MODBUS-TCP 协议

一　以太网的标准

以太网是一种局域网。早期标准为 IEEE 802.3，数据链路层使用 CSMA/CD，10Mb/s 速度物理层有：

(1)10 Base 5 粗同轴电缆，RG-8，一段最长为 500m；

(2)10 Base 2 细同轴电缆，RG-58，一段最长为 185m；

(3)10 Base T 双绞线，UTP 或 STP，一段最长为 100m。

快速以太网为 100Mb/s，标准为 802.3a，介质为 100 Base Tx 双绞线、100 Base Fx 光纤。

目前 10/100M 以太网使用最为普遍，很多企事业用户已实现 100M 到以太网桌面，确实体验到高速“冲浪”的快感，另外从距离而言，非屏蔽双绞线(UTP)为 100m，多模光纤可达 2～3km，单模光纤可大于 100km。千兆以太网 1000Mb/s 为 802.3z/802.3ab，万兆以太网 10Gb/s 为 802.3ae，将为新一轮以太网的发展带来新的机遇与冲击。

二　工业以太网与商用以太网的区别

什么是工业以太网？技术上，它与 IEEE802.3 兼容，故从逻辑上可把商用网和工业网看成是一个以太网，而用户可根据现场情况，灵活装配自己的网络部件，但从工业环境的恶劣和抗干扰的要求，设计者希望采用市场上可找到的以太网芯片和媒介，兼顾考虑下述工业现场的特殊要求：首先要考虑高温、潮湿、振动；二是对工业抗电磁干扰和抗辐射有一定要求，如满足 EN50081-2、EN50082-2 标准，而办公室级别的产品未经这些工业标准测试，表 1 列出了一些常用工业标准。为改善抗干扰性和降低辐射，工业以太网产品多使用多层线路板或双面电路板，且外壳采用金属如铸铝屏蔽干扰；三是电源要求，因集线器、交换机、收发器多为有源部件，而现场电源的品质又较差，故常采用双路直流电或交流电为其供电，另外考虑方便安装，工业以太网产品多数使用 DIN 导轨或面板安装；四是通信介质选择，在办公室环境下多数配线使用 UTP，而在工业环境下推荐用户使用 STP(带屏蔽双绞线)和光纤。

表 1　常用工业标准

标准	测试方法	描述
EN55024	EN61000-4-2	静电放电
EN55024	EN61000-4-3	抗辐射干扰
EN55024	EN61000-4-4	快速瞬态脉冲
EN55024	EN61000-4-5	浪涌电压
EN55024	EN61000-4-6	传导干扰
EN55024	EN61000-4-11	瞬降瞬断电压
EN55022	CISPR22	辐射放射
EN55022	CISPR22	传导辐射

三　TCP/IP

1. 为什么使用 TCP/IP？

最主要的一个原因在于它能使用在多种物理网络技术上，包括局域网和广域网技术。TCP/IP 协议的成功很大程度上取决于它能适应几乎所有底层通信技术。

20 世纪 80 年代初，先在 X.25 上运行 TCP/IP 协议；而后又在一个拨号语音网络(如电话系统)上使用 TCP/IP 协议，又有 TCP/IP 在令牌环网上运行成功；最后又实现了 TCP/IP 远程

分组无线网点与其他 Internet 网点间 TCP/IP 通信。所以 TCP/IP 协议极其灵活，具备连接不同网络的能力。

另外，使用 TCP/IP 也简化了 OSI 模型，因为它省略了表示层和会话层。如果现在把以太网的物理层和数据链路层加到 OSI 模型就构成了基于以太网的 TCP/IP 网，如图 1 所示。用以太网实现 TCP/IP 也是经济的一种方式。

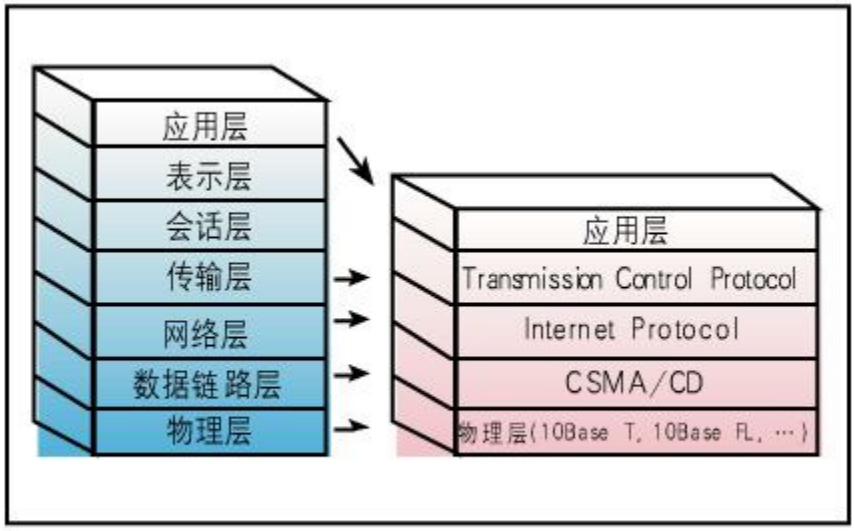

图 1　ISO/OSI 与以太网 TCP/IP 通信协议模型

2. Internet Protocol(IP)

IP 是 Internet 最基本的协议，用户可从 www.ietf.org 下载 RFC79 来得到其文件，(要求评论 RFC: Request For Comments：一系列备忘录的名称，包括概述、评价、意见、技术和研究，以及所提出的和被接受的互联网标准)。

IP 层主要目的是找到 IP 报文的“下一个连接点”，它可以是路由器、计算机、控制器甚至 I/O，关键该设备须有自己的 IP 地址。凡在网络层使用 IP 协议的网络，都通过 IP 地址寻址，所以使用时首先要进行复杂的设置，每个节点至少需一个“IP 地址”、一个“子网掩码”、一个“默认网点”和一个“主机名”，如此复杂的设置，对于一些初识网络的用户来说的确带来不便，不过随着对网络熟悉，有许多 IP 地址配置工具，可方便进行 IP 设置，甚至是自动设置。

IP 是面向报文的协议，它独立处理每个报文包，每个报文包必须含有完整的寻址信息。IP 报文包的格式如图 2 所示。

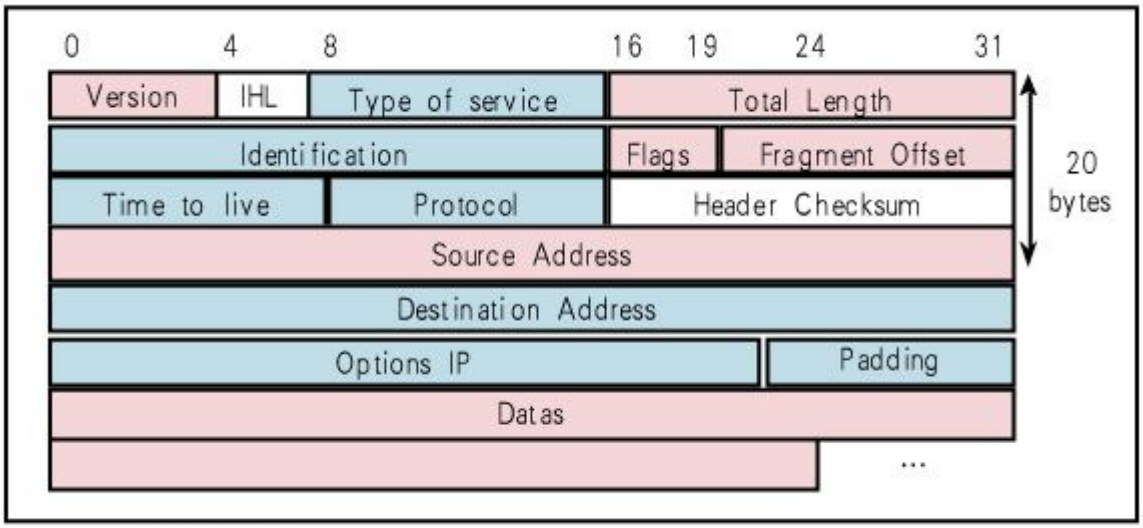

图 2　IP 报文包的格式

IP 地址的类型共有 4 种(如图 3 所示)：A 类用于处理超大型网络，最多 16387064 个主机(1～126)；B 类网络最多可有 64516 个主机(网络地址的第一段为 128～191)；C 类用于小型网络，最多可有 254 个主机(网络地址的第一段为 192～223)；D 类用于多点播送，用于多目的信息的传输。全零(“0.0.0.0”)地址对应于当前主机，全 1 地址(“255.255.255.255”)是当前子网的广播地址。

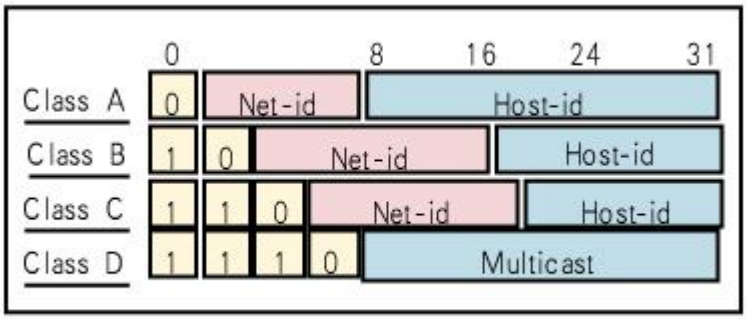

图 3　4 种 IP 地址类型

3. Transmission Control Protocol (TCP)

TCP 是基于传输层的协议(如图 4 所示)，协议文件可从 RFC793 得到，使用广泛，面向连接的可靠协议。它能把报文分解为数段，在目的站再重新装配这些段，支持重新发送未被收到的段，提供两台设备间的全双工连接，允许它们高效地交换大量数据。TCP 使用滑动窗口协议来高效使用网络。由于 TCP 很少干预底层投递系统的工作，它适应各种投递系统；且提供流量控制，能使各种不同速率的系统进行通信。报文段是 TCP 所使用的基本传输单元，用于传输数据或控制信息。

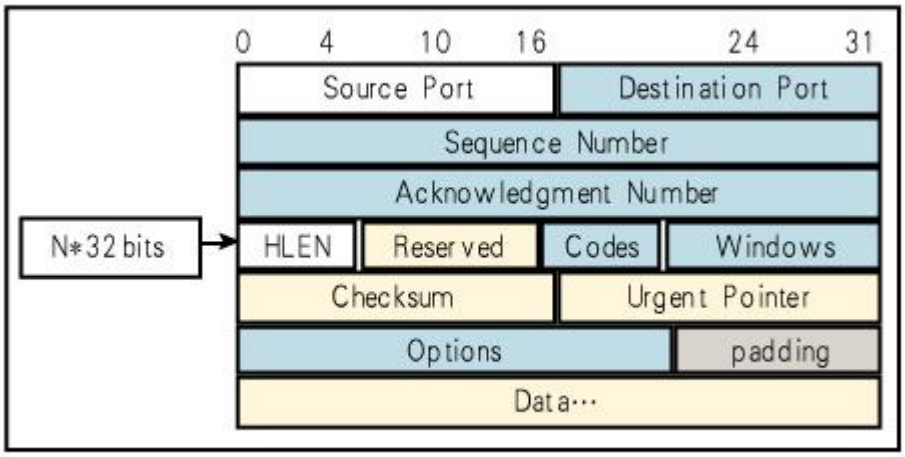

图 4　TCP 协议的报文段格式

4. TCP 端口

TCP 是使用端口(Socket)号把信息传到上层，为用户提供不同服务，端口号跟踪同一时间内通过网络的不同会话。RFC1700 中定义了众所周知的特殊端口号，常用端口如表 2 所列。其中 502 端口是自动化公司唯一所拥有的端口号码。

表 2　常用端口

十进制数	关键字	说明
20	FTP-Data	文件传输协议(数据)
21	FTP	文件传输协议
23	Telnet	远程登录
25	SMTP	简单邮件传输协议
53	Domain	域名服务器
67	Pootps	启动协议服务器
80	Http	超文本传输协议
110	POP3	邮件接收协议
502	Modbus	自动化信息传输

5. 协议(Protocal)的功能

组建网络时，必须选择一种网络通信协议，使得用户之间能相互进行“交流”。协议是网络设备用来通信的一套规则，可理解为一种彼此都能听懂的公用语言。如在网络层使用 IP 协议，在传输层使用 TCP 协议，就构成了目前常用的 TCP/IP 协议，现在几乎所有厂商和操作系统都支持它。同时，TCP/IP 也是 Internet 的基础协议。

如在应用层使用工业上事实标准的 Modbus 协议(如图 5 所示)，就构成了完整工业以太网应用。(www.hicode.cn)

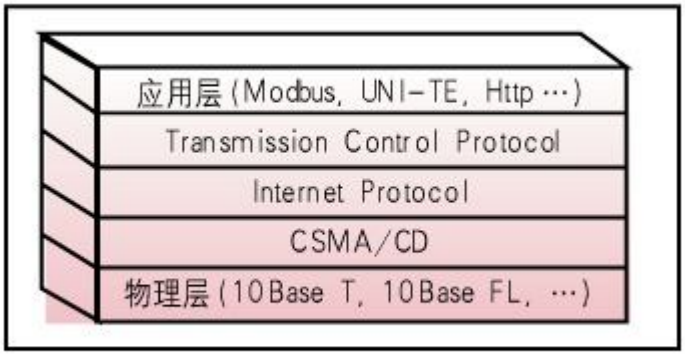

图 5 Modbus TCP/IP 模型

四 开放和标准的 Modbus TCP

Modbus 是开放协议，IANA(Internet Assigned Numbers Authority, 互联网编号分配管理机构)给 Modbus 协议赋予 TCP 端口 502，Modbus 协议可免费从 www.Modbus.org 得到。

Modbus 是标准协议，它已提交给 IETF(Internet Engineering Task Force, 互联网工程任务部)，将成为 Internet 标准。因自 1978 年，工业自动化行业已安装了百万计串口 Modbus 设备和十万计 Modbus TCP/IP 设备，拥有超过 300 个 Modbus 兼容设备厂商，还有 90%的第三厂家 I/O 支持 Modbus TCP/IP，所以是使用广泛的事实标准。Modbus 的普及得益于使用门坎很低，无论用串口还是用以太网，硬件成本低廉，Modbus 和 Modbus TCP 都可以免费得到，不需交任何费用，且在网上有很多免费资源，如 C/C++、JAVA 样板程序、ActiveX 控件、各种测试工具等，所以用户使用很方便。另外，几乎可找到任何现场总线到 Modbus TCP 的网点，方便用户实现各种网络之间的互联。

1. Modbus TCP/IP

如果使用 TCP/IP 以太网的 5 层：

第一层：物理层，提供设备的物理接口，与市售的介质/网络适配器相兼容；

第二层：数据链路层，格式化信号到源/目的硬件地址的数据帧；

第三层：网络层，实现带有 32 位 IP 地址的 IP 报文包；

第四层：传输层，实现可靠性连接、传输、查错、重发、端口服务、传输调度；

第五层：应用层，Modbus 协议报文。

2. Modbus TCP 数据帧

在 TCP/IP 以太网上传输，支持 Ethernet II 和 802.3 两种帧格式。图 6 所示，Modbus TCP 数据帧包含报文头、功能代码和数据 3 部分。

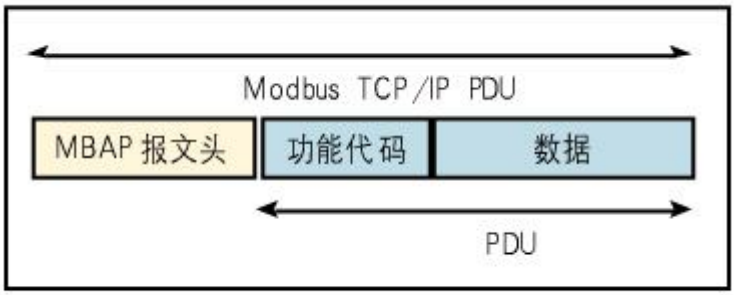

图 6 Modbus TCP 数据帧格式

MBAP 报文头(MBAP、Modbus Application Protocol、Modbus 应用协议)分 4 个域，共 7

个字节，如表 3 所示。

表 3　MBAP 报文头

域	长度(B)	描述	客户端	服务器端
传输标志	2	标志某个 Modbus 询问／应答的传输	由客户端生成	应答时复制该值
协议标志	2	0=Modbus 协议 1=UNI-TE 协议	由客户端生成	应答时复制该值
长度	2	后续字节计数	由客户端生成	应答时由服务器端重新生成
单元标志	1	定义连续于目的其他设备	由客户端生成	应答时复制该值

3. Modbus 功能代码

共有 3 种类型分别为：

(1)公共功能代码(如表 4 所示)：已定义好的功能码，保证其唯一性，由 Modbus.org 认可；

(2)用户自定义功能代码有两组，分别为 65～72 和 100～110，无需认可，但不保证代码使用的 唯一性。如变为公共代码，需交 RFC 认可；(3)保留的功能代码，由某些公司使用在某些传统设备的代码，不可作为公共用途。

表 4　Modbus 常用公共功能代码

常用公共功能代码			功能码		
			十进码	子码	十六进制
位操作	开关量输入	读输入点	02		02
	内部位或开关量输出	读线圈	01		01
		写单个线圈	05		
		写多个线圈	15		0F
16 位操作	模拟量输入	读输入寄存器	04		04
	内部寄存器或输出寄存器（模拟量输入）	读多个寄存器	03		03
		写单个寄存器	06		06
		写多个寄存器	16		10
		读／写多个寄存器	23		17
		屏蔽写寄存器	22		16
文件记录		读文件记录	20	6	14
		写文件记录	21	6	15
封装接口		读设备标识	43	14	2B

功能代码划分：按应用深浅，可分为 3 个类别。

1. 类别 0，对于客户机/服务器最小的可用子集：读多个保持寄存器(fc.3)；写多个保持

寄存器(fc.16)。

2. 类别 1，可实现基本互易操作的常用代码：读线圈(fc.1)；读开关量输入(fc.2)；读输入寄存器(fc.4)；写线圈(fc.5)；写单一寄存器(fc.6)。
3. 类别 2，用于人机界面、监控系统的例行操作和数据传送功能：
4. 强制多个线圈(fc.15)；读通用寄存器(fc.20)；写通用寄存器(fc.21)；屏蔽写寄存器(fc.22)；读写寄存器(fc.23)。

4. Modbus 应用举例

1.
2. 读寄存器(见表 5)。
3. Modbus TCP 请求报文举例(见表 6)。
4. Modbus TCP 客户端的实况。

用 Connect()命令建立目标设备 TCP 502 端口的连接数据通信的过程：

a. 准备 Modbus 报文，包括 7 个字节的 MBAP 在内的请求；
b. 使用 send()命令发送；
c. 在同一连接等待应答；
d. 同 recv()读报文，完成一次数据交换过程。

当通信任务结束时，关闭 TCP 连接，使服务器可以为其他服务。

5. Modbus TCP 的样板程序

用户可通过网站 www.transparent-factory.com 下载到：

a. JAVA 的应用程序；
b. 基于 Unix 系统下，C 的应用程序；
c. 基于 Win32 系统下，C 的应用程序。

6. Modbus TCP 协议

协议文本的英文版可从 www. modbus.org 下载，如需协议文本的中文版，可向施耐德电气(中国)投资有限公司各地区办事处索要。

表 5　读寄存器举例

请求	功能码	1 B	0 × 03
	起始地址	2 B	0 × 0000 到0 × FFFF
	寄存器数	2 B	1 到 125 (0 × 7D)
应答	功能码	1 B	0 × 03
	起始地址	1 B	2 × N
	寄存器的值 (N 为寄存器的数量)	N × 2 B	
出错	出错码	1B	0 × 83
	例外码	1B	01 或 02 或 03 或 04

表 6　Modbus TCP 请求报文举例

	描述	大小(B)	示例	备注
MBAP	传输标志 Hi	1	0 × 15	传输标志用于和应答配合使用
	传输标志 Lo	1	0 × 01	每对传输使用唯一的标志
	协议标志	2	0 × 0000	该域可用作寻址 Modbus/
	长度	2	0 × 0006	Modbus+ 子网络的路由，
	单元标志	1	0 × FF	这时该值含有目的设备的地址
Modbus 请求	功能代码	1	0 × 03	读寄存器
	起始地址	2	0 × 0005	
	寄存器数	2	0 × 0001	

五　使用 TCP/IP Modbus 的原因

1.
2. TCP/IP 已成为信息行业的事实标准：世界上 93%的网络都使用 TCP/IP，只要在应用层使用 Modbus TCP，就可实现工业以太网数据交换；
3. 易于与各种系统互连：可用于管理网、实时监控网及现场设备通信；
1. 网络实施价格低廉：可全部使用通用网络部件；
2. 用户强烈要求：目前中国已把 Modbus TCP 作为工业网络标准之一，用户可免费获得协议及样板程序，可在 Unix、Linux、Windows 下运行，不需要专门驱动程序。在国外，Modbus TCP 被国际半导体业 SEMI 定为网络标准，国际水处理、电力系统也把它作为应用的事实标准，还有越来越多行业作为标准来用；
1. 高速的数据：用户最关心的是所使用网络的传输能力，100M 以太网的传输结果为：每秒 4000 个 Modbus TCP 报文，而每个报文可传输 125 个字(16bit)，故相当于 4000×125=500000 个模拟量数据(8000000 开关量！)；
1. 厂家能提供完整解决方案：工业以太网的接线元件，包括工业集成器、工业交换机、工业收发器、工业连接电缆。工业以太网服务器，包括远程、分布式 I/O 扫描功能，设备地址 IP 的设置功能，故障设备在线更换。功能，分组的信息发布与订阅功能，网络动态监视功能，还有支持瘦客户机的 Web 服务。其他工控设备的支持：如工业用人机界面、变频器、软起动器、电动机控制中心、以太网 I/O、各种现场总线的网桥、甚至带 TCP/IPModbus 的传感器，都为用户使用提供了方便。