# 双目客流MODBUS通信协议

## 1 通信接口

### 1.1 接口标准

接口标准：RS-485（EIA/TIA-485）
硬件连接：2线模式

### 1.2 通信参数

波特率：9600
数据位：8
停止位：1
校验位：n

## 2 通信格式

### 2.1 主机发送格式

| 地址 | 功能码 | 寄存器地址 | | 数据 | | CRC低位 | CRC高位 |
|---|---|---|---|---|---|---|---|
| Address | Function | AddrH | AddrL | NumH | NumL | CRCL | CRCH |

a、址地：对应子节点的地址，范围（1-247），默认地址为 01，0为广播地址；
b、功能码：0x03 读取一个或多个寄存器，0x06 写一个寄存器；
c、寄存器地址：AddrH表示要读的寄存器的高字节地址，AddrL表示要读的寄存器的低地址;寄存器地址定议请参见：（2.3 保持寄存器地址定议）。
d、数据:主机要读的数据的个数，范围从1-8；
e、最后两字节为CRC校验校验码的高低字节
例如：从机要对地址为06的设备进行测量数据的读取，则发送数据格式如下：
主机发送：06 03 00 06 00 02 25 BD

### 2.2 从机应答格式

| 地址 | 功能码 | 字节数 | 数据 | CRC低位 | CRC高位 |
|---|---|---|---|---|---|
| Address | Function | byte | D0H,D0L...DNH,DNL | CRCL | CRCH |

从机接收到从机发来的数据后，对数据进行解包，只要地地址匹配，就会对主机进行响应。
a、 地址编码：从机的地址（1-254）；
b、 功能码：0x03 读取一个或多个寄存器，0x06 写一个寄存器；
c、 字节数：发送数据的个数，即数据D0L-DNH的字节数；

d、 数据：发送给主机的数据，个数等于字节数；
e、 最后两字节为CRC校验校验码的高低字节；
例如：从机对以上主机发来的数据响应如下：
从机响应：06 03 02 00 00 0D 84
其中第四第五字据的数据为00 00表示现在从机所测量的数据为0，假如所测得的数据为9968,则传送的数据为26 F0,即十进制9968。

## 2.3 保持寄存器地址定义

| 地址 | 寄存器信息 | 取值范围 | R/W | 说明 |
| --- | --- | --- | --- | --- |
| 0x0000 | modbus地址寄存器 | 1~247 | R/W | |
| 0x0001 | 设备信息查询 | | R | 设备SN+设备MAC<br>硬件版本+软件版本+接口版本 |
| 0x0002 | 设备时间 | | R/W | 同步设备系统时间、查询设备当前时间 |
| 0x0003 | 通信波特率 | | R | 波特率固定9600 |
| 0x0004 | 开关门数据查询 | | R | 公交车场景下接入的开关门信号查询<br>时间戳+开关门状态 |
| 0x0005 | 客流数据操作 | | R/W | 读取：查询客流数据<br>写入：重置客流数据 |
| | | | | |

## 2.4 寄存器说明

不论是读还是写指令，从机回复指令如果成功，则不变，如果失败，则最高位置1。

- 读指令03:
  - 成功，则返回的指令位置依旧为03
  - 失败，则在返回指令的03的最高位置1，即83
- 写指令则06:
  - 成功：06　　失败：86

**举例(修改从机地址01->02)**:

01 06 00 00 00 02 08 0B
成功返回：02 06 00 00 00 02 08 38
失败返回(示例)：01 86 01 83 A0

### 2.4.1 地址寄存器0x0000(读、写)

#### 2.4.1.1 查询modbus地址（**使用广播地址00进行从机地址查询，仅用于忘记从机地址，主机连接单台从机获取从机地址。**）

主机发送：00 03 00 00 00 01 85 DB

| 广播地址 | 指令 | 寄存器地址 | 寄存器个数 | CRC_L | CRC_H |
| --- | --- | --- | --- | --- | --- |
| 00 | 03 | 0000 | 0001 | 85 | DB |

00 使用广播地址查询
03 读寄存器指令
00 00 寄存器地址： 00 00

00 01 寄存器个数： 00 01 ， 1 个
85 DB 校验码
设备回应：01 03 02 00 01 79 84

| 地址 | 指令 | 长度 | 数据 | CRC_L | CRC_H |
| --- | --- | --- | --- | --- | --- |
| 01 | 03 | 02 | 0001 | 79 | 84 |

01 设备地址码
03 读寄存器指令,失败返回 83,正常为03
02 数据长度
00 01 数据为 00 01 ，即寄存器地址为01
79 84 校验码
设备回应（失败，后续指令不再单独列出失败指令）： 01 83 01 80 F0

| 地址 | 指令 | 异常码 | CRC_L | CRC_H |
| --- | --- | --- | --- | --- |
| 01 | 83 | 01 | 80 | F0 |

01 设备地址码
83 读寄存器指令,失败返回 83,正常为03
01 异常码，这里01仅仅举例参考，具体含义参考2.6 MODBUS 异常码
80 F0 校验码
备注：广播地址查询指令只有查询modbus地址指令会响应（只允许在单从机连接情况下进行查询，多从机查询数据不可信），其他指令一概不响应

#### 2.4.1.2 修改modbus地址

主机发送：01 06 00 00 00 03 C9 CB

| 地址 | 指令 | 寄存器地址 | 寄存器值 | CRC_L | CRC_H |
| --- | --- | --- | --- | --- | --- |
| 01 | 06 | 0000 | 0003 | C9 | CB |

设备回应（成功）： 03 06 02 00 03 81 49

| 地址 | 指令 | 长度 | 数据 | CRC_L | CRC_H |
| --- | --- | --- | --- | --- | --- |
| 03 | 06 | 02 | 0003 | 81 | 49 |

### 2.4.2 设备信息查询(0x0001)（只读）

#### 2.4.2.1 读取设备信息

主机发送：01 03 00 01 00 01 D5 CA

| 地址 | 指令 | 寄存器地址 | 寄存器个数 | CRC_L | CRC_H |
| --- | --- | --- | --- | --- | --- |
| 01 | 03 | 0001 | 0001 | D5 | CA |

设备回应（成功）： 01 03 14 00 07 24 18 69 74 50 21 4C BC 98 60 00 97 01 2C 01 D2 00 64 E0 DF

| 地址 | 指令 | 长度 | SN | MAC | 硬件 | 软件 | 接口 | CRC | |
|---|---|---|---|---|---|---|---|---|---|
| 01 | 03 | 14 | 0007241869745021 | 4CBC98600097 | 012C | 01D2 | 0064 | E0 | DF |

SN: 0x0007241869745021对应十进制：2010012104020001，即是SN
MAC：4CBC98600097对应：4C:BC:98:60:00:97
硬件版本：0x12C对应十进制300，除以100得到版本号：3.0.0
软件版本：0x1D2对应十进制466，除以100得到版本号：4.6.6
接口版本：0x0064对应十进制100，除以100得到版本号：1.0.0

### 2.4.3 设备时间(0x0002)（读、写）

#### 2.4.3.1 读取设备时间：

主机发送：01 03 00 02 00 01 25 CA

| 地址 | 指令 | 寄存器地址 | 寄存器个数 | CRC_L | CRC_H |
|---|---|---|---|---|---|
| 01 | 03 | 0002 | 0001 | 25 | CA |

设备响应：01 03 07 07 E5 0C 1F 0C 02 28 C2 89

| 地址 | 指令 | 长度 | 年 | 月 | 日 | 时 | 分 | 秒 | CRC_L | CRC_H |
|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 03 | 07 | 07E5 | 0C | 1F | 0C | 02 | 28 | C2 | 89 |

时间转换：07E 转换成十进制得到2021年，月日时分秒依次转成10进制得到时间为 2021-12-31 12:02:40

#### 2.4.3.2 修改设备时间

主机发送：01 06 00 02 07 E5 0C 1F 0F 02 28 25 83

| 地址 | 指令 | 寄存器地址 | 年 | 月 | 日 | 时 | 分 | 秒 | CRC_L | CRC_H |
|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 06 | 0002 | 07E5 | 0C | 1F | 0F | 02 | 28 | 25 | 83 |

设备响应：01 06 07 07 E5 0C 1F 0F 02 28 0D D9

| 地址 | 指令 | 长度 | 年 | 月 | 日 | 时 | 分 | 秒 | CRC_L | CRC_H |
|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 06 | 07 | 07E5 | 0C | 1F | 0F | 02 | 28 | 0D | D9 |

#### 2.4.3.3 同步设备时间

主机发送：00 06 00 02 07 E5 0C 1F 0F 02 28 21 7F

| 广播地址 | 指令 | 寄存器地址 | 年 | 月 | 日 | 时 | 分 | 秒 | CRC_L | CRC_H |
|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 06 | 0002 | 07E5 | 0C | 1F | 0F | 02 | 28 | 21 | 7F |

设备响应：无
备注：广播地址写命令只有设置设备时间指令会生效，用于多从机时间同步，由于设备无响应，建议连续发送3次确保同步成功

### 2.4.4 通信波特率查询(0x0003)（只读）

#### 2.4.4.1 读取通信波特率

主机发送：01 03 00 03 00 01 74 0A

| 地址 | 指令 | 寄存器地址 | 寄存器个数 | CRC_L | CRC_H |
|---|---|---|---|---|---|
| 01 | 03 | 0003 | 0001 | 74 | 0A |

设备响应：01 03 02 03 C0 B8 E4

| 地址 | 指令 | 长度 | 波特率 | CRC_L | CRC_H |
|---|---|---|---|---|---|
| 01 | 03 | 02 | 03C0 | B8 | E4 |

波特率转换：03 C0 –> 对应十六进制 0x03C0, 转成十进制得到960. 乘以10即得9600。

### 2.4.5 开关门数据查询(0x0004)（只读）

#### 2.4.5.1 读取开关门数据（仅用于公交车场景）

主机发送：01 03 00 04 00 01 C5 CB

| 地址 | 指令 | 寄存器地址 | 寄存器个数 | CRC_L | CRC_H |
|---|---|---|---|---|---|
| 01 | 03 | 0004 | 0001 | C5 | CB |

设备响应：01 03 09 07 E5 0C 1F 0C 02 28 01 01 31 63

| 地址 | 指令 | 长度 | 年 | 月 | 日 | 时 | 分 | 秒 | 门号 | 开关门 | CRC_L | CRC_H |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 03 | 09 | 07E5 | 0C | 1F | 0F | 02 | 28 | 01 | 01 | 31 | 63 |

年：07E5 转换成十进制得到2021年，月日时分秒依次转成10进制得到时间为 2021–12–31 12:02:40
门号：01，范围01~ff，目前预留固定为01
开关门：00 关门；01 开门

### 2.4.6 客流数据操作(0x0005)（读写）

#### 2.4.6.1 查询客流数据

主机发送：01 03 00 05 00 01 94 0B

| 地址 | 指令 | 寄存器地址 | 寄存器个数 | CRC_L | CRC_H |
|---|---|---|---|---|---|
| 01 | 03 | 0005 | 0001 | 94 | 0B |

设备响应：01 03 0B 07 E5 0C 1F 0C 02 28 00 24 00 20 BD 91

| 地址 | 指令 | 长度 | 年 | 月 | 日 | 时 | 分 | 秒 | 进入 | 离开 | CRC_L | CRC_H |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 03 | 0B | 07E5 | 0C | 1F | 0F | 02 | 28 | 0024 | 0020 | BD | 91 |

年：07E5 转换成十进制得到2021年，月日时分秒依次转成10进制得到时间为 2021-12-31 12:02:40
进客流数：00 24 -> 对应十六进制 0x0024, 转成十进制得到36
出客流数：00 20 -> 对应十六进制 0x0020, 转成十进制得到32

#### 2.4.6.2 重置客流数据

主机发送：01 06 00 05 00 01 58 0B

| 地址 | 指令 | 寄存器地址 | 寄存器个数 | CRC_L | CRC_H |
|---|---|---|---|---|---|
| 01 | 06 | 0005 | 0001 | 58 | 0B |

设备响应：01 06 0B 07 E5 0C 1F 0C 02 28 00 00 00 00 F0 47

| 地址 | 指令 | 长度 | 年 | 月 | 日 | 时 | 分 | 秒 | 进入 | 离开 | CRC_L | CRC_H |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 06 | 0B | 07E5 | 0C | 1F | 0F | 02 | 28 | 0024 | 0020 | F0 | 47 |

年：07E5 转换成十进制得到2021年，月日时分秒依次转成10进制得到时间为 2021-12-31 12:02:40
进客流数：00 00 -> 对应十六进制 0x0000, 转成十进制得到0
出客流数：00 00 -> 对应十六进制 0x0000, 转成十进制得到0
**注：重置客流数据返回重置后设备的客流数据，成功重置则进出均为0.**

## 2.5 ModbusCRC16校验代码

```
/* CRC16计算方式的代码 */
/* CRC16 =  X16+X15+X2+1 ,报文中低位在前，高位在后*/
/* len为msg的数据+ CRC码长度*/
uint16_t crc16(uint8_t *msg, uint8_t len)
{
    int i,j;
    unsigned short wCrc;
    wCrc = 0xffff;
    //wCrc = 0x00;
    for(i=0; i<len; i++)
    {
        wCrc ^= msg[i];
        for (j = 0; j < 8; j++)
        {
            if(wCrc & 0x0001)
            {
                wCrc >>= 1;
                wCrc ^= 0xA001;
            }
            else
                wCrc >>= 1;
        }
    }
    return wCrc;
```

```
}
```

## 2.6 MODBUS 异常码

| MODBUS 异常码 | | |
|---|---|---|
| 代码 | 名称 | 含义 |
| 01 | 非法功能 | 对于服务器(或从站)来说，询问中接收到的功能码是不可允许的操作。这也许是因为功能码仅仅适用于新设备而在被选单元中是不可实现的。同时，还指出服务器(或从站)在错误状态中处理这种请求，例如：因为它是未配置的，并且要求返回寄存器值。 |
| 02 | 非法数据地址 | 对于服务器(或从站)来说，询问中接收到的数据地址是不可允许的地址。特别是，参考号和传输长度的组合是无效的。对于带有 100 个寄存器的控制器来说，带有偏移量 96 和长度 4 的请求会成功，带有偏移量 96 和长度 5 的请求将产生异常码 02。 |
| 03 | 非法数据值 | 对于服务器(或从站)来说，询问中包括的值是不可允许的值。这个值指示了组合请求剩余结构中的故障，例如：隐含长度是不正确的。并不意味着，因为MODBUS 协议不知道任何特殊寄存器的任何特殊值的重要意义，寄存器中被提交存储的数据项有一个应用程序期望之外的值。 |
| 04 | 从站设备故障 | 当服务器(或从站)正在设法执行请求的操作时，产生不可重新获得的差错。 |
| 05 | 确认 | 与编程命令一起使用。服务器(或从站)已经接受请求，并切正在处理这个请求，但是需要长的持续时间进行这些操作。返回这个响应防止在客户机(或主站)中发生超时错误。客户机(或主站)可以继续发送轮询程序完成报文来确定是否完成处理。 |
| 06 | 从属设备忙 | 与编程命令一起使用。服务器(或从站)正在处理长持续时间的程序命令。当服务器(或从站)空闲时，用户(或主站)应该稍后重新传输报文。 |
| 08 | 存储奇偶性差错 | 与功能码 20 和 21 以及参考类型 6 一起使用，指示扩展文件区不能通过一致性校验。<br>服务器(或从站)设法读取记录文件，但是在存储器中发现一个奇偶校验错误。客户机(或主方)可以重新发送请求，但可以在服务器(或从站)设备上要求服务。 |
| 0A | 不可用网关路径 | 与网关一起使用，指示网关不能为处理请求分配输入端口至输出端口的内部通信路径。通常意味着网关是错误配置的或过载的。 |
| 0B | 网关目标设备响应失败 | 与网关一起使用，指示没有从目标设备中获得响应。通常意味着设备未在网络3中。 |