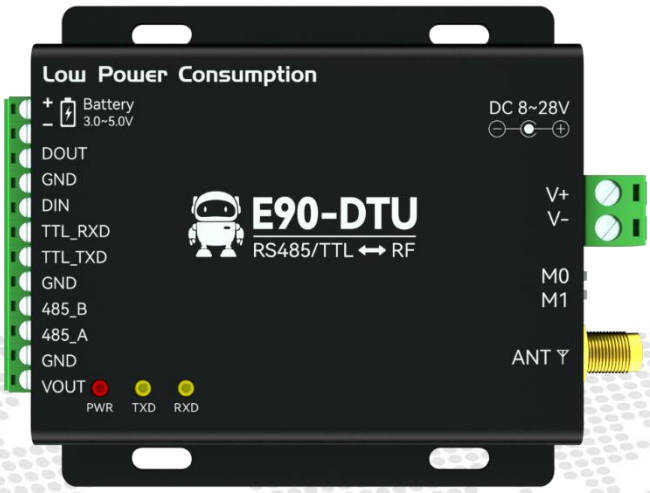
Chengdu Ebyte Electronic Technology Co.,Ltd

Wireless Modem

User Manual



E90-DTU(400SL30L)
Low-power digital radio
User Manual

CONTENT

Chapter 1 Product Description

1.1 Product introduction

E90-DTU (400SL30L) is a wireless data transmission radio using military-grade LoRa modulation technology. It has a variety of transmission methods and works in the (410.125~493.125MHz) frequency band (default 433.125MHz). The radio provides RS485 and TTL two kinds of serial communication Port, support 8~28V DC power supply or 4.2V lithium battery power input, support reverse constant current charging;

The introduction of the Modbus RTU protocol can configure the working mode of the digital radio through the configuration register, which is convenient for customers to access their own configuration system (HMI or SCADA software, etc.) through the Modbus protocol for radio management, and provides the convenience of a host computer that does not need to understand the Modbus protocol. Configuration by users who do not understand the protocol;

Ultra-low power consumption design, the lowest standby current consumption is only 38uA, supports battery power supply (3.7-4.2v) and reverse charging, and the radio integrates switch value acquisition (dry contact) and switch value output (transistor) for remote acquisition control, and the device can provide power for low-power sensors;

Multiple automatic polling commands can be configured to support automatic Modbus CRC check;

1.2 Features

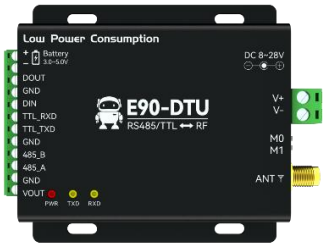
- Using the latest LoRa technology, the distance is farther and the performance is more powerful than the traditional LoRa digital radio;
- Using military-grade LoRa modulation technology, the transmission is more secure, and the packet length can be configured;
- Oversized single packet, single packet supports up to 240 bytes, and adapts to Modbus protocol;
- Based on standard Modbus RTU design, it is convenient to access different configuration systems;
- Support a variety of serial communication ports (TTL and RS485) to facilitate access to sensors of different protocols;
- Simple and high-efficiency power supply design, support power adapter or pressure line method, support DC 8 ~ 28V wide voltage input;
- Support lithium battery power supply and reverse charging, and support battery voltage detection and low battery feedback;
- The transmission power can reach up to 1W, and supports multi-level adjustment, and all technical indicators meet European industrial standards;

- Ultra-low power design, low power mode standby current is only 38uA;
- The sensor (VOUT) power output can be controlled to adapt to sensors with different power supplies;
- Integrate one switch value acquisition and one switch value output, which can realize device control without external remote IO;
- Support switch value acquisition status change and lithium battery low battery reporting;
- Support wireless sending Modbus commands to remotely configure or read radio parameters;
- Working temperature range: -40℃～+85℃, suitable for all kinds of harsh working environment, real industrial grade products;
- All aluminum alloy shell, compact size, easy installation, good heat dissipation; perfect shielding design, good electromagnetic compatibility, strong anti-interference ability;
- Multiple protection functions such as DC input reverse connection protection and antenna surge protection greatly increase the reliability of the radio;
- Powerful host computer, all parameters can be set by programming: such as power, frequency, air rate, address ID, etc., providing a remote configuration interface;

Chapter 2 Quick Start

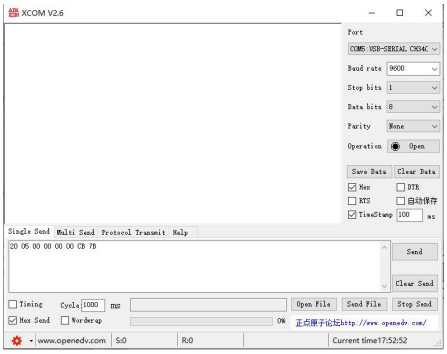
2.1 Hardware preparation

In order to test the E90-DTU (400SL30L), the following hardware is required:
One PC with more than two USB-A ports;
Two low-power output radios E90-DTU (400SL30L) (hereinafter referred to as "radio");
Two DC12V1A power adapters to provide power for low-power digital radio;
RS-485 cable and flat-blade screwdriver for connecting USB to RS-485 and radio;
TX433-JKD-20P, two 433MHz internal thread and internal needle antennas;

			
E90-DTU(400SL30L)*2	Power adapter (12V1A)*2	USB to RS-485*2	
			
PC	Several RS485 cables	Slotted screwdriver (SL-3.0)	TX433-JKD-20P *2

2.2 Software preparation

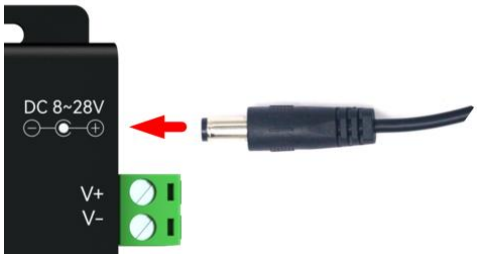
The product details on the Ebyte official website provide the configuration host computer "E90-DTU-400SL30L.exe" and the serial port assistant "XCOM.exe" to download, as shown in the figure below.
Official website address: https://www.ebyte.com.

	
E90-DTU-400SL30L.exe	XCOM.exe

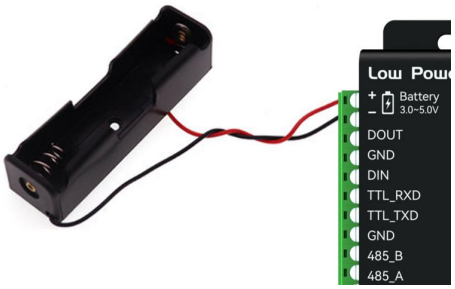
[Note] The pictures provided in the manual may be different from the software provided on the official website, and the official website shall prevail;

2.3 Equipment wiring

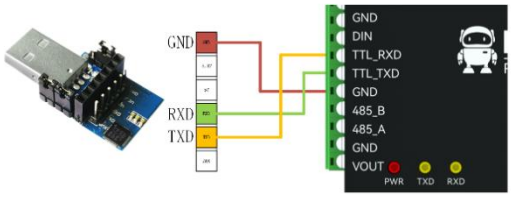
DC power access, support DC 8~28V input:



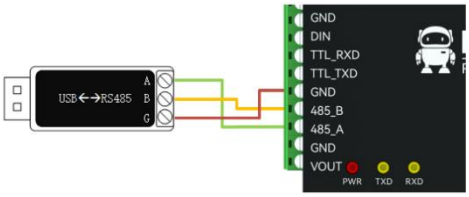
The battery power supply is connected. After connecting to the DC power supply, the battery power supply can be connected. The following figure takes the 18650 battery box as an example. The red (+), black (-), positive and negative poles must be connected correspondingly, otherwise the equipment will be damaged:



Signal line access, RS-485 or TTL-3.3V, serial ports cannot be used at the same time, only one of them can be used at the same time:



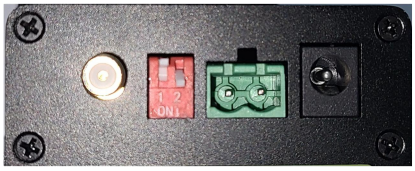
USB to TTL connected device



USB to RS485 connected device

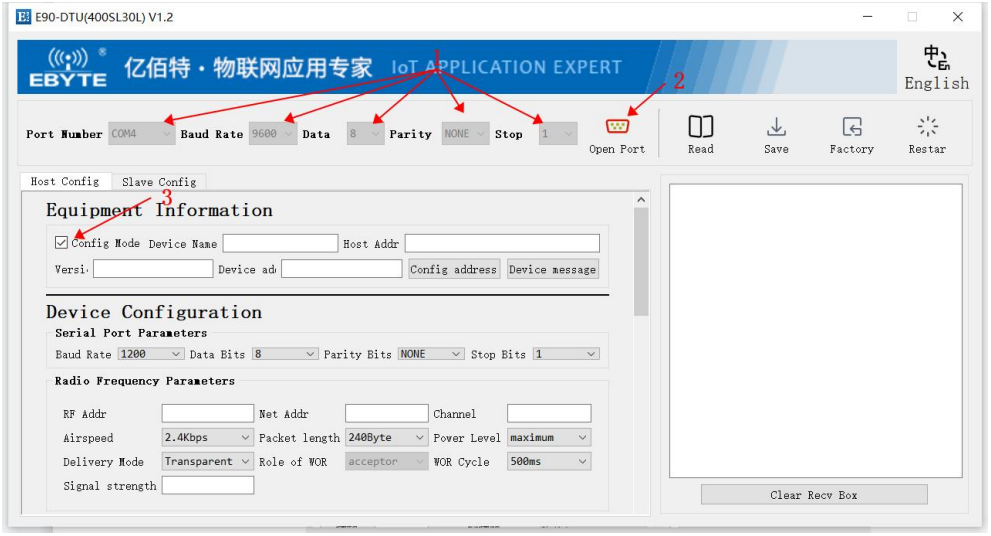
2.4 Quick to use

Switch the radio to configuration mode, as shown below:

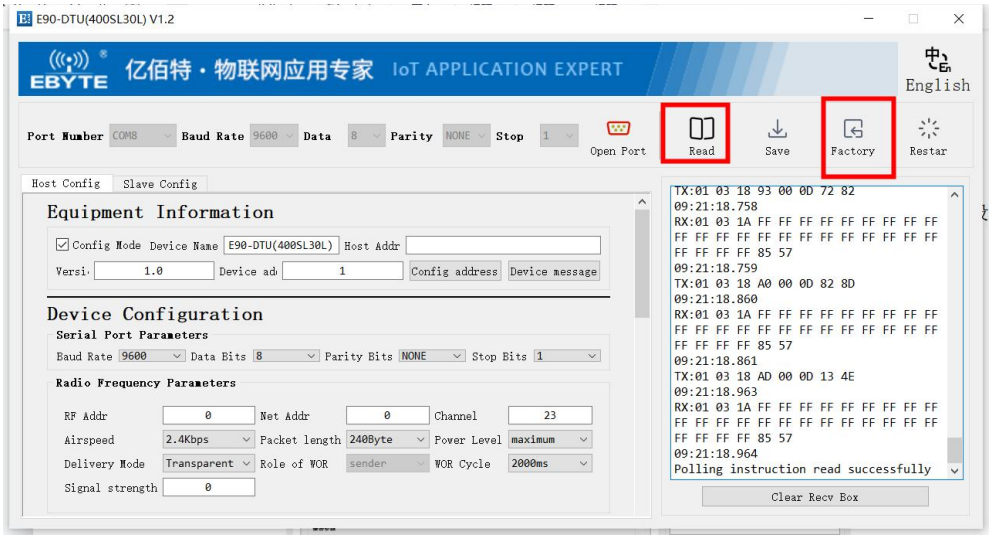


Config Mode

Turn on the host computer, confirm the correct baud rate parameter "1", click "Open serial port", confirm whether the host computer configuration mode is checked, the device is in configuration mode, this parameter should be checked, as shown in the following figure:



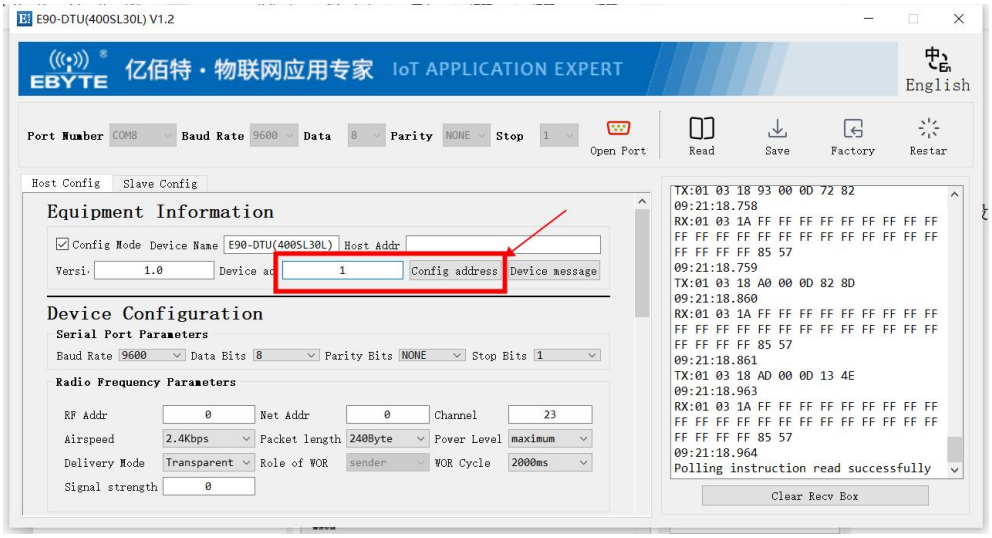
The purpose of the "Quick Start" here is to use the device quickly, and the parameters use the factory parameters. If the device has been configured before, click "Factory Settings" to restore the factory parameters:



Click "Read Parameters" to know that the default Modbus address of the device is 1. If the serial bus connected to the device already has address 1, the address can be configured to other values here. If Modbus RTU protocol transmission and remote configuration are not performed, it can be ignored. address parameter;

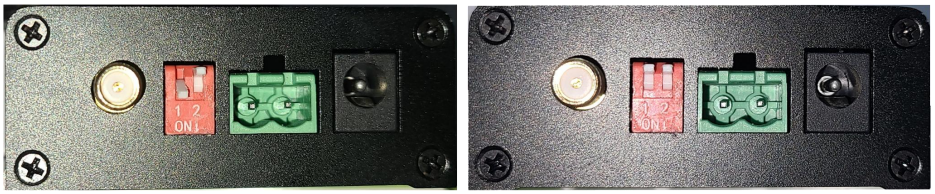
After the configuration is complete, click "Restart Device", and all parameters will take effect after restarting;

Use the same method to configure another low-power digital radio, and modify the Modbus address to 2 to avoid address conflict during remote configuration and Modbus RTU transmission. No Modbus RTU protocol transmission and remote configuration can be ignored, as shown in the following figure:

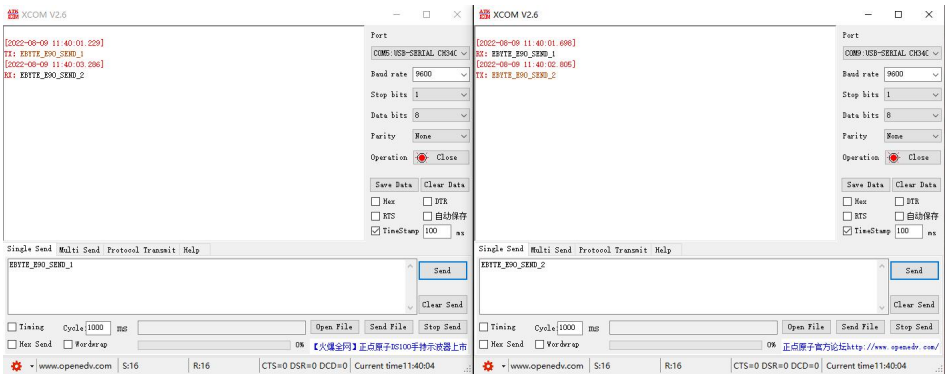


Click "Reboot Device":

To exit the "configuration mode" only need (M0 dial up), you can send and receive data, as shown in the figure below:



Send and receive as follows:



Chapter 3 Product Overview

3.1 Technical parameters

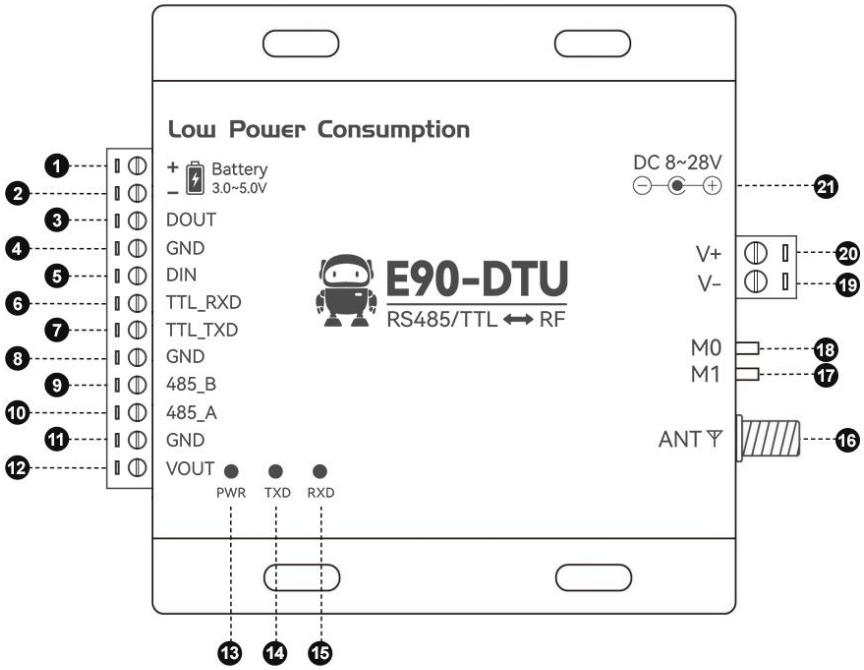
Item	Description	
Operating Voltage	DC 8～28V	Support DC head and terminal power supply access
Working current	DC powered	Standby current consumption: 11mA @ 12V Transmit current consumption: 288mA @ 12V Low power standby current consumption: 302uA @ 12V Transmit power is instantaneous power, standby power is average power Airspeed: 62.5kbps, WOR period: 4000ms
	Battery powered	Standby current consumption: 21mA @ 4.2V Transmit current consumption: 448mA @4.2V Low power standby current consumption: 38uA @ 4.2V Transmit power is instantaneous power, standby power is average power Airspeed: 62.5kbps, WOR period: 4000ms
Communication Interface	TTL	3.3V-TTL serial level communication interface
	RS-485	Standard RS-485 communication interface
Frequency Range	410.125～493.125MHz	
channel	0～83, the default is 23, the channel interval is 1MHz	
airspeed	2.4, 4.8, 9.6, 19.2, 38.4, 62.5Kbps, default 2.4Kbps	
Power regulation	Support 4 gear transmission power configuration	
reverse charging	120mA constant current charging, 4.2V preset charging voltage	
Communication distance	10Km	
User configuration	Host computer and Modbus RTU command	
Operating mode	Transparent transmission, Modbus slave, low power consumption, automatic acquisition	
Subcontracting mechanism	Support configuration as 32, 64, 128, 240Byte, default 240Byte	
Serial port baud rate	1200、2400、4800、9600bps(default)	
data bits	7, 8 (default 8)	
stop bit	1, 2 (default 1)	
Check Digit	NONE, ODD, EVEN (default NONE)	

Antenna interface	SMA-K, external thread internal hole
Product Size	84mm*82mm*25mm (length*width*height)
product weight	133 g ± 5 g
Working temperature and humidity	-40 to +85℃, 5% to 95%RH (non-condensing)
Storage temperature and humidity	-40 to +105℃, 5% to 95%RH (non-condensing)

【Note】:

1. The test transmission power is an instantaneous value. It is recommended to reserve 50% of the current margin when selecting the power supply, which is conducive to the stable operation of the radio for a long time;
2. The lower the transmit power, the closer the transmission distance is, but the working current will not decrease proportionally. It is recommended to use the maximum transmit power;
3. Use multiple groups of digital radios to communicate one-to-one at the same time in the same area. It is recommended that each group of digital radios set the channel interval to be more than 3MHz;

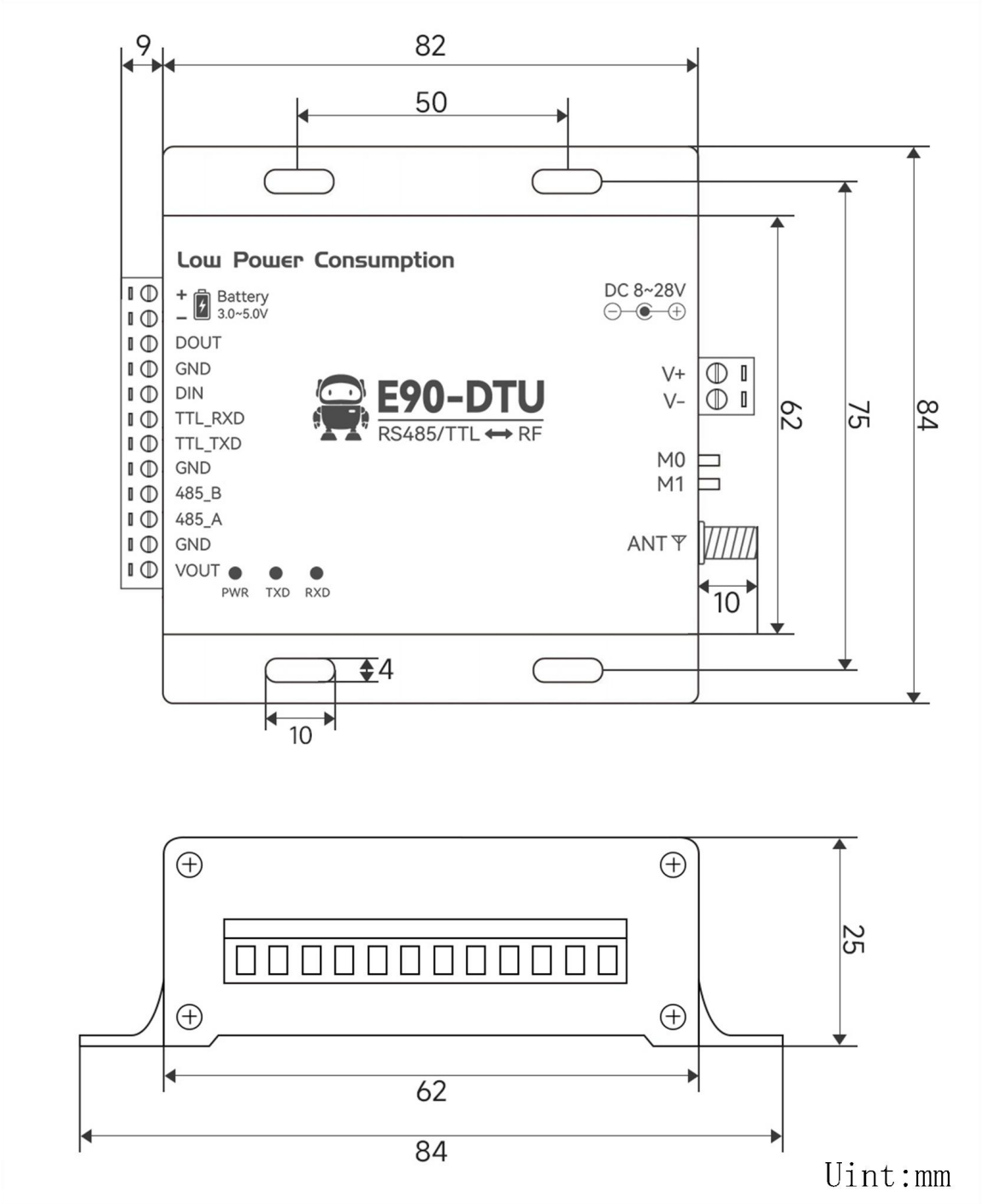
3.2 Interface and indicator description



Item	Tag	Function	Description
1	Battery+	Positive pole of battery power supply interface	DC 3.0 ~ 5.0V, pay attention to the positive and negative poles of the battery, do not

2	Battery -	Negative terminal of battery power supply interface	reverse, support the battery charging function
3	DOUT	transistor output	The output wiring mode is NPN, the load voltage is less than 30V, and the maximum allowable current is 100mA
4	GND	Input and output common terminal	
5	DIN	dry contact input	Switch input detection
6	TTL-RXD	TTL-3.3V signal input	When using TTL, it is necessary to connect the signal common terminal, and it cannot be used with the RS485 interface at the same time.
7	TTL-TXD	TTL-3.3V signal output	
8	GND	TTL-3.3V signal common terminal	
9	485-B	B of RS-485 signal	Cannot be used with TTL interface at the same time
10	485-A	A of RS-485 signal	
11	GND	Negative power output	The total current of the load connected through VOUT should be <1A
12	VOUT	Positive power output	
13	PWR	Power Indicator	Host: turn on the power and keep on; Slave: On when the low-power mode wakes up, off when entering low-power mode, and always on when not in low-power mode;
14	TXD	send indicator	Blinks when sending data
15	RXD	Receive indicator	Blinks when receiving data
16	ANT	Antenna interface	SMA-K
17	M1	Master-slave configuration dial	Dial down for the host
18	M0	configuration mode	Dial down for configuration mode
19	V-	Negative pole of DC 8~28 V	DC 8~28 V, 2*5.08mm phoenix terminal input; Do not supply power at the same time as the socket;
20	V+	Positive pole of DC 8~28 V	
21	DC-IN	DC power input	DC 8~28 V; In-line round hole, outer diameter 5.5mm, inner diameter 2.0mm; Do not supply power with the terminals at the same time;

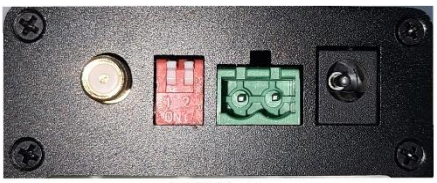
3.3 Dimensions

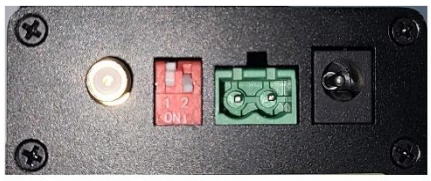


Chapter 4 Function Introduction

4.1 DIP configuration instructions


MODE 1


MODE 2


MODE 3

Icon	M0 (Dial 2)	M1 (Dial 1)	Mode
MODE 1	Up	Down	Host Mode (WOR Transmitter)
MODE 2	Up	Up	Slave Mode (WOR Receiver)
MODE 3	Down	X（Random）	Configuration Mode

Note: The external Modbus slave station needs to avoid the address used by the radio to avoid the communication bus address conflict:

4.1.1 Configuration mode

M0 (that is, dial code 2) is dialed and the device is in configuration mode, the device uses a fixed baud rate (9600-8N1), a fixed Modbus address (01H), or the Modbus address configured by the device (uncheck "Configuration Mode" , and enter the current device address in the "host address" input box, otherwise use a fixed address to access the device), the wireless transmission in the configuration mode enters the dormant state, and wireless transmission and reception cannot be performed.

4.1.2 Host mode

M1 (bottom) and M0 (top) devices are in host mode. The radio configured in host mode can obtain and configure the Modbus registers of the radio through the serial port. The parameters modified in host mode will take effect immediately. In low power mode HMI, SCADA software and other Modbus registers The host device needs to be connected to the host radio, and Modbus slaves such as PLC and remote IO need to be connected to the slave radio.

In the host mode, the VOUT interface of the radio does not output power, and does not support automatic serial port polling.

4.1.3 Slave mode

Both M1 and M0 dial up and the device is in slave mode. The radio configured as a slave cannot obtain and configure the Modbus register from the serial port of the radio. It can only remotely configure parameters through the connected host radio, and it needs to be restarted to take effect. Write 0001H to the device holding register 07EAH to restart the device.

In slave mode, the radio VOUT interface outputs power and supports serial port automatic polling function.

4.2 Device parameters

4.2.1 Baud rate parameters

Item	Range	Defaults
baud rate	1200、2400、4800、9600	9600
data bits	7、8	8
check digit	NONE、ODD、EVEN	NONE
stop bit	1、2	1

The device only has one serial port that supports RS-485 and 3.3V-TTL serial port protocols, and does not support simultaneous access to both interfaces.

If the RS-485 interface is used, it needs to be connected with the terminal equipment in the way of A to A, B to B, and the GND between the devices can be connected at the same time;

If the 3.3V-TTL interface is used, the TXD needs to be connected to the terminal device RXD, and the RXD is connected to the terminal device TXD, and the GND interface between the devices must be connected.

4.2.2 Local modbus address

The device supports configuration parameters through Modbus RTU protocol, so the device must have a unique device address in the network (non-Modbus RTU protocol transmission can ignore the device address),

support configuration is 1-247 (factory default: 1), when forgetting the device address At this time, you can use address 1 in the configuration mode (see "DIP Configuration Instructions") to read the device address information stored in the holding register 07E8H.

4.2.3 Battery level (VBAT) monitoring

By obtaining the 32-bit single-precision floating-point value stored in the holding registers 00C8H and 00C9H, the unit is V, the radio detects the power in a period of 10s in non-low power mode, and the low power mode needs to configure the detection period (holding register 1B5CH is used to store cycle, the factory default is 10 minutes).

[Note] Single-precision floating-point values are stored in standard IEEE754 format.

It supports DC input to charge the battery, using 120mA constant current charging, and the preset charging voltage is 4.2V.

4.2.4 Sensor (VOUT) power configuration

The sensor (VOUT) power supply can select the power source through the configuration holding register 1B5DH, which is configured as 0x00 (ie synchronous DC power supply, the output voltage is DC 8-28V), and configured as 0x01 (ie synchronous VBAT input power supply);

[Note] The total current of the load connected through VOUT should be <1A. Overload use will cause irreversible damage to the device. In addition, the output power of the device is related to the input power supply and has nothing to do with the device.

4.3 Wireless parameters

4.3.1 Basic parameters

(1) LORA device address

The device address is used to distinguish different devices when sending and receiving at a fixed point. For details, see the chapter "Sending at a fixed point". The same address should be configured for transparent transmission, otherwise data cannot be sent and received normally.

0xFFFF (ie 65535) is the broadcast address, which can monitor all data on the same channel.

(2) LORA network address

The network address is used to distinguish different communication networks, and the network addresses of devices that communicate with each other should be set to the same parameters.

The low-power radio cannot be used as a repeater, and can be used with the same series of digital radios (for example: E90-DTU (400SL30) as a repeater to relay data between low-power radios).

When the relay is in use, the low-power radio cannot use the low-power mode, otherwise it will not be able to send and receive data normally.

(3) Airspeed class

The higher the airspeed, the faster the transmission, the closer the transmission distance, the default is 2.4Kbps, and the airspeeds of the devices that communicate with each other must be consistent;

(4) Channel

Configure different transmission frequencies, support 84 channels (410.125 ~ 493.125), each channel is separated by 1MHz, and the channels of devices that communicate with each other must be consistent (non-fixed-point mode);

(5) Transmit power level

Support four kinds of transmit power adjustment: high (30dBm±0.5), medium (reference value: 27dBm), low (reference value: 24dBm), very low (reference value: 21dBm). The power will not reduce the power consumption of the whole machine in the same proportion, and it is not recommended to reduce the power usage;

(6) Subpackage length

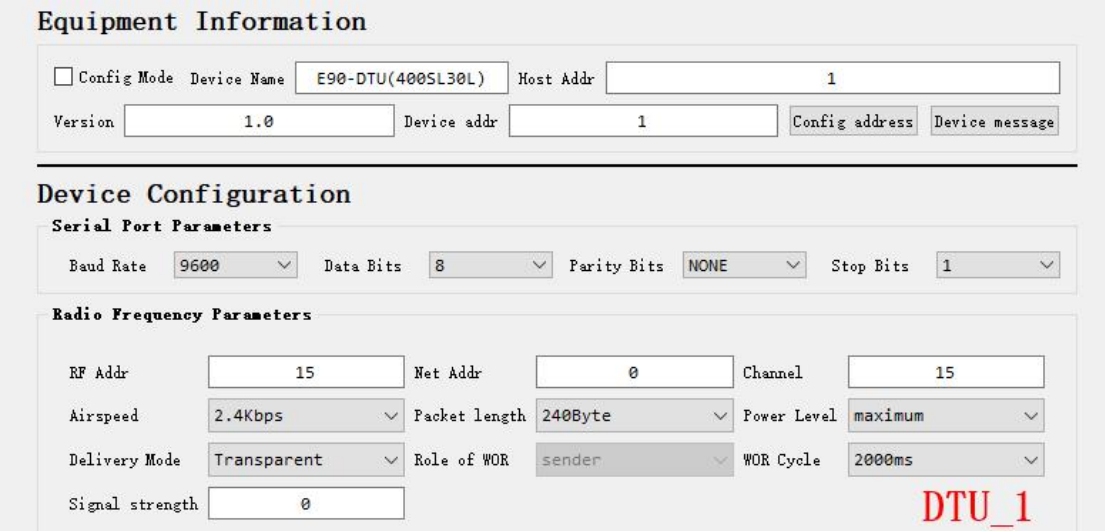
The maximum number of bytes of data in a single frame, data that exceeds the packet length is invalid, and the packet lengths of devices that communicate with each other must be the same;

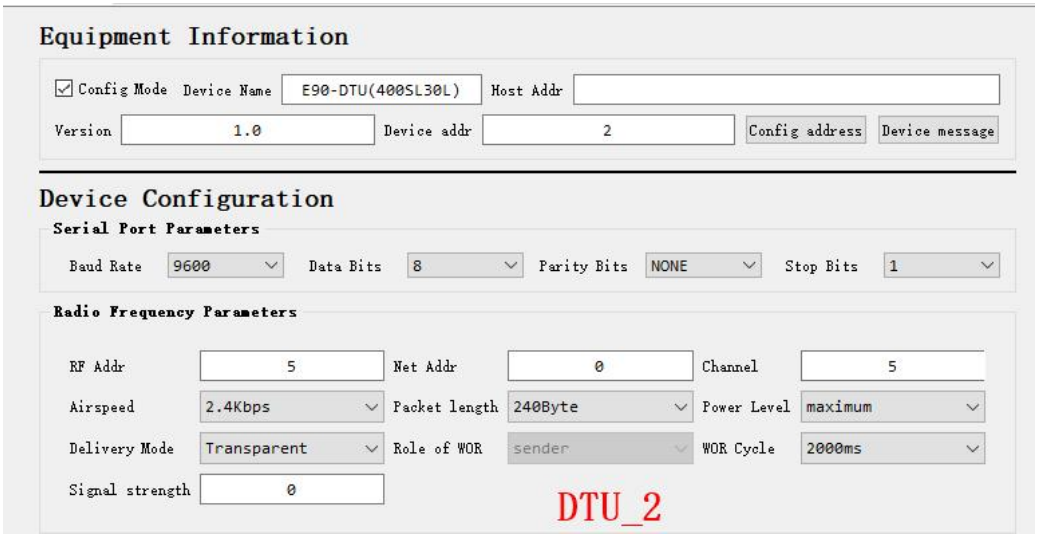
(7) Signal Strength Feedback (RSSI)

The initial state is 0. After receiving the data, the newly acquired signal strength will be stored in the holding register 0B88H. The closer the 256-RSSI is to 0, the better;

4.3.2 Fixed point sending

Support address function, the radio can transmit data to any address, any channel module, to achieve networking, relay and other applications: For example: DTU_1 (address is 0x000F, channel is 0x0F) need to send data to the radio DTU_2 (address is 0x0005, channel is 0x05) transmit data AABBCC (HEX: 414142424343), its communication format is: 000505414142424343 (HEX), where 0005 is the address of the radio station DTU_2, and 05 is the radio station DTU_2 channel.

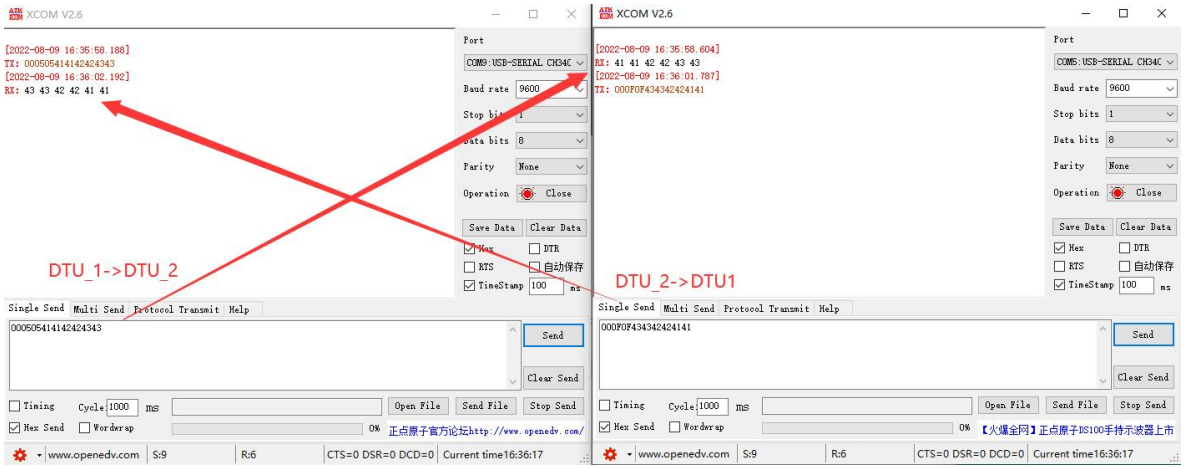




Fixed-point sending demo:

To send DTU_1 to DTU_2, you need to add 00 05 05 (HEX) before the data;

To send DTU_2 to DTU_1, add 00 0F 0F (HEX) before the data;



4.4 Remote IO acquisition control

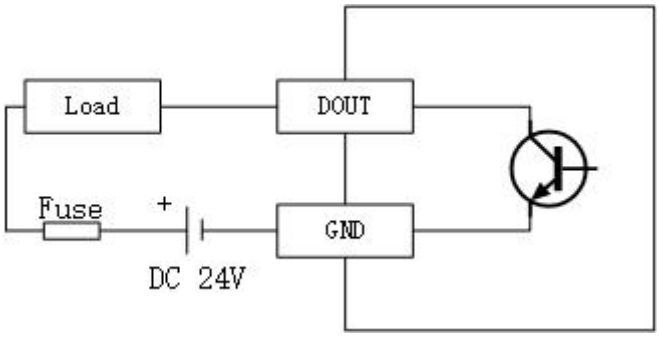
4.4.1 Switch value acquisition

The device has a dry contact input interface for detecting digital input, and the input status can be inquired through the Modbus RTU command (the DI register address is 20001, see "Modbus register table" for details).

In configuration mode, the input status can be queried through Modbus commands (HEX: 01 02 00 00 00 01 B9 CA).

4.4.2 Switch output

The switching value of the equipment adopts the equivalent circuit of transistor output type as shown in the figure below, and the transistor output can only be used for the DC24V load circuit. The output wiring mode is NPN, the load voltage is less than 30V, and the maximum allowable current is 100mA.



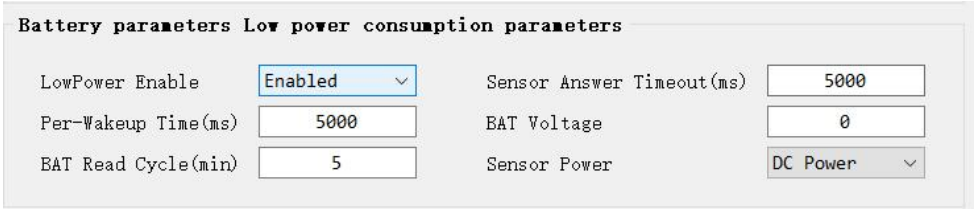
4.5 Low power operation

4.5.1 Function description

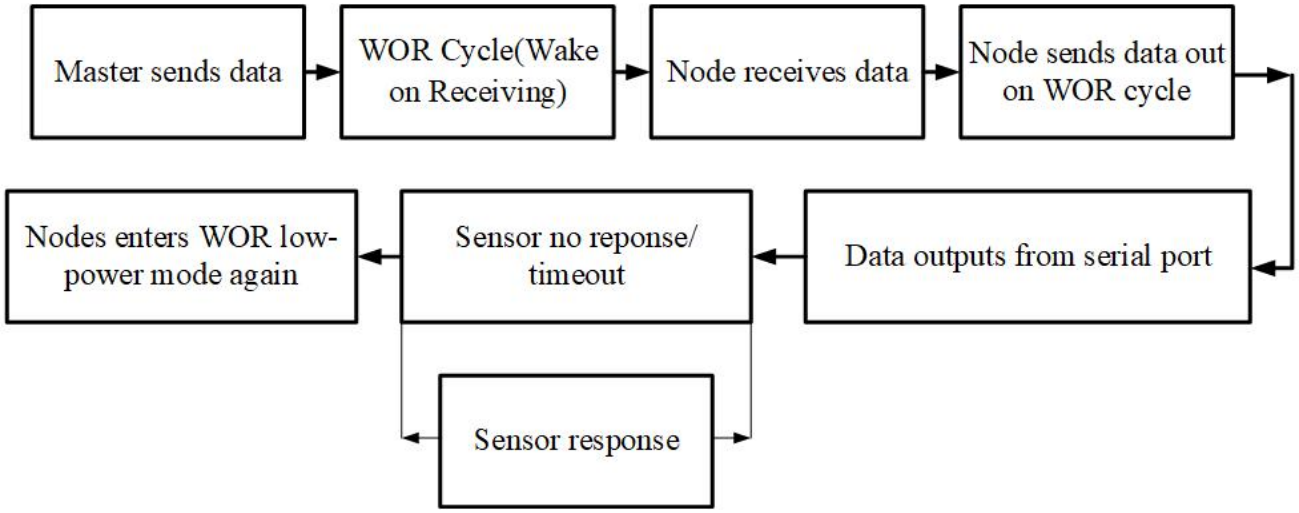
E90-DTU (400SL30L) digital radio supports ultra-low power consumption standby, using 4.2V lithium battery for power supply, the minimum standby power consumption can reach 38uA @ 12V, and can be adapted to outdoor applications where wiring is impossible or difficult.

The low-power mode requires the master and slave to be enabled at the same time. After the master is enabled, it will add a wake-up code before the data to wake up the slave. If the master uses a non-low-power mode, it will cause abnormal communication and cause data loss. The same "WOR period" needs to be used;

The low power consumption mode can only work in a working environment similar to the Modbus request method (that is, the master initiates a request, and the slave responds immediately). ” is used to output the sensor power in advance. If the sensor power is not controlled by the “radio”, this parameter can be configured as 0. “Sensor response timeout” is used for the time for the slave to receive serial data. Power consumption standby.



In low power consumption mode, after the host sends data, the slave will not output data from the serial port immediately, but will wait for the "WOR wake-up period" and "early wake-up time" before outputting data, and the slave will only output data when the "sensor response timeout" The data will be sent correctly within the time limit. The specific waiting process is shown in the figure below:

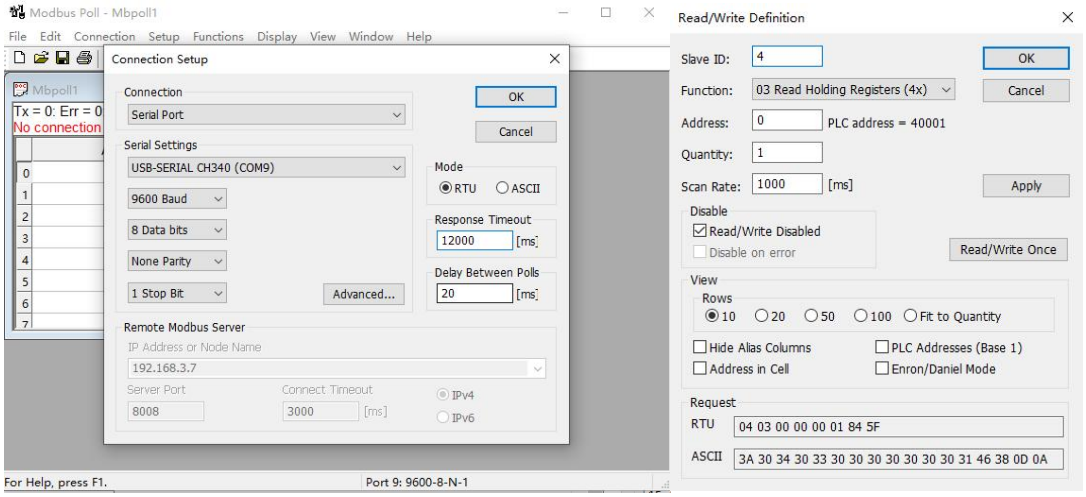


4.5.2 Modbus RTU protocol demonstration

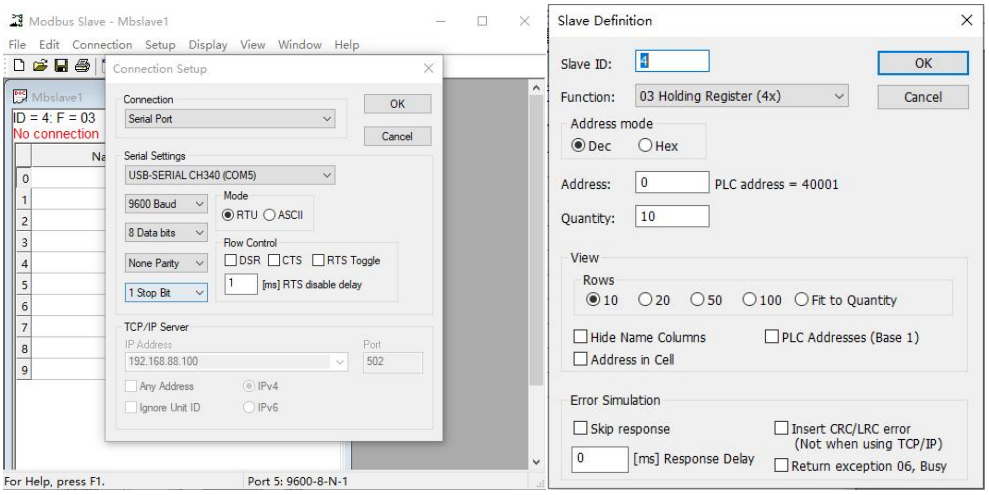
First dial down the M0 dial code, after the configuration parameters are completed, switch the host to the left mode and the slave to the right mode, and the host configuration parameters are as shown in the figure below (left), and the slave configuration parameters are as follows (right).

Use the Modbus simulation master (Modbus Poll) to connect with the "radio" configured as the master mode, and use the Modbus simulation slave (Modbus Slave) to connect with the "radio" configured as the slave mode.

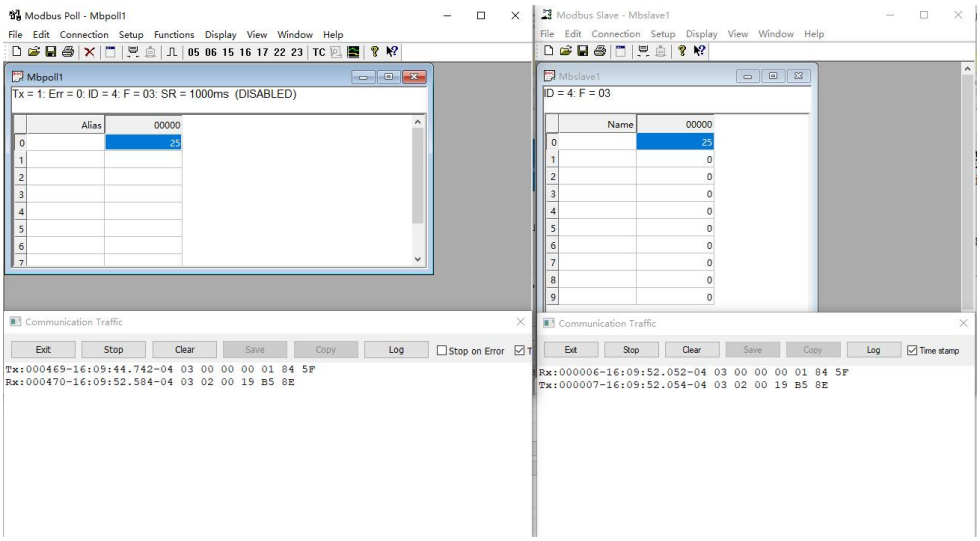
The host timeout time of Modbus Poll simulation needs to be adjusted according to "WOR period", "early wake-up time", "sensor timeout time", Modbus host timeout time = WOR period + early wake-up time + sensor timeout time, read device address configuration For 4, avoid addresses 1 and 2 used by "station";



The slave configuration of Modbus Slave simulation is as follows:

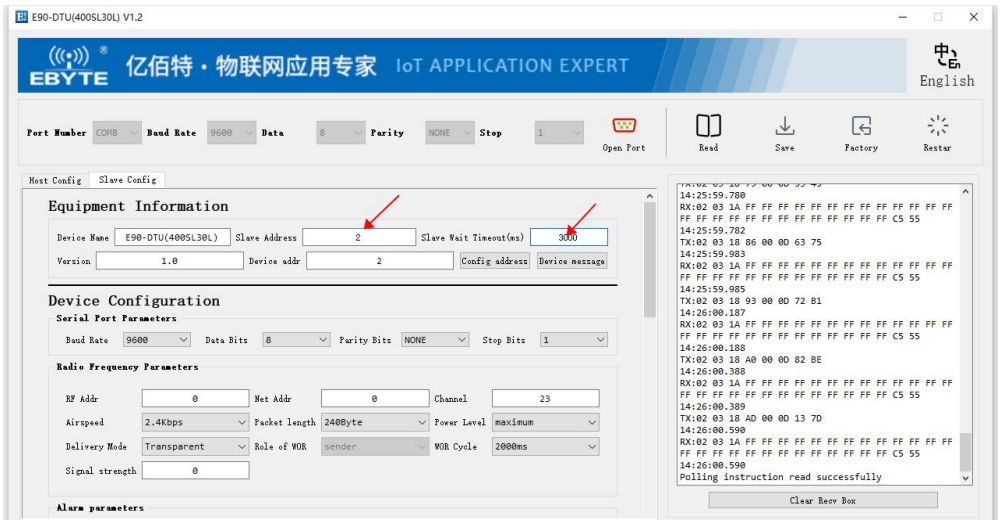


The communication effect is as follows, it can be seen that after the Modbus master sends data, it needs to wait for about 7000ms before outputting from the serial port of the slave radio station:



4.6 Remote configuration

The slave mode radio can be remotely configured through the radio configured as master mode. The Modbus address of the master radio is 1, and the Modbus address of the slave radio is 2. In the host computer slave configuration interface, configure the "slave address" as 2, Appropriately increase the "waiting for slave response time". In order to ensure stable communication, 3000ms is used here. Click "Read Configuration" to get the slave configuration parameters.



4.7 Serial port auto polling

When the device is in slave mode, it supports configuring multiple polling commands for automatic collection. The command length can be configured up to 20 bytes. It supports a variety of serial port protocols (RS485 and 3.3V-TTL cannot be used at the same time), and the collection cycle and command interval can be flexibly configured. Query interval, support automatic verification of Modbus-CRC (open by default).

4.7.1 Configuration instructions

The automatic polling instruction table starts from the holding register (0x1838), and there is a set of polling instruction data for every 13 registers (one register is 2 bytes), and supports configuration of up to 10 instructions. The details of the register bits are as follows:

<table>
<tr><th colspan="4">A set of 13 registers</th></tr>
<tr><th>register 1</th><th>register 2</th><th>register 3</th><th>Register 4 - Register 13 (stores Modbus commands)</th></tr>
<tr><td rowspan="2">instruction length</td><td>overtime time</td><td>instruction interval</td><td rowspan="2">Command content (hexadecimal), up to 20 bytes</td></tr>
<tr><td>>0 start, in milliseconds
0-65535ms</td><td>0-255ms</td></tr>
</table>

Command length: range (0x01-0x14), indicating the length of the command data, for example, to configure the Modbus command "0x010100000008", you need to configure the length to 0x06;

Timeout time: the configured command wait time for response, and start the command interval timer after the timeout. This parameter has the same meaning as the Modbus timeout time. The configured time needs to be consistent with the request waiting time. For example, the Modbus request needs to be configured with the timeout of the PLC/HMI/PC. The time is the same.

Command interval: the interval for sending the next command after sending one command is completed;

Instruction content: store the instruction in hexadecimal, up to 20 bytes can be stored:

4.7.2 Configuration demo

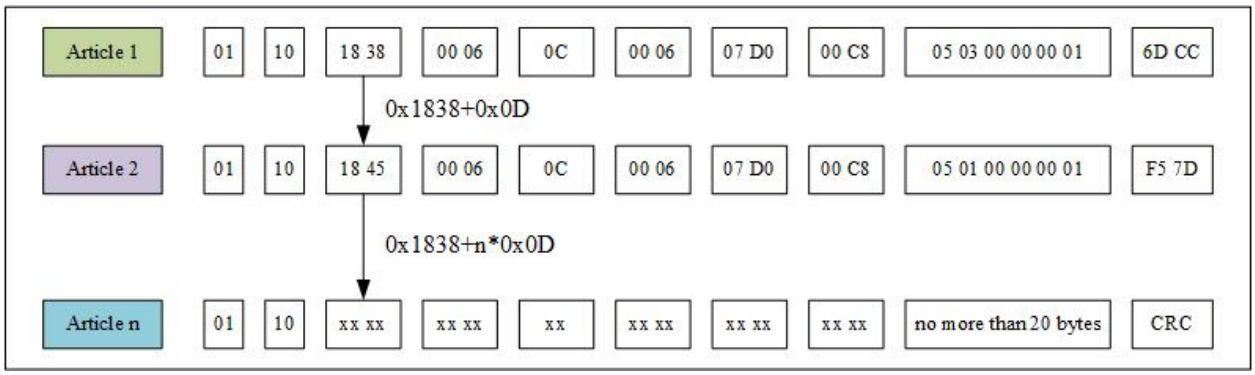
The following demo is based on the Modbus RTU protocol test, which needs to be enabled to automatically add Modbus-CRC check, if other protocols choose to turn off Modbus-CRC check according to actual needs.

Configure the first polling instruction table, the write timeout time is 2000ms, the interval for sending the next instruction is 200ms, and the query holding register address is the content stored in 0000H;

01 10 18 38 00 06 0C 00 06 07 D0 00 C8 05 03 00 00 00 01 6D CC

Configure the second polling command table, the write timeout time is 2000ms, the interval for sending the next command is 200ms, and the query address is the coil status of 0000H;

01 10 18 45 00 06 0C 00 06 07 D0 00 C8 05 01 00 00 00 01 F5 7D



"Article 1" states:

"01": The Modbus address of the device, the configuration mode is fixed to 01H, and the Modbus address corresponding to the device needs to be used for non-configuration;

"10": 13 holding registers need to be operated at the same time, so use the 10H function code for configuration, and can also be modified individually through 06H;

"18 38": the first address of the register, each instruction is separated by 13 registers, and supports up to 10 instructions (n supports up to 10);

"00 06": The number of configuration holding registers is related to the instruction length. For example, the instruction length in the figure is 6 bytes plus the fixed consumption of 6 bytes, so the next bit is "0x0C";

"00 06": The length of the storage instruction, the figure is "0x050300000001", a total of 6 bytes;

"07 D0": Timeout time, the figure is configured as 2000ms;

"00 C8": instruction interval, the configuration shown in the figure is 200ms;

"050300000001": storage instructions, up to 20 bytes of hexadecimal instructions;

4.8 Alarm function

When the device is in slave mode, DI status and battery power status feedback can be achieved by enabling the alarm level register combined with DI enable and battery power enable.

4.8.1 Alarm level

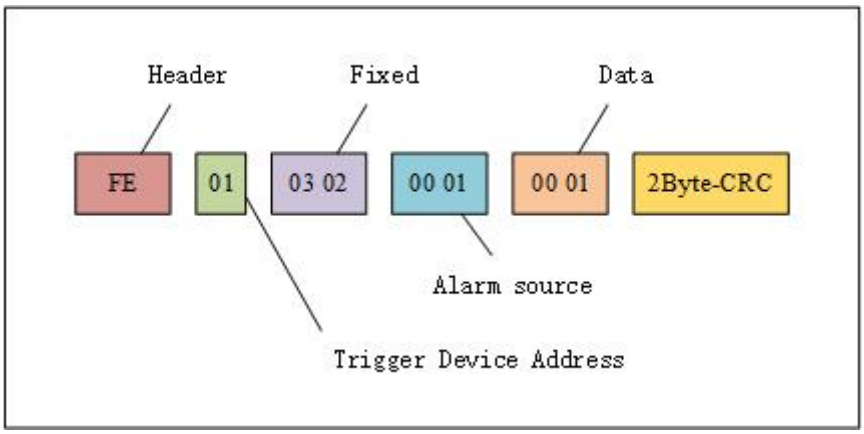
Two alarm modes are supported as shown in the table below：

Value	Function	Directions

0x00	turn off the alarm	Disable alarm function
0x01	send once	Send an alarm message
0x02	at least once	If the clear command is not received, it will be reported three times with a cycle of 5s

If the level 2 is used, the alarm status register needs to be cleared after the alarm is generated, otherwise the device reports three times to automatically cancel the alarm in a period of 5s, and immediately cancels the alarm status after receiving the clear alarm clear;

The format for reporting an alarm is as follows:



"Header": the first byte, used to identify the data frame as alarm data;

"Trigger Device Address": the second byte, the slave address that triggers the alarm state;

"Fixed": the third and fourth bytes, fixed at 0x0302;

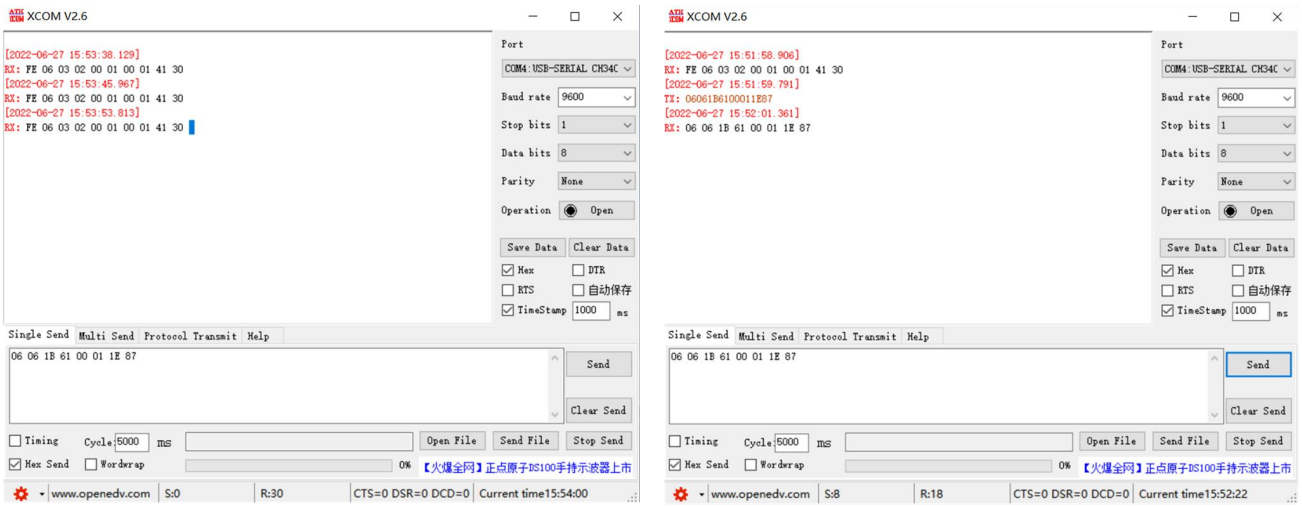
"Alarm source" and "Data"：

Type	Alarm source	Data
DI	0x0001	0x0001 (fixed)
AI	0x0002	reserved (not supported)
battery voltage	0x0004	Battery voltage, in mV

"2Byte-CRC": The last 2 bytes represent Modbus-CRC checksum data；

4.8.2 Alarm status clear

Demonstration of alarm level 2 clearing DI as an example:



The picture on the left shows the alarm report of the device without clearing after the alarm is generated, and the picture on the right shows the report of the device alarm after manual clearing.

4.8.3 Alarm source configuration

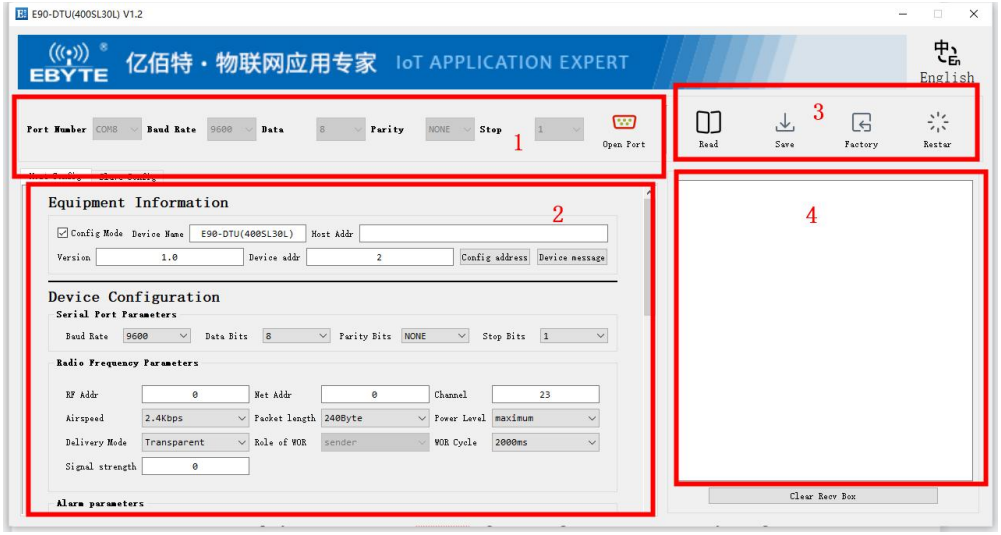
DI alarm source:

The alarm mode can be configured through the register. The normal mode supports the configuration of the disconnection alarm and the closing alarm. The device cannot use the disconnection alarm when the device is in low power mode. The closed alarm supports low-power wake-up.

Battery Alarm Voltage Configuration:

The configurable range (0x00-0x0F) increases by 0.05V, the minimum configuration is 3.45V (0x00), and the maximum configuration is 4.20V (ie 0x0F);

Chapter 5 Host Computer



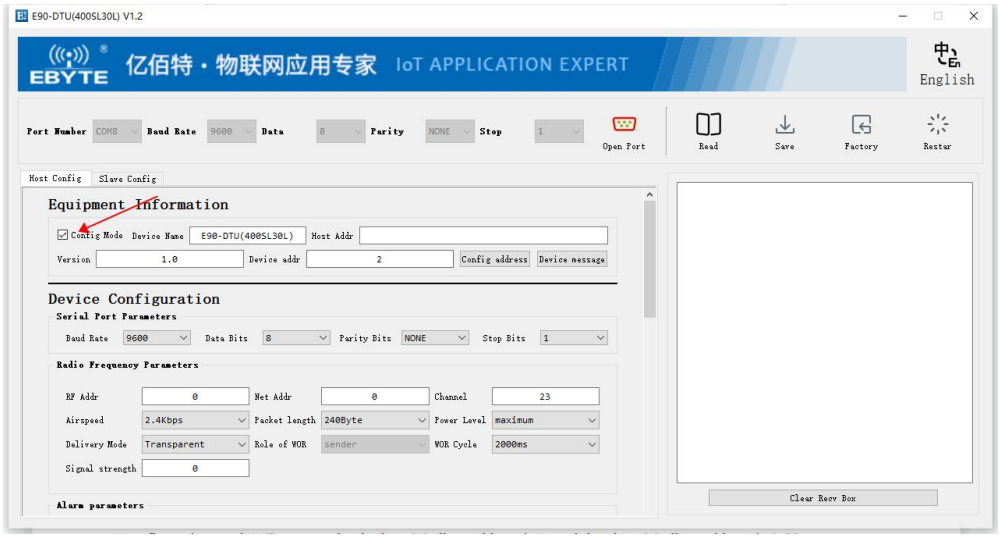
①Area 1 is the parameter configuration area used to connect the radio station, which needs to be configured corresponding to the radio station. For example, if the radio station is configured as 9600-8N1, then you need to select the port number of the USB to serial port connecting the radio station, configure the baud rate to 9600, and the data bit is 8, the parity bit is NONE, and the stop bit is 1;

②area is used to display the current device Modbus register configuration, write the newly configured parameters through this area, click "Save Parameters" in ③ area to write the Modbus register;

③area is used to read or write Modbus register parameters, and can also control the device through "factory device" and "restart device";

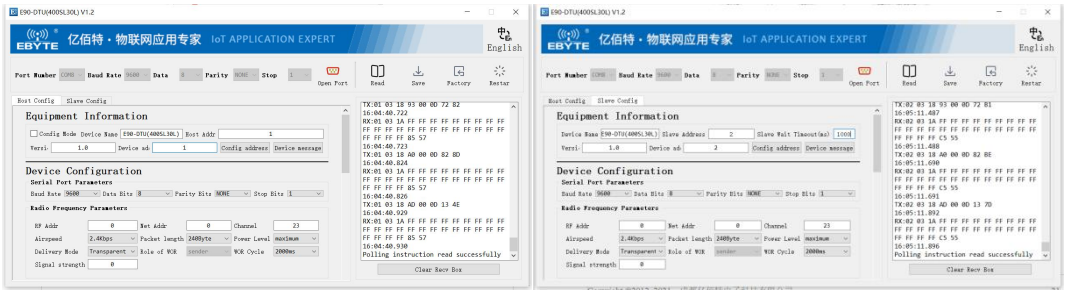
④area is used to display the operation log of the upper computer;

When the radio is in "configuration mode", the communication address can be fixed by checking the "configuration mode" of the upper computer (Modbus communication address is fixed at 1).



If you remember the device address, you can also modify the device parameters without entering the "configuration mode". For example, the host Modbus address is 1, and the slave Modbus address is 2. You can connect the host radio through the serial port to configure the parameters of the remote slave and local host.

Method As follows:



Chapter 6 Modbus Protocol Description

E90-DTU (400SL30L) adopts the standard Modbus RTU protocol for configuration, and the Modbus RTU communication protocol adopts the master-slave response method for data communication. First, the host (PC, HMI, etc.) initiates a request through a unique slave address, and the slave (terminal device) responds according to the host's request, that is, half-duplex communication. This protocol only allows the host to initiate a request and the slave to respond passively, so the slave will not actively occupy the communication line to cause data conflict.

The device provides a host computer developed based on the Modbus protocol for users to use, and can also be compatible with other Modbus host computers through the Modbus protocol. For detailed register descriptions, see "Modbus Register Table".

6.1 Introduction to Modbus RTU protocol

6.1.1 Communication format

Information transmission is asynchronous, using hexadecimal for communication, information frame format:

address code	function code	data area	CRC check code
1 byte	1 byte	N byte	2 byte

6.1.2 Communication information transmission process

When the communication command is sent by the master to the slave, the slave that matches the address code sent by the master receives the communication command. If the CRC check is correct, the corresponding operation is performed, and then the execution result (data) is returned to the master. The returned information includes address code, function code, executed data and CRC check code. If the address does not match or the CRC check error, nothing will be returned.

6.1.3 Address code

The address code is the first byte of each communication frame, and supports 1 to 247. Each slave must have a unique address on the bus, and only the slave that matches the address code sent by the master can respond to the returned data.

6.1.4 Function code

The function code is the second byte of each communication frame. The host sends, and informs the slave to perform the corresponding operation through the function code.

The device supports the following eight function codes:

function code	definition	operation
01H	read coil	Read one or more consecutive coil states
05H	write a single coil	Manipulate the status of the coil at the specified position
0FH	write multiple coils	Manipulate multiple consecutive coil states
02H	Read discrete input	Read one or more consecutive discrete input states
04H	read input register	Read one or more consecutive input register data
03H	read holding register	Read data from one or more holding registers
06H	Write a single holding register	Write two hexadecimal data to the corresponding location
10H	Write to multiple holding registers	Write 4*N hexadecimal data to N consecutive holding registers

6.1.5 Function code 01H: read coil

For example: if the host wants to read a coil state whose slave address is 01H and the starting coil address is 00H, the host sends:

Host sends		Send data (HEX)
address code		01
function code		01
Start coil address	high byte	00
	low byte	00
Number of coils	high byte	00
	low byte	01
CRC check	low byte	FD
	high byte	CA

If the slave register 00H coil is closed, the slave returns:

Slave return		Send data (HEX)
address code		01
function code		01
number of bytes		01
Coil Status		01
CRC check code	low byte	90
	high byte	48

6.1.6 Function code 05H: write single coil

For example: if the host wants to control the coil state with the slave address of 01H and the coil address of 0000H, the host sends:

Host sends	Send data (HEX)

address code		01
function code		01
Coil address	high byte	00
	low byte	00
control method	high byte	00 (open), FF (close)
	low byte	01
CRC check	low byte	XX
	high byte	XX

The slave returns the same as the master request;

6.1.7 Function code 0FH: write multiple coils

For example: if the host wants to control 4 coil states whose slave address is 01H and the starting coil address is 00H, the host sends:

Host sends		Send data (HEX)
address code		01
function code		0F
Start coil address	high byte	00
	low byte	00
Number of coils	high byte	00
	low byte	04
number of bytes written		01
control method		00 (all open), 0F (all closed)
CRC check	low byte	XX
	high byte	XX

Function code 0FH operate, slave return：

Slave return		Send data (HEX)
address code		01
function code		0F
Start coil address	high byte	00
	low byte	00
Number of coils	high byte	00
	low byte	04
CRC check	low byte	54
	high byte	08

6.1.8 Function code 02H: read discrete input

For example: the host wants to read 4 input states whose slave address is 01H and the starting discrete address is 00H, host sends：

Host sends		Send data (HEX)
address code		01
function code		02
Start discrete address	high byte	00
	low byte	00
number of reads	high byte	00
	low byte	04
CRC check	low byte	79
	high byte	C9

If all 4 discrete inputs starting from the machine head address 00H detect the input, slave return：

Slave return		Send data (HEX)
address code		01
function code		02
number of bytes		01
discrete input state		0F
CRC check code	low byte	E1
	high byte	8C

6.1.9 Function code 04H: read input register

For example: the host wants to read 1 input register data whose slave address is 01H and the starting register address is 02H, host sends：

Host sends		Send data (HEX)
address code		01
function code		04
start register address	high byte	00
	low byte	02
Number of registers	high byte	00
	low byte	01
CRC check	low byte	90
	high byte	0A

If the data of slave input register 02H is 3344H, slave return：

Slave return		Send data (HEX)
address code		01
function code		04
number of bytes		02
Register 05H data	high byte	33
	low byte	44

CRC check code	low byte	AD
	high byte	F3

6.1.10 Function code 03H: read holding register

For example: the host wants to read the data of 2 holding registers whose slave address is 01H and the starting register address is 05H, host sends：

Host sends		Send data (HEX)
address code		01
function code		03
start register address	high byte	00
	low byte	05
Number of registers	high byte	00
	low byte	02
CRC check	low byte	D4
	high byte	0A

If the data of slave holding registers 05H and 06H are 1122H and 3344H, slave returns：

Slave return		Send data (HEX)
address code		01
function code		03
number of bytes		04
Register 05H data	high byte	11
	low byte	22
Register 06H data	high byte	33
	low byte	44
CRC check code	low byte	4B
	high byte	C6

6.1.11 Function code 06H: write a single holding register

For example: the host writes the data of 9988H to the register with the slave address of 01H and the register address of 0050H, Host sends:

Host sends		Send data (HEX)
address code		01
function code		06
register address	high byte	00
	low byte	50
write value	high byte	99
	low byte	88

CRC check	low byte	E3
	high byte	ED

Slave return is the same as the host request;

6.1.12 Function code 10H: write to multiple holding registers

For example: the host wants to save the data 0005H and 2233H to the two registers whose slave address is 01H and the starting register address is 0020H. Host sends:

Host sends		Send data (HEX)
address code		01
function code		10
start register address	high byte	00
	low byte	20
Number of registers	high byte	00
	low byte	02
number of bytes written		04
0000H Register to be written	high byte	00
	low byte	05
0001H Register to be written	high byte	22
	low byte	33
CRC CHECK	low byte	B9
	high byte	03

function code 10H operate，Slave return：

Slave return		Send data (HEX)
address code		01
function code		10
start register address	high byte	00
	low byte	20
Number of registers	high byte	00
	low byte	02
CRC CHECK	low byte	40
	high byte	02

6.1.13 Data area

As can be seen from the detailed introduction of these function codes, the data area varies with function codes.

6.1.14 Error feedback

Address and CRC CHECK errors will not receive data feedback from the slave, and other errors will return an error code to the master. Adding 0X80 to the second bit of the data frame indicates that the request has an error (illegal function code, illegal data value, etc.), and the error data frame is as follows:

address code	function code	error code	CRC check code
1 byte	1 byte	1 byte	2 byte

The error code is as follows：

value	name	illustrate
01H	Illegal function code	This function code operation register is not supported
02H	illegal register address	Registers that are forbidden to be accessed by the device
03H	illegal data value	parameter exceeds limit
04H	Equipment failure	Equipment is working abnormally

6.2 Modbus register table

6.2.1 Device attribute related

parameter address	Parameter Description	register type	Data Format	Remark
0000H	DI status	discrete input	bit	read only
0000H	DO status	coil	bit	read and write
0064H	DO power-on state	coil	bit	read and write
00C8H	battery power	input register	Float (4Byte-ABCD)	read only
07D0H	Device model	holding register	String (14Byte-ASCII)	read only
07DCH	Firmware version	holding register	Int16	Read-only, high byte is the main version number, low byte is the minor version number, 0x0100 represents version 1.0
07E8H	Modbus address	holding register	Int16	Read and write, range 1-247, non-config mode is the device Modbus address
07E9H	reset	holding register	Int16	Write only, support 10H function

				code, but cannot be continuously written, write 0x01 device to execute
07EAH	Reboot the device	holding register	Int16	Write only, support 10H function code, but cannot be continuously written, write 0x01 device to execute
0834H	baud rate	holding register	Int16	Read-write, configuration scope: 0x00: 1200bps 0x01:2400bps 0x02:4800bps 0x03:9600bps (default) 0x04-0x07: Reserved
0835H	data bits	holding register	Int16	Read-write, configuration scope: 0x00: 8bit (default) 0x01: 7bit 0x02-0x03: reserved
0836H	Check Digit	holding register	Int16	Read-write, configuration scope: 0x00:NONE (default) 0x01: ODD 0x02: EVEN 0x03-0x04: reserved
0837H	stop bit	holding register	Int16	Read-write, configuration scope: 0x00: 1bit (default) 0x01: reserved 0x02: 2bit
1B5CH	battery power read cycle	holding register	Int16	Read and write, configuration range: 0-65535, unit points; If the alarm is enabled and the battery alarm enable is turned on, the battery alarm will be triggered every time the battery voltage is lower than the alarm voltage.;
1B5DH	Sensor Power Configuration	holding register	Int16	Read-write, configuration scope: 0x00: Synchronous DC power 0x01: Sync battery power

【Note】

Float (4Byte-ABCD) represents the single-precision floating point in the standard IEEE754 format, with a total of 32 bits (4 bytes). Single-precision floating-point size end mode is ABCD (high byte first, low byte last);

String(14Byte-ASCII) represents a 14-byte ASCII-encoded string;

In configuration mode, the device is fixed to open 01H (and can also be accessed through 07E8H stored value) address monitoring host request, using the fixed baud rate parameter 9600-8N1;

6.2.2 Wireless properties related

parameter address	Parameter Description	register type	Data Format	Remark
0B6FH	LORA device address	holding register	Int16	Read and write, configuration range: 0-65535
0B71H	LORA network address	holding register	Int16	Read and write, configuration range: 0-255
0B74H	airspeed	holding register	Int16	Read-write, configuration scope: 0x00-0x02: 2.4Kbps (default) 0x03:4.8Kbps 0x04:9.6Kbps 0x05:19.2Kbps 0x06:38.4Kbps 0x07:62.5Kbps
0B75H	channel	holding register	Int16	Read and write, configuration range 0-83
0B77H	transmit power level	holding register	Int16	Read-write, configuration scope: 0x00: High (default) 0x01: Medium 0x02: low 0x03: very low
0B78H	send mode	holding register	Int16	Read-write, configuration scope: 0x00: transparent transmission (default) 0x01: fixed point transmission
0B81H	Packet length	holding register	Int16	Read-write, configuration scope: 0x00: 240Byte (default) 0x00: 128Byte 0x00: 64Byte 0x00: 32Byte
0B88H	signal strength	holding register	Int16	Read-only, refresh after receiving data, the closer 256-RSSI is to 0, the better

【Note】

Transmit power level: high (30dBm±0.5), medium (reference value 27dBm), low (reference value 24dBm), extremely low (reference value 21dBm), the reference value is only used as a reference and cannot accurately reflect the transmit power of the device, if other transmit power is required It can be customized. Reducing the transmission power of the equipment will not reduce the power consumption of the whole machine in the same proportion. If you need other transmission power, it is recommended to purchase the corresponding power radio.

6.2.3 Automatic polling related

parameter address	Parameter Description	register type	Data Format	Remark
1838H	Automatic polling instructions	holding register	26Byte	Read and write, every 13 registers is a group of data, and up to 10 automatic polling instructions can be configured. For detailed instructions, see "Serial Port Automatic Polling"
…..	…..	…..	…..	…..
1B58H	Auto polling enabled	holding register	Int16	Read-write, configuration scope: 0x00: Disabled (default) 0x00: enable
1B59H	automatic polling cycle	holding register	Int16	Read and write, configuration range: 1-65535, unit points
1B5AH	CRC CHECK enable	holding register	Int16	Read-write, configuration scope: 0x00: Disabled (default) 0x00: enable
1B5BH	Clear polling order table	holding register	Int16	Write only, write 0x01 to clear the automatic polling command table

6.2.4 Alarm function related

parameter address	Parameter Description	register type	Data Format	Remark
1B60H	Alarm level	holding register	Int16	Read-write, configuration scope: 0x00: close the alarm (default) 0x01: send once 0x02: sent at least once For details, see "Alarm function"
1B61H	clear alarm status	holding register	Int16	For details, see "Alarm function"
1B62H	DI alarm enable	holding register	Int16	Read-write, configuration scope: 0x00: Disabled (default) 0x01: enable
1B63H	DI alarm source	holding register	Int16	Read-write, configuration scope: 0x00: disconnect the alarm (default) 0x01: close alarm
1B64H	Battery Alarm Enable	holding register	Int16	Read-write, configuration scope: 0x00: Disabled (default)

				0x01: enable
1B65H	battery alarm voltage	holding register	Int16	Read and write, configuration range: 0x00-0x0F, 0x00 is 3.45V and increases by 4.20V in turn, the maximum configurable 4.20V (ie 0x0F)

6.2.5 Low power consumption

parameter address	Parameter Description	register type	Data Format	Remark
0B79H	WOR monitor interval period	holding register	Int16	Read and write, configuration range: 0x00-0x07; Period T=(1+WOR)*500ms, maximum 4000ms, minimum 500ms; The longer the WOR monitoring interval period, the lower the average power consumption, but the greater the data delay; Default: 0x03 (ie 2000ms), both sender and receiver must agree
0B80H	WOR role	holding register	Int16	Read only, parameter range: 0x00: Slave (ie, WOR receiver), working in WOR monitoring mode, the monitoring period is "WOR period", which can save a lot of power consumption 0x01: The host (ie the WOR sender) adds a certain time wake-up code when transmitting data
1B5EH	Sensor early wake-up time	holding register	Int16	Read and write, configuration range: 0-65535, in milliseconds; Used to output sensor power in advance to avoid abnormal output of sensors that cannot work immediately after power-on
1B5FH	Sensor response timed out	holding register	Int16	Read and write, configuration range: 0-65535, in milliseconds; In low-power mode, after sending a command, the device waits for the

				configured timeout time (or receives a sensor response) and the device re-enters the low-power mode. After automatic polling is enabled, the configured time of the polling time shall prevail. This parameter does not take effect.
1B66H	Low power enable	holding register	Int16	Read-write, configuration scope: 0x00: Disabled (default) 0x01: enable

The final interpretation right belongs to Chengdu Ebyte Electronic Technology Co., Ltd.

Modification History

Version	revision date	Revision Notes	Maintenance man
1.0	2022-08-09	initial version	LC

About us

Hotline: 4000-330-990 Tel: 028-61399028
Support: support@cdebyte.com Website: https://www.cdebyte.com
Address: Building B5, No. 199, West District Avenue, High-tech West District, Chengdu City, Sichuan Province

成都亿佰特电子科技有限公司
Chengdu Ebyte Electronic Technology Co.,Ltd.