

Wireless Data Connectivity for Industrial applications

4G Wireless Industrial Router



Provide data wireless access internet acquisition control With AI/DI/DO, supports Modbus to TCP/MQTT/PLC protocol **4G Industrial VPN Router R40**



4G Wireless Router User Manual

Ver 1.1

Date Issued: 2020-09-30 King Pigeon Hi-Tech. Co., Ltd.

www.iot-solution.com



Table of contents

1. Descrip	otion	3
1. 1	Brief Introduction	3
1.2	Typically Applications	4
1.3	Safety Directions	9
1.4	Standard Packing List	10
1.5	Main Features	10
1.6	Technical Parameters	12
2. Hardw	are Description	
2.1	Size	16
2.2	Indicator light	16
2.3	Reset	17
2.4	SIM Card	17
2.5	Connect External Antenna	18
2.6	Router GND	18
2.7	Installation	19
3. Start u	ρ	
3.1	Switch on	
3.2	System running status	20
3.3	SIM Card Operation	20
3.4	Serial Port Instructions	21
3.5	Digital output Instructions	22
3.6	Digital input Instructions	23
3.7	Analog input Instructions	24
4. Prepar	ation before configuration	
4.1	Wired Connection	25
4.2	Wifi Connection	30
4.3.	Factory Default Settings	32
4.4.	Enter Web Settings	32
5. Router	Settings	
5.1	Status	33
5.2.	System	34

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

	5.3.	Service	37
	5.4	Network	41
	5.5	VPN	63
	5.6	Serial Port	68
	5.7	RTU IO	72
	5.8	Logical Operation	77
	5.9	Cloud Platform	77
	5.10	5	
6.	Comr	nunication Protocol	80
	6.1	Modbus RTU Protocol	81
	6.2	MQTT Protocol	91
7.		Command List	
8.	Warr	anty	97

UPGRADE HISTORY

DATE	FIRMWARE VERSION	HARDWARE VERSION	DESCRIPTION
2020.03.13	V 1.0	V 1.0	First edition
2020.11.13	V1.181	V1.1	Modify some configuration instructions

Model List

Model	Serial Port	WAN	LAN	WIFI	Digital input	Digital output	Analog input	Extend function	POE	GPS
R40	1RS485,1RS232	1	3	\checkmark	2	2	х	Modbus	Optional	Optional
								slave/MQTT		
R40A	1RS485,1RS232	1	3	\checkmark	2	2	х	Modbus	Optional	Optional
								master		
								/slave/MQTT		
R40B	1RS485,1RS232	1	3	\checkmark	2	2	4	Modbus	Optional	Optional
								master		
								/slave/MQTT		

1. Description

1.1 Brief Introduction

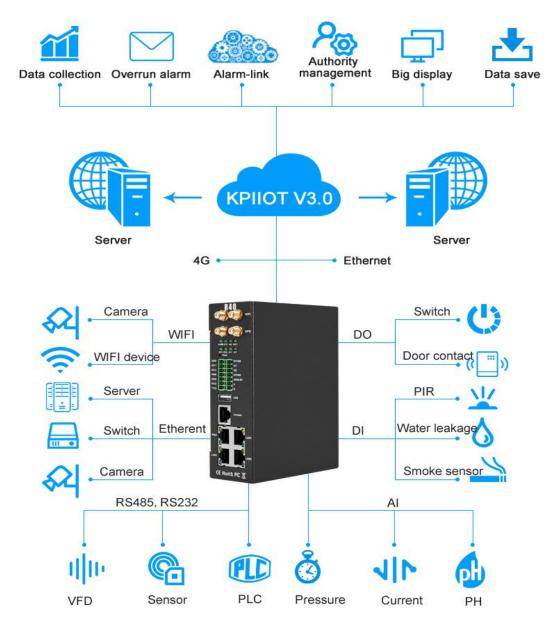
Industrial Router R40 is an industrial IoT high-speed router, compatible with 4G/3.5G/3G/2.5G network, flagship configuration, VPN link, industrial protection, wide temperature, wide voltage design, easy to set up high speed, stable The wireless transmission network uses the public LTE network to provide users with wireless long-distance data transmission, It is with 4 AI+2DI+2DO for options, can be used in multiple industrial applications.

It is an industrial-grade multifunctional Internet of Things terminal device that supports POE power supply,

4G Wireless Industrial Router Wireless Data Connectivity

comes with IO input and output, with 2 serial ports, supports transparent transmission, Modbus Master protocol for expanding IO and connecting PLC and other devices. It adopts dual SIM card redundancy design to ensure stable and reliable data transmission, supports MQTT protocol and Modbus protocol, and is compatible with most PLC protocols, greatly simplifying on-site wiring construction costs and reducing operation and maintenance costs.

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



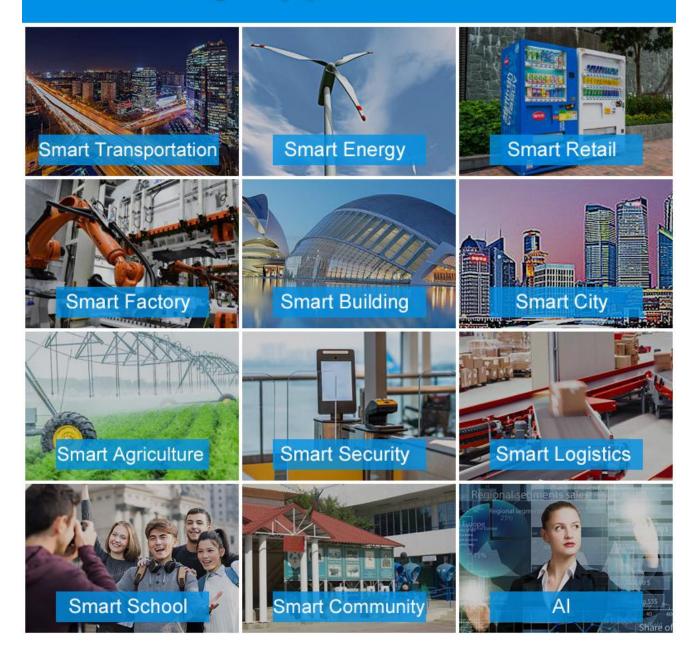
1.2 Typically Applications

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



Industry Application

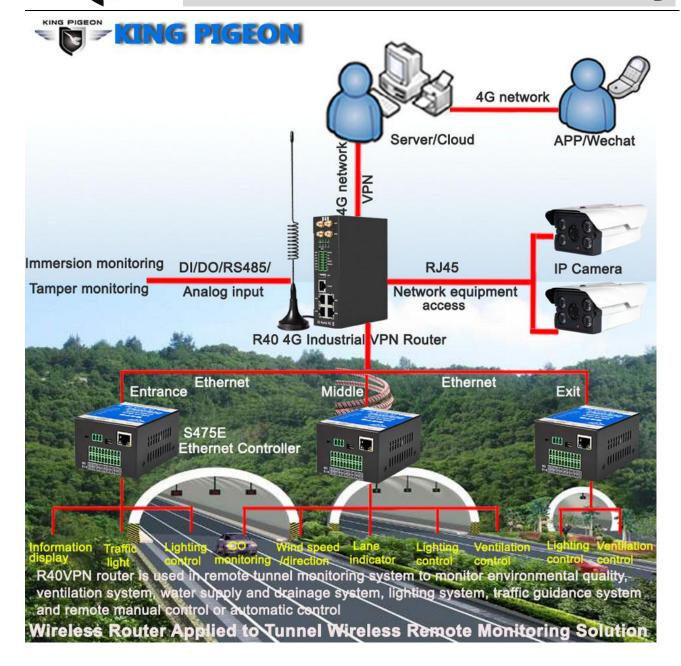
APPLICATION INDUSTRY



1.2.1 Tunnel wireless remote monitoring solution

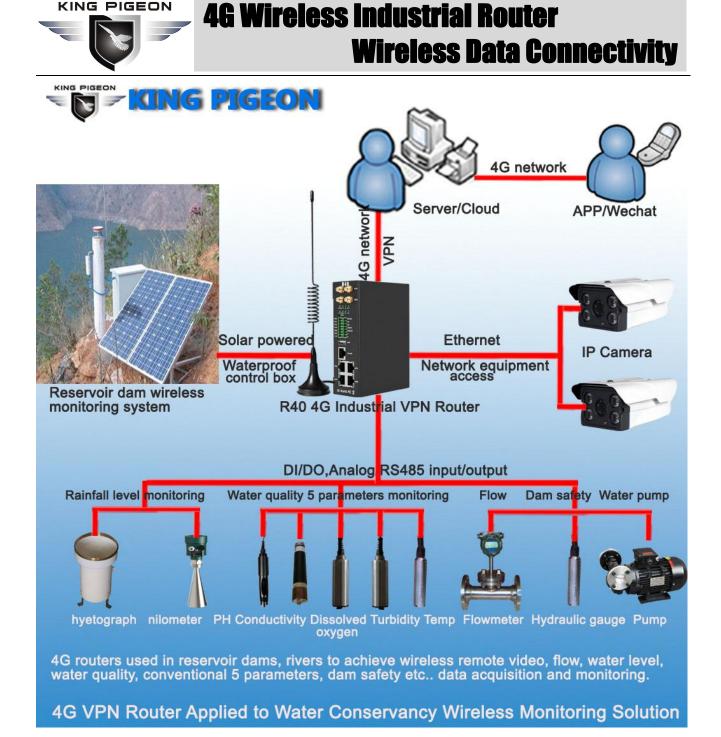
R40 4G industrial VPN wireless router is used in tunnel remote monitoring system to monitor environmental quality, ventilation system, water supply and drainage fire protection system, lighting system, traffic guidance system monitoring and remote manual control or automatic control.





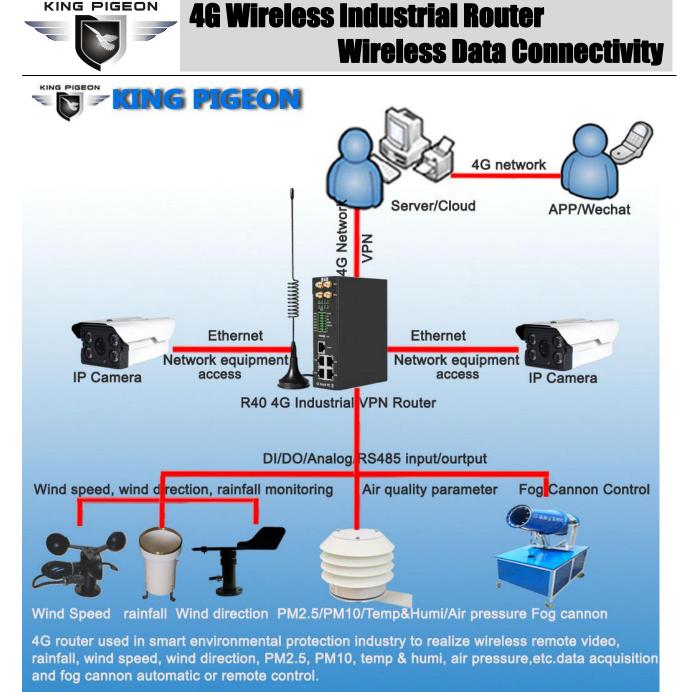
1.2.2 Water Conservancy Wireless Monitoring Solution

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



1.2.3 Smart Environmental Protection Wireless Monitoring Solution

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

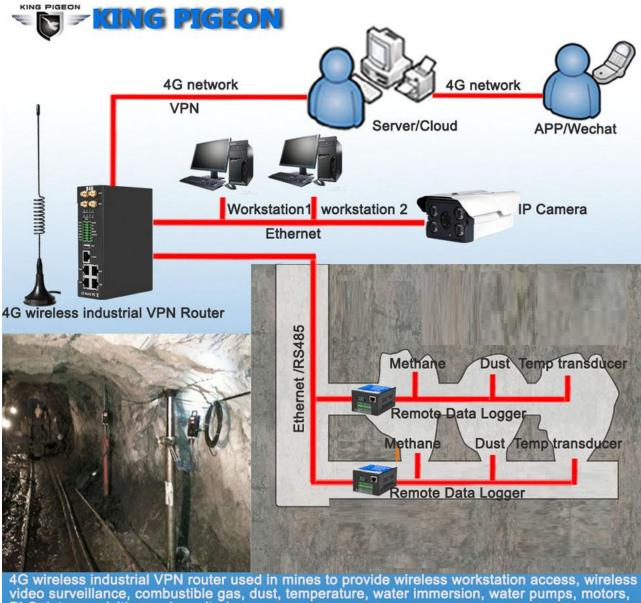


4G Router for Smart Environmental Protection Wireless Monitoring Solution



Mine Wireless Networking & Monitoring System Solution 1.2.4

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



4G wireless industrial VPN router used in mines to provide wireless workstation access, wireless video surveillance, combustible gas, dust, temperature, water immersion, water pumps, motors, PLC data acquisition and monitoring. R40 4G Router for Mine Wireless Networking & Monitoring System Solution

1.3 Safety Directions



Safe Start up

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

Interference

All wireless equipment might interfere network signals of the unit and influence its performance.



1.4 Standard Packing List

Router R40 X1, Power adaptor*1, GSM/3G/4G Antenna X1, 2.4G WIFI Antenna X3, User Manual X1 (QR code card), Wall-mounted snap kit x 2, 35mm Standard DIN rail fixed Bracket*1.



Note: The package does not include any SIM card.

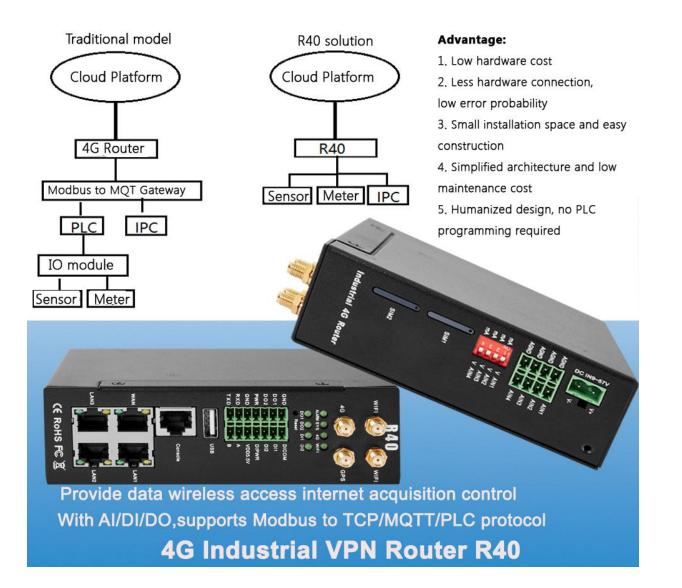
1.5 Main Features

- DIN(2 channel) :Support NO/NC/counting input, frequency<100, can set counting threshold, support alarm trigger.</p>
- > DO(2 channel): can be set according to the trigger condition.
- > AIN(4 channel): Support 0-5V, 0-20mA, 4-20mA, can set threshold value, support alarm trigger.
- Support SMS to query DI/DO/AI status and value, and set DO status;
- Support 4G wireless Internet access function, can set APN and other parameters;
- Two SIM card slots, support dual card switching;
- Support GPS, positioning data can be released through MQTT;
- > VPN: Support L2TP, IPSEC, OPENVPN and other VPN protocols.



- Interface: Support RS485 and RS232 serial port transparent transmission and MODBUS RTU to TCP, Support MODBUS master, can regularly read MODBUS slave node data through RS485, RS232 and Ethernet.
- Support address mapping, mapping RS485, RS232 and Ethernet access device addresses to router local addresses.
- Support monitoring the online status of network devices connected to the LAN port, which can be reported to the platform through Modbus or MQTT.
- Link switching: Support WAN port and 4G network connection switching, preferentially use WAN port wired network.
- > Platform connection: Support MODBUS and MQTT protocols, MQTT supports SSL encryption.
- > Alarm:Supports SMS and e-mail alarm.
- > Timer:Support one-time timer and period timer.
- Upgrade:Support remote upgrade through webpage







1.6 Technical Parameters

Item	Parameters	Description			
	Input voltage	9~57VDC			
Power	Input current	Normal:240mA@12V,max:800mA@12V			
Supply	Connection	5.08mm terminals			
	Protection	Anti-reverse connection Protection			
	Qty	1			
	Interface Spec	RJ45,10/100Mbps,Automatically adapted to MDI/MDIX			
WAN		ESD \pm 30kV (contact) , \pm 30kV (air)			
	Protection	EFT 40A (5/50ns)			
		Lightning strike 24A (8/20µs)			
	Qty	3			
	Interface Spec	RJ45,10/100Mbps,Automatically adapted to MDI/MDIX			
		Supports 3 POE power output			
		compatible IEEE802.3at/af			
LAN (POE)	POE(optional)	Single POE maximum output power 30W			
		With power management function			
		Voltage range 48 \sim 57V			
		ESD \pm 30kV (contact) , \pm 30kV (air)			
	Protection	EFT 40A (5/50ns)			
		Lightning strike 24A (8/20µs)			
	Qty	2			
	Туре	1 RS485,1 RS232			
	Baudrate	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600,			
	Baudrale	115200, 230400			
	Data Bit	5, 6, 7, 8			
Serial Port	Parity	None, Even, Odd			
Senarron	Stop Bit	1,2			
	Working mode Protection	Data transparent transmit, Modbus RTU to TCP, Modbus			
		master,Modbus slave			
		ESD (contact) : 8KV Surge: 4KV (8/20us)			
		ESD $\pm 8 \text{kV}~(\text{contact})$, $\pm 15 \text{kV}~(\text{air})$			
		EFT 4KV, 40A (5/50ns)			
	Qty	1			
Console	Туре	CONSOLE			
CONSOLE	Interface Spec	RJ45			
	Protection	ESD: $\pm 8 \text{kV}$ (contact) , $\pm 15 \text{kV}$ (air)			
USB	Qty	1			
(Reserved)	Туре	USB2.0 (HOST)			
	Protection	ESD $\pm 8kV$ (contact), $\pm 15kV$ (air)			
	Antenna qty	2			
	Antenna type	SMA			
WIFI	protocol	802.11a/b/g/n (mixed)			
	mode	AP mode,client mode			

	Frequency	2.4G
	Channel	Channel 1 - 13
	Security	Open,WPA,WPA2
	Encryption	AES,TKIP,TKIPAES
	Connection number	16 (Max)
	Speed	300Mbps (Max)
	Transmit Distance	Outdoor non-blocking/opening, covering up to 20 meters
	SSID	
	Broadcast Switch	support
	Antenna Port Qty	1
	Antenna Port Type	SMA
		GSM/EDGE: 900,1800MHz
		WCDMA: B1,B5,B8
	4G (L-E)	FDD: B1,B3,B5,B7,B8,B20
		TDD: B38,B40,B41
		GSM/EDGE: 850,900,1800MHz
		WCDMA: B1,B2,B5,B8
	4G (L- AU)	FDD: B1,B2,B3,B4,B5,B7,B8,B28
		TDD: B40
Cellular		WCDMA: B2,B4,B5
Network	4G (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	2
SIM	Interface Spec	Drawer interface, supports 1.8V/3V SIM/UIM 卡(NANO)
	Protection	In-built 15KV ESD Protection
	Antenna qty	1
	Antenna type	SMA
GPS	Tracking Sensitivity	> -148 dBm
(optional)	Horizontal Accuracy	2.5m
	Protocol	NMEA-0183 V2.3
	Qty	2
	Туре	Switch contact signal (dry node) or level signal (wet node)
		1:High level, 5~30VDC, close signal ;0:low level 0~1VDC open
Digital input	range	signal
	Pulse frequency	Max 100Hz
	Protection	Isolation voltage 3750Vrms
Digital	· · ·	Isolation voltage 3750Vrms 2

4G Wireless Industrial Router Wireless Data Connectivity

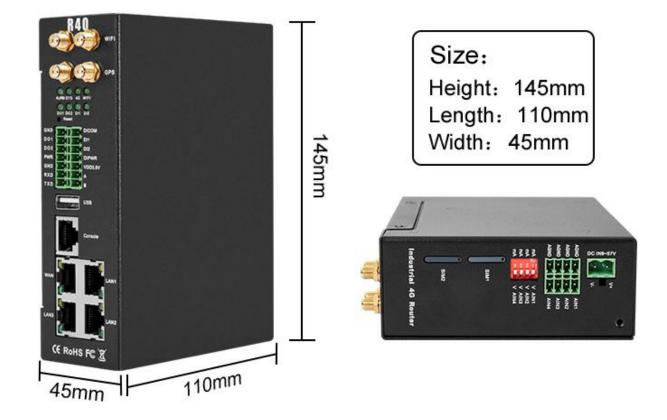
	Load voltage	Max 50VDC
	Load current	500mA (single), 625mW
	Protection	EFT: 40A (5/50ns)
	Qty	4
	Туре	0~5V, 4~20mA, 0~20mA
Analog input	ADCResolution	16bit
	Protection	EFT: 40A (5/50ns)
	ALARM	Alarm indicator light
	SYS	System running status indicator
Indicator	4G	4G status indicator
light	WiFi	WiFi status indicator
	DO1,DO2	Digital output indicator light
	DI1,DI2	Digital input indicator light
	CPU	MIPS CPU,Clock Speed 580Mhz
System	Storage	16MB (Scalable to 32MB)
	RAM	128MB (Scalable to 256MB)
		PPP, PPPoE, TCP, UDP,DHCP, ICMP,NAT,
	Network Portocol	HTTP, HTTPs,DNS, ARP, NTP,SMTP,SSH2,DDNS etc.
	VPN	lpsec,OpenVPN,L2TP
	Firewall	DMZ,DoS defense,IP packet, Domain name and MAC address
Software		filtering, port mapping, access control
	Remote Management	Support web remote configuration
	System Log	support
	Firmware Upgrade	Support serial port local TFTP/web firmware 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	EMS	IEC(EN)61000-4-5(Surge)
		IEC(EN)61000-4-6(CS)
		IEC(EN)61000-4-8
	Others	CE,FCC,ROHS,3C
	Working temperature	-40∼85℃
Working Enviorment	Storge temperature	-40∼105℃
Enviorment	Humidity	5~95%RH
	Enclosure	Metal
	Size	H145mm * L110mm * W45mm
Others	IP level	IP30
	Net weight	790g
	Installation	Wall-amount/ rail-amount

2. Hardware Description

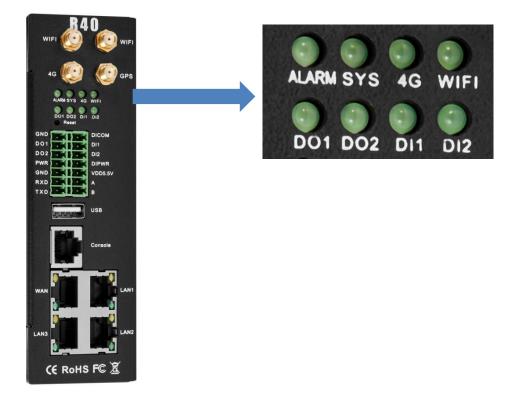




2.1 Size



2.2 Indicator light





LED Indicator light						
	Name	status	Description			
ALARM	Alarm indicator light	ON	DI or Al trigger alarm			
ALARIVI	Alarm indicator light	OFF	normal			
		flicks	normal			
SYS	System running status indicator	slowly	norma			
		OFF	abnormal			
			Signal normal			
4G	4G status indicator	fast	Signal normal			
		OFF	abnormal			
WIFI	WiFi status indicator	ON	WiFi normal			
VVIFI	WIFI status indicator	OFF	abnormal			
DO1	Digital output 1 indicator light	ON	DO1 close			
DOI	Digital output 1 indicator light	OFF	DO1 open			
DO2	Digital output 2 indicator light	ON	DO2 close			
	Digital output 2 indicator light	OFF	DO2 open			
DI1	Digital input 1 indicator light	ON	DI1 close			
	Digital input 1 indicator light	OFF	DI1 open			
DI2	Digital input 2 indicator light	ON	DI2 close			

2.3 Reset

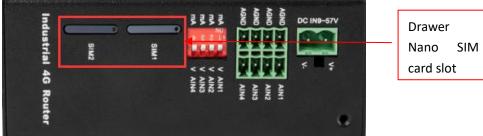
After the router runs normally, use a pointed stick to continue to hold down the Reset button for about 10 seconds until the WAN port indicator flashes slowly. At this time, restart the router to restore the factory default settings.



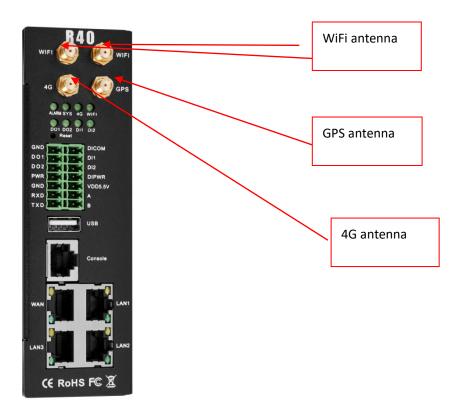
2.4 SIM Card

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



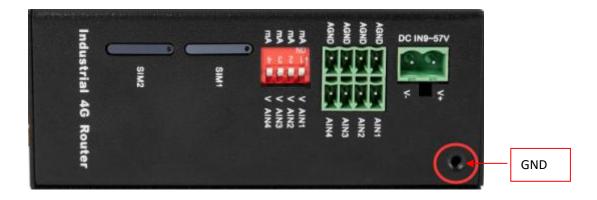


2.5 Connect External Antenna



2.6 Router GND

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

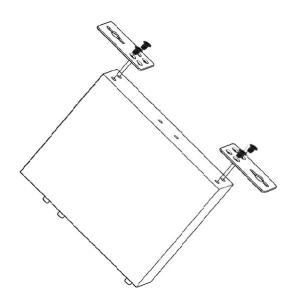




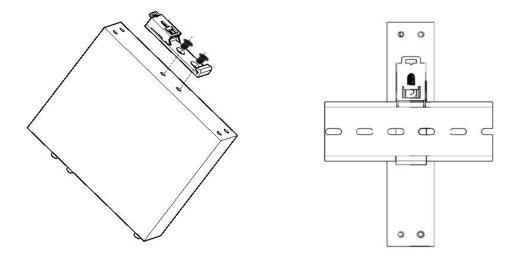
2.7 Installation

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

2.7.1 Wall-mounted installation



2.7.1 Rail mounting



3. Start up

3.1 Switch on

Power input port: R40 uses 9 ~ 57V DC voltage for power supply. If you need POE power supply



then power supply must meet 44V ~ 57V DC voltage power supply (recommend 48V / 2A).



3.2 System running status

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



3.3 **SIM Card Operation**

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



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

4G cellular network dial-up networking defaults to use SIM card 1, if you need to use SIM card 2, you need to enter the cellular network configuration interface, select card 2 in the column of selecting a phone card, save and apply to switch.

The dual card redundancy design of R40 can automatically switch to another SIM card for communication when the current SIM card network communication is abnormal (one minute).

For detailed configuration, please refer to 5.4.1.4.4G interface and 5.4.3 cellular network.

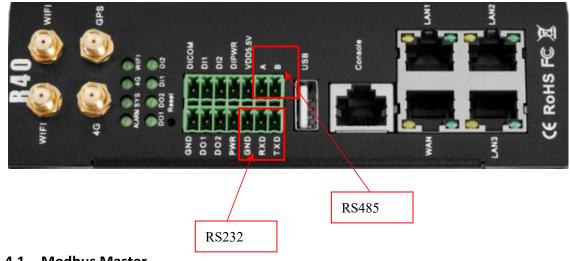


🖷 🖅 💽 R40B - 蜂窝网 - LuCI	× + ×		_		×
\leftarrow \rightarrow \heartsuit \textcircled{o} 19	22.168.3.1/cgi-bin/luci/admin/network/cell	□ ☆	\$≡ 1	2 6	
R40B 状态 - 系统 - 信号强度	服务 → 网络 → VPN → I/O → 接口 → 退出 				^
固件版本	EC25AUGCR06A02M1G				
IMSI	460007790314217				
IMEI	861585042306033				1
选择电话卡	 ‡1 ‡2				
四月13					
卡1 APN					
卡1用户名					
卡1密码					
启用GPS					
告警电话号码	+ 後收短信的移动电话号码				
短信语言	中文 (Chinese) ~				
	保	7并应用	保存	位	
Powered by KingPigeon Technol	ogy Co., Ltd. (v1.09) / 2020-05-13 01:40:25				~

3.4 Serial Port Instructions

The device has an RS485 and an RS232 communication interface, which can be used for Modbus master station (optional model to support), Modbus slave station, transparent transmission, Modbus RTU to TCP and other communications.

Note: Only one of the functions can be selected for the same serial port at the same time, and it cannot be reused. If it is found that the serial port cannot be selected on the configuration page, it means that the serial port has been set on the other function configuration page; different serial ports do not affect each other.



3.4.1 Modbus Master

Modbus master : Used as Modbus master, the serial port connected to Modbus slave equipment, through configuration Page 5.6.3. Modbus maste configures slave register and serial port parameters, the host collect slaves data through Modbus RTU protocol, and store the slave data in the local mapping register, can query the slave data directly on the configuration page, or you can 5.9. Cloud connection settings: Configure Modbus protocol or MQTT protocol to upload slave data to the server to realize Modbus RTU protocol to MQTT protocol.

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

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

3.4.2 Modbus Slave

Modbus slave function: When used as Modbus slave , the serial port will be connected to the Modbus master device. Configure the serial port parameters through the configuration page 5.6.2. Modbus slave, the master device will be able to collect the local I/O data through Modbus RTU or TCP protocol.

3.4.3 Transparent transmission

The device used as a data transfer station between the server and the slave device, through the configuration page 5.6.2. It transparently transmits the data uploaded from the slave to the server, and sends the data to the server Transparent transmission to the slave, without processing the data content, only forwarding data, to achieve data transparent transmission function.

3.4.4 Modbus RTU to TCP

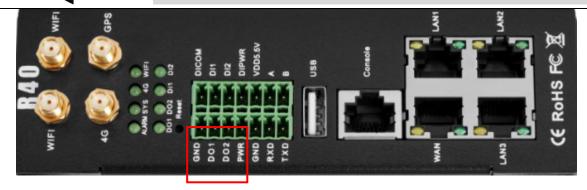
Master communicate with slave via Modbus RTU protocol, master communicate with slave via Modbus TCP protocol, through the configuration page 5.6.2.

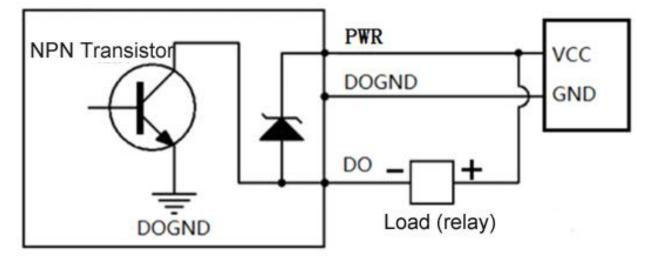
The device automatically converts Modbus TCP commands issued by the server into Modbus RTU commands and sends them to the slave, and then converts the Modbus RTU commands returned from the slave into Modbus TCP commands and replies to the server, so that the Modbus RTU slave device and the Modbus TCP server can be realized communication.

3.5 Digital output Instructions

3.5.1 Wiring







3.5.2 DO instruction:

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

1. DO1~DO2 are two-way NPN transistor open-collector output, and PWR is the clamp protection for the external power supply of the common terminal.

2. Digital output setting: Enter the router configuration interface-RTU I/O-digital input and output, and you can enable/disable or query and set the digital output status at the digital output port.

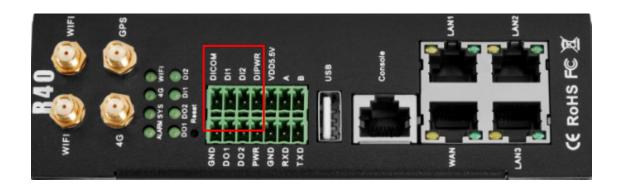
3. Trigger setting: According to the state of DI digital input or AIN analog input, you can set the trigger condition and control the DO digital output operation (the confirmation time is X seconds after the trigger condition is reached).

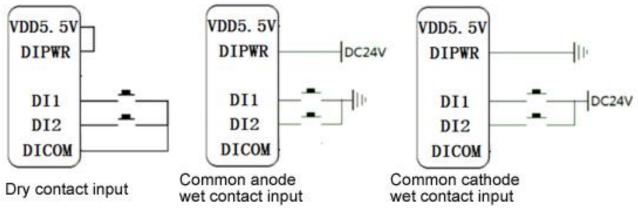
4. For detailed configuration, please refer to 5.7.2. Digital input and output.

3.6 Digital input Instructions



3.6.1 Wiring





3.6.2 DI instruction:

	qty	2
	type	Dry contact, wet contact
Digital input	Range	High level (digital 1) 5~30VDC, low level (digital 0) 0~1VDC
	Pulse frequency	<100Hz
	protection	Isolation voltage 3750Vrms

1. DI1~DI2 are two digital inputs. The default is wet contact input. Short-circuit VDD5.5V and DIPWR to switch to dry contact input.

2. Digital input setting: enter the router configuration interface-RTU I/O-digital input and output, and you can enable/disable or query the digital input status and pulse count value at the digital input port.

3. Trigger setting: The trigger condition can be set according to the DI digital input state to control DO digital output, restart and other operations (the confirmation time is X seconds after the trigger condition is reached).

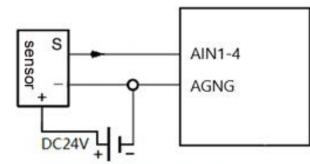
4. For detailed configuration, please refer to 5.7.2. Digital input and output.

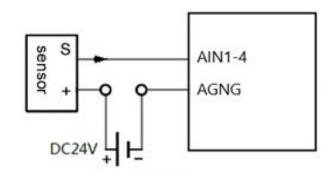
3.7 **Analog input Instructions**



3.7.1 Wiring







3 wire current/voltage sensor

2 wire current sensor

3.7.2 AI instruction:

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

1. Al-Al4 is a four-way analog input, the default is 0~5V voltage type analog input, you can switch to current type analog input by turning the dial switch to mA. The four-way dial switch Al1~Al4 is Four analog inputs correspond one to one, V corresponds to voltage type, and mA corresponds to current type.

2. Analog input setting: enter the router configuration interface-RTU I/O-analog input, in the mode you can select voltage 0~5V, current 4~20mA, current 0~20mA (note that the DIP switch should also be selected Corresponding mode), set the range in the minimum and maximum values, you can see the actual measured value in the current value.

Trigger settings: The trigger conditions can be set according to the AIN status to control DO digital output, restart and other operations (the confirmation time is X seconds after the trigger condition is reached).
 For detailed configuration, please refer to 5.7.3. Analog input

4. Preparation before configuration

The router supports web page configuration. There are two ways to connect the router. One is to connect the computer to any LAN port of the router through a wired connection; the other is to connect to the router through WIFI. The computer can automatically obtain IP through DHCP, or you can set a static IP on the same network segment as the router. After the connection is established, enter the router's default login address 192.168.3.1 on the computer browser to enter the router's WEB login interface. The default login The user name is admin and the password is blank.

4.1 Wired Connection

There are two ways to configure its IP address on PC, one is to enable automatic IP address acquisition on the

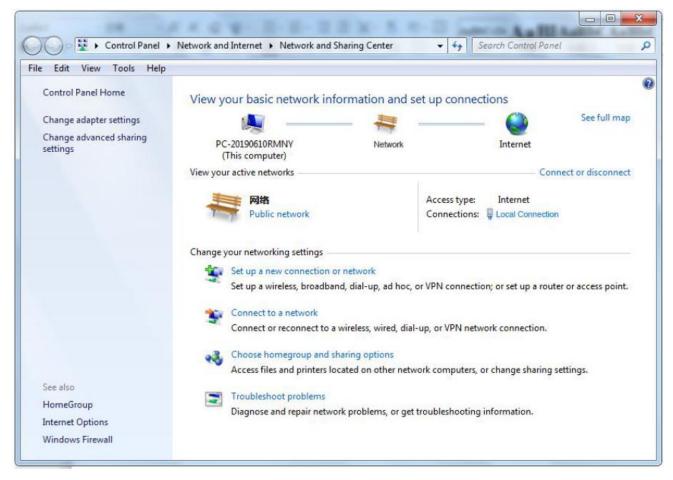
KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

local connection of the PC, and the other is to configure a static IP address on the same subnet as the router on the local connection of the PC.

Setting on Windows 7 as an example:

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



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



IPv4 Connect	ivity:	Internet
IPv6 Connect	ivity:	No Internet access
Media State:		Enabled
Duration:		07:35:18
Speed:		100.0 Mbps
Details		
Details	Sent —	Received
	0	
	Sent —	Received 833,590,410

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



	GbE Family Controller #2	
his connection uses	the following items:	Configure
Client for Mic	crosoft Networks	
Shrew Soft I		
QoS Packet	: Scheduler ter Sharing for Microsoft	t Networks
	ocol Version 6 (TCP/IP	
and the second se	ocol Version 4 (TCP/IP	
	opology Discovery Map	
	and the second	
	opology Discovery Res	ponder
	opology Discovery Res	Properties
🗹 🔺 Link-Layer T		
Link-Layer T Install Description Transmission Contr		Properties

4. Two ways to configure the IP address:

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



General	Alternate Configuration				
this cap	n get IP settings assigned au bability. Otherwise, you need appropriate IP settings.				
0	btain an IP address automati	ically			
- O U:	se the following IP address:				
IP a	ddress:		5. U.S.		
Subr	net mask:				
Defa	ult gateway:		•		
0	btain DNS server address au	tomatically			
O U:	se the following DNS server a	addresses:			
Pref	erred DNS server;			4	
Alter	mate DNS server:		,	,	
V	alidate settings upon exit			Adv	/anced

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



General	
	d automatically if your network supports need to ask your network administrator
🔘 Obtain an IP address auto	matically
OUSE the following IP addre	ss:
IP address:	192 . 168 . 3 . 2
Subnet mask:	255.255.255.0
Default gateway:	192.168.3.1
Obtain DNS server addres	s automatically
OUSE the following DNS serv	ver addresses:
Preferred DNS server:	192.168.3.1
Alternate DNS server:	· · · · ·
Validate settings upon ex	Advanced

5. Click "OK" to complete the configuration.

4.2 Wifi Connection

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



Dial-up and VPN	^	Î
Broadband Connection		1
Wireless Network Connection	^	
KINGPIGEON	lite.	
niuren	lite.	
ChinaNet-DFxQ	1100	
mazentop		
King-xxxxx	din.	
Connect automatically	Connect	
DIRECT-11-HP DeskJet 3630 series	100	
TP-E		

Step2: Click "connect" to establish a connection.



Currently connected to:	+3	^
King-xxxxxx Internet access		ш
Dial-up and VPN	~	
Broadband connection		
Wireless internet connection	~	
King-xxxxx	Connected	
niuren	lite.	
KINGPIGEON	line.	
ChinaNet-DFxQ	Ilter	
mazentop	Iller	
DIRECT-11-HP DeskJet 3630 series		Ŧ

4.3. Factory Default Settings

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

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

4.4. Enter Web Settings

(1).Open a browser, such as IE, Google, etc. and enter IP address: http://192.168.3.1

(2).Enter username and password, user name: admin ,Password is empty, no need to enter(default)



Sign in http://192.10	8.3 .1		
CALCER OF THE	ion to this site is not private		
Username	admin		
Password			
		_	
		Sign in	Cancel

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

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

5. Router Settings

5.1 Status

(10) R40B - Overview - LuCl	× +		- 0	×
← → C ▲ Not secu	ure 192.168.3.1/cgi-bin/luci/		☆ (9 :
🚻 Apps 隆 翻译 🥪 金線	物联网云V3.0			
	R40B Status - System - Services - I	Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout		Î
	Status			
	System			- 1
	Hostname	R40B		- 1
	Model	Mediatek MT7628AN evaluation board		- 1
	Architecture	MediaTek MT7628AN ver:1 eco:2		- 1
	Firmware Version	KingPigeon Technology Co., Ltd. v1.18		- 1
	Kernel Version	4.14.162		
	Local Time	2020-10-23 05:02:05		
	Uptime	0h 5m 28s		
	Load Average	1.25, 1.10, 0.54		
	Memory			
	Total Available	63.86 MB / 121.79 MB (52%)		
	Free	74.29 MB / 121.79 MB (60%)		
	Buffered	5.55 MB / 121.79 MB (4%)		
	Cached	17.49 MB / 121.79 MB (14%)		•

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



5.2. System

5.2.1 System Properties

🚻 Apps 隆 翻译 😺 金綿	勿联网云V3.0					11025 - C (1994) (C) - 72-
	R40B Status - System	n - Services - Network - VF	PN ▼ Serial Port ▼ RT	UI/O - Logical operation -	Cloud platform - Logout	
	System				AUTO REFRESH ON	
		aspects of your device like its hostna	ame or the timezone.			
	System Properties					
	General settings Logging T	ime Synchronization Language an	id Style Product Type			
	Local Time	10/23/2020, 1:02:59 PM	Sync with browser	Sync with NTP-Server		
	Hostname	R40B				
		Same as product Type(Cannot	modify)			
	Timezone	UTC	•			
		Please restart the router to take	e effect			
				Save & A	Apply - Save Reset	

Configure basic information , such as host name or time zone

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

5.2.2 Management Rights



(11) R40B - Router Password - LuCI ×	+	- 0	×
← → C ▲ Not secure 19	2.168.3.1/cgi-bin/luci/admin/system/admin	☆ 0	:
👖 Apps 隆 翻译 😡 金錦物联网云V	13.0		
R408	B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout		
Route	r Password SSH Access SSH-Keys		
	Iter Password es the administrator password for accessing the device		
5.000 -	Password		
	Confirmation *		
	Save		
Powere	ed by KingPigeon Technology Co., Ltd. (v1.18) / 2020-10-16		

Management Rights				
Item	Description			
Password	Change the administrator password to access the device			
SSH access	Provides SSH access and SCP services			
SSH keys	Compared with the use of ordinary passwords, the public key allows passwordless SSH login with higher security. To upload the new key to the device, paste the OpenSSH compatible public key line or drag the .pub file into the input field.			

5.2.3 Software Package

(••) R40B - Software - LuCI	× +				- 5 ×
← → C ▲ Not secu	re 192.168.3.1/cgi-bin/luci/ac	lmin/system/opkg			☆ 🔒 :
🏥 Apps 💁 翻译 🎯 金錦橋	勿联网云V3.0				
	R40B Status - System	- Services - Network - VI	PN - Serial Port - RTU I/O - L	ogical operation - Cloud platform -	Logout
	Software				
			94% (7.7 MB)		
	Filter:	Download and install	package: Actions:		
	Type to filter	Clear Package name or U	RL OK Update lis	ts Upload Package Conf	figure opkg
	Available Installed Updates				
	w.		No packages	3	
	Package name	Version	Size (.ipk)	Description	
	No information available				
	Powered by KingPigeon Technolog	y Co., Ltd. (v1.18) / 2020-10-16			



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

5.2.4 Backup/Upgrade

(*) R40B - Backup / Flash Firmwar × +	- 0	×
← → C 🔺 Not secure 192.168.3.1/cgi-bin/luci/admin/system/flash	☆ (9 :
🗰 Apps 峰 翻译 🍑 金鎬物联网云V3.0		
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout		^
Flash operations		
Actions Configuration		1
Backup		1
Click "Generate archive" to download a tar archive of the current configuration files.		- 1
Download backup Generate archive		- 1
Restore		. 1
To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).		. 1
Reset to defaults Perform reset		. 1
Restore backup Upload archive		- 1
Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.		. 1
Save mtdblock contents		- 1
Click "Save mtdblock" to download specified mtdblock file. (NOTE: THIS FEATURE IS FOR PROFESSIONALS!)		100
Choose mtdblock u-boot		
Download mtdblock Save mtdblock		

Backup/Upgrade				
Item	Description			
Backup	Click "Generate Backup" to download the tar archive of the			
	current configuration file.			
Restore	Upload a backup archive to restore the configuration. To			
	restore the firmware to its initial state, click "Perform			
	Reset" (only squashfs format firmware is valid)			
Save mtdblock content	Click "Save mtdblock" to download the specified mtdblock			
	file. (Note: This function is for professionals!)			
Flash new firmware	Upload a sysupgrade compatible image from here to			
	update the running firmware			

5.2.5 Reboot





5.3. Service

5.3.1 Dynamic DNS

Dynamic DNS allows a fixed and accessible domain name to be configured for a host with a dynamic IP.

The overview displays a list of currently configured DDNS settings and their current status. If you need to update the IPv4 and IPv6 addresses at the same time, you need to add two configuration items separately (for example, 'myddns_ipv4' and 'myddns_ipv6'). By default, IPv4 and IPv6 configurations have been added separately. Please click "Edit" to enter the modification of the DDNS service Detailed configuration.

Note: Before clicking "Add", you need to enter a name for identification, otherwise it cannot be added successfully.

5.3.1.1 Basic setting



(··) R40B - LuCl × +		-	٥	×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci	/admin/services/ddns/detail/myddns_jpv4	See 1	θ	
R40B Status - System	Services - Network - VPN - Serial Port - RTU I/O - Logical operation - Cloud platform - Logout			Â
	uter can be reached with a fixed hostname while having a dynamically changing IP address. mentation DDNS Client Configuration			
Details for: myddns_ip	v4			- 1
Configure here the details for sele	acted Dynamic DNS service.			- 1
Basic Settings Advanced Sett	ings Timer Settings Log File Viewer			
Enabled				
	If this service section is disabled it could not be started. Neither from LuCI interface nor from console			
Lookup Hostname	yourhost.example.com			
	Bostname/FQDN to validate, if IP update happen or necessary			
IP address version	IPv4-Address IPv6-Address			- 1
	Defines which IP address 'IPv4/IPv6' is send to the DDNS provider			
DDNS Service provider [IPv4]	dyn.com 🗸			
Domain	yourhost example.com			
	@ Replaces [DOMAIN] in Update-URL			
Username	your_username			Ŧ

DNS Basic Settings					
Item	Description				
enable	If the service configuration is disabled, then it cannot be				
епаріе	started.				
Lookup hostname	Hostname/FQDN verification, if IP update occurs or is				
	necessary				
IP address version	Set which IP address (IPv4 or IPv6) will be sent to the				
	DDNS provider				
DDNS	Choose DDNS service provider				
service provider					
Domain	Enter domain name				
Username	Enter username				
Password	Enter password				

5.3.1.2 Advanced Setting



(**) R40B - LuCi × +	- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/services/ddns/detail/myddns_ipv4	≅ ☆ 8 :
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	^
Dynamic DNS Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address. OpenWrt Wiki: DDNS Client Documentation DDNS Client Configuration	
Details for: myddns_ipv4	
Configure here the details for selected Dynamic DNS service.	
Basic Settings Advanced Settings Timer Settings Log File Viewer	
IP address source [IPv4] Network	
Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider	
Network [IPv4]→ wan ✓	
Defines the network to read systems IPv4-Address from	
Force IP Version	
@ OPTIONAL: Force the usage of pure IPv4/IPv6 only communication.	
DNS-Server mydns.lan	
OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'. Format: IP or FQDN	
PROXY-Server user:password@myproxy1an:8080	
OPTIONAL: Proxy-Server for detection and updates.	

DNS Advanced Setting				
Item	Description			
IP address source	Set the source of the IP address. This will be sent to the			
	DDNS provider			
Network	Read system IP address network			
Force IP version	Optional: Force to use only IPv4/IPv6 communication.			
	Optional: Use a non-default DNS server to detect			
DNS server	"registered IP addresses".			
	Format: IP or FQDN			
	Optional: Proxy server for detection and update.			
Brown convor	Format: [user:password@]proxyhost:port			
Proxy server	The IPv6 address must be filled in square brackets ("[]"):			
	[2001:db8::1]:8080			
	Write the log to the system log. Regardless of whether			
Log to system log	this option is enabled, error messages will always be			
	written to the system log.			
Log to file	Write detailed information to the log. The file will			
	automatically shrink.			

5.3.1.3 Timer setting



(•) R40B - LuCI	× +										-	٥	×
← → C ▲ Not sect	ure 192.168	.3.1/cgi-l	bin/luci/ad	min/services/d	dns/detail/r	myddns_ipv4						r (9 :
	R40B 5	Status -	System +	Services - N	letwork - \	√PN × Serial Port ×	rtu I/0 🗕	Logical operation -	Cloud platform -	Logout			
		allows that	it your router	r can be reached v		ostname while having a	dynamically (changing IP address.					
	Details for	: mydd	dns_ipv4	L.									
	Configure here	the detai	ls for selecte	ed Dynamic DNS s	ervice.								
	Basic Settings	Advar	iced Setting	Timer Settings	Log File V	liewer							- 1
		Check I	nterval 1	0	minutes	3	~						
			6	Interval to check Values below 5		IP 00 seconds are not sup	ported						
		Force I	nterval 7	2	hours		~						
			(Setting this para	meter to 0 wi	d to DDNS Provider ill force the script to onl except '0' are not supp							
	Err	or Retry C	ounter 0										
				On Error the sci The default sett		xecution after given nu etry infinite.	mber of retrys						
	En	ror Retry I	nterval 6	0	second	s	~						
			0	On Error the sci	ipt will retry th	he failed action after giv	en time						
	Back to C	Overview]					Save	& Apply Save	Reset			

Timmer Settings					
Item	Description				
Check interval	Time interval for checking whether IP has changed Values less than 5 minutes (300 seconds) are not supported				
Force interval	Mandatory time period to update DDNS to the provider Setting this parameter to 0 will make the script execute only once Values smaller than "check time period" are not supported (except 0)				
Error retry counter	When an error occurs, the script will retry the number of times before exiting The default setting "0" will retry indefinitely.				
Error retry interval	When an error occurs, the script will retry the number of failed actions				

5.3.1.4 Log File Viewer



N R40B - LuCI	x +	P 1	•
- > C (A N	Not secure 192.168.3.1/cgi-bin/luci/admin/services/ddns/detail/myddns_ipv4	See 1	Θ
	R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout		
	Dynamic DNS		
	Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address. OpenWrt Wiki: DDNS Client Documentation DDNS Client Configuration		
	Details for: myddns_ipv4		
	Configure here the details for selected Dynamic DNS service.		
	Basic Settings Advanced Settings Timer Settings Log File Viewer		
	Dasic settings Advanced Settings Timer Settings Log File Viewer		
	Read / Reread log file		
	031306 : ***********************************		
	031306 : ddns version : 2.7.8-12		
	031306 : uci configuration:		
	ddns.myddns_ipv4.domain='yourhost.example.com'		
	ddns.myddns_ipv4.enabled='0'		
	ddns.myddns_ipv4.interface='wan'		
	ddns.myddns_ipv4.ip_network='wan'		
	ddns.myddns_ipv4.ip_source= 'network'		
	ddns.myddns_ipv4.lookup_host='yourhost.example.com' ddns.myddns ipv4.password='***PW***'		
	ddns.myddns_rpv4.service_name='dyn.com'		
	ddns.myddns_ipv4.username='your username'		
	ddns.myddns ipv4=service		
	031307 : verbose mode : 0 - run normal, NO console output		
	031307 WARN : Service section disabled! - TERMINATE		
	031307 WARN : PID '3086' exit WITH ERROR '1' at 2020-11-02 03:13		

5.4 Network

5.4.1 Interface

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

- V

R40B	Status - Syste	em + Services + Network + VPN + Seria	Il Port ≠ RTU I/O ≠ Lo	gical operation - Clo	ud platform - Logout	
Interfaces	Global network o	ptions			AUTO REFRESH ON	
Interfac	es					
() R(g	AN	Protocol: Static address Uptime: 0h 47m 33s MAC: 46:68:A3:D3:DA:68 RX: 4.02 MB (37066 Pkts.) TX: 2.51 MB (8636 Pkts.) IPv4: 192.168:3.1/24 IPv6: fd83:fb6e:35eb::1/60	Restart	Stop	Edit Delete	
	AN h0.2	Protocol: DHCP client MAC: 46:68:A3 D3:DA:69 RX: 259.14 KB (2779 Pkts.) TX: 8:27 KB (61 Pkts.)	Restart	Stop	Edit Delete	
	ANG tho.2	Protocol: DHCPv6 client MAC: 46:68:A3 D3:DA:69 RX: 259.14 KB (2779 Pkts.) TX: 8.27 KB (61 Pkts.)	Restart	Stop	Edit Delete	
	4G 3-4G	Protocol: UMTS/GPRS/EV-DO RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Restart	Stop	Edit	
Add ne	ew interface					

5.4.1.1 LAN port



٥ (••) R40B - Network Settings - Lu C × + × → C A Not secure | 192.168.3.1/cgi-bin/luci/admin/network/network ← ☆ \varTheta : Interfaces » LAN General settings Advanced Settings Physical Settings Firewall Settings DHCP Server ~ Protocol Static address Bring up on boot IPv4 address 192.168.3.1 IPv4 netmask 255.255.255.0 IPv4 gateway IPv4 broadcast 192.168.3.255 Use custom DNS servers + • IPv6 assignment length 60 Assign a part of given length of every public IPv6-prefix to this interface

LAN Port					
Item		Description			
		Device: br-lan			
		Running time: 8h 57m 16s			
		MAC: E2:2F:C4:54:93:BA			
	Status	Receive: 18.81 MB (149126 data pack)			
		Send: 99.87 MB (132321 data pack)			
		IPv4: 192.168.3.1/24			
		IPv6: fdb2:428b:ddbe::1/60			
	Protocol	Static address			
	Bring up on boot	Default enable			
		Default 192.168.3.1, modify this setting			
	IPv4 address	to change the network segment that			
Pacie Setting		DHCP assigns IP to LAN port			
Basic Setting	IPv4 netmask	Default 255.255.255.0			
		Default is empty, when multiple IPv4			
	IPv4 gateway	addresses are set, the gateway address			
		needs to be specified			
	IPv4 broadcast	Default 192.168.3.255			
	Use custom DNS server	Default is empty			
		Assign a given length part of each			
	IPv6 allocation length	public IPv6 prefix to this interface,			
		default 60			
	IPv6 assignment tips	Assign this hexadecimal sub-ID prefix to			
		this interface			
	IPv6 suffix	Optional, allowed values: "eui64",			

Page 42 of 97 King Pigeon Hi-Tech. Co., Ltd. Ver 1.0



Advanced Use built-in IPv6 management Default for "::12"). When the Pv6 prefix (such as "::1") to synthesize an IPv6 address ("a:b::c::1") Assigned to this interface. Advanced Mandatory link Default enable Reset MAC address Modify MAC address Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing). default is enable. Reset MAC address Modify MAC address Reset MTU Default 100 Use Gateway Hop Default is enable. Enable STP Enable IGMP sniffing Enable IGMP sniffing Enable IGMP snopping on this bridge, default is disable. Firewall settings Create/Assign firewall zone Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xwaxe" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP server Basic Setting Customers Maximum number of address assignments. The default is 120. DHCP DHCP Provide DHCP service for all clients. If disabled, only customers with static leases tring <th></th> <th></th> <th></th> <th></th>						
Advanced settings IPv6 management Default enable Advanced settings Mandatory link Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing). default is enable. Reset MAC address Modify MAC address Bridge interface Create a bridge for the specified interface, default is disable. Enable STP Enable IGMP sniffing Enable IGMP snooping on this bridge, default is disable Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fi				example: "::1" or "::1:2"). When the IPv6 prefix (such as "a:b:c:d::") is obtained from the authorization server, use the suffix (such as "::1") to synthesize an IPv6 address		
Advanced settings Mandatory link Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing). default is enable. Reset MAC address Modify MAC address Reset MAC address Modify MAC address Reset MTU Default 1500 Use Gateway Hop Default 0 Bridge interface Create a bridge for the specified interface, default is enable. Enable STP Enable spanning tree protocol on this bridge, default is disable. Enable IGMP sniffing Enable IGMP snooping on this bridge, default is disable. Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxxi" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP server Basic Start Start network address, default is 100. Customers Start Start network address, default is 100. Customers assignments. The default is 120. Advanced settings DHCP Provide DHCP service for all clients. If disabled, only customers with static lease will be served. defa				Default enable		
Reset MTU Default 1500 Use Gateway Hop Default 0 Bridge interface Create a bridge for the specified interface, default is enable. Enable STP Enable spanning tree protocol on this bridge, default is disable. Enable IGMP sniffing Enable IGMP snoping on this bridge, default is disable. Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP service is not provided on this interface Start Start network address,default is 100. Basic Setting Lage term Maximum number of address assignments. The default is 150. DHCP service Lease term Maximum number of the leased address is at least 2 minutes (2m). The default is 12h.				interface, always use the application settings (if checked, the link status change will no longer trigger hotplug		
Reset MTU Default 1500 Use Gateway Hop Default 0 Bridge interface Create a bridge for the specified interface, default is enable. Enable STP Enable spanning tree protocol on this bridge, default is disable. Enable IGMP sniffing Enable IGMP snoping on this bridge, default is disable. Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP service is not provided on this interface Start Start network address,default is 100. Basic Setting Lage term Maximum number of address assignments. The default is 150. DHCP service Lease term Maximum number of the leased address is at least 2 minutes (2m). The default is 12h.		Reset MAC	address	Modify MAC address		
Use Gateway Hop Default 0 Bridge interface Create a bridge for the specified interface, default is enable. Enable STP Enable spanning tree protocol on this bridge, default is disable. Enable IGMP sniffing Enable IGMP snooping on this bridge, default is disable. Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP service is not provided on this interface. Start Start network address,default is 100. Basic Setting Customers Maximum number of address assignments. The default is 150. DHCP server Lease term Advanced settings DHCP service for all clients. If disable, the server. DHCP service for all clients. If disable, the server.		Reset MTU				
Bridge interface Create a bridge for the specified interface, default is enable. Enable STP Enable STP Enable IGMP sniffing Enable IGMP snooping on this bridge, default is disable. Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP server Basic Setting Ignore this interface DHCP service is not provided on this interface.default is disable Advanced settings DHCP The expiration time of the leased address is at least 2 minutes (2m). The default is 12h.			ау Нор			
Physical settings Enable IGMP sniffing Enable IGMP snooping on this bridge,default is disable. Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP Basic Setting Ignore this interface DHCP service is not provided on this interface. Basic Setting Customers Maximum number of address assignments. The default is 150. The expiration time of the leased address is at least 2 minutes (2m). The default is 12h. Advanced settings DHCP DHCP DHCP Provide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.				Create a bridge for the specified		
Physical settings Enable IGMP sniffing bridge,default is disable Firewall settings Interface Switch VLAN: "eth0.1" (lan), wireless network: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modified Firewall settings Create/Assign firewall zone Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it. DHCP Basic Setting Ignore DHCP service is not provided on this interface, default is disable DHCP Customers Start Start network address, default is 150. DHCP Advanced settings DHCP The expiration time of the leased address is at least 2 minutes (2m). The default is 12h. Provide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.		Enable STP				
Interfacenetwork: Master "King-xxxxx" (lan), set the physical interface using the LAN port, generally do not need to be modifiedFirewall settingsCreate/Assign - firewall zoneAssign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it.DHCPBasic SettingIgnore this interfaceDHCP service is not provided on this interface, default is disableDHCPCustomersMaximum number of address assignments. The default is 150.DHCPAdvanced settingsDHCPThe expiration time of the leased address is at least 2 minutes (2m). The default is 12h.Advanced settingsDHCPProvide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.	Physical settings	Enable IGM	P sniffing			
Firewall settingsCreate/Assign firewall zoneinterface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it.DHCP serverIgnore this interfaceDHCP service is not provided on this interface,default is disableDHCP serverStartStart network address,default is 100.Lease term ettingsMaximum number of address assignments. The default is 150.Advanced settingsDHCPProvide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.		Interface		network: Master "King-xxxxxx" (lan), set the physical interface using the LAN port, generally do not need to be		
DHCPthis interfaceinterface, default is disableSettingStartStart network address, default is 100.CustomersMaximum number of address assignments. The default is 150.Basic SettingLease termThe expiration time of the leased address is at least 2 minutes (2m). The default is 12h.Advanced settingsDHCPProvide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.	Firewall settings	-	-	interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate		
Basic SettingStartStart network address, default is 100.DHCP serverCustomersMaximum number of address assignments. The default is 150.DHCP serverLease termThe expiration time of the leased address is at least 2 minutes (2m). The default is 12h.Advanced settingsDHCPProvide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.			Ignore	DHCP service is not provided on this		
Basic SettingCustomersMaximum number of address assignments. The default is 150.DHCP serverLease termThe expiration time of the leased address is at least 2 minutes (2m). The default is 12h.Advanced settingsDHCPProvide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.			this interface	interface, default is disable		
Basic SettingCustomersMaximum number of address assignments. The default is 150.DHCP serverLease termThe expiration time of the leased address is at least 2 minutes (2m). The default is 12h.Advanced settingsDHCPProvide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.			Start	Start network address, default is 100.		
serverLease termaddress is at least 2 minutes (2m). The default is 12h.Advanced settingsDHCPProvide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.			Customers			
Advanced settings DHCP disabled, only customers with static leases will be served. default is enable.			Lease term	address is at least 2 minutes (2m). The		
Forcibly Even if another server is detected, it is			DHCP	disabled, only customers with static		
			Forcibly	Even if another server is detected, it is		



		mandatory to use DHCP on this
		network, default is disable.
	IPv4 Subnet	Reset the subnet mask sent to the
	mask	client.
		Set additional options for DHCP, for
		example,
	DHCP Options	setting "6,192.168.2.1,192.168.2.2"
		means to announce different DNS
		servers to clients.
	Route	
	Advertisement	Default server mode
	Service	
	DHCPv6 server	Default server mode
	HDP proxy	Default disable
IPv6	DHCPv6 mode	The default is stateless + stateful
	Always	Even if there is no public network prefix
setting	advertise the	available, it still advertises itself as the
	default route	default route, default is disable
	Advertised DNS	Default is empty
	server	Default is empty
	Advertised DNS	Default is amont
	domain name	Default is empty

5.4.1.2 WAN port

(**) R40B - Network Settings - LuC × +		- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci	admin/network/network	☆ \varTheta :
R40B Status - Syste	n + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	*
Interfaces » WAN		
Ir General settings Advan	ed Settings Physical Settings Firewall Settings	
St	tus Device: eth0.2 MAC: 46.68.A3 D3:DA:69 RX: 259.14 KB (2779 Pkts.) TX: 8.27 KB (61 Pkts.)	
Prot	DHCP client	
Bring up on	oot 🗹	
Hostname to send w requesting Di		
	Dismiss Save	
etn0.2	TX: 8.27 KB (61 Pkts.)	
4G 50 39-4G	Protocol: UMTS/GPRS/EV-DO RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) Error: Network device is not present	
	Save & Apply - Save Reset	~

WAN Port		
Item Description		



	Status	Device: eth0.2 Running time: 9h 37m 16s MAC: E2:2F:C4:54:93:BB Receive: 113.65 MB (290226 data pack) Send: 19.02 MB (137282 data pack) IPv4: 192.168.1.173/24	
General Setting	Protocol	Default DHCP client; if the network connected to the WAN requires an account and password to log in, please select PPPoE protocol or other corresponding protocol	
	Bring up on boot	Default is enable	
	Hostname sent when requesting DHCP	Default is product model	
	Use built-in IPv6 management	Default is enable	
	Mandatory link	Regardless of the link status of the interface, always use the application settings (if checked, the link status change will no longer trigger hotplug event processing). Default is disable.	
	Use broadcast tags	Needed by some ISPs, for example: coaxia network DOCSIS 3,default is disable.	
Advanced settings	Default gateway	Leave blank to not configure the default route, default is enable.	
	Obtain DNS	Leave blank to ignore the advertised DNS	
	server automatically	server address, default is enable.	
	Use Gateway Hop	Default is empty	
	Client ID sent when requesting DHCP	Default is empty	
	Vendor Class option sent when requesting DHCP	Default is empty	
	Reset MAC address	Modify MAC address	
	Reset MTU	Default is 1500	
	Bridge interface	Create a bridge for the specified interface, default is disable	
Physical settings	Interface	Switch VLAN: "eth0.2" (wan, wan6), set which physical interface to use, generally do not need to be modified	
Firewall settings	Create/Assign firewall zone	Assign the firewall area to which this interface belongs, select Unspecified to move the interface out of the associated area, or fill in the creation field to create a new area and associate the current interface with it.	



5.4.1.3 WAN6 Port

(··) R40B - Network Settings - LuC × +		-)	0	×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/ad	lmin/network/network	☆	Θ	:
R40B Status - System	« Services » Network » VPN » Serial Port » RTU I/O » Logical operation » Cloud platform « Logout			^
	AUTO REFRESH ON			
Interfaces » WAN6				
General settings Advanced	Settings Physical Settings Firewall Settings			
Statu	s 💯 Device: eth0.2			
	MAC: 46:68:43:D3:DA:69 RX: 259:14 KB (2779 Pkts.) TX: 8:43 KB (62 Pkts.)			
Protoco	DHCPv6 client			
Bring up on boo				
Request IPv6-addres	s try 🗸			
Request IPv6-prefix of lengt	Automatic •			
Request Pro-preix of lengt	Automatic			
	Dismiss Save			
4G	Protocol: UMTS/GPRS/EV-DO			
3g-4G	RX: 0 B (0 Pkts.) Restart Stop Edit Delete			
Add new interface				
	Save & Apply + Save Reset			

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



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

5.4.1.4 4G Port

(••) R40B - Network Settings - LuC × +		- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/adm	n/network/network	☆ \varTheta :
R40B Status - System -	Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	Â
Interfaces » 4G	(AUTO REFRESH ON	
General settings Advanced Set	ttings Firewall Settings	
Status	Device: 3g-4G RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	
Protocol	UMTS/GPRS/EV-DO V	
Bring up on boot		
Modem device	/dev/ttyUSB4 •	
Service Type	UMTS/GPRS ·	
APN	cmnet	
PIN		
PAP/CHAP username		
PAP/CHAP password		
Dial number	*99***1#	
	Dismiss Save	-

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



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

5.4.2 WIFI



R40B - WiFi - LuCI	× +							- 0	×
→ C ▲ Not secur	re 192.168.3.1/cgi-	bin/luci/admin/networ	k/wireless					* 6	•
	R40B Status -	System - Services -	- Network - VPN -	Serial Port - RTU	I/O - Logical operation	n → Cloud platfo	rm + Logout		
	WiFi Settings						AUTO REFRESH ON		
	🙊 radio0	Media Tek MT76x8 8 Channel: 11 (2.462 GHz			Restart	Scan	Add		
	0%	SSID: King-2b77b3 Mo BSSID: EC:0C:45:81:26:			Disable	Edit	Remove		
	Associated Stat	tions							
	Network	MAC-Address	Host	Signal / Noise	RX F	Rate / TX Rate			
			No info	ormation available					
					Save	& Apply	ave Reset		
	Powered by KingPigeo	on Technology Co., Ltd. (v1	.18) / 2020-10-16						

Supports both WLAN hotspot and WLAN client.

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

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

5.4.2.1 WLAN Hotspot(Wifi AP mode)

(•) R40B - WiFi - LuCl × +		-	٥	×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admir	/network/wireless	☆	0	(;)
R40B Status - System -	Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout			^
W Wireless Network: Master	"King-2b77b3" (wlan0)			
Device Configuration				
General Setup Advanced Settin	gs			
A	Mode: Master SSID: King-2b77b3 0% BSSID: EC: 0C:45:81:26:51 Encryption: None Channel: 11 (2:452 GHz) Tx-Power: 20 dBm Signal: 0 dBm Noise: 0 dBm Bitrate: 0.0 Mbit/s Country: 00			
Wireless network is enabled	Disable Mode Channel Width			
Operating frequency	N V 11 (2462 Mhz) V 20 MHz V			
Maximum transmit power	driver default 🗸 - Current power: 20 dBm			
P.	Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.			
Interface Configuration				
General Setup Wireless Securit	y MAC-Filter Advanced Settings			
Mode	Access Point			
ESSID	King-2b77b3			-

The default SSID is King-xxxxx, no encryption method, other clients can directly search the wireless network to connect to this hotspot.

Quick configuration: Select the wireless configuration in Master mode in the wireless profile, click

4G Wireless Industrial Router Wireless Data Connectivity

"Edit" to enter the configuration page, find "Interface Configuration"-"Basic Settings"-"ESSID" to modify the WiFi hotspot name, find "Interface Configuration"- -"Wireless Security"-"Encryption" can modify the encryption method to set the WiFi password.

Note: When using WiFi connection to enter the router configuration, to modify the WLAN hotspot configuration, you need to select "force application", please click the drop-down button behind "save and apply" and select "force application"

Wireless network AP hotspot device configuration			
Item		Description	
General	Status	 97% Mode: Master SSID: King-ff4a8a BSSID: EE:0C:45:81:26:51 Encryption: None Channel: 6 (2.437 GHz) Transmission power: 20 dBm Signal: -42 dBm Noise: 0 dBm Transmission rate: 58.5 Mbit/s Country: 00 	
Setup	Wireless network is enabled	Default is enable	
	Operating frequency	If there are too many devices in use at the current frequency, please change one	
	Maximum transmit power	Specify the maximum transmit power. Depending on regulatory requirements and usage, the driver may limit the actual transmit power below this value.	
	Country code	Driver default	
	Allow traditional 802.11b rate	Default is enable	
	Distance optimization	The distance (meter) of the furthest network user. Automatic by default, automatically adjust the transmission power according to the distance	
Advanced	Fragmentation threshold	Automatically send data when the data length exceeds the threshold, generally use the default value	
settings	RTS/CTS Threshold	Request to send/allow sending protocol. When the data length exceeds the threshold, start the protocol to avoid signal conflicts caused by multiple terminals sending data to the AP. Usually use default value	
	Force 40MHz mode	Even if the auxiliary channels overlap, the 40MHz channel is always used. Using this option is not compliant with IEEE 802.11n-2009! Default is disable.	
	Beacon interval	Indicates the interval at which the wireless	

router periodically broadcasts its SSID. Usually use default value.

V	Vireless network AP h	otspot interface configuration
Item		Description
	Mode	Access Point
	ESSID	Default King-xxxxx (xxxxxx is Random numbers or letters)
Pasic Sotting	Network	lan
Basic Setting	Hide ESSID	Default is disable
	WMM mode	Wi-Fi Multimedia,providing different priorities for different services to ensure service quality,default is enable
Wireless security	encryption	No encryption by default (open network)
MAC filter	MAC address filter	Default is disable
	Isolate the client	Forbid communication between clients, default is disable
	Interface name	Reset the default interface name
	Short Preamble	Different rates need to use different Preamble (preamble), default is enable
	DTIM interval	As a terminal node, periodically wake up to send traffic indication message interval
Advanced settings	Interval for re-encrypting GTK	Temporary key (GTK), Use default
	Disable inactive polling	Default is disable
	Inactive site restrictions	Default is empty
	Max allowed listening interval	Default is empty
	Disconnect on low Ack response	Allow AP mode to disconnect wireless terminal under low ACK, default is enable.

5.4.2.2 WLAN Client

40B - WiFi - LuCl	× + secure 192.168.3.1/cgi-bin/luci/admin/net	work (wiroloss				- 0 \$
			 VPN - 	Serial Port - RTU I/O -	- Logical operation - Cloud platform - Logout	ч
					AUTO REFRESH ON	
Join Networ	k: Wireless Scan					
Signal	SSID	Channel	Mode	BSSID	Encryption	
48%	jingekeji	1	Master	24:69:68:82:3C:96	mixed WPA/WPA2 PSK (CCMP) Joi	n Network
37%	DIRECT-58-HP DeskJet 3630 series	6	Master	40:B0:34:63:EB:59	WPA2 PSK (CCMP) Joi	n Network
34%	King-e4f82b	11	Master	EC:0C:45:81:26:54	None Joi	n Network
30%	BioLock	6	Master	60:3A:7C:0D:00:16	mixed WPA/WPA2 PSK (CCMP) Joi	n Network
						Dismiss
					Save & Apply Save Reset	
	Powered by KingPigeon Technology Co., Ltd.	(v1.18) / 2020-1				

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

		Device Configuration
Item		Description
Basic Setting	Status	 100% Mode: Client SSID: jingekeji BSSID: EC:0C:45:81:26:51 Encryption: WPA2 PSK (CCMP) Channel: 6 (2.437 GHz) Transmission power: 20 dBm Signal: -38 dBm Noise: 0 dBm Transmission rate: 1.0 Mbit/s Country: 00
	Wireless network is enabled	Default is enable
	Working frequency	If there are too many devices in use at the current frequency, please change one
	Max transmission power	Specify the maximum transmit power. Depending on regulatory requirements and usage, the driver may limit the actual transmit power below this value.
	Country code	Driver default
Advanced	Allow traditional 802.11b rate	Default is enable
settings	Distance optimization	The distance (meter) of the furthest network user. By default, the transmission power is automatically adjusted according to the distance



Fragmentation	Automatically send data when the data length exceeds					
threshold	the threshold, usually use default value.					
	Request to send/allow to send protocol. When the data					
RTS/CTS	length exceeds the threshold, start the protocol to avoid					
Threshold	signal collision caused by multiple terminals sending data					
	to the AP, usually use default value.					
Force 40MHz mode	Even if the auxiliary channels overlap, the 40MHz channel					
	is always used. Using this option is not compliant with					
	IEEE 802.11n-2009! default is disable.					
Deces interval	Indicates the interval at which the wireless router					
Beacon interval	periodically broadcasts its SSID, usually use default value.					
	threshold RTS/CTS Threshold Force 40MHz					

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

5.4.3 Cellular Network



(++) R40B - Cellular Network - LuCI × +		- c	9	×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci	admin/network/cell	☆	θ	:
R40B Status ≁ System	✓ Services ✓ Network ✓ VPN ✓ Serial Port ✓ RTU I/O ✓ Logical operation ✓ Cloud platform ✓ Logout			
Cellular Network				
Cellular Network				
Register Staus	Unregistered,Searching station			
Operator	NA			
Signals	6 @ Normal range of signal value 14~31			
Firmware Version	EC25AUGCR06A02M1G			
IMSI	CME			
IMEI	861585042306033			
SIM Card ID	NA			
Card Select	Card 1 🗸			
Card1 Number				
Card1 APN				ļ
Card1 Username				
Card1 Password				

	Cellular Network			
Item	Description			
Register status	Registered			
Operator	N/A			
Signal	Normally is 14-31			
Firmware version	EC25AUGCR06A02M1G			
IMSI	SIM card IMSI number			
IMEI	Device IMEI number			
SIM card ID	SIM card ICCID number			
Card select	Card 1, Card 2, this selection as the preferred SIM card, When the preferred SIM card cannot be connected to the network, it will automatically switch to another card to try to connect to the network			
Card 1 /2 number	Enter sim card 1 number			
SIM card 1/2 APN	Enter APN			
SIM card 1/2 username	Enter username			
SIM card 1/2 passwrod	Enter password			
Enable GPS	Default is disable, when choosing a module with GPS function, please select enable, GPS data will be uploaded through MQTT protocol			

5.4.4 DHCP/DNS

4G Wireless Industrial Router Wireless Data Connectivity

B - DHCP and DNS -	LuCI × +						-	٥
C A Not se	ecure 192.168.3.1/	cgi-bin/luci/admin/netwo	rk/dhcp				☆	
	R40B Status	- System - Services -	Network - VPN - Se	rial Port + RTU I/O +	Logical operation	ation - Cloud platform - Logout		
	DHCP and Dnsmasq is a comb	DNS ined DHCP-Server and DNS-I	Forwarder for NAT firewalls			AUTO REFRESH ON		
	Server Setting	gs	kontensites					
	General settings	Resolv and Hosts Files TF	TP Settings Advanced Settin	ngs Static Leases				
	Hostname	MAC-Address	IPv4-Address	Lease time	DUID	cific lease time, e.g. 12h, 3d or infinite.		
			This section cor	tains no values yet				
	Add							
	Active DHCP L	eases						
	Hostname	IPv4-Address	MAC-Ado	Iress	Leasetime	e remaining		
			There are n	o active leases				
	Active DHCPv6	Leases						
	Host		IPv6_Address	DUID		Leasetime remaining		

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

	Server Settings					
Item		Description				
	lgnore empty domain name resolution	Do not forward resolution requests without DNS names, checked by default				
	Unique authorization	This is the only DHCP server in the local network, default is enable				
	Local server	Local domain rules. Names matching this domain are never forwarded, only resolved from DHCP or HOSTS files				
	Local domain name	The local domain name suffix will be added to the DHCP and HOSTS file entries				
Conoral	Record query log	Write received DNS request to system log, defaule is disable				
General	DNS forward	List of DNS servers to which requests are forwarded				
Setting	Rebinding	Discard RFC1918 upstream response data, default is enable				
	protection Allow local	Allow upstream response within 127.0.0.0/8 loopback range, for example: RBL service, default is enable.				
	Domain name whitelist	List of domain names that allow RFC1918 to respond				
	Local service only	DNS service is only provided in the subnet to which the network card belongs, default is enable.				
	Not all addresses	Dynamically bind to interface instead of wildcard address (recommended as linux default), default is enablee				

4G Wireless Industrial Router Wireless Data Connectivity

	Listening interface	Only listen to these interfaces and loopback interfaces.								
	Exclude interface	Do not listen to these interfaces.								
	use /etc/ethers	Configure DHCP server according to								
	Configuration	/etc/ethers,default is enable.								
HOSTS& parse	Lease documents	The file used to store the assigned DHCP lease, default is :/tmp/dhcp.leases								
the file	Ignore parsing file	Default is disable								
	Ignore /etc/hosts	Default is disable								
	Additional HOSTS file	Default is empty								
TFTP setting	Enable TFTP server	Default is disable								
	No log	Does not record general operation logs of these protocols, default is disable.								
	Sequential	IP addresses are assigned sequentially starting from								
	allocation IP	the lowest available address, default is disable.								
-	Filter local	Reverse queries without forwarding the local								
	packages	network,default is enable.								
	Filter useless	Do not forward requests that the public domain								
	packets	name server cannot respond, default is disable								
		If multiple IPs are available, the host name is								
	Localized query	localized according to the subnet from which the								
		request originated, default is enable								
	Expand the host suffix in the HOSTS file	Add the local domain name suffix to the domain name in the HOSTS file, default is enable								
	Disable invalid information cache	Do not cache useless responses, for example: domain names that do not exist, default is disable								
Advanced settings	Additional SERVERS	This file may contain formats such as "server=/domain/1.2.3.4" or "server=1.2.3.4" .The former specifies a DNS server for a specific domain, while the latter does not limit the resolution range of the server.								
	Strict order checking	Query DNS server in the order of "parse file", default is disable.								
	All server	Query all available upstream DNS servers, default is disable.								
	Ignore fake empty domain name resolution	List of servers allowed to respond with fake empty domain names								
	DNS server port	Inbound DNS query port								
	DNS query port	Specified DNS query source port								
	Max DHCP leases No.	Maximum number of DHCP leases allowed								
	Max EDNS0 data pack size	Allowed max EDNS.0 UDP data pack size								



	Maximum concurrent queries number	Maximum number of concurrent DNS queries allowed					
	DNS Query cache	Cached DNS entries numbers (maximum 10000, 0					
	size	means no cache)					
		Static leases are used to assign fixed IP addresses and host IDs to DHCP clients. Only the specified host can be connected, and the interface must be non-dynamically configured. Use the Add button to add a new lease entry. The values of the IPv4 address and host name fields will be fixedly assigned to the hosts identified by the MAC address field. The lease period is an optional field, and the length of the DHCP lease period can be set separately for each host, for example: 12h, 3d, infinite, Respectively 12 hours, 3 days, permanent.					

5.4.5 Host names

(10) R40B - Hostnames - LuCl	× +		- 0 ×						
← → C ▲ Not secu	re 192.168.3.1/cgi-bin/luci/admin/network/hosts		☆ 😑 :						
	R40B Status - System - Services - Network - Vi	PN → Serial Port → RTU I/O → Logical operation → Cloud pla	atform 👻 Logout						
	Hostnames Host entries								
	Hostname	IP address							
	This								
	Add								
		Save & Apply -	Save						
	Powered by KingPigeon Technology Co., Ltd. (v1.18) / 2020-10-16								

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

5.4.6 Routes



(••) R40B - Static Routes - LuCI	× +								- đ	5	×
← → C ▲ Not secure	e 192.168.3.1/c	cgi-bin/luci/admin/ne	etwork/routes						☆	θ	:
	R40B Statu	ıs - System - Serv	rices - Network - VPI	N 👻 Serial Port 👻	rtu I/o 👻	Logical operation -	Cloud platform +	Logout			
	Routes Routes specify over which interface and gateway a certain host or network can be reached.										
	Static IPv4 Routes	Static IPv6 Routes									
	Static IPv4 R	outes									
	Interface	Target	IPv4-Netmask	IP	v4-Gateway	Metric	On-Link route				
		Host-IP or Network	if target is a net	work							
			This s	ection contains no val	ues yet						
	Add										
						Save & Ap	oply • Save	Reset			
	Powered by KingPi	igeon Technology Co., Lt	d. (v1.18) / 2020-10-16								

The routing table describes the reachable path of the packet

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

5.4.7 Diagnosis

	4 G Wirele		rial Router ss Data Con	
(••) R40B - Diagnostics - LuCl × +				- o ×
← → C ▲ Not secure 192.168.3.1,	cgi-bin/luci/admin/network/diagnostic	s		☆ \varTheta :
R40B Stat	us - System - Services - Network -	VPN - Serial Port - RTU I/O -	Logical operation - Cloud platform - Log	gout
Diagnost Network Uti openwrt.org	ities		openwrt.org Nslookup	
Powered by Kingl	Pigeon Technology Co., Ltd. (v1.18) / 2020-10-	-16		

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

5.4.8 Firewall

5.4.8.1 Zone settings

(*) R40B - General settings - LuCl × +	-	٥	×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/network/firewall	☆	Θ	:
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout			-
General settings Port Forwards Traffic Rules Custom Rules			
Firewall - Zone Settings			
The firewall creates zones over your network interfaces to control network traffic flow.			
General settings			
Enable SYN-flood protection			
Drop invalid packets			
Input accept ~			
Output accept ~			
Forward accept			
Routing/NAT Offloading			
Experimental feature. Not fully compatible with QoS/SQM.			
Software flow offloading			
Ø Software based offloading for routing/NAT			
Zones			
Zone ⇒ Forwardings Input Output Forward Masquerading			
Ian ⇒ (wan accept ✓ accept ✓ Image: Second sec			•

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

		Firewall-Zone Settings
Item		Description
General	This section defin	es the general properties of "lan". The inbound data and

Setting	outbound traffic i forwarding strate	otions are used to set the default strategy for inbound and n this area, and the forwarding options describe the traffic gy between different networks in the area. The covered
		es the networks belonging to this area.
	Name	lan
	Input	Default is accept
	Output	Default is accept
	Forward	Default is accept
		The LAN port does not need to be set, and the WAN port
	IP Dynamic	address may change during dynamic allocation. You need
	camouflage	to set up dynamic disguise to connect to the external network
	MSS Clamp	Automatically adjust MSS according to MTU
	Covered networks	lan
	Allow forwarding to	wan
	target area	wan
	Allow	
	forwarding from	unspecified
	source area	
	(lan) and other a lan. The forward areas whose dest example, forward	tions control the forwarding strategy between this area reas. The target area receives the forwarded traffic from ing traffic matching the source area comes from other ination is lan. The role of forwarding rules is one-way. For ing traffic from lan to wan does not mean allowing reverse fic from wan to lan.
	Covered equipment	This option can classify regional traffic on original, non-UCI-hosted network devices.
	Subnets covered	This option can classify regional traffic by source or destination subnet instead of network or device.
Advanced settings	Restricted address	IPv4,IPv6
	To restrict the source subnet of IP dynamic masquerading	Default is empty
	Target subnets to restrict IP dynamic masquerading	Default is empty
	Enable logging in this area	Default is disable
Conntrack setting	Allow "invalid traffic"	Do not install additional rules to deny forwarded traffic with conntrack status invalid. This may be a necessary setting for complex asymmetric routing, default is disable



	Automatic assistant assignment	Automatically assign conntrack assistant according to traffic protocol and port, default is enable.					
Additional	classification rule the interface or s	ptables parameter to the source and destination traffic s, you can match packets based on other conditions than subnet. Use these options with extreme caution, as invalid the firewall rule set and expose all services to the outside					
iptables parameter	Additional source parameters Additional target parameters	 Additional iptables parameters are used to classify regional inflows. For example: -p tcpsport 443 only matches inbound HTTPS traffic. Additional iptables parameters are used to classify regional outgoing traffic. For example: -p tcpdport 443 only matches outbound HTTPS traffic. 					

5.4.8.2 Port forwards

(••) R40B - Port Forwards - Lu	ci × +				- 0 ×					
← → C ▲ Not sec	ure 192.168.3.1/cgi-bin/lu	uci/admin/network/firewall/f	forwards		☆ 🔒 :					
	R40B Status - Sys	stem - Services - Network	 vPN → Serial Port → RTU I/O 	 Logical operation - Cloud platform - Logout 						
	General settings Port Forwards Traffic Rules Custom Rules Firewall - Port Forwards Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.									
	Port Forwards									
	Name	Match	Forward to	Enable						
	Add									
	Save & Apply - Save Reset									
	Powered by KingPigeon Technology Co., Ltd. (v1.18) / 2020-10-16									

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

Firewall-Port Forwarding						
Item		Description				
	Name	Forward naming				
	Protocol	TCP+UDP,TCP,UDP,ICMP optional				
	Source area	wan				
General Setting		Match inbound traffic to the specified				
General Setting	External port	target port or target port range on this				
		host				
	Target area	lan				
	Internal IP address	Redirect matching inbound traffic to the				



		specified internal host				
	Internal port	Redirect matching inbound traffic to the				
	internal port	port of the internal host				
	Source MAC address	Match only inbound traffic from these				
	Source MAC address	MACs				
	Source IP address	Only match inbound traffic from this IP or				
		IP range				
	Source port	Only match inbound traffic originating				
Advanced settings		from a given source port or source port				
Auvanceu settings		range on the client host				
		Only match inbound traffic for the				
	LAGEINALIF AUGLESS	specified destination IP address				
	Enable NAT loopback	Default is enable				
	Additional parameters	Extra parameters passed to iptables. use				
	Additional parameters	caution!				

5.4.8.3 Traffic rules

→ C (A Not secure 192.16	8.3.1/cgi-bin/luci/admin/network/firewall/rules				☆ €
	R40B	Status + System + Services + Network + VPN + Serial Port + RT	U I/O 🗕 Logical ope	eration -	Cloud platform - Logout	
	General set	tings Port Forwards Traffic Rules Custom Rules				
	Firewa	II - Traffic Rules				
		define policies for packets traveling between different zones, for example to reject tr	affic between certain h	osts or to	o open WAN ports on the router.	
	Traffic R					
	Name	Match	Action	Enabl	le	
	Allow-	IPv4-UDP				
	DHCP-	From any host in wan	Accept input	~	≡ Edit Delete	
	Renew	To any router IP at port 68 on this device				
	Allow-	IPv4-ICMP with type echo-request				
	Ping	From any host in wan	Accept input		≡ Edit Delete	
	T mg	To any router IP on this device				
	Allow-	IPv4-IGMP				
	IGMP	From any host in wan	Accept input	-	≡ Edit Delete	
	IOM	To any router IP on this device				
		IPv6-UDP				
	Allow- DHCPv6	From IP fc00::/6 in wan	Accept input		≡ Edit Delete	
	DHCPV6	To IP fc00::/6 at port 546 on this device				
		IPv6-ICMP with types 130/0, 131/0, 132/0, 143/0				
	Allow-	From IP fe80::/10 in wan	Accept input		≡ Edit Delete	
	MLD	To any router IP on this device				
		IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big,				
	Allow-	time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-	Accept input and			
	ICMPv6-	solicitation, router-advertisement, neighbour-advertisement	limit to 1000 pkts.		Edit Delete	
	Input	From any host in wan	per second			

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

5.4.8.3 Custom rules

		46 WIREless Indi			outer Ita Connec	tivity
(**) R40B - Traffic Rules - LuCI	× +					- 0 ×
← → C ▲ Not secu	ire 192.16	8.3.1/cgi-bin/luci/admin/network/firewall/rules				☆ \varTheta :
	R40B	Status - System - Services - Network - VPN - Serial Port - RT	U I/O 👻 Logical ope	eration + (Cloud platform - Logout	î.
	Firewa	tings Port Forwards Traffic Rules Custom Rules III - Traffic Rules define policies for packets traveling between different zones, for example to reject tr ules	affic between certain h	osts or to op	pen WAN ports on the router.	
	Name	Match	Action	Enable		
	Allow- DHCP- Renew	IPv4-UDP From <i>any host</i> in wan To <i>any router IP</i> at port 68 on this device	Accept input		Edit Delete	
	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input		Edit Delete	
	Allow- IGMP	IPv4-IGMP From any host in wan To any router IP on this device	Accept input		Edit Delete	- 1
	Allow- DHCPv6	IPv6-UDP From IP /c00::/6 in wan To IP /c00::/6 at port 546 on <i>this device</i>	Accept input		Edit Delete	
	Allow- MLD	IPv6-ICMP with types 130/0, 131/0, 132/0, 143/0 From IP fe8/0.//0 in wan To any router IP on this device	Accept input		Edit Delete	
	Allow- ICMPv6- Input	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour- solicitation, router-advertisement, neighbour-advertisement From any host in wan	Accept input and limit to 1000 pkts. per second		Edit Delete	

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

5.5 VPN

5.5.1 IPSec

(1) R40B - IPSec - LuCI	× +							- ø ×
← → C ▲ Not sect	ure 192.168.3.	1/cgi-bin/luci/admi	n/vpn/ipsec#					☆ 🛛 :
	R40B St	atus + System +	Services - Netwo	rk ▼ VPN ▼ Serial Por	t + RTU I/O + Logical ope	eration - Cloud platform -	Logout	
	IPSec Security Al	liance						
	Name	Tunnel ends			State	Running time		
				This section contains n	o values yet			
	Security Po Below is a list of	olicy i configured IPSec inst	ances and their curre	nt state				
	Name	Remote Gateway	r	Remote Subnet	Local Subnet	Enable		
				This section contains n	o values yet			
		A	bb					
						Save & Apply Save	Reset	
	Powered by Kin	gPigeon Technology C	o., Ltd. (v1.18) / 2020	-10-16				

IPSec is an open network layer security framework protocol formulated by the Internet Engineering Task Force (IETF). It is not a single protocol, but a collection of protocols and services that provide security for IP networks. IPSec mainly includes security protocols AH (Authentication Header) and

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

ESP (Encapsulating Security Payload), key management exchange protocol IKE (Internet Key Exchange) and some algorithms used for network authentication and encryption.

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

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

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

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

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

		IPSec
ltem		Description
	enable	Tick to enable
	Package type	Optional tunnel mode, transmission mode. Tunnel mode means host-to-host, host-to-subnet or subnet-to-subnet tunnel. The transmission mode indicates the transmission method from the
IPSec	Door gotowov	host to the host.
Configuration Phase 1 settings	Peer gateway	Peer gateway which connect with IPSEC
	Local subnet IP/mask	In the tunnel mode, the tunnel from the subnet to the subnet needs to specify the local and opposite terminal network ranges
	Peer Subnet	In the tunnel mode, the tunnel from the subnet to the subnet
	IP/Mask	needs to specify the local and opposite terminal network ranges
	Pre-shared key	Default authenticate using pre-shared key
Pre-shared key		Phase 1 mainly negotiates encryption parameters, exchanges key information, and verifies device identity
Phase 1 settings IKE Encryption Algorithm		Specify IKE (Internet Key Exchange) negotiation message encryption algorithm
Authentication a	algorithm	Specify the digital signature authentication algorithm for encrypted messages
IP/Mas Pre-sha Phase 1 settings IKE Encryption Algorithm Authentication algorithm DH group		Specify which key group to use for DH (DiffieHellman) key exchange
IKE version		IKEv1 or IKEv2
Exchange mode		Main mode or brutal mode. The main mode is more secure than the brutal mode, and the brutal mode is faster. If the responder (server) cannot know the address of the initiator (end user) in advance, or the address of the initiator is always changing, and both parties want to use the pre-shared key authentication method to create an IKE SA, Brutal mode can be used at this time
Negotiation mod	de	Responder or initiator, the initiator is equivalent to the end user, and the responder is equivalent to the server
Local ID		Can be IP address, standard domain name, email address or proper name, default is local IP
Peer ID		Can be IP address, standard domain name, email address or



4G Wireless Industrial Router Wireless Data Connectivity

	proper name, default is peer IP						
IKE live time	Re-negotiate the key time						
Phase 2 setting	The purpose of Phase 2 is to establish an IPSec security association for data transmission						
ESP Encryption Algorithm							
Authoritication algorithm	Specify digital signature authentication algorithm for encrypted						
Authentication algorithm	data						
DES group	PFS (Perfect Forward Secrecy), which means that a key is cracked						
PFS group	and does not affect the security of other keys						
Survive time	How long should it take from the negotiation to the connection						
Survive time	instance						
	DPD (Dead Peer Detect), When no traffic occurs for a period of						
DPD detection cycle	time, the local end sends a DPD message to check the status of						
	the peer before sending traffic						

5.5.2 L2TP

L2TP (Layer 2 Tunneling Protocol, Layer 2 Tunneling Protocol) is a type of VPDN (Virtual Private Dial-up Network, Virtual Private Dial-up Network) tunneling protocol.

VPDN (Virtual Private Dial Network) refers to the use of public network (such as ISDN and PSTN) dial-up function and access network to achieve a virtual private network, providing access services for enterprises, small ISPs, and mobile office personnel.

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

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

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



••) R40B - L2TP - LuCI	× +						- 0	×
- > C A Not sec	cure 192.168.	3.1/cgi-bin/luci/admin	/vpn/l2tp				☆	0 :
	R40B	Status - System - S	Services - Network - VPN	I ≁ Serial Port ≁ RTU I/O ≁	Logical operation - Clo	ud platform → Logout		
	L2TP							
	L2TP inst	ances						
	Below is a list	of configured L2TP instar	nces and their current state					
	Name	User Name	Server/Client	IPSec Encryption	State	Enable		
			This se	ction contains no values yet				
		Add	d					
					Save & Appl	y Save Reset		
	Powered by K	(ingPigeon Technology Co	., Ltd. (v1.18) / 2020-10-16					

	L2TP
Item	Description
Enable	Tick to enable
Username	User name for PPP authentication
Password	Password for PPP authentication
Server/client	Server, client optional
Server address	LNS (L2TP Network Server, L2TP network server) address
IPSec encryption	You can choose whether to use IPSec encryption or not, and choose to use the default IPSec security policy during encryption. You do not need to manually configure IPSec. When you choose to use a security policy, you need to configure the IPSec policy in advance
Pre-shared key	When selecting encryption, you need to set the IPSec pre-shared key
Security strategy	Configured IPSce security policy

5.5.3 OpenVPN

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

The virtual network card is a driver software implemented using the underlying network programming technology, and can be configured like other network cards. If the application accesses a remote virtual address (belongs to the address series used by the virtual network card, which is different from the real address), the operating system will send data packets (TUN mode) or data frames (TAP mode) to the virtual network card through the routing mechanism. After the service program receives the data and performs corresponding processing, it is sent from the external network through SOCKET, and the remote service program receives the data from the

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

external network through SOCKET, and after corresponding processing, it is sent to the virtual network card, and the application software can receive At this point, a one-way transmission process is completed, and vice versa. OpenVPN provides two virtual network interfaces: universal Tun/Tap driver, through which you can establish a layer 3 IP tunnel or a virtual layer 2 Ethernet. The latter can transmit any type of layer 2 Ethernet data, and the transmitted data can be passed through the LZO algorithm compression.

The SSL protocol (Secure Socket Layer) mainly uses the public key system and X.509 digital certificate technology to protect the confidentiality and integrity of information transmission. It includes: server authentication, client authentication (optional), SSL chain Data integrity on the road and data confidentiality on the SSL link. The SSL protocol is independent of the application layer protocol. High-level application layer protocols (such as HTTP, FTP, Telnet, etc.) can be transparently built on the SSL protocol. The SSL protocol has completed the encryption algorithm, communication key negotiation and server authentication before the application layer protocol communication. After that, the data transmitted by the application layer protocol will be encrypted to ensure the privacy of the communication.

(••) R40B - OpenVPN - LuCI	× +							- 0 ×
← → C ▲ Not secu	re 192.168.3.	1/cgi-bin/luci/admin/v	pn/openvpn					☆ \varTheta :
- -	R40B st	tatus - System - Ser	vices - Network - VPN	 Serial Port 	- RTU I/O - Logical	operation - Cloud p	latform - Logout	
	OpenVP	'N						
	OpenVPN i Below is a list of		ances and their current state					
	Name	Mode Protocol	Remote Address	Port	TUN/TAP device	Connected	Enable	
			This sec	ction contains no	values yet			
		Add)					
						Save & Apply	Save Reset	
	Powered by Kin	gPigeon Technology Co., L	td. (v1.18) / 2020-10-16					

	OpenVPN
Item	Description
Enable	Tick to enable
Configure client mode	Tick to client mode
VPN Subnet IP address/mask	TAP mode, as a server, it can transmit from host to subnet
Server address	Server address which establish VPN connect with client
Port	The TCP/UDP port provided by the server for establishing a connection, default is 1194
Protocol	UDP,TCP-Server,TCP-Client,default is UDP.
TUN/TAP device	TUN mode establishes a three-layer tunnel to achieve point-to-point transmission. TAP mode establishes a Layer 2 tunnel, which can realize the transparent transmission of IP packets
Username/passwrod	When security certificate authentication is not applicable, user

	name/password authentication can be used
Encryption Algorithm	Choose data encryption algorithm
Authentication and	Coloct file upload root cortificate provided by conver
authorization (root certificate)	Select file upload, root certificate provided by server
Local certificate	Select file upload, the client certificate generated by the user based
	on the root certificate
Local private key	Select the file upload, the key corresponding to the client certificate
DH Koy ovchange parameters	Used for key exchange, can be generated by openssl dhparam -out
DH Key exchange parameters	dh2048.pem 2048
Compression algorithm	LZO,LZ4
Keepalive interval (seconds)	The interval at which the server sends a probe message to the client
Kaanaliya timaayut (sacanda)	If the server does not receive a response to the probe message at
Keepalive timeout (seconds)	this time, it restarts the connection

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

5.6 Serial Port

5.6.1 Serial Port settings

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

5.6.2 Serial Port Application



46 Wireless Industrial Router Wireless Data Connectivity

(··) R40B - Serial Port Applicatio	on × +								- 0 ×
← → C ▲ Not secur	re 192.168.3	3.1/cgi-bin/luci/a	dmin/serial/ser2ne	t					☆ Θ :
	R40B \$	Status - System		twork - VPN -	Serial Port 👻 RTU I	D 👻 Logical operati	on - Cloud platform -	Logout	
	Serial P Serial State	Port							
	Index	Serial Name	Serial Type	Received	Bytes	ransmitted Bytes	Clear Statio	tis	
				This section	contains no values yet				
	Parameter	r Setting							
	Device	Baudrate	Usage Mode	Net Protocol type	Host IP or	lomain Po	rt		
							Edit	Delete	
							Edit	Delete	
	Add								
							ave & Apply Save	Reset	

Powered by KingPigeon Technology Co., Ltd. (v1.18) / 2020-10-16

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

5.6.3 Modbus Master



(••) R40B - Modbus Master - LuCI 🗙	× +										-	٥	×
← → C ▲ Not secure	192.168.3.1/	'cgi-bin/luci/ad	min/serial/mo	dbus							☆	Θ	:
R4	0B State	us + System +	Services -	Network -	VPN - Serial Port -	rtu I/o -	Logical operation	- Cloud	l platform -	- Logout			
	odbus I odbus Sett									ISAVED CHANGES: 1			
Na	Alias ame	Slave Address		Function Code	Register Start Address	Data Number	Mapping Address	Enable	Query	Detail Settings			
				Th	is section contains no ve	alues yet							
			Add										
							Sav	e & Apply	Save	Reset			
Pow	vered by KingP	Pigeon Technology	v Co., Ltd. (v1.18	i) / 2020-10-16									

R40B s	Status - System -	Services -	Network -	VPN	l ▼ Serial Port ▼	rtu I/o 🗸	Logical operation -	Cloud platform -	Logout		
Config Config De								TUN SAV	ED CHANGES: 13		
Mapping Address	Alias	Data Type	Input Typ	be	Confirm time(s)	Enable alarm	Action	Hold time(s)	Publish		
64		Bool	Open	~			None 🗸				
65		Bool	Open	•			None 🗸				
66		Bool	Open	•			None 🗸				
67		Bool	Open	~			None 🗸				
68		Bool	Open	•			None 🗸				
69		Bool	Open	•			None 🗸				
70		Bool	Open	•			None 🗸				
71		Bool	Open	•			None 🗸				
			Open				None 🗸				

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

Modbus Master	
Item	Description
Enable	Tick to enable
Slave address	Slave Modbus device ID, If the cloud connection setting
	selects Modbus protocol, please set an address different
	from the local Modbus device ID
Register type	Boolean,16-bit, 32-bit, 64-bit
Function code	01,02,03,04;
	01/02 Function codes apply to Boolean data types, 03/04

KING PIGEON



4G Wireless Industrial Router Wireless Data Connectivity

		Function codes apply to 16/32/64 bit data type;
		01 function code supports 05/15 function code at the same
		time, 03 function code supports 06/16 function code at the
		same time.
Register start address		Set according to slave register address
Data number		Set according to the number of slave registers
Mapping address assignment		Automatic / manual
Mapping start address		Select Manual Assignment Visible;
		Boolean type mapping register address 64~127,
		16 bit type mapping register address 20000~20127,
		32 bit type mapping register address 20128~20254,
		64 bit type mapping register address 20256~20508
Timed reading cycle (se	conds)	Data collection cycle
		RS485,RS232,Ethernet
Slave interface		If RS485 or RS232 is already connected as a serial device,
		this is not visible here
Slave IP address		Visible when selecting Ethernet
Port		Visible when selecting Ethernet
	Can be set when slav	e interface select RS485 or RS232
	Device	RS485 or RS232
		1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600,
Serial setting	Baud rate	115200, 230400
	Data bits	5,6,7,8
	Parity Bit	None, Even and Odd optional
	Stop Bit	1,2
	Mapping address	Slave register address
	Data type	Slave register data type
	Input type	Boolean data type is visible
	Coefficient	16/32/64 bit data type is visible, ratio coefficient between
Detailed configuration		register value and real value
	Confirm time (s)	16/32/64 bit data type is visible,
		Over-threshold confirmation trigger time
	High threshold	16/32/64 bit data type is visible
	Low threshold	16/32/64 bit data type is visible
	Action	Linkage local DO close or open
	Hold time	Do action time
	Publish	Tick to publish data via MQTT



5.7 RTU IO

5.7.1 E-mail & SMS

(*) R40B - Email&SMS Setting - L × +	- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/io/email	☆ \varTheta :
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	
UNSAVED CHANGES*13	
Email	
Email Setting	
Enable send email	
Email Server smtp.xxx.com	
Port 25	
Recipient name recipient@xxx.com	
Sender name sender@xxx.com	
User Name user name	
Password *	
SMS Setting	
This section contains no values yet	
Save & Apply Save Reset	

Powered by KingPigeon Technology Co., Ltd. (v1.18) / 2020-10-16

E-mail setting		
Item	Description	
Enable send mail	Tick to allow send e-mail	
Mail Server	Enter the SMTP mail server address	
Port	Enter the SMTP mail server port number	
Recipient name Enter mail receiving address, you can add multiple, enter address and click the "+" on the right to save, at the sa time the second input box will appear below, you continue to add or leave blank to no longer add		
Sender name	Enter the email sending account address	
User name	Enter the email sending account username	
Password	Enter the email sending account address password	

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

5.7.2 Digital input/output

2442	8.3.1/cgi-bin/luci/ad					· · · · · · · · · · · · · · · · · · ·		z
R40B	Status - System -	Services - Netw	vork - VPN - S	Serial Port - RT	UI/O ▼ Logical	operation - Cloud	platform - Logout	
DIDO DI							UNSAVED CHANGES: 15	J
Index	In Name	Mode	State	Count	Clean	Enable/Disable		
1	DI1	in	Low	0	Clean	Enabled		
2	DI2	in	Low	0	Clean	Enabled		
DO								
Index	In Name	Mode	State	Set State	Enable/Disable			
1	DO1	out	Low	Set High	Enabled			
2	DO2	out	Low	Set High	Enabled			
Trigger S	etting							
In Name	Trigger Condition	Threshold Value	Confirm Time	(s) Action	Hold Time(s) Triggering		
DI1	DI Low	0	44	Reboot		Not trigger	Edit Delete	
DI2	DI Low	0	1	DO2Close	5	Not trigger	Edit Delete	

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

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



5.7.3 Analog input

R40B Status - S	System - Services - Network - VPN	- Seria	Il Port ∓ RTU I/O ∓	Logical ope	ration - Cloud plat	form - Logout	\$
AIN AIN Seting						UNSAVED CHANGES: 15	
In Name	Mode	ľ	Min Value Ma	ax Value	Curent Value	Unit	
AIN1	Voltage 0-5V	•			0.005609		
AIN2	Voltage 0-5V	•			0.004327		
AIN3	Voltage 0-5V	•			0.007372		
AIN4	Voltage 0-5V	•			0.004648		
Trigger Setting							
In Trigger Name Condition	Threshold Resume Value Threshold	Con Tim	firm Action e(s)	Hold Time(s)	Triggering		
						Edit Delete	
Add							
					Save & Apply	Save	

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

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

5.7.4 Device Monitor



(••) R40B - Device Monitor&Ala	rm × +							-	٥	×
← → C ▲ Not secur	re 192.168.3.1/cgi-b	in/luci/admin/io/monite	or					r	9	:
	R40B Status +	System - Services -	Network - VPN - Se	rial Port + RTU I/C) - Logica	l operation 👻 Clou	d platform 👻 Logout			
	Device Moni	tor					UNSAVED CHANGES: 15			
	Device Monitor									
	Register Address	In Name Status	Device IP Address	Ping Times	Action	Hold time(s)	Enable setting			
			This section cor	ntains no values yet						
	Add									
						Save & Apply	Save Reset			
	Powered by KingPigeon	Technology Co., Ltd. (v1.18	3) / 2020-10-16							

Up to 20 IPs can be set to detect

	Device Monitor						
Item	Description						
Register address	Range 2~63						
In name	DI3~DI64, Automatically generated according to the register						
III name	address, MQTT report data identifier						
Device IP address	Detect IP						
	According to the set value PING how many times, if there is no						
PING times	PING, then the detection equipment is disconnected from the						
	network						
Action	Linkage DO close or open						
Hold time (seconds)	DO action time						
Trriggering	Tick to enable alarm						

5.7.5 Event and Alarm

4G Wireless Industrial Router Wireless Data Connectivity

(••) R40B - Alarm Setting - LuC	1 × +							-	٥	×
\leftrightarrow \rightarrow C A Not secu	ıre 192.168.3.1/cgi-l	oin/luci/admin/io	/alarm					☆	0	:
	R40B Status +	System - Ser	vices - Network -	VPN - Serial Port	- RTU I/O -	Logical operation - Clou	ud platform 👻 Logout			
							UNSAVED CHANGES: 15			
	Event And A	Alarm								
	Index	Alarm Name		Alarm Description		Alarm Ti	ime			
				This section contains no	values yet					
	Add Alarm									
	Alarm Name	Send	SMS Short Mes	sage Content	Send Email	Email Content				
	DI1:open	× 🗹					Delete			
	DI1:open	 ✓ 					Delete			
	DI1:open	¥ 🔽					Delete			
	Add									
						Save & Apply	y Save Reset			
	Powered by KingPigeo	n Technology Co., L	td. (v1.18) / 2020-10-	16						

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.

5.7.6 Timer

(··) R40B - Timer - LuCI	× +	- 0 ×
← → C ▲ Not sect	ure 192.168.3.1/cgi-bin/luci/admin/io/timer	☆ \varTheta :
	R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	
	Timer	
	Please make sure that the time set is consistent with your time zone	
	Cycle Timer	
	Week day Hour Minute Action Enable	
	This section contains no values yet	
	Add	
	Once Timer	
	Month Day Hour Minute Action Enable	
	This section contains no values yet	
	Add	
	Save & Apply Save Reset	
	Powered by KingPigeon Technology Co., Ltd. (v1.18) / 2020-10-16	

Timed task: can choose to close or open DO, send mail, and restart.

Cycle timer: can be executed daily or weekly.

Once timer: can be executed regularly according to the specified date



5.8 Logical Operation

(*) R408 - Logical operation - LuC × +	- ø ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/logic/logic	☆ \varTheta :
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	
Logical operation	
Bool input	
Name Input1 Condition Relationship Input2 Condition Output Address Output Value Logic Value	
1 REG64 Open Logic And DI1 Open REG64 Open 1 Edit Delete	
Add	
Numberical input	
Name Input1 Condition Threshold Relationship Input2 Condition Threshold Output Address Output Value Logic Value	
This section contains no values yet	
Add	
Combined input	
Name Input1 Condition Relationship Input2 Condition Output Address Output Value Logic Value	
This section contains no values yet	
Add	-

Provides powerful local logic operation function, and can freely set various combinations between local I/O (digital input and output, analog input) and slave I/O (slave register set by Modbus master) Linkage.

5.9 Cloud Platform

5.9.1 Private Cloud

(••) R40B - Custom Cloud - LuCI × +					- 5 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/a	admin/cloud/host_set				☆ 🛛 :
	✓ Services ✓ Network ✓	VPN ≁ Serial Port ≁ R	TU I/O + Logical operation +	Cloud platform - Logout	
Cloud connection	_				
Cloud connection sett	ings				
Enable setting					
Cloud platform	King Pigeon IIoT V2	~			
Link Protocol	MODBUS RTU	~			
Modbus Device ID	1 Ø Modbus device ID is set in	Serial Port Settings			
Register Packet					
Heartbeat Packet					
Heartbeat Response Packet					
Heartbeat Period(s)	60				
Host Silence Time(s)	600				
			Save &	Apply Save Reset	
Powered by KingPigeon Technology	ogy Co., Ltd. (v1.18) / 2020-10-1	6			
	Cloud	d Connection S	ettings		

KING PIGEON



4G Wireless Industrial Router Wireless Data Connectivity

Item		Description					
Enable setting		Tick to enable					
Cloud Platform		King Pigeon IIOT V2,IIOT V3,others					
Host IP or domain 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					
	Register packet	Server register handshake protocol package, if need contact salesman					
Modbu Protocol Parameters	Heartbeat packet	Heartbeat content to avoid network offline					
	Heartbeat response packet	The server responds to the heartbeat packet					
	Heartbeat period (s)	Network keep online heartbeat interval time					
	Host Silence time (s)	The server sends silent time without data, and will reconnect if it times out					
	MQTT Client ID	The client identifier used in the MQTT connection message, the server uses the client identifier to identify the client, and each client connected to the server has a unique client identifier.					
	Username	The user name used in the MQTT connection message, which can be used by the server for authentication and authorization.					
	Password	The password used in the MQTT connection message, which can be used by the server for authentication and authorization.					
MQTT Protocol	Publish topic	The subject name used in the MQTT publish message. The subject name is used to identify the information channel to which the payload data should be published. The subject name in the publish message cannot contain wildcards.					
Parameters	Subscribe topic	The topic name used in MQTT subscription messages. After the subscription, the server can send publish messages to the client to achieve control.					
	Publish Period (seconds)	MQTT data timing publish interval					
	Publisher QOS	Service quality level guarantee for application message distribution: 0-at most once, 1-at least once, 2-only once					
	Encryption	Optional unencrypted, encrypted (root certificate), encrypted (self-signed)					
	Authentication and authorization (root certificate)	Choose file upload					
	Local certificate	Choose file upload					
	Local private key	Choose file upload					
	Enable data transfer	Enable to work					



5.9.2 Ali Cloud

(••) R40B - Ali Cloud - LuCl	× +							_	٥	×
← → C ▲ Not sect	ure 192.168.3.1/cgi-bin/luci/a	admin/cloud/ali_cloud						4	θ	:
	R40B Status - System	- Services - Network - VF	PN - Serial Port -	RTU I/O - L	ogical operation -	Cloud platform -	Logout			
	Cloud connection	n settings				UNSAVE	D CHANGES: 15			
	Cloud connection setti	_								
	Enable setting									
	Authentication method	Device Serect	×							
	Product Key(ProductKey)									
	Device Name(DeviceName)									
	Device Serect(DeviceSerect)									
	Region ID	Please choose	•							
	Publish Period(s)	> 60								
					Save &	Apply Save	Reset			
	Powered by KingPigeon Technolo	rgy Co., Ltd. (v1.18) / 2020-10-16								

Ali Cloud Connection Settings Item Description Tick to enable Enable setting Authenticatioin method Device secret key, X509 certificate **Product Key** Set the product key on Alibaba Cloud **Device Name** Set the device name on Alibaba Cloud **Device Serect** Set the device key on Alibaba Cloud **Region ID** Ali cloud region Publish period (seconds) >60 Certification authority (root certificate) Choose file upload Local certificate Choose file upload Local key Choose file upload

5.9.3 AWS Cloud



(··) R40B - Aws Cloud - LuCI × + ٥ → C A Not secure | 192.168.3.1/cgi-bin/luci/admin/cloud/aws_cloud 4 ☆ 0 1 R40B Serial Port - RTU I/O - Logical operation - Cloud platform -Logou Cloud connection settings **Cloud connection settings** Enable setting Host(EndPoint) Client ID Thing Name Publish Topic Publish Period(s) >= 60 Certificate authority Select file... /etc/mqtt/root.crt Local certificate Select file... /etc/mqtt/local.crt Local private key Select file... /etc/mqtt/private.key

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

5.10 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

(+) R40B - Custom Cloud - LuCI × +		- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/	dmin/cloud/host_set	☆ \varTheta :
R40B Status - System	Services Network VPN Serial Port RTU I/O Logical operation Cloud platform Logout	
Cloud connectio	n settings	
Cloud connection set		
Enable setting		
Cloud platform	King Pigeon IIoT V2 🗸	
Link Protocol	MODBUS RTU 🗸	
Modbus Device ID	1 Ø Modbus device ID is set in Serial Port Settings	
Register Packet		
Heartbeat Packet		
Heartbeat Response Packet		
Heartbeat Period(s)	60	
Host Silence Time(s)	600	
	Save & Apply Save Reset	
Powered by KingPigeon Technol	gy Co., Ltd. (v1.18) / 2020-10-16	

1. Set the platform server IP and port, select Modbus RTU protocol and set the local Modbus device ID (the effective range of Modbus device ID is 1^{247})

 Set relevant message information according to the platform to be connected (if not, you can not set it) [Registrer Package]: The registration package sent by the device to the server when connected to the server. [Heartbeat Packet]: A heartbeat packet sent by the device to the server to maintain the connection. [Heartbeat period]: The heartbeat packet sending period.

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

6.1.2 Read Device Register Address

6.1.2.1 DI / DO / AI DI pulse counter Register Address

Modbus Register Address(Decima I)	PLC or configuration address (Decimal)	Data Name	Data Type	Description
0	10001	DI1	Bool	Dry contact: 0: Open

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



					1: Close
	1		CLO CLO		Wet contact:
	T	10002	DI2		0: Low level (0~1VDC)
					1: High level (5~30VDC)
			Network		
	2~21 10003~1002		disconnection 10003~10022 detection device IP		0:offline
		10003~10022			
			(max 20 IPs can be		1:online
			set)		

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

Modbus Register Address(Decima I)	PLC or configuratio n address (Decimal)	Data Name	Data Type	Description
0	00001	DO1	Deel	0: Open
1	00002	DO2	Bool	1: Close

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

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

6.1.2.2 Read Device Digital input Status

Master Send Data Format

Content	Byte	Data	Description
Device address	1	01H	01H Device, Range: 1-247, according to setting
			address
Function code	1	02H	02 read input coil DIN status
DIN Register address	2	00 00H	Range:0000H-0001H,stands for DI1-DI2
Read DIN register Qty	2	00 02H	Range:0001H-0002H, read qty of DIN status
16CRC verify	2	F9 CBH	CRC0 CRC1 low byte in front, high byte behind

Receiver Return Data Format

Content	Byte	Data	Description
Device address	1	01H	01H Device, according to setting address
Function code	1	02H	Read input holding coil
Return bytes Qty	1	01H	Return data length

KING PIGEON

IG Wireless Industrial Router Wireless Data Connectivity

Returning data	1	01H	Return DI data
16CRC Verify	2	6048H	CRC0 CRC1 low byte in front, high byte behind

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

Server send: 01 02 00 00 00 02 F9 CB

01= Device address; 02= Inquiry DIN status; 00 00= DIN Starting address; 00 08= Serial reading 2 DIN status; F9 CB = CRC verify.

Device return: 01 02 01 01 60 48

01= Device address; 02= Inquiry DIN status; 01= Returning data bytes qty; 01= DIN status, each byte stands for one DIN status, 01H converter to binary 0000 0001 from low to high byte, stands for DIN1-DIN2 status, 0= Open, 1= Close.

DI2	DI1
0	1
Open	Close

60 48: 16 byte CRC verify.

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

6.1.2.3 Read Device Digital Output DO Status

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read the hold coil, function code 01
Register Starting Address	2	00 00H	Range: 0000H-0001H, stands for DO1-DO2
Read Register Qty	2	00 02H	Range: 0000H-0001H
16 CRC Verify	2	BD CBH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

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

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

Server Send: 01 01 00 00 00 02 BD CB

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

Device Answer: 01 01 01 02 DO 49

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

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

DO2	D01			
1	0			
Close	Open			

D0O49: 16 byte CRC verify

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

6.1.2.4 Control Device Digital Output Status

1) Control 1 channel o	device DO output
------------------------	------------------

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description		
Device Address	1	01H	01H Device, Range: 1-247, according to setting address		
Function Code	1	05H	Write single holding coil type, function code 05		
DO Register Address	2	00 00H	Range: 0000H-0003H		
Active	2	FF 00H	This value: FF 00H or 00 00H, FF 00H= Close relay, 00 00H= Open relay		
16CRC Verify	2	8C 3AH	CRC0 CRC1 low byte in front, high behind		

Receiver Return Data Format:

Content	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 type		
DO Register Address	2	00 00H	Range: 0000H-0003H		
Active	2	FF 00H	This value: FF 00H or 00 00H, FF 00H= Already actived close relay, 00 00H= Already actived open relay		
16CRC Verify	2	8C 3AH	CRC0 CRC1 low byte in front, high behind		

Example: Control relay DO1 close, then:

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

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

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

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

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

2) Multiple Control DO outputs

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	0FH	Write multi holding coil, function code 15
DO Starting Register Address	2	00 00H	Range: 0000H-0001H, stands for DO0-DO1
Control Relay Qty	2	00 02H	Range: 0000H-0001H
Write Byte Qty	1	01H	Write 1 byte, since device only 2DO, use 4 binary can do it
Writing Data	1	03H	Send status data to control DO
16CRC Verify	2	9E 96H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description	
Device Address	1	01H	01H Device, according to the data Master send	
Function Code	1	OFH	Write multi holding coil type	
DO Register Address	1	00 00H	Range: 0000-0001, stands for DO1-DO2	
Active	1	00 02H	Range:0001H-0002H, stands for already actived relays	
16CRC Verify	2	D4 0AH	CRC0 CRC1 low byte in front, high behind	

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

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

01= Device address; 0F= Control multi relay; 00 00= Relay DO0 starting address; 00 02= Control 2 relays; 01= Send data qty; 03= Data sent converter to binary 0000 0011 from low to high stands for DO1-DO2 status, 0stands for open relay,1 stands for close relay:

DO2	D01	
1	1	
Close	Close	

9E 96 CRC verify.

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

01= Device address; 0F= Control multi relay; 00 00= Relay DO0 starting address; 00 02= Actived 2 relays; D4 0A CRC verify.

6.1.2.5 Read Device AIN Status and DIN Pulse counter

Master Send Data Format:



Content	Bytes	Bytes Data Description (H: HEX)				
Device Address	1	01H	01H Device, Range: 1-247, according to setting address			
Function Code	1	04H	Read input register, function code 04			
Register Starting Address	2	00 00H	Every 2 16-bit address corresponds to 1 AI 32- register			
Read Register Qty	2	00 OCH	A total of 12 16-bit addresses are read, each of the two 16-bit addresses is combined into a 32-bit address, a total of 6 32-bit addresses, that is, the number of read AI 4 and the DI pulse count 2			
16 CRC Verify	2	FOOFH	CRC0 CRC1 low byte in front, high behind			

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H device, consistent with download data
Function Code	1	04H	Read the hold coil
Return Bytes Qty	1	18H	Return data length
Returning Data	16	3B 98 4E 40 40 80 00 00 3C 89 15 BE 3B D7 51 8B 00 00 00 03 00 00 00 06H	Return AI data,32-bit float,ABCD
16 CRC Verify	2	22 80H	CRC0 CRC1 low byte in front, high behind

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

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

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

Device return: 01 04 18 3B 98 4E 40 40 80 00 00 3C 89 15 BE 3B D7 51 8B 00 00 00 03 00 00 06 22 80 01= Device address; 04= read input register; 18= Return data bity ; 3B 98 4E 40 40 80 00 00 3C 89 15 BE 3B D7 51 8B 00 00 00 03 00 00 00 6=return data, detail as follows:

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

22 80: CRC verify.

6.1.3 Read Mapping Address

6.1.3.1 Mapping Register Address

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

Modbus Register Address(Decim al)	PLC or configuration address (Decimal)	Data Name	Data Type	Description
64	00065 or 10065	Bool 64	Bool	De alexante a c
65	00066 or 10066	Bool 65	Bool	Boolean type,
66	00067 or 10067	Bool 66	Bool	slave mapping address, can
			Bool	map the slave input coil and holding coil state,
			Bool	64 addresses in total.
127	00128 or 10128	Bool 127	Bool	

2) 16 Bit Slave Register Assignment Table

	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	Sort AB, its data type according to slave mapping data type	According to configurator set mapping rules, this address will sort slave mapping data to AB, stock in this address, for cloud easy reading together, can mapping slave inputting and holding register.		
20002	420003 or 320003	16 Bit data 20002	Same as above	Same as above		
20003	420004 or 320004	16 Bit data 20003	Same as above	Same as above		
	127 data similar as above		Same as above	Same as above		
20127	420128 or 320128	16 Bit data 20127	Same as above	Same as above		

3) 32 Bit Slave Register Assignment Table

	Holding Register and input Register(Function Code 03,04, 06, 16)						
Modbus Register Address(Decim al)	PLC or configuratio n address (Decimal)	Data name	Data Type	Description			
20128	420129 or 320129	32 Bit data 20128	Sort ABCD, its data type according to slave mapping data type	According to configurator set mapping rules, this address will sort slave mapping data to ABCD, stock in this address, for cloud easy reading together,			





				can mapping slave inputting and holding	
				register.	
20130	420131 or	32 Bit data	Same as above	Same as above	
20150	320131	20130	Same as above		
20132	420133 or	32 Bit data	Same as above	Same as above	
20132	320133	20132	Same as above		
	64 data				
	similar as		Same as above	Same as above	
	above				
20254	420255 or	32 Bit data	Come on obour		
20254	320255	20254	Same as above	Same as above	

6.1.3.2 Read Boolean Mapping Address Data

Master Send Data Format:

Content	Bytes	Data	Description
Device ID	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read holding coil type, function code 01
Boolean Register	2	00 40H	Range: 0040H-007FH, address refer to ["Slave
Starting Address	2	00 401	Mapping Register Address"]
Read Register Qty	2	00 0AH	Range: 0001H-0004H
16 CRC Verify	2	BD D9H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data	Description				
Device ID	1	01H	01H Device, Range: 1-247, according to setting address				
Function Code	1	01H	Read holding coil type				
Return Data Length	1	02H	Return data length				
Returning Data	2	73 01H					
16 CRC Verify	2	5D 0CH	CRC0 CRC1 low byte in front, high behind				

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

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

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

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

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

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

The address value higher than 10 digits will be seen as invalid. 5D 0C CRC Verify.

6.1.3.3 Modify Boolean Mapping Address Data

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

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-00 7FH, 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

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	05H	Write single holding coil					
Boolean Mapping	2	00 40H	Range: 00 40H-00 7FH, address refer to ["					
Register Address	2	00 40 1	Mapping Register Address"]					
Write value	2	FF 00H	This value: FF 00H or 00 00H. FF 00H stands for write					
write value			1,00 00H stands for write 0.					
16 CRC Verify	2	8D EEH	CRC0 CRC1 low byte in front, high behind					

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

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

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

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

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

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

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

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

6.1.3.4 Read Data Type Mapping Address Data

Master Send Data Format:

Content Bytes Data Description (H: HEX)



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	One address can read 2 bytes. Mapping data type address range, refer to ["Slave Mapping Register Address"] at manual bottom.
Read Mapping Register Qty	2	00 0AH	Read input register qty.
16 CRC Verify	2	82 EFH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

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

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

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

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

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

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

Register Mapping	20010	20000	20009 20008	20007	20006	20005	20004	20003	20002	20001
Address	20010	20009	20008	20007	20000	20005	20004	20003	20002	20001
Value	00 2A	00 14	00 25	00 0A	00 41	00 4B	00 32	00 28	00 1E	00 14

FB 34=16 CRC Verify.

6.1.3.5 Modify Data Type Mapping Address Data

If need to revise slave data which RS485 connected, need to add slave in salve list of configurator. Write command 03 for mapping, when mapping address value modified, will write to RS485 matched slave address. If address 20001 mapping slave data type is Signed Int, sort AB.

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	2	4E 21H	Mapping data type address range, refer to ["Slave

Master Send Data Format:

G Wireless Industrial Router Wireless Data Connectivity

Address			Mapping Register Address"]
Write Data	2	00 64H	Data writing value is Decimal data 100
16 CRC Verify	2	CF 03H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	06H	Write single holding register
Mapping Register	2	4E 21H	Mapping data type
Address	-		
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.

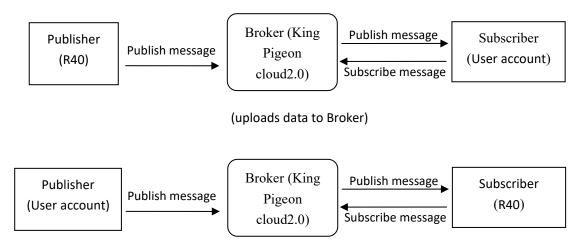
6.2.2 MQTT Principle

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



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

6.2.3 Device Communication Application

(The setting page is in 5.9Cloud Platform)

Client configuration

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

2. Connection protocol: MQTT.

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 serial number.

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

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

9. Publisher QOS: The service quality level guarantee for application message distribution, 0-at most once, 1-at least once, 2-only once, you can choose according to your needs.

10. Encryption: You can use encryption to connect to the server according to your needs, and you can choose not to encrypt when you connect to King Pigeon Cloud 2.0.

11. Enable data retransmission: Check enable, after enabling, when reconnecting to the cloud platform, the data during the offline period will be retransmitted.

12. Data packing: After checking, send multiple data in one message, when unchecked, one message corresponds to one I/O data point.

After the configuration is complete, the client will initiate a connection to the server:

CONNECT: The client sends a CONNECT connection message request to the server;

CONNACK: The server responds with a CONNACK confirmation connection message, indicating that the

KING PIGEON

{



Nireless Industrial Router Wireless Data Connectivity

connection is successful;

After the client establishes a connection, it is a long connection, and the client can publish or subscribe to the message on the server;

For example the device and the client's mobile phone as the client:

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

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

6.2.4 Publish MQTT Format

If data packing is ticked 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 checked, one The message only corresponds to one I/O data point, the two publishing formats are slightly different, so you need to pay attention

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

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

```
"sensorDatas":
  [
     {
     // switch type,
     "switcher":"1",
                                                // Data type and value
     "flag":"DI1"
                                               //Read and write Flag
     },
     {
     // Slave switch type
     "switcher":"0",
                                             // Data type and value
     "flag":"REG64"
                                             //Read and write Flag
     },
     {
      //value
     "value":"10.00",
     "flag":"AI1"
     },
   {
     //Slave value
     "value":"217.5",
     "flag":"REG2001"
     },
   {
     //Positioning
     "lng":"116.3",
                                               // longitude data
     "lat":"39.9",
                                              // latitude data
      "spd":"0.0",
                                              // speed data
   "dir":"0.0",
                                           // direction data
     "flag":"GPS"
     }
```



],

"time":"1602324850"

//Time , data release timestamp UTC format

"state":"alarm",

//Alarm and recovery identification (only for alarm or recovery data, but nottimly report)
"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 "Ing" and the value is: "data value".

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

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

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

Read and write Flag:

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

Device own I/O Port

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

Extend I/O Port

Data name	Flag	Data type	Description
Boolean	REG64~127	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"

//Alarm and recovery identification: the character is "state", followed by "alarm" or "recovery" (alarm represents alarm data and recovery represents recovery data)

//Retransmission flag: the character is "retransmit", followed by "enable"

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

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

Publish Topic: serial numbers

G Wireless Industrial Router Wireless Data Connectivity

"switcher": "0", "flag": "DI1", "time": "1602324850"

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

6.2.5 Device Subscribe MQTT Format

The payload data format in the device subscription message

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

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

Note:

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

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

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

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

2. The numeric character is " value " followed by: "data value"

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

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

7. SMS Command List

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

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

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

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

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

5. If the password is correct but the command is incorrect, the device will return: SMS Format Error, Please



check Caps Lock in Command! So please check the Command, or add the country code before the telephone

number or check the input is in ENGLISH INPUT METHOD and CAPS LOCK. If password incorrect then will not

any response SMS.

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

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

1) Modify Password, 4 digits, default is 1234

SMS Command	Return SMS Content		
Old Password + P + New Password	Password reset complete		
2) Inquiry Current Status SMS Command	·		
SMS Command	Return SMS Content		
password+EE	Model:xxx		
	Version:xxx		
	IMEI:xxx		
	GSM Signal Value:xxx		

3) Inquiry DIN Status

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

4) Set Digital Output

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

5) Inquiry AIN Status

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

6) Digital Pulse Counter

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



8. Warranty

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

The End! Any questions please help to contact us feel free. <u>Http://www.IOT-SOLUTION.com</u>