通讯协议

一、通用协议：ModbusTCP

二、Server端地址

IP地址：192.168.1.200 192.168.1.201

子网掩码：255.255.255.0

网关：192.168.1.1

端口：502

三、格式

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TCP Header** | | | **地址** | **功能码** | **起始地址** | **数据** |
| 识别码 | 通讯方式 | 数据长度 |
| **2byte** | **2byte** | **2byte** | **1byte** | **1byte** | **2byte** | **Nbyte** |
| **00 00** | **00 00** | **00 xx** | **01** |  |  |  |

识别码（Transaction ID）：会产生2个Byte的随机值，用来识别该次通讯。

通讯方式（Protocal ID）：0000表示为 Modbus / TCP

数据长度（Length）：用来定义从Address开始 ~ data字段结束，所占的总长度。

四、 读取设备寄存器内容（功能码 0x03）

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 0x0003  
00 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0x00  
00 01 00 00 00 09 01 03 06 00 21 00 00 00 00

五、 写设备寄存器内容（功能码 0x06）

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0x000A  
00 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

七、点表

|  |  |
| --- | --- |
| **读写保持寄存器（功能码3,6）** | |
| **地址** | **内容** |
| **0x0000(ADDR40001)** | **本地/远程状态 0：本地 1：远程**  **6楼电控阀本地自动状态 0：关闭 1：开启**  **7楼电控阀本地自动状态 0：关闭 1：开启**  **8楼电控阀本地自动状态 0：关闭 1：开启**  **9楼电控阀本地自动状态 0：关闭 1：开启**  **10楼电控阀本地自动状态 0：关闭 1：开启**  **11楼电控阀本地自动状态 0：关闭 1：开启**  **12楼电控阀本地自动状态 0：关闭 1：开启**  **15楼电控阀本地自动状态 0：关闭 1：开启**  **16楼电控阀本地自动状态 0：关闭 1：开启**  **17楼电控阀本地自动状态 0：关闭 1：开启**  **18楼电控阀本地自动状态 0：关闭 1：开启**  **19楼电控阀本地自动状态 0：关闭 1：开启** |
| **0x0001(ADDR40002)** | **6楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0002(ADDR40003)** | **7楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0003(ADDR40004)** | **8楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0004(ADDR40005)** | **9楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0005(ADDR40006)** | **10楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0006(ADDR40007)** | **11楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0007(ADDR40008)** | **12楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0008(ADDR40009)** | **15楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0009(ADDR40010)** | **16楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x000a(ADDR40011)** | **17楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x000b(ADDR40012)** | **18楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x000c(ADDR40013)** | **19楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x000d(ADDR40014)** | **20楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x000e(ADDR40015)** | **21楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x000f(ADDR40016)** | **22楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0010(ADDR40017)** | **23楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0011(ADDR40018)** | **25楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0012(ADDR40019)** | **26楼电控阀本地状态时自动开启状态 0：关闭 1：开启** |
| **0x0013(ADDR40020)** | **6楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0014(ADDR40021)** | **7楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0015(ADDR40022)** | **8楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0016(ADDR40023)** | **9楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0017(ADDR40024)** | **10楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0018(ADDR40025)** | **11楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0019(ADDR40026)** | **12楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x001a(ADDR40027)** | **15楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x001b(ADDR40028)** | **16楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x001c(ADDR40029)** | **17楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x001d(ADDR40030)** | **18楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x001e(ADDR40031)** | **19楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x001f(ADDR40032)** | **20楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0020(ADDR40033)** | **21楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0021(ADDR40034)** | **22楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0022(ADDR40035)** | **23楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0023(ADDR40036)** | **25楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0024(ADDR40037)** | **26楼电控阀开关状态 0：关闭 1：开启 2：中间状态 65535：开关同时使能** |
| **0x0025(ADDR40038)** | **6楼电控阀开控制 5555：开启 (只写)** |
| **0x0026(ADDR40039)** | **6楼电控阀关控制 5555：关闭 (只写)** |
| **0x0027(ADDR40040)** | **7楼电控阀开控制 5555：开启 (只写)** |
| **0x0028(ADDR40041)** | **7楼电控阀关控制 5555：关闭 (只写)** |
| **0x0029(ADDR40042)** | **8楼电控阀开控制 5555：开启 (只写)** |
| **0x002a(ADDR40043)** | **8楼电控阀关控制 5555：关闭 (只写)** |
| **0x002b(ADDR40044)** | **9楼电控阀开控制 5555：开启 (只写)** |
| **0x002c(ADDR40045)** | **9楼电控阀关控制 5555：关闭 (只写)** |
| **0x002d(ADDR40046)** | **10楼电控阀开控制 5555：开启 (只写)** |
| **0x002e(ADDR40047)** | **10楼电控阀关控制 5555：关闭 (只写)** |
| **0x002f(ADDR40048)** | **11楼电控阀开控制 5555：开启 (只写)** |
| **0x0030(ADDR40049)** | **11楼电控阀关控制 5555：关闭 (只写)** |
| **0x0031(ADDR40050)** | **12楼电控阀开控制 5555：开启 (只写)** |
| **0x0032(ADDR40051)** | **12楼电控阀关控制 5555：关闭 (只写)** |
| **0x0033(ADDR40052)** | **15楼电控阀开控制 5555：开启 (只写)** |
| **0x0034(ADDR40053)** | **15楼电控阀关控制 5555：关闭 (只写)** |
| **0x0035(ADDR40054)** | **16楼电控阀开控制 5555：开启 (只写)** |
| **0x0036(ADDR40055)** | **16楼电控阀关控制 5555：关闭 (只写)** |
| **0x0037(ADDR40056)** | **17楼电控阀开控制 5555：开启 (只写)** |
| **0x0038(ADDR40057)** | **17楼电控阀关控制 5555：关闭 (只写)** |
| **0x0039(ADDR40058)** | **18楼电控阀开控制 5555：开启 (只写)** |
| **0x003a(ADDR40059)** | **18楼电控阀关控制 5555：关闭 (只写)** |
| **0x003b(ADDR40060)** | **19楼电控阀开控制 5555：开启 (只写)** |
| **0x003c(ADDR40061)** | **19楼电控阀关控制 5555：关闭 (只写)** |
| **0x003d(ADDR40062)** | **20楼电控阀开控制 5555：开启 (只写)** |
| **0x003e(ADDR40063)** | **20楼电控阀关控制 5555：关闭 (只写)** |
| **0x003f(ADDR40064)** | **21楼电控阀开控制 5555：开启 (只写)** |
| **0x0040(ADDR40065)** | **21楼电控阀关控制 5555：关闭 (只写)** |
| **0x0041(ADDR40066)** | **22楼电控阀开控制 5555：开启 (只写)** |
| **0x0042(ADDR40067)** | **22楼电控阀关控制 5555：关闭 (只写)** |
| **0x0043(ADDR40068)** | **23楼电控阀开控制 5555：开启 (只写)** |
| **0x0044(ADDR40069)** | **23楼电控阀关控制 5555：关闭 (只写)** |
| **0x0045(ADDR40070)** | **25楼电控阀开控制 5555：开启 (只写)** |
| **0x0046(ADDR40071)** | **25楼电控阀关控制 5555：关闭 (只写)** |
| **0x0047(ADDR40072)** | **26楼电控阀开控制 5555：开启 (只写)** |
| **0x0048(ADDR40073)** | **26楼电控阀关控制 5555：关闭 (只写)** |