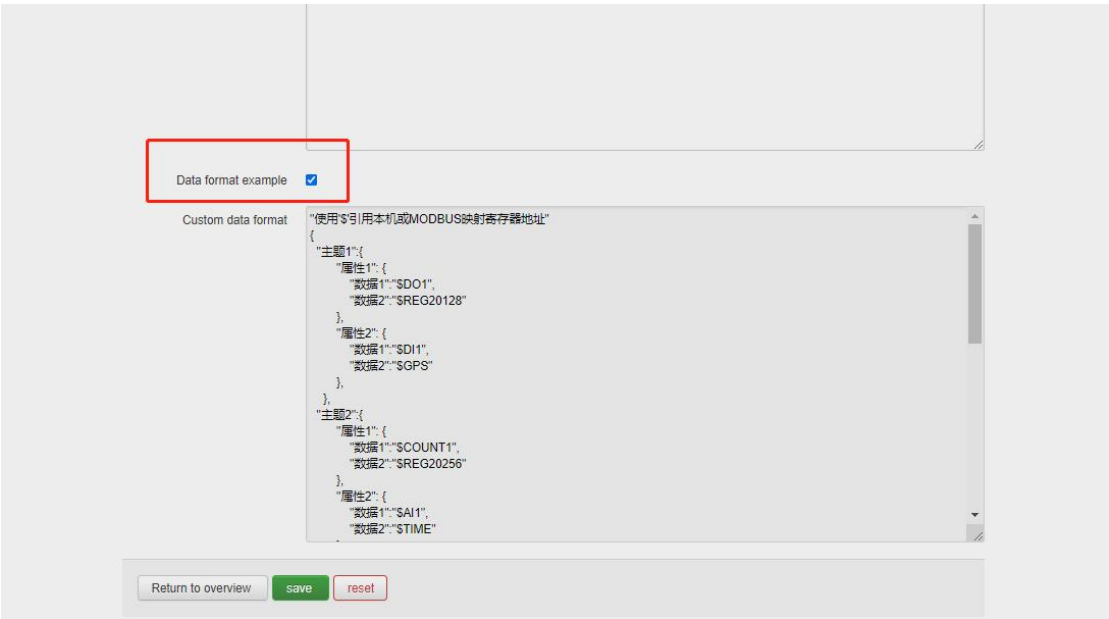
Connection to KingPigeon cloud KPIIOT V3.0 by Modbus RTU protocal, see below setting



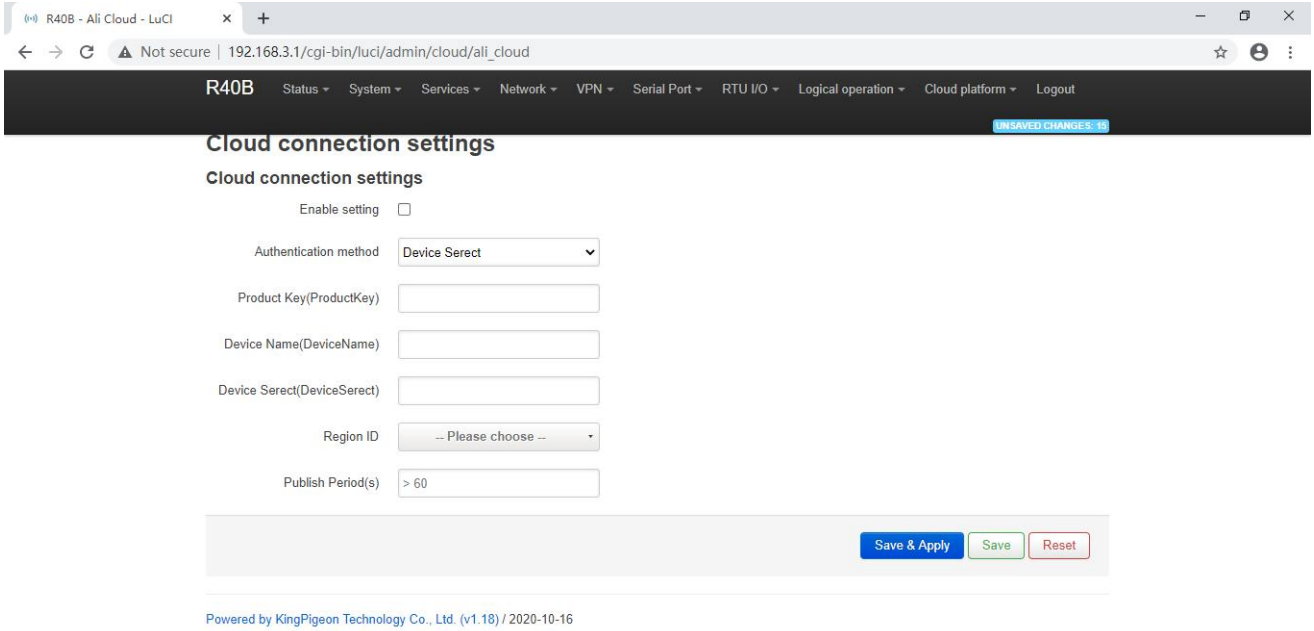
5.8.1.2 Other Private Cloud --- Custom MQTT

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


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

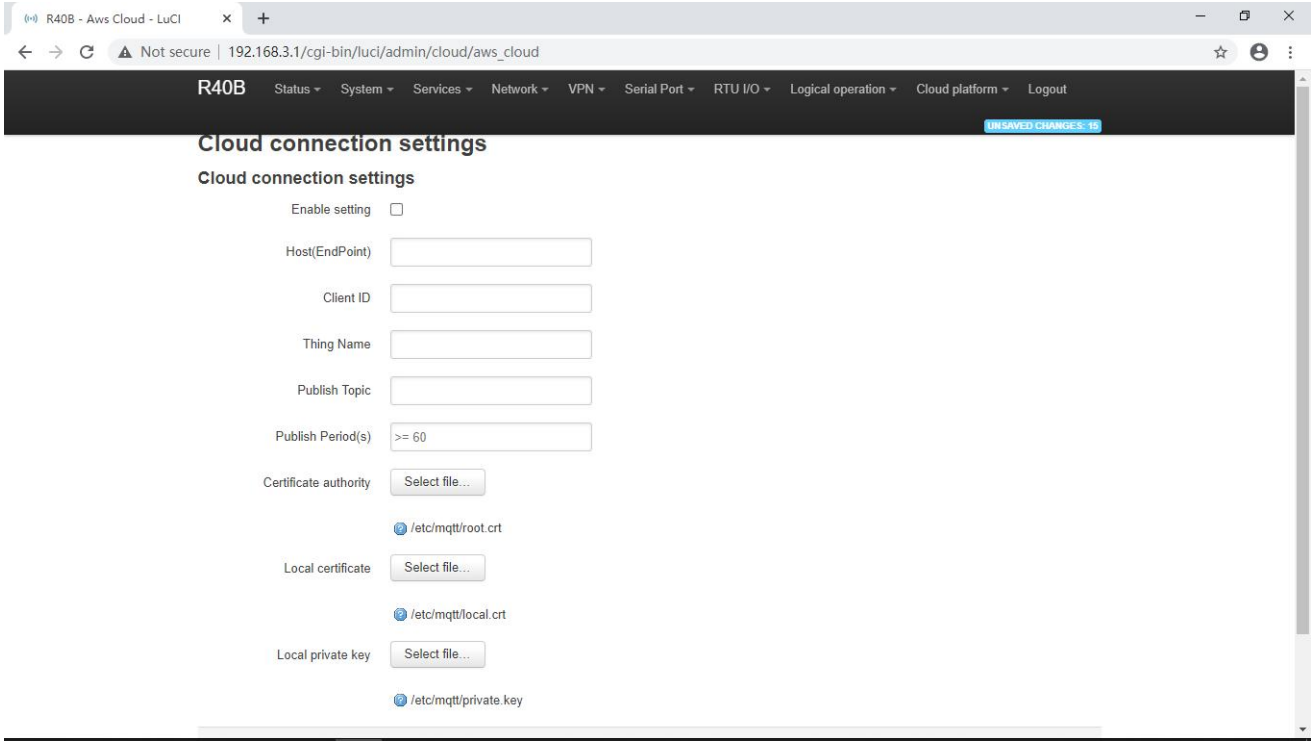

Data format example
Custom data format
"使用$引用本机或MODBUS映射寄存器地址"
{
"主题1":{
"属性1": {
"数据1":"$DO1",
"数据2":"$REG20128"
},
"属性2": {
"数据1":"$DI1",
"数据2":"$GPS"
},
},
"主题2":{
"属性1": {
"数据1":"$COUNT1",
"数据2":"$REG20256"
},
"属性2": {
"数据1":"$AI1",
"数据2":"$TIME"
Return to overview
save
reset

5.8.2 Alibaba Cloud Platform



Ali Cloud Connection Settings	
Item	Description
Enable setting	Tick to enable
Authenticatioin 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 Serect	Set the device key on Alibaba Cloud
Region ID	Ali cloud region
Publish period (seconds)	>60s
Certification authority (root certificate)	Choose file upload
Local certificate	Choose file upload
Local key	Choose file upload
Only publish changed data	Click to enable

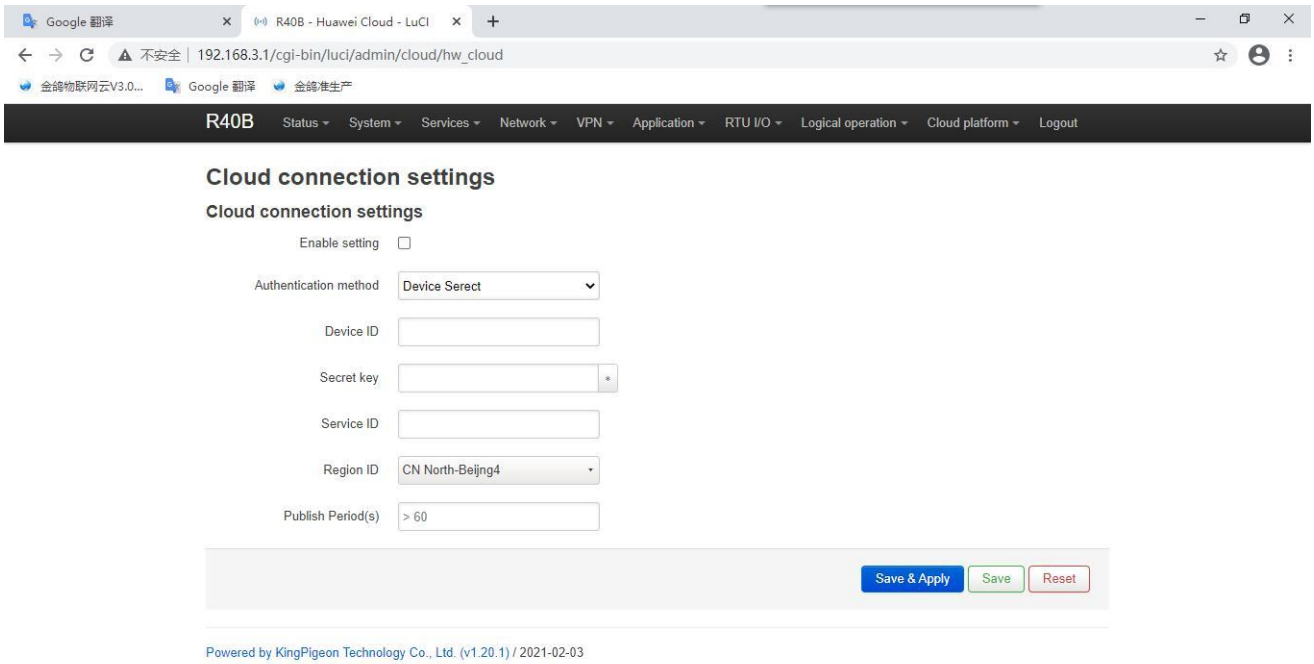
5.8.3 AWS Cloud

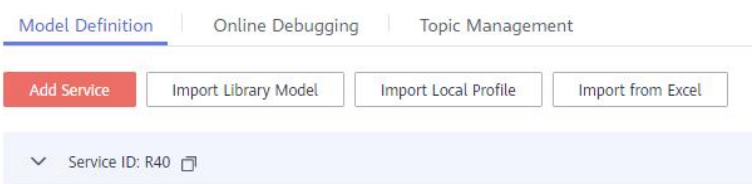


AWS Cloud Connection Settings	
Item	Description
Enable setting	Tick to enable
Host（Endpoint）	Set End point
Client ID	The client identifier used in the MQTT connection message, the server uses the client identifier to identify the client, and each client connected to the server has a unique client identifier.
Thing name	Set thing 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)	>60s
Certification authority (root certificate)	Choose file upload
Local certificate	Choose file upload
Local key	Choose file upload
Only publish changed data	Click to enable

5.8.4 Huawei Cloud

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

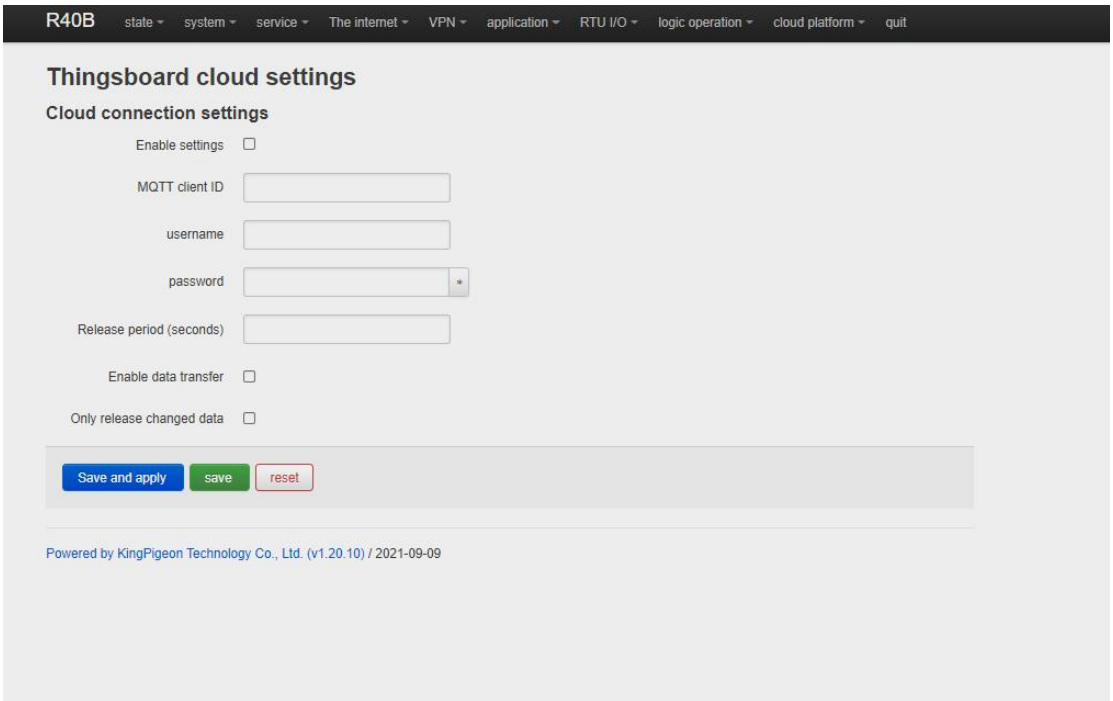


Huaweicloud connection settings	
Item	Description
Enable setting	Tick to enable
Authentication method	The device secret key method and the authentication certificate method can be selected, and the authentication certificate method needs to upload the certificate
Devicde ID	The ID of the device when HUAWEI CLOUD creates the device,eg, 
Service ID	The product needs to create a service to report data,eg. 
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
Only publish changed data	Click to enable

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	Tick to enable
Host（Endpoint）	Set End point
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.
Thing name	Set thing 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)	>60s
Certification authority (root certificate)	Choose file upload
Local certificate	Choose file upload
Local key	Choose file upload
Enable data retransmission	Click to enable this function
Only publish changed data	Click to enable this function

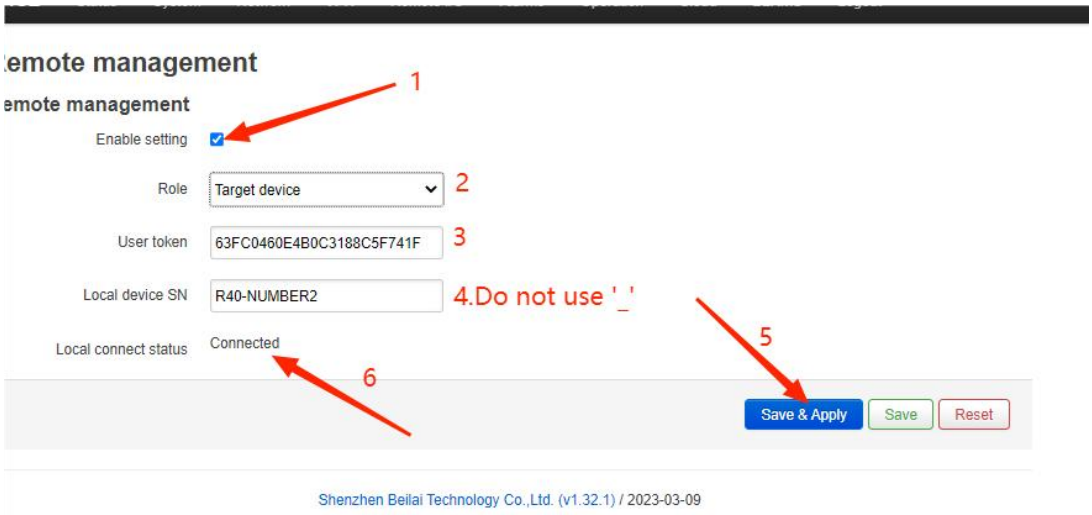
For Thingsboard cloud device user manual, please refer to the Thingsboard Getting Started document

5.9 BLRMS (Remote Management devices System)

5.9.1 Introduction

R40 edge computing router supports remote configuration and remote upgrade functions. These functions are utilized with the help of BLiioT's software platform BLRMS (BLiioT Remote Management System). To use these functions, people must have an R40 router device beside himself. It is called local device. The remote management targe device R40 router is called as target device. In short, people remotely manage target R40 device by local R40 via BLRMS platform.

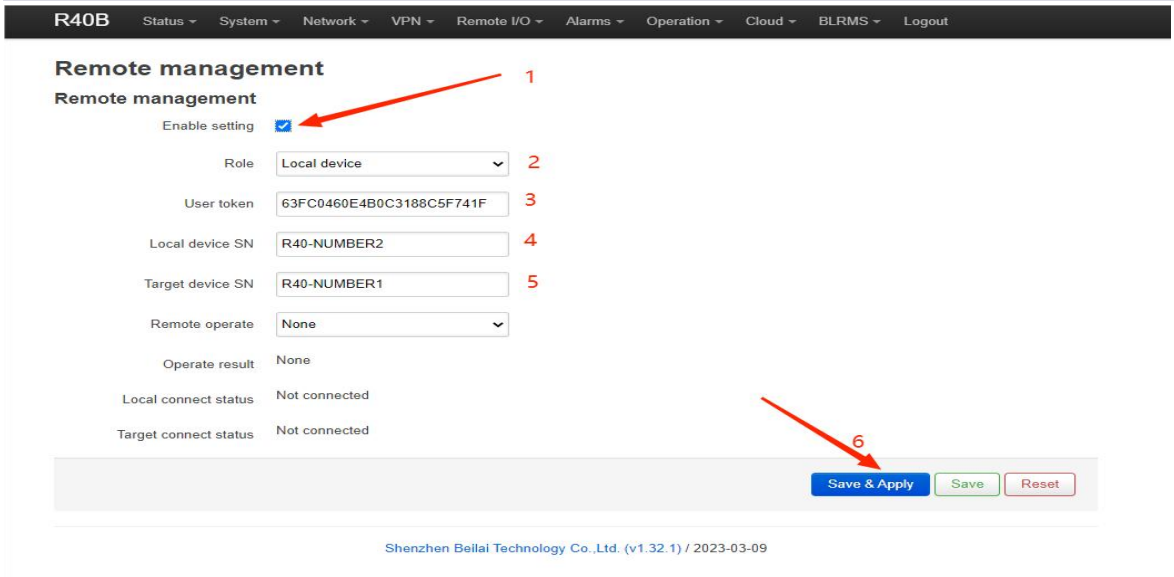
Target device R40 configuration page is shown below:



Remote Management Setting

Item	Description
Enable setting	Tick to enable
Role	Select “Target device”
User token	The user token is given by BLRMS, "device management" - "communication key"
Local device SN	SN is serial number of the device. People can name it by himself, maximum 128 characters. Never duplicate SN to cause conflict.
Local connection status	Status of connection to the BLRMS system

Local device R40 configuration page is shown below:



Remote Management Setting	
Item	Description
Enable setting	Tick to enable
Role	Select “Local device”
User token	Must be same as that on Target device
Local device SN	SN is serial number of the device. People can name it by himself, maximum 128 characters. Never duplicate SN to cause conflict.
Target device SN	When the role is choosen “Target device” , It is the Local device SN
Remote operate	Choose from Read configuration, Write configuration, Update firmware
Operate result	show the result
Local connect status	The status of connection local device to BLRMS
Target connect status	The status of connection Target device to BLRMS

Note: The configuration will take effect only after clicking "Save and Apply".

5.9.2 Operation example

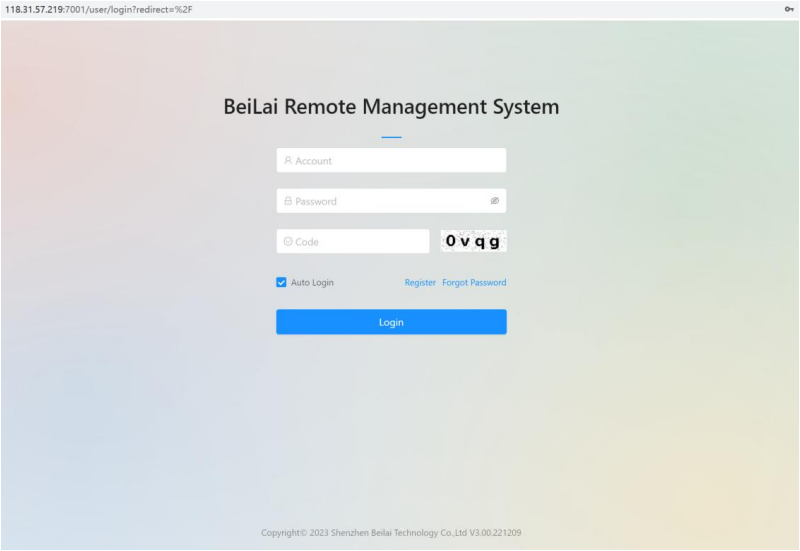
5.9.2.1 Register account at BLRMS

BLRMS platform website: my-rtu.com

After the registration is successful, return to the main page and enter the account password to log in to the system.

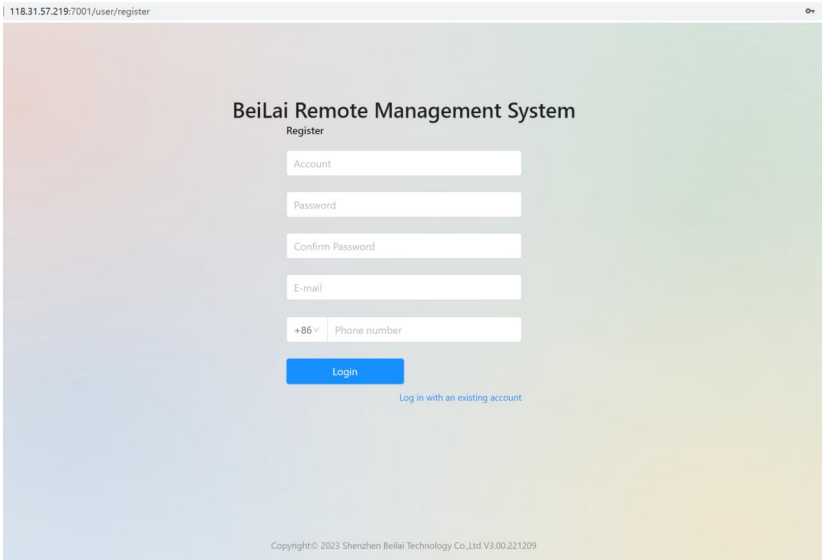
After logging in to the system, the system will automatically generate a Token for you.

The login and registration pages are as follows:



1-1

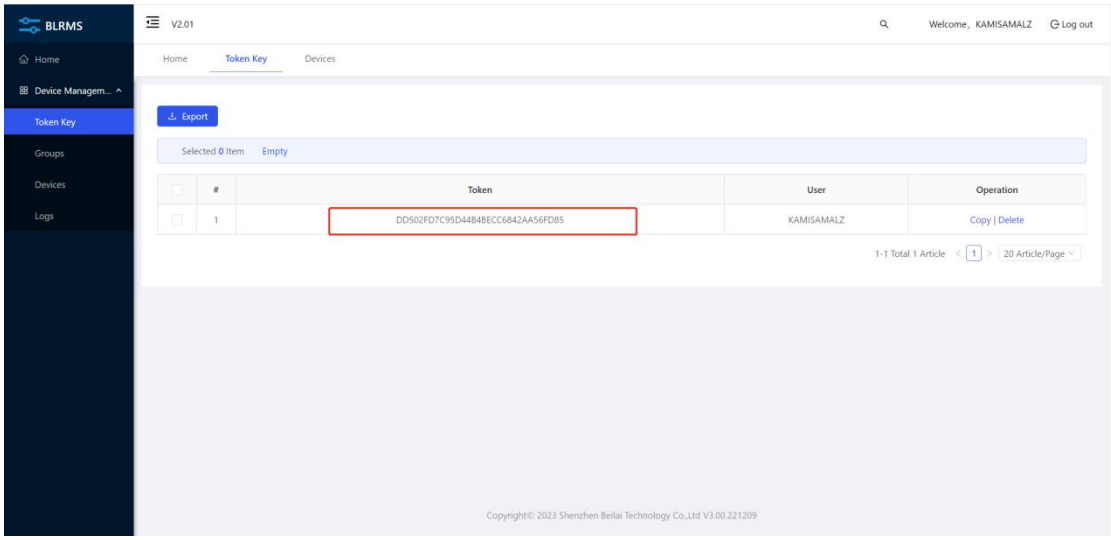
Register



1-2

5.9.2.2 Obtain communication key (the token)

After register an account successfully, the BLRMS system automatically generates a Token for user. It is the communication key, as the associated identification number.
Click the item "Device Management" - "Token Key" in the left menu, and you can see the Token, as shown in the picture below.
Please put this Token on the IoT device. All IoT devices used by this user should use the same Token.



1-3

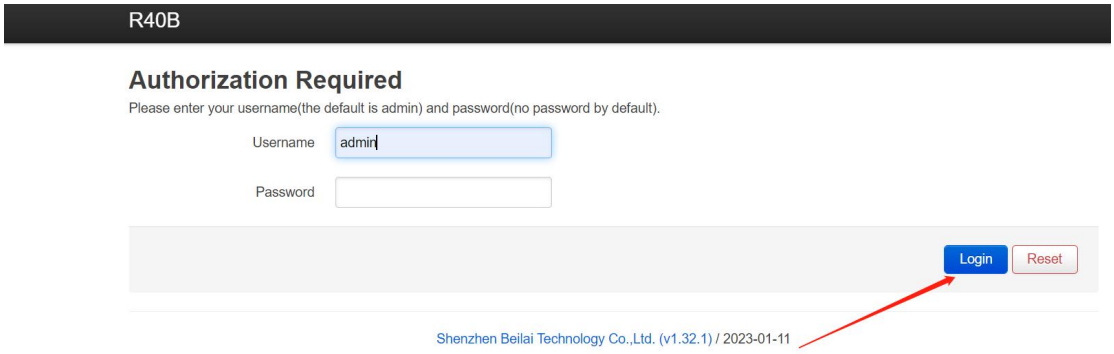
5.9.2.3 Configure the device to associate it with the BLRMS platform

Note below Requirements for using the BLRMS service.
You need two R40 devices, one as local device and the other as the target device.
The remote management targe device R40 router is called as target device

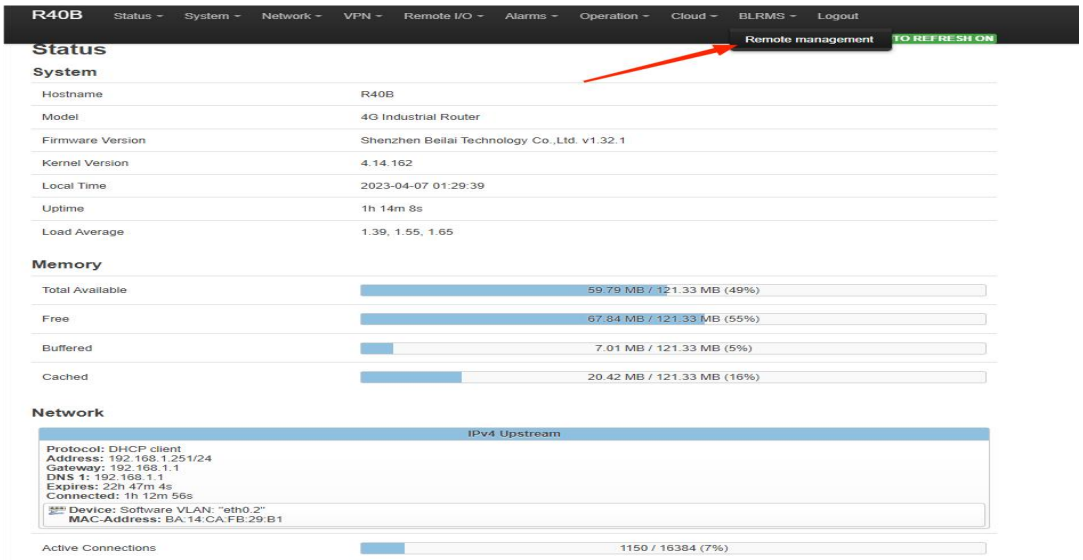
When you use the BLRMS service for the first time, you need to update the firmware programs of the two devices before associating them with the BLRMS platform.

5.9.2.3.1 Configue the target device

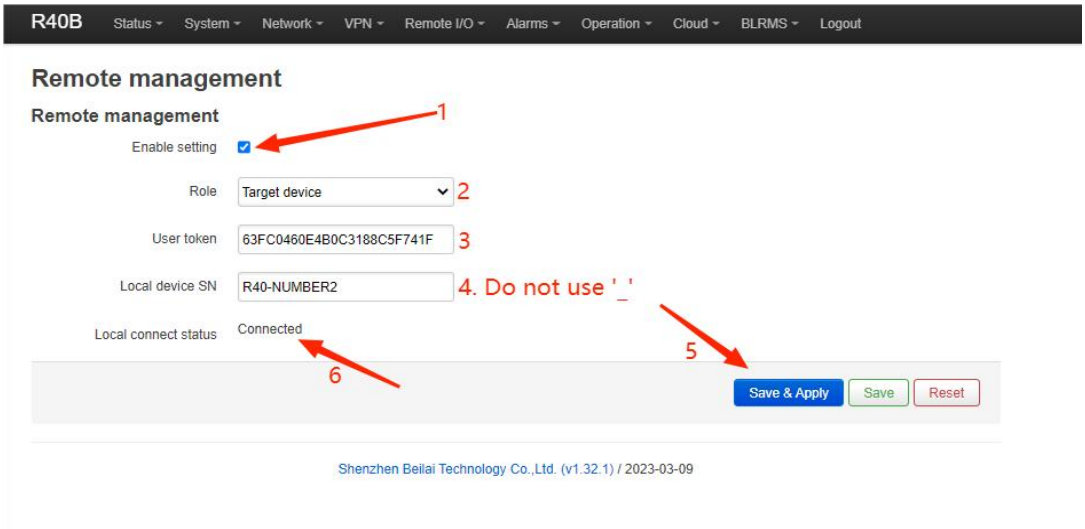
Open the browser and enter the IP address of the R40 device
And then enter the R40 device configuration interface. See below
Default IP of R40 device: 192.168.3.1



1-4

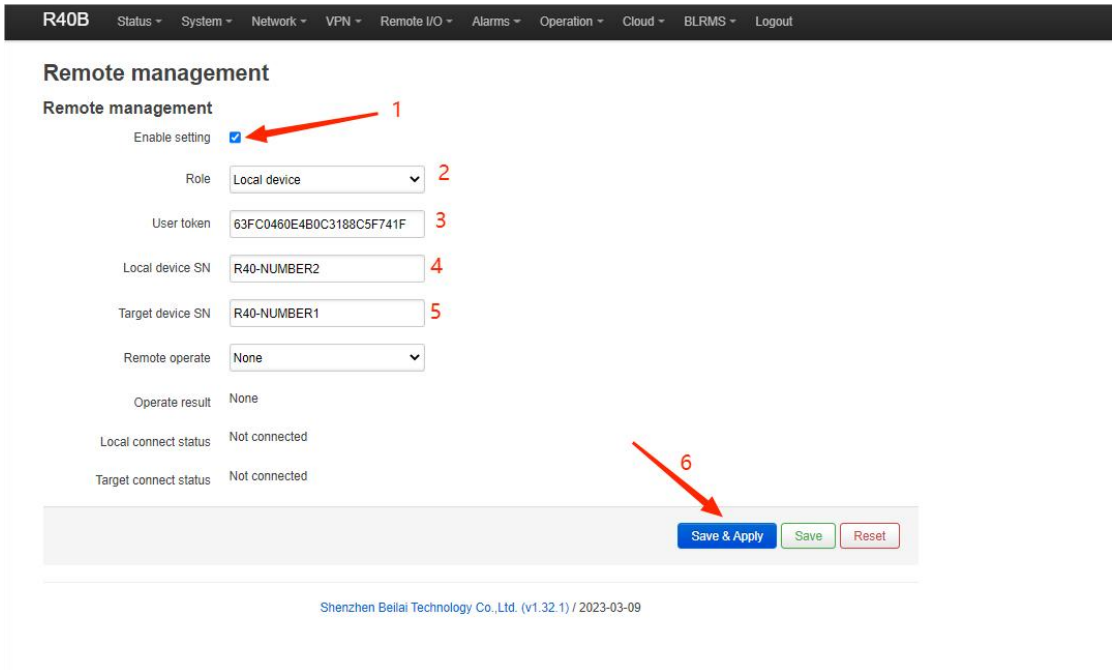


1-5



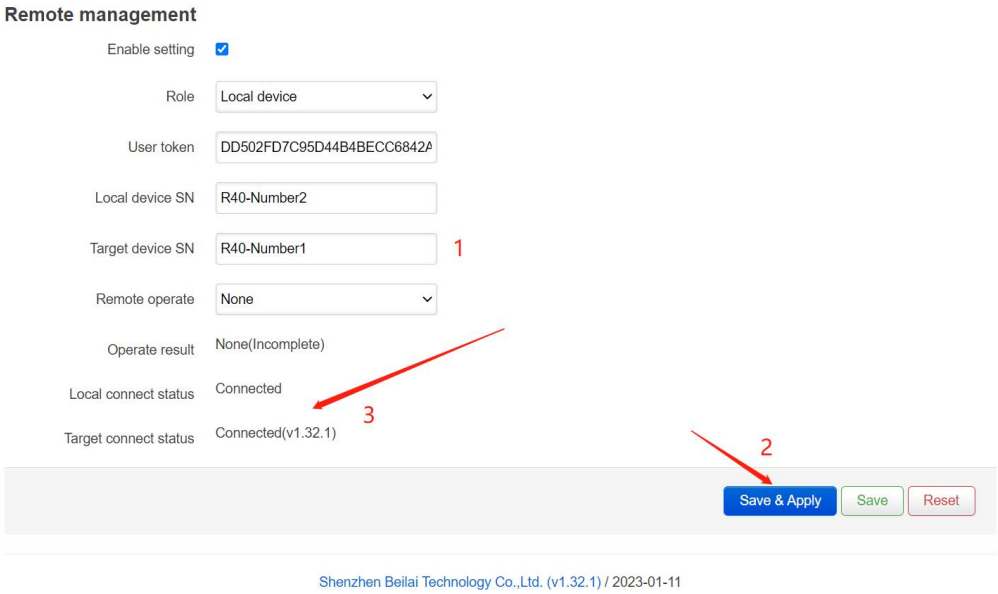
1-6

5.9.2.3.2 Configue the local device

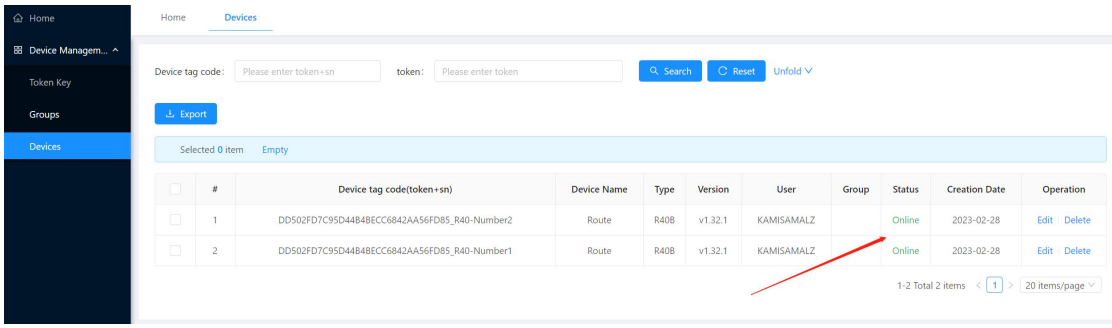


1-7

The device is associated with the platform successfully



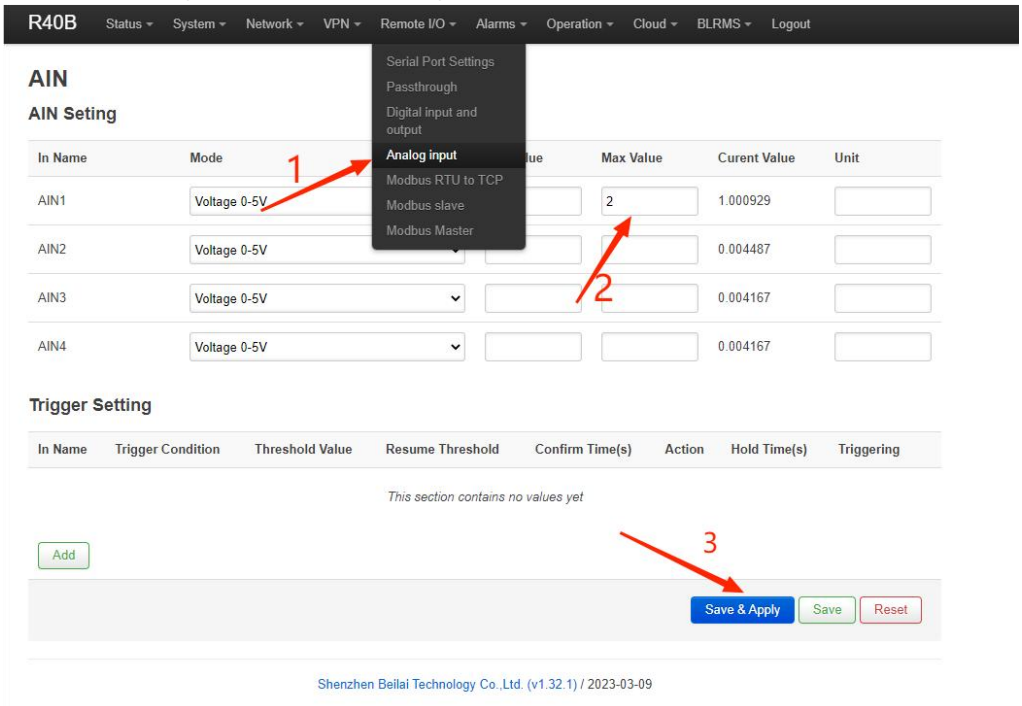
1-8



1-9

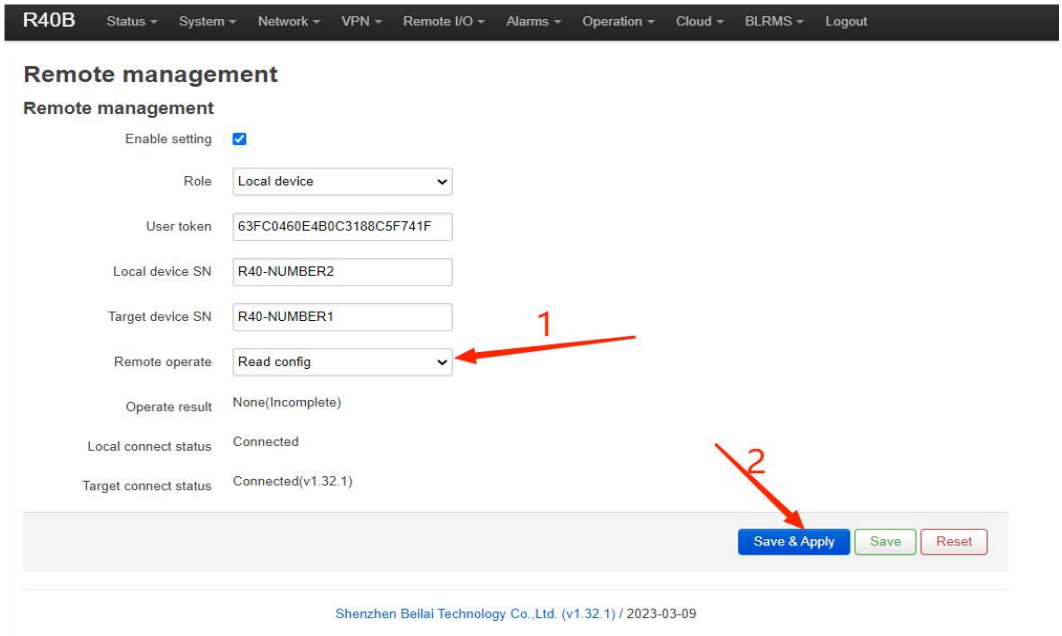
5.9.2.4 Operation: remotely read the R40 device setting

Save the configuration after the target device adds the value

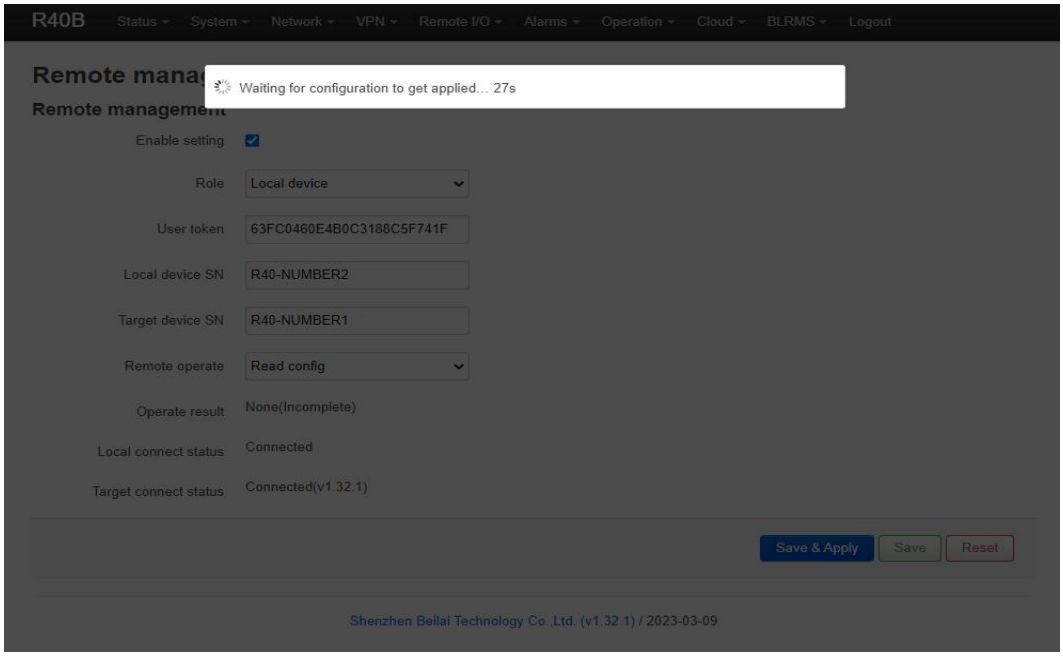


2-1

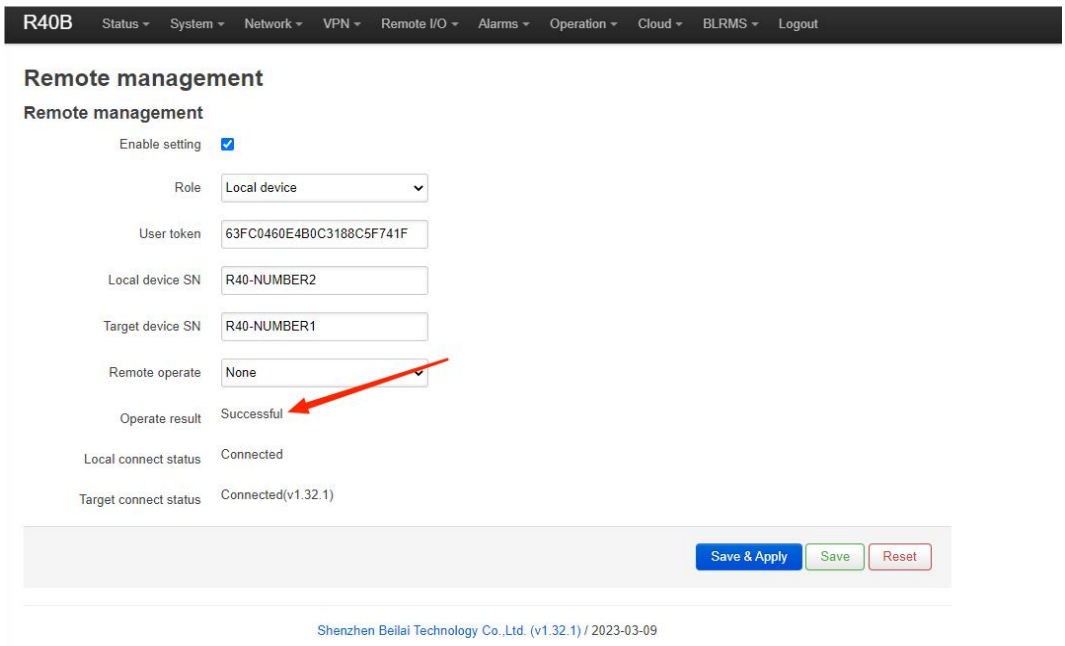
The local device reads the configuration file of the target device


R40B
Status
System
Network
VPN
Remote I/O
Alarms
Operation
Cloud
BLRMS
Logout
Remote management
Remote management
Enable setting
Role
Local device
User token
63FC0460E4B0C3188C5F741F
Local device SN
R40-NUMBER2
Target device SN
R40-NUMBER1
Remote operate
Read config
Operate result
None(Incomplete)
Local connect status
Connected
Target connect status
Connected(v1.32.1)
1
2
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-03-09

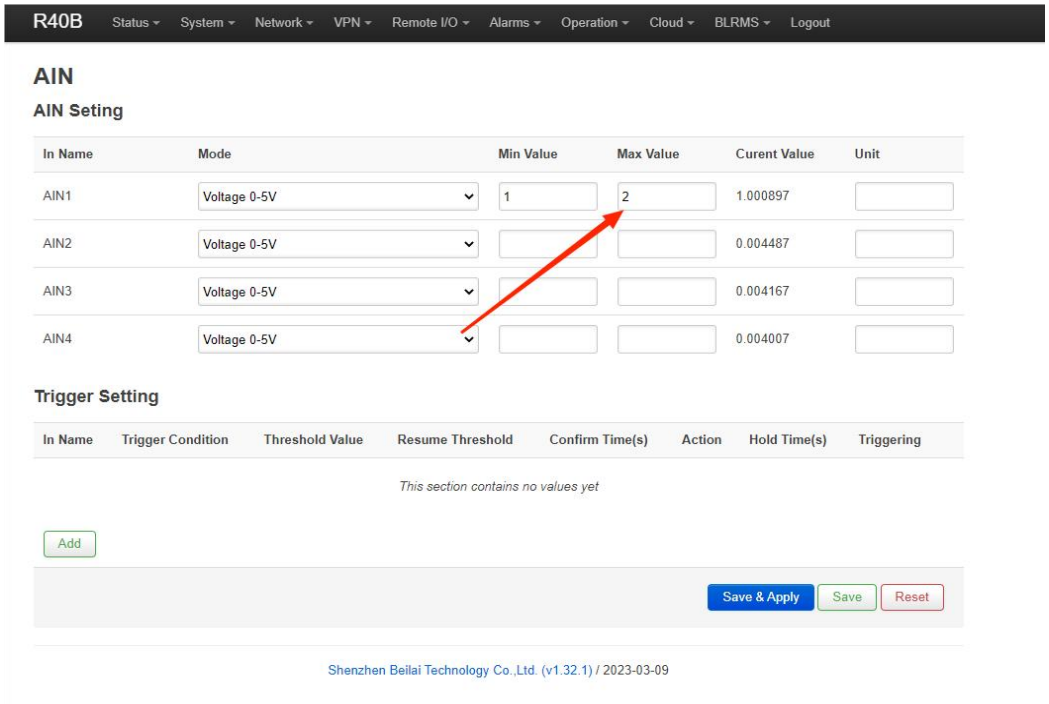
2-2


R40B
Waiting for configuration to get applied... 27s
Enable setting
Role
Local device
User token
63FC0460E4B0C3188C5F741F
Local device SN
R40-NUMBER2
Target device SN
R40-NUMBER1
Remote operate
Read config
Operate result
None(Incomplete)
Local connect status
Connected
Target connect status
Connected(v1.32.1)
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-03-09

2-3


R40B
Status System Network VPN Remote I/O Alarms Operation Cloud BLRMS Logout
Remote management
Remote management
Enable setting
Role
Local device
User token
63FC0460E4B0C3188C5F741F
Local device SN
R40-NUMBER2
Target device SN
R40-NUMBER1
Remote operate
None
Operate result
Successful
Local connect status
Connected
Target connect status
Connected(v1.32.1)
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-03-09

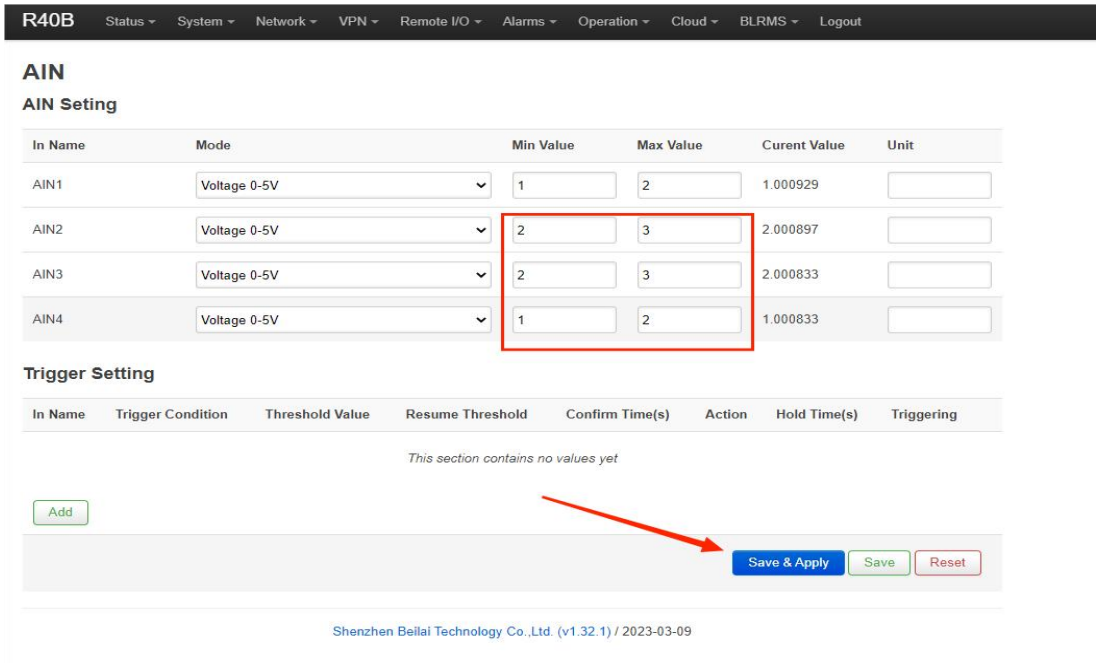
2-4


R40B
Status System Network VPN Remote I/O Alarms Operation Cloud BLRMS Logout
AIN
AIN Seting
In Name Mode Min Value Max Value Curent Value Unit
AIN1 Voltage 0-5V 1 2 1.000897
AIN2 Voltage 0-5V 0.004487
AIN3 Voltage 0-5V 0.004167
AIN4 Voltage 0-5V 0.004007
Trigger Setting
In Name Trigger Condition Threshold Value Resume Threshold Confirm Time(s) Action Hold Time(s) Triggering
This section contains no values yet
Add
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-03-09

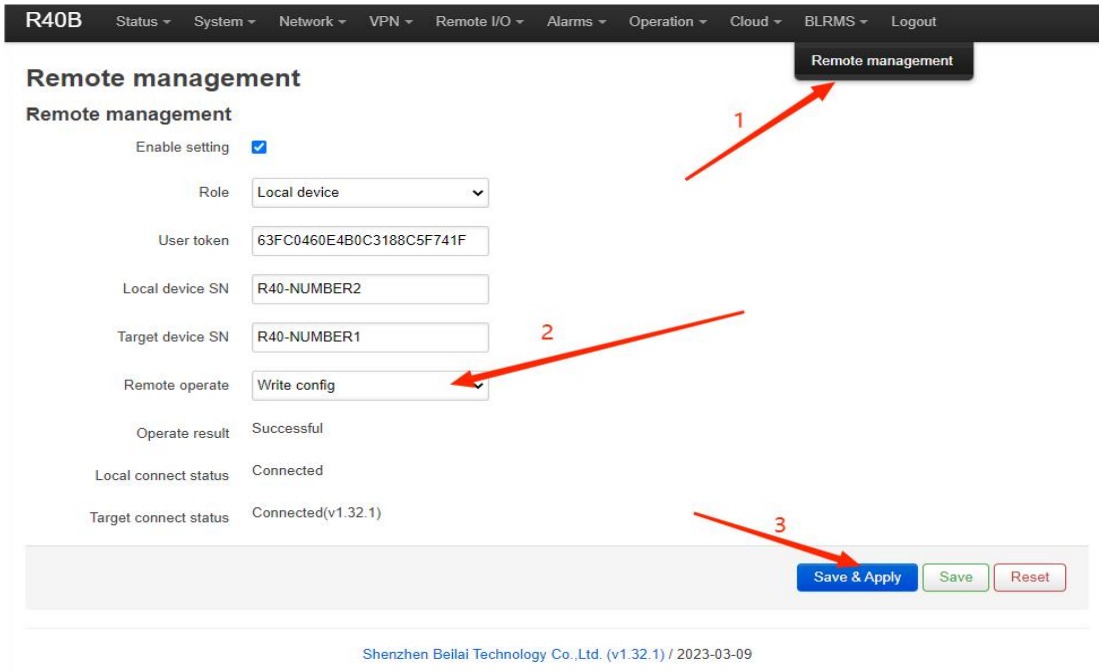
2-5

5.9.2.5 Operation: remotely write the setting to R40 device

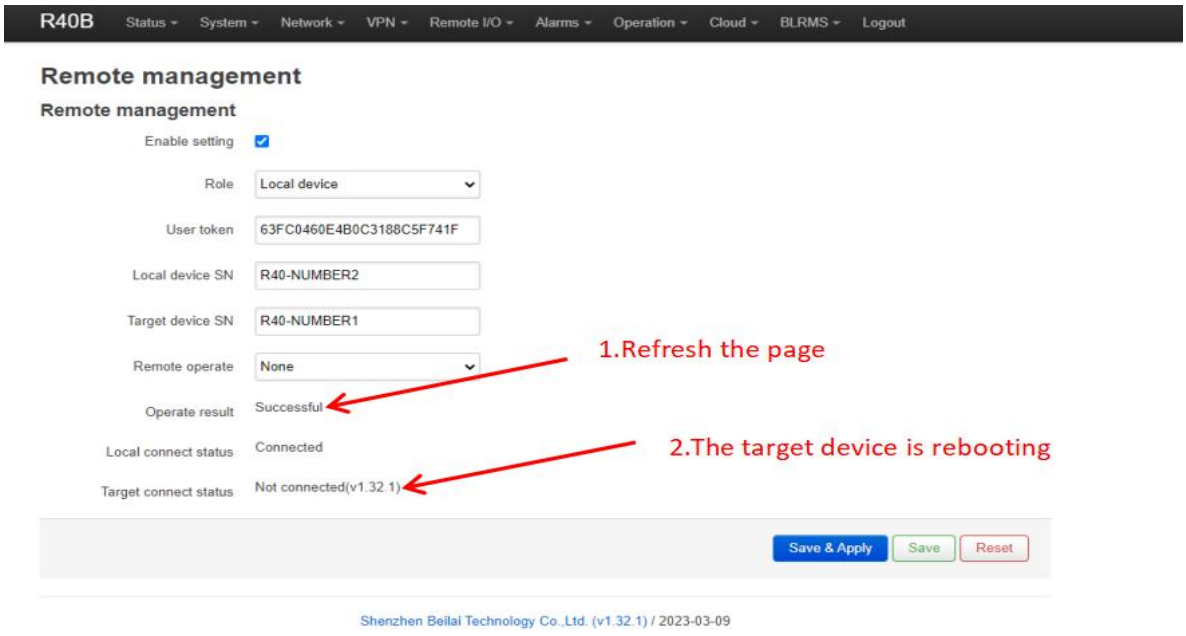
"Remote Write Configuration" this operation will reboot the target device



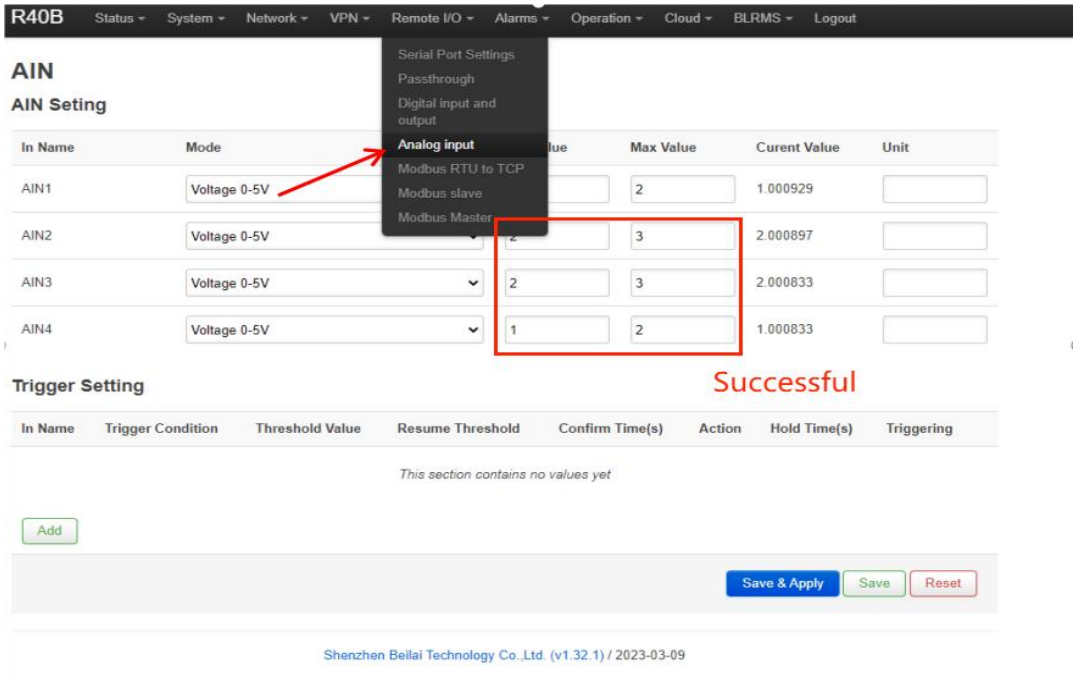
2-6



2-7



2-8



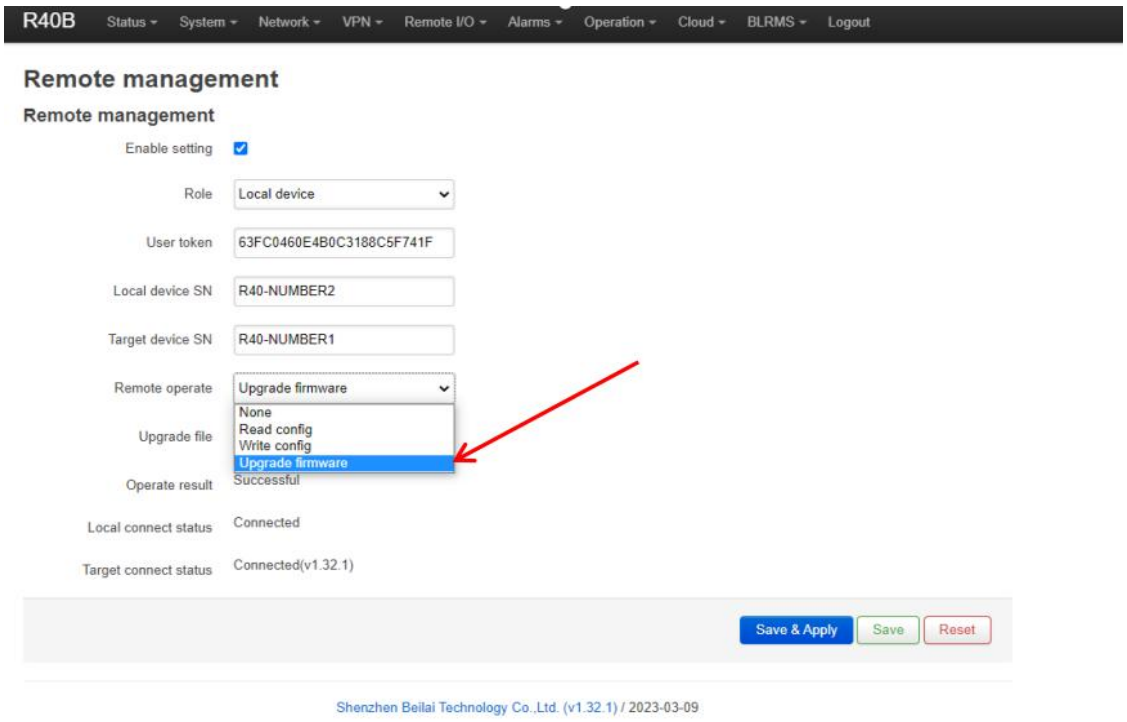
2-9

Note:

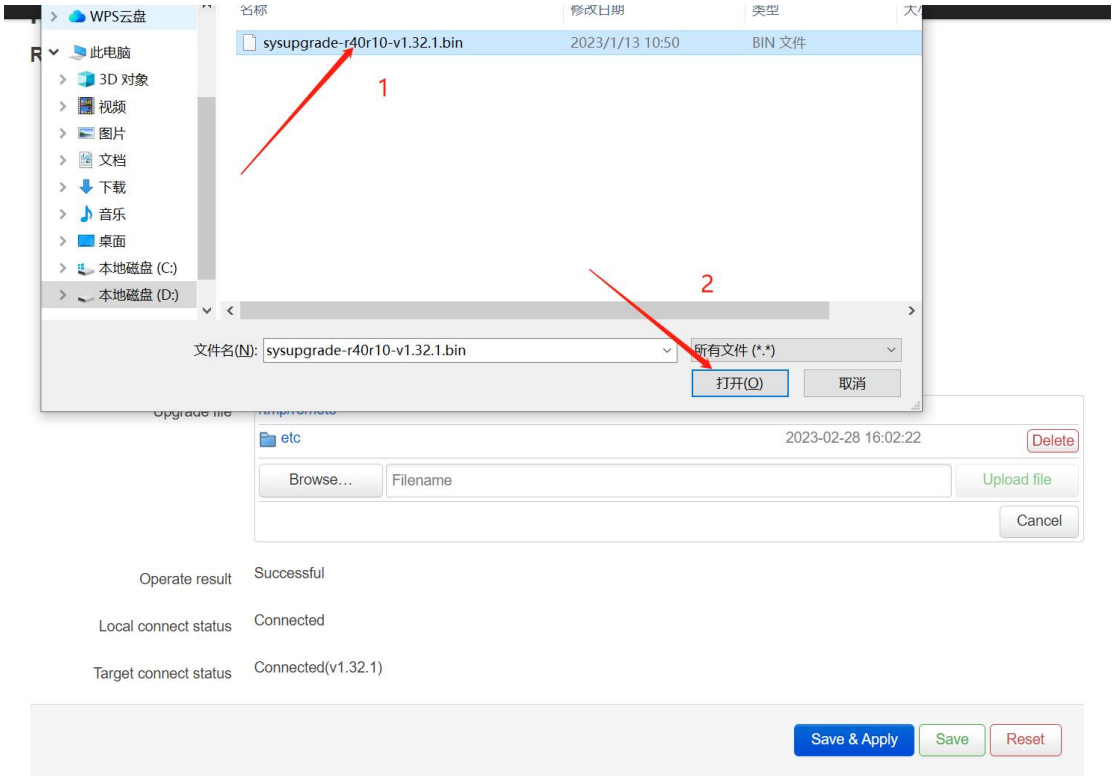
Those setting related to networking cannot be written, such as IP addresses.

All other configuration information can be writen.

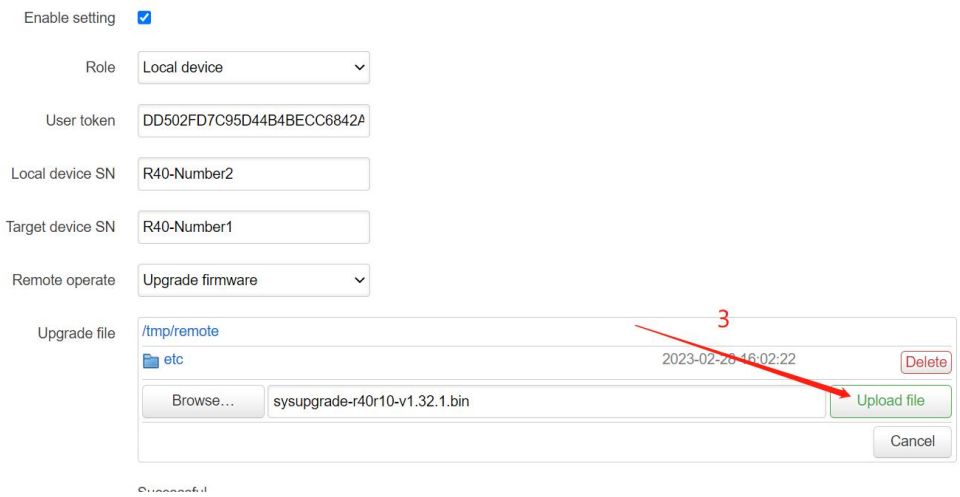
5.9.2.6 Operation: remotely upgrade the firmware of R40 device


R40B
Status
System
Network
VPN
Remote I/O
Alarms
Operation
Cloud
BLRMS
Logout
Remote management
Remote management
Enable setting
Role
Local device
User token
63FC0460E4B0C3188C5F741F
Local device SN
R40-NUMBER2
Target device SN
R40-NUMBER1
Remote operate
Upgrade firmware
None
Read config
Write config
Upgrade firmware
Upgrade file
Operate result
Successful
Local connect status
Connected
Target connect status
Connected(v1.32.1)
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-03-09

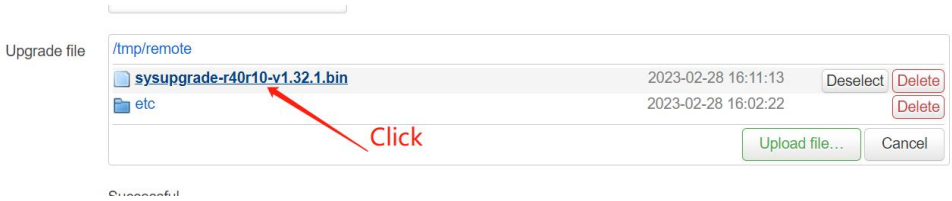
2-10


WPS云盘
此电脑
3D 对象
视频
图片
文档
下载
音乐
桌面
本地磁盘 (C:)
本地磁盘 (D:)
名称
修改日期
类型
sysupgrade-r40r10-v1.32.1.bin
2023/1/13 10:50
BIN 文件
1
2
文件名(N):
sysupgrade-r40r10-v1.32.1.bin
所有文件 (*.*)
打开(O)
取消
etc
2023-02-28 16:02:22
Delete
Browse...
Filename
Upload file
Cancel
Operate result
Successful
Local connect status
Connected
Target connect status
Connected(v1.32.1)
Save & Apply
Save
Reset

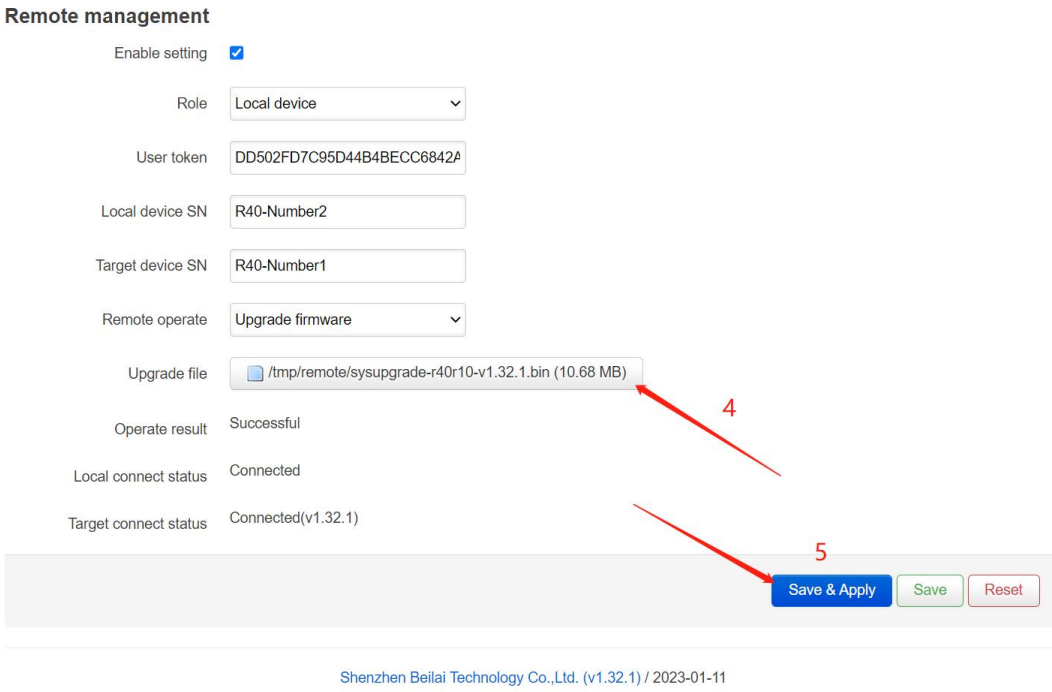
2-11


Enable setting
Role
Local device
User token
DD502FD7C95D44B4BECC6842A
Local device SN
R40-Number2
Target device SN
R40-Number1
Remote operate
Upgrade firmware
Upgrade file
/tmp/remote
etc
2023-02-28 16:02:22
Delete
3
Browse...
sysupgrade-r40r10-v1.32.1.bin
Upload file
Cancel

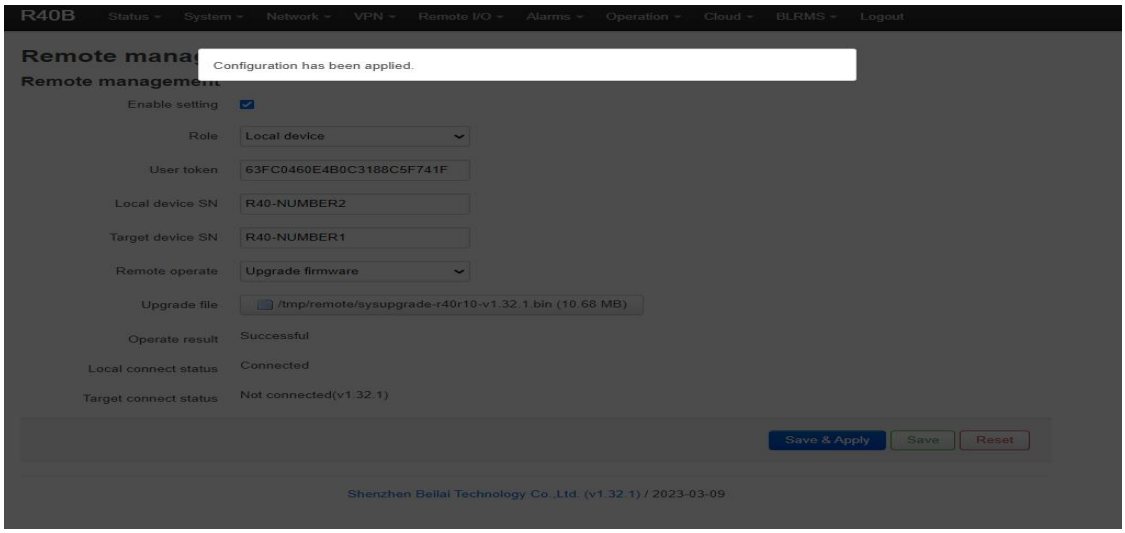
2-12


Upgrade file
/tmp/remote
sysupgrade-r40r10-v1.32.1.bin
2023-02-28 16:11:13
Deselect
Delete
etc
2023-02-28 16:02:22
Delete
Click
Upload file...
Cancel

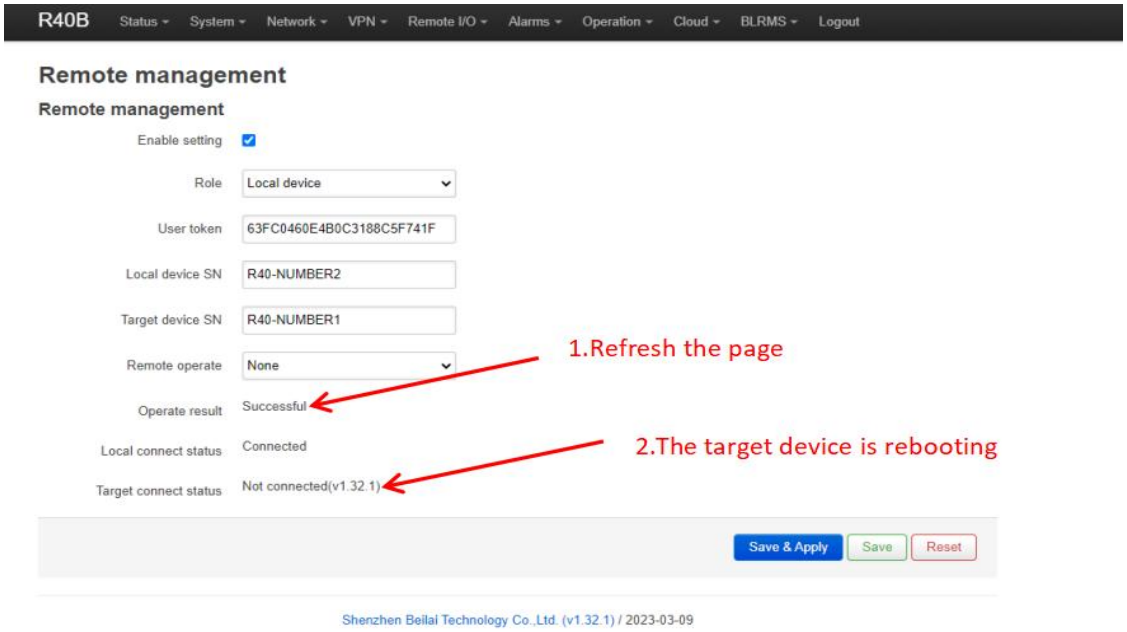
2-13


Remote management
Enable setting
Role
Local device
User token
DD502FD7C95D44B4BECC6842A
Local device SN
R40-Number2
Target device SN
R40-Number1
Remote operate
Upgrade firmware
Upgrade file
/tmp/remote/sysupgrade-r40r10-v1.32.1.bin (10.68 MB)
4
Operate result
Successful
Local connect status
Connected
Target connect status
Connected(v1.32.1)
5
Save & Apply
Save
Reset
Shenzhen Beilai Technology Co.,Ltd. (v1.32.1) / 2023-01-11

2-14

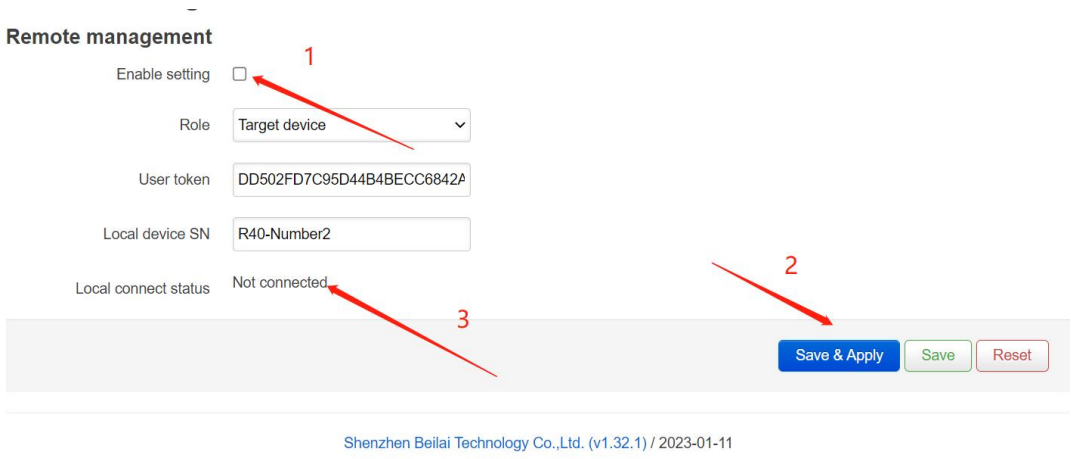


2-15



2-16

5.9.2.7 Disconnect BLRMS service



2-17

Summary of BLRMS service usage process:

1. Register an account on the "Barium Rhenium Remote Management System BLRMS" platform and obtain the token value.

2. Two R40 router devices, one selects the target device: enter the "User Token" and "Local Device SN" and then "Save and Apply" to connect to the platform. The other selects the local device: after entering the relevant configuration information, "Save and Apply", you can perform remote read, write and upgrade operations on the local device.

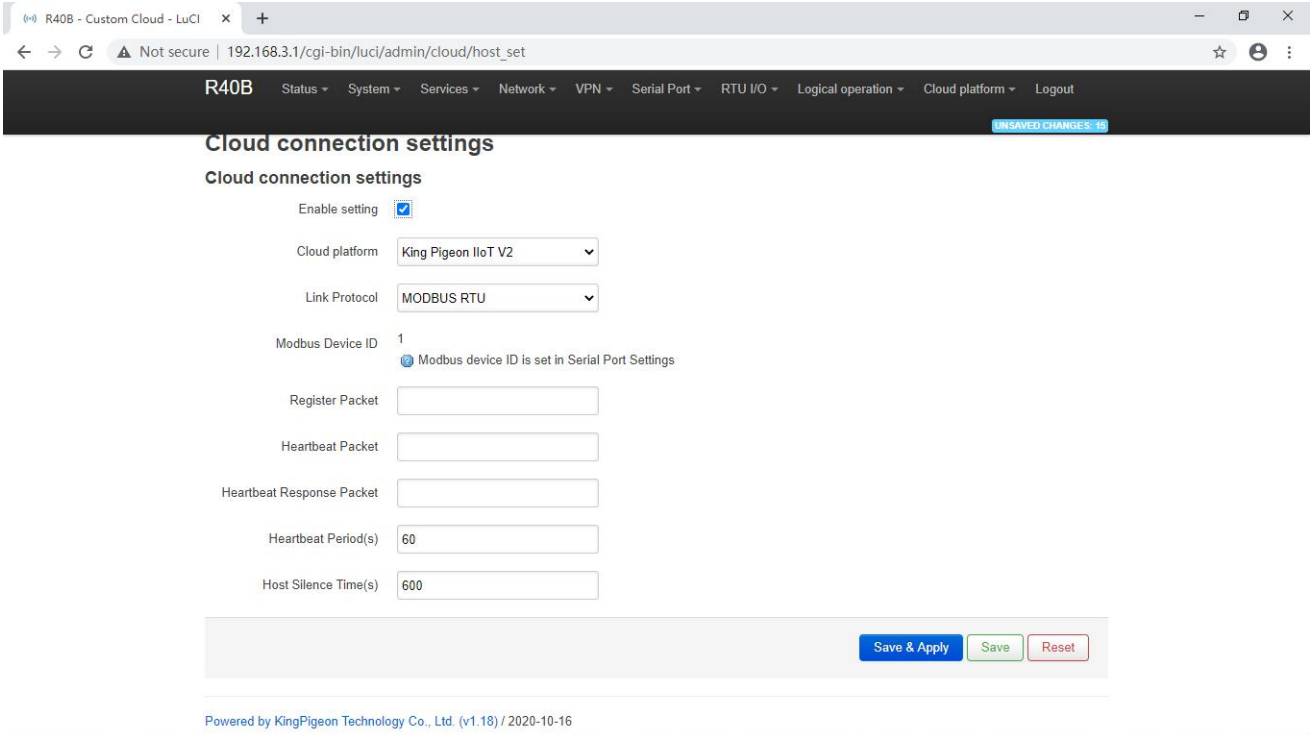
3. If you need to disconnect the BLRMS service on the R40 client, uncheck "Enable Settings" and then "Save and Apply".

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)
[Registrer Package]: The registration package sent by the device to the server when connected to the server.
[Heartbeat Packet]: A heartbeat packet sent by the device to the server to maintain the connection.
[Heartbeat Response Packet]: Server responds to the device's heartbeat packets.

[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 Device Register Address

6.1.2.1 DI / DO / AI DI Pulse Counter Register Address

1) Read input Coil(Function Code 02:Read coil)

Modbus Register Address(Decimal)	PLC or configuration address (Decimal)	Data Name	Data Type	Description

0	10001	DI1	Bool	Dry contact: 0: Open 1: Close Wet contact: 0: Low level (0~1VDC) 1: High level (5~30VDC)
1	10002	DI2	Bool	
2~21	10003~10022	Network disconnection detection device IP (max 20 IPs can be set)	Bool	0:offline 1:online

2) Read &Write Holding Coil (Function Code 01, Function Code 05, Function Code 15)

Modbus Register Address(Decimal)	PLC or configuration address (Decimal)	Data Name	Data Type	Description
0	00001	DO1	Bool	0: Open 1: Close
1	00002	DO2		

3) Read input Register (Function Code 04:Read input register.)

Modbus Register Address(Decimal)	PLC or configuration address (Decimal)	Data Name	Data Type	Description
0~1	30001~30002	AI1	(32 Bit Float) ABCD	Real value = register value
2~3	30003~30004	AI2		
4~5	30005~30006	AI3		
6~7	30007~30008	AI4		
8~9	30009~30010	DI1 pulse counter	32-bit unsigned integer ABCD	
10~11	30011~30012	DI2 pulse counter		

6.1.2.2 Read Device Digital Input Status

Master Send Data Format

Content	Byte	Data	Description
Device address	1	01H	01H Device, Range: 1-247, according to setting address
Function code	1	02H	02 read input coil DIN status

DIN Register address	2	00 00H	Range:0000H-0001H,stands for DI1-DI2
Read DIN register Qty	2	00 02H	Range:0001H-0002H, read qty of DIN status
16CRC verify	2	F9 CBH	CRC0 CRC1 low byte in front, high byte behind

Receiver Return Data Format

Content	Byte	Data	Description
Device address	1	01H	01H Device, according to setting address
Function code	1	02H	Read input holding coil
Return bytes Qty	1	01H	Return data length
Returning data	1	01H	Return DI data
16CRC Verify	2	6048H	CRC0 CRC1 low byte in front, high byte behind

Example: Inquiry device 2 DIN data at same time, then:

Server send: 01 02 00 00 00 02 F9 CB

01= Device address; 02= Inquiry DIN status; 00 00= DIN Starting address; 00 08= Serial reading 2 DIN status;

F9 CB = CRC verify.

Device return: 01 02 01 01 60 48

01= Device address; 02= Inquiry DIN status; 01= Returning data bytes qty; 01= DIN status, each byte stands for one DIN status, 01H converter to binary 0000 0001 from low to high byte, stands for DIN1-DIN2 status,

0= Open, 1= Close.

DI2	DI1
0	1
Open	Close

60 48: 16 byte CRC verify.

If need to inquiry multi DIN status, only need to change "DIN Starting Address", "Reading DIN Register Qty", calculate CRC verify again.

6.1.2.3 Read Device Digital Output DO Status

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	01H	Read the hold coil, function code 01
Register Starting Address	2	00 00H	Range: 0000H-0001H, stands for DO1-DO2
Read Register Qty	2	00 02H	Range: 0000H-0001H
16 CRC Verify	2	BD CBH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H device, consistent with download data
Function Code	1	01H	Read the hold coil
Return Bytes Qty	1	01H	Return data length
Returning Data	1	02H	Data returned
16 CRC Verify	2	D0 49H	CRC0 CRC1 low byte in front, high behind

Example: Read 2 DO states, device address 1,then,

Server Send: 01 01 00 00 00 02 BD CB

01= Device address; 01= Read Relay DO function code;00 00= Register starting address; 00 02= Continuous reading of 2 DO data; BD CB= CRC verify.

Device Answer: 01 01 01 02 DO 49

01= Device address; 01= Read relay function code; 01=Return data bytes Qty; 02=The returned data is converted into binary: 0000 0010 from low to high byte,status value:

DO2	DO1
1	0
Close	Open

D0O49: 16 byte CRC verify

If you want to read the state of a DO or several DO states, you only need to modify the "DO register start address" and "the number of read registers", then recalculate the CRC, and the returned data is parsed according to the above description.

6.1.2.4 Control Device Digital Output Status

1) Control 1 channel device DO output

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 type, function code 05
DO Register Address	2	00 00H	Range: 0000H-0001H
Active	2	FF 00H	This value: FF 00H or 00 00H, FF 00H= Close relay, 00 00H= Open relay
16CRC Verify	2	8C 3AH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Byte	Data	Description

	s	(H: HEX)	
Device Address	1	01H	01H Device, Range 1-2, according to the data Master send
Function Code	1	05H	Write single holding coil type
DO Register Address	2	00 00H	Range: 0000H-0003H
Active	2	FF 00H	This value: FF 00H or 00 00H, FF 00H= Already actived close relay, 00 00H= Already actived open relay
16CRC Verify	2	8C 3AH	CRC0 CRC1 low byte in front, high behind

Example: Control relay DO1 close, then:

Server send: 01 05 00 00 FF 00 8C 3A

01=Device address;05= Control single relay command;00 00=Relay DO0 address;FF 00=DO0 close;8C 3A=CRC verify.

Device answer: 01 05 00 00 FF 00 8C 3A

01=Device address;05=Control single relay command;00 00=Relay DO0 address;FF 00= Active DO0 close;

8C 3A=CRC verify.

If single control other relay outputs, only need to change "DO Register Address" and "Active", calculate CRC verify again.

2) Multiple Control DO outputs

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	0FH	Write multi holding coil,function code 15
DO Starting Register Address	2	00 00H	Range: 0000H-0001H, stands for DO0-DO1
Control Relay Qty	2	00 02H	Range: 0000H-0002H
Write Byte Qty	1	01H	Write 1 byte, since device only 2DO, use 4 binary can do it
Writing Data	1	03H	Send status data to control DO
16CRC Verify	2	9E 96H	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	0FH	Write multi holding coil type
DO Register	1	00 00H	Range: 0000-0001,stands for DO1-DO2

Address			
Active	1	00 02H	Range:0001H-0002H, stands for already actived relays
16CRC Verify	2	D4 0AH	CRC0 CRC1 low byte in front, high behind

Example: Close device 2 DO at same time, then:

Server send: 01 0F 00 00 00 02 01 03 9E 96

01= Device address; 0F= Control multi relay; 00 00= Relay DO0 starting address; 00 02= Control 2 relays;

01= Send data qty; 03= Data sent converter to binary 0000 0011 from low to high stands for DO1-DO2 status, 0stands for open relay,1 stands for close relay:

DO2	DO1
1	1
Close	Close

9E 96 CRC verify.

Device answer: 01 0F 00 00 00 02 D4 0A

01= Device address; 0F= Control multi relay; 00 00= Relay DO0 starting address; 00 02= Actived 2 relays;

D4 0A CRC verify.

6.1.2.5 Read Device AIN Status and DIN Pulse Counter

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	04H	Read input register, function code 04
Register Starting Address	2	00 00H	Every 2 16-bit address corresponds to 1 AI 32-bit register
Read Register Qty	2	00 0CH	A total of 12 16-bit addresses are read, each of the two 16-bit addresses is combined into a 32-bit address, a total of 6 32-bit addresses, that is, the number of read AI 4 and the DI pulse count 2
16 CRC Verify	2	F00FH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H device, consistent with download data
Function Code	1	04H	Read the hold coil

Return Bytes Qty	1	18H	Return data length
Returning Data	16	3B 98 4E 40 40 80 00 00 3C 89 15 BE 3B D7 51 8B 00 00 00 03 00 00 00 06H	Return AI data,32-bit float,ABCD
16 CRC Verify	2	22 80H	CRC0 CRC1 low byte in front, high behind

Example: Inquiry device 4 AIN and 2 DIN pulse data at same time, then:

Server send: 01 04 00 00 00 0C F0 0F

01= Device address; 04= read input register; 00 00= Starting address ; 00 0C= Serial reading 12 input register value:,F0 0F= CRC verify.

Device return: 01 04 18 3B 98 4E 40 40 80 00 00 3C 89 15 BE 3B D7 51 8B 00 00 00 03 00 00 00 06 22 80

01= Device address; 04= read input register; 18= Return data byte ; 3B 98 4E 40 40 80 00 00 3C 89 15 BE 3B D7 51 8B 00 00 00 03 00 00 00 06=return data, detail as follows:

Analog input	AI4	AI3	AI2	AI1	DI1 pulse	DI2 pulse
Receiving Data（32-bit floating）	3B D7 51 8B	3C 89 15 BE	40 80 00 00	3B 98 4E 40	3B 98 4E 40	3B 98 4E 40
Real value	0.006571	0.016734	4	0.004648	3	6

22 80: CRC verify.

6.1.3 Read Mapping Address

6.1.3.1 Mapping Register Address

1) Boolean Slave Mapping Register Address, holding 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 Register Assignment Table

Read and Write Holding Register (Function Code 03,04, 06, 16)				
Modbus	**PLC or**	**Data**	**Data Type**	**Description**

Register Address(Decimal)	configuration address (Decimal)	name		
20001	420002 or 320002	16 Bit data 20001	Sort AB, its data type according to slave mapping data type	According to configurator set mapping rules, this address will sort slave mapping data to AB, stock in this address, for cloud easy reading together, can mapping slave inputting and holding register.
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 Register Assignment Table

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	Sort ABCD, its data type according to slave mapping data type	According to configurator set mapping rules, this address will sort slave mapping data to ABCD, stock in this address, for cloud easy reading together, can mapping slave inputting and holding register.
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

6.1.3.2 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 ["Slave Mapping Register Address”]
Read Register Qty	2	00 0AH	Range：0001H-00C1H
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, Range: 1-247, according to setting address
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.

6.1.3.3 Modify Boolean Mapping Address Data

If control slave's relay status which connected to RS485, need to add slave in salve list of configurator. Write
command 15 for mapping, when mapping address value modified, will write to RS485 matched slave address.

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, pls check function 15 of Modbus protocol.

6.1.3.4 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 21H	One address can read 2 bytes. Mapping data type address range, refer to **["Slave Mapping Register Address"]** at manual bottom.
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	One address can read 2 bytes
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.

6.1.3.5 Modify Data Type Mapping Address Data

If need to revise slave data which RS485 connected, need to add slave in salve list of configurator. Write command 03 for mapping, when mapping address value modified, will write to RS485 matched slave address.

If address 20001 mapping slave data type is Signed Int, sort AB.

Master Send Data Format:

Content	Byte	Data	Description

	s	(H: HEX)	
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

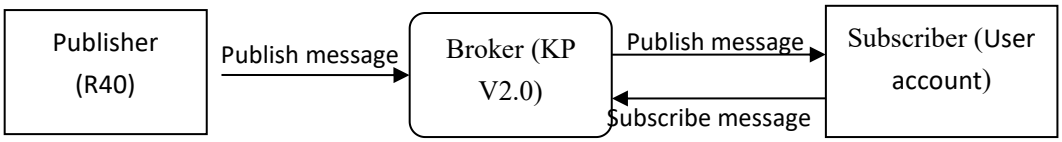
cases, including restricted environments such as machine to machine (M2M) communication and the Internet of Things (IoT). It is widely used in satellite link communication sensors, occasionally dialed medical devices, smart homes, and some miniaturized devices. The MQTT protocol runs on TCP/IP or other network protocols, providing ordered, lossless, two-way connectivity.

6.2.2 MQTT Principle

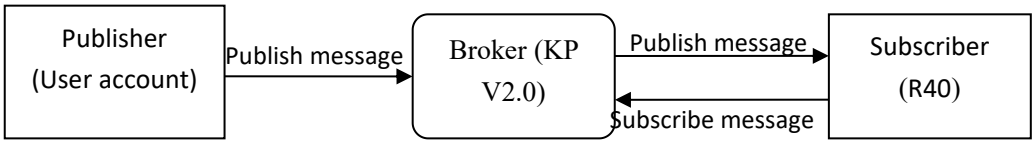
There are three identities in the MQTT protocol: Publisher (Publish), Broker (Server), Subscriber (Subscribe). Among them, the publisher and subscriber of the message are both clients, the message broker is the server, and the message publisher can be the subscriber at the same time.

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 R40 receives the downlink message from the Broker to implement control of the R40)

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 protocal.
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 Golden Pigeon Cloud 2.0 cycle needs to be set to 10 seconds or more. If it is more 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 retransmission: Check enable, after enabling, when reconnecting to the cloud platform, the data during the offline period will be retransmitted.
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 “pack the data” is checked, multiple I/O data points will be sent in one message. In case there are too many data points, they will be sent separately by multiple messages. each message contains multiple data points. If "Data Packing" is not checked, a message contains only one I/O data point. Please kindly take noted about such differences between the two publishing formats.

(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"

//Retransmission flag: the character is "retransmit", 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 "retransmit" 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"

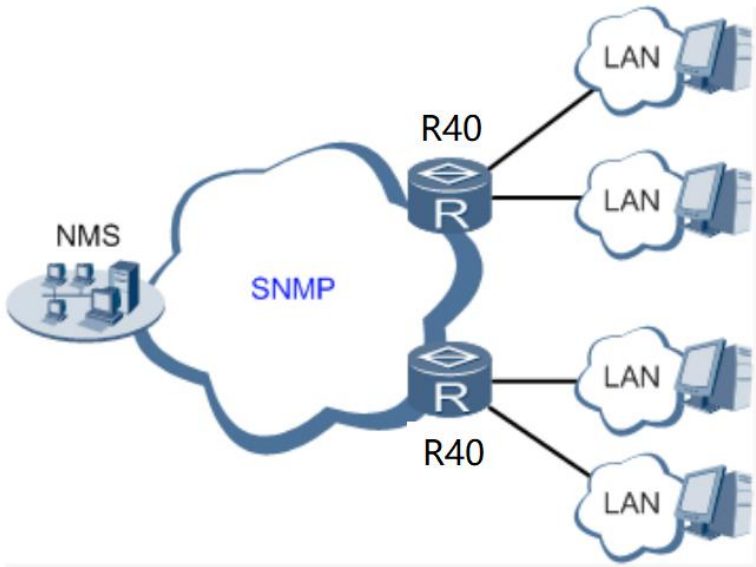
// "down" confirmation data sent to subscribers by the platform.

6.3 SNMP Protocol

6.3.1 Introduction of R40 support SNMP

In order to configure and manage devices across an entire network, administrators need to access devices that are widely dispersed. However, it is not practical for administrators to configure devices on-site. Furthermore, if these network devices are sourced from different manufacturers and each manufacturer provides an independent management interface (such as using different command lines), it will result in a huge amount of work to batch configure network devices. In this case, if traditional manual methods are used, it will result in high costs and low efficiency. Therefore, network administrators can take advantage of the edge computing router R40.

Different network devices can be connected to R40, which supports the SNMP protocol. The network management system can obtain R40 status information through the SNMP protocol to achieve real-time monitoring of managed devices. The diagram below shows how network management can manage devices through SNMP protocol.



SNMP Management with R40

The network management system (NMS) can obtain real-time status information of devices through R40 at any time and remotely control managed devices. Currently, R40 supports SNMPv1 and SNMPv2c versions, which adopt community name authentication.

SNMP Mibs (SNMP Management Information Bases) are the main modules in SNMP protocol software. R40 uses the ENTITY-SENSOR-MIB information base to operate R40 local IO (including DI/DO/AI) , It can also operate mapping registers established using the "Modbus master station" function, so as to achieve the function of Modbus and SNMP protocol conversion.

6.3.2 SNMP Application Operation Example

Let's take this as an example

The MG-SOFT MIB Browser tool connects to the R40 through SNMP, and the R40 connects to a network slave.

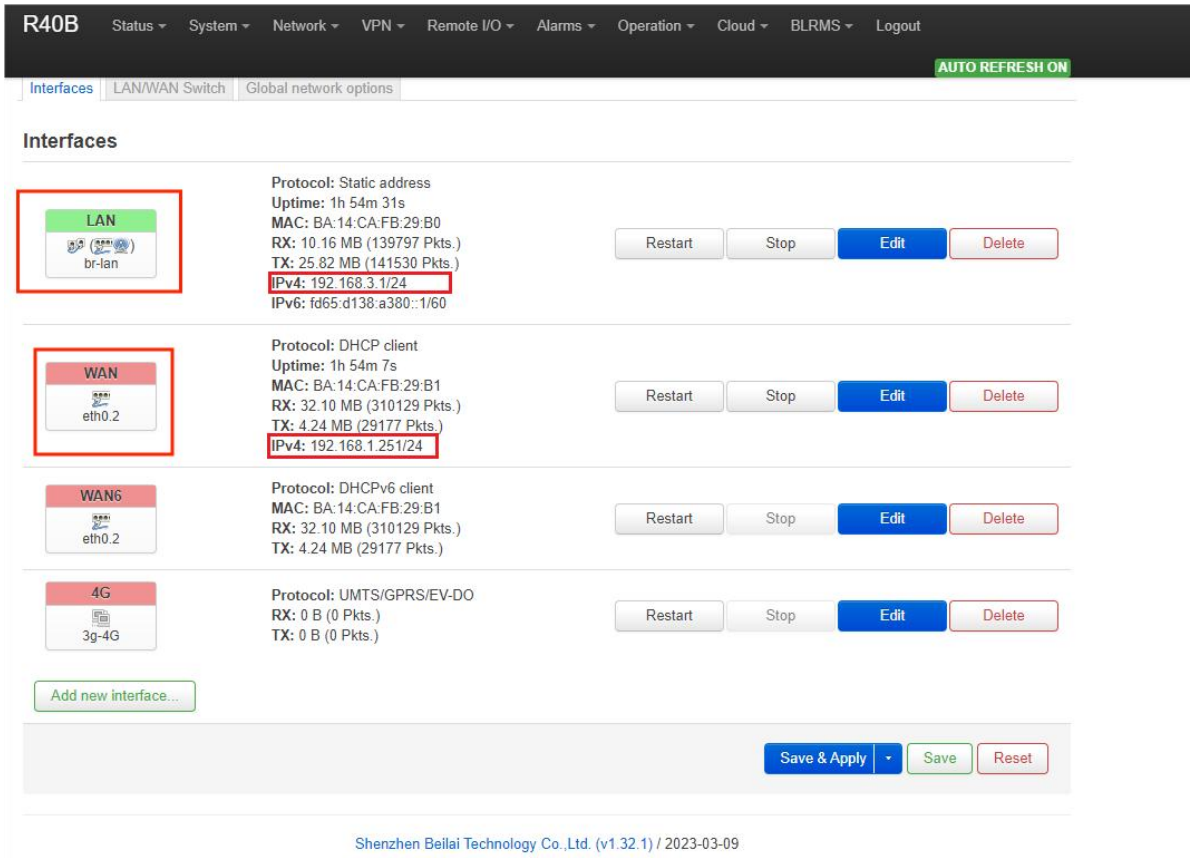
Open MG-SOFT MIB Browser and enter the IP address of R40. It depends on the server where the MG-SOFT MIB Browser is located, see comments below.

If the server is connected through R40's LAN port, enter 192.168.3.1 (the LAN default).

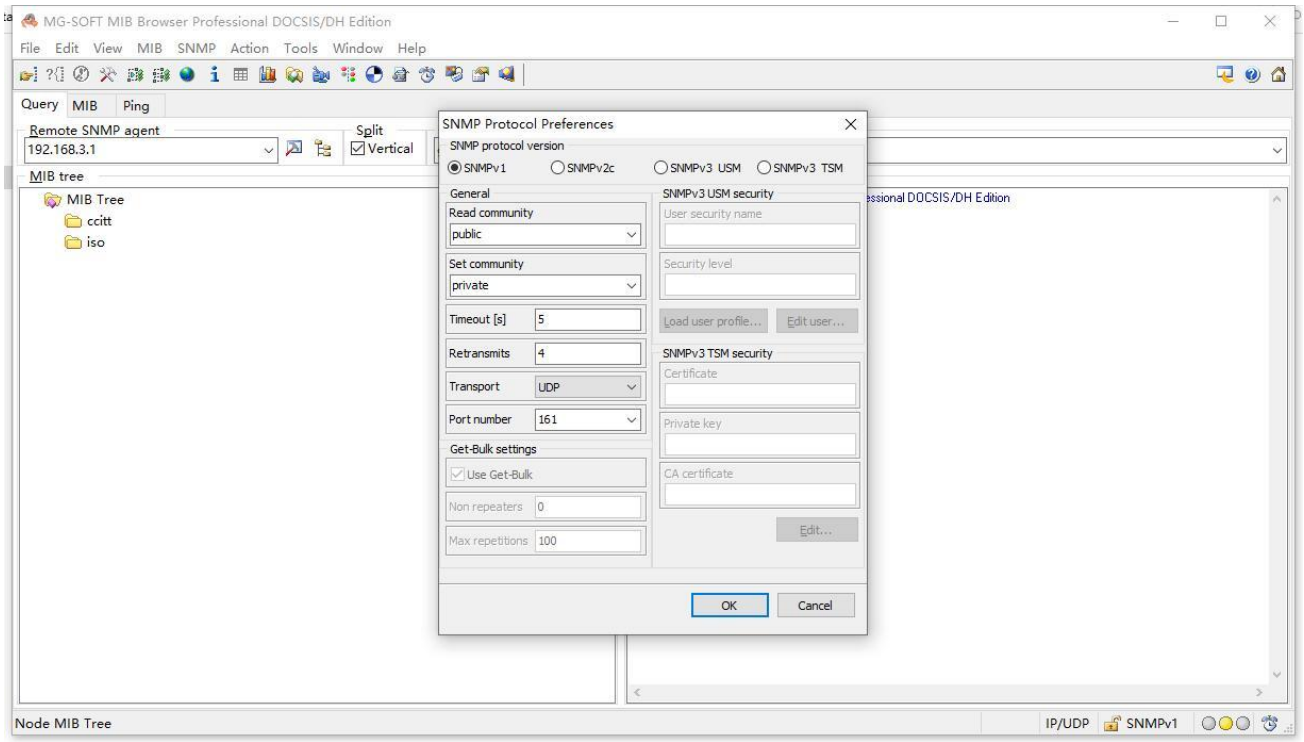
If the server is on the same LAN as the R40 WAN port, enter the IP address of the R40 WAN.

The UDP port is 161

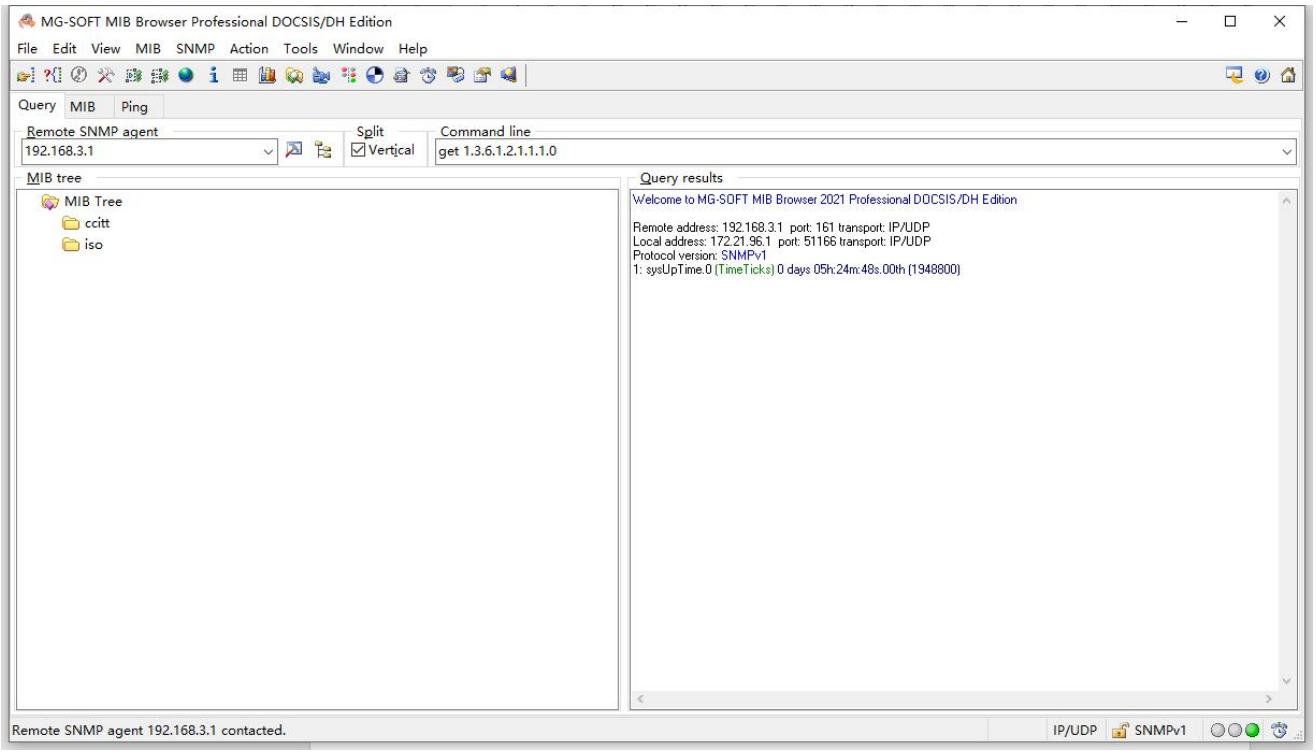
The connection IP address is selected



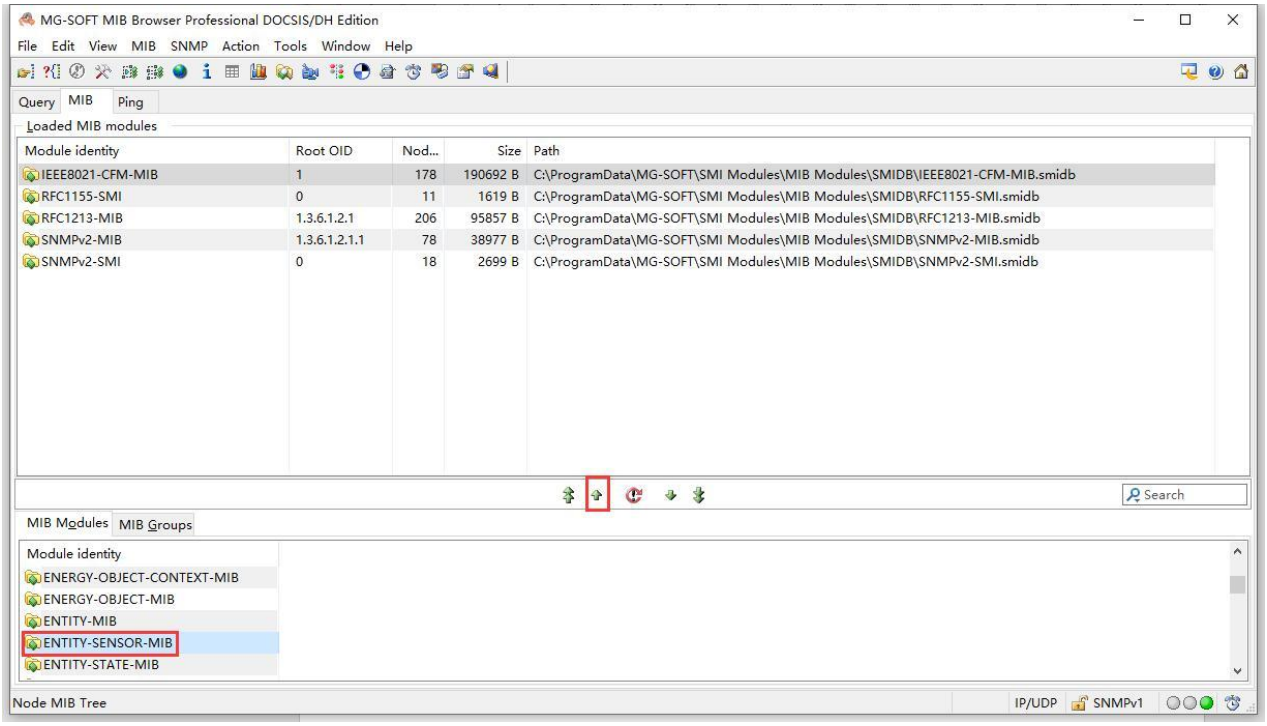
MG-SOFT MIB Browser configuration, select SNMPV1.

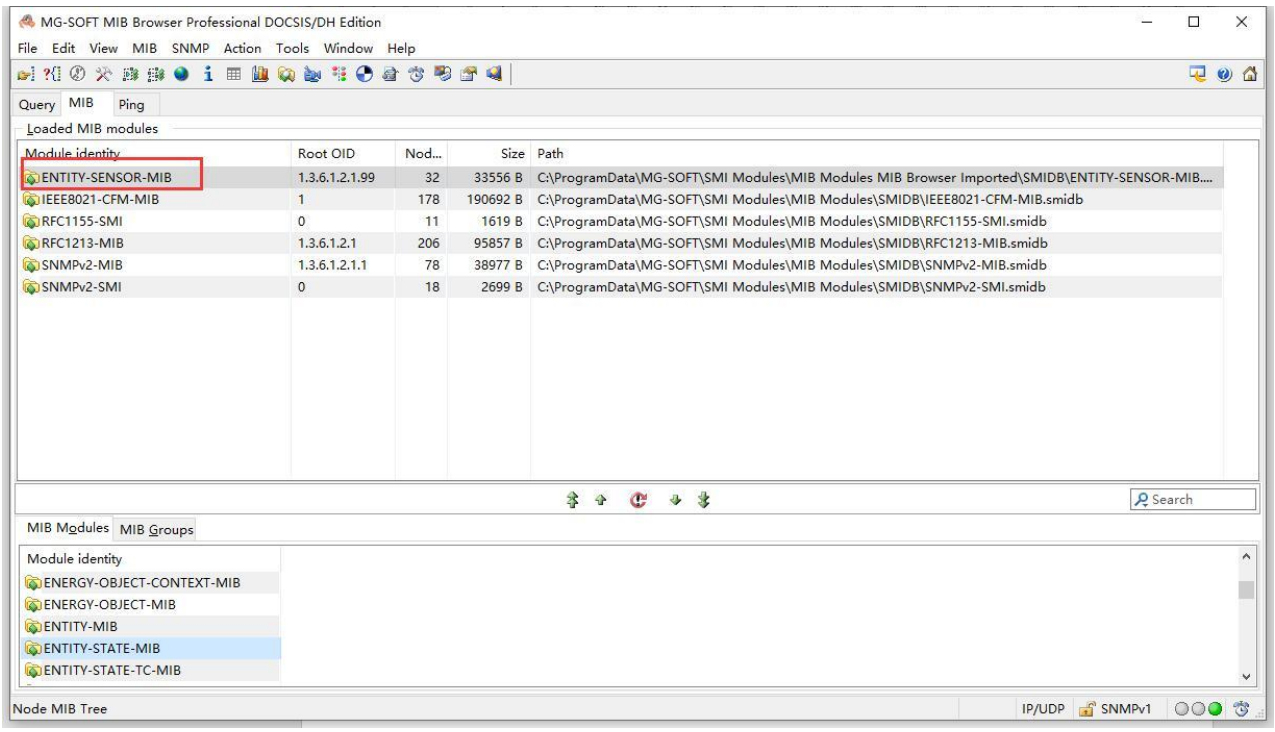


Click "OK" and then connect successfully.

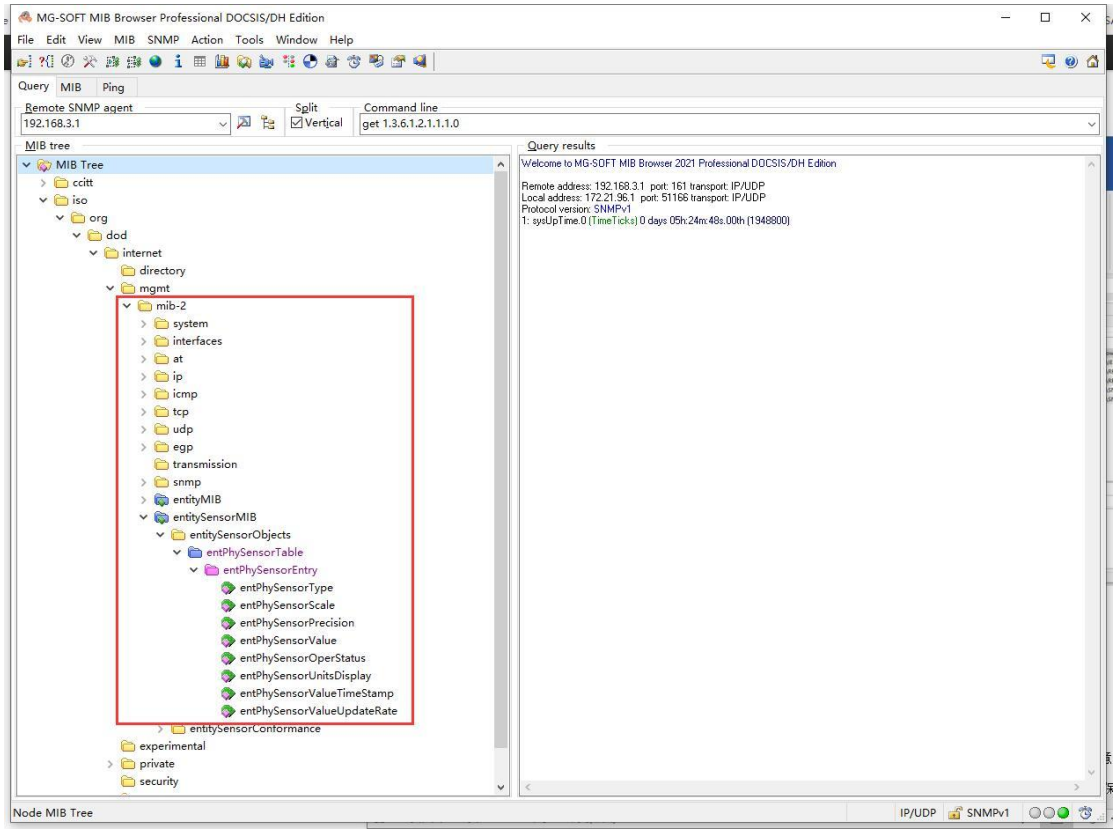


Add MIB infobase, select ENTITY-SENSOR-MIB from MIB Modules, and load the infobase.



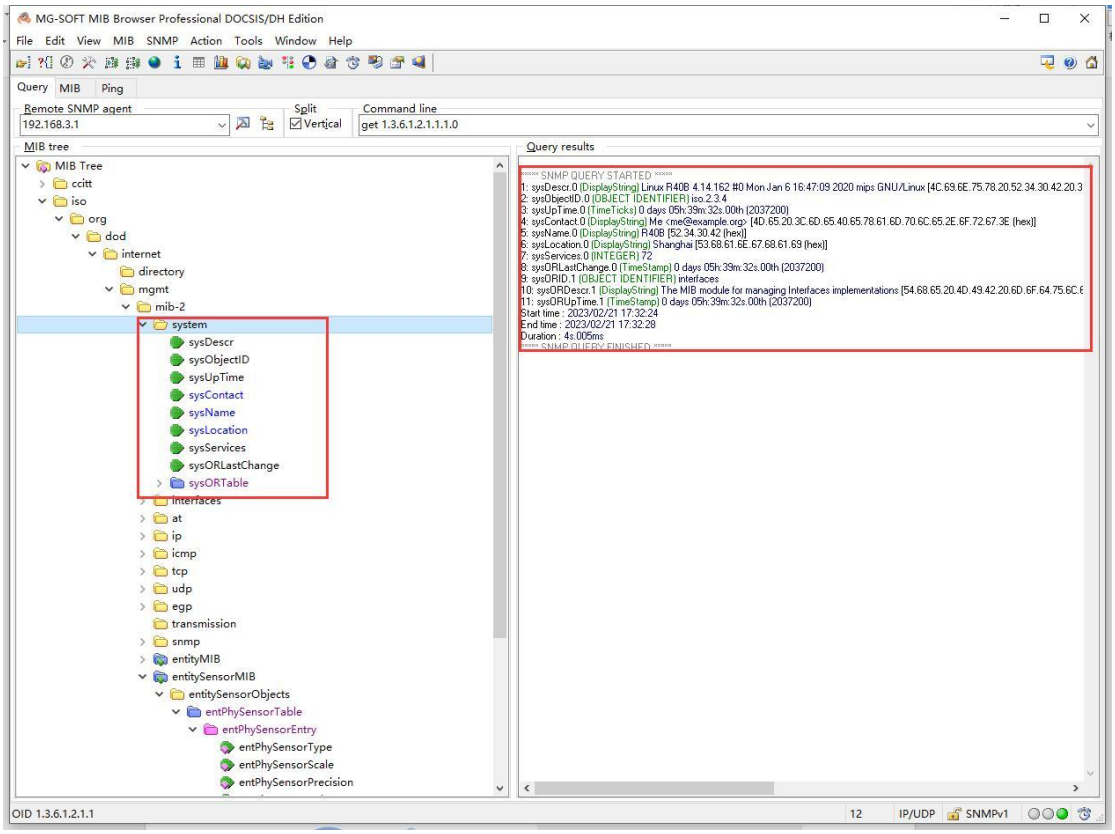


Information base node

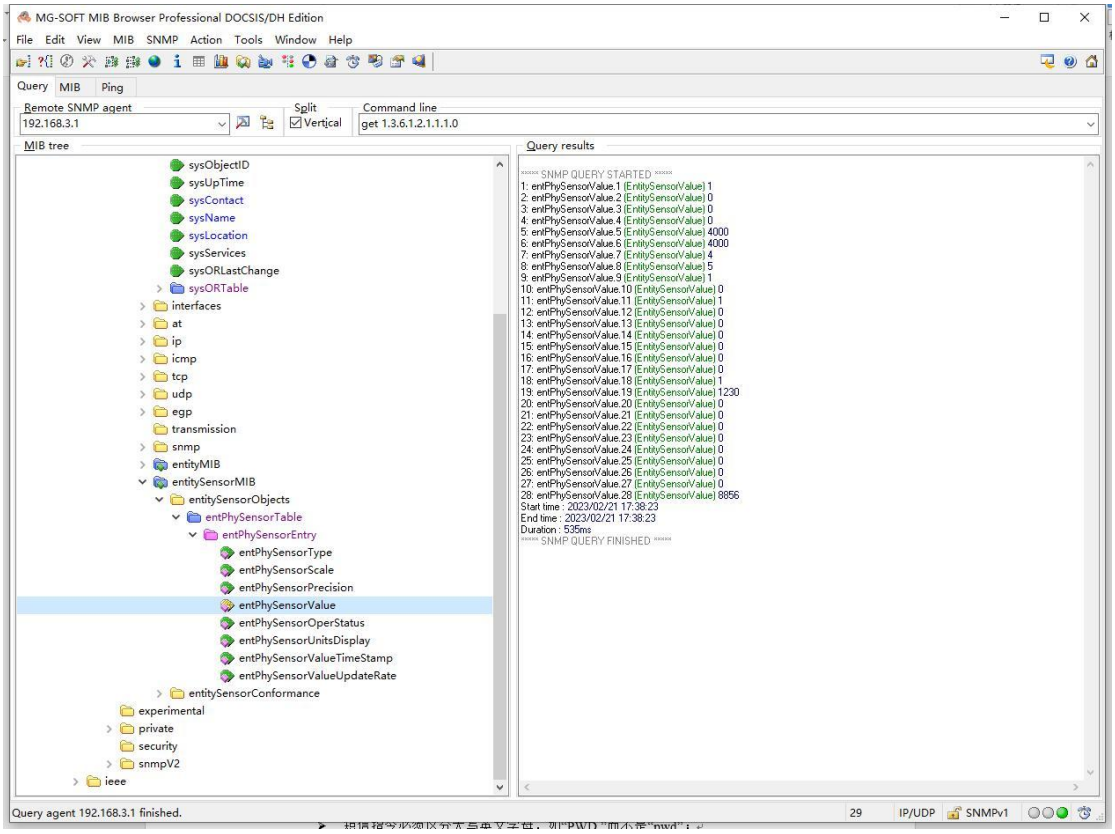


Walk R40 system information,

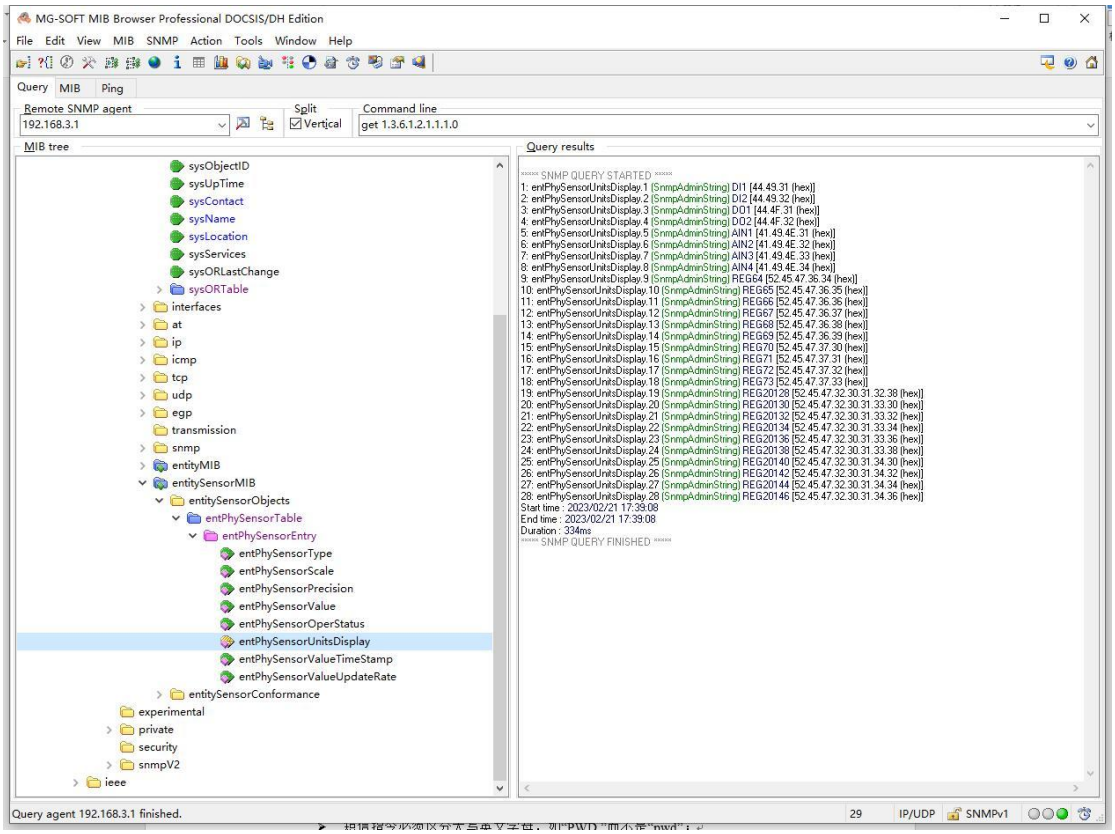
click "System", right-click the mouse and choose "walk" to read all information.



To monitor the data points of the network devices controlled by the R40, click entPhySensorValue and choose Walk, Get or Get Next from the right mouse button to monitor the data of the R40.



The entPhySensorUnitsDisplay node displays the ID of the R40 data point.



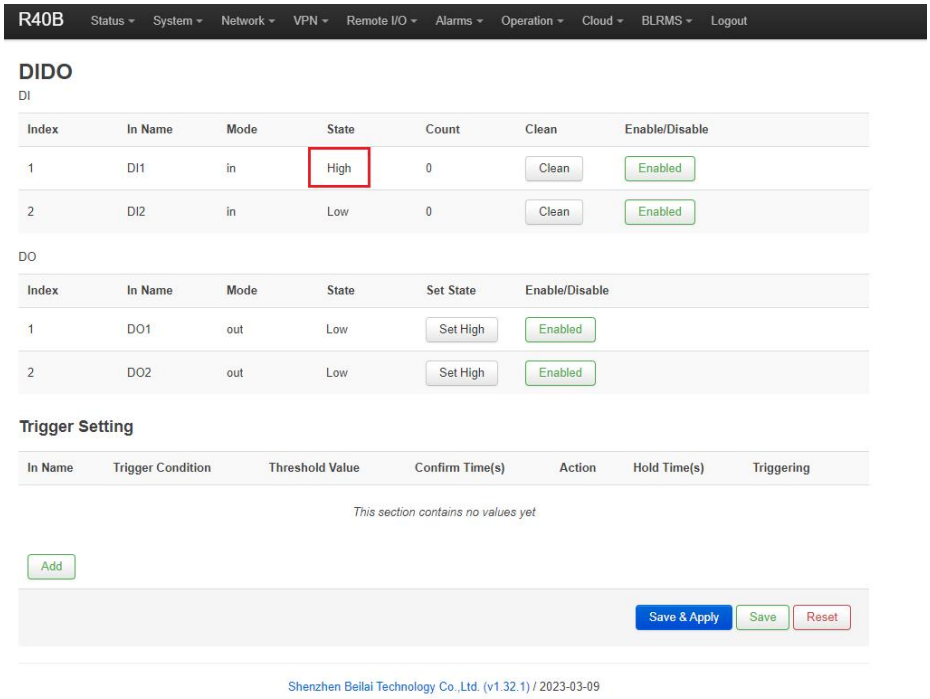
The value of the data point obtained on the network management system is compared with the value of the data point monitored on the R40 web page.

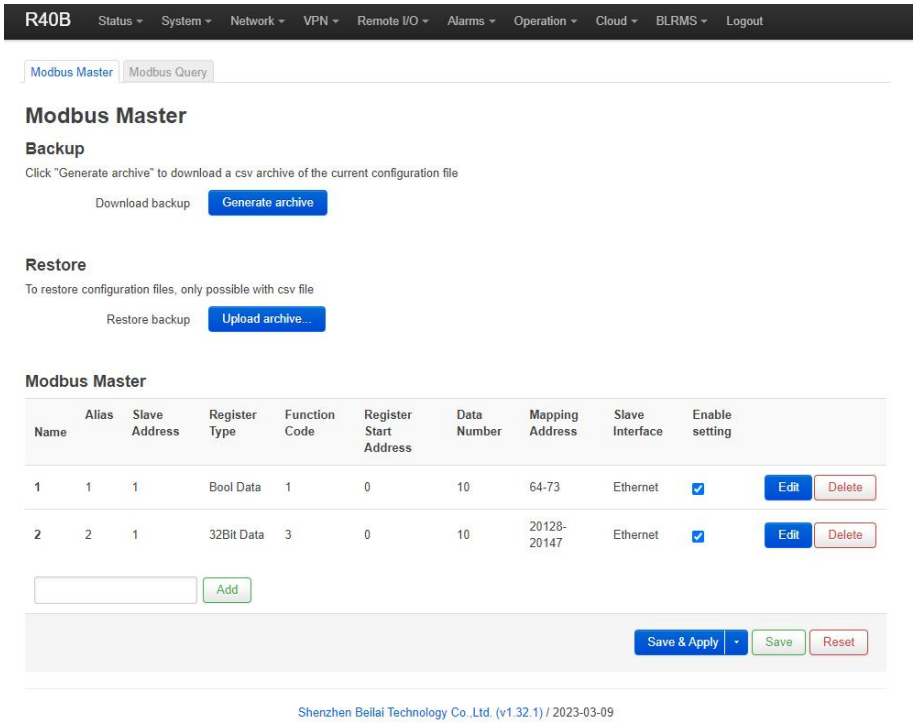
On the entPhySensorUnitsDisplay node, 1 is DI1 and 19 is REG20128.

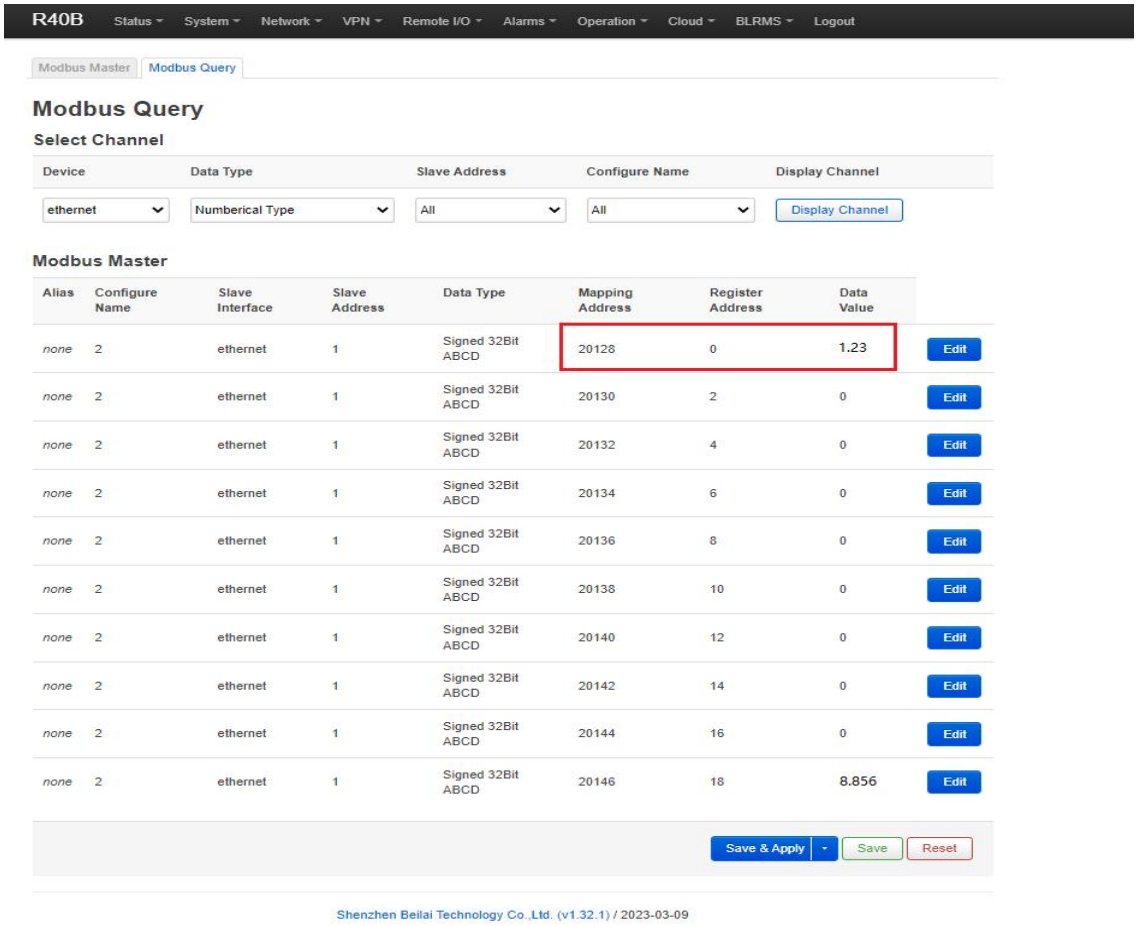
You can view the corresponding value on the entPhySensorValue node. If 1 is 1, DI1 is in the closed state, and if 19 is 1230, REG20128 is 1.23. The value of numeric data on SNMP is increased by 1000, and the Boolean value remains the original value.

In the entPhySensorScale node, you can view how many times each data point has grown or shrunk.

On the R40 page, "DI1" and "REG2018" are monitored as follows:

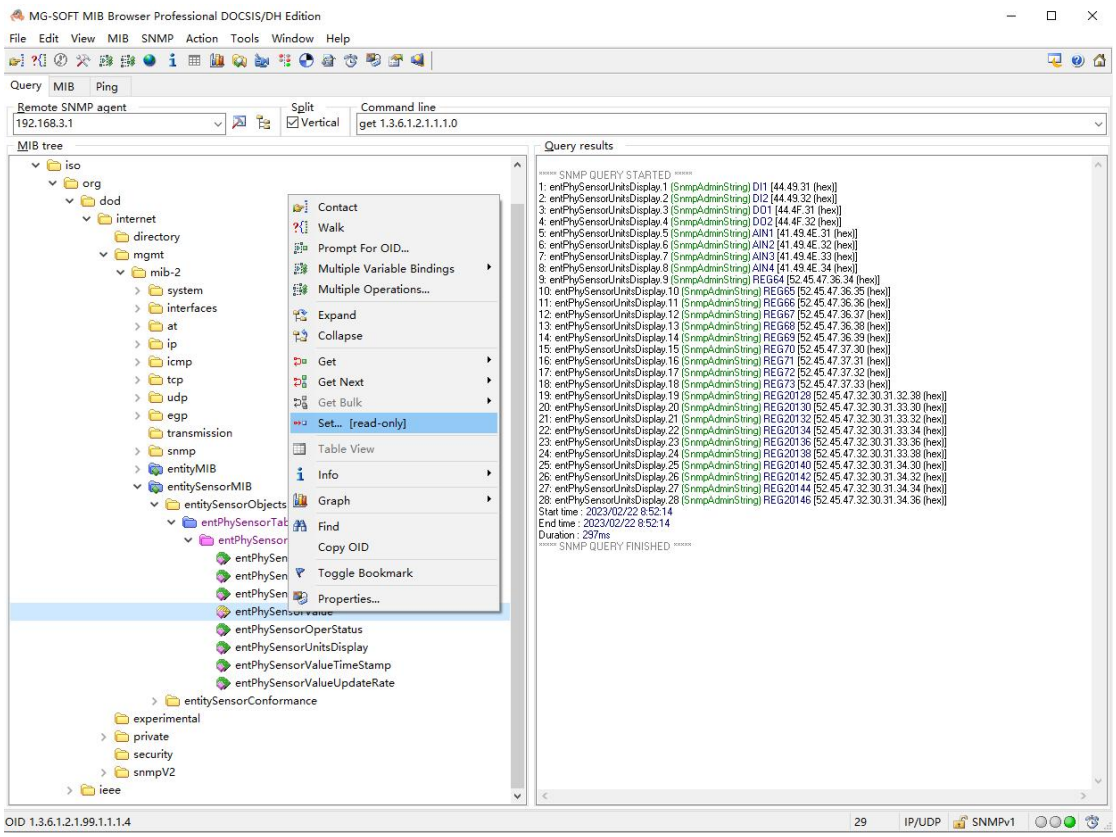




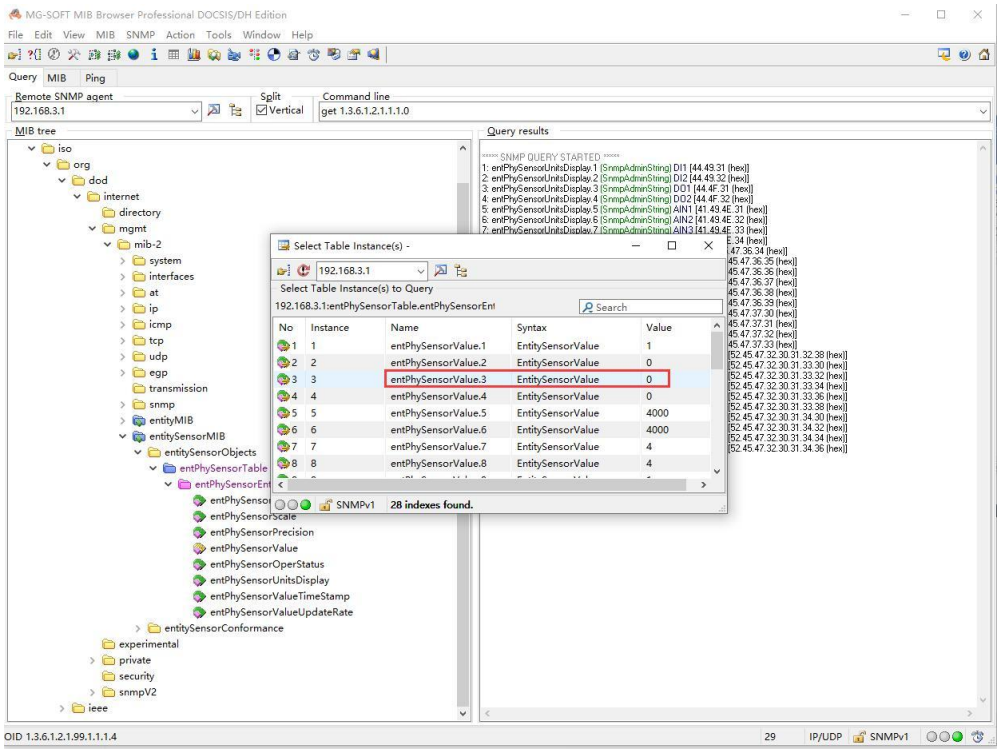


Use the network management system to control R40. For example, write "3" (DO1) to "1" (on R40) and "20" (REG20130) to "2356" (2.356 on R40).

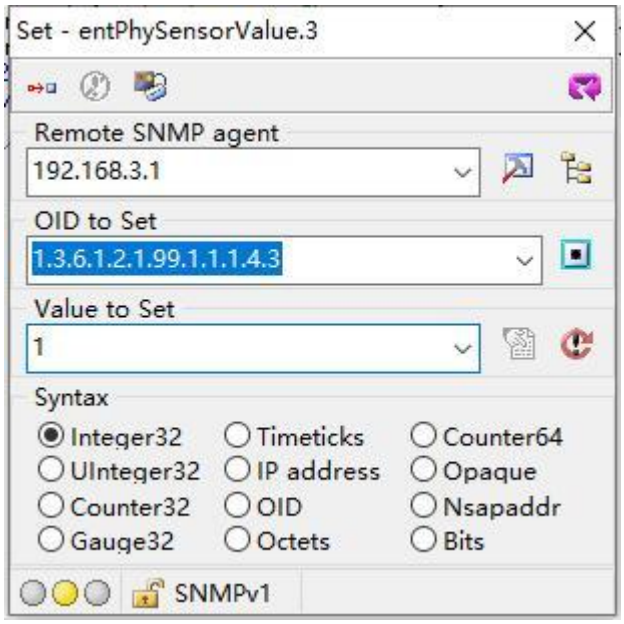
On MG-SOFT MIB Browser, click the "entPhySensorValue" node, right-click, and select "set... [read-only]".



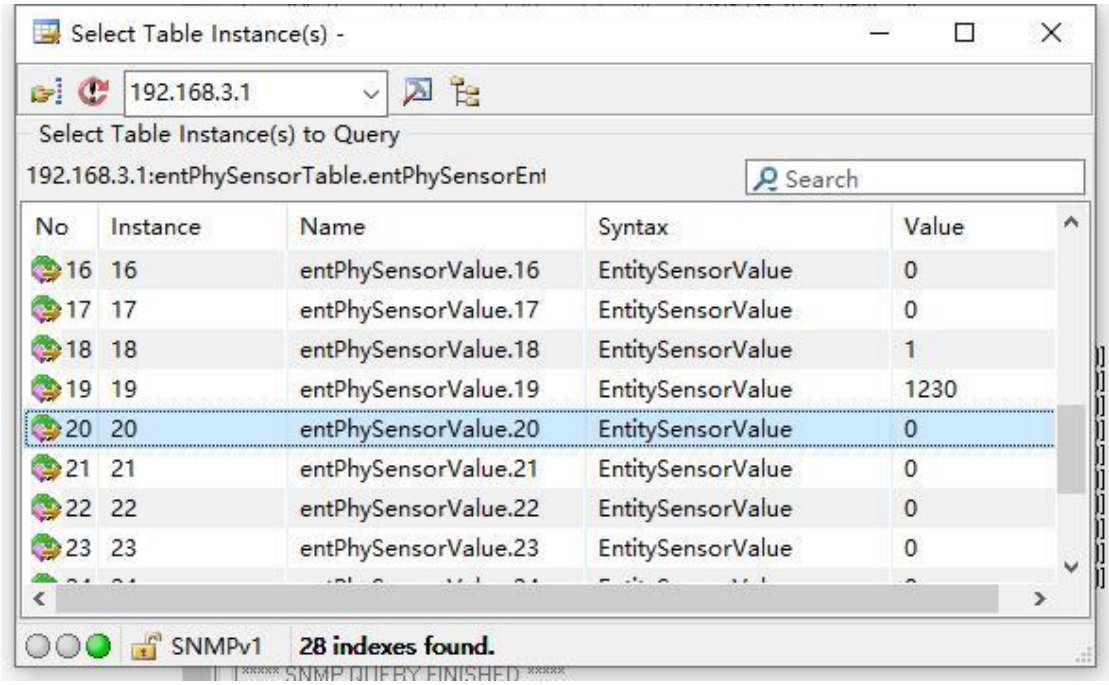
Click entPhySensorValue.3 (DO1) in the displayed box. You can also view that the current value of entPhySensorValue.3 is 0.



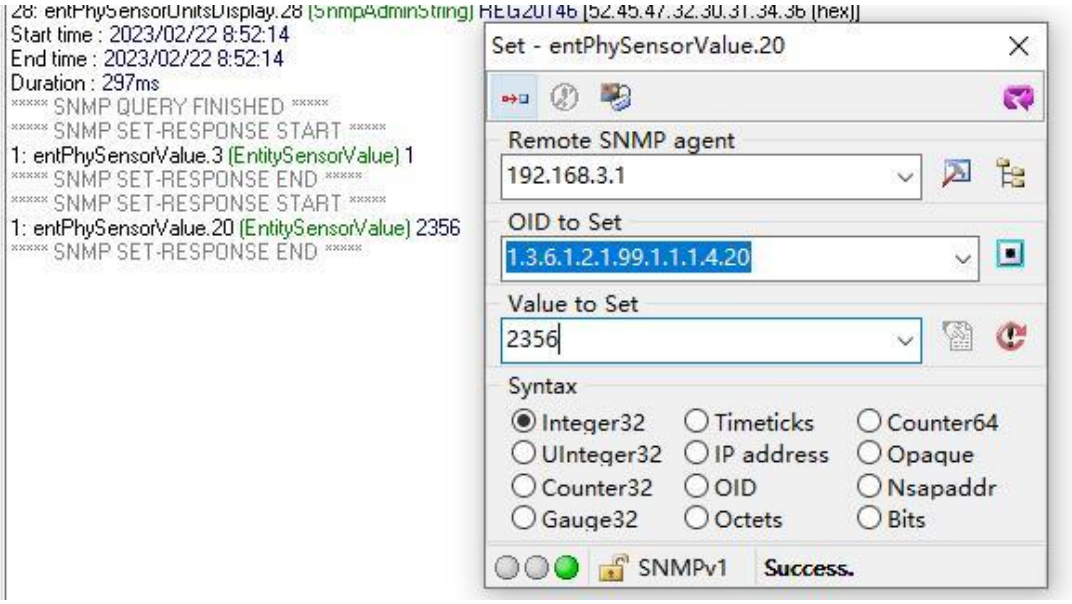
Enter "1" in "Value to Set" and click the icon.



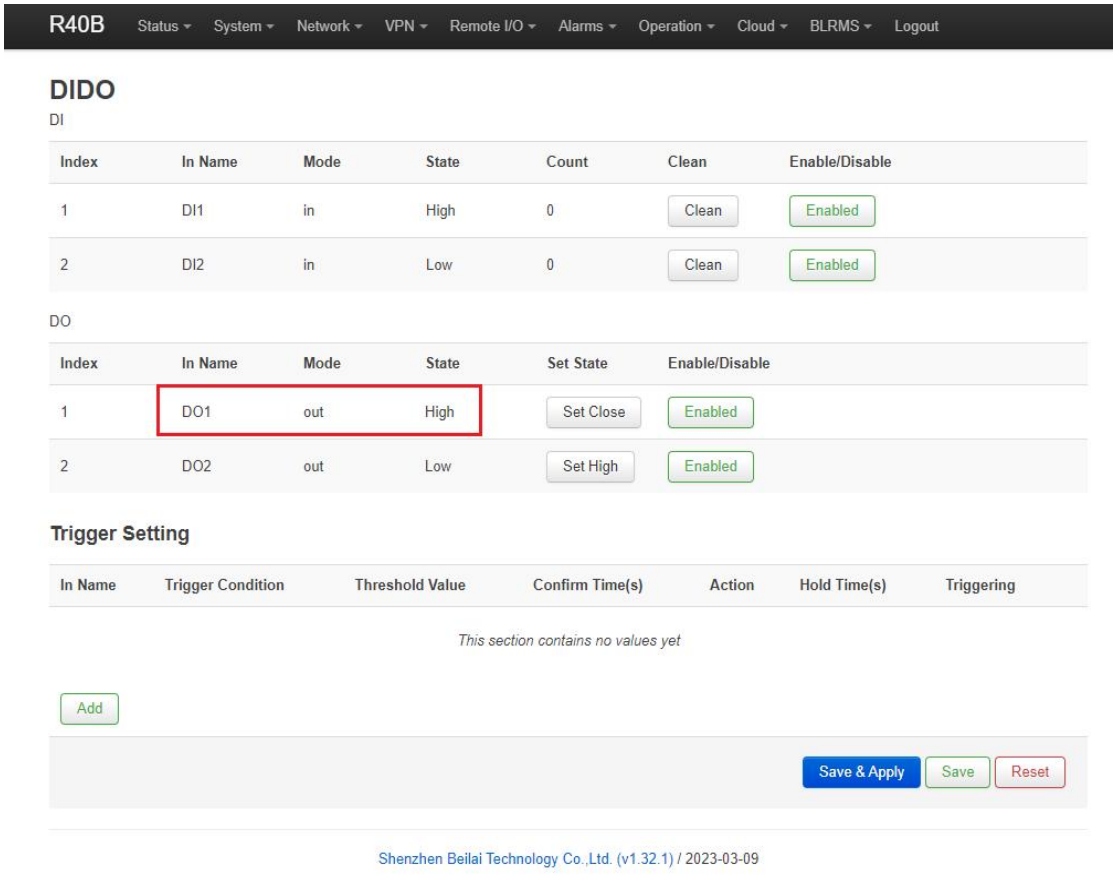
Click "entPhySensorValue.20" (REG20130) in the box in the same way as controlling DO1. You can also monitor that the current value of "entPhySensorValue.20" is "0" in the box.



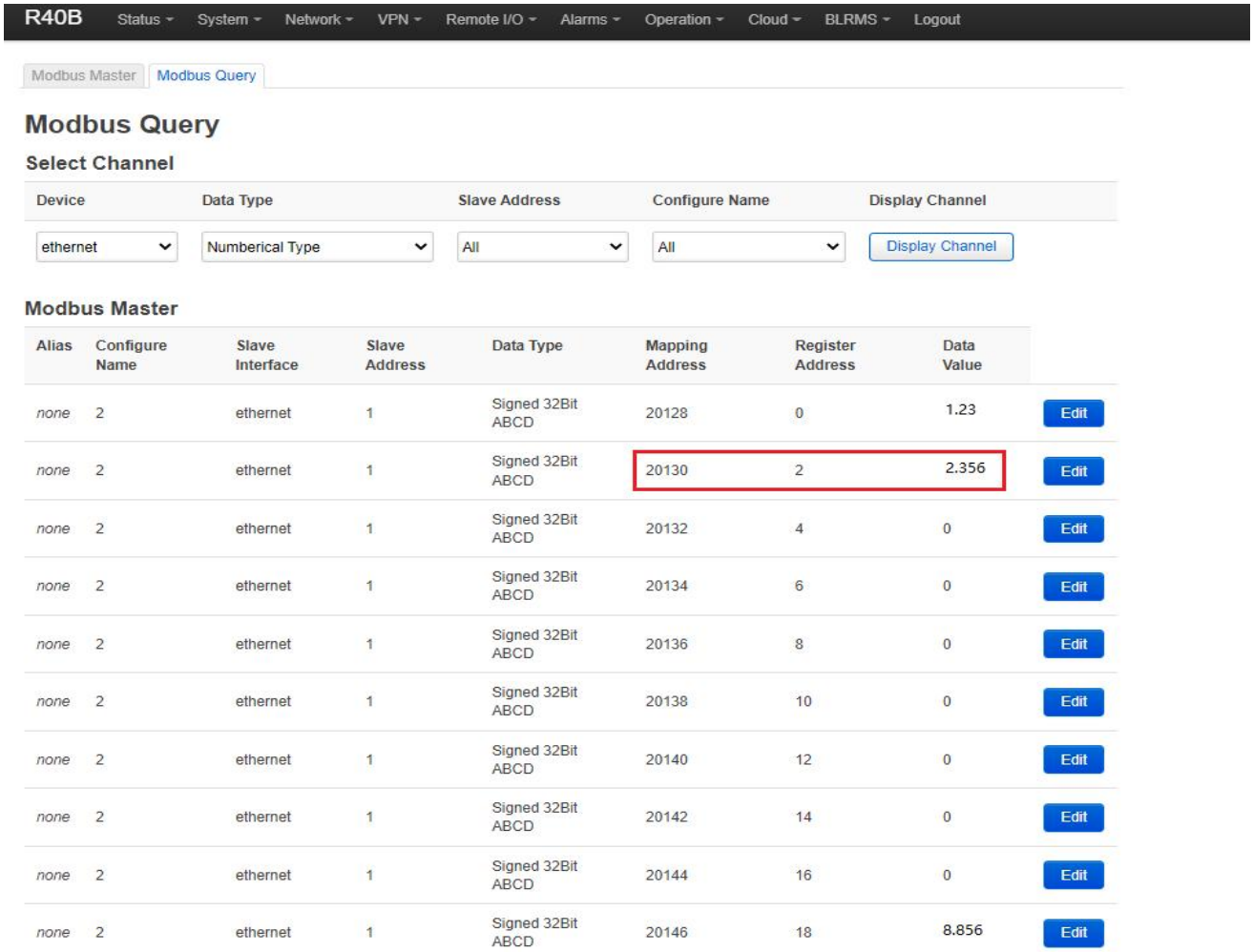
Enter 2356 in "Value to Set" and click the icon.



Check the status of DO1 on the R40 page as closed.



Check the value of register 20130 of the network port slave on the R40 page as "2.356".



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

3) Inquiry DIN Status

SMS Command		Return SMS Content
Inquiry Status	password+DINE	DIN1:Open/Close DIN2: Open/Close -----

4) Set Digital Output

SMS Command		Return SMS Content
Switch ON DO1(Close)	password+DOC1	DO1: ON
Switch OFF DO1(Open)	password+DO1	DO1: OFF
Switch ON DO2(Close)	password+DOC2	DO2: ON
Switch OFF DO2(Open)	password+DO2	DO2: OFF
Inquiry DO Current Status	password+DOE	DO1: ON/OFF DO2:ON/OFF

5) Inquiry AIN Status

SMS Command		Return SMS Content
Inquiry Status	password+AINE	AIN1:xxx AIN2: xxx AIN3:xxx AIN4: xxx

6) Digital Pulse Counter

SMS Command		Return SMS Content
Inquiry Pulse Counter Value	password+PR	DI1 counter value:xxx DI2 counter value:xxx
Clear DI1 Pulse Counter	password+DI1CLR	DI1 clear successfully
Clear DI2 Pulse Counter	password+DI2CLR	DI2 clear successfully

8. Warranty

1) This equipment will be repaired free of charge for any material or quality problems within one year from the date of purchase.
2) This one-year warranty does not cover any product failure caused by man-made damage, improper operation, etc

Shenzhen Beilai Technology Co., Ltd.
Website: https://www.bliiot.com