

modbus-RTU 通讯协议说明

四川旗芯电子科技有限公司

Modbus 是一种串行通信协议，是 Modicon 公司（现在的施耐德电气 Schneider Electric）于 1979 年为使用可编程逻辑控制器（PLC）通信而发表。Modbus 已经成为工业领域通信协议的业界标准（De facto），并且现在是工业电子设备之间常用的连接方式。

Modbus-RTU 协议是一种总线协议，采用一主多从的结构。即同一个总线网络中，只能一个主机(主站)，多个从机(从站)。

通讯时采用一问一答的方式，主动发送请求帧的是主机，被动回复响应帧的是从机，从机不会主动发送数据。

本协议采用标准 modbus-rtu 协议，在原有基础上进行裁剪，只保留常用功能，使得操作更灵活和简便。

RS485 和 modbusRTU 的关系：

RS485 是一种传输数据的通讯方式，modbusRTU 是一种通讯协议。

两者的关系类似声音和语言的关系，RS485 是声音，ModbusRTU 是其中一种语言，两个人说话，能听到对方的声音，但是听不懂对方的语言，是无法交流理解的。

所以请不要再问：“我这个设备是 485 信号输入/输出，能用你们的产品吗？”这类问题，不知道具体协议是没法判断的。

相关名词解释：

设备地址：设备的通讯地址、站号。

功能码：对数据帧的功能编号。

寄存器：存放某类数据的内存区域。一个设备可能有多种寄存器，不同的寄存器存放不同类别的数据。

寄存器地址：某个数据在寄存器里的编号。不同的设备定义不同。

注：下文所有 0x 开头数值和举例中请求帧响应帧均表示十六进制数。

1、 功能码：

读离散输入状态寄存器： 0x02

读多个保持寄存器： 0x03

读多个输入寄存器： 0x04

写单个保持寄存器： 0x06

写多个保持寄存器： 0x10

注：产品支持的功能码以相应产品使用说明为准。

2、数据帧结构解析：

A. 0x02 读多个离散输入寄存器：

发送帧

设备地址	功能码	寄存器起始地址		寄存器数		CRC 校验	
1 字节	1 字节	2 字节		2 字节		2 字节	
ID	0x02	高	低	高	低	低	高

应答帧

设备地址	功能码	数据长度	数据 1	数据 2	...	CRC 校验	
1 字节	1 字节	1 字节	1 字节	1 字节	N 字节	2 字节	
ID	0x02	n	D1	D2	Dn	低	高

举例：读取设备地址 0x01，从离散寄存器 0x0000 开始，连续读 0x000A 个寄存器

请求帧：01 02 00 00 00 0A F8 0D

响应帧：01 02 02 08 01 7F B8

数据长度 0x02 个字节，数据为 0x08 0x01，

第一个字节 0x08 表示 0x0000~0x0007 寄存器，二进制为 0000 1000，分解如下：

寄存器	0x07	0x06	0x05	0x04	0x03	0x02	0x01	0x00
值	0	0	0	0	1	0	0	0
状态	OFF	OFF	OFF	OFF	ON	OFF	OFF	OFF

第二个字节 0x01 表示 0x0008~0x0009 寄存器，二进制为 0000 0001，分解如下：

寄存器	-	-	-	-	-	-	0x09	0x08
值	0	0	0	0	0	0	0	1
状态	-	-	-	-	-	-	OFF	ON

注：一个字节最少 8 位，但只读了 8+2 个寄存器，所以第二个字节的高 6 位为补位的 0，并非表示寄存器 0x0A~0x0F 状态为 0。

B. 0x03 读多个保持寄存器:

发送帧

设备地址	功能码	寄存器起始地址		寄存器数		CRC 校验	
1 字节	1 字节	2 字节		2 字节		1 字节	1 字节
ID	0x03	高	低	高	低	低	高

响

应答帧

设备地址	功能码	数据长度	数据 1		数据 N	CRC 校验	
1 字节	1 字节	1 字节	2 字节		2 字节	2 字节	
ID	0x03	2*N	高	低		高	低

举例: 读取设备地址 0x01, 从保持寄存器 0x0000 开始, 连续读 0x0002 个寄存器

请求帧: 01 03 00 00 00 02 C4 0B

响应帧: 01 03 04 01 60 01 61 3B A9

数据长度 0x04 个字节, 因为一个寄存器 2 个字节

第 1 个寄存器 = 0x0160 = 352

第 2 个寄存器 = 0x0161 = 353

C. 0x04 读多个输入寄存器:

发送帧

设备地址	功能码	寄存器起始地址		寄存器数		CRC 校验	
1 字节	1 字节	2 字节		2 字节		1 字节	1 字节
ID	0x04	高	低	高	低	低	高

响

应答帧

设备地址	功能码	数据长度	数据 1		数据 N	CRC 校验	
1 字节	1 字节	1 字节	2 字节		2 字节	2 字节	
ID	0x04	2*N	高	低		高	低

举例: 读取设备地址 0x01, 从输入寄存器 0x0000 开始, 连续读 0x0002 个寄存器

请求帧: 01 04 00 00 00 02 71 CB

响应帧: 01 04 04 01 60 01 61 3A 1E

数据长度 0x04 个字节，因为一个寄存器 2 个字节

第 1 个寄存器 = 0x0160 = 352

第 2 个寄存器 = 0x0161 = 353

D. 0x06 写单个保持寄存器:

发送帧

设备地址	功能码	寄存器地址		寄存器值		CRC 校验	
1 字节	1 字节	2 字节		2 字节		1 字节	1 字节
ID	0x06	高	低	高	低	低	高

响应帧与发送帧相同表示成功。

举例：将设备地址 0x01 的保持寄存器 0x0020 的值修改为 0x0001

请求帧：01 06 00 20 00 01 49 C0

响应帧：01 06 00 20 00 01 49 C0

E. 0x10 写多个保持寄存器:

发送帧

设备地址	功能码	寄存器地址	寄存器数	数据长度	数据 1		数据 N	CRC 校验
1 字节	1 字节	2 字节	2 字节	1 字节	2 字节		2 字节	2 字节
ID	0x10	高 低	N	2*N	高 低		高 低	低 高

响应帧

设备地址	功能码	寄存器地址	寄存器数	CRC 校验
1 字节	1 字节	2 字节	2 字节	2 字节
ID	0x10	高 低	N	低 高

举例：将设备地址 0x01，从寄存器 0x0020 开始，连续修改 0x0002 个寄存器，修改的值依次是 0x0001、0x0003，所以数据长度共 0x04 个字节

请求帧：01 10 00 20 00 02 04 00 01 00 03 E0 76

响应帧：01 10 00 20 00 02 40 02

D. 错误返回帧:

设备地址	功能码	数据长度	错误码	CRC 校验	
1 字节	1 字节	1 字节	1 字节	2 字节	
ID	CODE	0x01	ERR	低	高

当发送指令不能正确执行时，返回此错误帧。

CODE: 请求帧功能码最高位置 1。如 0x03 功能码，返回 CODE=0x83

ERR: 报错代码，用于分辨错误类型, 取值如下:

错误码	错误类型
0x01	功能码不支持
0x02	寄存器地址不合法
0x03	寄存器值不合法
0x04	校验错误
0x06	设备忙或者寄存器值不能更改
0xFF	其它错误

举例: 尝试修改保持寄存器 0x2000 的值为 0x0001, 但实际没有这个寄存器

请求帧: 01 06 02 00 00 01 49 B2

响应帧: 01 86 01 02 60 60

错误代码 0x02: 寄存器地址不合法

3. PLC 寄存器地址与 modbus 寄存器地址对照表:

注: 对照关系由 PLC 决定, 此表仅适用市面上部分品牌, 具体以 PLC 厂家说明为准。

寄存器类型	PLC 寄存器地址	Modbus 寄存器地址
线圈寄存器	00001~09999	0x0000~0xFFFF
离散输入寄存器	10001~19999	0x0000~0xFFFF
保持寄存器	40001~49999	0x0000~0xFFFF
	400001~465535	0x0000~0xFFFF
输入寄存器	30001~39999	0x0000~0xFFFF

4. CRC16 校验算法

```
unsigned short count_crc(unsigned char *data,unsigned char length)
{
    unsigned char i,j;
    unsigned short crc=0xffff;
    for(i=0;i<length;i++)
    {
        crc=crc^*data;
        for(j=0;j<8;j++)
        {
            if(crc&0x01)
            {
                crc=(crc>>1)^0xa001;
            }
            else
            {
                crc=(crc>>1);
            }
        }
        data++;
    }
    return crc;
}
```

修订记录		
23-10-17	V1.4	增加协议介绍
23-9-19	V1.3	勘误
2022-1-10	V1.2	增加 0x02 0x04 功能码 说明、排版优化
2020-1-27	V1.1	初版

四川旗芯电子科技有限公司