Modbus-TCP 协议文档说明

1、指令格式说明（文档中所有数据要求为 16 进制）

(1)、功能码 03---查询从设备寄存器数据内容

主设备报文

序列	数据举例	数据内容	字节数
1	00 00	为此次通信事务处理标识符，一般每次通信之后将被要求加 1 以区别不同的通信数据报文	2
2	00 00	表示协议标识符，固定	2
3	00 06	为数据长度，用来指示接下来数据的长度（4-7 序列数据长度）	2
4	01	从设备地址，可变（1-256），说明为 1	1
5	03	功能码	1
6	00 00	数据起始寄存器地址，参照产品寄存器点表	2
7	00 02	读取寄存器个数（读取 2 个寄存器数据）	2

从设备正确报文

序列	数据举例	数据内容	字节数
1	00 00	为此次通信事务处理标识符，应答报文要求与先前对应的请求保持一致；	2
2	00 00	表示协议标识符，与发送的固定保持一致	2
3	00 07	为数据长度，用来指示接下来数据的长度（4-7 序列数据长度）	2
4	01	从设备地址，与发送保持一致	1
5	03	功能码，与发送保持一致	1
6	04	数据区返回的字节个数(2*读取寄存器个数)	1
7	12 34 56 78	数据区，返回的数据长度；每个寄存器为 2 个字节	4（可变）

举例：读取数据 8 个寄存器参数：

标识符	协议代码	数据长度	功能码	起始寄存器地址		寄存器个数	
00 00	00 00	00 06	03	00	00	00	08

说明：从寄存器 0 开始连续读 8 个寄存器数据，每一路电流数据占用一个寄存器；

数据返回格式：（**数据后的 H 代表 16 进制**）

标识符	协议代码	数据长度	从设备地址	功能码	数据区字节个数	返回数据区
00 00	00 00	00 13H	01	03	10H	（16 个数据）……

说明：数据区总共有 36 组数据，72 个字节；CRC 校验码要根据实际数据得出；

数据最小为:0000H,最大值为:2710H(十六进制),10000D(十进制)

(2)、功能码 06---对从设备单个寄存器置数

主设备报文

序列	数据举例	数据内容	字节数
1	00 00	为此次通信事务处理标识符，一般每次通信之后将被要求加 1 以区别不同的通信数据报文	2
2	00 00	表示协议标识符，固定	2
3	00 06	为数据长度，用来指示接下来数据的长度（4-7 序列数据长度）	2
4	01	从设备地址，可变（1-256），说明为 1	1

5	06	功能码	1
6	00 01	数据寄存器地址，参照产品寄存器点表	2
7	00 03	写入的数据内容	2

从设备正确报文

序列	数据举例	数据内容	字节数
1	00 00	为此次通信事务处理标识符，应答报文要求与先前对应的请求保持一致；	2
2	00 00	表示协议标识符，与发送的固定保持一致	2
3	00 06	为数据长度，用来指示接下来数据的长度（4-7 序列数据长度）	2
4	01	从设备地址，返回与发送保持一致	1
5	06	功能码，返回与发送保持一致	1
6	00 01	数据寄存器地址，返回与发送一致	2
7	00 03	数据内部，返回与发送一致	2

举例：单个寄存器写数：

标识符	协议代码	数据长度	从设备地址	功能码	寄存器地址		写入数据	
00 00	00 00	00 06	01	06	00	01	00	03

说明：对寄存器 0001 地址写入数据 0003；

数据返回格式：（**数据后的 H 代表 16 进制**）

标识符	协议代码	数据长度	从设备地址	功能码	寄存器地址		写入数据	
00 00	00 00	00 06	01	06	00	01	00	03

说明：返回与发送的一致；

Modbus-TCP 协议与 Modbus-RTU 协议比较：

1、数据尾无 CRC 校验码；

2、多出前面 6 个字节的数据头；

关于使用本公司的网口通讯的采集模块，很多客户误解网口通讯 TCP/IP 协议与 Modbus-TCP 的协议，把两者弄为一个协议；Modbus-TCP 协议是基于网口 TCP/IP 协议上传输的数据内容，类似于串口通讯的 Modbus-RTU 通讯协议的使用方法；所以请大家区别对待两个 TCP 协议；

本公司网口型产品出厂都默认为 Modbus-RTU 协议出厂，如果需要修改为 Modbus-TCP 协议需要按说明书上的协议修改寄存器发以下命令方式修改为 Modbus-TCP 协议；

协议转换设置(网络通讯接口产品可选择使用 Modbus-TCP 协议)

寄存器地址(Hex)	寄存器内容	寄存器个数	寄存器状态	数据范围
0060H	协议转换	1	写	00：Modbus-RTU 协议 01：Modbus-TCP 协议

协议修改命令举例：

从设备地址	功能码	寄存器地址		写入数据		CRC-L	CRC-H
01H	06H	00H	60H	00H	01H	48H	14H

说明：用 06 功能码协议修改为 Modbus-TCP 通讯协议；

数据返回格式：

从设备地址	功能码	寄存器地址		写入数据		CRC-L	CRC-H
01H	06H	00H	60H	00H	01H	48H	14H

使用发命令修改的工具软件可以到本公司网站上下载一个测试工具去发命令修改,下载地址为:
http://www.szzczh.cn/z.aspx?id=71&P=upload/file/sscom5.13.1%E5%B7%A5%E5%85%B7.zip

软件页面设置与发送格式如下:(产品出厂默认 IP 为 192.168.2.7 20108 端口),发送后有数据返回即为修改成功.