**MODBUS TCP通讯协议**

**1：端口号502。**

**2：该设备作为服务器端使用。电脑作为客户端使用。**

**3：IP地址是可通过网口和屏幕菜单进行设置的。出厂默认IP地址是：**

**IP地址：192.168.0.X X为群组码**

**子网掩码：255.255.255.0**

**默认网关：192.168.0.1**

**4：MODBUS TCP协议：**

**4.1读取寄存器请求**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 意义 | 所占字节 | 字节存放格式 |
| 1 | 事物处理标识 | 两个字节 | 高字节在前 |
| 2 | 协议标识 | 两个字节 | 高字节在前 |
| 3 | 长度 | 两个字节 | 高字节在前 |
| 4 | 单元标识 | 1个字节 | 0x00-0xff |
| 5 | 功能码 | 1个字节 | 0x03 |
| 6 | 起始寄存器基地址 | 两个字节 | 高字节在前 |
| 7 | 寄存器个数 | 两个字节 | 高字节在前 |

事物处理标识：该标识在主机和从机都是一样的，亦即是说从机收到MODBUS协议包时，该标识原封不动的传给主机。

协议标识：0表示MODBUS协议。

长度：该长度指紧随其后的数据长度。

单元标识：即为群组码。

**读取寄存器回应**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 意义 | 所占字节 | 字节存放格式 |
| 1 | 事物处理标识 | 两个字节 | 高字节在前 |
| 2 | 协议标识 | 两个字节 | 高字节在前 |
| 3 | 长度 | 两个字节 | 高字节在前 |
| 4 | 单元标识 | 1个字节 | 0x00-0xff |
| 5 | 功能码 | 1个字节 | 0x03 |
| 6 | 数据长度 | 1个字节 | 寄存器个数X2 |
| 7 | 数据 | 寄存器个数X2 | 每个寄存器高字节在前 |

例子：读群组01的9个点的温度。

读寄存器数据串：

00 00 00 00 00 06 01 03 00 00 00 09

读寄存器回应：

00 00 00 00 00 15 01 03 12 00 FE 00 FD 00 FC 00 00 00 FD 00 FE 00 FD 00 FC 00 00

**4.2写单个寄存器请求**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 意义 | 所占字节 | 字节存放格式 |
| 1 | 事物处理标识 | 两个字节 | 高字节在前 |
| 2 | 协议标识 | 两个字节 | 高字节在前 |
| 3 | 长度 | 两个字节 | 高字节在前 |
| 4 | 单元标识 | 1个字节 | 0x00-0xff |
| 5 | 功能码 | 1个字节 | 0x10 |
| 6 | 寄存器地址 | 两个字节 | 00 66 |
| 7 | 寄存器值 | 两个字节 | 高字节在前 |

**写单个寄存器回应**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 意义 | 所占字节 | 字节存放格式 |
| 1 | 事物处理标识 | 两个字节 | 高字节在前 |
| 2 | 协议标识 | 两个字节 | 高字节在前 |
| 3 | 长度 | 两个字节 | 高字节在前 |
| 4 | 单元标识 | 1个字节 | 0x00-0xff |
| 5 | 功能码 | 1个字节 | 0x10 |
| 6 | 寄存器地址 | 两个字节 | 00 66 |
| 7 | 寄存器值 | 两个字节 | 高字节在前 |

例子：将群组码由01改为02.

写单个寄存器数据串：

00 00 00 00 00 06 01 10 00 66 00 02

写单个寄存器回应：

00 00 00 00 00 06 01 10 00 66 00 02

**4.3写多个寄存器请求**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 意义 | 所占字节 | 字节存放格式 |
| 1 | 事物处理标识 | 两个字节 | 高字节在前 |
| 2 | 协议标识 | 两个字节 | 高字节在前 |
| 3 | 长度 | 两个字节 | 高字节在前 |
| 4 | 单元标识 | 1个字节 | 0x00-0xff |
| 5 | 功能码 | 1个字节 | 0x10 |
| 6 | 起始寄存器地址 | 两个字节 | 00 55 |
| 7 | 寄存器个数 | 两个字节 | 00 0C |
| 8 | 数据长度 | 1个字节 | 18 |
| 9 | 数据 | 寄存器个数X2个字节 | 每个寄存器高字节在前 |

**写多个寄存器回应**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 意义 | 所占字节 | 字节存放格式 |
| 1 | 事物处理标识 | 两个字节 | 高字节在前 |
| 2 | 协议标识 | 两个字节 | 高字节在前 |
| 3 | 长度 | 两个字节 | 高字节在前 |
| 4 | 单元标识 | 1个字节 | 0x00-0xff |
| 5 | 功能码 | 1个字节 | 0x10 |
| 6 | 起始寄存器地址 | 两个字节 | 00 55 |
| 7 | 寄存器个数 | 两个字节 | 00 0C |

例子：将IP地址由192.168.0.1改为192.168.0.2.（子网掩码和网关不改也要输入）

IP: 192.168.0.1

子网掩码:255.255.255.0

网关: 192.168.0.1

更改为：

IP: 192.168.0.2

子网掩码:255.255.255.0

网关: 192.168.0.1

写多个寄存器数据串：

00 00 00 00 00 1f 01 10 00 55 00 0C 18 00 C0 00 A8 00 00 00 02 00 FF 00 FF 00 FF 00 00 00 C0 00 A8 00 00 00 01

写多个寄存器回应：

00 00 00 00 00 06 01 10 00 55 00 0C

注意：更改IP地址要重新建立网口连接。