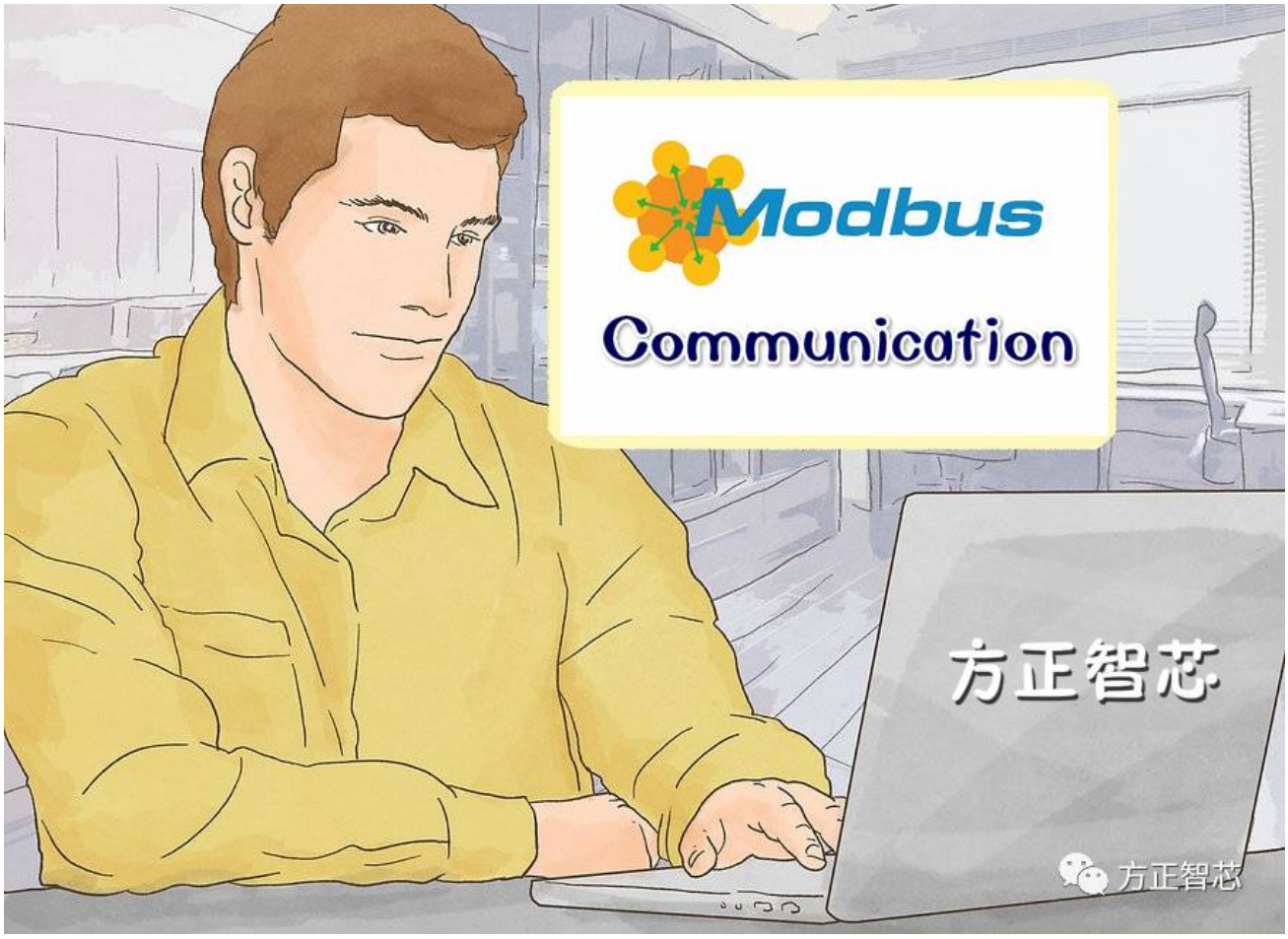
我是Modbus-RTU协议，我有两个兄弟

原创文章，转载请注明出处。

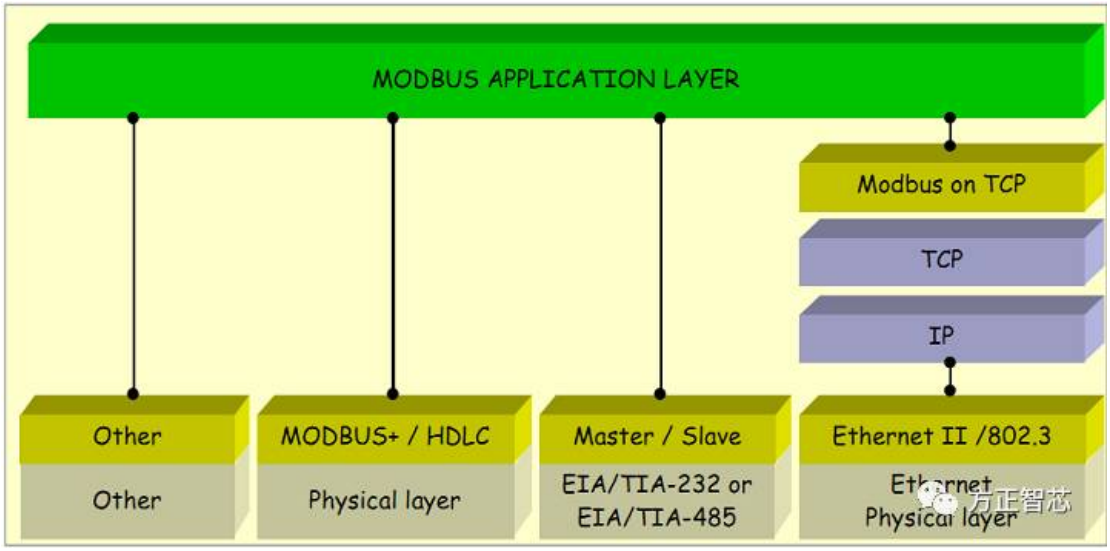
更多实用资料请登录方正智芯官网：www.founderchip.com

作者：北岛李工

我是Modbus RTU协议，我来自Modbus大家庭。早在1971年，Modicon公司首次推出了Modbus协议，我和我大哥——Modbus ASCII 都诞生在这里。后来施耐德电气（Schneider Electric）收购了Modicon公司，并在1997年推出了Modbus TCP协议，这就是我的三弟。2004年，中国国家标准委员会正式把Modbus作为了国家标准，开启了我们为中国工业通信做贡献的新篇章。

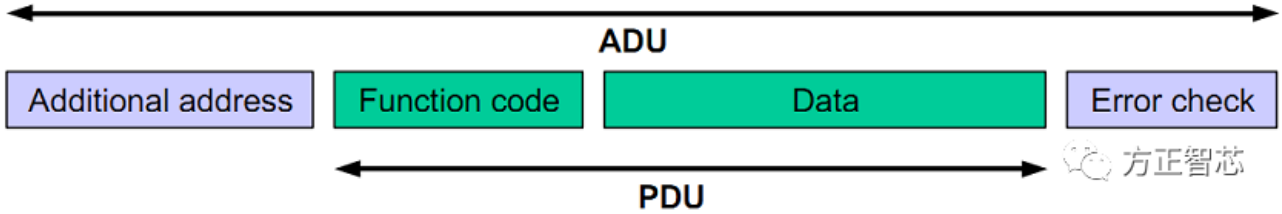


我们三兄弟在工业通信中应用广泛，我和我大哥（Modbus ASCII）主要活跃在串行通信领域，而我三弟（Modbus TCP）则擅长以太网通信。你可以看看下面这张图：



在串行链路中，我们（Modbus）使用一种简单的主从协议（客户机/服务器协议）进行通信。客户机作为主站，向服务器发送请求；服务器（从站）接到请求后，对请求进行分析并作出应答。我和小伙伴的通信帧被称为应用数据单元

（Application Data Unit，ADU），它包括通信地址段、功能代码段、数据段和校验段，如下图：



其中，功能代码段和数据段组合称为协议数据单元（Protocol Data Unit，PDU）。功能代码段占用一个字节，取值范围为1~255，其中128~255为保留值，用于异常消息应答报文。1~127为功能代码编号，其中65~72和100~110为用户自定义编码，具体请看下面这张图片：

值	Modbus功能编码	
127 111	Public function code	通用功能编码
110 100	User defined function code	用户自定义功能编码
99 73	Public function code	通用功能编码
72 65	User defined function code	用户自定义功能编码
64 1	Public function code	通用功能编码

通用功能编码（Public function code）是已经公布的功能代码，有确定的功能，用户不能修改。比如：0x01表示读取线圈，0x02表示读取离散量的输入等等。下图是一些常用的功能代码的描述：

方正智芯(founder chip)——Modbus功能代码(部分)		
功能编号(16进制)	功能描述	访问方式
01 H	读取线圈（read coils）	位（Bit）
02 H	读取离散量输入(read discrete inputs)	位（Bit）
03 H	读取保持寄存器值(read holding registers)	字（WORD）
04 H	读取输入寄存器值(read input registers)	位（Bit）
05 H	写单个线圈(write single coil)	位（Bit）
06 H	写单个寄存器(write single register)	字（WORD）
07 H	读取异常状态(read exception status)	诊断
08 H	诊断(Diagnostic)	诊断
0F H	写多个线圈(write multiple coils)	位（Bit）
10 H	写多个寄存器(write multiple registers)	字（WORD）

早期在RS485串行通信中规定ADU的最大长度为256个字节，其中：通信地址占用1个字节，校验段占用2个字节，所以协议数据单元（PDU）的最大长度为256-1-2=253 字节。而我三弟（Modbus TCP）因为要增加一个7个字节的MBAP（MODBUS Application Protocol）的报文头，所以他的ADU的长度=253+7=260 字节。

下面这张图是我（Modbus -RTU）的通信数据单元（ADU）的结构：

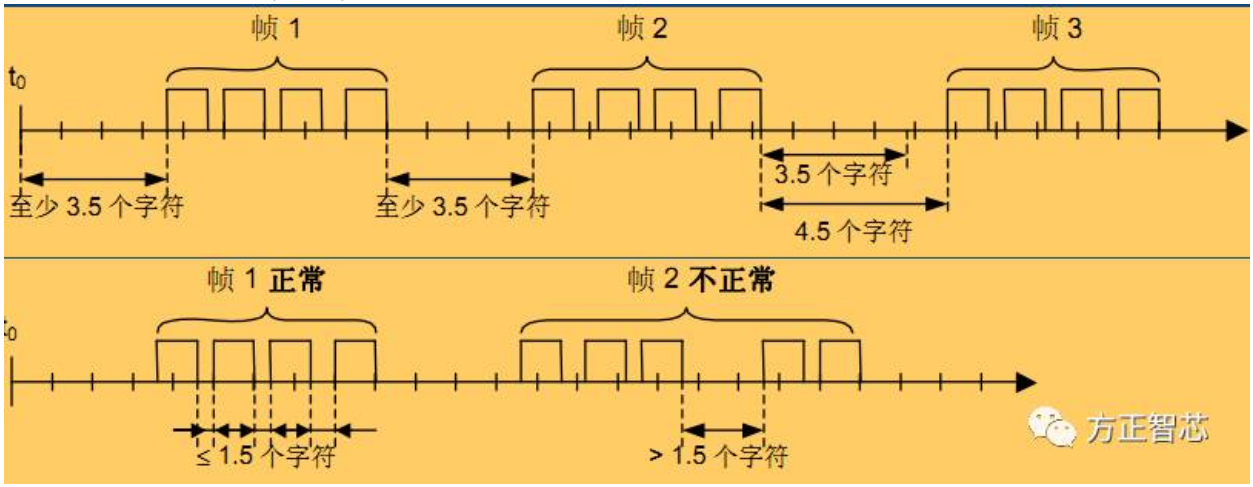
方正智芯(founder chip)——Modbus RTU ADU				
从站地址	功能代码	数据	校验段	
			CRC1	CRC2
1 字节	1 字节	0~252个字节	1 字节	1字节

我可以使用不同功能代码来完成不同的功能，比如下面表格左边的请求（request）指令使用0x05功能来使线圈173变为ON状态：

方正智芯-Modbus 将线圈173置位（ON）			
Modbus RTU PDU			
Request		**Response**	
Field Name	**Hex**	**Field Name**	**Hex**
Function	05	Function	05
Output address Hi	00	Output address Hi	00
Output address Lo	AC	Output address Lo	AC
Output value Hi	FF	Output value Hi	FF
Output value Lo	00	Output value Lo	00

该PDU指令中，第一个字节表示功能号“05”表示对单独线圈进行写操作（write single coil）；第二个字节表示线圈地址的高字节位，第三个字节表示线圈地址的低字节位（线圈的编号从0开始）。本例程中，第173号线圈的序号为172（0x00AC）；第四个字节表示输出值得高字节位，第五个字节表示输出值的低字节位。对于单独线圈操作，0xFF00表示置位（ON），0x0000表示复位（OFF）；不同的功能代码，其参数的字节的定义不同，使用时要参考下手册哦。

由于我（Modbus RTU）的报文格式没有定义帧的起始与结束字符，因此对于帧识别有时间上的要求：帧与帧之间的时间间隔要大于3.5个字符（字节）的时间；而帧内部的字符之间的间隔不能大于1.5个字符的时间，如下图：



我大哥（Modbus - ASCII）的帧的起始和停止有明确的字符定义；而我三弟（Modbus TCP）在传输过程中要增加一个报文头—MBAP，以后有时间我再给你们介绍；

好了，有空去官网看看吧，可以下载PDF版本：