SIEMENS西门子山东省济南市（授权）一级代理商——西门子华北总代理

产品名称	SIEMENS西门子山东省济南市（授权）一级代理商——西门子华北总代理
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子总代理:PLC 西门子一级代:驱动 西门子代理商:伺服电机
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房
联系电话	15903418770 15915421161

产品详情

Modbus由MODICON公司于1979年开发，是一种工业现场总线协议标准。1996年施耐德公司推出基于以太网TCP/IP的Modbus协议：ModbusTCP。Modbus协议是一项应用层报文传输协议，包括ASCII、RTU、TCP三种报文类型。标准的Modbus协议物理层接口有RS232、RS422、RS485和以太网接口，采用master/slave方式通信。（视频：先来了解什么是Modbus通讯？）

，时长04:32

，时长04:32

AModbus TCP数据帧ModbusTCP的数据帧可分为两部分：MBAP+PDU。（一）报文头MBAP：MBAP为报文头，长度为7字节，组成如下：

（二）帧结构PDU：PDU由功能码+数据组成。功能码为1字节，数据长度不定，由具体功能决定。

（1）功能码：Modbus的操作对象有四种：线圈、离散输入、保持寄存器、输入寄存器。

（2）根据对象的不同，Modbus的功能码有：

（3）说明更详细的表：

BPDU详细结构

（1）0x01：读线圈：在从站中读1~2000个连续线圈状态，ON=1,OFF=0

请求：MBAP 功能码 起始地址H 起始地址L 数量H 数量L（共12字节）响应：MBAP 功能码 数据长度 数据（一个地址的数据为1位）如：在从站0x01中，读取开始地址为0x0002的线圈数据，读0x0008位00 01 00 00 00 06 01 01 00 02 00 08回：数据长度为0x01个字节，数据为0x01，第一个线圈为ON，其余为OFF00 01 00 00 00 04 01 01 01 01

（2）0x05：写单个线圈：将从站中的一个输出写成ON或OFF，0xFF00请求输出为ON,0x000请求输出为OFF。

请求：MBAP 功能码 输出地址H 输出地址L 输出值H 输出值L（共12字节）响应：MBAP 功能码 输出地址H 输出地址L 输出值H 输出值L（共12字节）如：将地址为0x0003的线圈设为ON00 01 00 00 00 06 01 05 00 03 FF 00回：写入成功00 01 00 00 00 06 01 05 00 03 FF 00

（3）0x0F：写多个线圈：将一个从站中的一个线圈序列的每个线圈都强制为ON或OFF，数据域中置1的位请求相应输出位ON，置0的位请求响应输出为OFF。

请求：MBAP 功能码 起始地址H 起始地址L 输出数量H 输出数量L 字节长度 输出值H 输出值L响应：MBAP 功能码 起始地址H 起始地址L 输出数量H 输出数量L

（4）0x02：读离散量输入：从一个从站中读1~2000个连续的离散量输入状态。

请求：MBAP 功能码 起始地址H 起始地址L 数量H 数量L（共12字节）响应：MBAP 功能码 数据长度 数据（长度：9+ceil（数量/8））如：从地址0x0000开始读0x0012个离散量输入00 01 00 00 00 06 01 02 00 00 00 12回：数据长度为0x03个字节，数据为0x01 04 00，表示第一个离散量输入和第11个离散量输入为ON，其余为OFF00 01 00 00 00 06 01 02 03 01 04 00

（5）0x04：读输入寄存器：从一个远程设备中读1~2000个连续输入寄存器。

请求：MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L（共12字节）响应：MBAP 功能码 数据长度 寄存器数据(长度：9+寄存器数量×2)如：读起始地址为0x0002，数量为0x0005的寄存器数据00 01 00 00 00 06 01 04 00 02 00 05回：数据长度为0x0A，第一个寄存器的数据为0x0c，其余为0x0000 01 00 00 00 0D 01 04 0A 00 0C 00 00 00 00 00 00 00 00

（6）0x03：读保持寄存器：从远程设备中读保持寄存器连续块的内容。

请求：MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L（共12字节）响应：MBAP 功能码 数据长度 寄存器数据(长度：9+寄存器数量×2)如：起始地址是0x0000，寄存器数量是 0x000300 01 00 00 00 06 01 03 00 00 00 03回：数据长度为0x06，第一个寄存器的数据为0x21，其余为0x0000 01 00 00 00 09 01 03 06 00 21 00 00 00 00

（7）0x06：写单个保持寄存器：在一个远程设备中写一个保持寄存器。

请求：MBAP 功能码 寄存器地址H 寄存器地址L 寄存器值H 寄存器值L（共12字节）响应：MBAP 功能码 寄存器地址H 寄存器地址L 寄存器值H
寄存器值L（共12字节）如：向地址是0x0000的寄存器写入数据0x000A00 01 00 00 00 06 01 06 00 00 00 0A回：写入成功00 01 00 00 00 06 01 06 00 00 00 0A

（8）0x10：写多个保持寄存器：在一个远程设备中写连续寄存器块（1~123个寄存器）。

请求：MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L 字节长度
寄存器值（13+寄存器数量×2）响应：MBAP 功能码 起始地址H 起始地址L 寄存器数量H 寄存器数量L（共12字节）如：向起始地址为0x0000，数量为0x0001的寄存器写入数据，数据长度为0x02，数据为0x000F
00 01 00 00 00 09 01 10 00 00 00 01 02 00 0F

回：写入成功00 01 00 00 00 06 01 10 00 00 00 01

CModbus TCP示例报文

ModBusTcp与串行链路Modbus的数据域是一致的，具体数据域可以参考串行Modbus。这里给出几个ModbusTcp的链路解析说明，辅助新人分析报文。

DModbus TCP通信

（一）通信方式

Modbus设备可分为主站(poll)和从站(slave)。主站只有一个，从站有多个，主站向各从站发送请求帧，从站给予响应。在使用TCP通信时，主站为client端，主动建立连接；从站为server端，等待连接。

主站请求：功能码+数据从站正常响应：请求功能码+响应数据从站异常响应：异常功能码+异常码，其中异常功能码即将请求功能码的最高有效位置1，异常码指示差错类型需要超时管理机制，避免无期限的等待可能不出现的应答IANA（Internet Assigned Numbers Authority，互联网编号分配管理机构）给Modbus协议赋予TCP端口号为502，这是目前在仪表与自动化行业中唯一分配到的端口号。

（二）通信过程

connect 建立TCP连接准备Modbus报文使用send命令发送报文在同一连接下等待应答使用recv命令读取报文，完成一次数据交换通信任务结束时，关闭TCP连接

E仿真软件

Modbus poll 和Modbus slave是一组Modbus仿真软件，可以实现Modbus RTU、TCP、串口仿真等。

仿真软件网址：https://modbustools.com/download.html

在ModbusTCP中，Modbus poll 作为客户端请求数据，Modbus slave 作为服务器端处理请求。

使用c语言编写客户端连接Modbus slave时，注意数据格式，一条指令一次性发出，否则连接会出错。

使用软件时，需要指定功能码，在setup->slave definition或者poll definition中进行设置。 – slave ID：从站编号（事务标识符） – function：功能码，0x01对应线圈操作，0x02对应离散量操作，0x03对应保持寄存器操作，0x04对应输入寄存器操作 – address：开始地址 – quantity：寄存器/线圈/离散量 的数量