Industrial Cellular Router R10 R10A





Industrial cellular Router

R10 R10A

User Manual

Ver 1.0

Date updated: 2022-8-26 Shenzhen Beilai Technology Co.,Ltd www.iot-solution.com



Preface

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

Copyright statement

The ownership of this manual is owned by Shenzhen Beilai Technology Co., LTD. Without the written permission of the company, any units and individuals have no right to copy, disseminate or reprint any part of this manual in any form, otherwise all consequences shall be borne by the violators

Disclaimer

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

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

Revision History

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

Models Selection Table

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



Directory

1. Product introduction	
1.1. Brief Introduction	6
1.2. Typically Applications	
1.3. Safety instructions	9
1.4. Standard Packing List	9
1.5. Main Features	11
1.6. Technical parameters	12
1.7. Models Selection Table	
2. Hardware description	15
2.1. Device size	16
2.2. Indicator light	17
2.3. Reset button	
2.4. SIM card	
2.5. Connect the external antenna	
2.6. Ground the router	
2.7. Installation	19
2.7.1 Wall-mounted installation	19
2.7.2 Rail mounting	19
3. Router operation (basic operation)	
3.1. Start the Router device	
3.1.1. Power on the device	
3.1.2. System running status	
3.2. SIM Card operation instructions	
3.3. Serial port operation	21
3.3.1. Modbus master	
3.3.2. Modbus slave	22
3.3.3. Transparent transmission	
3.3.4. Modbus RTU to TCP protocol convert	23

BLIOT MAKE IIOT EASIER

Industrial cellular Router R10 R10A

4. Prepare (Configuration router by WEB	
4.1. Wire	ed connection router	23
4.2. WiF	i Connection router	
4.3. Fact	ory default Settings	27
4.4. Logi	in configuration page on WEB browser	
5. Configur	e router	29
5.1. Statu	us	29
5.2. Syst	em	
521	System Pronerties	30
5.2.1.	System Management Dights	31
5.2.2.	System Management Rights	
5.2.3.	Software Package	
5.2.4.	Backup/Upgrade	
5.2.5.	Reboot	
5.3. Netw	vork	
5.3.1	Network setting Interface (WAN/LAN switching, 4G, WAN6)	
	5.3.1.1 LAN port	
	5.3.1.2 WAN port	
	5.3.1.3 WAN/LAN switching	
	5.3.1.4 WAN6 Port	
	5.3.1.5 4G Port	40
5.3.2	WIFI (AP mode or WLAN Client)	
	5.3.2.1 WLAN Hotspot (Wifi AP mode)	
	5.3.2.2 WLAN Client (WiFi Client Mode)	
5.3.3	Cellular Network	
5.3.4	DHCP/DNS	
5.3.5	Host names	
5.3.6	Static Routes	52
5.3.7	Diagnosis	
5.3.8	Firewall	53
	5.3.8.1 Zone settings	53
	5.3.8.2 Port forwarding	56
	5.3.8.3 Traffic rules	
	5.3.8.4 Custom rules	
5.4. VPN	1	59



Industrial cellular Router R10 R10A

5.4.1	IPSec						
5.4.2	L2TP	61					
5.4.3	OpenVPN						
5.5. Rem	ote I/O and Serial Port setting	65					
5.5.1	Serial Port settings						
5.5.2	Transparent Transmission data						
5.5.3	Modbus RTU to TCP						
5.5.4	Modbus Slave	67					
5.5.5	Modbus Master	67					
5.6. Ever	nt and Alarm (without RTU IO)	71					
5.6.1	Alarm by E-mail & SMS	71					
5.6.2	Device monitor (device disconnection alarm)	72					
5.6.3	Event and Alarm	73					
5.7 Edg	ge computing and logical control	74					
5.7.1	Timer	74					
5.7.2	Arithmetic operation & logical operation	75					
	5.7.2.1 Introduction of arithmetic operation	75					
	5.7.2.2 Introduction of logical operation						
5.7.3	Combined conditions operation	80					
5.8 Co	nnection to Cloud Platform	83					
5.8.1	Private cloud (KPIIOT or Custom MQTT cloud)						
	5.8.1.1 KingPigeon Cloud Platform (KPIIOT)						
593	5.8.1.2 Other private cloud custom MQTT						
5.8.2							
5.8.5							
5.8.4	Huawei cloud						
5.8.5	Thingsboard cloud platform						
5.9 Log	gout						
6. Commun	5. Communication Protocol						
6.1 Mo	dbus RTU Protocol						
6.1.1	Platform connection setting						
6.1.2	Read Device Register Address	94					
Page	5 of 105 Shenzhen Beilai Technology Co.,Ltd	Ver 1.1					



Industrial cellular Router R10 R10A

6.1.2.1 Mapping Register Addr	ess
6.1.2.2 Read Boolean Mappi	ng Address Data95
6.1.2.3 Modify Boolean Map	ping Address Data
6.1.2.4 Read Data Type Map	ping Address Data97
6.1.2.5 Modify Data Type M	apping Address Data
6.2 MQTT Protocol	
6.2.1 MQTT Introduction	
6.2.2 MQTT Principle	
6.2.3 Device Communication	n Application
6.2.4 Publish MQTT Format	
6.2.5 Device Subscribe MQT	T Format101
7. SMS Command List	
8. Warranty	

1. Product introduction

1.1. Brief Introduction

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

Router function:

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

Data acquisition DAQ and cloud monitoring :

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

Extension function :

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



Industrial IoT Edge Router R10 Application Diagram





1.2. Typically Applications

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

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





1.3. Safety instructions



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



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

1.4. Standard Packing List

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

• 1 x Router device



• 1 x 7PIN 3.5mm Terminal





• 1 x antenna for 2G/3G/4G cellular



• 2 x antenna for WIFI 2.4G



• 2 x bracket kit for wall-mounted



• 1 x bracket kit for DIN rail mounted



11

T



- 1 x Instruction Manual (PDF version) Note: Please scan the card QR code to download
- 1 x Certificate of QC pass



• 1 x Warranty card



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

1.5. Main Features

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



> Monitors the online status of network devices connected to the LAN port and reports the

status through the platform;

- Support IPTABLES firewall, various network protocols;
- Support WAN port and 4G network connection switch, preferentially use WAN port wired network;
- Supports MODBUS and MQTT protocols, and MQTT supports SSL encryption;
- Alarms are sent by SMS or email;
- Supports one-time timers, periodic timers, and cyclic timers;
- Supports remote upgrade through web pages.
- Dynamic DDNS: Supports peanut shell, 88IP, and dynDNS;

1.6. Technical parameters

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



Industrial cellular Router R10 R10A

	Protocol	802.11a/b/g/n (mixed)		
	Mode	AP mode, client mode		
	Frequency	2.4G		
	Channel	Channel 1 - 13		
	Security	Open, WPA, WPA2		
	Encryption	AES, TKIP, TKIPAES		
	Connection number	16(Max)		
	Speed	300Mbps(Max)		
	Transmit Distance	Max. 20 meters in open space where there is no obstruction		
	SSID	Support		
	Broadcast Switch	Support		
	Antenna Port Qty	1		
	Antenna Port Type	SMA hole type		
		GSM/EDGE: 900,1800MHz		
		WCDMA: B1,B5,B8		
	40(L-L)	FDD: B1,B3,B5,B7,B8,B20		
		TDD: B38,B40,B41		
		GSM/EDGE: 850,900,1800MHz		
		WCDMA: B1,B2,B5,B8		
	4G(L- AO)	FDD: B1,B2,B3,B4,B5,B7,B8,B28		
Collular		TDD: B40		
Network		WCDMA: B2,B4,B5		
NELWOIK	40(L-A)	FDD: B2,B4,B12		
	4G(L-V)	FDD: B4,B13		
		WCDMA: B1,B3,B8,B18,B19,B26		
	4G(L-J)	FDD: B2,B4,B12		
		TDD: B41		
		GSM/EDGE: 900,1800MHz		
		WCDMA: B1,B8		
	4G(L-CE)	TD-SCDMA: B34,B39		
		FDD: B1,B3,B8		
		TDD: B38,B39,B40,B41		
	Qty	1		
SIM	Interface Spec	Drawer interface, support 1.8V/3V SIM/UIM card (NANO)		
	Protection	Built-in 15KV ESD protection		
	Antenna qty	1		
GDS	Antenna type	SMA hole type		
(ontional)	Tracking Sensitivity	> -148 dBm		
(Optional)	Horizontal Accuracy	2.5m		
	Protocol	NMEA-0183 V2.3		
Indicator		System running indicator (blinking for 2S and then off after		
light	515	normal operation)		
IIBLIC	4G	4G cellular operating status indicator (when SIM registered		



Industrial cellular Router R10 R10A

		successfully, this indicator always on)			
	WAN	WAN status indicator			
	LAN	LAN status indicator			
	CPU	MIPS CPU, main frequency 580Mhz			
System	Storage	128Mbits SPI Flash			
	RAM	1024Mbits DDR2			
	Network Dustant	PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT,			
	Network Protocol	HTTP, HTTPs, DNS, ARP, NTP, SMTP, SSH2, DDNS			
	VPN	IPsec, OpenVPN, L2TP			
	Einer auf	DMZ, DoS defense, IP packet, domain name and MAC			
Software	Firewall	address filtering, port mapping, access control			
	Remote				
	Management	Supports web remote configuration			
	System Log	Support			
	Firmware Update	Supports serial port local TFTP and Web upgrade			
	EMI	EN 55022: 2006/A1: 2007			
		IEC(EN)61000-4-2(ESD)			
		IEC(EN)61000-4-3(RS)			
Contificate	ENAC	IEC(EN)61000-4-4(EFT)			
Certificate	EIVIS	IEC(EN)61000-4-5(Surge)			
		IEC(EN)61000-4-6(CS)			
		IEC(EN)61000-4-8			
	Others	CE, FCC, ROHS, 3C			
	Working	20~+65°C			
Working	temperature	-20 +105 C			
Environment	Storage	40~,±85°C			
Environment	temperature	-40~+85~0			
	Humidity	5 ~ 95%RH (non-condensation)			
	Enclosure	Metal material			
	Size	Height 110mm * Length 83mm * Width 30mm			
Others	IP level	IP30			
	Net weight	300g			
	Installation	Wall mounted, DIN rail			



1.7. Models Selection Table

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

2. Hardware Description





2.1. Device Size





2.2. Indicator light



LED Indicator light							
	Name	Status	Description				
CVC	System running status indicator	Always on	Working normally				
515	System running status indicator	Light off	Device fail				
		Clow flach	Cellular network normal				
4G	4G cellular status indicator	SIOW HASH	(registration successful)				
		Light off	abnormal				
	WAN status indicator	Fast flash	WAN port normal				
VVAN		Light off	abnormal				
	I AN status indicator	Always on	LAN port is normal				
		Light off	abnormal				

2.3. Reset button

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



2.4. SIM card

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



2.5. Connect the external antenna



2.6. Ground the Router

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





2.7. Installation

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

2.7.1 Wall-mounted installation



2.7.2 Rail mounting





3. Router operation (basic operation)

3.1. Start the Router device

3. 1. 1. Power on the device

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



3. 1. 2. System running status

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





3.2. SIM Card operation instructions

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

After the device is powered on and running properly, log in to the router configuration interface -- Network -- Cellular network (For login operations, see<u>4.Log in to the Web page and configure</u> 4G cellular dial-up networking by default SIM card For details, see<u>5.3.1Network setting</u> <u>interface</u> and <u>5.3.3.The cellular network</u>

R10A	
condition ≁ system ≁ The	internet + VPN + Remote I/O + Events and Alerts + Operations and Control + cloud platform + quit
cellular network	UNSAVED CONFIGURATIONS : 2
Enable cellular	
registration status	registered
operator	China Unicom
signal strength	19 Signal value normal range 14-31
Firmware version	EC200NCNLAR03A02M08
IMSI	460015426281730
IMEI	865016056486590
SIM card ID	89860120801848168834
card number	
Card APN	
card username	
card password	
GPS enabled	
automatic network switch	0
save and apply save	reset

3. 3. Serial port operation

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

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





3. 3. 1. Modbus Master

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

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

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

3. 3. 2. Modbus slave

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



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

3. 3. 3. Transparent transmission

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

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

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

4. Prepare Configuration router by WEB

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

4.1. Wired connection router

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

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



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

	× + + = = = = = = × - 1	
Control Panel >	Network and Internet Network and Sharing Center	r 🗸 44 Search Control Panel 🔎
File Edit View Tools Help		
Control Panel Home	View your basic network information a	and set up connections
Change adapter settings	A	See full map
Change advanced sharing settings	PC-20190610RMNY Netw (This computer)	rork Internet
	View your active networks	Connect or disconnect
	Public network	Access type: Internet Connections: Connection
	Change your networking settings	
	Set up a new connection or network Set up a wireless, broadband, dial-up, ad	I hoc, or VPN connection; or set up a router or access point.
	Connect to a network	
	Connect or reconnect to a wireless, wired	d, dial-up, or VPN network connection.
	Choose homegroup and sharing options	5
	Access files and printers located on othe	r network computers, or change sharing settings.
See also	Troubleshoot problems	
HomeGroup	Diagnose and repair network problems, o	or get troubleshooting information.
Internet Options		
Windows Firewall		

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

IPv4 Connec	tivity:	Internet
IPv6 Connec	tivity:	No Internet access
Media State:		Enabled
Duration:		07:35:18
Speed:		100.0 Mbps
Details		
Details	Sent —	Received
ctivity	Sent — 102,166,751	Received

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



		Configure
his connection uses	the following items:	Configure
Client for Mic	rosoft Networks	
Shrew Soft L	ightweight Filter	
 File and Print 	scheduler er Sharing for Microsoft	Networks
 Internet Proto 	col Version 6 (TCP/IP	v6)
🗹 📥 Internet Proto	ocol Version 4 (TCP/IP	v4)
Link-Layer To	opology Discovery Map	pper I/O Driver
✓ ▲ Link-Layer 10	opology Discovery Res	ponder
Install	Uninstall	Properties
Description		
Transmission Contro	ol Protocol/Internet Pro	tocol. The default
wide area network		

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

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

General Alternate Configuration					
You car this cap for the	get IP settings assigned auton ability. Otherwise, you need to appropriate IP settings.	natically if ask your r	your n netwo	etwork s rk admin	supports strator
O Oł	tain an IP address automatical	ly			
O Us	e the following IP address:				
IP ac	ldress:			+	
Subr	et mask:				
Default gateway:					
() Oł	tain DNS server address auton	natically			
O Us	e the following DNS server add	resses:			
Prefe	erred DNS server:				
Alter	nate DNS server:		,	,	
V	alidate settings upon exit			Adva	anced



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

eneral						
You car this cap for the	n get IP settings assigned a bability. Otherwise, you ner appropriate IP settings.	automaticall ed to ask yo	y if y iur n	our n etwor	etwork 'k admir	supports histrator
0	btain an IP address automa	atically				
O Us	se the followin <mark>g</mark> IP address					
IP ad	ddress:		•			
Subr	net mask:					
Default gateway:						
() O	btain DNS server address a	utomatically	,			
O Us	se the following DNS server	addresses	-			
Prefe	erred DNS server:				+	
Alter	mate DNS server:			,	2	
V	alidate settings upon exit				Adv	anced

5. Click OK to complete the configuration



4.2. WiFi Connection router

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



Dial-up and VPN	^	*
Broadband Connection		1
Wireless Network Connection	^	
KINGPIGEON	liter	
niuren	lite	
ChinaNet-DFxQ	liter	
mazentop	lite.	
King-xxxxx	lte.	
Connect automatically	Connect	
DIRECT-11-HP DeskJet 3630 series	Ite.	
TP-E	100	+

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

Currently connected to:	+1	^
King-xxxxx Internet access		-
Dial-up and VPN	~	-
Broadband connection		- 22
Wireless internet connection	~	
King-xxxxx	Connected	
niuren	lite.	
KINGPIGEON	line.	
ChinaNet-DFxQ	Itee	
mazentop	lite.	
DIRECT-11-HP DeskJet 3630 series		+

4. 3. Factory default Settings

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



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

4.4. Login configuration page on WEB browser

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

← → →

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

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

R10
Authorization required Please enter your username (default is admin) and password (default is no password). username password
Log in Powered by KingPigeon Technology Co., Ltd. (v1.20.8) / 2021-07-22



5. Configure router

5.1. Status

R10A	
condition - system - The internet - VPN -	Remote I/O + Events and Alerts + Operations and Control + cloud platform + quit
	UNSAVED CONFIGURATIONS : 2 AUTO REFRESH ON
system	
CPU name	R10A
Host model	R10A-4G Industrial Router
Firmware version	KingPigeon Technology Co., Ltd. v1.30.2
kernel version	4.14.162
local time	2022-03-03 17:57:57
operation hours	0h 29m 25s
load average	0.06, 0.06, 0.09
RAM	
Available numbers	61.88MB / 121.33MB (50%)
number of idle	70.69MB / 121.33MB (58%)
buffered	6.78MB / 121.33MB (5%)
cached	19.10MB / 121.33MB (15%)
_	
i ne internet	
IPv4 upstream	IPv4 upstream
Protocci: UMTS/GPRS/EV-DO Address: 10 139:110:21032 Gateway: 10:64.64.64 DNS 1: 120:80:80 DNS 2: 2215:88:88 Connected: 0h 27m 4s	Protocol: DHCP Client Address: 192.168.1.220/24 Gateway: 192.168.1.1 DNS 1: 202.96.128.166 DNS 2: 114.114.114.114 Expiration Time: In 32m.26s Connected: 0h.27m.34s
	THE Devices College VII AND Table 2"

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



5.2. System

5. 2. 1. System Properties

F	R10A
	condition • system • The internet • VPN • Remote I/O • Events and Alerts • Operations and Control • cloud platform • quit
	UNSAVED CONFIGURATIONS 2 AUTO REFRESH ON
5	System properties
	basic settings log time synchronization Language and Interface
	local time 2022/3/3 7745.59.02 Sync browser time Synchronize with NTP server
	CPU name R10A
	Time zone 亚洲小上海
	save and apply - save reset
	Powered by KingPigeon Technology Co., Ltd. (v1.30.2) / 2022-02-21

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

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



5. 2. 2. System Management Rights

R10A					
condition - system - The	e internet - VPN - Remote I/O -	Events and Alerts +	Operations and Control +	cloud platform +	quit
				UNSAVED CO	NFIGURATIONS : 2
host password					
Change the administrator passw	ord to access the device				
password		*			
confirm password		*			
					save
	Powered by KingPigeo	n Technology Co., Ltd. (v	1.30.2) / 2022-02-21		

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

5. 2. 3. Software Package

This function provides software installation, removal, and upgrade.



Industrial cellular Router R10 R10A

filter: Enter to filter	Clear Package r	and install the package: ame or URL confi	action: update list	Upload package	configure opkg
available It has been installed	d renew	no package		*	
package name	Versio	n	size (.ipk)	describe	
No information available					
	Powered by	KingPigeon Technology Co., L	.td. (v1.30.2) / 2022-02-2	I	

(Note: This is advanced function for professionals!)

5. 2. 4. Backup/Upgrade

R10A	
condition 🔹 system 👻 The internet 👻 VPN 👻 Remote I/O 👻 Events and Alerts 👻 Operations and Control 👻 cloud platform 👻 quit	
UNSAVED CONFIGURATIONS :	2
acuon comgure	
backup	
Click "Make Backup" to download a tar archive of the current configuration file.	
Download backup generate backup	
recover	
Upload a backup archive to restore the configuration. To restore the firmware to its original state, click Perform Reset (only squashfs formatted firmware works).	
restore to factory settings perform a reset	
restore configuration Upload backup	
Oustom files (certificates, scripts) remain on the system. If you don't need to keep it, please perform a factory reset first.	
Save mtdblock content	
Click Save mtdblock to download the specified mtdblock file. (Note: This feature is for professionals!)	
select mtdblock u-boot	
download mtdblock save mtdblock	
flash new firmware	
Upload a sysupgrade compatible image from here to update running firmware.	
firmware file Flash the firmware	

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



Industrial cellular Router R10 R10A

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

5.2.5. **Reboot**

Click Perform Reboot to restart the system on your device.

R10A									
conditio		system +	The internet +	VPN +	Remote I/O +	Events and Alerts +	Operations and Control +	cloud platform 👻	quit
								UNSAVED CO	NFIGURATIONS : 2
Warnin	g: Some	e unsaved c	configurations will	be lost aft	er reboot!				
perfor	m a res	tart							
				Doword	d by KingPigoon	Technology Co., Ltd. (v	1 30 2) / 2022 02 21		
				Fowere	a by Kingrigeon	Technology Co., Ltd. (v	1.30.2)72022-02-21		

5.3. Network

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

You can restart, close, edit, or delete an existing interface, or add a new interface. By default, interfaces such as LAN, WAN, WAN6, and 4G are configured. You can click Edit to modify detailed configurations.



interface		U.	ISAVED CONFIGU	ATIONS : 2 A	JTO REFRESH
LAN	Protocol: Static Address Runtime: 0h 34m 55s MAC: BE:52:50:C9:D8:2B				
br-lan	Receive: 3.50 MB (23523 packets) Send: 6.45 MB (25563 packets) IPv4: 192.168.3.2/24 IPv6: fd3b:3dbb:e566::1/60	reboot	closure	edit	delete
WAN	Protocol: DHCP Client Run Time: 0h 33m 49s MAC: EE-52-50:C0:D8:2C				C
eth0.2	Receive: 4.21 MB (31541 packets) Send: 3.29 MB (18732 packets) IPv4: 192.168.1.220/24	reboot	closure	edit	delete
WAN6	Protocol: DHCPv6 Client MAC: BE:52:50:C9:D8:2C	reboot	closure	edit	delete
eth0.2	Receive: 4.21 MB (31541 packets) Send: 3.29 MB (18732 packets)				
4G	Protocol: UMTS/GPRS/EV-DO Runtime: 0h 33m 19s				
3g-4G	Receive: 66 B (5 packets) Send: 180 B (19 packets) IPv4: 10.139.110.210/32	reboot	closure	edit	delete

5.3.1.1 LAN port

R10A					
condition - svsta	m ≠ The interne	t= VPN= Re	emote I/O + Even	ts and Alerts - Operations and Control - cloud platform - quit	
Interface » L/	AN				n (j
ir basic settings	advanced settings	physical setup	Firewall settings	DHCP server	
	condition	Device: br-lan Runtime: 0h 34 MAC: BE:52:50 Receive: 3.34 I Send: 6.15 MB IPv4: 192.168.3 IPv6: fd3b:3db	4m 11s 0:C9:D8:2B MB (22861 packets) (24779 packets) 3:2/24 b:e566::1/60		
	protocol	tatic address	~		
A	uto run at boot 🛛 💆	1			
	IPv4 address	92.168.3.2			
IPv-	4 subnet mask 2	55.255.255.0	•		
	IPv4 gateway				
1	Pv4 broadcast	92 <mark>.16</mark> 8.3.255			
Use a custo	m DNS server		+		
IPv6 al	location length	0) Allocate the give	• en length portion of e	each public IPv6 prefix to this interface	
IPv6 As	signment Tips) Assign this hexa	idecimal subID prefit	x to this interface.	
	IPv6 suffix	1 Optional, allower "a:b:c:d::") is obt	d values: "eui64", "ra tained from the auth	andom" and other fixed values (eg: "::1" or "::1-2"). When the IPv6 prefix (eg ortzation server, use the suffix (eg "::1") to synthesize the IPv6 address	
		("aːbːcːdːː1") ass	signed to this interfac	ce.	

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



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



	Use gateway hops		The default 0
	Duidaa	interfaces	Create a bridge for the specified interface.
	Dridge	mernaces	This parameter is selected by default.
	Opent	he STD	Enable spanning tree protocol on this bridge,
physical setting	opent		not selected by default.
	Enable	e IGMP sniffing	Enable IGMP snooping on this bridge, not
	Endor	ionin shiring	selected by default.
			VLAN: eth0.1 (LAN) for switches and
			Master king-xxxxx (LAN) for wireless
	Interfa	ce	networks. You do not need to change the
			Settings of physical interfaces that use LAN
			Assign a firewall area to the interface, select
Firewall	Create	/assign firewall	unspectified to remove the interface from the
Settings	areas		associated area, or fin in the create field to
			interface with it
			The DHCP service is not provided on this
	Basi c setup	Ignore this	interface. This parameter is not selected by
		interface	default.
			The starting base address assigned to a
		start	network address. The default of 100.
		The customer	Maximum number of addresses allocated.
		number	The default of 150.
		Lesse	The minimum expiration time of the rented
		Lease	address is 2 minutes (2m). The default 12 h.
			Provides DHCP services for all clients. If
		Dynamic DHCP	disabled, only customers with static leases
			will be served. This parameter is selected by
DHCP	Adv		default.
server	ance		Force DHCP on this network even if another
	d	Mandatory	server is detected. This parameter is not
	Setti	ID-1	selected by default.
	ngs	IPv4 subnet mask	Reset the subnet mask sent to the client.
		DUCP ontions	set the DHCP additional options, such as
		DHCP options	different DNS server to the client
		Routing	different Divis server to the chent.
		Advertisement	Default Server mode
		service	
	IPv6	DHCPv6 service	Default Server mode
	is set	HDP agent	Disabled by default
		DHCPv6 mode	The default is stateless + stateful
		Always advertise	It advertises itself as the default route even if


the default re	oute	no public network prefix is available. This
		parameter is deselected by default.
DNS serve	r for	This parameter is not required based on actual
notification		Settings
The adve	rtised	This non-motor is not required based on estual
DNS d	omain	Settings
name		Settings

5.3.1.2 WAN port

R10A			
condition = system = TI	ne internet + VPN + Remote I/O + Events a	nd Alerts - Operations and Control - cloud platform -	quit
Interfaces » WAN			ON
ir basic settings advance	d settings physical setup Firewall settings		
cond	Ition Provided and the second		
pro	tocol DHCP client 🗸		
Auto run at	boot 🔽		-
Hostname sent v requesting D	HCP R10A		
		Cancel	save
eth0.2	Send: 3.36 MB (18967 packets)		
4G 3g-4G	Protocol: UMTS/GPRS/EV-DO Runtime: 0h 33m 40s Receive: 66 B (5 packets) Send: 180 B (19 packets) IPv4: 10.139.110.210/32	reboot closure edit	delete
Add new interface			
		save and apply 💌 se	

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



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

5.3.1.3 WAN/LAN switching

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



R40B state - system - service - The internet - VPN - application - RTU I/O - logic operation - cloud platfor	m − quit
Interface LAN/WAN switch Global network options	AUTO REFRESH ON
Switch MAN part to I AN part	
Save and apply	save
Powered by KingPigeon Technology Co., Ltd. (v1.20.10) / 2021-09-09	

5.3.1.4 WAN6 Port

condition - system - The inter	net - VPN - Remote I/O - Events and Ale	erts • Operations and Control •	cloud platform + quit
Interfaces » WAN6			ON 1
ir basic settings advanced settin	gs physical setup Firewall settings		
condition	 Device: eth0.2 MAC: BE:52:50:C9:D8:2C Receive: 4.28 MB (32070 packets) Send: 3.42 MB (19115 packets) 		
protocol	DHCPv6 client		
Auto run at boot			
request IPv6 address	try 🗸		
Request an IPv6 prefix of the specified length	automatic *		
			Cancel save
	ienu, 5.42 mb (10110 packets)		
4G 30-40	Irotocol: UMTS/GPRS/EV-DO Runtime: 0h 33m 55s Geceive: 66 B (5 packets) iend: 180 B (19 packets) Pv4: 10 139 110 210/32	reboot closure	edit delete
		save and	d apply - save reset

	V	VAN6
Project		Instructions
		Equipment: eth0.2
Basic setup	state	MAC: E2:2F:C4:54:93:BB
		Reception: 115.31 MB (299495 packets)



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

5.3.1.5 4G Port



	~				
ir basic settings	advanced setting	s Firewall settings			
	condition	Device: 3g-4G Runtime: 0h 34m 15s Receive: 66 B (5 packets) Send: 180 B (19 packets) IPv4: 10.139.110.210/32			
	protocol	UMTS/GPRS/EV-DO	~		
A	uto run at boot	2			
10	modem device	/dev/ttyUSB2	•		
	Service type	UMTS/GPRS	•		
	APN	cmnet			
	PIN				
PAP/CH	HAP username				
PAP/CI	HAP password		*		
	dial number	*99***1#			

4G

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



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

5.3.2 WIFI (AP mode or WLAN Client)

MAC address host Signal/Noise Receive Rate/Transmit Rate No information available No <	
No information available	
save and apply + save	reset
Powered by KingPigeon Technology Co., Ltd. (v1.30.2) / 2022-02-21	



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

5.3.2.1 WLAN Hotspot (WiFi AP mode)

R10A
condition - evision - The internet - VPN - Remote #0 - Events and Alarts - Operations and Control - could platform - out
Device Configuration
basic settings
Condition Mode: Master SSID: King-R10TEST 0% BSSID: C8:EE:A6:99.88.1 Encryption: None Channels: 11 (2:462 CHz) Transmit Power: 20 dBm Signal: 0 dBm Noise: 0 dBm Transmit Rate: 0.0 Mbit/s Country: 00
wireless network enabled disabled
model channel bandwidth working frequency N ✓ 11 (2452 Mhz) ✓ 40MHz ✓
maximum transmission power driver default v Current power : 20 dBm
Specifies the maximum transmit power. Depending on regulatory requirements and usage, the onver may limit the actual transmit power below this value.
Interface configuration
basic settings wireless security MAC filtering advanced settings
model access point AP
ESSID King-R10TEST
The internet Ian: 🕎 🙊 🗘 🗘 🗸 🗸 🕜 The internet Ian: Image Ian
Hide ESSID
WMM mode 🗾

The default SSID is KING-XXXXXX (XXXXXX is a 6-digit random number and letter combination). The encryption mode does not exist. Other clients (such as mobile phones and computers) can directly search for wireless networks and connect to this hotspot.

Quick configuration: Select the wireless configuration in Master mode in WiFi Settings, click "Edit" to enter the configuration page, find "Interface Configuration" -- "Basic Settings" -- "ESSID" to modify the WiFi hotspot name, find "Interface Configuration" -- "Wireless Security" --"Encryption" to modify the encryption mode and set the WiFi password.

Note: If you use WiFi to access router configurations, select Force Apply to modify WLAN hotspot configurations. In this case, click Save and Apply and select Force Apply.





Wireless AP hotspot device configuration				
Project		Instructions		
		4 97%		
		Pattern: Master SSID: King - ff4a8a		
		BSSID: EE:0C:45:81:26:51		
	State	Encryption: None		
		Channel: 6 (2.437 GHz)		
		Transmission power: 20 dBm		
		Noise signals: - 42 dBm : 0 dBm		
		Transfer rate: 58.5 Mbit/s countries: 00		
Basic setup	Wireless network enabled	Enabled by default		
		If the current frequency has too many devices		
	Working frequency	in use, please change the frequency to reduce		
		interference and optimize the signal		
		Specifies the maximum transmitted power.		
	Maximum transmission	Depending on regulatory requirements and		
		usage, the driver may limit the actual		
	power	transmitted power below this value. The		
		signal		
	Country code	Driven by default		
	Allows traditional	Check the default		
	802.11b rates			
		Distance of the farthest network user (in		
	Distance optimization	meters). Default automatic, according to the		
		distance to automatically adjust the		
		transmission power		
		When the data length exceeds the threshold,		
	Fragmentation threshold	fragments are automatically sent. The default		
		value is generally used		
Advanced		Request send/Permit send protocol. When the		
Settings		data length exceeds the threshold, enable this		
	The RTS/CTS threshold	protocol to avoid signal conflicts caused by		
		multiple terminals sending data to the AP.		
		The default value is generally used		
		The 40MHz channel is always used even		
		when the auxiliary channels overlap. Using		
	Mandatory 40MHz mode	this option does not comply with IEEE		
		802.11N-2009! This parameter is not selected		
		by default.		
		Indicates the interval at which a wireless		
	Beacon interval	route broadcasts its SSID periodically. The		
		default value is generally used		



Configure AP hotspot interfaces on wireless networks				
Project		Instructions		
	Model	Access point AP		
	ESCID	Default king-xxxxx (XXXXXX is a 6-digit		
		random number and letter combination)		
		Default LAN, select the network assigned to		
Basic setun	network	this wireless interface, or fill in the Create		
Dusie setup		field to create a new network.		
	Hide the ESSID	Not selected by default		
		WiFi multimedia: Provides different priorities		
	WMM mode	for different services to ensure service		
		quality. This parameter is selected by default		
Wireless	Encryption	Default no encryption (open network)		
security				
MAC	MAC Address Filtering	Disabled by default		
filtering				
	Quarantine client	Disable communication between clients. This		
		parameter is not selected by default		
	The name of the interface	Reset the default interface name		
	Short Preamble	Different rates require different preambles.		
		This parameter is selected by default		
	DTIMinterval	As a terminal node, periodically wakes up		
A 1 1	T: :	and sends traffic indication message intervals		
Advanced	Time interval for	Ine temporary secret key (GIK) uses the		
Settings	Disable inective polling	Not colocted by default		
	Disable mactive poining	The default 200 seconds		
	Maximum listoning	The default 500 seconds		
	interval allowed	Default maximum of 65535		
		Disconnect a windless terminal in law ACK		
	Disconnect on low Ack	mode when AP mode is enabled This		
	reply	narameter is selected by default		
		parameter is selected by default		

5.3.2.2 WLAN Client (WiFi Client Mode)



conditions and tender. Will + Iterated Will + Iterated IO + Excels and Alexis - Considers and Control + Ideal distance - out						
Signal	SSID	channel	model	BSSID	encryption	
60%	jinge	1	Master	24:69:68:82:3C:96	mixed WPA/WPA2 PSK (CCMP)	Join the network
41%	King-dc4c08	11	Master	C0:1C:30:00:0A:CE	None	Join the network
35%	OrayBox-8778	1	Master	A0:C5:F2:BB:87:78	WPA2 PSK (CCMP)	Join the network
al 34%	ChinaNet-vwRV	3	Master	F0:92:B4:29:6F:B1	mixed WPA/WPA2 PSK (TKIP, CCMP)	Join the network
34%		4	Master	3A:54:9B:3C:16:72	mixed WPA/WPA2 PSK (CCMP)	Join the network
28%	DIRECT-58-HP DeskJet 3630 series	6	Master	40:B0:34:63:EB:59	WPA2 PSK (CCMP)	Join the network
wenty four%	KingPigeon	11	Master	20:DC:E6:FF:D2:23	mixed WPA/WPA2 PSK (CCMP)	Join the network
wenty one%	xingchen	1	Master	30:FC:68:A7:84:46	mixed WPA/WPA2 PSK (CCMP)	Join the network
20%	King-b42dd6	11	Master	EC:0C:45:81:17:68	None	Join the network
						Cancel

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

Wireless network client device configuration			
Project		Instructions	
		1 00%	
		Pattern: Client SSID: jingekeji	
		BSSID: EC:0C:45:81:26:51	
	State	Encryption: WPA2 PSK (CCMP)	
		Channel: 6 (2.437 GHz)	
		Transmission power: 20 dBm	
		Noise signals: - 38 dBm : 0 dBm	
Basic setup		Transfer rate: 1.0 Mbit/s countries: 00	
	Wireless network enabled	Enabled by default	
		If the current frequency has too many devices	
	Working frequency	in use, please change the frequency to reduce	
		interference and optimize the signal	
		Specifies the maximum transmitted power.	
	Maximum transmission	Depending on regulatory requirements and	
	power	usage, the driver may limit the actual	
		transmitted power below this value.	
	Country code	Driven by default	
	Allows traditional	Selected by default	
	802.11b rates		
		Distance of the farthest network user (in	
Advanced Settings	Distance ontimization	meters). By default, the transmission power is	
	Distance optimization	automatically adjusted according to the	
		distance	
		When the data length exceeds the threshold,	
	Fragmentation threshold	fragments are automatically sent. The default	
		value is generally used	



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

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



5.3.3 Cellular Network

R10A					
condition - system - The	internet - VPN - Remote I/O -	Events and Alerts -	Operations and Control -	cloud platform - quit	
cellular network				UNSAVED CONFIGURATIONS : 2	Ì
Enable cellular					
registration status	registered				
operator	China Unicom				
signal strength	19 Ø Signal value normal range 14-31				
Firmware version	EC200NCNLAR03A02M08				
IMSI	460015426281730				
IMEI	865016056486590				
SIM card ID	89860120801848168834				
card number					
Card APN					
card username					
card password					
GPS enabled					
automatic network switch					
save and apply save	reset				

The cellular network				
Project	Instructions			
Registration status	Displays cellular registration status			
Operator	The operator of the SIM card is displayed			
Signal strength	Signal value normal range 14 to 31			
Firmware version	Displays the module firmware version			
IMSI	The IMSI code of the SIM card is displayed			
IMEI	Displays the IMEI of the module			
	The ICCID number of the SIM card is			
SIM card ID	displayed			
The card number	Enter card 1 number			
Card APN	Enter the SIM card access point			
The card user name	Enter SIM card Internet access account			
Card password	Enter the SIM card Internet access password			
	Default is disable,			
	When the router you bought supports GPS			
	function, please check this item to enable			
Evel1. CDS	GPS function. GPS data will be uploaded			
Enable GPS	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

R10A	
condition - system - The	internet • VPN • Remote I/O • Events and Alerts • Operations and Control • cloud platform • quit
	UNSAVED CONFIGURATIONS : 2 AUTO REFRESH ON
Server settings	
basic settings HOSTS and part	rsing files TFTP settings advanced settings static address assignment
Ignore empty domain name resolution	 Do not forward resolve requests without <u>DNS names</u>
unique authorization	This is the only DHCP server on the local network
local server	/lan/
local domain name	Ian Or The local domain name suffix will be added to the DHCP and HOSTS file entries
Record query log	Write incoming DNS requests to the system log
DNS forwarding	/example.org/10.1.2.3 + <u>List of DNS</u> servers to forward requests to
rebinding protection	 Discard RFC1918 upstream response data
Allow native	 Upstream responses within the loopback range of 127.0.0.0/8 are allowed, for example: RBL service
Domain whitelist	ihost.netflix.com + @ List of domain names allowed for RFC1918 responses

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

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



	Dehinding protection	Discard RFC1918 uplink response data. This			
	Rebinding protection	parameter is selected by default			
		Allows uplink responses in the 127.0.0.0/8			
	Allow the machine	loopback range, such as RBL service. This			
		parameter is selected by default			
	Domain nome whitelist	List of domain names allowed to respond to			
		RFC1918			
		The DNS service is available only on the			
	Local service only	subnet to which the NIC belongs. This			
		parameter is selected by default			
		Dynamically bound to an interface rather than			
	Non-full address	a wildcard address (recommended as the			
		Linux default), selected by default			
	Listening to the interface	Listen only on these and loopback interfaces.			
	Eliminate interface	Do not listen on these interfaces.			
HOSTS and parse files	Use/etc/ethers	Configure the DHCP server based on			
	configuration	/etc/ethers. This parameter is selected by			
		default			
	The lease documents	Leases a file used to hold assigned DHCP			
		leases. The default value is/TMP /dhcp.leases			
	Ignoring parsing files	Not selected by default			
	Ignore the/etc/hosts	Not selected by default			
	Additional HOSTS files	The default empty			
TFTP set	Enabling the TFTP Server	Not selected by default			
		Do not record routine operation logs of these			
	Not logging	protocols. This parameter is not selected by			
		default			
	Sequential IP address	IP addresses are assigned from the lowest			
	assignment	available addresses in sequence. This			
		parameter is not selected by default			
	Filtering local Packets	This parameter is selected by default			
		Do not forward requests that the public			
	Filtering useless packets	domain name server cannot respond to. This			
Advanced		parameter is not selected by default			
Settings		If more than one IP is available, the host			
	Localized query	name is localized based on the subnet from			
		which the request came, selected by default			
	Extend the host suffix in	Add the local domain name suffix to the			
	the HOSTS file	domain name in the HOSTS file. This			
		parameter is selected by default			
	Disable invalid	Do not cache useless responses, for example,			
		non-existent domain names. This parameter is			
	information caching	1			
	information caching	not selected by default			



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



5.3.5 Host names

R10A								
condition -	system -	The internet +	VPN -	Remote I/O -	Events and Alerts -	Operations and Control -	cloud platform - quit	
							UNSAVED CONFIGURATIONS : 2	
HOSUDOM								
CPU name					IP address			
					No configuration yet			
Add to								
						save a	nd apply save reset	
			Powere	d by KingPigeon	Technology Co., Ltd. (v	v1.30.2) / 2022-02-21		

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

5.3.6 Static Routers

Static IPv4	4 routing				
interface	Target	IPv4 subnet mask	IPv4 gateway	hop count	On-Link routing
	host IP or network	if the object is a network			
				save and	apply - save reset
		Powered by KingPigeon Techno	logy Co., Ltd. (v1.30.2) / 20	122-02-21	



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

Routing tables describe the reachable paths of packets ${\scriptstyle \circ}$

5.3.7 Diagnosis

www.baidu.com	openwrt.org	openwrt.org
IPv4 V Ping	IPv4 V Traceroute	Nslookup
PING www.baidu.com (14.215.177.38): 56 data bytes	
64 bytes from 14.215.177.38: seq=	0 ttl=56 time=7.115 ms	
64 bytes from 14.215.177.38: seq=	1 ttl=56 time=8.042 ms	
64 bytes from 14.215.177.38: seq=	2 ttl=56 time=6.813 ms	
64 bytes from 14.215.177.38; seq=	3 ttl=56 time=7.229 ms	
64 bytes from 14.215.177.38: seq=	4 ttl=56 time=6.987 ms	
www.baidu.com ping statistics		
5 packets transmitted, 5 packets	received, 0% packet loss	
<pre>round-trip min/avg/max = 6.813/7.</pre>	237/8.042 ms	

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

5.3.8 Firewall

5.3.8.1 Zone settings



					UNSAVED CONFIGURA
Firewall - Zo	one Setting ork traffic by creating z	S ones on network interfac	es.		
basic settings					
Enable SYN-flood	defense 🗹				
Drop invalid	packets 🗌				
Inbo	und data accept		•		
Outbo	und data accept		•		
	Forward accept		~		
	ffloading	are-based Routing/NAT	offload		
Software traffic o	Gon				
Software traffic o area Area ⇒ Forward	Inbound data	Outbound data	Forward	IP Dynamic Masquerading	
Software traffic o area Area ⇒ Forward	Inbound data	Outbound data	Forward accept	IP Dynamic Masquerading	= edit (
Software traffic o area Area ⇒ Forward Ian ⇒ wan wan ⇒ Accept	Inbound data	Outbound data accept ~ accept ~	Forward accept ~ accept ~	IP Dynamic Masquerading	edit c

Firewalls control network traffic by creating zones on network interfaces $_{\circ}$

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



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



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

5.3.8.2 Port forwarding

Firewall - Port Forwarding Port forwarding allows remote computers on the Internet to connect to specific computers or services on the Internal network.						
oort forwa ^{名称}	rding matching rules	forward to	enable			
		No configuration yet				
Add to			save and apply - save	reset		
	Powered by F	KingPigeon Technology Co., Ltd. (v1.30.2) / 202	2-02-21			

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

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



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

5.3.8.3 Traffic rules



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

5.3.8.4 Custom rules



be executed immediately	after the default rules are run.	t are not part of the firewall fr	amework. Each ume ure nrewa	ris restaneu, trese commanus wii
# This file is interpreted a # Put your custom iptabl # be executed with each	s shell script. s rules here, they will firewall (re-)start.			
# Internal uci firewall cha # put custom rules into tl # special user chains, e.	ns are flushed and recreated on reload, s e root chains e.g. INPUT or FORWARD c . input_wan_rule or postrouting_lan_rule	o or into the		
				save
	Powered by KingPi	geon Technology Co., Ltd. (v	.30.2) / 2022-02-21	

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



5.4. VPN

5.4.1 IPSec

Security /	Alliance			UNSAVED CONFIGURA
name	Both ends of the tunnel		condition	operation hours
		No configura	ation vet	
security s	strategy			
Below is the c	configuration and current status of IP	Sec		
名称	peer gateway	peer network	local subnet	enable
名称	peer gateway	peer network	local subnet	enable
名称	peer gateway	peer network No configure	local subnet	enable
名称	peer gateway	peer network	local subnet	enable
名称	peer gateway	peer network	local subnet	enable
名称 save and	peer gateway Add to d apply save reset	peer network	local subnet	enable
名称	peer gateway Add to d apply save reset	peer network	local subnet	enable

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

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

Including:

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

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

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

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



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



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

5.4.2 L2TP

R10A						
condition	- system -	The internet -	VPN - Rem	ote I/O - Events and Alerts -	Operations and Control $-$	cloud platform - quit
212.00	nnection					UNSAVED CONFIGURATION
Below is the	configuration a	nd current statu	s of L2TP			
名称	username	5	server/client	IPSec encryption	condition	enable
				No configuration yet		
		Add to				
save a	nd apply	save rese	t			
			Powered by Ki	ingPigeon Technology Co., Ltd. (v1.30.2) / 2022-02-21	

Layer 2 Tunneling Protocol (L2TP) is a Virtual Private Dial-up Network (VPDN) tunnel Protocol. The Virtual Private Dial Network (VPDN) uses the dial-up function and access Network of public networks (such as ISDN and PSTN) to implement the Virtual Private Network (VPDN) to provide access services for enterprises, small ISPs, and mobile office workers.

VPDN uses a dedicated network encryption communication protocol to establish secure virtual private networks for enterprises on public networks. An enterprise's overseas offices and



employees on business trips can remotely connect to the enterprise headquarters over the public network through a virtual encrypted tunnel. However, other users on the public network cannot access resources on the enterprise network through the virtual tunnel. The Layer Two Tunneling Protocol (L2TP) is the most widely used VPDN tunnel Protocol.1.

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

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



5.4.3 OpenVPN

名称	model	protocol	remote address	port	TUN/TAP device	connected	enable
				No configurati	on yet		
		Add to)				
save	and apply	save reset]				
			Powered by KingPige	on Technology C	o., Ltd. (v1.30.2) / 2022-02-	21	
			Powered by KingPige	on Technology C	o., Ltd. (v1.30.2) / 2022-02-	21	

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

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

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

OpenVPN				
Project	Instructions			



Enable	Check the enable				
Configure the client mode	Select client mode				
VDNI Colored ID - 1 dress / wester	In TAP mode, the server can transfer data				
VPN Sublet IP address/mask	from a host to a subnet				
Comun address	IP address of the server with which the client				
Server address	establishes a VPN connection				
	TCP/UDP port provided by the server for				
Port	establishing connections. The default value is				
	1194				
Use agreement	UDP, TCP-server, and TCP-client are used by				
	default				
	TUN mode Establishes layer 3 tunnels to				
	implement point-to-point transmission. Lay				
TUN/TAPequipment	2 tunnels are established in TAP mode to				
	implement transparent transmission of IP				
	packets				
	When security certificate authentication is not				
User name/password	applicable, you can use the user name and				
	password for authentication				
Encryption algorithm	Select an encryption algorithm for data				
Authentication and Authorization (Root	Select the root certificate provided by the				
Certificate)	server for file upload				
Local certificate	If file upload is selected, the client certificate				
	is generated based on the root certificate				
A local private key	Select the key corresponding to the client				
	certificate for file upload				
	This command is used for key exchange and				
DH key exchange parameters	can be generated by openssl dhparam-out				
	dh2048.pem 2048				
Compression algorithm	LZO _N LZ4				
Keepalive interval time (seconds)	Interval at which the server sends probe				
	packets to the client				
	If the server does not receive any response				
Keepalive timeout time (s)	trom the probe packet at this time, the				
	connection is restarted				

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



5.5. Remote I/O and Serial Port setting

5.5.1 Serial Port settings

R10A								
condition -	system -	The internet +	VPN ~	Remote I/O -	Events and Alerts -	Operations and Control -	cloud platform +	quit
							UNSAVED CO	NFIGURATIONS : 2
Senai por	r settings							
	equipm	ent serial port						
	baud r	ate 9600		*				
	data t	oits 8		~				
	Check D	igit without		~				
	stop	bit 1		~				
save and	apply	save						
			Power	ed by KingPigeon	Technology Co., Ltd. (v	1.30.2) / 2022-02-21		

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



5.5.2 Transparent Transmission data

R10A			
condition - system - The inte	met - VPN - Remote I/O -	Events and Alerts - Operations and Control	- cloud platform - quit
Serial port transparent tra	ansmission		5 : 2
S equipment		~	
network protocol type	TCP client	~	
Host IP or domain name	0.0.0.0;host.domain.xxx		
port	5000		
registration package]
heartbeat packet			-
Heartbeat response packet			
Heartbeat period (seconds)	60		
Host silent time (seconds)	3600		
Enable retransmission			
			Cancel save

5.5.3 Modbus RTU to TCP

R10A			
condition - system - The inte	met - VPN - Remote I/O -	Events and Alerts * Operations and Control * cl	oud platform 👻 quit
Modbus RTU to TCP			5.2
N equipment	•		
network protocol type	TCP client	•	
Host IP or domain name	0.0.0;host.domain.xxx		
port	5000		
registration package			1
heartbeat packet			
Heartbeat response packet			
Heartbeat period (seconds)	60		
Host silent time (seconds)	3600		
			Cancel save



5.5.4 Modbus Slave

condition	nternet ≁ VPN ≁ Remote I/O ≁	Events and Alerts - Operations and Control	cloud platform - quit
Modbus slave			
Native Modbus Device ID	2		
RTU Modbus Slave			
equipment	serial port 🗸		
TCP Modbus Slave			
port	503		
		sav	re and apply • save reset
	Powered by KingPigeon	Technology Co., Ltd. (v1.30.2) / 2022-02-21	

5.5.5 Modbus Master

名称	alias	slave address	register type	function code	Register first address	number of data	map address	Slave Interface	Enable settings	
123	1	3	boolean data	1	0	10	64-73	Ethernet		edit delete
234	2	4	16-bit data	3	0	10	20001- 20010	Ethernet		edit delete
345	3	5	32-bit data	3	0	10	20128- 20147	Ethernet		edit delete
			Add to							
								sav	e and apply 🔹	save

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

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



R10A								
condition	n ▼ system ▼	The internet + VI	PN + Remote	I/O - Events and Alerts -	Operations an	id Control 👻	cloud platform + quit	
							UNSAVED CONFIGU	RATIONS : 2
Modb	ous query							
Select	cnannei							
equipme	ent 1	ype of data	slave	e address Con	figuration name		display channel	
Etherne	t 🗸	Numeric type	✓ all	✓ all		~	display channel	
Modbu	s master							
alias	Configuration name	Slave Interface	slave address	type of data	map address	register address	Numerical value	
without	234	Ethernet	4	16-bit signed number Al	3 20001	0	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20002	1	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20003	2	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20004	3	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20005	4	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20006	5	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20007	6	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20008	7	0	edit
without	234	Ethernet	4	16-bit signed number Al	3 20009	8	0	edit

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

Nodbus Master - 123					
alias	1				
slave address	3				
register type	boolean data	~			
function code	01	~			
Register first address	0				
number of data	10				
map address assignment	automatic	~			
Polling period (seconds)					
Deserve the set (seconds)	If not set, the default	is 0.2 seconds			
Response timeout (seconds)	If not set, the default	is 0.5 seconds			
Slave Interface	Ethernet	~			
Slave IP address	192.168.3.232				
port	503				
				Cancol	0.001



Click "	Edit"	under d	etailed	configuratior	n to enter	the interf	ace of	setting s	slave data	points:
---------	-------	---------	---------	---------------	------------	------------	--------	-----------	------------	---------

condition + system + The inter	net - VPN - Remote	I/O - Events and Alerts -	Operations and	d Control – cl	oud platform –	aulit
Modbus query						S 1 2
A alias						
S type of data	16-bit signed number AB	~				
coefficient	1					
high threshold	100					
N High threshold recovery	80					
low threshold	0					
low threshold recovery	20					
Confirmation time (seconds)	1					
Enable alerts						
release						
					Cancel	save
without 234 Eth	ernet 4	16-bit signed number AB	20006	5	0	edit
without 234 Eth	ernet 4	16-bit signed number AB		6		edit
				7		

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



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



5.6. Event and Alarm (without RTU IO)

5.6.1 Alarm by E-mail & SMS

			UNSAVED CONFIGURATIONS
E-Mail settings			
Allow sending mail			
sender mail server	smtp.xxx.com		
port	465		
mail recipient	recipient@xxx.com		
mail sender	sender@xxx.com		
username	user name		
password		*	
SMS settings			
Alert phone number	13040884077	×	
	Ø Mobile phone number to receiption of the second secon	+ ve text messages	
01101	Chinese (Chinese)	~	

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

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



5.6.2 Device monitor (device disconnection alarm)

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

(••) R40B - Device Monitor&Ala	m × +							-	٥	×
\leftrightarrow \rightarrow C \blacktriangle Not secu	re 19 <mark>2.168.3.1/</mark> cgi-bi	in/luci/admin/io/mo	onitor						* 6	Э:
	R40B Status *	System - Services	s ≁ Network ≁ VPN ≁ S	Serial Port + RTU I/C) 🗸 🕴 Logical	operation - Clou	id platform 👻 Logout			
	Device Monitor Device Monitor									
	Register Address	In Name Sta	tus Device IP Address	Ping Times	Action	Hold time(s)	Enable setting			
	This section contains no values yet									
	Add									
						Save & Apply	Save Reset			
	Powered by KingPigeon	Technology Co., Ltd. (1	r1.18) / 2020-10-16							



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


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

5.6.3 Event and Alarm

		No c	onfiguration yet	
add alert				
Alarm name	texting	text message content	send email	content of email
REG64: close		DObj		
REG20001: Overthreshold 🗸		Alcx		
				42.04

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

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

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



5.7 Edge computing and logical control

5.7.1 Timer

R40	B	state	- system -	service -	The internet	- VPN -	application -	RTU I/O	 logic operati 	on ~ . c	cloud platform *	quit	
Tin	ner										UNSAVED CO	NFIGURATION : 2	
Time	er se	tting											
			Alias	CCC									
		т	ime interval	1									
			time unit	minute		~							
			action	All DO		~							
			DO status	closure		~							
	н	old time	e (seconds)	30									
		Sta	irt/stop time	every day		~							
		Start t	ime (hours)	14		~							
	S	tart tim	ie (minutes)	11		~							
		Sto	op condition	Cycles		~	1						
		L	Cycles	8									
	Return	to over	view	ve res	et								
F	R10A												
	conditi	on -	system +	The internet	+ VPN + F	Remote I/O -	Events and	Alerts + O	perations and C	ontrol -	cloud platform	← quit	
L	.001	o tir	ner								UNSAVED	CONFIGURATIONS	2
L	.oop	time	r										
	名称	a <mark>l</mark> ias	time interval	time unit	action	start (year)	start (month)	start (day)	starting time)	start (min)	enable		
	1A	Yes	1	minute	TREG-1A: close	without	without	without	16	32		edit delete)
	2a	Time	1	minute	REG72: close	without	without	without	16	32		edit delete]
				Add t	0								
									1	save a	ind apply	save reset	
					Powered I	oy KingPigeo	n Technology C	o., Ltd. (v1.3	0. <mark>2)</mark> / 2022-02-21	1			

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

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



Once timer: Execution only one time at a certain appointed time, similar to Alarm clock Cycle timer: Execution cycle at a certain time interval, such as every 5 seconds, every 1 hours

5.7.2 arithmetic operation & logical operation

5.7.2.1 Introduction of arithmetic operation

R10A						
condition - system - The Inte	met = VPN = Remot	te I/O + Events and A	lerts + Operations and	Control + cloud p	latform + quit	
Arithmetic Operations - A	DECONCIL					S:2
a Enter 1	REG20001	*				
a operation	+	~				
Enter 2	REG20002	~				
operation	*	~				
Enter 3	REG20003	~				
output address	REG20005	~]
					Cancel save	



名称	输入1	运算	输入2	运算	输入3	输出地址	输出值	
G	REG20001	х^у	1.53	*	0.5354	REG40000	23.978699	编辑 删除
		添加						
							保	存并应用・保存 复位
			Powered	l by KingPig	eon Technolog	y Co., Ltd. (v1.31.1)	2022-05-06	

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:



名称	输入1	运算	输入2	运算	输入3	输出地址	输出值	
G	REG20001	х^у	1.53	*	0.5354	REG40000	23.978699	编辑删除
A	REG20001	+	REG20002	+	REG20003	REG20004	12	編輯
		添加						
							保存并应	用・保存复位
			Powered b	y KingPiged	on Technology Co.,	Ltd. (v1.31.1) / 2022	2-05-06	

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.

🤉 мь	oslave1				
) = 2	:: F = 03				
	Alias	00000	223	^	
0	REG20001	15			
1	REG20002	20			
2	REG20003	30			
3	REG20004	1050			
4	REG20005	0			
5	REG20006	0			
6	7	0			
7	8	0			
8		0		~	

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



(+•) R408 - 逻辑运算 - LuCl × +	• - • >
← → C ▲ 不安全 192.168.3.1/cgi-bin/luci/admin/logic/logic/logic	☆ 🛓 :
R40B	
算术运算 逻辑运算 逻辑运算 布尔逻辑	
名称 输入1 条件 关系 输入2 条件 输出地址 输出值 逻辑值	
11A ALARM-REG20001 闭合 逻辑与 alarm20002 闭合 REG20003 5555 1 编辑	删除
添加	
数值逻辑	
名称 输入1 条件 门限值 关系 输入2 条件 门限值 输出地址 输出值 逻辑值	
尚无任何配置	
添加	
组合逻辑	
名称 输入1 条件 关系 输入2 条件 输出地址 输出值 逻辑值	
尚无任何配置	
志力	
保存井应用 - 保存	复位

5.7.2.2 Introduction of logical operation

ogi	c opera	ation										
oole	ean logic											
名称	Enter 1	condition	relation	Enter 2	condition	n output	address	output value	logical	value		
1b	REG72	closure	without	without	without	without		without	0		edit	delete
2b	TREG-1A	closure	without	without	without	without		without	0		edit	delete
			Add to									
ume	erical log	ic										
名 称	Enter 1	condition	Threshold value	relation	Enter 2	condition	Threshold value	output address	output value	logical value		
1c	REG20001	more than the	80	without	without	without	without	without	without	0	edit	delete
			Add to									
oml	oinatorial	logic										
名称	Enter 1	condition	relation	Enter 2	conditio	n output	address	output value	logical	value		
1d	1b	true	logical and	2b	true	REG20	002	1111	0		edit	delete



R40B 状态 - 系统 -	服务 - 网络 -	VPN - 应用 -	RTU I/O - 逻辑	运算 - 云平台 -	退出	未保存的配置
逻辑设置						
组合逻辑输入						
输入1		~				
条件	为真	~				
关系	逻辑与	~				
输入2		~				
条件	为真	~				
輸出类型	布尔类型	~				
輸出地址	DO1	~				
布尔值	断开	~				
输出延时(毫秒)						
设置默认值						
返回至概况						保存复位

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:

为小汉 \$	ĂΑ			B			Y			
名称	输入1	条件	孫关	输入2	条件	输出地址	输出值	逻辑值		
1	DI1	断开	逻辑与	DI2	断开	DO1	闭合	undefined	編輯	删除
			添加							
女 值逻辑	胄 <mark>C</mark>			D				Y		
名称	输入1	条件()	限值关系	(输入2	条件	门限值	输出地址	輸出值 逻辑值		
2	AJN1	大于 10)0 逻辑	武 AIN1	小于	30	DO2	闭合 undefined	编辑	删除
			添加							
目合逻辑	咠						Y			
名称	输入1	条件	茶茶	输入2	条件	输出地址	输出值	逻辑值		
3	1	为真	逻辑与	2	为真	REG20005	10000	undefined	编辑	删除
			· The state of the							

Logical operation example (1)

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

logical operation example (2)

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



logical operation example (3)

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

Similarly, you could create more combined logical operations.

5.7.3 Combined conditions operation

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

	_UY #2											
名称	别名	定时间隔	时间单位	动作	开始(年)	开始(月)	开始(日)	开始(时) 	开始(分)	启用		~
123	元	1	万钟	TREG-123.天团	π	元	π	π	π			¥
			添加									
									保存并	f应用 •	保存复位	
												_
				Powered by King	Pigeon Tech	nology Co., I	.td. (v1.31.1)	/ 2022-05-06	i .			



3 REG20001 水ツ 1.53 * 0.5354 REG40000 23.978899 単紙目 単版目 A REG20001 * REG20022 * REG2003 REG2004 1.2 単成目 単版目 REG2001 * REG2002 * REG2003 REG2004 1.2 単成目 単版目 REG2007 * REG2003 REG2004 1.2 単成目 単版目 REG2003 REG2004 1.2 単成目 単成目 REG2007 REG2003 REG2004 1.2 単成目 単成目 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007 REG2007	G REG2001 x*y 1.53 * 0.5354 REG4000 23.978999 ●新聞 勝節 A REG2001 * REG2002 * REG2003 REG2004 12 SS留 勝節 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● </th
本 E622001 ・ RE622002 ・ RE622003 RE622004 12 ● 回答 ● 回答	A REG20001 + REG20002 + REG20003 REG20004 12 単編集 通知 <t< th=""></t<>
Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06 大佐菜 法件运算 小古菜草 DORDL Lebble用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 漆 条件(点) 輸入1 运算 輸入2 运算 輸入3 輸出蜡烛 輸出值 下EE-123 0 60 + REG40002 2877.443848 受援書 暖録 液田	Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06 米広節 梁桃志算 #竹云算 2002以上比地出开于保存中间计算结果、可通过MOTT发布、或通过Modbus读和 2012以上地出开于保存中间计算结果、可通过MOTT发布、或通过Modbus读和 2013 G 60 + REG40002 2877.443848 愛媛麗 麗樂 2014 TREG-123 G 60 + REG40002 2877.443848 愛媛麗 麗樂 正面
中wered by KingPigeon Technology Co., Ltd. (v1.31.1)/2022-05-06 本正篇 登報运算 条件运算 (什运算) 作运算 POWERD BL/L地址用于保存中間计算结果,可通过MOTT发布,或通过Modbusig和 按 条件(再) 输入1 运转 输入2 运转 输入3 输出地址 输出值 TREG-123 G * 60 + REG40002 REG40002 2877.443848 正 原用 Powered by KingPigeon Technology Co., Ltd. (v1.31.1)/2022-05-06	本运算 医输运算 条件运算 :什运算 :什运算 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06 :并运算 /竹运算 100及以上地址用于保存中間计算结果,可通过MOTT发布,或通过Modbus读取 :非 条件(真) 输入1 运算 输入2 运算 输入3 输出通趾 输出通 TREG-123 G * 60 + REG40002 REG40002 2877.443848 : (原行并放用 • 原子 集位) : (原行 并放用 • 原子 集位) : (原行 集位) : (原行 集位)
大変質 変報定算 条件运算 学行左算	大区間 安排运算 大区間 会件运算 けた算算 100及以上地址用于保存中间计算绘果、可通过MOTT发布、或通过Modbus读取 111 協力1 运算 输入2 运算 输入3 输出地址 输出值 111 TREG-123 6 * 60 * REG40002 2877.443848 編編 翻編 111 原加 <t< th=""></t<>
大区第 変報送算 条件送算 子 子 子 子 子 子 子 子 子	**22篇 26個22篇 条件違算
大弦笛 変幅広算 大弦笛 変幅広算 (竹运算) 2002以上地址用于保存中間计算结果、可通过MOTT发布、或通过Modbus读取 液 条件(角) 输入1 运算 输入2 运算 输入3 输出地址 输出值 下 EG-123 6 60 + REG40002 2877.443848	大弦算 条件遊算 注け运算 200及以上地址用于保存中時計算結果,可邀过MOTT发布,或邀述Modbus读取 技作 条件(真) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出値 TREG-123 G * 60 + REG40002 REG40002 2877.443848 等端 郵除 添加 </th
大弦篇 変確広算 大体広算 大体広算 内辺以上地地用于保存中間计算結果、可通过MOTT发布、或通过Modbusig取 液体 条件(海) 输入1 运算 输入2 运算 输入3 输出地址 输出值 TREG-123 G * 60 + REG40002 2877.443848 業編 郵除 液加 液加 原用 原産 便症 液加 「保存并应用 保存 反使 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	大区算 条件运算 注け运算 200以上地址用于保存中間计算结果、可重过MOTT发布、或通过Modbus读取 液<
水広算 愛媛広算 条件运算 件运算 <th< th=""></th<>	大弦算 愛姆弦算 会件运算 件运算
* 注	本法算 愛羅法算 条件波算
* 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法	*法算 愛職运算 条件运算 注 什运算 200及以上地址用于保存中间计算結果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算結果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算結果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算結果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算結果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 200及以上地址目示和LTL表示、LTL表示、LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL表示和LTL
大広葉 変雑运算 (竹石算) 少 ジャンク <	水道 変細波算 条件返算 件运算 <
**注意 愛媛遊賞 全体遊算 **件运算 P的及以上地地用于保存中间计算结果,可通过MOTT发布, 或通过Modbusi接取 · 「	*米运算 登録运算 条件运算 #は午运算 MODQULL地地比用于保存中间计算结果、可通过MOTT发布、或通过Modbus读取 #本 条件(角) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 TREG-123 G * 60 + REG40002 2877.443848 余編 膨除 下ででのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでので
木英麗 変編送算 条件运算 CHICE算 POURULHUBUH用于保存中间计算结果,可通过MOTT发布,或通过Modbus读取 TREG-123 G * 60 + REG40002 2877.443848 %解 删除 派加 「派加 「原存井应用 • 保存 <u>象</u> 位	*法算 登報送算 条件送算 #仕运算 POD及以上地址用于保存中的计算结果、可通过MOTT发布、或通过Modbus读取 都 条件(角) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 TREG-123 G * 60 + REG40002 2877.443848 下 下 下 下 下 「 依 府 研 加
大弦算 愛報送算 会件运算 (井运算) D02以上地址用于保存中间计算结果、可通过MQTT发布、或通过Modbusi获取 液 条件(角) 输入1 运算 输入2 运算 输入3 输出地址 输出值 水 条件(角) 輸入1 运算 输入2 运算 输入3 输出地址 输出值 水 6 + REG40002 2877.443848 郵編 郵除 液加	水道算 登備运算 CH立算 Photopic Photopic With UPT 保存中前计算结果、可通过MOTT发布、或通过Modbusig和 液体(丸) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 TREG-123 G * 60 + REG40002 2877.443848 %編 添加
秋田菜 条件/算 条件/算 線入1 运算 線入2 运算 输入3 輸出地址 輸出值 水田 小 6 + REG40002 2877.443848 編輯 郵酬 水田 60 + REG40002 2877.443848 編輯 郵酬 水田	学校运算 条件运算 作は写算 Provide a contraction of a con
大広算 28第运算 24注算 (井运算) 2010 1 25第 100 2011 1 25第 100 100 2012 1 100 100 100 100 2013 1 100 100 100 100 100 2014 1 100 100 100 100 100 100 2015 1 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 <th>米运算 愛知送算 愛生送算 (件运算) 100及以上地址用于保存中间计算结果,可通过MOTT发布,或通过Modbus读取 17REG-123 G * 60 + REG40002 2877.443848 ※留 删除 添加 アevered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06</th>	米运算 愛知送算 愛生送算 (件运算) 100及以上地址用于保存中间计算结果,可通过MOTT发布,或通过Modbus读取 17REG-123 G * 60 + REG40002 2877.443848 ※留 删除 添加 アevered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06
件运算 200及以上地地用于保存中间计算结果,可通过MOTT发布,或通过Modbusig取 液 条件(角) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 TREG-123 G * 60 * REG40002 2877.443848 実績 削除 添加	竹运算 読述MODTU 送布、或通过Modbusignt 部 条件(角) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 TREG-123 G * 60 * REG40002 2877.443848
「井丘昇戸 00及以上地址用于保存中间计算结果,可通过MQTT发布,或通过Modbus读取 液水 条件(角) 输入1 运算 输入2 运算 输入3 输出地址 输出值 TREG-123 G * 60 + REG40002 2877.443848 添加	竹込算 100及以上地址用于保存中间计算结果,可通过MQTT发布,或通过Modbus读取 370 条件(角) 输入1 运算 输入2 运算 输入3 输出地址 输出值 TREG-123 G * 60 + REG40002 2877.443848 编辑 删除 添加
00及以上地址用于保存中间计算结果,可通过MOTT按布, 配通过Motbus读取 #称 条件(直) 输入1 运算 输入2 运算 输入3 输出地址 输出值 TREG-123 G * 60 + REG40002 2877.443848 编辑 删除 添加 Fowered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	100及以上地址用于保存中间计算结果,可通过MQTT发布,或通过Modbus读取
(株 条件(真) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 市休 条件(真) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 TREG-123 G * 60 * REG40002 2877.443848	森 条件(真) 輸入1 运算 輸入2 运算 輸入3 輸出地址 輸出值 市田G-123 G * 60 + REG40002 REG40002 2877.443848 編編 編編 編編 添加 添加 <td< th=""></td<>
TREG-123 G * 60 + REG40002 2877.443848 編輯 翻錄 添加 添加 <	TREG-123 G * 60 * REG40002 2877.443848 編編 删除 添加 添加
様存并应用 ・ 保存 复位 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	添加
保存并应用 · 保存 复位 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	保存并应用 • 保存 复位 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06
保存并应用 • 保存 复位 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	保存并应用 • 保存 复位 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06
保存升业中 で 保存 复立 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	RF开設が用 ・ RF开 E位 Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06
Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06
Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06
Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06	Powered by KingPigeon Technology Co., Ltd. (v1.31.1) / 2022-05-06
Powered by KingPigeon recimology Co., Ed. (V1.51.1)72022-05-00	Powered by Kingrigeon rechnology Co., Ltd. (V1.31.1)/ 2022-03-00.

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

巴歇尔槽自由流流量公	式: Q = CH ⁿ
巴歇尔槽规格: 5	(1~25号)
水位高度: 0.1	(0~2.13m)
2 5#円歇尔捕参数:	始转换
☐ 开: ☐ 5#巴歇尔槽参数: 自由流流量公式:	始转换 Q = 0.5354 * H ^{1.53}
✓ 5#巴歇尔槽参数: 自由流流量公式: 喉道宽(b值);	始转换 Q = 0.5354 * H ^{1.53} 228 mm
✓ 5#巴歇尔槽参数: 自由流流量公式: 喉道宽(b值): 流量范围:	始转换 Q = 0.5354 * H ^{1.53} 228 mm <mark>9~903.6</mark> m ³ /h





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.

Golden Pigeon Cloud V2	modbus.dtuip.com	6651	MODBUS RTU	Edit delete
Golden Pigeon Cloud V2	mqtt.dtuip.com	1883	MQTT	Edit delete
Golden Pigeon Cloud V2	mbtcp.dtuip.com	6655	MODBUS TCP	Edit delete
thingsboard	thingsboard.cloud	<mark>1</mark> 883	MQTT	Edit
Add to				
Save and apply sav	reset			
Deward by KingDigson Tasha	alami Ca. 144 (ut 20.0) (2024.07.2	2		

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



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



5.8.1.1 KingPigeon Cloud Platform (KPIIOT)

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

Cloud connection sett	ngs	on owned of the state of the st
cloud platform	Golden Pigeon Cloud V2 🗸	
link agreement	MODBUS RTU 🗸	
Native Modbus Device ID	2 The native Modbus device ID is set in the serial port settings	
registration package	BR8SH70 C	
heartbeat packet		
Heartbeat response packet		
Heartbeat period (seconds)	60	
Host silent time (seconds)	600	
return to overview sa	reset	

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

R10A					
condition - system - The	internet ≁ VPN ≁ Remote I/O ≁	Events and Alerts -	Operations and Control 🕶	cloud platform -	quit
Cloud connection sett	ngs			UNSAVED COM	FIGURATIONS : 2
cloud platform	Golden Pigeon Cloud V2				
link agreement	MODBUS TCP 👻				
Native Modbus Device ID	2 ② The native Modbus device ID is set	et in the serial port setti	ngs		
registration package	BR8SH70GQ C				
heartbeat packet					
Heartbeat response packet					
Heartbeat period (seconds)	60				
Host silent time (seconds)	600				
return to overview sav	ereset				
	Powered by KingPigeon	Technology Co., Ltd. (v	1.30.2) / 2022-02-21		

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



Cloud connection sett	ings				
cloud platform	Golden Pigeon Cloud V2	~			
link agreement	MQTT	~			
MQTT client ID					
Release cycle (seconds)					
Enable data upload					
return to overview sa	ve reset				
	Powered by Kin	gPigeon Te	chnology Co., Ltd. (v1.3	0.2) / 2022-02-21	

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

Cloud connection sett	igs	TIGORAT
cloud platform	Golden Pigeon Cloud V3	
link agreement	MODBUS RTU 🗸	
Native Modbus Device ID	2 () The native Modbus device ID is set in the serial port settings	
registration package	BR8SF	
heartbeat packet		
Heartbeat response packet		
Heartbeat period (seconds)	60	
Host silent time (seconds)	600	
return to overview sav	reset	

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



	ngs		and the second se
cloud platform	Other cloud platforms		
Cloud platform name			
Host IP or domain name	n		
port			
link agreement	MODBUS RTU ~		
Native Modbus Device ID	2 2 Image: The native Modbus device ID is a second seco	et in the serial port settings	
registration package	BR8SI		
heartbeat packet			
Heartbeat response packet			
Heartbeat period (seconds)	60		
	600		

R40B state - system -	service - The internet -	VPN - applicati	on - RTU I/O -	logic operation -	cloud platform -	quit
Cloud connection	seffings				UNSAVED CO	NFIGURATION : 2
Cloud connection setti	nas					
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 forma	"使用"S目用本机或MODBUS缺射表存髓地址" {	ŕ
	"主题1"{ "雇性1":{ "敬媚1"."\$DO1".	
	"数据2":"\$REG20128" }, "零性::?" /	
	"数据1*."\$DI1", "数据2*."\$GPS"	
	, }, "主题2":{	
	"犀性1""。 "数据1"."\$COUNT1"。 "数据2"."\$RE620256"	
), "犀性之";{ "翠姑是4~~~5 A14"	
	*数据2":"\$TIME"	h

5.8.2 Alibaba Cloud platform

Alibaba Cloud Setting	S	UNSAVED CONFIGURATIONS : 2
Enable settings		
verification method	device key 🗸	
ProductKey		
Device Name (DeviceName)		
Device Secret (DeviceSerect)		
Region (Region ID)	East China 2 •	
Release cycle (seconds)		
Post only changed data		

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



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

Ali cloud device creation certificate creation and details reference <u>Ali Cloud help documentation</u> <u>guide</u>

5.8.3 AWS Cloud

R10A		
condition - system - The	internet + VPN + Remote I/O + Events and Alerts + Operations and Control + cloud platform + quit	
Amazon Cloud Setup	UNSAVED CONFIGURATIONS : 2	1
Enable settings		
host (endpoint)		
Client ID		
Item Name		
Authentication and Authorization (Root Certificate)	Select the file	
	i /etc/mqtt/root.crt	
Device certificate	Select the file	
	@ /etc/mqtt/local.crt	
Device private key	Select the file	
	Ø /etc/mqtt/private.key	
publish data format	Default data format	
Post topic		
Release cycle (seconds)		
Post only changed data		
save and apply save	reset	

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



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

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

5.8.4 Huawei cloud

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

	ngs			UNSAVED CON	FIGURATIONS : 2
Enable settings					
verification method	device key 🗸				
Device ID					
key		*			
Service ID					
Region (Region ID)	North China - Beijing IV 🗸 🗸				
Release cycle (seconds)					
Post only changed data					
save and apply save	reset				
	Powered by KingPigeor	n Technology Co., Ltd. (v1.30	0.2) / 2022-02-21		

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



	R40A Offlir	le			
	Node ID	R40A			
	Device ID	5ee965a0496bac073bb6120d_R40A 🗍			
	Registered	Jun 17, 2020 08:37:57 GMT+08:00			
	Node Type	Directly connected			
	Software Version	v1.0			
	The product needs	to create a service to report data.			
	Model Definition C	Online Debugging Topic Management			
Service ID	Add Service ID Add Service Import Library Model Import Local Profile In	Library Model Import Local Profile Import from Excel			
	✓ Service ID: R40 司	Service ID: R40			
Region ID	The location of the platform	device can be queried on the HUAWEI CLOUD			
Publish Period (s)	Above 60s				
	For the password e	entered when creating the device certificate,			
Secret key	you can refer to the	e HUAWEI CLOUD help document to create a			
	test certificate				
Certification	Root certificate prov	vided by Huawei:rootcert.pem, It's included in the			
authority (root	release version, generation	ally don't need to upload			
	Device certificate de	wiceCert nem Unload to the /etc/conf directory			
Device certificate	and select the file	you can refer to the HUAWEL CLOUD help			
	document to create	a test certificate			
	Device kev/deviceCer	t.key,Upload to the /etc/conf directory and			
Device kev	select the file. vo	u can refer to the HUAWEI CLOUD help			
, ,	document to create	a test certificate			

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



5.8.5 Thingsboard cloud platform

R10A					
condition - system - The	e internet - VPN - Reme	ote I/O - Events and Alerts -	Operations and Control -	cloud platform -	quit
Cloud connection set	ings			UNSAVED CO	NFIGURATIONS: 2
Enable settings					
MQTT client ID					
usemame					
password		*			
Release cycle (seconds)					
Enable data upload					
Post only changed data					
save and apply save	reset				
	Powered by Ki	ngPigeon Technology Co., Ltd. (v	1.30.2) / 2022-02-21		

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

For thingsboard cloud device user manual, please refer to the

Thingsboard Getting Started document



5.9 Logout

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

6. Communication Protocol

The device supports Modbus RTU protocol, Modbus TCP protocol and MQTT protocol. For specific communication protocol, please refer to relevant materials. The following introduces the application of Modbus RTU and MQTT protocol on the device.

Modbus TCP and RTU protocol are very similar, as long as an MBAP header is added to the RTU protocol, and the two byte CRC check code of the RTU protocol can be removed.

6.1 Modbus RTU Protocol

6.1.1 Platform connection setting

cloud platform	Golden Pigeon Cloud V2	~		
Link Agreement	MODBUS RTU	~		
Native Modbus device ID	1 The local Modbus device	ID is set in the serial po	rt settings	
Registration package	168Y2M4U6K95H5L0			
Heartbeat package				
Heartbeat response packet				
Heartbeat cycle (seconds)	60			
Host slient time (seconds)	600			
Return to overview	reset			

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^{2}

2. Set relevant message information according to the platform to be connected (if not, you can not set it)



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

[Heartbeat Response Packet]: The server responds to the heartbeat packet

[Heartbeat period]: The heartbeat packet sending period.

[Host Silent Time]: Silent time when no data is sent from server, timeout will reconnect.

6.1.2 Read Mapping Address

6.1.2.1 Mapping Register Address

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

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

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

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



20003	420004 or	16 Bit data	Same as	Same as above
	320004	20003	above	
	127 data		Same as	
	similar as		Same as	Same as above
	above		above	
20127	420128 or	16 Bit data	Same as	Samo as abovo
20127	320128	20127	above	Same as above

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

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

6.1.2.2 Read Boolean Mapping Address Data

Master Send Data Format:

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

Receiver Return Data Format:

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



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

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

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

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

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

01= Device ID; 01 = Read holding coil; 02= Return Data byte; 73 01= Return 10 Boolean status. High byte stands for low address data, low address stands for high address.

According to Modbus protocol, fix 73 01H real value to be 01 73H, converter to Binary as below:

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

The address value higher than 10 digits will be seen as invalid. 5D OC CRC Verify.

6.1.2.3 Modify Boolean Mapping Address Data

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

Master Send Data Format:

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



Receiver Return Data Format:

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

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

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

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

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

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

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

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

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

6.1.2.4 Read Data Type Mapping Address Data

Master Send Data Format:

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

(H: HEX)



Device Address	1	01H	01H Device, according to the data Master send	
Function Code	1	03H	Read holding register	
Range Data Bytes	1	14H		
Returning Data	20	00 14 00 1E 00		
		28 00 32 00 4B	Poturning Data	
		00 41 00 0A 00		
		25 00 14 00 2AH		
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	20010	20000	20008	20007	20006	20005	20004	20002	20002	20001
Address	20010	20009	20008	20007	20000	20005	20004	20005	20002	20001
Value	00 2A	00 14	00 25	00 0A	00 41	00 4B	00 32	00 28	00 1E	00 14

FB 34=16 CRC Verify.

6.1.2.5 Modify Data Type Mapping Address Data

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

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

Master Send Data Format:

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	2		Manning data tuna	
Address		40 210		
Write Data	2	00 64H	Write 100 successfully	
16 CRC Verify	2	CF 03H	CRC0 CRC1 low byte in front, high behind	

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

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

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

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

01= Device address; 06= Modify single holding register value; 4E 20= R Modify address 20001 register value; 00 64= Modify to Decimal value 100, CE 03=16 CRC Verify. If need to modify multiple data type mapping address, pls check function code 16 in Modbus protocol.

6.2 MQTT Protocol

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

6.2.1 MQTT Introduction

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

6.2.2 MQTT Principle

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



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

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



(uploads data to Broker)



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

6.2.3 Device Communication Application

Client configuration

1. Connect Platform: KPIIOT cloud platform 2.0 or other cloud platform to enter the corresponding IP and port.

2. Connection protocol: MQTT protocol.

3. MQTT client ID: the unique identification of the device, which can be a serial number, device ID, or IMEI code; (King Pigeon 2.0 device ID defaults is the serial number).

4. MQTT account: the account where the device publishes the theme on the proxy server (King Pigeon 2.0 defaults is MQTT).

5. MQTT password: the device's account password for publishing the theme on the proxy server (King Pigeon 2.0 defaults is MQTTPW).

6. Publish topic: refers to the topic of the device publishing uplink data to the platform, King Pigeon Cloud 2.0 is the cloud service ID / +.

7. Subscription topic: refers to the topic that the device subscribes to when receiving downlink data, King Pigeon Cloud 2.0 is the cloud platform serial number/+.

8.Release cycle (seconds): MQTT data release interval, in seconds. The King Pigeon Cloud 2.0 cycle needs to be set to 10 seconds or more. If it is less than 10 seconds, the platform will disable the device.

Publisher QOS: The service quality level guarantee for application message distribution,
 0-at most once, 1-at least once, 2-only once, you can choose according to your needs.
 10. Encryption: You can use encryption to connect to the server according to your needs, and you can choose not to encrypt when you connect to King Pigeon Cloud 2.0. non-encrypted
 11. Enable data re-transmission: Check enable, after enabling, when reconnecting to the



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

After the configuration is complete, the client will initiate a connection to the server: **CONNECT:** The client sends a CONNECT connection message request to the server; CONNACK: The server responds with a CONNACK confirmation connection message, indicating that the connection is successful; After the client establishes a connection, it is a long connection, and the client can publish or subscribe to the message on the server; For example the device and the client's mobile phone as the client:

After the device publishes the topic on the proxy server, customers can view the data through subscription. That is, the device is the publisher and the customer's mobile phone is the subscriber.

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

Publish MQTT Format 6.2.4

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

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

```
Publish Topic Name: serial numbers // Corresponding configured topic options
"sensorDatas":
  ſ
      {
      // 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"
    }
1,
"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:

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	DI3~DI22	Switcher	0 is offline,1 is online
failure			
Pulse count	COUNT1,COUNT2	Value	

Device own I/O Port



Extend I/O Port

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

Note:

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

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

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

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

Publish Topic	serial numbers
{	
"sw	/itcher": "0",
"fla	g": "DI1",
"tir	ne": "1602324850"
}	

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

6.2.5 Device Subscribe MQTT Format

The payload data format in the device subscription message

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

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

Note:

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



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

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

- 1. The switch character is " switcher " followed by: "0"or "1",0 is open,1 is close.
- 2. The numeric character is " value " followed by: "data value"
- //Read write flag: the character is "flag" followed by "flag"
- // "down" confirmation data sent to subscribers by the platform.

7. SMS Command List

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

1. The default password is 1234, you can edit the SMS command to modify the password;

2. The "password" in the SMS command refers to the device password, such as 1234, just enter the password directly;

3. The "+" sign in the SMS command is not used as the content of the SMS, please do not add any spaces or other characters;

4. The SMS command must be CAPITAL LETTERS, such as "PWD" instead of "pwd";

5. If the password is correct but the command is incorrect, the device will return: SMS Format Error, Please check Caps Lock in Command! So please check the Command, or add the country code before the telephone number or check the input is in ENGLISH INPUT METHOD and CAPS LOCK. If password incorrect then will not any response SMS.

6. If the password is entered incorrectly, no information will be returned;

7. Once the Unit received the SMS Command, will return SMS to confirmation, if no SMS return, please check your command or resend again.

1) Modify Password, 4 digits, default is 1234

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

2) Inquiry Current Status SMS Command

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



8. Warranty

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

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