

# MODBUS-RTU数据帧格式、报文实例

## MODBUS -RTU报文模型

设备地址	功能代码	数据格式	CRC校验L	CRC校验H
8bit	8bit	N*8bit	8bit	8bit

一个报文就是一帧数据，一个数据帧就一个报文：指的是一串完整的指令数据，就像上面的一串数据。

### 主机对从机写数据操作

如果单片机接收到一个报文那么就对报文进行解析执行相应的处理

0x01	06	00 01	00 17	98 04
从机地址	功能号	数据地址	数据	CRC校验

### 主机对从机读数据操作

0x01	03	00 01	00 01	D5 CA
从机地址	功能号	数据地址	读取数据个数	CRC校验

单片机接收到这串数据根据数据计算 CRC校验 判断数据是否正确，如果判断数据无误，则结果是：返回信息给主机，返回的信息也是有格式的：

从机对主机返回内容

0x01	03	02	00 17	F8 4A
从机地址	功能号	数据字节个数	两个字节数据	CRC校验

这样MODBUS主机就完成了一次对从机数据的读操作，实现了通讯。

## MODBUS-RTU常用功能码

数据类型	读功能码	写功能码	对象类型
离散量输入	02		单个位
线圈状态	01	05,15	单个位
输入寄存器	04		16位字
保持寄存器	03	06,16	16位字

### 寄存器起始地址（起始数据地址）

数据类型	参数地址,寄存器编号
离散量输入	00001~0FFFF
线圈状态	10001~1FFFF

输入寄存器	30001~3FFFF
保持寄存器	40001~4FFFF

举例：  
Modbus协议中寄存器地址从1开始，而实际存储中地址从0开始。假如要读取寄存器编号为40005（4为块编号，5为modbus中寄存器地址）的寄存器的数据，则应把0004放入报文的地址域。寄存器定义，又名码表或者信息点表，应由厂家提供的。

寄存器编号	属性	定义	系数	备注
40001	RO	A相电压		从40048中读取电压系数
40002	RO	B相电压		

如要读A相电压，则应将0x00 0x00放入寄存器起始地址域中。

报文实例

1、读40005、40006两个寄存器，假设从机地址为1

下行报文：01 03 00 04 00 02 85 ca

从机地址	功能码	寄存器起始地址	读取寄存器个数	CRC校验
01	03	00 04	00 02	85 ca

上行报文：01 03 04 00 00 00 00 21 33

从机地址	功能码	返回字节个数	寄存器40005数据	寄存器40006数据	CRC校验
01	03	04	00 00	00 00	21 33

2、向40005寄存器中写入0x12，0x34，假设从机地址为1

下行报文：01 06 00 04 00 01 12 34 4a b0

从机地址	功能码	寄存器起始地址	读取寄存器个数	要写入的数据	CRC校验
01	03	00 04	00 01	12 34	85 ca

上行报文：01 06 00 04 00 01 12 34 4a b0

从机地址	功能码	寄存器起始地址	读取寄存器个数	写入的数据	CRC校验
01	03	00 04	00 01	12 34	85 ca