



MODBUS-RTU Protocol

1 Protocol Overview

Communication is performed using the MODBUS-RTU (National Standard GB/T19582-2008) protocol, which supports one master station controlling multiple slave stations. Up to 247 slave addresses can be configured via the built-in host computer (0 for broadcast address, 1-247 for unicast addresses). The master station can be a single-chip microcomputer, PLC, PC, etc.

2 Communication Parameters

The default serial port configuration at factory is as follows: baud rate is 115200bps, 8 data bits, no parity, 1 stop bit. The baud rate can be configured within 4800~256000bps, and the default communication address (station number) of the driver is 1.

3 Modbus-RTU Frame Format

This driver supports MODBUS functions 0x03 (Read Holding Registers), 0x06 (Write Single Register), 0x10 (Write Multiple Registers), and 0x83 (Exception Code). Supported exception codes are 0x01 (Illegal Function) and 0x02 (Illegal Data Address).

3.1 Read Holding Registers 0x03

Master Station Transmission:

Byte	1	2	3	4	5	6	7	8
Content	Slave Address	0x03	Register Address High	Register Address Low	Read Data Length High	Read Data Length Low	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247)
- **Byte 2 0x03:** Function code for reading register values
- **Bytes 3-4:** Starting address of the register to read

- **Bytes 5-6:** Length of data to read
- **Bytes 7-8:** CRC16 checksum of Bytes 1–6

Slave Normal Response:

Byte	1	2	3	4、 5	6、 7	...	n-1、 n	n+1	n+2
Content	Slave Address	0x03	Total Register Bytes	Register Data 1	Register Data 2		Register Data m	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247)
- **Byte 2 0x03:** Function code for reading register values
- **Byte 3:** Total number of register bytes from Byte 4 to n (inclusive)
- **Bytes 4~n:** m register data read, where $m=(n-3)/2$; (n-1) is the high-order byte, n is the low-order byte
- **Bytes n+1–n+2:** CRC16 checksum of Bytes 1–n

Slave Abnormal Response:

Byte	1	2	3	4	5
Content	Slave Address	0x83	0x02	CRC High Byte	CRC Low Byte

3.2 Write Single Register 0x06

Master Station Transmission:

Byte	1	2	3	4	5	6	7	8
Content	Slave Address	0x06	Register Address High	Register Address Low	Register Data High	Register Data Low	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247)
- **Byte 2 0x06:** Function code for writing to a single register
- **Bytes 3-4:** Address of the register to write

- **Bytes 5-6:** Data to write to the register
- **Bytes 7-8:** CRC16 checksum of Bytes 1–6

Slave Normal Response:

Byte	1	2	3	4	5	6	7	8
Content	Slave Address	0x06	Register Address High	Register Address Low	Register Data High	Register Data Low	CRC High Byte	CRC Low Byte

Slave Abnormal Response:

Byte	1	2	3	4	5
Content	Slave Address	0x86	Exception Code	CRC High Byte	CRC Low Byte

- Exception Code: 0x02 = Illegal master request address; 0x03 = Illegal request data

3.3 Write Multiple Registers 0x10

Master Station Transmission:

Byte	1	2	3	4	5	6	7	8、9	10、11	...	n-1、n	n+1	n+2
Content	Slave Address	0x10	Register Address High	Register Address Low	Register Length High	Register Length Low	Total Register Bytes	Register Data 1	Register Data 2	...	Register Data m	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247)
- **Byte 2 0x10:** Function code for writing to multiple registers
- **Bytes 3-4:** Address of the register to write (3 = high-order byte, 4 = low-order byte)
- **Bytes 5-6:** Length m of registers to write
- **Byte 7:** Total number of bytes from Byte 8 to n (inclusive)
- **Bytes 8~n:** m register data to write, where $m=(n-7)/2$; (n-1) = high-order byte, n = low-order byte
- **Bytes n+1–n+2:** CRC16 checksum of Bytes 1 to n

Slave Normal Response:

Byte	1	2	3	4	5	6	7	8
Content	Slave Address	0x10	Register Address High	Register Address Low	Register Length High	Register Length Low	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247)
- **Byte 2 0x10:** Function code for writing to multiple registers
- **Bytes 3-4:** Address of the register to write
- **Bytes 5-6:** Length of registers to write
- **Bytes 7-8:** CRC16 checksum of Bytes 1–6

Slave Abnormal Response:

Byte	1	2	3	4	5
Content	Slave Address	0x90	Exception Code	CRC High Byte	CRC Low Byte

- Exception Code: 0x02 = Illegal master request address; 0x03 = Illegal request data

3.4 Query Slave Device ID 0x17

Master Station Transmission:

Byte	1	2	3	4
Content	Slave Address	0x17	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247). Using 0 broadcast ID is allowed when only one slave device is connected to the bus.
- **Byte 2 0x17:** Function code
- **Bytes 3-4:** CRC16 checksum of Bytes 1–3

Slave Normal Response:

Byte	1	2	3	4	5	6	7	8
Content	Slave Address	0x17	3	Slave Address	Status Code High	Status Code Low	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247)
- **Byte 2 0x17:** Function code
- **Byte 3:** Number of valid bytes returned
- **Byte 4:** Slave address code (1–247)
- **Bytes 5-6:** Status code
- **Bytes 7-8:** CRC16 checksum of Bytes 1–6

3.5 Restart Specified Slave Device 0x65

Master Station Transmission:

Byte	1	2	3	4
Content	Slave Address	0x65	CRC High Byte	CRC Low Byte

- **Byte 1 Slave Address:** Slave address code (1–247). Using 0 as broadcast ID restarts all slave devices on the bus.
- **Byte 2 0x65:** Function code
- **Bytes 3-4:** CRC16 checksum of Bytes 1–3