EBYTE

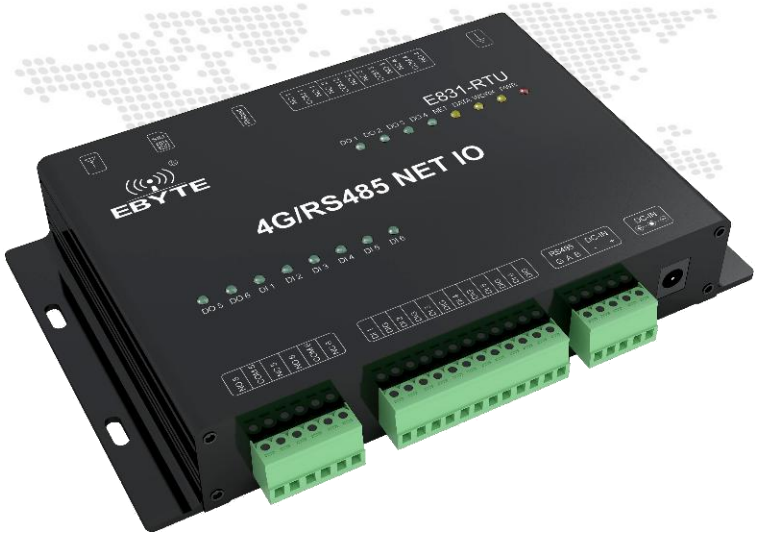
成都亿佰特电子科技有限公司

Chengdu Ebyte Electronic Technology Co.,Ltd.

Wireless Modem

USER MANUAL

# E831-RTU(6060-4G) Product Manual






Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

## Table of contents

Features ..... 2
I. Quick Start ..... 3
1.1 Port Connection ..... 3
1.1.1 RS485 connection ..... 3
1.1.2 Switch input connection ..... 3
1.1.3 Relay output connection ..... 4
1.2 Simple use ..... 4
1.2.1 RS485 bus control ..... 4
1.2.2 Network Control ..... 5
II. Product Introduction ..... 7
2.1 Basic parameters ..... 7
2.2 Dimensions and interface description ..... 8
2.3 Reload Touch Button Description ..... 12
III. Modbus ..... 13
3.1 Register Address Table ..... 13
3.2 Modbus address table ..... 15
3.3 RS485 serial port baud rate code value table ..... 15
3.4 RS485 serial port check bit code value table ..... 15
3.5 Parameter configuration via host computer ..... 15
IV. Product Function ..... 16
4.1 Working Mode ..... 16
4.1.1 Slave Mode ..... 16
4.1.2 Host Mode ..... 17
4.2 Basic IO functions ..... 17
4.2.1 Switching DO output ..... 17
4.2.2 Read switch DI input ..... 20
4.3 IO Features ..... 20
4.3.1 Pulse Counting and Count Reset ..... 20
4.3.2 Switch input DI automatically reports ..... 22
4.3.3 Switch output DO time setting ..... 22
4.3.4 Restart switch output state setting ..... 22
4.4 Network related functions ..... 23
4.4.1 Server IP or domain name, port, TCP or UDP settings (Socket) ..... 23
4.4.2 Customized Registration Package ..... 24
4.4.3 Heartbeat Packet ..... 26
4.4.4 Heartbeat Packet Time ..... 27
4.4.5 Ebyte Cloud Transmission ..... 27
4.4.6 IMEI Reading ..... 27
4.4.7 SN Read ..... 28
4.4.8 Base station positioning value LBS reading ..... 28
Important Statement ..... 28
Revision History ..... 29
About Us ..... 29

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

# Features

- Support 6-channel digital input, default dry contact;
- Support 6-way relay output;
- Support socket connection to remote server, support TCP/UDP;
- Adopt Modbus TCP/RTU protocol data processing;
- Support connection to Ebyte Cloud and command control;
- Supports 2 working modes, host mode and slave mode. The slave can cascade multiple devices via RS485;
- Support Reload. Touch the button and press it for 5s to restore the Modbus device address, RS485 serial port baud rate and check bit to factory settings.
- Hardware watchdog, with high reliability;
- Multiple indicator lights show working status;
- The power supply has good over-current, over-voltage, and reverse connection protection functions.

Note: Customers can customize functions, such as conditional control (determine how to output according to the input status)

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.

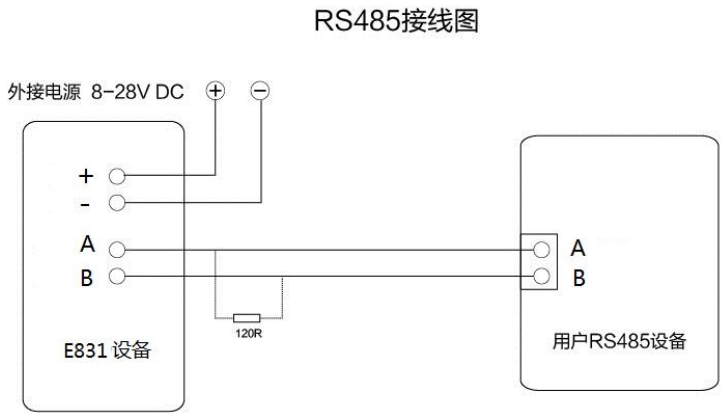

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

# I. Quick Start

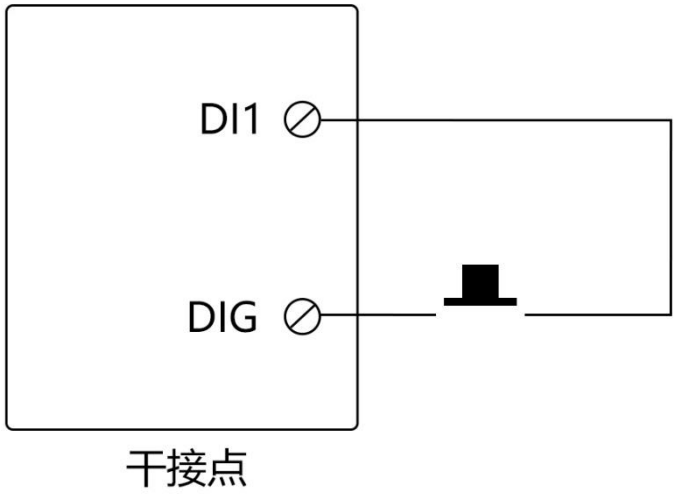
This chapter is a quick introduction to the E831-RTU (6060-4G) series products. It is recommended that users read this chapter systematically and follow the instructions to have a systematic understanding of the module products. Users can also select the chapters they are interested in to read as needed. For specific details and instructions, please refer to the subsequent chapters.

## 1.1 Port Connection

### 1.1.1 RS485 connection



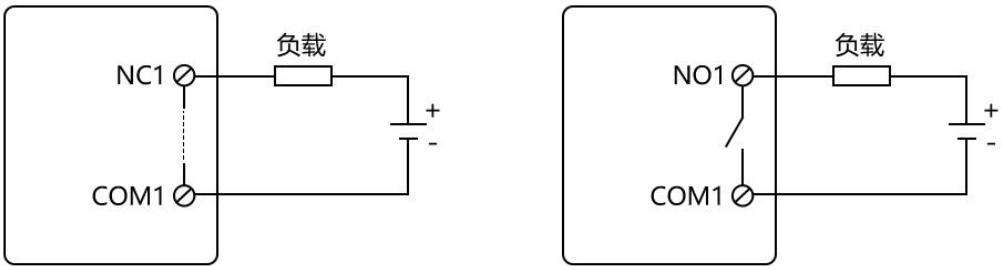

### 1.1.2 Switch input connection




Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

### 1.1.3 Relay output connection

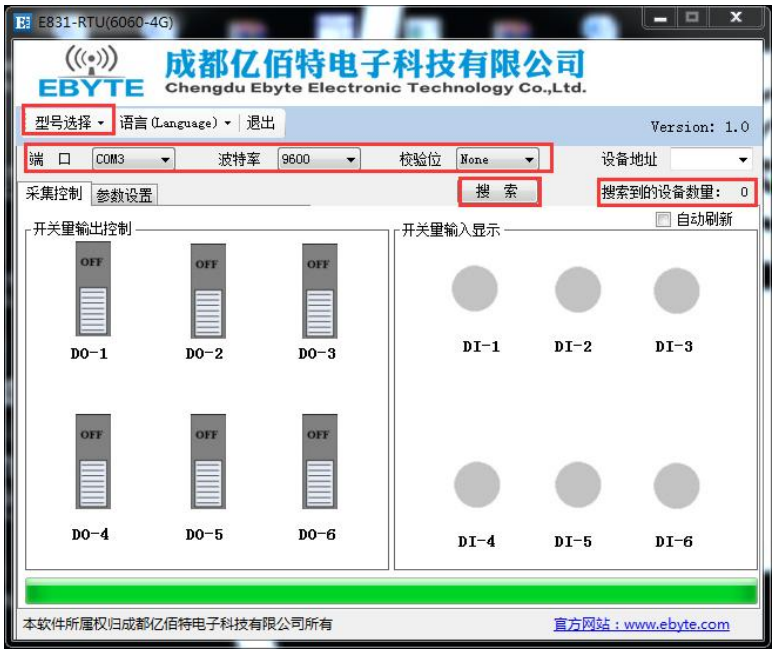



## 1.2 Easy to use

Wiring: The computer is connected to E831-RTU (6060-4G) via USB to RS485.
Connect to the Internet: Insert a SIM card when the power is off.
Power supply: The working voltage of E831-RTU (6060-4G) is DC 8~28V.

### 1.2.1 RS485 bus control

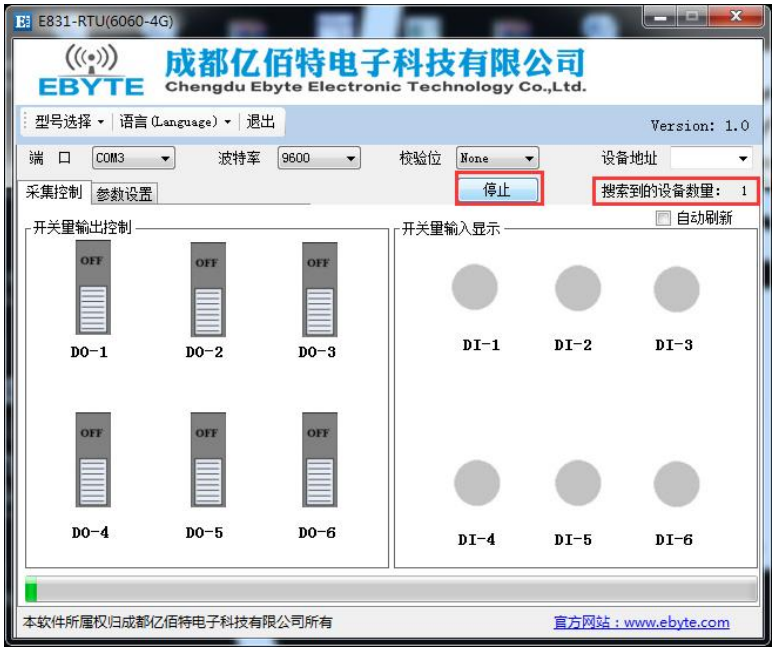
Select the corresponding model and port, and click Search to search for the device.



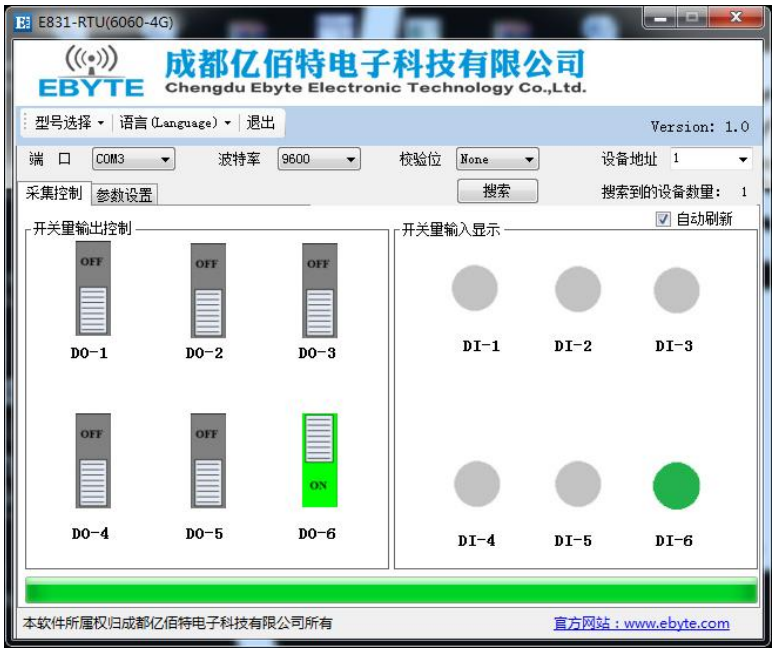

After the device is found, click Stop.



Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000




At this time, you can see the device address of the current device, and process "Auto Refresh" to perform switch output control and switch input reading .

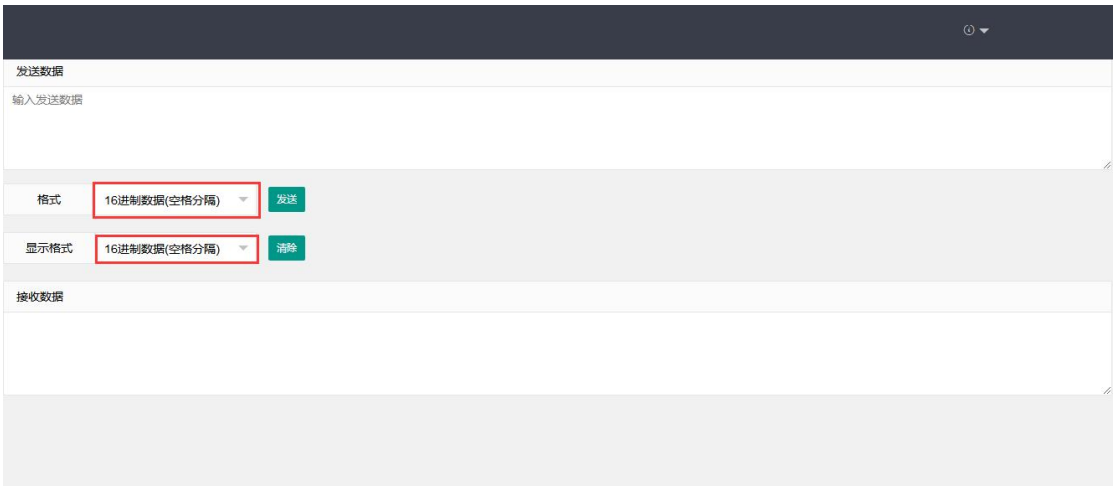



## 1.2.2 Network Control

Enter the URL http://yun.cdebyte.com/www/data_direct and you can control the acquisition through commands. The commands use Modbus TCP / RTU protocol .

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000




Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

# II. Product Introduction

E831-RTU (6060-4G) is a network IO product that supports 6 digital inputs (default dry contacts) and 6 relay outputs. It supports Modbus TCP/RTU protocol. This product is highly easy to use and users can easily and quickly integrate it into their own systems to achieve remote control based on 4G.

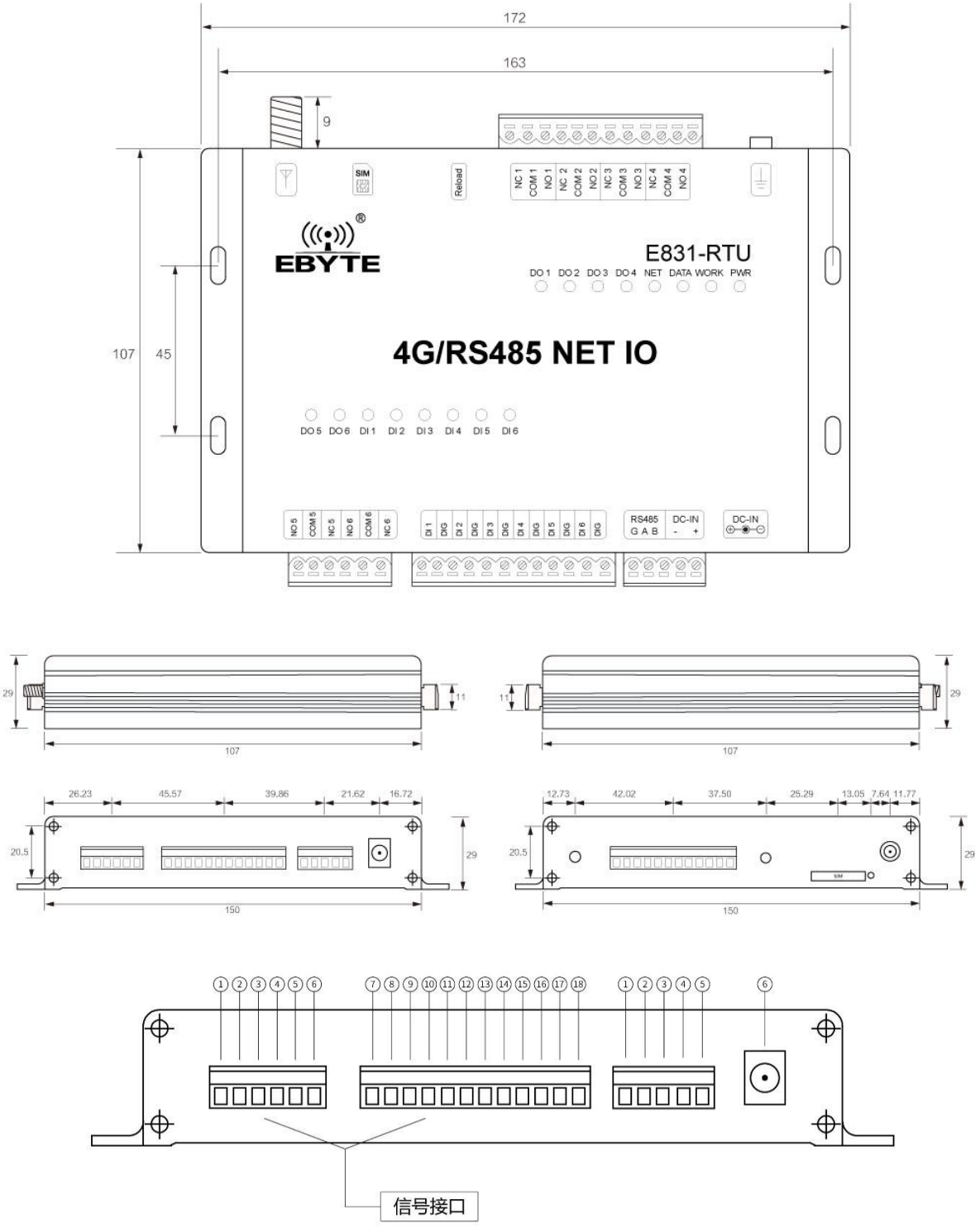
## 2.1 Basic parameters

| | Project | Index |
|---|---|---|
| Wireless parameters | Standard frequency band | LTE-FDD: B1/B3/B5/B8 |
| | | LTE-TDD: B38/B39/B40/B41 |
| | | WCDMA: B1/B8 |
| | | TD-SCDMA: B34/B39 |
| | | CDMA: BC0 |
| | | GSM: 900/1800MHz |
| Hardware Parameters | Product size (H*W*D) | 172*107*29mm |
| | Product Weight | 484.5±5 g |
| | Operating temperature | -20℃~+70℃ |
| | Storage temperature | -40℃~+85℃ |
| | Operating humidity | 5%~95% |
| | Storage humidity | 1%~95% |
| | Operating voltage | 8V~28V |
| | Data Interface | RS485: 1200~115200bps |
| Software Parameters | Network Type | 4G |
| | Configuration Commands | Modbus TCP/RTU |
| | Network Protocol | Modbus TCP/RTU |
| | Working Mode | Master mode, slave mode |
| | Data transmission method | TCP/UDP |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.

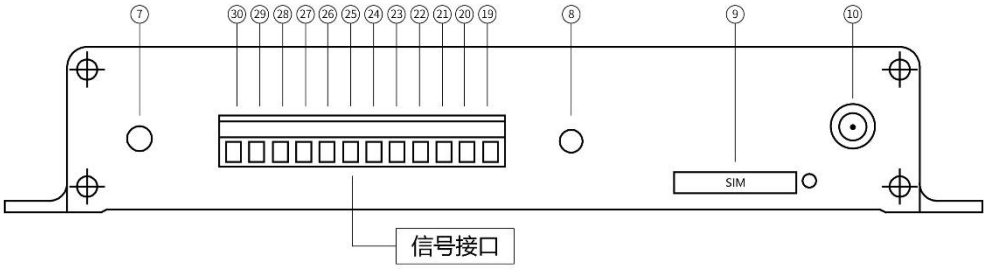

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

## 2.2 Dimensions and interface description






Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000




| Serial number | Port and other definitions | Function | Illustrate |
|---|---|---|---|
| 1 | RS485 G | Signal reference ground | Signal reference ground, not connected |
| 2 | RS485 A | RS485 interface A | RS485 interface A is connected to device A interface |
| 3 | RS485 B | RS485 interface B | RS485 interface B is connected to device B interface |
| 4 | DC-IN - | Press-wire power input negative pole | Power reference ground |
| 5 | DC-IN + | Press-wire power input positive terminal | Power input, DC 8V~36V, 12V/24V recommended |
| 6 | DC-IN socket | DC socket 5.5*2.1mm | Power input terminal, DC 8V~36V, 12V/24V recommended |
| 7 | Ground screw | Connecting with the Earth | Connecting with the Earth |
| 8 | Reload | Reset button | Long press for 5 seconds to work. |
| 9 | SIM card slot | SIM card slot | Insert SIM card and connect to the Internet |
| 10 | ANT | Antenna interface | GPRS Antenna |
| **Signal interface** | | | |
| 1 | NO 5 | Relay 5 Normally Open Pin | Used with relay 5 common terminal |
| 2 | COM 5 | Relay 5 common terminal | Used with relay 5 normally open pin/normally closed pin |
| 3 | NC 5 | Relay 5 Normally Closed Pin | Used with relay 5 common terminal |
| 4 | NO 6 | Relay 6 Normally Open Pin | Used with relay 6 common terminal |
| 5 | COM 6 | Relay 6 common terminal | Used with relay 6 normally open pin/normally closed pin |
| 6 | NC 6 | Relay 6 Normally Closed Pin | Used with relay 6 common terminal |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | | | |
|---|---|---|---|
| 7 | DI 1 | Switch input channel 1 | Form dry contact with DIG |
| 8 | DIG | Switch input ground | Can be used in pair with DI 1 |
| 9 | DI 2 | Switch input channel 2 | Form dry contact with DIG |
| 10 | DIG | Switch input ground | Can be used in pairs with DI 2 |
| 11 | DI 3 | Switch input channel 3 | Form dry contact with DIG |
| 12 | DIG | Switch input ground | Used in pair with DI 3 |
| 13 | DI 4 | Switch input channel 4 | Form dry contact with DIG |
| 14 | DIG | Switch input ground | Can be used in pairs with DI 4 |
| 15 | DI 5 | Switch input channel 5 | Form dry contact with DIG |
| 16 | DIG | Switch input ground | Can be used in pairs with DI 5 |
| 17 | DI 6 | Switch input channel 6 | Form dry contact with DIG |
| 18 | DIG | Switch input ground | Can be used in pairs with DI 6 |
| 19 | NC 1 | Relay 1 Normally Closed Pin | Used with relay 1 common terminal |
| 20 | COM 1 | Relay 1 common terminal | Used with relay 1 normally open pin/normally closed pin |
| twenty one | NO 1 | Relay 1 Normally Open Pin | Used with relay 1 common terminal |
| twenty two | NC 2 | Relay 2 Normally Closed Pin | Used with relay 2 common terminal |
| twenty three | COM 2 | Relay 2 common terminal | Used with relay 2 normally open pin/normally closed pin |
| twenty four | NO 2 | Relay 2 Normally Open Pin | Used with relay 2 common terminal |
| 25 | NC 3 | Relay 3 normally closed pin | Used with relay 3 common terminal |
| 26 | COM 3 | Relay 3 common terminal | Used with relay 3 normally open pin/normally closed pin |
| 27 | NO 3 | Relay 3 Normally Open Pin | Used with relay 3 common terminal |
| 28 | NC 4 | Relay 4 Normally | Used with relay 4 common terminal |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | | | |
|---|---|---|---|
| | | Closed Pin | |
| 29 | COM 4 | Relay 4 common terminal | Used with relay 4 normally open pin/normally closed pin |
| 30 | NO 4 | Relay 4 Normally Open Pin | Used with relay 4 common terminal |
| **LED Light** | | | |
| 1 | DO 5 | Relay 5 output indication | Green LED, NO 5, COM 5 closed and lit |
| 2 | DO 6 | Relay 6 output indication | Green LED, NO 6, COM 6 closed and lit |
| 3 | DI 1 | Switch input channel 1 indication | Green LED, DI 1 and DIG short-circuited, lights up |
| 4 | DI 2 | Switch input channel 2 indication | Green LED, DI 2 and DIG short-circuited, lights up |
| 5 | DI 3 | Switch input channel 3 indication | Green LED, DI 3, DIG short circuit lights up |
| 6 | DI 4 | Switch input channel 4 indication | Green LED, DI 4, DIG short circuit lights up |
| 7 | DI 5 | Switch input channel 5 indication | Green LED, DI 5, DIG short circuit lights up |
| 8 | DI 6 | Switch input channel 6 indication | Green LED, DI 6, DIG short circuit lights up |
| 9 | DO 1 | Relay 1 output indication | Green LED, NO 1, COM 1 closed and lit |
| 10 | DO 2 | Relay 2 output indication | Green LED, NO 2, COM 2 closed and lit |
| 11 | DO 3 | Relay 3 output indication | Green LED, NO 3, COM 3 closed and lit |
| 12 | DO 4 | Relay 4 output indication | Green LED, NO 4, COM 4 closed and lit |
| 13 | NET | Network Instructions | Yellow LED, always on after connecting to the network |
| 14 | DATA | Serial port data indication | Yellow LED, lights up when there is data transmission on the RS485 interface (flashes) |
| 15 | WORK | Working/reset indication | Yellow LED, flashes regularly/flashes quickly after reset |
| 16 | PWR | Power indicator | Red LED, long on |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Notice:

Grounding: It is recommended to connect the shell to the ground

## 2.3 Reload Touch Button Description

Long press for 5S to be effective. After the reset is successful, the WORK light flashes quickly, and the Modbus device address, RS485 serial port baud rate and parity bit are restored to factory settings.

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

# III. Modbus

## 3.1 Register Address Table

| Register address table (function code: 0x01H, 0x05H, 0x0FH, 0x03H, 0x06H, 0x10H) | | | | | |
|---|---|---|---|---|---|
| Register Address | Number of registers | Register attributes | Register Type | Register value range | Support function code |
| 00017 (0x0010) | 1 | DO1 switch output | Read/Write | 0x0000 or 0xFF00 (0x05 function code) 0-1 (0x01, 0x0F function code) | 0x01 0x05 0x0F |
| 00018 (0x0011) | 1 | DO2 switch output | Read/Write | | |
| 00019 (0x0012) | 1 | DO3 switch output | Read/Write | | |
| 00020 (0x0013) | 1 | DO4 switch output | Read/Write | | |
| 00021 (0x0014) | 1 | DO5 switch output | Read/Write | | |
| 00022 (0x0015) | 1 | DO6 switch output | Read/Write | | |
| Reserve | | | | | |
| 10017 (0x0010) | 1 | DI1 switch input | Read-only | 0-1 | 0x02 |
| 10018 (0x0011) | 1 | DI2 switch input | Read-only | | |
| 10019 (0x0012) | 1 | DI3 switch input | Read-only | | |
| 10020 (0x0013) | 1 | DI4 switch input | Read-only | | |
| 10021 (0x0014) | 1 | DI5 switch input | Read-only | | |
| 10022 (0x0015) | 1 | DI6 switch input | Read-only | | |
| Reserve | | | | | |
| 40049 (0x0030) | 1 | DI1 pulse count value | Read-only | 0-65535 | 0x03 |
| 40050 (0x0031) | 1 | DI2 pulse count value | Read-only | 0-65535 | |
| 40051 (0x0032) | 1 | DI3 pulse count value | Read-only | 0-65535 | |
| 40052 (0x0033) | 1 | DI4 pulse count value | Read-only | 0-65535 | |
| 40053 (0x0034) | 1 | DI5 pulse count value | Read-only | 0-65535 | |
| 40054 (0x0035) | 1 | DI6 pulse count value | Read-only | 0-65535 | |
| Reserve | | | | | |
| 40065 | 1 | DI1-DI6 pulse | Write | 0x00 - 0x0F | 0x06 |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | | | | | |
|---|---|---|---|---|---|
| (0x0040) | | count reset | only | | |
| Reserve | | | | | |
| 40078 (0x004D) | 1 | Device Address | Read/Write | 1 - 247 | 0x03 0x06 0x10 |
| 40079 (0x004E) | 1 | Baud rate | Read/Write | 0 - 7 | |
| 40080 (0x004F) | 1 | Check digit | Read/Write | 0 - 2 | |
| 40081 (0x0050) | 1 | Master mode or slave mode | Read/Write | 0 - 1 | |
| 40082 (0x0051) | 1 | Automatic reporting of switch quantity | Read/Write | 0 - 2 | |
| 40083 (0x0052) | 1 | Switch output time setting (milliseconds) | Read/Write | 300-65535 | |
| Reserve | | | | | |
| 40085 (0x0054) | 1 | Switch restart output status setting | Read/Write | 0x00 - 0x40 | 0x03 0x06 0x10 |
| Reserve | | | | | |
| 40100 (0x0063) | twenty two | Server IP or domain name (domain name in ASCII) | Read/Write | -- | 0x03 0x06 0x10 |
| 40122 (0x0079) | 1 | Server Port | Read/Write | 1 - 65535 | |
| 40123 (0x007A) | 1 | Protocol type (UDP, TCP) | Read/Write | 0 - 1 | |
| 40124 (0x007B) | twenty two | Custom Registration Package | Read/Write | -- | |
| 40146 (0x0091) | 1 | Registration package mechanism | Read/Write | 0 - 4 | |
| 40147 (0x0092) | twenty two | Heartbeat Packet | Read/Write | -- | |
| 40169 (0x00A8) | 1 | Heartbeat packet time | Read/Write | 0 - 65535 | |
| 40170 (0x00A9) | 1 | Cloud transparent transmission function | Read/Write | 0 - 1 | |
| 40171 (0x00AA) | 11 | IMEI value | Read-only | -- | 0x03 |
| 40182 (0x00B5) | 11 | SN code value | Read-only | -- | |
| 40193 (0x00C0) | 20 | LBS | Read-only | -- | |
| Reserve | | | | | |
| 40300 (0x012B) | 1 | Version Number | Read-only | -- | 0x03 |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

## 3.2 Modbus address table

| Modbus Address Table | |
|---|---|
| 1 (default) | 1 |
| 2 | 2 |
| 3 | 3 |
| … | … |
| 245 | 245 |
| 246 | 246 |
| 247 | 247 |

## 3.3 RS485 serial port baud rate code value table

| Baud rate code value table | |
|---|---|
| 0 | 1200 |
| 1 | 2400 |
| 2 | 4800 |
| 3 (default) | 9600 |
| 4 | 19200 |
| 5 | 38400 |
| 6 | 57600 |
| 7 | 115200 |

## 3.4 RS485 serial port check bit value table

| Check digit value table | |
|---|---|
| 0 (default) | No verification |
| 1 | Even parity |
| 2 | Odd Parity |

## 3.5 Configuring parameters through the host computer

Select the "Parameter Setting" column to read parameters, write parameters, and see the product function introduction below for specific functions.

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000




# IV. Product Functions

## 4.1 Working Mode

The working mode is divided into host mode and slave mode, which is configured through Modbus register 40081 (0x0050). When the register value is 0, it is the host mode; when the register value is 1, it is the slave mode, and the default is slave mode.

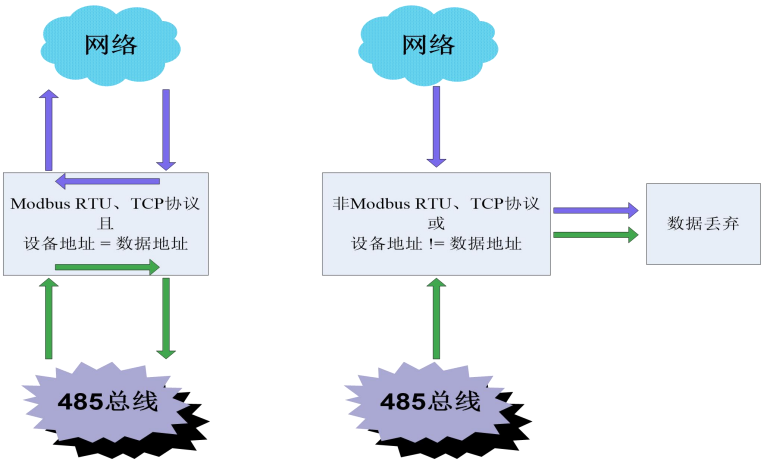
### 4.1.1 Slave Mode

In slave mode (register value is 0x01), the data sent by the network or 485 bus (sender) to the device meets the Modbus RTU and Modbus TCP protocols, and the address in the data is the device address. The device will respond to the sender with the same protocol; if the data sent by the network or 485 bus to the device does not meet the Modbus RTU and Modbus TCP protocols, or meets the Modbus RTU and Modbus TCP protocols but the data address is not the device address, the data from the sender will be discarded.

In slave mode, the device can be directly connected to the device in host mode through the 485 bus, so that when the slave is not connected to the Internet, the network end can also access the slave data through the host.

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.

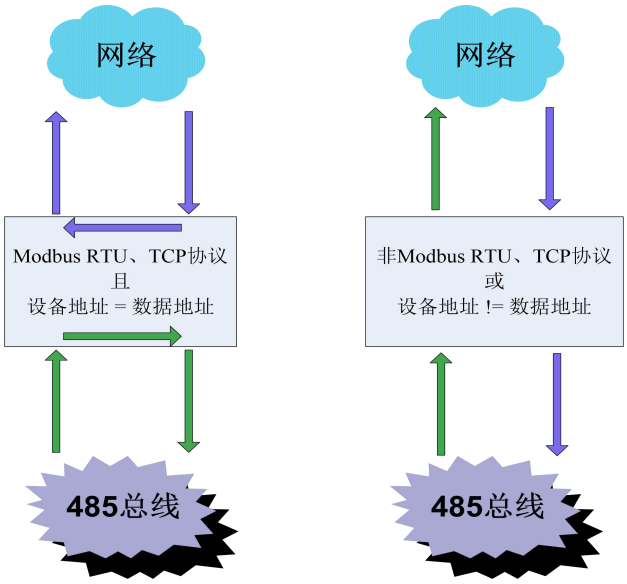

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000




### 4.1.2 Host Mode

In the host mode (register value is 0x00), the data sent by the network or 485 bus (sender) to the device meets the Modbus RTU and Modbus TCP protocols, and the address in the data is the device address, and the device will respond to the sender with the same protocol; if the data sent by the network or 485 bus to the device does not meet the Modbus RTU and Modbus TCP protocols, or meets the Modbus RTU and Modbus TCP protocols but the data address is not the device address, the data from the 485 bus will be transmitted to the network, and the data from the network will be transmitted to the 485 bus.

This function of host mode can realize device cascading function and data transmission between 485 bus and network.




## 4.2 Basic IO Functions

### 4.2.1 Switching DO output

- Read switch DO output

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Function code: 01, read coil status

Address range: 00017 (0x0010) ~ 00022 (0x0015)

Note: The relay of the device has passive output. When the coil is not energized, the NC port of the relay is normally closed with the COM port, and the NO port is normally open with the COM port, and the value is 0. When the coil is energized, the phenomenon is the opposite, the NC port of the relay is disconnected with the COM port, and the NO port is closed with the COM port, and the value is 1. Query the relay status through instructions.

example:

Read the status of 6 switch outputs. Assume that the return value is 03, which corresponds to the binary bit 0000 0011. The lower six bits represent the status of the switch outputs, which are DO6, DO5, DO4, DO3, DO2, and DO1.

Modbus RTU protocol reads switch output:

| | | | | | |
|---|---|---|---|---|---|
| Send | 01 | 01 | 00 10 | 00 06 | BD CD |
| | Device ModBus address | Function code | Switch value starting address | Read switch quantity | CRC checksum |

| | | | | | |
|---|---|---|---|---|---|
| Receive | 01 | 01 | 01 | 03 | 11 89 |
| | Device ModBus address | Function code | Returns the number of bytes | Switching output value | CRC checksum |

Modbus TCP protocol reads switch output:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 00 01 | 00 00 | 00 06 | 01 | 01 | 00 10 | 00 06 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Switch value starting address | Read switch quantity |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Receive | 00 01 | 00 00 | 00 04 | 01 | 01 | 01 | 03 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Returns the number of bytes | Switching output value |

- Control switch DO output

Function code: 05, write single coil status; 0F, write multiple coil status

Address range: 00017 (0x0010) ~ 00022 (0x0015)

Description: The relay of the device has passive output. When the coil is not energized, the NC port of the relay is closed with the COM port, and the NO port is disconnected with the COM port. When the coil is energized, the NC port of the relay is disconnected with the COM port, and the NO port is closed with the COM port. The relay state is controlled by instructions.

example:

Function code 0x05 writes DO2 switch output, disconnects NC2 and COM2, closes NO2 and COM2, and writes a value of FF 00; closes NC2 and COM2, disconnects NO2 and COM2, and writes a value of 00 00.

Modbus RTU protocol writes switch output:

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | | | | | |
|---|---|---|---|---|---|
| Send | 01 | 05 | 00 11 | FF 00 | DC 3F |
| | Device ModBus address | Function code | Switch address | Write value | CRC checksum |

| | | | | | |
|---|---|---|---|---|---|
| Receive | 01 | 05 | 00 11 | FF 00 | DC 3F |
| | Device ModBus address | Function code | Switch address | Write value | CRC checksum |

Modbus TCP protocol writes switch output:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 00 01 | 00 00 | 00 06 | 01 | 05 | 00 11 | FF 00 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Switch address | Write value |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Receive | 00 01 | 00 00 | 00 06 | 01 | 05 | 00 11 | FF 00 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Switch address | Write value |

Function code 0x0F writes DO2 and DO3 switch outputs, making NC2 and COM2 open and NO2 and COM2 closed; making NC3 and COM3 open and NO3 and COM3 closed. The written value should be 0x03, corresponding to the binary bit 0000 0011

Modbus RTU protocol writes switch output:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 01 | 0F | 00 11 | 00 02 | 01 | 03 | 62 95 |
| | Device ModBus address | Function code | Switch address | Write switch quantity | Number of bytes | Write value | CRC checksum |

| | | | | | |
|---|---|---|---|---|---|
| Receive | 01 | 0F | 00 11 | 00 02 | 84 0F |
| | Device ModBus address | Function code | Switch address | Write value | CRC checksum |

Modbus TCP protocol writes switch output:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Send | 00 01 | 00 00 | 00 08 | 01 | 0F | 00 11 | 00 02 | 01 | 03 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Switch address | Write switch quantity | Number of bytes | Write value |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Receive | 00 01 | 00 00 | 00 06 | 01 | 0F | 00 11 | 00 02 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Switch address | Write switch quantity |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

### 4.2.2 Read switch DI input

Function code: 02, read (switch quantity) input status

Address range: 10017 (0x0010) ~ 10022 (0x0015)

Note: The device defaults to dry contact input. When DI and COM are short-circuited, the read value should be 1; when DI and COM are not short-circuited, the read value should be 0.

example:

Read the 6-way switch input value, DI input terminal DI1, COM1 short-circuited, DI2, COM2 not short-circuited, DI3, COM3 short-circuited, DI4, COM4 not short-circuited, DI5, COM5 not short-circuited, DI6, COM6 not short-circuited. The read switch input value is 0x05, corresponding to the binary bit 0000 0101, the lower six bits represent the switch input value, which are DI6, DI5, DI4, DI3, DI2, DI1.

Modbus RTU protocol reads switch input:

| | | | | | |
|---|---|---|---|---|---|
| Send | 01 | 02 | 00 10 | 00 06 | F9 CD |
| | Device ModBus address | Function code | Switch value starting address | Read switch quantity | CRC checksum |
| Receive | 01 | 02 | 01 | 05 | 61 8B |
| | Device ModBus address | Function code | Returns the number of bytes | Switch input value | CRC checksum |

Modbus TCP protocol reads switch input:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 00 01 | 00 00 | 00 06 | 01 | 02 | 00 10 | 00 06 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Switch value starting address | Read switch quantity |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Receive | 00 01 | 00 00 | 00 04 | 01 | 02 | 01 | 05 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Returns the number of bytes | Switch input value |

## 4.3 IO Features

### 4.3.1 Pulse counting and count clearing

The pulse count will not be saved after power failure, and the pulse level maintenance time must be greater than 10ms to be effective. The switch input changes from the open state to the closed state and maintains the closed state for more than 10ms, and then changes to the open state to complete a pulse count.

- Read pulse count value

Function code: 03, read holding register

Address range: 40049 (0x0030) ~ 40054 (0x00335)

Note: The maximum value of pulse count is 65535

example:

DI1 has currently detected 16 pulses, DI2 has currently detected 3 pulses, read the DI1 and DI2 switch input count values

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Modbus RTU protocol reads pulse count value:

| | | | | | |
|---|---|---|---|---|---|
| send | 01 | 03 | 00 30 | 00 02 | C4 04 |
| | Device ModBus address | Function code | Starting address | Read quantity | CRC checksum |

| | | | | | | |
|---|---|---|---|---|---|---|
| take over | 01 | 03 | 04 | 00 10 | 00 03 | BB F7 |
| | Device ModBus address | Function code | Returns the number of bytes | DI1 count value | DI2 count value | CRC checksum |

Modbus TCP protocol reads pulse count value:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 00 01 | 00 00 | 00 06 | 01 | 03 | 00 30 | 00 02 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Starting address | Read quantity |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Receive | 00 01 | 00 00 | 00 07 | 01 | 03 | 04 | 00 10 | 00 03 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | Returns the number of bytes | DI1 count value | DI2 count value |

- Clear pulse count value

Function code: 06, write holding register

Address range: 40065 (0x0040)

Note: The lower six bits of the register value represent the counts of DI6, DI5, DI4, DI3, DI2, and DI1 respectively. Writing "1" means the count is cleared and the pulse counting starts again.

example:

Clear the pulse count values of DI2 and DI4, and keep the pulse count values of DI1, DI3, D5, and D6. The written value should be 0x0a, and the corresponding binary value is 0000 1010.

Modbus RTU protocol clears pulse count value

| | | | | | |
|---|---|---|---|---|---|
| Send | 01 | 06 | 00 40 | 00 0a | 08 19 |
| | Device ModBus address | Function code | address | Write value | CRC checksum |

| | | | | | |
|---|---|---|---|---|---|
| Receive | 01 | 06 | 00 40 | 00 0a | 08 19 |
| | Device ModBus address | Function code | address | Write value | CRC checksum |

Modbus TCP protocol clears pulse count value

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 00 01 | 00 00 | 00 06 | 01 | 06 | 00 40 | 00 0a |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Write value |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Receive | 00 01 | 00 00 | 00 06 | 01 | 06 | 00 40 | 00 0a |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Write value |
|---|---|---|---|---|---|---|---|

### 4.3.2 Automatic reporting of switch input DI

The automatic reporting function of switch input is to transmit the changed value when the switch value changes. You can choose to transmit via RS485 or GPRS, or turn off the automatic reporting function.

The Modbus register corresponding to the automatic reporting setting of the switch value is 40082 (0x0051), and the value corresponds to the function:

Disable the automatic reporting function of switch quantity

Switching quantity is automatically reported via RS485 transmission

Switching quantity is automatically reported and transmitted via GPRS network

The switch quantity change upload protocol is listed in the following table, where the frame header 0xAA and 0xBB are fixed, and the value range of DI1, DI2, DI3, DI4, DI5, and DI6 is 0x00, 0x01, and 0xFF.

0x00 means the switch input is disconnected.

0x01 means the switch input is closed.

0xFF means the switch input has not changed.

The values of DI1, DI2, DI3, DI4, DI5, and DI6 in the table indicate that the status of DI1 and DI2 are updated to open, the status of DI3 is updated to close, and the status of DI4, DI5, and DI6 are unchanged. The last two bytes are the calculated values of modbus CRC16.

| Frame Header | DI1 | DI2 | DI3 | DI4 | DI5 | DI6 | Modbus CRC |
|---|---|---|---|---|---|---|---|
| AA BB | 00 | 00 | 01 | FF | FF | FF | F1 7B |

### 4.3.3 Switch output DO time setting

The switch pulse output time setting is to set the switch output time (relay NO, COM closing time). The corresponding Modbus register is 40083 (0x0052), and its value range is 300-65535ms. If the value is lower than 300ms, the default switch output closure is in the hold state, that is, the switch output is always held after closing. If it is set to 300ms or more, such as 500ms, after sending the switch output closing command, the switch closure will be maintained for 500ms, and then automatically disconnected after 500ms.

### 4.3.4 Restart switch output status setting

Whether the device maintains the state before power failure or restarts to maintain a specific output state after power failure. This function is only valid when the device switch output time setting register value is less than 300ms.

The Modbus register corresponding to the switch quantity restart output state setting is 40085 (0x0054), and its value range is 0x00-0x40. When the register value is 0x40, the last switch quantity output state is maintained after power off and restart; when the register value is 0x00-0x3F, the lower six bits determine the device restart switch quantity output state, bit6 corresponds to DO6, bit5 corresponds to DO5, bit4 corresponds to DO4, bit3 corresponds to DO3, bit2 corresponds to DO2, and bit1 corresponds to DO1. For example, when power is on, DO6, DO5, DO4, and DO2 are in a closed state (relay NO, COM closed) and DO3 and DO1 are in an open state (relay NO, COM open). The corresponding register value is 0011 1010,

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

that is, 0x3A, "1" is a closed state, and "0" is an open state.

## 4.4 Network related functions

### 4.4.1 Server IP or domain name, port, TCP or UDP settings (Socket)

The server IP or domain name is stored in 22 modbus registers. The first register is used to store the ASCII code length corresponding to the IP or domain name, and the remaining registers are used to store the ASCII code value corresponding to the IP or domain name. For example, if the IP is 116.62.42.192, the port is 31687, and there are 13 characters in total, that is, the length is 0x000D, and the ASCII code value corresponding to the IP is 31 31 36 2E 36 32 2E 34 32 2E 31 39 32. The corresponding modbus register storage value is as shown in the following table. If it is a domain name, the corresponding domain name is also converted into the hexadecimal corresponding to ASCII for storage. (Note: The maximum length of the domain name does not exceed 40 ASCII codes)

| 40101 (0x0063) | 40101(0x0064) -- 40121(0x0078) |
|---|---|
| length | IP or domain name value |
| 00 0D | 31 31 36 2E 36 32 2E 34 32 2E 31 39 32 |

Port 31687 corresponds to hexadecimal 7BC7; protocol type (TCP, UDP) is saved using protocol registers, value 0x0001 corresponds to TCP protocol, value 0x0000 corresponds to UDP protocol. That is, when the IP is 116.62.42.192, port is 31687, TCP protocol, unused IP or domain name registers can be filled with "0" or not filled. If you need to use function code "0x10" to write IP, domain name, port, and protocol type at one time, then the unused registers must be filled with values to continuously write modbus registers. The corresponding register values are as follows:

| 40100 (0x0063) | 40101(0x0064) -- 40121(0x0078) | 40122 (0x0079) | 40123 (0x007A) |
|---|---|---|---|
| IP or domain name length | IP or domain name value | Server Port | TCP |
| 00 0D | 31 31 36 2E 36 32 2E 34 32 2E 31 39 32 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 7B C7 | 00 01 |

Since the length of the IP or domain name register is greater than the length of the IP or domain name value, the length of the IP or domain name needs to be considered when writing the IP register, that is, how many registers are needed. For example, write the above IP to the modbus register:

Modbus RTU protocol writes Socket registers:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 01 | 10 | 00 63 | 00 18 | 30 | 00 0D 31 31 36 2E 36 32 2E 34 32 2E 31 39 32<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 7B<br>C7 00 01 | 7B F0 |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | Device ModBus address | Function code | address | Register length | Number of bytes | Write value | CRC Check code |
|---|---|---|---|---|---|---|---|

| Receive | 01 | 10 | 00 63 | 00 18 | 30 1D |
|---|---|---|---|---|---|
| | Device ModBus address | Function code | address | Register length | CRC checksum |

Modbus TCP protocol writes Socket registers:

| Send | 00 01 | 00 00 | 00 37 | 01 | 10 | 00 63 | 00 18 | 30 | 00 0D 31 31 36 2E 36 32 2E 34 32 2E 31 39 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7B C7 00 01 |
|---|---|---|---|---|---|---|---|---|---|
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Register length | Number of bytes | Write value |

| Receive | 00 01 | 00 00 | 00 06 | 01 | 10 | 00 63 | 00 18 |
|---|---|---|---|---|---|---|---|
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Register length |

### 4.4.2 Custom Registration Package

The custom registration package can be ASCII code or hex. The length of hex code cannot be greater than 20 bytes, and the length of ASCII code cannot be greater than 40 bytes. The first register of the custom registration package is used to store the registration package type. The value 0x0000 indicates that the registration package is in hex format, and the value 0x0001 indicates that the registration package is in ASCII format. When the value is 0x0001, the registration package value is ABCDEFGHIJ, and the corresponding ASCII code value is the registration package value in the following table. The second register of the custom registration package is used to store the length of the registration package value. The registration package value length is 10, corresponding to hexadecimal 0x0A. Like the IP register, the unused registration package value register can be filled with "0" or not filled.

| 40124 (0x007B) | 40125 (0x007C) | 40126(0x007D) -- 40145(0x0090) | 40146 (0x0091) |
|---|---|---|---|
| type | length | Registration Package Value | Registration package mechanism |
| 00 01 | 00 0A | 41 42 43 44 45 46 47 48 49 4A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 00 01 |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | | | |
|---|---|---|---|
| | | 00 00 00 00 00 00 00 00 00 00 | |

The registration package mechanism has 5 modes:

| Registration Packet Mechanism Register Value (0x0091) | Corresponding function description |
|---|---|
| 00 00 | Disable the registration package mechanism |
| 00 01 | Add MAC/IMEI as registration package data before each packet sent to the server |
| 00 02 | Add custom registration package data before each packet sent to the server |
| 00 03 | Only send a MAC/IMEI registration packet when connecting to the server for the first time |
| 00 04 | A user-defined registration packet is sent only when connecting to the server for the first time |

Modbus RTU protocol write registration packet register:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Send | 01 | 10 | 00 7B | 00 17 | 2E | 00 01 00 0A 41 42 43 44 45 46 47 48 49 4A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 | 00 F4 |
| | Device ModBus address | Function code | address | Register length | Number of bytes | Write value | CRC Check code |

| | | | | | |
|---|---|---|---|---|---|
| Receive | 01 | 10 | 00 7B | 00 17 | F0 1E |
| | Device ModBus address | Function code | address | Register length | CRC checksum |

Modbus TCP protocol write registration packet register:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Send | 00 01 | 00 00 | 00 33 | 01 | 10 | 00 7B | 00 17 | 2E | 00 01 00 0A 41 42 43 44 45 46 47 48 49 4A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Register length | Number of bytes | Write value |

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Receive | 00 01 | 00 00 | 00 06 | 01 | 10 | 00 7B | 00 17 |
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Register length |

### 4.4.3 Heartbeat Packet

The heartbeat packet can be ASCII code or hex. The length of hex code cannot be greater than 20 bytes, and the length of ASCII code cannot be greater than 40 bytes. The first register of the heartbeat packet is used to store the heartbeat packet data type. The value 0x0000 indicates that the heartbeat packet is in hex format, and the value 0x0001 indicates that the heartbeat packet is in ASCII format. When the value is 0x0000, the heartbeat packet value is 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09. The second register of the heartbeat packet is used to store the length of the heartbeat packet value. The heartbeat packet value length is 10, corresponding to decimal 0x0A. Like the custom registration package register, the unused heartbeat packet value register can be filled with "0" or not filled.

| 40147 (0x0092) | 40148 (0x0093) | 40149(0x0094) -- 40168(0x00A7) |
|---|---|---|
| type | length | Registration Package Value |
| 00 00 | 00 0A | 00 01 02 03 04 05 06 07 08 09<br>00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 |

Modbus RTU protocol write registration packet register:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| send | 01 | 10 | 00 92 | 00 16 | 2C | 00 00 00 0A 00 01 02 03 04 05 06 07 08 09 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 52 9E |
| | Device ModBus address | Function code | address | Register length | Number of bytes | Write value | CRC Check code |

| | | | | | |
|---|---|---|---|---|---|
| take over | 01 | 10 | 00 92 | 00 16 | E0 2A |
| | Device ModBus address | Function code | address | Register length | CRC checksum |

Modbus TCP protocol write registration packet register:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| send | 00 01 | 00 00 | 00 33 | 01 | 10 | 00 92 | 00 16 | 2C | 00 00 00 0A 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Register length | Number of bytes | Write value |
|---|---|---|---|---|---|---|---|---|---|

| take over | 00 01 | 00 00 | 00 06 | 01 | 10 | 00 92 | 00 16 |
|---|---|---|---|---|---|---|---|
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Register length |

### 4.4.4 Heartbeat Packet Time

The heartbeat packet time setting range is 0-65535 seconds. When the heartbeat packet time is set to 0, the heartbeat packet is turned off. Set the heartbeat packet time to 5s as follows.

Modbus RTU protocol write heartbeat packet time register:

| Send | 01 | 06 | 00 A8 | 00 05 | C8 29 |
|---|---|---|---|---|---|
| | Device ModBus address | Function code | address | Write value | CRC checksum |

| Receive | 01 | 06 | 00 A8 | 00 05 | C8 29 |
|---|---|---|---|---|---|
| | Device ModBus address | Function code | address | Write value | CRC checksum |

Modbus TCP protocol Modbus RTU protocol write heartbeat packet time register:

| Send | 00 01 | 00 00 | 00 06 | 01 | 06 | 00 A8 | 00 05 |
|---|---|---|---|---|---|---|---|
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Write value |

| Receive | 00 01 | 00 00 | 00 06 | 01 | 06 | 00 A8 | 00 05 |
|---|---|---|---|---|---|---|---|
| | Transmission ID | Protocol Identifier | length | Unit identification | Function code | address | Write value |

### 4.4.5 Ebyte Cloud Transmission

The Ebyte Cloud transparent transmission function can be turned on or off. The corresponding register for this function is 40170 (0x00A9), supporting 0x03, 0x06, and 0x10 function codes:

When the register value is 0x0000, the cloud transparent transmission function is disabled;

When the register value is 0x0001, the cloud transparent transmission function is enabled;

The default factory setting is to disable cloud transparent transmission.

### 4.4.6 IMEI reading

The starting address of IMEI register reading is 40171 (0x00AA), and the total length of register is 11, among which the first register is the IMEI length, and the second to eleventh registers store the IMEI value.

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

For example, IMEI:867732035802677, the corresponding register value is as shown in the following table. In the register, the IMEI value exists in hexadecimal ASCII value.

| 40171 (0x00AA) | 40172 (0x00AB) --40181 (0x00B4) |
|---|---|
| IMEI length | IMEI value |
| 00 0F | 38 36 37 37 33 32 30 33 35 38 30 32 36 37 37 00 00 00 00 00 |

### 4.4.7 SN Read

The SN register read start address is 40182 (0x00B5), and the total register length is 11, of which the first register is the SN length, and the second to eleventh registers store the SN value. For example, if SN: 181101194228B027, the corresponding register value is as shown in the following table. In the register, the SN value exists in hexadecimal ASCII value.

| 40182 (0x00B5) | 40183 (0x00B6) --40192 (0x00BF) |
|---|---|
| SN length | SN value |
| 00 10 | 31 38 31 31 30 31 31 39 34 32 32 38 42 30 32 37 |

### 4.4.8 Reading the base station positioning value LBS

The base station positioning register reads the starting address 40193 (0x00C0), and the total length of the register is 20, of which the first register is the base station positioning information length, and the second to twentieth registers store the base station positioning value. For example, the base station positioning value LAC: 812F, CID: 8056B08, the corresponding register value is as shown in the following table. In the register, the base station positioning value exists in hexadecimal ASCII value.

| 40193 (0x00C0) | 40194 (0x00C1) --40213 (0x00D4) |
|---|---|
| Base station positioning value length | Base station positioning value |
| 00 14 | 4C 41 43 3A 38 31 32 46 2C 43 49 44 3A 38 30 35 36 42 30 38 |

# Important Notice

- Ebyte reserves the final right of interpretation and modification of all contents in this manual.
- Due to the continuous improvement of the product hardware and software, this manual may be changed without prior notice. The latest version of the manual shall prevail.
- Protecting the environment is everyone's responsibility: To reduce paper usage, this manual is only printed in Chinese. The English manual is only available in electronic format. If necessary, please download it from our official website. In addition, unless otherwise requested by the user, when placing a bulk order, we will only provide product manuals in proportion to the order quantity. Not every digital radio will be provided with a manual. Please understand.

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

# Revision History

| Version | Revision Date | Revision Notes | Maintainer |
|---|---|---|---|
| 1.1 | 2025-05-26 | Format revision | lyl |

# About Us

Technical support: support@cdebyte.com
Documents and RF Setting download link: www.cdebyte.com/en/
Tel：+86-28-61399028
Fax：028-64146160
Web：www.cdebyte.com/en/
Address：Innovation Center D347, 4# XI-XIN Road,Chengdu, Sichuan, China

Copyright@2025, Chengdu Ebyte Electronic Technology Co.,Ltd.


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000