

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**

KING PIGEON



4G Wireless Router User Manual

Ver 1.3

Date Issued: 2021-03-18 King Pigeon Hi-Tech. Co., Ltd.

www.iot-solution.com



Table of contents

1. De s	scrip	tion		3
1	1. 1	Brief Introduction	3	
1	1.2	Typically Applications	4	
Ĺ	1.3	Safety Directions	9	
í	1.4	Standard Packing List	9	
1	1.5	Main Features	10	
1	1.6	Technical Parameters	11	
2. Ha	rdwa	are Description		14
Ź	2.1	Size	16	
ź	2.2	Indicator light	16	
2	2.3	Reset	17	
2	2.4	SIM Card	17	
ź	2.5	Connect External Antenna	18	
2	2.6	Router GND	18	
Ź	2.7	Installation	19	
3. Sta	rt u	p		19
3	3.1	Switch on	19	
3	3.2	System running status	20	
3	3.3	SIM Card Operation	20	
3	3.4	Serial Port Instructions	21	
3	3.5	Digital output Instructions	22	
Э	3.6	Digital input Instructions	23	
Э	3.7	Analog input Instructions	24	
4. Pre	par	ation before configuration		24
Z	4.1	Wired Connection	25	
Z	1.2	Wifi Connection	29	
Z	4.3.	Factory Default Settings	31	
2	1.4.	Enter Web Settings	31	
5. Roi	uter	Settings		32
5	5.1	Status	32	
5	5.2.	System	32	

KING PIGEON

G Wireless Industrial Router Wireless Data Connectivity

3.	Warr	anty	
7.	SMS (Command List	
	6.2	MQTT Protocol	.92
	6.1	Modbus RTU Protocol	.81
5.	Comm	nunication Protocol	
	5.10	Logout	81
	5.9	Cloud Platform	76
	5.8	Logical Operation	.76
	5.7	RTU IO	71
	5.6	Serial Port	.67
	5.5	VPN	.62
	5.4	Network	.40
	5.3.	Service	.36

UPGRADE HISTORY

DATE	FIRMWARE VERSION	HARDWARE VERSION	DESCRIPTION
2020.03.13	V 1.0	V 1.0	First edition
2020.09.30	V1.1	V1.0	Modify some configuration instructions
2021.2.25	V1.2	V1.0	Added link to Huawei Cloud IO platform
2021.03.18	V1.3	V1.0	Add device mapping register address from
			64-127 to 64-256

Model List

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

1. Description

1.1 Brief Introduction

Router industrial router 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, comes

4G Wireless Industrial Router Wireless Data Connectivity

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.



4G VPN Router Applied to Water Conservancy Wireless Monitoring Solution

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

1.2.4 Mine Wireless Networking & Monitoring System Solution

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, 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.

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

- 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
	POE(optional)	Single POE maximum output power 30W
LAN (POE)		With power management function
		Voltage range 48 \sim 57V
		ESD \pm 30kV (contact) , \pm 30kV (air)
	Protection	EFT 40A (5/50ns)
		Lightning strike 24A $(8/20\mu s)$
	Qty	2
	Туре	1 RS485,1 RS232
	Doudrata	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600,
	Baudrate	115200, 230400
	Data Bit	5, 6, 7, 8
Sorial Dort	Parity	None, Even, Odd
Serial Port	Stop Bit	1,2
	Working mode	Data transparent transmit, Modbus RTU to TCP, Modbus
		master
	Protection	ESD (contact) : 8KV Surge: 4KV (8/20us)
		ESD \pm 8kV (contact) , \pm 15kV (air)
		EFT 4KV, 40A(5/50ns)
	Qty	1
Concolo	Туре	CONSOLE
Console	Interface Spec	RJ45
	Protection	ESD: \pm 8kV (contact) , \pm 15kV (air)
	Qty	1
USB (December 1)	Туре	USB2.0 (HOST)
(Reserved)	Protection	ESD \pm 8kV (contact) , \pm 15kV (air)
	Antenna qty	2
	Antenna type	SMA
	protocol	802.11a/b/g/n (mixed)
	mode	AP mode,client mode
	Frequency	2.4G
WIFI	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	support
	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
	4G (L-CE)	WCDMA: B1,B8
		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 (NANO)
	Protection	In-built 15KV ESD Protection
	Antenna qty	1
CDC	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)
Disital in sut		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
	Qty	2
Digital	Туре	SINK output
	Load voltage	Max 50VDC
output	Load current	500mA (single), 625mW
	Protection	EFT: 40A (5/50ns)
	Qty	4
Analog innut	Туре	0~5V, 4~20mA, 0~20mA
	ADCResolution	16bit
	Protection	EFT: 40A (5/50ns)

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

	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)
	Notwork Portocol	PPP, PPPoE, TCP, UDP,DHCP, ICMP,NAT,
	Network Portocol	HTTP, HTTPs,DNS, ARP, NTP,SMTP,SSH2,DDNS etc.
	VPN	Ipsec,OpenVPN,L2TP
Coffeenance	Financell	DMZ,DoS defense,IP packet, Domain name and MAC address
Software	Firewall	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)
Cortificato	ENAS	IEC(EN)61000-4-4(EFT)
Certificate	EIVIS	IEC(EN)61000-4-5(Surge)
		IEC(EN)61000-4-6(CS)
		IEC(EN)61000-4-8
	Others	CE,FCC,ROHS,3C
Working	Working temperature	-40∼85℃
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				
	Alexan indicator light	ON	DI or Al trigger alarm				
ALARIVI	Alarm Indicator light	OFF	normal				
		flicks	normal				
SYS	System running status indicator	slowly	normai				
		OFF	abnormal				
		flicks	Signal normal				
4G	4G status indicator	fast	Signal normal				
		OFF	abnormal				
		ON	WiFi normal				
VVIFI	WIFI Status Indicator	OFF	abnormal				
DO1	Disitel extend 1 indicator light	ON	DO1 close				
DOI	Digital output 1 indicator light	OFF	DO1 open				
003	Digital output 2 indicator light	ON	DO2 close				
DOZ		OFF	DO2 open				
DI1	DI1 Digital input 1 indicator light		DI1 close				
UIT			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





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 - LuCl	× + ~		_		×
\leftarrow \rightarrow \heartsuit \textcircled{O}	92.168.3.1/cgi-bin/luci/admin/network/cell	□ ☆	⊯∥	Ŕ	
R40B 状态 - 系统 - 信号强度	服务 ← 网络 ← VPN ← I/O ← 接口 ← 退出 21,35				^
固件版本	EC25AUGCR06A02M1G				
IMSI	460007790314217				
IMEI	861585042306033				1
选择电话卡	<mark>†1</mark> †2				1
<u>►158</u>					
卡1 APN					
卡1用户名					
卡1密码					
启用GPS					
告警电话号码	*				
	接收起信的移动电话号约 十六 (0):				
短信语言	中文 (Chinese) V				
	क्र	字并应用	存复位		1
Powered by KingPigeon Technol	ogy Co., Ltd. (v1.09) / 2020-05-13 01:40:25				0

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

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

Modbus master : Used as Modbus master, the serial port connected to Modbus slave equipment, through configuration Page 5.7.2. 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 5.7.1. 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 5.7.3. 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 5.7.4. 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 5.7.4.

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



Disital input	qty	2
Digital input	type	Dry contact, wet contact



			_
	Range	High level (digital 1) 5~30VDC, low level (digital 0) 0~1VDC	
	Pulse frequency	<100Hz	
	protection	Isolation voltage 3750Vrms	

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

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

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

4. For detailed configuration, please refer to 5.7.2. 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. AI-AI4 is a four-way analog input, the default is 0~5V voltage type analog input, you can switch to current type analog input by turning the dial switch to mA. The four-way dial switch AI1~AI4 is Four analog inputs correspond one to one, V corresponds to voltage type, and mA corresponds to current type.

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

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

KING PIGEON

4G Wireless Industrial Router Wireless Data Connectivity

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 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 Connectiv	vity:	Internet
IPv6 Connectiv	ity:	No Internet access
Media State:		Enabled
Duration:		07:35:18
Speed:		100.0 Mbps
ctivity		
ctivity —	Sent —	- Received
ctivity —	Sent —	— Received
ctivity	Sent — 102,166,751	Received 833,590,410

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



	abe Family Controller #2	
		Configure
Tis connection uses	the following items:	
Shrew Soft L	ightweight Filter	
🗹 📕 QoS Packet	Scheduler	
File and Print	er Sharing for Microsoft	Networks
Internet Proto	ocol Version 6 (TCP/IPv	r6)
 Link-Layer To 	opology Discovery Map	per I/O Driver
🗹 🔺 Link-Layer To	opology Discovery Resp	oonder
	Lipinstall	Properties
Install	Graniactan	
Install Description	Orimacai	
Install Description Transmission Contro	ol Protocol/Internet Prot	ocol. The default

4. Two ways to configure the IP address:

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



serierai	Alternate Configuration				
You can this cap for the	n get IP settings assigned aut bability. Otherwise, you need appropriate IP settings.	tomatically if to ask your	f your n netwo	etwork rk admin	supports istrator
0	btain an IP address automatic	cally			
- O U:	se the followin <mark>g</mark> IP address: -				
IP a	ddress:				
Subr	net mask:				
Defa	ault gateway:				
0	btain DNS server address aut	tomatically			
O U:	se the following DNS server a	ddresses:			
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".



seneral	
You can get IP settings assigned this capability. Otherwise, you r for the appropriate IP settings.	d automatically if your network supports need to ask your network administrator
🔘 Obtain an IP address auto	matically
• Use 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
O Use 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	~	1
Broadband Connection		
Wireless Network Connection	^	
KINGPIGEON	liter	
niuren	lite.	
ChinaNet-DFxQ	Ine.	
mazentop	lite.	
King-xxxxx	lte.	
Connect automatically	Connect	
DIRECT-11-HP DeskJet 3630 series	ite.	
TP-E	-11	

Step2: Click "connect" to establish a connection.



Currently connected to:	43	*
King-xxxxxx Internet access		11
Dial-up and VPN	~	
Broadband connection		
Wireless internet connection	^	
King-xxxxx	Connected	
niuren	lite.	
KINGPIGEON	line.	
ChinaNet-DFxQ	liter	
mazentop	llee	
DIRECT-11-HP DeskJet 3630 series	line.	-

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
	SSID: King-xxxxx
VVIFI	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: admin



http://192.10	68.3 .1			
Your connec	tion to th	is site is no	ot private	
Use <mark>rna</mark> me	admin	1		
Password				
				_

5. Router Settings

5.1 Status

(**) R40B - Overview - LuCl × +		-	٥	×
← → C ▲ Not secure 192.168.3.1/c	:gi-bin/luci/	\$	Θ	:
🚻 Apps 隆 翻译 🥪 金錦物联网云V3.0				
R40B Status	 System - Services - Network - VPN - Serial Port - RTU I/O - Logical operation - Cloud platform - Logout 			^
Status				71
System				
Hostname	R40B			
Model	Mediatek MT7628AN evaluation board			
Architecture	MediaTek: MT7628AN ver:1 eco:2			
Firmware Version	KingPigeon Technology Co., Ltd. v1.18			
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



(**) R40B - System Settings - LuCl × +	- 0 ×		
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/system/system	☆ 🛛 :		
🚻 Apps 💁 翻译 🕑 金錦物联网云V3.0			
R40B Status = System = Services = Network = VPN = Serial Port = RTU I/O = Logical operation = Cloud platform = Lo	egout		
i ontal	REFRESH ON		
System			
Here you can configure the basic aspects of your device like its hostname or the timezone.			
System Properties			
General settings Logging Time Synchronization Language and 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 effect			
Save & Apply - Save F	leset		
Powered by KingPigeon Technology Co., Ltd. (v1.18) / 2020-10-16			

Configure basic information , such as host name or time zone

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

5.2.2 Management Rights



(••) R40B - Router Password - LuCI ×	+	- o ×	
← → C ▲ Not secure 1	92.168.3.1/cgi-bin/luci/admin/system/admin	☆ \varTheta :	
👖 Apps 峰 翻译 😺 金錦物联网云	V3.0		
R40	B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout		
Rout	er Password SSH Access SSH-Keys		
Ro	uter Password ges the administrator password for accessing the device		
	Password *		
	Confirmation *		
	Save		
Powe	red 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	× +				- 0 ×
← → C ▲ Not secur	re 192.168.3.1/cgi-bin/luci/adn	nin/system/opkg			☆ 🛛 :
🏥 Apps 峰 翻译 🍛 金錦物	1联网云V3.0				
	R40B Status - System -	Services - Network - VPN -	Serial Port	gical operation - Cloud platform - Logout	
	Software				
			94% (7.7 MB)		
	Filter:	Download and install pac	kage: Actions:		
	Type to filter	Clear Package name or URL	. OK Update lists.	Upload Package Configure opkg	J
	Available Installed Updates				
	ĸ		No packages	э	
	Package name	Version	Size (.ipk)	Description	
	No information available				
	Powered by KingPigeon Technology	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 Firmwa: × +	- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/system/flash	☆ \varTheta :
👖 Apps 💁 翻译 ⊌ 金錦物联网云V3.0	
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	^
Flash operations	
Actions Configuration	
Backup	
Click "Generate archive" to download a tar archive of the current configuration files.	
Download backup Generate archive	
Restore	
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).	
Reset to defaults Perform reset	
Restore backup Upload archive	
Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.	
Save mtdblock contents	
Click "Save mtdblock" to download specified mtdblock file. (NOTE: THIS FEATURE IS FOR PROFESSIONALSI)	
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 - LuCI × +		-	5 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci	/admin/services/ddns/detail/myddns_ipv4	©≊ ☆	0:
R40B Status - System	* Services * Network * VPN * Serial Port * RTU I/O * Logical operation * Cloud platform * Logout		Î
Dynamic DNS Dynamic DNS allows that your ro OpenWrt Wiki: DDNS Client Doc	uter can be reached with a fixed hostname while having a dynamically changing IP address. umentation DDNS Client Configuration		
Details for: myddns_ip	w4		- 1
Configure here the details for sel	ected Dynamic DNS service.		
Basic Settings Advanced Set	ings Timer Settings Log File Viewer		- 1
Enabled			
	If this service section is disabled it could not be started. Neither from LuCl interface nor from console		
Lookup Hostname	yourhost.example.com		
	Hostname/FQDN to validate, if IP update happen or necessary		- 1
IP address version	● IPv4-Address ○ IPv6-Address		
	Optimes 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		-

DNS Basic Settings				
Item	Description			
anabla	If the service configuration is disabled, then it cannot be			
enable	started.			
Lookun hostnamo	Hostname/FQDN verification, if IP update occurs or is			
LOOKup nostname	necessary			
ID addross vorsion	Set which IP address (IPv4 or IPv6) will be sent to the			
IP address version	DDNS provider			
DDNS	Chaosa DDNS sarvisa providar			
service provider	Choose DDNS 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/lu-	ci/admin/services/ddns/detail/myddns_ipv4	ष ☆ 🛛 :	
	R40B Status - Syste	m + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	^	
	Dynamic DNS Dynamic DNS allows that your OpenWrt Wiki: DDNS Client Do	router can be reached with a fixed hostname while having a dynamically changing IP address. cumentation DDNS Client Configuration		
	Details for: myddns_i	ipv4		
	Configure here the details for se	elected Dynamic DNS service.		
	Basic Settings Advanced Se	ttings Timer Settings Log File Viewer		
	IP address source [IPv4]	Network		
	Network [IPv4]→	 Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider wan 		
		Optimes the network to read systems IPv4-Address from		
	Force IP Version			l
		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@myproxy.lan:8080		
		OPTIONAL: Proxy-Server for detection and updates.		

	DNS Advanced Setting				
Item	Description				
ID addross source	Set the source of the IP address. This will be sent to the				
IP address source	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.				
Dreve com com	Format: [user:password@]proxyhost:port				
PTOXY 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 filo	Write detailed information to the log. The file will				
	automatically shrink.				

5.3.1.3 Timer setting



(••) R40B - LuCl × +		- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luc	/admin/services/ddns/detail/myddns_ipv4	
R40B Status - System	n + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	ŕ
Dynamic DNS Dynamic DNS allows that your re OpenWrt Wiki: DDNS Client Doc	outer can be reached with a fixed hostname while having a dynamically changing IP address. umentation DDNS Client Configuration	
Details for: myddns_i	ov4	
Configure here the details for set	ected Dynamic DNS service.	
Basic Settings Advanced Set	tings Timer Settings Log File Viewer	
Check Interval	10 minutes V	
	Interval to check for changed IP Values below 5 minutes == 300 seconds are not supported	
Force Interval	72 hours 🖌	
	Interval to force updates send to DDNS Provider Setting this parameter to 0 will force the script to only run once Values lower 'Check Interval' except '0' are not supported	
Error Retry Counter	0	
	On Error the script will stop execution after given number of retrys The default setting of '0' will retry infinite.	
Error Retry Interval	60 seconds 🗸	
	On Error the script will retry the failed action after given time	
Back to Overview	Save & Apply Save Reset	

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

5.3.1.4 Log File Viewer



(*4 R408 - LuCi X +	– 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/services/ddns/detail/myddns_jpv4	⊠ ☆ \varTheta :
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	<u>^</u>
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	
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.ababled='0'	
ddns.myddns_ipv4.interface='wan'	
ddns.myddns_ipv4.1p_network='wan' ddns.myddns_ipv4.ip_source='retwork'	
ddns.myddns_ipv4.lookup_host='yourhost.example.com'	
ddns.myddns_ipy4.password="***Ply***' ddns.myddns_ipy4.password="***Ply***'	
ddns.myddns_ipv4.username='your_username'	
ddns.myddns_ipy4=service 031307 - ywehnee mode : 0 - run normal NO console outnut	
031307 WARN I Service section disabled - TERNINATE	
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.

R40B	Status -	System -	Services -	Network -	VPN -	Serial Port -	RTU I/O 🗕	Logical operation +	Cloud platform	- Logout		
Interfaces	Global net	work options								AUTO REFRESH ON	,	
Interfac	es											
br	AN () lan		Protocol: St. Uptime: 0h 4 MAC: 46:68: RX: 4.02 MB TX: 2.51 MB IPv4: 192.16 IPv6: fd83.fb	atic address I7m 33s A3:D3:DA:68 (37066 Pkts.) 8.3.1/24 6e:35eb::1/60).		Restart	Stop	Edit	Delete		
W ett	AN 10.2		Protocol: DH MAC: 46:68: RX: 259.14 k TX: 8.27 KB	ICP client A3:D3:DA:69 (B (2779 Pkts.) (61 Pkts.)	-)		Restart	Stop	Edit	Delete		
W/	AN6		Protocol: DF MAC: 46:68: RX: 259.14 k TX: 8.27 KB	ICPv6 client A3:D3:DA:69 (B (2779 Pkts (61 Pkts.)	.)		Restart	Stop	Edit	Delete		
4 3g	IG HG		Protocol: UN RX: 0 B (0 Pl TX: 0 B (0 Pl	/ITS/GPRS/E\ kts.) cts.)	V-DO		Restart	Stop	Edit	Delete		
Add ne	w interface											

5.4.1.1 LAN port



٥ ×

☆ 🛛 :

_

(**) R40B - Network Settings - LuC × +

← → C ▲ Not secure | 192.168.3.1/cgi-bin/luci/admin/network/network Interfaces » LAN

Image: Terminal settings Advanced Settings Physical Settings Freewall Settings DHCP Server Status \$* Device: br-lan Uptime: th 49m 4s MAC: 466 A2: 33.0A.68 RX: 4.06 M8 (37.443 Pkts.) TX: 2.67 M8 (6883 Pkts.) TY: 4.57 M8 (6883 Pkts.
Status
Protocol Static address Bring up on boot IPv4 address IPv4 address 192 168.3.1 IPv4 netmask 255.255.0 IPv4 gateway IPv4 gateway IPv4 broadcast 192.168.3.255 Use custom DNS servers + IPv6 assignment length 60
Bring up on boot IPv4 address 192.168.3.1 IPv4 netmask 255.255.0 IPv4 gateway IPv4 broadcast 192.168.3.255 Use custom DNS servers *
IPv4 address 192.168.3.1 IPv4 netmask 255.255.0 IPv4 gateway
IPv4 netmask 255.255.255.0 IPv4 gateway IPv4 broadcast 192.168.3.255 Use custom DNS servers + IPv6 assignment length 60
IPv4 gateway IPv4 broadcast 192.168.3.255 Use custom DNS servers + IPv6 assignment length 60 •
IPv4 broadcast 192.168.3.255 Use custom DNS servers + IPv6 assignment length 60 •
Use custom DNS servers + IPv6 assignment length 60 •
IPv6 assignment length 60 ·
(a) Assign a part of given length of every public IPv6-prefix to this interface

	t			
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		
Decis Catting		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 ting	Assign this hexadecimal sub-ID prefix to		
		this interface		
	IPv6 suffix	Optional, allowed values: "eui64",		



			"random" and other fixed values (for example: "::1" or "::1:2"). When the IPv6 prefix (such as "a:b:c:d::") is obtained from the authorization server, use the suffix (such as "::1") to synthesize an IPv6 address ("a:b:c:d::1") Assigned to this interface.		
	Use built-in IPv6 manag	ement	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		
	Reset MTU		Default 1500		
	Lise Gatewa	av Hon	Default 0		
	Bridge inter	face	Create a bridge for the specified interface, default is enable.		
	Enable STP		Enable spanning tree protocol on this bridge, default is disable.		
Physical settings	Enable IGM	P 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.		
		Ignore	DHCP service is not provided on this		
		this interface	interface, default is disable		
		Start	Start network address, default is 100.		
DHCP server	Basic Setting	Customers	Maximum number of address assignments. The default is 150.		
		Lease term	The expiration time of the leased address is at least 2 minutes (2m). The default is 12h.		
	Advanced settings	DHCP	Provide DHCP service for all clients. If disabled, only customers with static leases will be served. default is enable.		
		Forcibly	Even if another server is detected, it is		



		mandatory to use DHCP on this network, default is disable.			
	IPv4 Subnet mask	Reset the subnet mask sent to the client.			
	DHCP Options	Set additional options for DHCP, for example, setting "6,192.168.2.1,192.168.2.2" means to announce different DNS servers to clients.			
	Route Advertisement Service	Default server mode			
	DHCPv6 server	Default server mode			
	HDP proxy	Default disable			
	DHCPv6 mode	The default is stateless + stateful			
IPV0	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 server	Default is empty			
	Advertised DNS domain name	Default is empty			

5.4.1.2 WAN port

(**) R40B - Network Settings - LuC × +		- o ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/ad	min/network/network	☆ \varTheta :
R40B Status - System -	Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	*
Interfaces » WAN		
Ir General settings Advanced	Settings Physical Settings Firewall Settings	
Status	Device: eth0.2 MAC: 46:68 A3:D3:DA:69 RX: 259:14 KB (2779 Pkts.) TX: 8.27 KB (61 Pkts.)	
Protocol	DHCP client	
Bring up on boot		
lister to set the	D 400	
requesting DHCP	K4UD	
	Dismiss Save	
	TX: 8.27 KB (61 Pkts.)	
4G 3g-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	



100				
	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: coaxial 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		
	Lise 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 × +		- 6	ı ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/a	lmin/network/network	☆	Θ :
R40B Status - System	✓ Services ✓ Network ✓ VPN ✓ Serial Port ✓ RTU I/O ✓ Logical operation ✓ Cloud platform ✓ Logout		ه. ا
Interfaces » WAN6			
General settings Advance	Settings Physical Settings Firewall Settings		
State	s 27 Device: eth0.2 MAC: 46:68:A3:D3:DA:69 DY:356:14/08:0770.0Hz		
	TX: 8.43 KB (62 Pkts.)		
Protoc	DHCPv6 client.		
Bring up on bo	it 🗹		
Request IPv6-addres	s try -		
Request IPv6-prefix of leng	h Automatic -		
	Dismiss Save		
4G 39-4G	Protocol: UMTS/GPRS/EV-DO RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)		
Add new interface			
	Save & Apply - Save Reset		

WAN6				
Item		Description		
	Status	Device: eth0.2 MAC: E2:2F:C4:54:93:BB		
	Status	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 server automatically	Leave blank to ignore the advertised DNS server address, default is enable.		
	Client ID sent when requesting	Default is empty		



	DHCP	
	Reset MAC address	Modify MAC address
	Reset MTU	Default 1500
	Bridge interface	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
Firowall cottings	Create/Assign	move the interface out of the associated
rirewall 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	☆ 🛛 :
R40B Status + System +	Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout	*
Interfaces » 4G	AUTO REPRESE ON	
General settings Advanced Se	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				



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

5.4.2 WIFI



					_					
R40B - WiFi - LuCI	× +							-	٥	×
\rightarrow C A Not se	cure 192.168.3.1/cg	gi-bin/luci/admin/network/w	rireless					\$	θ	•
	R40B Status		Network - VPN -	Serial Port - RTU I/O	- Logical operation	n 👻 Cloud platfo	orm - Logout			
							AUTO REFRESH ON			
	WiFi Settings									
	🙊 radio0	Media Tek MT76x8 802. Channel: 11 (2.462 GHz) B	11bgn Bitrate: ? Mbit/s		Restart	Scan	Add			
	ali 0%	SSID: King-2b77b3 Mode: BSSID: EC:0C:45:81:26:51	Master Encryption: None		Disable	Edit	Remove			
	Associated St	ations								
	Network	MAC-Address	Host	Signal / Noise	RX F	Rate / TX Rate				
			No info	rmation available						
					Save	& Apply - S	ave Reset			
	Powered by KingPig	eon 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)

(*4 R40B - WiFi - LuCI X +	- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/network/wireless	☆ \varTheta 🗄
R40B Status + System + Services + Network + VPN + Serial Port + RTU 1/0 + Logical operation + Cloud platform + Logo	^
Altro REFF	RESH ON
Wireless Network: Master "King-2b77b3" (wlan0)	
Device Configuration	
General Setup Advanced Settings	
Status Mode: Master SSID: King-2b77b3 0% BSSID: EC:0C:45:81:26:51 Encryption: None Channel: 11 (2:462 GHz) Tx-Power: 20 dBm Signab: 0 dBm Noise: 0 dBm Bitrate: 0.0 Mbit/s Country: 00	
Wireless network is enabled Disable Mode Channel Width	
Operating frequency N 🗸 11 (2462 Mhz) V 20 MHz V	n l
Maximum transmit power driver default - Current power: 20 dBm	
P. P.<	
Interface Configuration	
General Setup Wireless Security 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.

Wireless network AP hotspot interface configuration				
Item		Description		
	Mode	Access Point		
	ESSID	Default King-xxxxx (xxxxxx is Random numbers or letters)		
Pacie Sotting	Network	lan		
Dasic 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	Allow AP mode to disconnect wireless terminal		
	Ack response	under low ACK, default is enable.		

5.4.2.2 WLAN Client

0B - WiFi - LuCl	× +	at work (wireless				-
G A NOL	R40B Status - System - Se	rvices - Network	+ VPN -	Serial Port - RTU I/O		ਸ
_					AUTO REFRESH ON	
Join Netwo	rk: Wireless Scan	Channel	Mode	BSSID	Encryption	
48%	jingekeji	1	Master	24:69:68:82:3C:96	mixed WPA/WPA2 PSK (CCMP) Join N	letwork
37%	DIRECT-58-HP DeskJet 3630 series	6	Master	40:B0:34:63:EB:59	WPA2 PSK (CCMP)	letwork
34%	King-e4f82b	11	Master	EC:0C:45:81:26:54	None Join N	letwork
30%	BioLock	6	Master	60:3A:7C:0D:00:16	mixed WPA/WPA2 PSK (CCMP) Join N	letwork
						Dismiss
					Save & Apply - Save Reset	
	Downrad by KingPingon 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 Working	Default is enable If there are too many devices in use at the current		
	frequency	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.
	Decen interval	Indicates the interval at which the wireless router
	Beacon Interval	periodically broadcasts its SSID, usually use default value.

Interface configuration				
Item		Description		
	Mode	Client		
Pacic Sotting	ESSID	Wireless network name		
Dasic Setting	BSSID	none		
	Network	Wwan,no need modify it		
	Encryption	WPA2-PSK (Strong security)		
	Algorithm	auto		
	Password	Wireless network password		
Wireless security	802.11w Management Frame Protection	Requires the full version of wpad/hostapd, and WiFi driver support, default is disabled		
	Interface name	Reset the default interface name		
	Short Preamble	Different rates require different Preambl (preamble), default is enable		
	DTIM interval	As a terminal node, periodically wake up to send traffic indication message interval		
	Re-encrypt GTK	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 × +		-	٥	×
← → 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 Ø 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				
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

(··) R40B - DHCP and DNS -	- LuCl × +						-		1
← → C ▲ Not se	ecure 192.168.3.1	/cgi-bin/luci/admin/netw	ork/dhcp				☆	Θ	
	R40B Stat	us - System - Services	✓ Network ✓ VPN ✓ Serial	Port - RTU I/O -	Logical opera	ation - Cloud platform - Logout			
	DHCP an	DNS				AUTO REFRESH ON			I
	Dnsmasq is a com	bined DHCP-Server and DNS	-Forwarder for NAT firewalls						l
	Server Settin	ngs							l
	General settings	Resolv and Hosts Files T	FTP Settings Advanced Settings	Static Leases					
	Static leases are u where only hosts v Use the <i>Add</i> Butto assigned as a sym	ised to assign fixed IP address with a corresponding lease are n to add a new lease entry. Th ibolic name to the requesting h	ses and symbolic hostnames to DH served. Ine <i>MAC-Address</i> identifies the host nost. The optional <i>Lease time</i> can b	CP clients. They are a the <i>IPv4-Address</i> sp be used to set non-sta	also required for ecifies the fixed ndard host-spec	non-dynamic interface configurations address to use, and the <i>Hostname</i> is cific lease time, e.g. 12h, 3d or infinite.			
	Hostname	MAC-Address	IPv4-Address	Lease time	DUID	<u>IPv6</u> -Suffix (hex)			l
	Add		This section contai	ns no values yet					
	Active DHCP	_eases							
	Hostname	IPv4-Address	MAC-Addre	\$\$	Leasetime	e remaining			
			There are no a	ctive leases					
	Active DHCPv	6 Leases							
	Heat		IDv6 Addroop	DUID		Logostimo romaining			

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	This is the only DHCP server in the local			
	authorization	network,default is enable			
	Local server	Local domain rules. Names matching this domain are never forwarded, only resolved from DHCP or HOSTS files			
	Local domain name	The local domain name suffix will be added to the DHCP and HOSTS file entries			
	Record query log	Write received DNS request to system log, defaule is disable			
General	DNS forward	List of DNS servers to which requests are forwarded			
Setting	Rebinding	Discard RFC1918 upstream response data, default is			
	protection	enable			
	Allow local	Allow upstream response within 127.0.0.0/8 loopback range, for example: RBL service, default is enable.			
	Domain name whitelist	List of domain names that allow RFC1918 to respond			
	Local service only	DNS service is only provided in the subnet to which the network card belongs, default is enable.			
	Not all addresses	Dynamically bind to interface instead of wildcard address (recommended as linux default), default is enablee			

KING PIGEON



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.				
		The file used to store the assigned DHCP				
HOSTS& parse	Lease documents	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				
	N. 1	Does not record general operation logs of these				
	No log	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	Do not cache useless responses, for example:				
	information cache	domain names that do not exist, default is disable				
Advanced		This file may contain formats such as				
settings	Additional SERVERS	"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	Query DNS server in the order of "parse file", default				
	checking	is disable.				
	All server	Query all available upstream DNS servers, default is disable.				
	Ignore fake empty	List of servers allowed to respond with fake empty				
	resolution	domain names				
	DNS server port	Inhound 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 EDINS.U ODP 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 address as	ssignment	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

(••) R40B - Hostnames - LuCl	× +		– ø ×			
← → C ▲ Not secu	re 192.168.3.1/cgi-bin/luci/admin/network/hosts		☆ \varTheta :			
	R40B Status - System - Services - Network - VPN -	Serial Port + RTU I/O + Logical operation + Cloud platform + Logout				
	Hostnames Host entries					
	Hostname					
	This section					
	Add					
		Save & Apply - Save Reset				
	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



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	
	Routing	

5.4.7 Diagnosis

	46 Wi i	eless Indu Wire	strial Route less Data Co	r D nnectivity
(••) R40B - Diagnostics - LuCl × +				- 0 ×
← → C ▲ Not secure 192.168.3	3.1/cgi-bin/luci/admin/netwo	rk/diagnostics		☆ Θ :
R40B	Status - System - Services	- Network - VPN - Serial Port - I	RTU I/O - Logical operation - Cloud platform -	▪ Logout
Diagno Network L openwrt.org IPv4 ~ f Powered by Ki	stics Jtilities	openwrt.org IPv4 V Traceroute 1.18) / 2020-10-16	openwrt.org Nslookup	

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 × +	- ø ×
← → C ▲ Not secure 192.168.3.1/cgl-bin/luci/admin/network/firewall	☆ \varTheta :
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	
Zones	
Zone⇒Forwardings Input Output Forward Masquerading	
Ian ⇒ wan accept ✓ accept ✓	

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

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

•					
Setting	outbound data options are used to set the default strategy for inbound and outbound traffic in this area, and the forwarding options describe the traffic forwarding strategy between different networks in the area. The covered				
	network designates the networks belonging to this area.				
	Name	lan			
	Input	Default is accept			
	Output	Default is accept			
	Eorward				
		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			
	camounage	network			
	MSS Clamp	Automatically adjust MSS according to MTU			
	Covered				
	networks	lan			
	Allow				
	forwarding to	wan			
	target area				
	Allow				
	forwarding from	unspecified			
	source area				
	The following op	tions control the forwarding strategy between this area			
	(lan) and other areas. The target area receives the forwarded traffic from				
	lan. The forwarding traffic matching the source area comes from other				
	areas whose destination is lan. The role of forwarding rules is one-way. For				
	example, forwarding traffic from lan to wan does not mean allowing reverse				
	forwarding of traf	fic from wan to lan.			
	Covered	This option can classify regional traffic on original,			
	equipment	non-UCI-hosted network devices.			
	Subnets covered	This option can classify regional traffic by source or destination subnet instead of network or device.			
Advanced	Restricted				
settings	address				
	To restrict the				
	source subnet	Default is empty			
	of IP dynamic				
	masquerading				
	Target subnets				
	to restrict IP	Default is empty			
	dynamic 				
	masquerading				
	Enable logging	Default is disable			
	in this area	De net instell edditional subscite des fair autorit. ff			
Conntrack	Allow "invalid	with construct status involid. This may be a necessary			
setting	traffic"	with connitack 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	By passing the iptables parameter to the source and destination classification rules, you can match packets based on other conditions the interface or subnet. Use these options with extreme caution, as invalues may break the firewall rule set and expose all services to the or world.					
iptables parameter	Additional source parameters	Additional iptables parameters are used to classify regional inflows. For example: -p tcpsport 443 only matches inbound HTTPS traffic.				
	Additional target parameters	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 - Luc	ci × +						-	ð	×
← → C ▲ Not sect	ure 192.168.3.1/cgi-bin/luc	i/admin/network/firewall/fc	prwards				☆	Θ	:
	R40B Status - Syst	em - Services - Network	- VPN - Serial Port - RTU	I/O - Logical ope	ration - Cloud platform -	Logout			
	General settings Port Forw	ards Traffic Rules Custom F	Rules						
	Firewall - Port F Port forwarding allows remote	orwards computers on the Internet to con	nect to a specific computer or servi	ce within the private	LAN.				
	Port Forwards								
	Name	Match	Forward to	E	nable				
			This section contains no values ye	et					
	Add								
					Save & Apply - Save	Reset			
	Powered by KingPigeon Techn	iology 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			
Conoral Sotting		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
		Redirect matching inbound traffic to the
	internarport	port of the internal host
	Source MAC address	Match only inbound traffic from these
	Source MAC address	MACs
	Source ID address	Only match inbound traffic from this IP or
	Source ip address	IP range
	Source port	Only match inbound traffic originating
Advanced cettings		from a given source port or source port
Auvanced settings		range on the client host
		Only match inbound traffic for the
	External IP address	specified destination IP address
	Enable NAT loopback	Default is enable
		Extra parameters passed to iptables. use
	Additional parameters	caution!

5.4.8.3 Traffic rules

(10) R40B - Traffic Rules - LuCI × +				- 0 >
\leftrightarrow \rightarrow C A Not secure 192.16	58.3.1/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	
General set	tings Port Forwards Traffic Rules Custom Rules			
Firewa	III - Traffic Rules			
I rattic rules	define policies for packets traveling between different zones, for example to reject tr	affic between certain h	nosts or to open WAN ports on the router.	
Traffic R	ules			
Name	Match	Action	Enable	
Allow- DHCP- Renew	IPv4-UDP From any host in wan To any router IP 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	✓ Ξ Edit Delete	
Allow- IGMP	IPv4-IGMP From any host in wan To any router IP on this device	Accept input	Edit Delete	
Allow- DHCPv6	IPv6-UDP From IP <i>fc00:1/6</i> in wan To IP <i>fc00:1/6</i> at port <i>546</i> on <i>this device</i>	Accept input	Edit Delete	
Allow- MLD	IPv6-ICMIP with types 130/0, 131/0, 132/0, 143/0 From IP fe80//10 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	✓ Ξ Edit Delete	

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 Ind Wire	ustria eless	l Rout Data (er Conne(ctivity
(1) R40B - Traffic Rules - LuC	1 × +					- 0 ×
← → C ▲ Not see	cure 192.16	8.3.1/cgi-bin/luci/admin/network/firewall/rules				☆ \varTheta :
	R40B	Status - System - Services - Network - VPN - Serial Port - RT	UI/O - Logical ope	eration - Cloud platform	- Logout	^
	General set Firewa Traffic rules Traffic R	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 open WAN ports	; on the router.	
	Name	Match	Action	Enable		
	Allow- DHCP- Renew	IPv4-UDP From any host in wan To any router IP at port 68 on this device	Accept input		dit Delete	
	Allow- Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input		dit Delete	
	Allow- IGMP	IPv4-IGMP From any host in wan To any router IP on this device	Accept input	E	dit Delete	
	Allow- DHCPv6	IPv6-UDP From IP <i>fc00:16</i> in wan To IP <i>fc00:16</i> at port <i>546</i> on <i>this device</i>	Accept input		dit Delete	
	Allow- MLD	IPv6-ICMP with types 130/0, 131/0, 132/0, 143/0 From IP fe80://10 in wan To any router IP on this device	Accept input		dit Delete	
	Allow- ICMPv6-	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	Accept input and limit to 1000 pkts.		dit 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

(··) R40B - IPSec - LuCI	× +					- 0 ×
← → C ▲ Not se	cure 192.168.3	3.1/cgi-bin/luci/admin/vpn/ipsec	#			☆ \varTheta :
	R40B	Status + System + Services +	Network - VPN - Serial Port -	RTU I/O 👻 Logical operation	n	
	IPSec Security A	Alliance				
	Name	Tunnel ends		State	Running time	
			This section contains no valu	ies yet		
	Security F Below is a list	Policy of configured IPSec instances and the	ir current state			
	Name	Remote Gateway	Remote Subnet	Local Subnet	Enable	
			This section contains no valu	ies yet		
		Add				
				Sa	ve & Apply Save Reset	
	Powered by K	ingPigeon Technology Co., 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							
Item		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 host to the host					
IPSec	Poor gatoway	Poor gatoway which connect with IPSEC					
Configuration	Leeel subret	In the turned mode, the turned from the subnet to the subnet					
	IP/mask	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					
Phase 1 settings		Phase 1 mainly negotiates encryption parameters, exchanges key information, and verifies device identity					
IKE Encryption Al	gorithm	Specify IKE (Internet Key Exchange) negotiation message encryption algorithm					
Authentication al	gorithm	Specify the digital signature authentication algorithm for encrypted messages					
DH group		Specify which key group to use for DH (DiffieHellman) key exchange					
IKE version		IKEv1 or IKEv2					
Exchange mode		Main mode or brutal mode. The main mode is more secure than the brutal mode, and the brutal mode is faster. If the responder (server) cannot know the address of the initiator (end user) in advance, or the address of the initiator is always changing, and both parties want to use the pre-shared key authentication					
		method to create an IKE SA, Brutal mode can be used at this time					
Negotiation mode	2	Responder or initiator, the initiator is equivalent to the end user, and the responder is equivalent to the server					
Local ID		Can be IP address, standard domain name, email address or proper name, default is local IP					
Peer ID		Can be IP address, standard domain name, email address or					

	proper name, default is peer IP							
IKE live time	Re-negotiate the key time							
Bhase 2 sotting	The purpose of Phase 2 is to establish an IPSec security							
	association for data transmission							
ESP Encryption Algorithm	Specify the algorithm used for data encryption							
Authoritization algorithm	Specify digital signature authentication algorithm for encrypted							
Authentication algorithm	data							
DES group	PFS (Perfect Forward Secrecy), which means that a key is cracked							
	and does not affect the security of other keys							
Survivo timo	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.



0 R40B - L2TP - LuCI	× +						– Ø ×
→ C ▲ Not sec	ure 192.16	8.3.1/cgi-bin/luci/admi	in/vpn/l2tp				☆ \varTheta :
	R40B	Status - System -	Services - Network - VPN	N ≁ Serial Port ≁ RTU I/O ≁	Logical operation - C	Cloud platform - Logout	
	L2TP L2TP in: Below is a l	stances ist of configured L2TP insta	ances and their current state				
	Name	User Name	Server/Client	IPSec Encryption	State	Enable	
			This se	ection contains no values yet			
		A	dd				
					Save & Ap	pply Save Reset	
	Powered by	r KingPigeon Technology C	:o., 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	erver,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	× +							- o ×
← → C ▲ Not secu	re 192.168.3.1/cgi	-bin/luci/admin/vp	n/openvpn					☆ 🔒 :
	R40B Status -	System - Serv	ices - Network - VPN		- RTU I/O - Logical	l operation - Cloud p	latform - Logout	
	OpenVPN							
	OpenVPN insta Below is a list of config	I NCES gured OpenVPN insta	nces 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 KingPige	on Technology Co., Lt	d. (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	Select file uplead reat cartificate provided by conver
authorization (root certificate)	Select file upload, root certificate provided by server
	Select file upload, the client certificate generated by the user based
Local certificate	on the root certificate
Local private key	Select the file upload, the key corresponding to the client certificate
DIL Kov ovehenge nerometers	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
Reepairve 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 Port Settings								
Item		Description							
Modbus Device ID		Range 1~247, default is 1							
	Paud 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							
	Roud rate	1200,2400,4800,9600,14400,19200,38400,57600,							
	Bauurale	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

(11) R40B - Serial Port Applicatio	on × +							-	- 0	×
← → C ▲ Not secur	re 192.168.3	8.1/cgi-bin/luci/a	admin/serial/ser2ne	t					☆ 8) :
	R40B 8	Status 👻 System	- Services - Ne	etwork - VPN - Se	rial Port + RTU I/O +	Logical operation -	Cloud platform - Logout			
	Serial P Serial State	Port								
	Index	Serial Name	Serial Type	Received By	tes Transi	mitted Bytes	Clear Statictis			
				This section cor	tains no values yet					
	Parameter	r <mark>Setting</mark>								
	Device	Baudrate	Usage Mode	Net Protocol type	Host IP or Doma	in Port				
							Edit Delete)		
							Edit Delete			
	Add									
						Save 8	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 Davias ID	Set when mode is modbus slave, default is 1, please modify in the serial									
	port settings									
Network Protocol	TCP server,TCP client,UDP server,UDP client									
Host IP or domain name	Select the client to be visible, set the connection server address here									
Dest	Set the connection server port when the client is selected, and set the									
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

4G Wireless Industrial Router Wireless Data Connectivity

(0) R40B - Modbus Master - LuCI	× -	F										-	- 0	×
← → C ▲ Not secure	e 192.1	<mark>68.3.1/</mark> c	gi-bin/luci/ad	min/serial/m	odbus								\$ E	9 :
1	R40B	Statu	s - System -	Services -	Network -	VPN - Serial Port -	rtu i/o 🚽	Logical opera	ition - Cloud	l platform	- Logout			
1	Modk Modbu	ous N s Setti	Master ing								NSAVED CHANGES: 1			
	Name	Alias	Slave Address	Register Type	Function Code	Register Start Address	Data Number	Mapping Address	Enable	Query	Detail Settings			
					5	This section contains no v	alues yet							
				Add										
									Save & Apply	Save	Reset			
F	Powered I	oy KingPi	geon Technology	y Co., Ltd. (v1.1	8) / 2020-10-1	6								

(m) R40B - LuCI	× +										-	٥	×
$\leftarrow \rightarrow \mathbf{C}$ A Not set	ecure 192.168	.3.1/cgi-bin/luci/adi	min/serial/m	odbus/deta	il/test						Ť	7 0) :
	R40B s	Status - System -	Services -	Network +	VPN ·	- Serial Port -	rtu I/0 -	Logical operation -	Cloud platform -	Logout			Ê
	Config De	Detail							UNSA	VED CHANGES: 13			
	Mapping Address	Alias	Data Type	Input Typ)e	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 🗸					
	72		Bool	Open	•]	None 🗸					
	73		Bool	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 Modbus device ID, If the cloud connection setting			
Slave address	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 assigr	nment	Automatic / manual				
		Select Manual Assignment Visible;				
		Boolean type mapping register address 64~256,				
Mapping start address		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 slave	e interface select RS485 or RS232				
	Device	RS485 or RS232				
		1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600				
Serial setting	Baud rate	115200, 230400, 460800				
	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 × +	– o ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/admin/io/email	☆ 🛛 :
R40B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Lo	ogical operation - Cloud platform - Logout
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	m 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 an address and click the "+" on the right to save, at the same time the second input box will appear below, you can 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

(••) R40B - Digital input and output ×	+							_	٥	>
\leftrightarrow \rightarrow C A Not secure 192	2.168.3.1/cgi-bin/luci/ac	lmin/io/dido						\$	Θ	
R40B	Status + System +	Services - Netw	vork + VPN + S	erial Port + RT	J I/O 🗕 Logical o	operation + Cloud p	platform + Logout			
DIDC)						UN SAVED CHANGES: 15			
Index	In Name	Mode	State (Count	Clean	Enable/Disable				
1	DI1	in	Low (D	Clean	Enabled				
2	DI2	in	Low (D	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					
Trigge	r Setting									
In Nam	e Trigger Condition	Threshold Value	Confirm Time(s) Action	Hold Time(s)	Triggering				
DI1	DI Low	0	44	Reboot		Not trigger	Edit Delete			
D12	DI Low	0	1	DO2Close	5	Not trigger	Edit Delete			
Add										

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

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

Digital output Instructions

Wiring




instruction:

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

5.7.3 Analog input

R40B Statu	us - System - Services -	Network - VPN -	Serial Port + R	TU I/O 👻 I	Logical oper	ation + Cloud plati	form - Logout	
AIN							UN SAVED CHANGES: 15	
AIN Seting								
In Name	Mode		Min Value	Max	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 Setti	ng							
In Trigg Name Cond	ger Threshold dition Value	Resume Threshold	Confirm Time(s)	Action	Hold Time(s)	Triggering		
							Edit Delete	
Add								
						Savo & Apply	Sava	

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



4G Wireless Industrial Router Wireless Data Connectivity

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

5.7.4 Device Monitor

(••) R40B - Device Monitor&Al	arm × +							-	٥	×
← → C ▲ Not sect	ure 192.168.3.1/cgi-bi	n/luci/admin/io/monito)r						☆ (9 :
	R40B Status -	System - Services -	Network - VPN - Se	rial Port - RTU I/O	- Logical ope	eration - Clou	d platform → Logout			
	Device Monifor	tor					UNSAVED CHANGES: 15			
	Register Address	In Name Status	Device IP Address	Ping Times	Action H	lold time(s)	Enable setting			
			This section cor	tains no values yet						
	Add									
						Save & Apply	Save Reset			
	Powered by KingPigeon	Technology Co., Ltd. (v1.18	i) / 2020-10-16							

Device Monitor				
Item	Description			
Register address	Range 2~63			
	DI3~DI64, Automatically generated according to the register			
	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

(••) R40B - Alarm Setting - Luc	ci × +							- 6	×
← → C ▲ Not sect	ure 192.168.3.1/c	gi-bin/luci/a	dmin/io/alarm					ቷ	0 ()
	R40B Statu	s - System	✓ Services ✓	Network - VPN -	Serial Port + RTU I/O +	Logical operation -	Cloud platform - Log	jout	
	Event And	Alarm					UNSAVED CH	ANGES: 15	
	LVCIILAIIC	Παιτιί							
	Index	Alarm N	ame	Alarm De	scription	Alarr	m Time		
				This section of	contains no values yet				
	Add Alarm								
	Alarm Name		Send SMS	Short Message Conten	t Send Email	Email Content			
	DI1:open	~					De	alete	
	DI1:open	~					De	alete	
	DI1:open	~					De	alete	
	Add								
						Save & A	Apply Save Re	eset	
	Powered by KingPi	geon Technolo	gy Co., Ltd. (v1.	8) / 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 ×
\leftrightarrow \rightarrow C A Not secu	ure 192.168.3.1/cgi-bin/luci/admin/io/timer	☆ 🛛 :
	R40B Status * System * Services * Network * VPN * Serial Port * RTU I/O * Logical operation * Cloud platform * Logout	
	LINSAVED CHANGES 15	
	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	

4G Wireless Industrial Router Wireless Data Connectivity

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

(1) R40B - Logical operation - Lu	c x +	- 0	×
← → C ▲ Not secure	e 192.168.3.1/cgi-bin/luci/admin/logic/logic	☆	9 :
R	240B Status + System + Services + Network + VPN + Serial Port + RTU I/O + Logical operation + Cloud platform + Logout		Î
L	ogical operation		
B	lool input		- 1
	Name Input1 Condition Relationship Input2 Condition Output Address Output Value Logic Value		- 1
8	1 REG64 Open Logic And DI1 Open REG64 Open 1 Edit Delete		- 1
	Add		- 1
N	lumberical input		- 1
	Name Input1 Condition Threshold Relationship Input2 Condition Threshold Output Address Output Value Logic Value		- 1
	This section contains no values yet		- 1
	Add		- 1
c	combined input		- 1
	Name Input1 Condition Relationship Input2 Condition Output Address Output Value Logic Value		- 1
	This section contains no values yet		- 1
	Add		Ţ
c	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 × +							-	٥	×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/	admin/cloud/host_set						۲	7 0	:
R40B Status - System	n - Services - Network -	VPN - Serial Port -	RTU I/O 👻 🛛 L	Logical operation 👻	Cloud platform -	Logout			
Cloud connectio	n settings				UNSAVI	ED CHANGES: 15			
Cloud connection set	tings								
Enable setting									
Cloud platform	King Pigeon IIoT V2	~							
Link Protocol	MODBUS RTU	~							
Modbus Device ID	1 @ 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 Co., Ltd. (v1.18) / 2020-10-16

Cloud Connection Settings						
Item		Description				
Enable setting		Tick to enable				
Cloud Platform		King Pigeon IIOT V2,IIOT V3,others				
Host IP or domain	n name	Connect Server Port				
Port		Connect to other cloud platform server ports				
Link Protocol		Modbus RTU, Modbus TCP , MQTT				
	Modbus Device ID	Default is 1				
D.4. dlava	Register packet	Server register handshake protocol package, if need contact salesman				
	Heartbeat packet	Heartbeat content to avoid network offline				
Protocol	Heartbeat response packet	The server responds to the heartbeat packet				
Parameters	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.				
MQTT Protocol Parameters	Username	The user name used in the MQTT connection message, which can be used by the server for authentication and authorization.				
	Password	The password used in the MQTT connection message, which can be used by the server for authentication and authorization.				
	Publish topic	The subject name used in the MQTT publish message. The subject name is used to identify the information channel to which the payload data should be published.				



		The subject name in the publish message cannot contain				
		wildcards.				
		The topic name used in MQTT subscription messages.				
	Subscribe topic	After the subscription, the server can send publish				
		messages to the client to achieve control.				
	Publish Period (seconds)	MQTT data timing publish interval				
		Service quality level guarantee for application message				
	Publisher QOS	distribution: 0-at most once, 1-at least once, 2-only once				
	Encruption	Optional unencrypted, encrypted (root certificate),				
	ЕПСТУРЛОП	encrypted (self-signed)				
	Authentication and					
	authorization	Choose file upload				
	(root certificate)					
	Local certificate	Choose file upload				
	Local private key	Choose file upload				
	Enable data transfer	Enable to work				
	Data packing	Send multiple data in one message				

5.9.2 Ali Cloud

(••) R40B - Ali Cloud - LuCl	× +										- 0 ×
← → C ▲ Not secu	re 192.168.3.1/cgi-	bin/luci/ad	dmin/cloud/ali_	cloud							☆ \varTheta :
	R40B Status -	System ·	- Services -	Network -	VPN -	Serial Port -	rtu I/o 🕶	Logical operation -	Cloud platform -	Logout	
				_					UNSA	VED CHANGES: 15	
	Cloud conn	ection	settings								
	Cloud connecti	on settir	ngs								
	Enab	e setting									
	Authentication	n method	Device Serect		~						
	Product Key(Pro	ductKey)									
	Device Name(Devi	c <mark>e</mark> Name)									
	Device Serect(Devic	eSerect)									
	F	egion ID	Please of	choose	•						
	Publish	Period(s)	> 60								
								Save 8	Apply Save	Reset	

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

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

4G Wireless Industrial Router Wireless Data Connectivity

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

(10) R40B - Aws Cloud - LuCl × +					- 0 ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci	/admin/cloud/aws_cloud				☆ \varTheta :
R40B Status - System	✓ Services ✓ Network ✓ V	/PN - Serial Port - RTU I/	O ▼ Logical operation ▼	Cloud platform - Logout	
Cloud connection	n settings			UNSAVED CHANC	HES: 15
Cloud connection sett	ngs				
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				
	(g) /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			
Publich tonic	name is used to identify which information channel the payload			
	data should be published to. The subject name in the published			
	message cannot contain wildcards.			
Publish period (seconds)	>60			
Certification authority (root certificate)	Choose file upload			
Local certificate	Choose file upload			
Local key	Choose file upload			

5.9.4 Huaweicloud



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

certificate:

💁 Google 翻译 🛛 🗙 (**) R40B - Huawei Cloud - LuCl 🗙 🕂		- o ×
← → C ▲ 不安全 192.168.3.1/cgi-bin/luci/admin/cloud/hw_cloud		☆ 🛛 :
🥪 金錦物联网云V3.0 🤹 Google 翻译 🛛 🤕 金錦准生产		
R40B Status + System + Services + Network + VI	PN + Application + RTU I/O + Logical operation + Cloud platform + Logout	



entication method	Device Serect	~		
Device ID				
Secret key		*		
Service ID				
Region ID	CN North-Beijng4	•		
Publish Period(s)	> 60			

Powered by KingPigeon Technology Co., Ltd. (v1.20.1) / 2021-02-03

	Huaweicloud co	onnection settings				
Item	Description					
Enable setting	Tick to enable					
Authentication method	The device secret key method and the authentication certificate method can be selected, and the authentication certificate method needs to upload the certificate					
	The ID of the de device,eg, R40A • Offlir	evice when HUAWEI CLOUD creates the				
Doviedo ID	Node ID	R40A				
Device iD	Device ID	5ee965a0496bac073bb6120d_R40A				
	Registered	Jun 17, 2020 08:37:57 GMT+08:00				
	Node Type	Directly connected				
	Software Version	v1.0				
Service ID	The product needs Model Definition Add Service Import Service ID: R40	S to create a service to report data,eg. Online Debugging Topic Management Library Model Import Local Profile Import from Excel				
Region ID	The location of th	e device can be gueried on the HUAWEI				



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

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

5.10 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

	: Wirele	ss Ind Wi	lust reie	rial R ss Da	oute Ita Co	r Dnne	
(**) R40B - Custom Cloud - LuCI × +							- o ×
← → C ▲ Not secure 192.168.3.1/cgi-bin/luci/	admin/cloud/host_set						☆ 🛛 :
R40B Status - System	n - Services - Network -	VPN - Serial Port -	RTU I/O -	Logical operation -	Cloud platform -	Logout	
Cloud connectio	n settings				UNSAV	ED CHANGES: 15	
Cloud connection set	tings						
Enable setting							
Cloud platform	King Pigeon IIoT V2	~					
Link Protocol	MODBUS RTU	~					
Modbus Device ID	1 Modbus device ID is set in S	erial Port Settings					
Register Packet							
Heartbeat Packet							
Heartbeat Response Packet							
Heartbeat Period(s)	60						
Host Silence Time(s)	600						
				Save 8	Apply Save	Reset	
Powered by KingPigeon Technol	ogy 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: Close
1	10002	DI2		Wet contact: 0: Low level (0~1VDC) 1: High level (5~30VDC)
2~21	10003~10022	Network disconnection detection device IP (max 20 IPs can be set)		0:offline 1:online

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

4G Wireless Industrial Router Wireless Data Connectivity

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	Peel	0: Open
1	00002	DO2	DUUI	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
Returning data	1	01H	Return DI data
16CRC Verify	2	6048H	CRC0 CRC1 low byte in front, high byte behind

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

Server send: 01 02 00 00 00 02 F9 CB

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

Device return: 01 02 01 01 60 48

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



0= Open, 1= Close.

DI2	DI1
0	1
Open	Close

60 48: 16 byte CRC verify.

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

6.1.2.3 Read Device Digital Output DO Status

Master Send Data Format:

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

Receiver Return Data Format:

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

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

Server Send: 01 01 00 00 00 02 BD CB

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

Device Answer: 01 01 01 02 DO 49

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

DO2	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 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	OFH	Write multi holding coil, function code 15
DO Starting	2	00.0011	Demons 202011 202111 stands for DOO DO1
Register Address	Z	00 00H	

IG Wireless Industrial Router Wireless Data Connectivity

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	1	00.0011	Parace 0000 0001 stands for DO1 DO2
Address		00 00H	
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

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	04H	Read input register, function code 04
Register Starting Address	2	00 00H	Every 2 16-bit address corresponds to 1 AI 32-bit register
Read Register Qty	2	00 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 Al 4 and the DI pulse count 2

Master Send Data Format:



16 CRC Verify

FOOFH

2

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 06=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	Dealacatura
65	00066 or 10066	Bool 65	Bool	Boolean type,
66	00067 or 10067	Bool 66	Bool	slave mapping address, can
			Bool	holding coil state
			Bool	102 addrossos in total
256	00257or 10257	Bool 256	Bool	

2) 16 Bit Slave Register Assignment Table

Read and Write Holding Register (Function Code 03,04, 06, 16)				
Modbus 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 320131	32 Bit data 20130	Same as above	Same as above
20132	420133 or 320133	32 Bit data 20132	Same as above	Same as above
	64 data similar as above		Same as above	Same as above
20254	420255 or 320255	32 Bit data 20254	Same as above	Same as above



6.1.3.2 Read Boolean Mapping Address Data

Master Send Data Format:

Content	Bytes	Data	Description
Device ID	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	01H	Read holding coil type, function code 01
Boolean Register	2	00.4011	Range: 0040H-0100H, address refer to ["Slave
Starting Address	2	00 40 1	Mapping Register Address"]
Read Register Qty	2	00 0AH	Range: 0001H-00C1H
16 CRC Verify	2	BD D9H	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

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

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

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

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

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

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

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

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

5D 0C CRC Verify.

6.1.3.3 Modify Boolean Mapping Address Data

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

Master Send Data Format:					
Content	Bytes	Data	Description		



Wireless Industrial Router 46 **Wireless Data Connectivity**

		(H: HEX)	
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	2	00.400	Range: 00 40H-0100FH, address refer to ["
Register Address	2	00 40H	Mapping Register Address"]
W/rito valuo	2		This value: FF 00H or 00 00H, FF 00H stands for write 1;
	2	FFUUH	00 00H stands for write 0
16 CRC Verify	2	8D EEH	CRC0 CRC1 low byte in front, high behind

Receiver Return Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, according to the data Master send
Function Code	1	05H	Write single holding coil
Boolean Mapping	2	00.4011	Range: 00 40H-0100FH, address refer to ["
Register Address	2	00 40H	Mapping Register Address"]
Write value	2		This value: FF 00H or 00 00H. FF 00H stands for write
white value	2		1,00 00H stands for write 0.
16 CRC Verify	2	8D EEH	CRC0 CRC1 low byte in front, high behind

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

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

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

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

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

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

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

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

6.1.3.4 Read Data Type Mapping Address Data

Master Send Data Format:

Content	Bytes	Data (H: HEX)	Description
Device Address	1	01H	01H Device, Range: 1-247, according to setting address
Function Code	1	03H	Read holding register, function code 03
Mapping Register Starting Address	2	4E 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:

Wireless Industrial Router **Wireless Data Connectivity**

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
		00 14 00 1E 00	
Returning Data	20	28 00 32 00 4B	Poturning Data
		00 41 00 0A 00	
		25 00 14 00 2AH	
16 CRC Verify	2	FB 34H	CRC0 CRC1 low byte in front, high behind

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

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

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

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

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

Register Mapping	20010	20000	20008	20007	20006	20005	20004	20002	20002	20001
Address	20010	20009	20008	20007	20000	20005	20004	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	45.2111	Mapping data type address range, refer to ["Slave
Address	2	4E 21H	Mapping Register Address"]
Write Data	2	00 64H	Data writing value is Decimal data 100
16 CRC Verify	2	CF 03H	CRC0 CRC1 low byte in front, high behind

Master Send Data Format:

Receiver Return Data Format:

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





(uploads data to Broker)



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

6.2.3 Device Communication Application

Client configuration

1. Connect Platform: 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 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
    "Ing":"116.3",
                                             // longitude data
    "lat":"39.9",
                                            // latitude data
    "spd":"0.0",
                                            // speed data
  "dir":"0.0",
                                         // direction data
    "flag":"GPS"
    }
],
"time":"1602324850"
                                     //Time , data release timestamp UTC format
    "retransmit":"enable"
 //Retransmission flag, indicating historical data (retransmission historical data only has this flag,
```

```
real-time data does not have this flag)
```

```
}
```



Note:

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

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

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

The GPS longitude character is "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	REG64~256	Switcher	Defined according to slave data
16 Bit	REG20000~20127	Value	Defined according to slave data
32 Bit	REG20128~20254	Value	Defined according to slave data

Note:

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

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

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

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

Publish Topic: serial numbers					
"switcher": "0",					
"flag": "DI1",					
"time": "1602324850"					

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

Device Subscribe MQTT Format 6.2.5

The payload data format in the device subscription message

4G Wireless Industrial Router Wireless Data Connectivity

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

4G Wireless Industrial Router Wireless Data Connectivity

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>

