1. Modbus ASCII 报文帧格式

起始位	设备(Slave)地址	功能代码	数据	LRC检验码	结束符
0x3A	2 Bytes	2 Bytes	n Bytes	2 Bytes	0x0D 0x0A

网络上的从机不断侦测起始符，当一个起始符被侦测到时，每个设备都解码下个域（地址域）的数据来判断数据是否是发给自己的。
数据中字符的发送时间间隔不能超过1s

2. Modbus RTU 报文帧格式

起始位	设备(Slave)地址	功能代码	数据	LRC检验码	结束符
>3.5个Byte传输时间的间隔	8 Bits	8 Bits	n * 8 Bits	2 * 8 Bits	>3.5个Byte传输时间的间隔

网络上的设备不断侦测网络总线，当地址域被侦测到，每个设备都解码判断消息是否是发给自己的。最后一个字符传输完成后，一个至少3.5 个字符时间的停顿标志了消息传输结束

- 地址域：每个从机设备都有一个唯一的地址码（1-247，0代表广播），只有地址码匹配的设备才能响应 Master 设备的请求。从机设备响应时，会附带自己的地址码。
- 功能码： Modbus 协议定义了 127 种功能码
- 数据域：主机需要从机执行的动作命令或者主机向从机请求的数据代号。从机的响应数据域包含了数据的字节长度+数据
- 校验码：可用于校验数据是否有效

FreeMODBUS

FreeMODBUS 是 Modbus 协议的一个开源实现（只有从机系统开源，主机系统收费），目前版本支持10种功能码

代码	中文名
0x03	读保持寄存器
0x04	读输入寄存器
0x06	写单个寄存器
0x10	写多个寄存器
0x17	读/写多个寄存器
0x01	读线圈状态
0x05	写单个线圈

代码	中文名
0x0F	写多个线圈
0x02	读输入状态
0x11	报告从机地址