



EBYTE

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

Wireless Modem

用户使用手册



本说明书可能会随着产品的改进而更新，请以最新版的说明书为准
成都亿佰特电子科技有限公司保留对本说明中所有内容的最终解释权及修改权

Content

DISCLAIMER.....	3
FEATURES.....	4
1. QUICK START.....	5
1.1 PORT CONNECTION.....	5
1.1.1 RS485 connection.....	5
1.1.2 Switch input connection.....	5
1.1.3 Relay output connection.....	5
1.2 SIMPLE TO USE.....	5
1.2.1 RS485 bus control.....	6
1.2.2 network control.....	7
2. PRODUCT DESCRIPTION.....	7
3. MODBUS.....	12
3.1 REGISTER ADDRESS TABLE.....	12
3.2 MODBUS ADDRESS TABLE.....	13
3.3 RS485 SERIAL PORT BAUD RATE CODE TABLE.....	14
3.4 RS485 SERIAL PORT CHECK DIGIT VALUE TABLE.....	14
3.5 CONFIGURE PARAMETERS THROUGH THE HOST COMPUTER.....	14
4. PRODUCT FEATURES.....	15
4.1 WORKING MODE.....	15
4.1.1 Slave Mode.....	15
4.1.2 Host Mode.....	15
4.2 BASIC FUNCTIONS OF IO.....	16
4.2.1 Digital DO output.....	16
4.2.2 Reading digital DI input.....	18
4.3 IO FEATURES.....	19
4.3.1 Pulse count and count clear.....	19
4.3.2 Automatic reporting of digital input DI:.....	20
4.3.3 Switch output DO time setting.....	21
4.3.4 Restart switch output state setting.....	21
4.4 NETWORK RELATED FUNCTIONS.....	21
4.4.1 Server IP or Domain Name, Port, TCP or UDP Settings (Socket).....	21
4.4.2 Custom Registration Package.....	23
4.4.3 Heartbeat Packet.....	25
4.4.4 Heartbeat Packet Time.....	26
4.4.5 EBYTE cloud transmission.....	26
4.4.6 IMEI read.....	27
4.4.7 SN read.....	27
4.4.8 Base station positioning value LBS reading.....	27
IMPORTANT NOTICE.....	28
REVISION HISTORY.....	29
ABOUT US.....	29

Disclaimer

EBYTE reserves all rights to this document and the information contained herein. Products, names, logos and designs described herein may in whole or in part be subject to intellectual property rights. Reproduction, use, modification or disclosure to third parties of this document or any part thereof without the express permission of EBYTE is strictly prohibited.

The information contained herein is provided “as is” and EBYTE assumes no liability for the use of the information. No warranty, either express or implied, is given, including but not limited, with respect to the accuracy, correctness, reliability and fitness for a particular purpose of the information. This document may be revised by EBYTE at any time. For most recent documents, visit www.ebyte.com.

Features

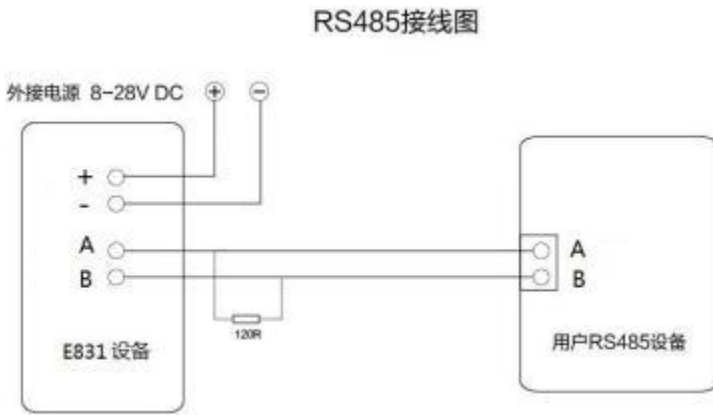
- Support 6 digital inputs, default dry contact;
- Support 6 relay outputs;
- Support socket connection to remote server, support TCP/UDP;
- Adopt Modbus TCP/RTU protocol data processing;
- Support connection to Ebyte cloud, command control;
- Support 2 working modes, master mode, slave mode, the slave can cascade multiple devices through RS485;
- Support Reload light touch button, long press for 5s, Modbus device address, RS485 serial port baud rate and parity bit are restored to factory settings; Hardware watchdog, with high reliability;
- Multiple indicator lights show working status;
- The power supply has good overcurrent, overvoltage, anti-reverse connection and other functions.
- Note: Customers can customize functions, such as condition control (determine how to output according to the input state)

1. Quick start

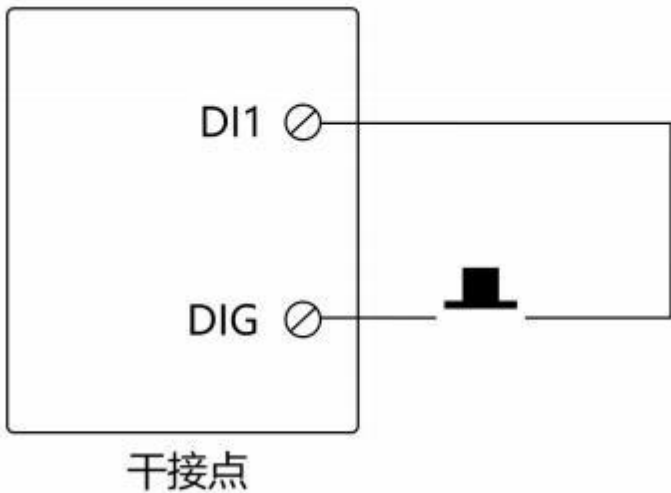
This chapter is a quick introduction to the E831-RTU (6060-4G) series products. It is recommended that users read this chapter and operate according to the instructions. They will have a systematic understanding of the module products. Users can also choose according to their needs. chapter to read. Refer to subsequent chapters for specific details and instructions.

1.1 Port connection

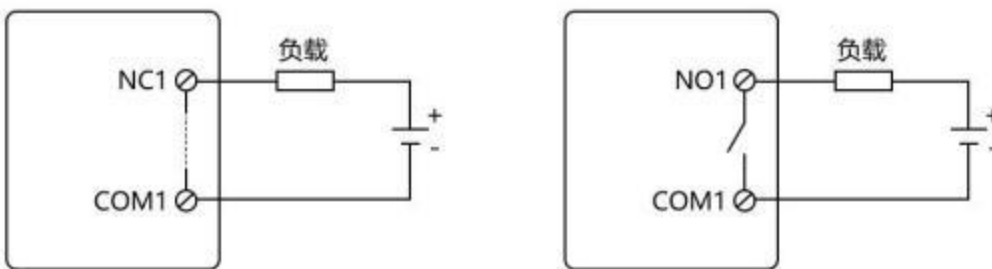
1.1.1 RS485 connection



1.1.2 Switch input connection



1.1.3 Relay output connection



1.2 Simple to use

Wiring: The computer is connected to E831-RTU (6060-4G) via USB to RS485.

Networking: Insert the SIM card while the power is off.
Power supply: E831-RTU (6060-4G) operating voltage is DC 8~28V.

1.2.1 RS485 bus control

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



After the device is discovered, click Stop.

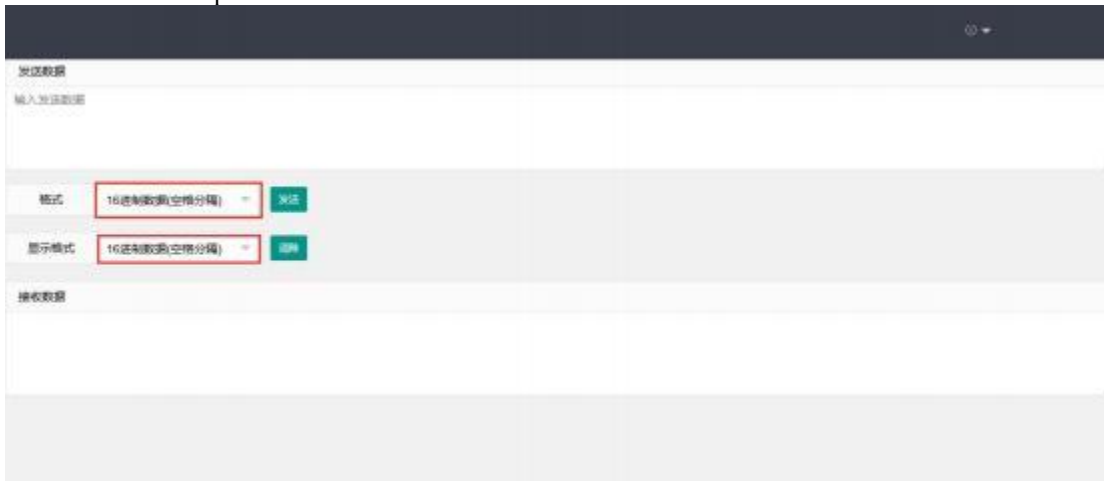


At this time, the device address of the current device can be seen, and the "automatic refresh" processing can be performed to control the switch output and read the switch input.



1.2.2 network control

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



2. Product description

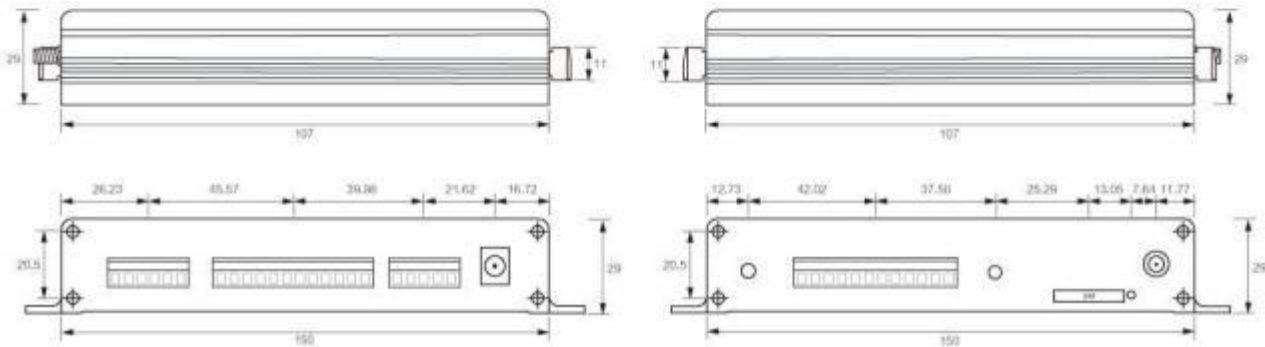
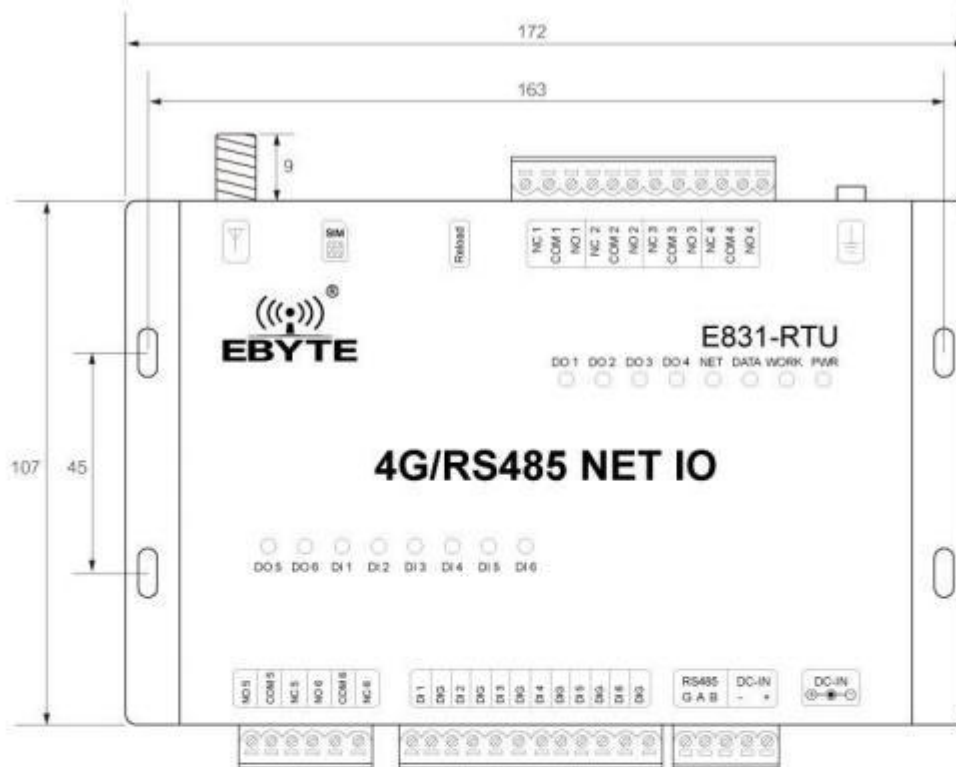
E831-RTU(6060-4G) is a network IO product that supports 6-channel digital input (default dry contact) and 6-channel relay output. Support Modbus TCP/RTU protocol. The product is highly usable, and users can easily and quickly integrate into their own systems to achieve 4G-based remote control.

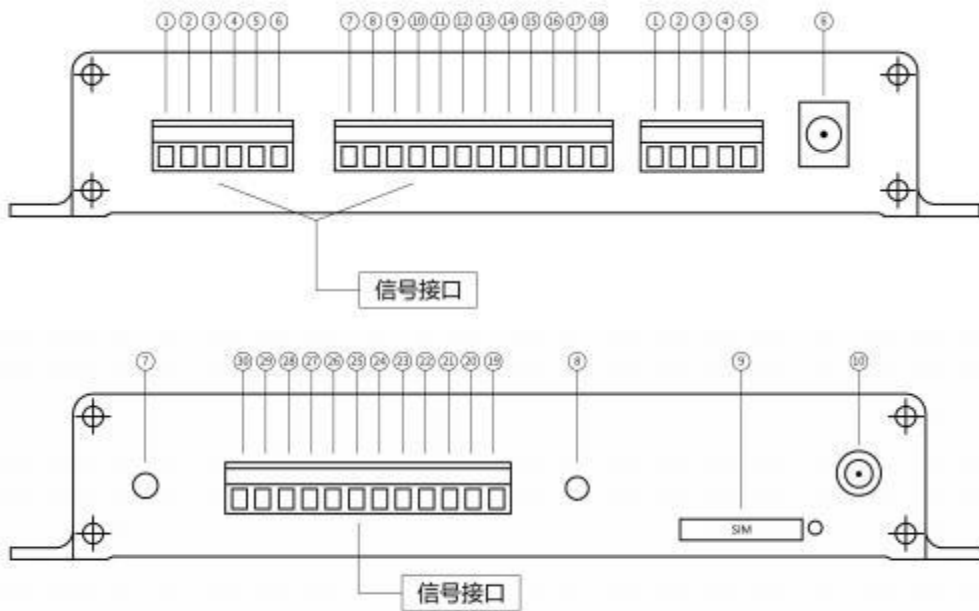
2.1 Basic parameters

	Project	Norm
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
	Size(H*W*D)	172*107*29mm
	Weight	484.5±5g
	Operating	-20°C~+70°C

Hardware parameters	temperature	
	Storage temperature	-40°C~+85°C
	Working humidity	5%~95%
	Storage humidity	1%~95%
	Operating Voltage	8V~28V
	Data interface	RS485: 1200~115200bps
Software parameters	Network Type	4G
	Configuration command	Modbus TCP/RTU
	Network protocol	Modbus TCP/RTU
	Operating mode	master mode, slave mode
	Data transmission method	TCP/UDP

2.2 Dimensions and interface description





No.	Port and Other Definitions	Function	Directions
1	RS485 G	Signal reference ground	Signal reference ground, not connected
2	RS485 A	RS485 interface A	RS485 interface A is connected to the device A interface
3	RS485 B	RS485 interface B	RS485 interface B is connected to the device B interface
4	DC-IN -	Crimp power input negative pole	Power reference ground
5	DC-IN +	Crimp power input positive pole	Power input, DC 8V~36V, 12V/24V recommended
6	DC-IN seat	DC socket 5.5*2.1mm	Power input terminal, DC 8V~36V, 12V/24V recommended
7	ground screw	connect with the earth	connect with the earth
8	Reload	reset button	Long press for 5s works
9	SIM card slot	SIM card slot	Insert SIM card, connect to the Internet
10	ANT	Antenna interface	GPRS antenna
Signal interface			
1	NO 5	Relay 5 normally open pin	For use with relay 5 common
2	COM 5	Relay 5 Common	For use with relay 5 NO pin/NC pin
3	NC 5	Relay 5 normally closed pin	For use with relay 5 common
4	NO 6	Relay 6 normally open pin	For use with relay 6 common
5	COM 6	Relay 6 Common	For use with relay 6 NO pin/NC pin
6	NC 6	Relay 6 normally closed pin	For use with relay 6 common
7	DI 1	Switch input channel 1	Form dry contact with DIG
8	DIG	Switch input ground	Can be paired with DI 1
9	DI 2	Switch input channel 2	Form dry contact with DIG
10	DIG	Switch input	Can be paired with DI 2

		ground	
11	DI 3	Switch input channel 3	Form dry contact with DIG
12	DIG	Switch input ground	Used in pairs with DI 3
13	DI 4	Switch input channel 4	Form dry contact with DIG
14	DIG	Switch input ground	Can be paired with DI 4
15	DI 5	Switch input channel 5	Form dry contact with DIG
16	DIG	Switch input ground	Can be paired with DI 5
17	DI 6	Digital input channel 6	Form dry contact with DIG
18	DIG	Switch input ground	Can be paired with DI 6
19	NC 1	Relay 1 normally closed pin	For use with relay 1 common
20	COM 1	Relay 1 Common	For use with Relay 1 NO pin/NC pin
21	NO 1	Relay 1 normally open pin	For use with relay 1 common
22	NC 2	Relay 2 normally closed pin	For use with relay 2 common
23	COM 2	Relay 2 Common	For use with Relay 2 NO/NC pins

24	NO 2	Relay 2 normally open pin	For use with relay 2 common
25	NC 3	Relay 3 normally closed pin	For use with relay 3 common
26	COM 3	Relay 3 Common	For use with relay 3 NO pin/NC pin
27	NO 3	Relay 3 normally open pin	For use with relay 3 common
28	NC 4	Relay 4 normally closed pin	For use with relay 3 common
29	COM 4	Relay 4 Common	For use with relay 4 NO pin/NC pin
30	NO 4	Relay 4 normally open pin	For use with relay 4 common
LED light			
1	DO 5	Relay 5 output indication	Green LED, NO 5, COM 5 is closed and lights up
2	DO 6	Relay 6 output indication	Green LED, NO 6, COM 6 closed on
3	DI 1	Switch input channel 1 indication	Green LED, lights up when DI 1, DIG are short-circuited
4	DI 2	Switch input channel 2 indication	Green LED, DI 2, DIG short-circuited on
5	DI 3	Switch input channel 3 indication	Green LED, lights up when DI 3, DIG are short-circuited
6	DI 4	Switch input channel 4 indication	Green LED, lights up when DI 4, DIG are short-circuited
7	DI 5	Switch input channel 5 indication	Green LED, lights up when DI 5, DIG are short-circuited
8	DI 6	Digital input channel 6 indication	Green LED, lights up when DI 6, DIG are short-circuited
9	DO 1	Relay 1 output indication	Green LED, ON when NO 1, COM 1 are closed
10	DO 2	Relay 2 output indication	Green LED, ON when NO 1, COM 1 are closed
11	DO 3	Relay 3 output indication	Green LED, NO 3, COM 3 closed and illuminated
12	DO 4	Relay 4 output indication	Green LED, NO 4, COM 4 closed and illuminated
13	NET	network indication	Green LED, NO 4, COM 4 closed and illuminated
14	DATA	Serial data indication	Yellow LED, lights up when there is data transmission on the RS485 interface (flashing)
15	WORK	Work/Reset Indication	Yellow LED, lights up when there is data transmission on the RS485 interface (flashing)
16	PWR	Power indicator	Red LED, always on

Notice:

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

2.3 Reload touch button description

Long press for 5S is valid. 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.

3. Modbus

3.1 Register address table

Register address table (function code: 0x01H, 0x05H, 0x0FH, 0x03H, 0x06H, 0x10H)					
Register address	register quantity	Register properties	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 (0x0040)	1	DI1-DI6 Pulse count clear	只写	0x00 - 0x0F	0x06
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	read/wri	0 - 2	

		reporting of switch value	te		
40083 (0x0052)	1	Switch output time setting (millisecond)	read/write	300-65535	
reserve					
40084 (0x0053)	1	Switch value restart output state Setting	read/write	0x00 - 0x40	0x03 0x06 0x10
reserve					
40100 (0x0063)	22	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	agreement type(UDP、TCP)	read/write	0 - 1	
40124(0x007B)	22	custom registration package	read/write	--	
40146(0x0091)	1	Registration package mechanism	read/write	0 - 4	
40147(0x0092)	22	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

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 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 digit value table

Check Digit Value Table	
0 (default)	no verification
1	even parity
2	Odd parity

3.5 Configure parameters through the host computer

Select the "parameter setting" column to read and write parameters. For specific functions, see the product function introduction below.



4. Product Features

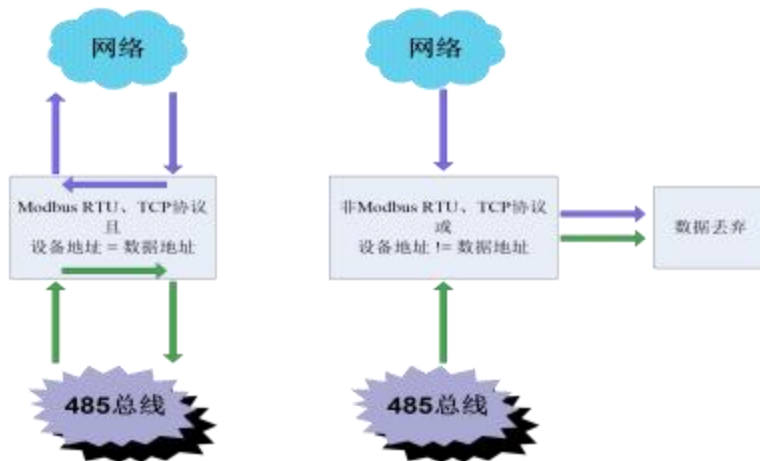
4.1 Working Mode

The working mode is divided into master mode and slave mode, which are configured through Modbus register 40081 (0x0050). When the register value is 0, it is the master mode; when the register value is 1, it is the slave mode, and the default 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 complies with the Modbus RTU and Modbus TCP protocols, and the address in the data is the device address, and the device will respond with the same protocol. If the data sent by the network end or the 485 bus end to the device does not meet the Modbus RTU and Modbus TCP protocols, or if it meets the Modbus RTU and Modbus TCP protocols but the data address is not the device address, the data at the sending end will be discarded.

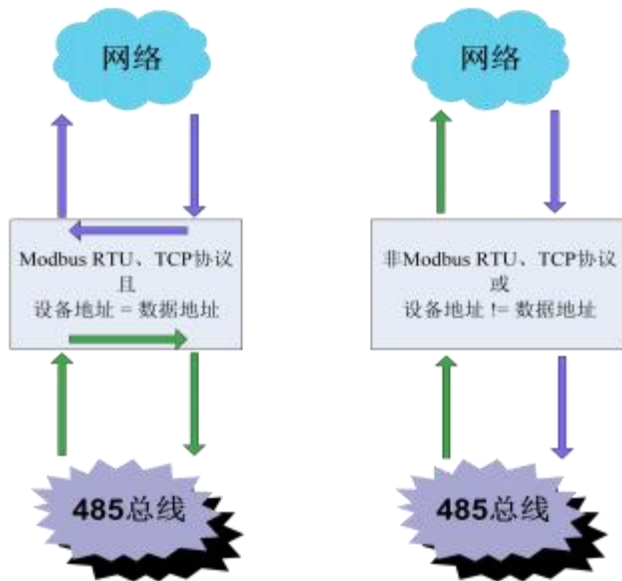
In the slave mode, the device can directly connect to the device in the master mode through the 485 bus, so that when the slave is not connected to the Internet, the network can also access the data of the slave through the host.



4.1.2 Host Mode

In the host mode (the register value is 0x00), the data sent by the network terminal or the 485 bus terminal (sender) to the device complies with 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 terminal or the 485 bus terminal to the device does not meet the Modbus RTU, Modbus TCP protocol, or meet the Modbus RTU, Modbus TCP protocol but the data address is not the device address, the data from the 485 bus will be transmitted to the network , the data from the network will be transmitted to the 485 bus.

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



4.2 Basic functions of IO

4.2.1 Digital DO output

Read digital DO output

Function code: 01, read coil status

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

Description: The equipment relay is passively output. When the coil is not energized, the relay NC port and COM port are normally closed, and the NO port and COM port are normally open, and the value is 0; when the coil is energized, the phenomenon is opposite, the relay NC port and COM port are disconnected Open, NO port and COM port are closed, the value is 1. Query the relay status by command.

example:

Read the 6-channel switching output status, assuming the return value is 03, corresponding to the binary bit 0000 0011, the lower six bits represent the switching output status, which are DO6, DO5, DO4, DO3, DO2, DO1 in sequence.

Modbus RTU protocol to read digital output:

send	01	01	00 10	00 06	BD CD
	Device ModBus address	function code	Switch start address	Number of read switches	CRC check code

receive	01	01	01	03	11 89
---------	----	----	----	----	-------

	Device ModBus address	function code	returns the number of bytes	Switch output value	CRC check code
--	-----------------------	---------------	-----------------------------	---------------------	----------------

Modbus TCP protocol to read digital output:

send	00 01	00 00	00 06	01	01	00 10	00 06
	Transport ID	Protocol ID	length	Unit ID	function code	Switch start address	Number of read switches

receive	00 01	00 00	00 04	01	01	01	03
	Transport ID	Protocol ID	length	Unit ID	function code	returns the number of bytes	Number of read switches

Control switch DO output

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

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

Description: The device relay is passively output, the coil is not energized, the relay NC port and COM port are closed, and the NO port and COM port are disconnected; the coil is energized, the relay NC port and COM port are disconnected, and the NO port and COM port are closed. Control relay state by command.

example:

Function code 0x05 Write DO2 digital output, make NC2, COM2 open, NO2, COM2 close, the write value is FF 00; make NC2, COM2 close, NO2, COM2 open, write the value 00 00.

Modbus RTU protocol write switch output:

send	01	05	00 11	FF 00	DC 3F
	DeviceModBus address	function code	switch address	write value	CRC check code

receive	01	05	00 11	FF 00	DC 3F
	Device ModBus address	function code	switch address	write value	CRC check code

Modbus TCP protocol write switch output:

send	00 01	00 00	00 06	01	05	00 11	FF 00
	Transport ID	Protocol ID	length	Unit ID	function code	switch address	write value

receive	00 01	00 00	00 06	01	05	00 11	FF 00
	Transport	Protocol	length	Unit ID	function code	switch address	write value

	ID	ID					
--	----	----	--	--	--	--	--

Function code 0x0F Write DO2, DO3 digital output, make NC2, COM2 open, NO2, COM2 close; make NC3, COM3 open, NO3, COM3 close. The write value should be 0x03, corresponding to binary bits 0000 0011

Modbus RTU protocol write switch output:

send	01		0F	00 11	00 02	01	03	62 95
	Device address	ModBus address	Function code	switch address	Number of write switches	of number of bytes	write value	CRC check code

receive	01		0F	00 11	00 02	84 0F		
	Device address	ModBus address	function code	switch address	write value	CRC check code		

Modbus TCP protocol write switch output:

Send	00 01	00 00	00 08	01	0F	00 11	00 02	01	03
	Transport ID	Protocol ID	length	Unit ID	function code	switch address	Number of write switches	of number of bytes	write value

Receive	00 01	00 00	00 06	01	0F	00 11	00 02		
	Transport ID	Protocol ID	length	Unit ID	function code	switch address	Number of write switches		

4.2.2 Reading digital DI input

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

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

Description: 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-channel switching value input value, DI input terminal DI1, COM1 short circuit, DI2, COM2 not short circuit, DI3, COM3 short circuit, DI4, COM4 not short circuit, DI5, COM5 not short circuit, DI6, COM6 not short circuit catch. The read digital input value is 0x05, corresponding to binary 0000 0101, and the six lower six bits represent the digital input value, which are DI6, DI5, DI4, DI3, DI2, DI1 in sequence.

Modbus RTU protocol to read digital input:

send	01		02	00 10	00 06	F9 CD		
	Device address	ModBus address	function code	Switch start address	Number of switches	of read	CRC check code	
Receive	01		02	01	05	61 8B		

	Device ModBus address	function code	returns the number of bytes	Switch input value	CRC check code
--	-----------------------	---------------	-----------------------------	--------------------	----------------

Modbus TCP protocol to read digital input:

send	00 01	00 00	00 06	01	02	00 10	00 06
	Transport ID	Protocol ID	length	Unit ID	function code	Switch start address	Number of read switches

Receive	00 01	00 00	00 04	01	02	01	05
	Transport ID	Protocol ID	length	Unit ID	function code	returns the number of bytes	Switch input value

4.3 IO Features

4.3.1 Pulse count and count clear

The pulse count will not be saved after power off, and the pulse level maintenance time must be greater than 10ms to be effective. The digital input changes from the open state to the closed state and maintains the closing time of more than 10ms, and then changes to the open state to complete one pulse count.

Read pulse count value

Function code: 03, read holding register

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

Description: The maximum value of pulse count is 65535

example:

DI1 has detected 16 pulses currently, DI2 has detected 3 pulses currently, read the digital input count value of DI1 and DI2

Modbus RTU protocol read pulse count value:

Send	01	03	00 30	00 02	C4 04
	Device ModBus address	function code	initial address	number of reads	CRC check code

Receive	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 check code

Modbus TCP protocol read pulse count value:

Send	00 01	00 00	00 06	01	03	00 30	00 02
	Transport ID	Protocol ID	length	Unit ID	function code	initial address	number of reads

Receive	00 01	00 00	00 07	01	03	04	00 10	00 03
	Transport ID	Protocol ID	length	Unit ID	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)

Description: 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 count is restarted. example:

Clear the pulse count value of DI2, DI4, keep the pulse count value of DI1, DI3, D5, D6. The write value should be 0x0a, the corresponding binary value is 0000 1010, the pulse count value of Modbus RTU protocol clear

Send	01	06	00 40	00 0a	08 19
	Device address	ModBusfunction code	address	write value	CRC check code

Receive	01	06	00 40	00 0a	08 19
	Device ModBus address	function code	address	write value	CRC check code

Modbus TCP protocol clear pulse count value:

Send	00 01	00 00	00 06	01	06	00 40	00 0a
	Transport ID	Protocol ID	length	Unit ID	Function code	address	write value

Receive	00 01	00 00	00 06	01	06	00 40	00 0a
	Transport ID	Protocol ID	length	Unit ID	Function code	address	write value

4.3.2 Automatic reporting of digital input DI:

The automatic reporting function of digital input is to transmit the change value when the digital value changes. You can choose to transmit through RS485 or GPRS, or you can 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:

Turn off the automatic reporting function of the switch value

The switch value is automatically reported and transmitted through RS485

The switch value is automatically reported and transmitted through the GPRS network

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

0x00 means the digital input is disconnected,

0x01 means the switch input is closed,

0xFF means that the digital input has not changed,

The values of DI1, DI2, DI3, DI4, DI5, DI6 in the table represent that the status of DI1 and DI2 is updated to open, the status of DI3 is updated to be closed, and the status of DI4, DI5, and DI6 has not changed. The last two bytes are the modbus CRC16 calculation value.

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 digital pulse output time setting is to set the digital 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 digital output Closed is the hold state, that is, the switch output is held all the time after it is closed. If it is set to 300ms and above, such as 500ms, after sending the switch output close command, the switch value will be closed for 500ms, and then automatically disconnected after 500ms.

4.3.4 Restart switch output state setting

Whether the device keeps the state before power off or restarts to keep the specific output state, 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 restart output state setting is 40085 (0x0054), and its value range is 0x00-0x40. When this register value is 0x40

After power off and restart, the last switch output state is maintained; when the value of this register is 0x00-0x3F, the lower six bits determine the switch output state when the device is restarted, 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 the power is turned on, DO6, DO5, DO4, DO2 are in closed state (relay NO, COM is closed) DO3, DO1 is in open state (relay NO, COM is open), The corresponding register value is 0011 1010, that is, 0x3A, "1" is the closed state, and "0" is the 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 by 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, IP is 116.62.42.192, port is 31687, a total of 13 characters, that is, the length is 0x000D, the corresponding ASCII code value of IP is 31 31 36 2E 36 32 2E 34 32 2E 31 39 32, the corresponding modbus register storage value is as follows surface. 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, corresponding to hexadecimal 7BC7; the protocol type (TCP, UDP) is stored in the protocol register, the value 0x0001 corresponds to the TCP protocol, and the value 0x0000 corresponds to the UDP protocol. That is, when the IP is 116.62.42.192, the port is 31687, and the TCP protocol is used, the unused IP or domain name register can be filled with "0" or not filled. If you need to use the function code "0x10" to write the IP, domain name, port at one time , protocol type, 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 protocol
00 0D	31 31 36 2E 36 32 2E 34 32 2E 31 39 32 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, it is necessary to consider the length of the IP or domain name when writing the IP register, that is, how many registers need to be occupied. For example, write the above IP into the modbus register:

Modbus RTU protocol write Socket register:

Send	01	10	00 63	00 18	30	00 0D 31 31 36 2E 36 32 2E 34 32 2E 31 39 32 00 7B C7 00 01	7B F0
	equipment 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 check code

Modbus TCP protocol write Socket register:

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 7B C7 00 01
	Transport ID	Protocol ID	length	Unit ID	function code	address	register length	number of bytes	write value

receive	00 01	00 00	00 06	01	10	00 63	00 18
	Transport ID	Protocol ID	length	Unit ID	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 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 code format. When the value is 0x0001, the registration package value is ABCDEFGHIJ, and the corresponding ASCII code value Register package values as shown in the following table. The second register of the custom registration package is used to store the length of the registration package value. The length of the registration package value is 10, and the corresponding hexadecimal value is 0x0A. Like the IP registers, the unused registration packet value registers can be filled with "0" or not filled.

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

The registration package mechanism has 5 modes:

Register Packet Mechanism Register Value(0x0091)	Corresponding function description
00 00	Close the registration package mechanism
00 01	Add MAC/IMEI as registration packet data before each packet sent to the server
00 02	Add custom registration packet 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	Only send a user-defined registration packet 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 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 address	ModBus code	function code	address	register length	CRC code

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 01
	Transp ort ID	Protoc ol ID	length	Unit ID	function code	addres s	register length	number of bytes	write value

receive	00 01	00 00	00 06	01	10	00 7B	00 17
	Transport ID	Protocol ID	length	Unit ID	function code	address	register length

4.4.3 Heartbeat Packet

The heartbeat packet can be ASCII code or hex, the length of hex 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 data type of the heartbeat packet. The value 0x0000 means the heartbeat packet is in hex format, and the value 0x0001 means 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 length of the heartbeat packet value is 10, corresponding to decimal 0x0A. Like the custom registration packet register, the unused heartbeat packet value register can be filled with "0" or not.

40147 (0x0092)	40148 (0x0093)	40149 (0x0094) -- 40168 (0x00A7)
Type	length	register package value
00 00	00 0A	00 01 02 03 04 05 06 07 08 09 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	52 9E
	Device ModBus address	Function code	address	register length	number of bytes	write value	CRC check code

Receive	01	10	00 92	00 16	E0 2A	
	Device address	ModBus	Function code	address	register length	CRC code

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
	Transport ID	Protocol ID	length	Unit ID	function code	address	register length	number of bytes	write value

Receive	00 01	00 00	00 06	01	10	00 92	00 16
	Transport ID	Protocol ID	Unit ID	Unit ID	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 duration to 5s as follows. Modbus RTU protocol write heartbeat packet time register:

Send	01	06	00 A8	00 05	C8 29
	Device address	ModBus	function code	address	write value

Receive	01	06	00 A8	00 05	C8 29
	Device address	ModBus	function code	address	write value

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

Send	00 01	00 00	00 06	01	06	00 A8	00 05
	Transport ID	Protocol ID	length	Unit ID	function code	address	write value

Receive	00 01	00 00	00 06	01	06	00 A8	00 05
	Transport ID	Protocol ID	length	Unit ID	function code	address	write value

4.4.5 EBYTE cloud transmission

Ebyte cloud transparent transmission function can be turned on or off. The corresponding design register for this function is 40170 (0x00A9), which supports 0x03, 0x06, 0x10 function codes: When the value of this register is 0x0000, the cloud transparent transmission function is turned off;

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

By default, cloud transparent transmission is disabled.

4.4.6 IMEI read

The starting address for reading the IMEI register is 40171 (0x00AA), and the total length of the register is 11. The first register is the IMEI length, and the second to eleventh registers store the IMEI value. For example, IMEI: 867732035802677, the corresponding register value is as follows. 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 starting address for reading the SN register is 40182 (0x00B5), and the total length of the register is 11. The first register is the SN length, and the second to eleventh registers store the SN value. For example, SN:181101194228B027, the corresponding register value is as shown in the table below. 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 Base station positioning value LBS reading

The starting address for reading the base station location register is 40193 (0x00C0), and the total length of the register is 20. The first register is the length of the base station location information, and the second to twentieth registers store the base station location value. For example, the base station positioning value LAC: 812F, CID: 8056B08, the corresponding register value is as follows. 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 right of final interpretation and modification of all contents in this manual.

Due to the continuous improvement of the hardware and software of the product, this manual may be changed without prior notice, and the latest version of the manual shall prevail. Everyone is responsible for protecting the environment: In order to reduce the use of paper, this manual only prints the Chinese part, and the English manual only provides electronic documents. If necessary, please come to our company

In addition, if it is not a special request of the user, when the user orders in bulk, we only provide the product manual according to a certain proportion of the order quantity, not every digital radio is equipped with one by one, please understand.

Revision history

Version	Date	Description	Issued by
1.0	-	Initial version	-
1.1	2019/8/14	Format revision	lyl
1.2	2022/4/13	Mmodbus address bug fix (register address 0x54 was corrected and replaced with 0x53)	龚路

About us

Technical support: support@cdebyte.com

Documents and RF Setting download link: www.ebyte.com

Thank you for using Ebyte products! Please contact us with any questions or suggestions: info@cdebyte.com

Official hotline: 028-61399028 ext. 821

Web: www.ebyte.com

Address: Innovation Center D347, 4# XI-XIN Road, Chengdu, Sichuan, China



Chengdu Ebyte Electronic Technology Co.,Ltd.