Chengdu Ebyte Electronic Technology Co.,Ltd

Wireless Modem

User Manual

All rights to interpret and modify this manual belong to
Chengdu Ebyte Electronic Technology Co., Ltd.

Contents

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

E851-RTU(4440-ETH) Features

- Support 4 differential analog inputs, default current detection;
- Support 4 digital inputs, default dry contact;
- Support 4 relay outputs;
- Support socket connection to remote server, support TCP Client;
- Using Modbus TCP/RTU protocol data processing;
- Support connection to Ebyte cloud, command control;
- Support 2 working modes, host mode and slave mode, the slave can cascade multiple devices through RS485;
- Support Reload touch button, long press for 5s, Modbus device address, RS485 serial port baud rate and parity digit restore factory settings;
- Hardware watchdog with high reliability;
- Multiple indicator lights show working status;
- The power supply has good over-current, over-voltage, anti-reverse and other functions.

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

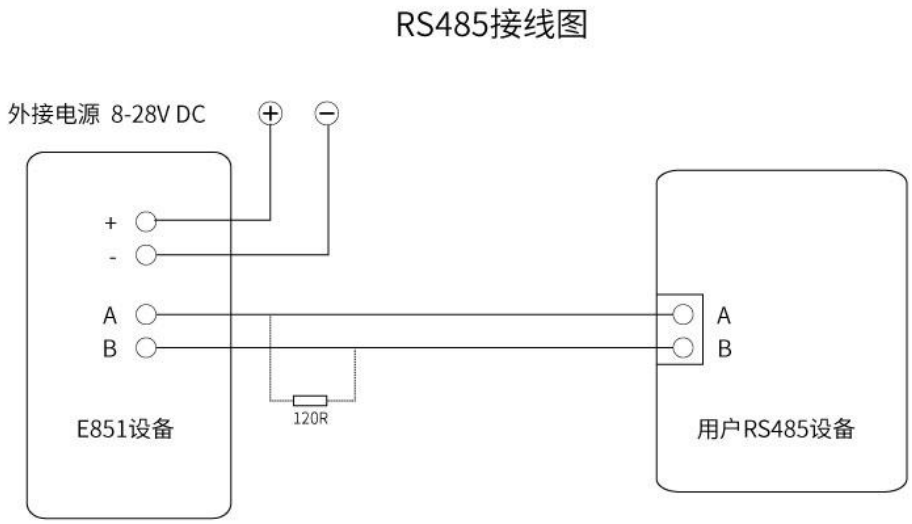
Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

1 Quick Start

This chapter is a quick introduction to the E851-RTU (4440-ETH) series products. It is recommended that users systematically read this chapter and follow the instructions to have a systematic understanding of the module products. Users can also choose what you are interested in according to their needs. chapters to read. For specific details and instructions, refer to subsequent chapters.

1.1 port connection

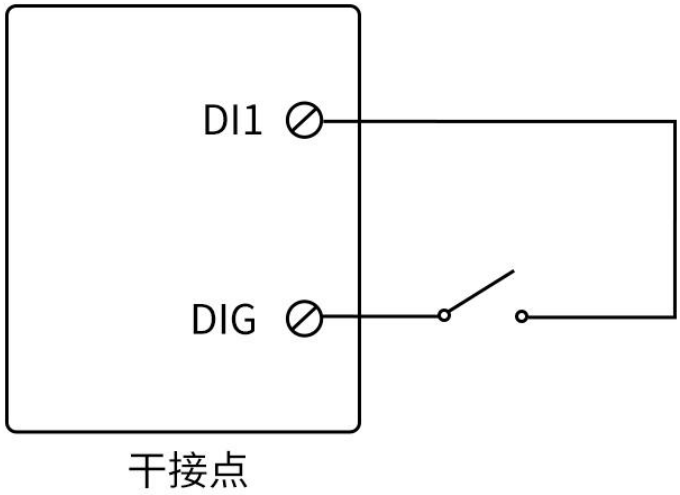
1.1.1 RS485 connection



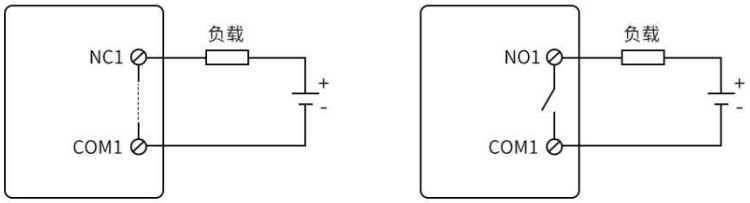
Note: When the 485 bus high-frequency signal is transmitted, the signal wavelength is shorter than the transmission line, and the signal will form a reflected wave at the end of the transmission line, which will interfere with the original signal. Therefore, it is necessary to add a terminal resistor at the end of the transmission line so that the signal does not reflect after reaching the end of the transmission line. The terminal resistance should be the same as the impedance of the communication cable, the typical value is 120 ohms. Its function is to match the bus impedance and improve the anti-interference and reliability of data communication.

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

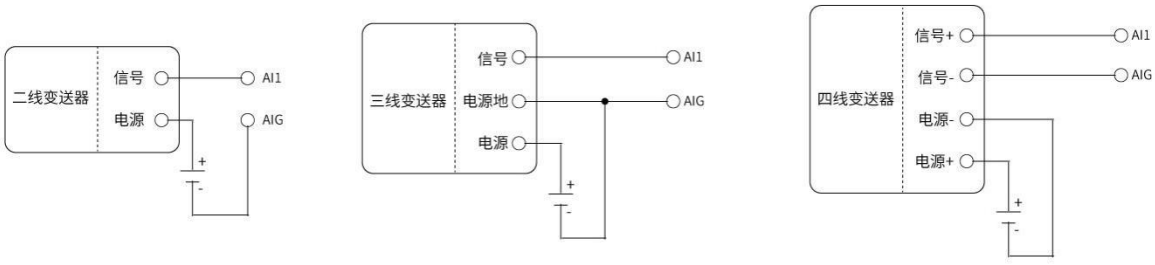
1.1.2 Digital input connection



1.1.3 Relay output connection



1.1.4 Differential Analog Input Connections



模拟量输入连接

1.2 Quck Use

Wiring: Computer connects to E851-RTU (4440-ETH) via USB to RS485

Networking: the network cable is inserted into the RJ45 port

Power supply: E851-RTU (4440-ETH) working voltage is DC 8~28V

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

1.2.1 RS485 bus control

Select the corresponding port and click Search to search for devices.

After the device is found, click Stop .

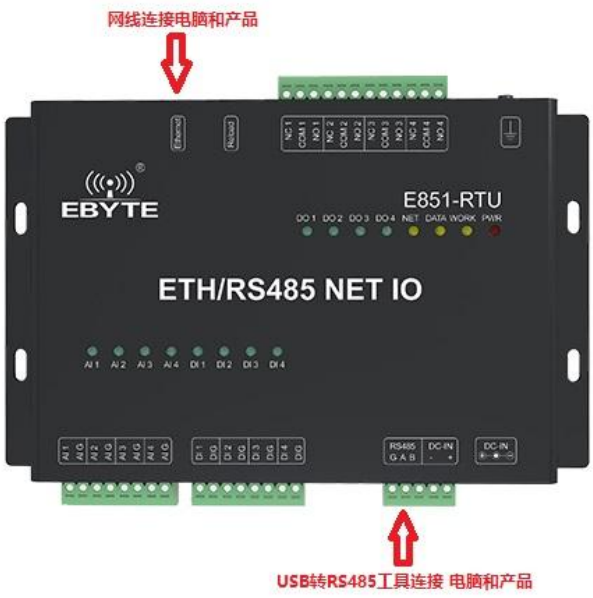
At this time, you can see the device address of the current device, and for the "automatic refresh" √ process, you can perform switch output control, switch input reading, and differential analog input reading .

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

1.2.2 Network acquisition control (static IP connection directly controls the product)

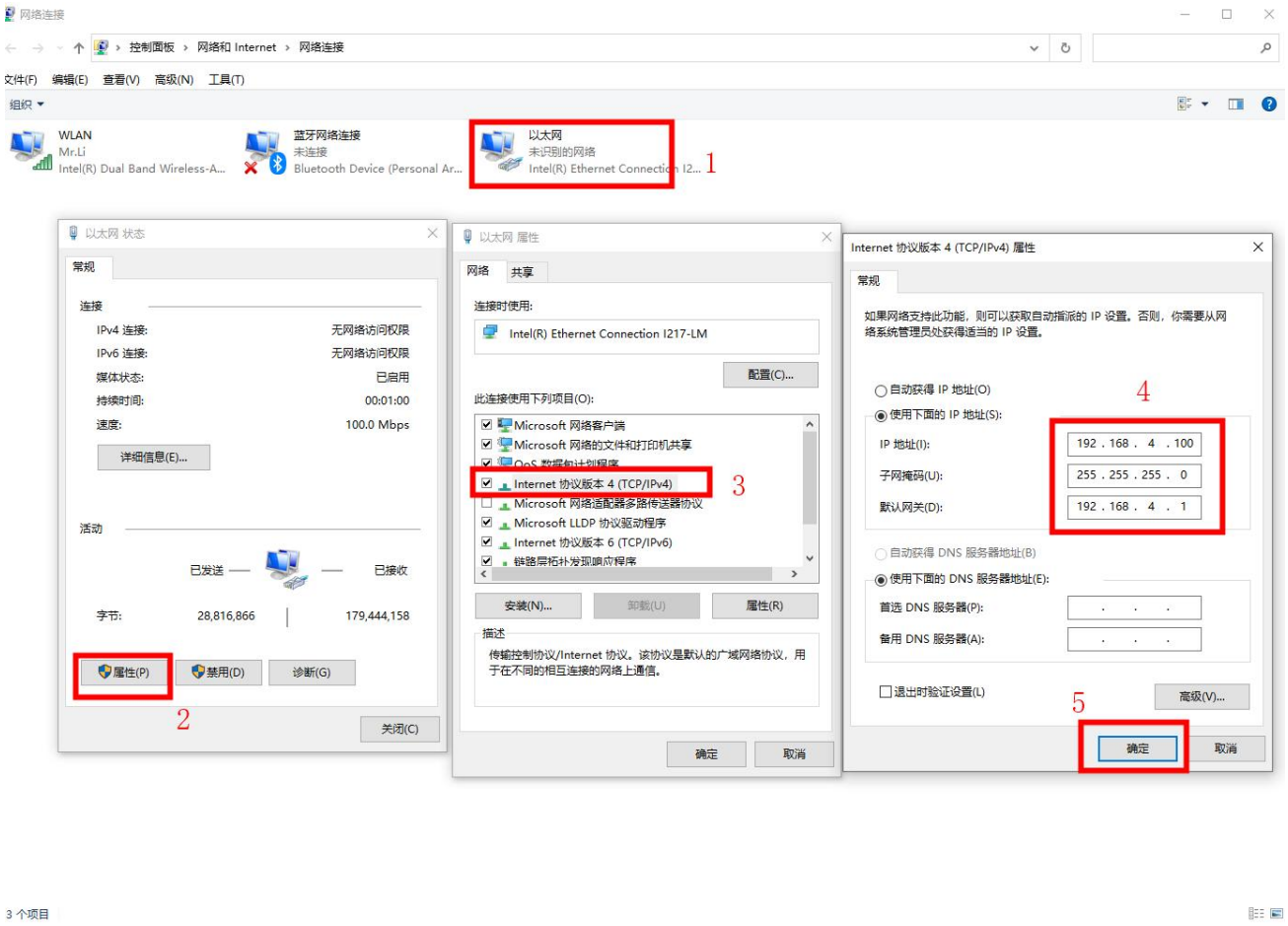
Step preview: network control hardware connection - PC computer settings - product connection parameter setting - use network debugging tools to connect products - send control/acquisition instructions

(1) Network acquisition control hardware connection: use a network cable to directly connect the computer network port to this product, and use a USB to RS485 tool to connect the computer USB to the product RS485.



Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

(2) PC-side computer settings: set the computer to a static IP, the steps are as shown in the figure below.

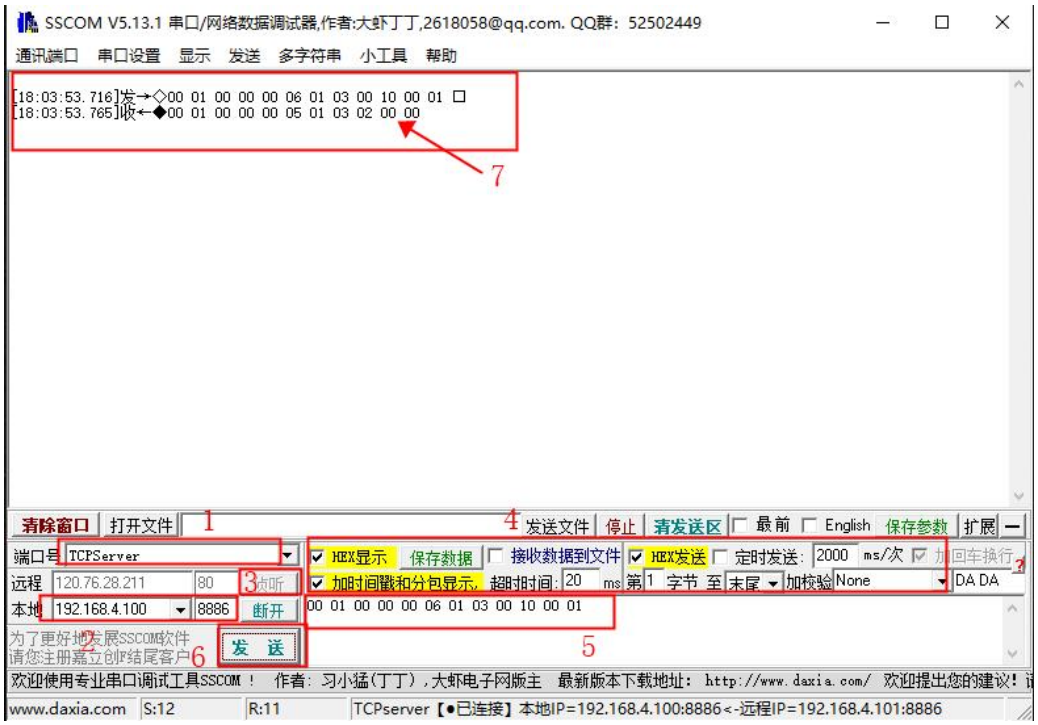


（3）Product connection parameter setting: as shown in the figure below (default factory setting).

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

（4）Connect to the product with a network debugging tool: here we take the sscom .exe debugging tool as an example.

1 Open a TCPServer service——2 Output the server IP connected to the product: 192.168.4.101 and service port 8886——3 Click Listen (that is, connect to the product, if the word "Listen" cannot be grayed out, please check the above Parameter setting and hardware connection) - 4 Set data sending rules - 5 Edit product instructions (the picture shows reading the AI1 channel acquisition value, see " Chapter 4 Product Functions " for more instructions) - 6 Click "Send" ——7 Return message received——successful.



（5）See " 4.1 Working Mode " for more connection methods.

2 Product Introduction

E851-RTU (4440-ETH) is a network IO product that supports 4 digital inputs (default dry contact), 4 differential analog inputs, and 4 relay outputs. Support Modbus TCP/RTU protocol. The product is highly usable, and users can easily and quickly integrate it into their own systems to realize Ethernet-based remote control.

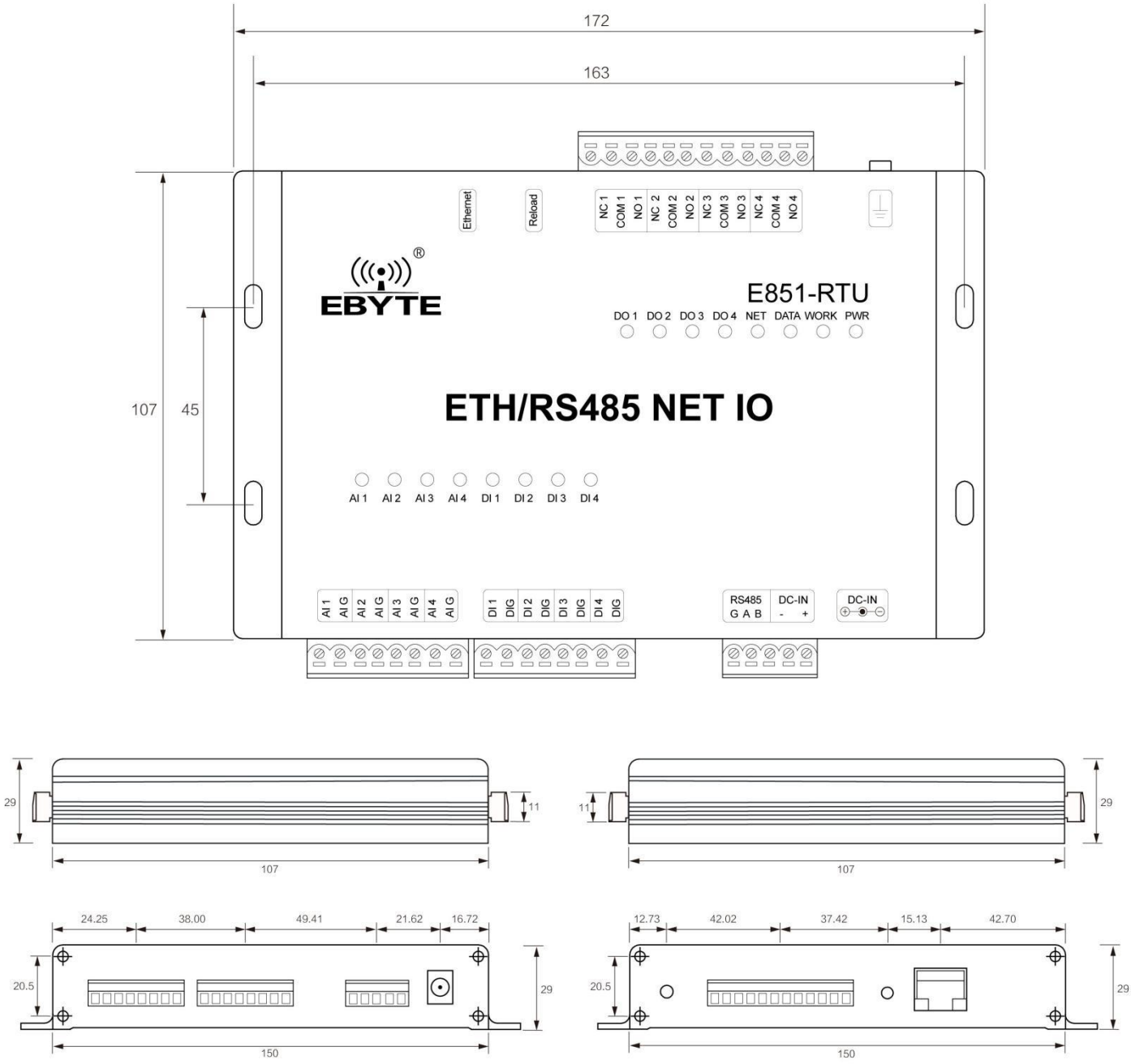
2.1 Basic parameters

	project	index
hardware parameters	Product size (H*W*D)	172*107*29mm
	product weight	457.5± 5g
	Operating temperature	-20℃~+70℃
	storage temperature	-40℃~+85℃
	Working humidity	5%~95%
	storage humidity	1%~95%
	Operating Voltage	8V~28V

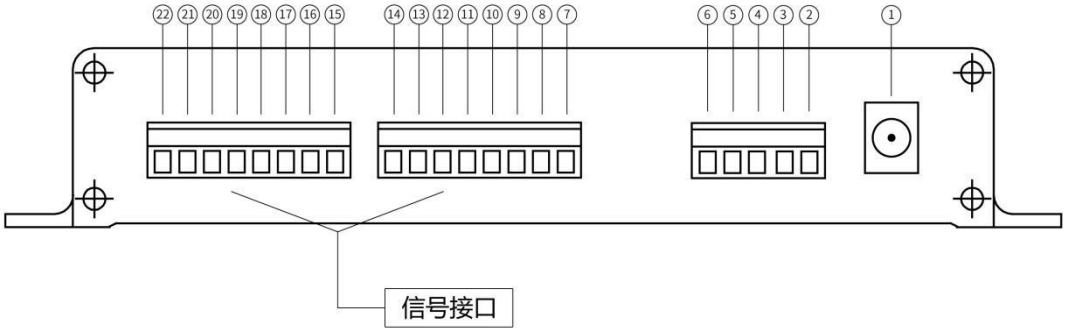
Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

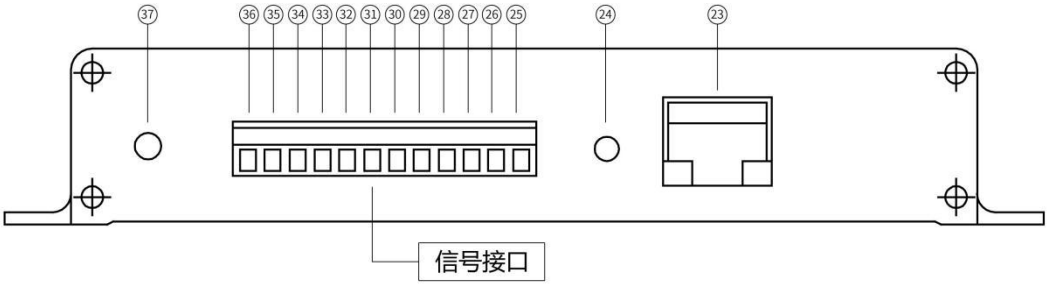
	Current acquisition range	0mA~20mA
	precision	0.2%
	Data interface	RS485: 1200~115200bps
software parameters	Network Type	ethernet
	configuration command	Modbus TCP/RTU
	Network protocol	Modbus TCP/RTU
	Operating mode	Master mode, slave mode
	data transfer method	TCP Client

2.2 Dimensions, interface description



Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.





serial number	Port and other definitions	Features	illustrate
1	DC-IN seat	DC socket 5.5*2.1mm	Power input terminal, DC 8V~28V, 12V/24V is recommended, and it cannot be powered at the same time as the crimping terminal
2	DC-IN+	Pressure wire type power input positive pole	Power input, DC 8V~28V, it is recommended that 12V/24V cannot be powered simultaneously with the DC socket
3	DC-IN -	Negative pole of crimping power input	power reference ground
4	RS485B	RS485 interface B	RS485 interface B is connected to device B interface
5	RS485A	RS485 interface A	RS485 port A is connected to device A port
6	RS485G	signal reference ground	Signal reference ground, may not be connected
7	DIG	switch input ground	Can be paired with DI 4
8	DI 4	Digital input channel 4	Form dry contact with DIG
9	DIG	switch input ground	Pair with DI 3
10	DI 3	Digital input channel 3	Form dry contact with DIG
11	DIG	switch input ground	Can be paired with DI 2
12	DI 2	Digital input channel 2	Form dry contact with DIG
13	DIG	switch input ground	Can be used as a pair with DI 1
14	DI 1	Digital input channel 1	Form dry contact with DIG
15	AIG	Differential analog input ground	Can be paired with AI 4
16	AI 4	Differential analog input channel 4	Differential analog input pin, forms input with AIG
17	AIG	Differential analog input	Can be paired with AI 3

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

		ground	
18	AI 3	Differential analog input channel 3	Differential analog input pin, forms input with AIG
19	AIG	Differential analog input ground	Can be paired with AI 2
20	AI 2	Differential analog input channel 2	Differential analog input pin, forms input with AIG
twenty one	AIG	Differential analog input ground	Can be paired with AI 1
twenty two	AI 1	Differential analog input channel 1	Differential analog input pin, forms input with AIG
twenty three	Ethernet	Network port	Ethernet port
twenty four	Reload	reset button	Long press 5s to work
25	NC 1	Relay 1 normally closed pin	Used in conjunction with relay 1 common
26	COM 1	Relay 1 common terminal	Works with Relay 1 normally open pin/normally closed pin
27	NO 1	Relay 1 normally open pin	Used in conjunction with relay 1 common
28	NC 2	Relay 2 normally closed pin	Use with Relay 2 Common
29	COM 2	Relay 2 common terminal	Works with Relay 2 normally open pin/normally closed pin
30	NO 2	Relay 2 normally open pin	Use with Relay 2 Common
31	NC 3	Relay 3 normally closed pin	Used in conjunction with relay 3 common
32	COM 3	Relay 3 common terminal	Works with Relay 3 normally open pin/normally closed pin
33	no 3	Relay 3 normally open pin	Used in conjunction with relay 3 common
34	NC 4	Relay 4 normally closed pin	Use with relay 4 common
35	COM 4	Relay 4 common terminal	Works with Relay 4 normally open pin/normally closed pin
36	no 4	Relay 4 normally open pin	Use with relay 4 common
37	ground screw	connected to the earth	connected to the earth
led light			
AI 1	Differential analog input channel 1 indication	Green LED, lights up for sufficiently large input (≥0.5mA)	
AI 2	Differential analog input channel 2 indication	Green LED, lights up for sufficiently large input (≥0.5mA)	
AI 3	Differential analog input channel 3 indication	Green LED, lights up for sufficiently large input (≥0.5mA)	
AI 4	Differential analog input channel 4 indication	Green LED, lights up for sufficiently large input (≥0.5mA)	

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

DI 1	Digital input channel 1 indication	Green LED, DI 1, DIG short circuit lights up
DI 2	Digital input channel 2 indication	Green LED, DI 2, DIG short circuit lights up
DI 3	Digital input channel 3 indication	Green LED, DI 3, DIG short circuit lights up
DI 4	Digital input channel 4 indication	Green LED, DI 4, DIG shorted on
DO 1	Relay 1 output indication	Green LED, NO 1, COM 1 closed light up
DO 2	Relay 2 output indication	Green LED, NO 2, COM 2 closed light up
DO 3	Relay 3 output indication	Green LED, NO 3, COM 3 closed light up
DO 4	Relay 4 output indication	Green LED, NO 4, COM 4 closed light up
NET	network instructions	Yellow LED, always on after connecting to the network
DATA	Serial port data indication	Yellow LED, lights up when the RS485 interface has data transmission (expressed as flashing)
WORK	Work/reset indication	Yellow LED, flashes regularly/flashes quickly after successful reset
PWR	Power indicator	Red LED, always on

Notice:

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

2.3 Description of Reload touch button

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

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

3 Modbus

3.1 Modbus address table

Register address table (function code: 0x01H, 0x05H, 0x0FH, 0x03H, 0x06H, 0x10H)					
register address	number of registers	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		
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		
reserve					
30017 (0x0010)	1	AI1 input value, unit (uA)	read only	0-20000	0x03 0x04
30018 (0x0011)	1	AI2 input value, unit (uA)	read only		
30019 (0x0012)	1	AI3 input value, unit (uA)	read only		
30020 (0x0013)	1	AI4 input value, unit (uA)	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	
reserve					
40065 (0x0040)	1	DI1-DI4 pulse count reset	just write	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	Switching value automatic reporting	read/write	0 - 2	
40083 (0x0052)	1	Switching output time setting (milliseconds)	read/write	300-65535	
40084(0x0053)	1	Analog range setting	read/write	0 - 1	
40085 (0x0054)	1	Switch value restart output state setting	read/write	0x00 - 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	

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

40124(0x007B)	twenty two	custom registration package	read/write	--	
40146(0x0091)	1	Registry 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	Heartbeat mode	read/write	0 - 1	
40171 (0x00AA)	1	cloud transmission	read/write	0-1	
40172 (0x00AB)	3	keep alive connection	read/write	0, 2-7200	
40173 (0x00AE)	1	Ethernet timeout restart	read/write	0,60-65535	
40174 (0x00AF)	1	clear cache	read/write	0 - 1	
40175 (0x00B0)	1	local port number	read/write	0-65535	
40176 (0x00B1)	1	IP acquisition method	read/write	0-1	
40177 (0x00B2)	11	local IP address	read/write	--	
40188 (0x00BD)	11	subnet mask	read/write	--	
40199 (0x00C8)	11	gateway	read/write	--	
40210 (0x00D3)	11	Preferred DNS	read/write	--	
40221 (0x00DE)	11	Alternate DNS	read/write	--	
40232 (0x00E9)	11	MAC value	read only	--	0x03
40243 (0x00F4)	11	SN code value	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 value table

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

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

3.4 RS485 serial port parity code value table

check digit code value table	
0 (default)	no parity
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.

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

4 Product Functions

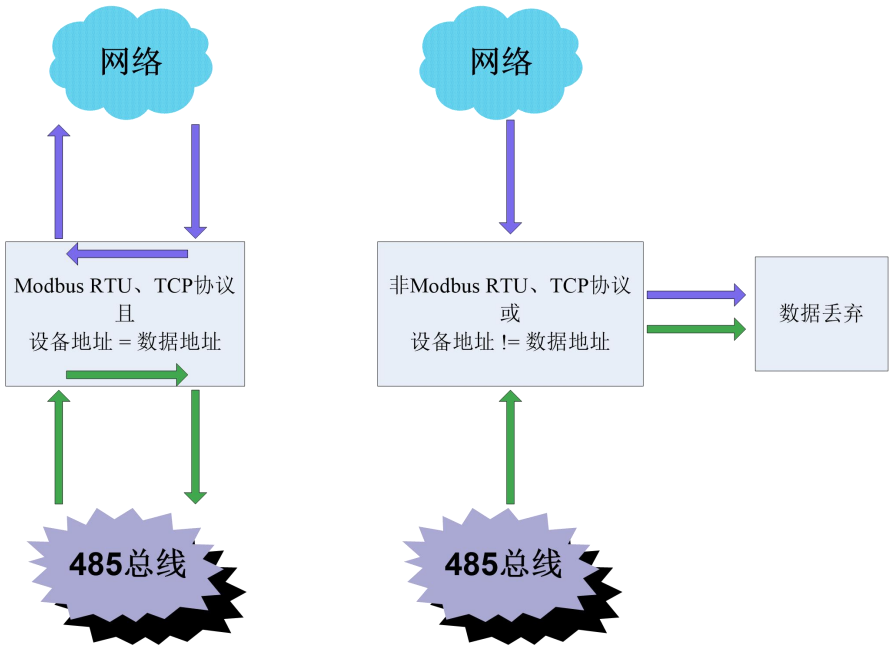
4.1 Working mode

The working mode is divided into master mode and slave mode, 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 the slave mode (register value is 0x01), the data sent by the network end or the 485 bus end (transmitter) 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 with the same protocol to send If the data sent by the network end or 485 bus end to the device does not meet the Modbus RTU, Modbus TCP protocol, or meets the Modbus RTU, Modbus TCP protocol 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 master.



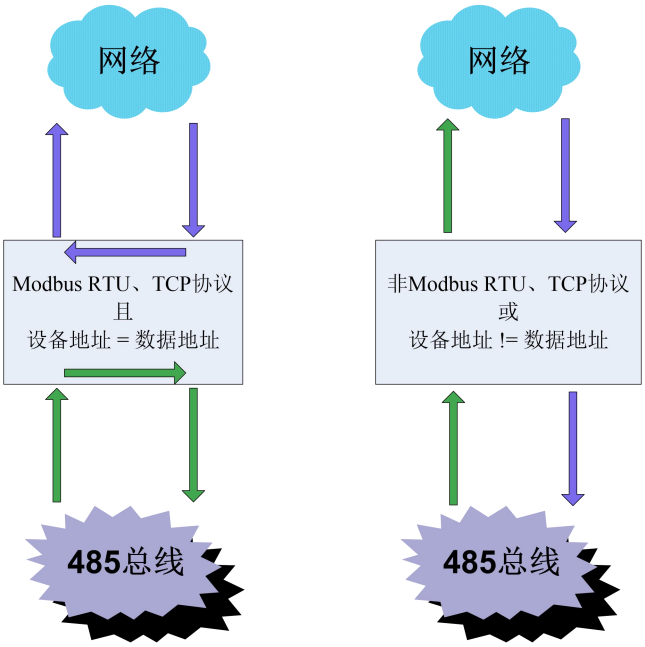
4.1.2 Host Mode

In the host mode (the register value is 0x00), the data sent by the network terminal or the 485 bus terminal (transmitter) 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 end or the 485 bus end to the device does not meet the Modbus RTU, Modbus TCP protocol, or meets the Modbus RTU, Modbus TCP protocol but the data address is not the device address,

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

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 IO basic functions

4.2.1 Digital DO output

4.2.1.1 Read switch DO output

Function code: 01, read coil status

Address range: 00017(0x0010)~00020(0x0013)

Explanation: When the device relay is passive output, when the coil is not powered, the NC port and COM port of the relay are normally closed, and the NO port and COM port are normally open, and the value is 0; when the coil is powered on, the phenomenon is opposite, and the relay NC port and COM port are disconnected. Open, the NO port and the COM port are closed, and the value is 1. Query the status of the relay through the command.

example:

Read the 4-way switching output status, assuming the return value is 03, corresponding to the binary digits 0000 0011, the lower four bits represent the switching output status, which are DO4, DO3, DO2, DO1 in sequence.

Modbus RTU protocol to read switch output:

send	01	01	00 10	00 04	3C 0C
	Device ModBus address	function code	switch start address	Read switch quantity	CRC check code

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

take over	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 switch output:

send	00 01	00 00	00 06	01	01	00 10	00 04
	Transmission ID	Protocol ID	length	Unit ID	function code	switch start address	Read switch quantity

take over	00 01	00 00	00 04	01	01	01	03
	Transmission ID	Protocol ID	length	Unit ID	function code	returns the number of bytes	Switch output value

4.2.1.2 Control switch DO output

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

Address range: 00017(0x0010)~00020(0x0013)

Explanation: The device relay is passively output, the coil is not powered, the NC port of the relay is closed to the COM port, and the NO port is disconnected from the COM port; the coil is powered on, the NC port of the relay is disconnected from the COM port, and the NO port is closed to the COM port. The state of the relay is controlled by commands.

example:

Function code 0x05 writes DO2 switching 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 write switch output:

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

take over	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
	Transmission ID	Protocol ID	length	Unit ID	function code	switch address	write value

take over	00 01	00 00	00 06	01	05	00 11	FF 00
	Transmission ID	Protocol ID	length	Unit ID	function code	switch address	write value

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

Modbus RTU protocol write switch output:

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

send	01	0F	00 11	00 02	01	03	62 95
	Device ModBus address	function code	switch address	Write switch quantity	Bytes	write value	CRC check code

take over	01	0F	00 11	00 02	84 0F
	Device 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
	Transmission ID	Protocol ID	length	Unit ID	function code	switch address	Write switch quantity	Bytes	write value

take over	00 01	00 00	00 06	01	0F	00 11	00 02
	Transmission ID	Protocol ID	length	Unit ID	function code	switch address	Write switch quantity

4.2.2 Read digital DI input

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

Address range: 10017(0x0010)~10020(0x0013)

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:

To read the 4-way switch input value, the DI input terminals DI1 and COM1 are short-circuited, DI2 and COM2 are not short-circuited, DI3 and COM3 are short-circuited, and DI4 and COM4 are not short-circuited. The read digital input value is 0x05, corresponding to the binary bit 0000 0101, and the lower four bits represent the digital input value, which are DI4, DI3, DI2, and DI1 in turn.

Modbus RTU protocol to read digital input:

send	01	02	00 10	00 04	78 0C
	Device ModBus address	function code	switch start address	Read switch quantity	CRC check code

take over	01	02	01	05	61 8B
	Device ModBus address	function code	returns the number of bytes	Switch value input value	CRC check code

Modbus TCP protocol to read digital input:

send	00 01	00 00	00 06	01	02	00 10	00 04
	Transmission ID	Protocol ID	length	Unit ID	function code	switch start address	Read switch quantity

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

take over	00 01	00 00	00 04	01	02	01	05
	Transmission ID	Protocol ID	length	Unit ID	function code	returns the number of bytes	Switch value input value

4.2.3 Read analog AI input

Function code: 03, read holding register; 04, read input register

Address range: 30017(0x0010)~30020(0x0013)

Note: The unit of differential analog input value is uA

example:

Function code 0x03, read AI1 input, assuming AI1 input is 9946uA, the corresponding value should be 0x0x26DA

Modbus RTU protocol to read differential analog inputs:

send	01	03	00 10	00 01	85 CF
	Device ModBus address	function code	Analog starting address	Number of reads	CRC check code

take over	01	03	02	26DA	23 BF
	Device ModBus address	function code	returns the number of bytes	Differential analog input value	CRC check code

Modbus TCP protocol to read differential analog input:

send	00 01	00 00	00 06	01	03	00 10	00 01
	Transmission ID	Protocol ID	length	Unit ID	function code	Analog starting address	Number of reads

take over	00 01	00 00	00 05	01	03	02	26DA
	Transmission ID	Protocol ID	length	Unit ID	function code	returns the number of bytes	Differential analog input value

Function code 0x04, read AI1 input, assuming AI1 input is 9946uA, the corresponding value should be 0x0x26DA

Modbus RTU protocol to read differential analog inputs:

send	01	04	00 10	00 01	30 0F
	Device ModBus address	function code	Analog starting address	Number of reads	CRC check code

take over	01	04	02	26DA	22 CB
	Device ModBus address	function code	returns the number of bytes	Differential analog input value	CRC check code

Modbus TCP protocol to read differential analog input:

send	00 01	00 00	00 06	01	04	00 10	00 01
	Transmission ID	Protocol ID	length	Unit ID	function code	Analog starting address	Number of reads

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

take over	00 01	00 00	00 05	01	04	02	26DA
	Transmission ID	Protocol ID	length	Unit ID	function code	returns the number of bytes	Differential analog input value

4.2.4 Analog AI range setting

When the register 0x40084 (0x0053) value is 0, the differential analog input range is 0 -- 20mA;
When the register 0x40084 (0x0053) value is 1, the differential analog input range is 4 -- 20mA;

4.3 IO Features

4.3.1 Pulse count and count reset

The pulse count will not be saved after power off, and the pulse level maintenance time must be greater than 10ms to be valid. The switch value 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.

4.3.1.1 Read pulse count value

Function code: 03, read holding register
Address range: 40049 (0x0030)~40052 (0x0033)
Description: The maximum value of pulse count is 65535
example:
DI1 has currently detected 16 pulses, DI2 has currently detected 3 pulses, read the count values of DI1 and DI2 digital inputs,
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

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 check code

Modbus TCP protocol read pulse count value:

send	00 01	00 00	00 06	01	03	00 30	00 02
	Transmission ID	Protocol ID	length	Unit ID	function code	initial address	Number of reads

take over	00 01	00 00	00 07	01	03	04	00 10	00 03
	Transmission ID	Protocol ID	length	Unit ID	function code	returns the number of bytes	DI1 count value	DI2 count value

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

4.3.1.2 Clear pulse count value

Function code: 06, write holding register

Address range: 40065 (0x0040)

Explanation: The lower four bits of the register value represent the counting of DI4, DI3, DI2, and DI1 respectively. Writing "1" means that the counting is cleared, and the pulse counting is restarted.

example:

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

Modbus RTU protocol clear pulse count value :

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

take over	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
	Transmission ID	Protocol ID	length	Unit ID	function code	address	write value

take over	00 01	00 00	00 06	01	06	00 40	00 0a
	Transmissio n ID	Protocol ID	length	Unit ID	function code	address	write value

4.3.2 Automatic reporting of digital input DI

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

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

Turn off the switch value automatic reporting function

The switching value is automatically reported and transmitted through RS485

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

The upload protocol for switching value changes is listed in the table below, where the frame headers 0xAA and 0xBB are fixed, and the value ranges of DI1, DI2, DI3, and DI4 are 0x00, 0x01, and 0xFF.

0x00 means that 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, and DI4 in the table represent that the state of DI1 and DI2 is updated to be open, the state of DI3 is updated to be closed, and the state of DI4 has not changed. The last two bytes are modbus CRC16 calculation value.

frame header	DI1	DI2	DI3	DI4	Modbus CRC
0xAA 0xBB	0x00	0x00	0x01	0xff	0xBD 0xDA

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

4.3.3 Time setting of digital output DO

Switching value pulse output time setting is to set the switching value output time (relay NO, COM closing time), the corresponding Modbus register is 40083 (0x0052), the value range is 300-65535ms, if the value is lower than 300ms, the default switching value output Closed is the holding state, that is, the switching value output is kept after it is closed. If it is set to 300ms and above, such as 500ms, after sending the switching value output closing command, the switching value will be closed for 500ms, and then it will be automatically disconnected after 500ms.

4.3.4 Digital DO restart output state setting

Whether the device is powered off and restarted to maintain the state before power failure or restart to maintain a specific output state setting, 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 0x00-0x10. When the value of this register is 0x10, the last switching output state will be maintained after power off and restarting; when the value of this register is 0x00-0x0F, the lower four bits determine the switching output state of the device restart, bit4 corresponds to DO4, and bit3 corresponds to DO3, bit2 corresponds to DO2, and bit1 corresponds to DO1. For example, when power is turned on, DO4 and DO2 are closed (relay NO and COM are closed) DO3 and DO1 are disconnected (relay NO and COM are disconnected), and the corresponding register value is 0000 1010, namely 0xa0, "1" is closed state, "0" is 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 saved 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, the IP is 116.62.42.192, the port is 31687, a total of 13 characters, 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 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, the unused IP or domain name registers can be filled with "0" or not. If you need to use the function code "0x10" to write the IP, domain name, and port at one time , protocol type, then the unused registers must be filled with values in order 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 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

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

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

or domain name needs to be considered when writing the IP register, that is, how many registers need to be occupied. If the above IP is written 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 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 00 00 00 00 C 7 00 0	7B F0
	Device ModBus address	function code	address	register length	Bytes	write value	CRC check code

take over	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 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 00 00 00 00 C 7 00 0
	Transmission ID	Protocol ID	length	Unit ID	function code	address	register length	Bytes	write value

take over	00 01	00 00	00 06	01	10	00 63	00 18
	Transmission 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 type of the registration package. 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 Register the package value 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, corresponding to 0x0A in hexadecimal. Like IP registers, unused register packet value registers can be filled with "0" or not filled.

40124(0x007B)	40125(0x007C)	40126(0x007D) -- 40145(0x0090)	40146(0x0091)
Types of	length	Registry package value	Registry 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 01

The registration package mechanism has 5 modes:

Register package mechanism	Corresponding function description

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

register value (0x0091)	
00 00	Close the registration package mechanism
00 01	Add MAC/IMEI as registration packet data before the data sent to the server in each packet
00 02	Add custom registration package data before the data sent to the server in each package
00 03	Send a MAC/IMEI registration packet only 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 register package 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 01	00 F4
	Device ModBus address	function code	address	register length	Bytes	write value	CRC check code

take over	01	10	00 7B	00 17	F0 1E
	Device ModBus address	function code	address	register length	CRC check code

Modbus TCP protocol write register package 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 01
	Transmission ID	Protocol ID	length	Unit ID	function code	address	register length	Bytes	write value

take over	00 01	00 00	00 06	01	10	00 7B	00 17
	Transmission 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 that the heartbeat packet is in hex format, and the value 0x0001 means 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 length of the heartbeat packet value is 10, corresponding to decimal 0x0A. Like the custom registration package register, the unused heartbeat package value register can be filled with "0" or not filled.

40147(0x0092)	40148(0x0093)	40149(0x0094) -- 40168(0x00A7)

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

Types of	length	Registry package value
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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Modbus RTU protocol write register package register:

send	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	52 9E
	Device ModBus address	function code	address	register length	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 check code

Modbus TCP protocol write register package 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	Transmission ID	Protocol ID	length	Unit ID	function code	address	register length	Bytes	write value

take over	00 01	00 00	00 06	01	10	00 92	00 16
	Transmission ID	Protocol ID	length	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 ModBus address	function code	address	write value	CRC check code

take over	01	06	00 A8	00 05	C8 29
	Device ModBus address	function code	address	write value	CRC check code

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	Protocol	length	Unit ID	function	address	write value

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

	ID	ID			code		

take over	00 01	00 00	00 06	01	06	00 A8	00 05
	Transmissio n ID	Protocol ID	length	Unit ID	function code	address	write value

4.4.5 Heartbeat packet mode

The heartbeat packet mode is divided into serial port heartbeat packet and network heartbeat packet (the default is network heartbeat packet). When writing 0 to this register, it is a network heartbeat packet, and when writing 1, it is a serial port heartbeat packet.

Modbus RTU protocol write heartbeat packet mode register:

send	01	06	00 A9	00 01	98 2A
	Device ModBus address	function code	address	write value	CRC check code

take over	01	06	00 A9	00 01	98 2A
	Device ModBus address	function code	address	write value	CRC check code

Modbus TCP protocol write heartbeat packet mode register:

send	00 01	00 00	00 06	01	06	00 A9	00 00
	Transmission ID	Protocol ID	length	Unit ID	function code	address	write value

take over	00 01	00 00	00 06	01	06	00 A9	00 00
	Transmissio n ID	Protocol ID	length	Unit ID	function code	address	write value

4.4.6 Local WAN port IP parameter setting

Local IP acquisition methods are divided into static IP acquisition and dynamic IP acquisition (DHCP), and the related registers are 34 registers from 0XB1 to 0XD2. When the value in the first register (0XB1) is 1, it is the static IP mode, and when it is 0, it is the dynamic acquisition mode. A total of 11 registers from 0XB2 to 0XBC store the local ip address, among which 0XB2 stores the length of the ip address, and 0XB3 to 0XBC store the ASCII code value of the IP address. A total of 11 registers from 0XBD to 0XC7 store the subnet mask information, among which 0XBD stores the length of the subnet mask address, and 0XBE to 0XC7 store the ASCII code value of the subnet mask address. A total of 11 registers from 0XC8 to 0XD2 store the gateway address, among which 0XC8 stores the length of the gateway address, and 0XC9 to 0XD2 store the ASCII code value of the gateway address.

You can use the 10 function code to write in one time and appeal the parameter information. Note that it is the same as the server IP setting, and the unfilled registers are filled with 0. The following command indicates that it is set to static IP, the local IP address is 192.168.4.101, the subnet mask is 255.255.255.0, and the gateway is 192.168.4.1. Note that the corresponding ASCII code value should be written when writing, and the Convert to hexadecimal.

Modbus RTU protocol configuration WAN port parameters :

send	01	10	00 B1	00 22	44	00 01 00 0D 31 39 32 2E 31 36 38 2E 34 2E 31 30 31 00 00 00 00 00 00 00 00 0D 32 35 35 2E 32 35 35 2E 32 35 35 2E 30 00 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36	31 16

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

						38 2E 34 2E 31 00 00 00 00 00 00 00 00	
	Device ModBus address	function code	address	register length	Bytes	write value	CRC check code

take over	01	10	00 B1	00 22	10 37
	Device ModBus address	function code	address	register length	CRC check code

Modbus TCP protocol writes WAN port parameters:

send	00 01	00 00	00 4B	01	10	00 B1	00 22	44	00 01 00 0D 31 39 32 2E 31 36 38 2E 34 2E 31 30 31 00 00 00 00 00 00 00 00 0D 32 35 35 2E 32 35 35 2E 32 35 35 2E 30 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36 38 2E 34 2E 31 00 00 00 00 00 00 00 00 00 00
	Transmission ID	Protocol ID	length	Unit ID	function code	address	register length	Bytes	write value

take over	00 01	00 00	00 06	01	10	00 B1	00 22
	Transmission ID	Protocol ID	length	Unit ID	function code	address	register length

4.4.7 DNS settings

There are 22 registers starting from 0XD3 to 0XDE, which store DNS information. DNS addresses are divided into preferred DNS and standby DNS. Register 0xD3 stores the address length of the preferred DNS, and registers 0xD4 to 0xDD store the ASCII code value of the preferred DNS address. Register 0XDE stores the length of the standby DNS address, and 0XDE to 0XE8 store the ASCII code value of the standby DNS address.

You can use the 10 function code to configure the preferred DNS and standby DNS at one time. The following table shows that the preferred and standby DNS are 61.139.2.69 and 192.168.4.1 respectively.

Modbus RTU protocol configuration preferred and alternate DNS :

send	01	10	00 D3	00 16	2C	00 0B 36 31 2E 31 33 39 2E 32 2E 36 39 00 00 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36 38 2E 34 2E 31 00 00 00 00 00 00 00 000	D9 F2
	Device ModBus address	function code	address	register length	Bytes	write value	CRC check code

take over	01	10	00 D3	00 16	B0 3E
	Device ModBus address	function code	address	register length	CRC check code

Modbus TCP protocol configuration preferred and alternate DNS :

send	00 01	00 00	00 33	01	10	00 D3	00 16	2C	00 0B 36 31 2E 31 33 39 2E 32 2E 36 39 00 00 00 00 00 00 00 00 00 0B 31 39 32 2E 31 36 38 2E

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

									34 2E 31 00 00 00 00 00 00 000
	Transmission ID	Protocol ID	length	Unit ID	function code	address	register length	Bytes	write value

take over	00 01	00 00	00 06	01	10	00 D3	00 16
	Transmission ID	Protocol ID	length	Unit ID	function code	address	register length

4.4.8 Ebyte cloud transparent transmission

Ebyte cloud transparent transmission function can be turned on or off. The design register corresponding to this function is 40169 (0x00AA), and supports 0x0003, 0x0006, 0x0010 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;

The factory default is to close the cloud transparent transmission state.

4.4.9 Clear cache

Register 0xAF can set whether to clear the cache in the network SOKET, support 0x0003, 0x0006, 0x0010 function codes:

When the value of this register is 0x0000, the clear cache function is enabled;

When the value of this register is 0x0001, the function of clearing the cache is disabled;

4.4.10 Keep Alive Connection

Register 40170 (0x00AB) is the keep-alive connection register, which needs to be used with 40171 (0x00AC) and 40172 (0x00AD).

The 40170 (0x00AB) register indicates the number of seconds after the TCP connection has no data message transmission to start the detection message. When the value of this register is 0, it means that this function is turned off. When it is 2~7200, it means that this function is turned on, and the latter two registers will take effect parameters.

The 40171 (0x00AC) register indicates the time interval between the previous detection message and the next detection message, and its value is 2~7200, in seconds

40172 (0x00AD) register indicates the maximum detection failure times, when sniffing this number, the TCP connection will be disconnected, its value is 2~255, unit: times

4.4.11 Timeout restart

This register 40173 (0x00AE) is used to set how long the Ethernet physical layer module in the RTU restarts after there is no data in the network. The range is 0, 60-65535 seconds. When it is set to 0, it means that this function is turned off. Set to When the parameters in 60-65535 are used, this parameter takes effect.

4.4.12 SOCKET local port setting

The register 40175 (0x00B0) is used to set the SOCKET local port number, and supports 0x0003, 0x0006, and 0x0010 function codes. When the value is 0, it means that the random port number is used, and 1-65535 means that it is set to the corresponding port number.

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

4.4.13 MAC Read

The starting address for reading the MAC register is 40232 (0x00E9), and the total length of the registers is 11. Among them, the first register is the length of the MAC, and the second register to the eleventh register store the MAC value. For example, MAC: B2FAEAF2C427, the corresponding register value is as follows, in the register, the IMEI value exists in hexadecimal ASCII value.

40171 (0x00AA)	40172 (0x00AB) --40181 (0x00B4)
MAC length	MAC value
00 0C	42 32 46 41 45 41 46 32 43 34 32 37 00 00 00 00 00 00 00 00

4.4.14 SN read

The starting address for reading the SN register is 40243 (0x00F4), and the total length of the registers is 11. Among them, the first register is the length of the SN, and the second register to the eleventh register store the SN value. For example, SN: 190521135939C140, the corresponding register value is as follows. In the register, the SN value exists in hexadecimal ASCII value.

40182 (0x00B5)	40183 (0x00B6) --40192 (0x00BF)
SN length	SN value
00 10	31 39 30 35 32 31 31 33 35 39 33 39 43 31 34 30 00 00 00 00

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.

Revision history

Version	revision date	Revision Notes	v'vd
1.0	-	initial version	-
1.1	2019/8/19	formatting revisions	lyl
1.2	2023/1/13	Revise Section 1.2.2	Karry

Contact 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

---

Fax: 028-64146160 Web: www.ebyte.com

Address: B5 Mould Industrial Park, 199# Xiqu Ave, High tech Zone, Chengdu, Sichuan, China

Chengdu Ebyte Electronic Technology Co.,Ltd.

Copyright © 2012, Chengdu Ebyte Electronic Technology Co., Ltd.