1. 协议框架：（该协议是在modbus协议基础上扩展得出，红色部分为扩展内容）

服务器请求报文：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 群组识别号 | 从机地址 | 功能码 | 数据区 | CRC |
| ICCID(10字节) | 1字节 | 1字节 | N字节 | 2字节 |

支持的功能码：

03：读取保持寄存器；

06：预置单个寄存器；

16：预置多个寄存器；

DTU正常应答报文：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 群组识别号 | 从机地址 | 功能码 | 数据长度 | 回传数据内容 | CRC |
| ICCID(10字节) | 1字节 | 1字节 | 1字节 | N字节 | 2字节 |

备注：

1. CRC计算的是除了群组识别号和CRC区外的其他数据；
2. 群组识别号作为DTU的唯一标识，用于区分组号；
3. 从机地址1~16分别对应一台DTU下的设备；其中从机地址0对应DTU本身，用于修改DTU本身参数；地址0xff为广播地址，用于统一修改参数使用。

命令示例：服务器下发命令，设置10号设备进入云端模式

服务器下发：向10号设备110地址写入1。

89 86 02 84 03 16 30 03 13 70 0A 06 00 6E 00 01 AC 28

DTU应答：

89 86 02 84 03 16 30 03 13 70 0A 06 00 6E 00 01 AC 28

1. 心跳协议内容框架：

心跳默认3分钟一次（可更改），主要为了保持DTU与服务器的长链接，同时报送DTU存储的状态信息，无需服务器应答。

|  |  |
| --- | --- |
| 设备地址 | ICCID(10字节) |
| 备用 | 1字节 |
| 心跳功能码 | 1字节，0xFF |
| 心跳周期 | 2字节，单位秒 |
| DTU下从设备总数,N | 1字节，最多16 |
| DTU下在线从设备总数,M | 1字节，最多16 |
| DTU下从设备在线标志 | 4字节，共32位，每一位代表一个设备 |
| 设备1状态 | 6字节，485链接断开时填充0 |
| 设备2状态 | 6字节，485链接断开时填充0 |
| …… |  |
| 设备N状态 | 6字节，485链接断开时填充0 |

从设备状态信息定义：

|  |  |
| --- | --- |
| PM2.5数值 | 2字节 |
| 滤网剩余天数 | 2字节 |
| 开关状态 | 1字节 |
| 工作模式 | 1字节 |

1. CRC计算方法：

uint16\_t CRC16\_Modbus(uint8\_t \*buf, uint16\_t len)

{

uint16\_t crc=0xFFFF;

uint16\_t i, j;

for(j=0;j<len;j++)

{

crc=crc ^\*buf++;

for(i=0;i<8;i++)

{

if((crc&0x0001)>0)

{

crc=crc>>1;

crc=crc^0xa001;

}

else

{

crc=crc>>1;

}

}

}

return (crc);

}

1. MODBUS寄存器定义：

参见MODBUS地址定义表.