

# Modbus 通讯协议 ( 13032011 )

## 1. 传输格式

RTU 协议：信息传输为 RS-485 半双工异步方式，并以字节为单位。传输速度固定为 9600bps。在主站和从站之间传递的通讯信息是 11 位的字格式：

起始位 ( 1 )	数据位 ( 8 )								奇偶校验 ( 1 )	停止位 ( 1 )
0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	无	1

## 2 帧格式

地址码(Device Address Field)
功能码(Function Code Field)
数据域(Data Field)
校验(Error Check Field)

主站询问：

Field Name	Example(Hex)
Slave Address	01-FFH
Function	03
Starting Address Hi	00
Starting Address Lo	00
Number of Points Hi	00
Number of Points Lo	xx
CRC16 Lo	xx
CRC16 Hi	xx

子站回答：

子站返回数据中，每个寄存器地址由两个字节组成，第一个字节包含高位信息，第二个字节包含低位信息。

Byte Count 字节的内容指数据的长度。

Field Name	Example(Hex)
Slave Address	01-FFH
Function	03
Byte Count	xx
Data 1	
Data2	
Data3	
Data4	
Data 5	
Data6	
...	
CRC16 Lo	xx
CRC16 Hi	xx

### 2.1 地址码

占用一个字节，地址码是每次通讯信息帧的第一字节，范围 0~255(00H~FFH)。出厂默认为 1

### 2.2 功能码

占用一个字节，03H 查询，10H 设置

### 2.3 数据域

数据长度不定，但最长为 60 个字节。数据域是主站和子站以读写寄存器的方式来进行数据交换的。

### 2.4 校验

占用二个字节，为帧的校验字，低位在前，高位在后。CRC16 算法：

冗余循环码（CRC）包含 2 个字节，即 16 位二进制。CRC 码由发送设备计算，放置于发送信息的尾部。接收信息的设备再重新计算接收到信息的 CRC 码，比较计算得到的 CRC 码是否与接收到的相符，如果两者不相符，则表明出错。

CRC 码的计算方法是，先预置 16 位寄存器全为 1。再逐步把每 8 位数据信息进行处理。在进行 CRC 码计算时只用 8 位数据位，起始位及停止位，如有奇偶校验位的话也包括奇偶校验位，都不参与 CRC 码计算。

在计算 CRC 码时，8 位数据与寄存器的数据相异或，得到的结果向低位移一字节，用 0 填补最高位。再检查最低位，如果最低位为 1，把寄存器的内容与预置数相异或，如果最低位为 0，不进行异或运算。

这个过程一直重复 8 次。第 8 次移位后，下一个 8 位再与现在寄存器的内容相异或，这个过程与以上一样重复 8 次。当所有的数据信息处理完后，最后寄存器的内容即为 CRC 码值。CRC 码中的数据发送、接收时低字节在前。

- 计算 CRC 码的步骤为：
- 1 预置 16 位寄存器为十六进制 FFFF（即全为 1）。称此寄存器为 CRC 寄存器；
  - 2 把第一个 8 位数据与 16 位 CRC 寄存器的低位相异或，把结果放于 CRC 寄存器；
  - 3 把寄存器的内容右移一位(朝低位)，用 0 填补最高位，检查最低位；
  - 4 如果最低位为 0：重复第 3 步(再次移位)；如果最低位为 1：CRC 寄存器与多项式 A001( 1010 0000 0000 0001 )进行异或；
  - 5 重复步骤 3 和 4，直到右移 8 次，这样整个 8 位数据全部进行了处理；
  - 6 重复步骤 2 到步骤 5，进行下一个 8 位数据的处理；
  - 7 最后得到的 CRC 寄存器即为 CRC 码。

3 实例

3.1 查询帧：

D0	D1	D2	D3	D4	D5	D6	D7
地址	功能码 03	寄存器起始地址		寄存器个数		CRC	

D0 表示设备地址，D1 表示功能码，

D2，D3 表示寄存器起始地址的高低位（D2 为高位，D3 为低位）

D4，D5 表示要查询寄存器个数高低位（D4 为高位，D5 为低位）

D6，D7 应该要表示 CRC 的高低字节（D6 为低位，D7 为高位）。最后两字节 CRC 的高低字节。

3.2 查询应答帧：

D0	D1	D2	D3	D4		
地址	功能码 03	返回的字节数	数据		CRC	

D0 表示设备地址，D1 表示功能码，

D2 表示返回的字节数，

D3.....返回的数据，高低位（D3 为高位，D4 为低位）。最后两字节 CRC 的高低字节。

3.3 设置帧：

D0	D1	D2	D3	D4	D5	D6	D7....		
地址	功能码 10H	寄存器起始地址		寄存器个数		字节数	数据码	CRC	

D0 表示设备地址，D1 表示功能码，

D2，D3 表示起始地址的高低位（D2 为高位，D3 为低位）

D4，D5 表示寄存器个数（D4 为高位，D5 为低位）

D6 表示有效的字节数

D7，D8 数据，高低位（D7 为低位，D8 为高位）。最后两个字节表示 CRC 的高低字节。

3.4 设置应答帧：

D0	D1	D2	D3	D4	D5	D6	D7
地址	功能码 10H	寄存器起始地址		寄存器个数		CRC	

D0 表示设备地址，D1 表示功能码，

D2，D3 表示寄存器起始地址的高低位（D2 为高位，D3 为低位）

D4，D5 表示要查询寄存器个数高低位（D4 为高位，D5 为低位）

D6，D7 应该要表示 CRC 的高低字节。（D6 为低位，D7 为高位）