SRWF-6009通信协议

Version 1.0

贰叁玖陆

|  |  |
| --- | --- |
| 项目名称： | SRWF-6009 |
| 创建时间： | 2015-08-22 |
| 修改时间： | 2015-08-22 |

上海桑锐电子科技有限公司

# 修改历史

|  |  |  |  |
| --- | --- | --- | --- |
| 版本/状态 | 修订人 | 修改日期 | 备注 |
| 初稿 | 张吉太 | 2015.9.13 | 协议制定 |
|  | 张吉太 | 2016-7-15 | 增加有线调试协议 |
|  | 张吉太 | 2016-7-21 | 修改表端模块主动上传数据的数据类型编号，见4.1章节 |
|  | 张吉太 | 2016-7-22 | 修改UART的通信协议，详见6章节 |
|  | 张吉太 | 2016-8-26 | 增加RF休眠策略协议定义 |
|  | 张吉太 | 2016-9-13 | 增加注释22中的模块测试状态 |
|  | 张吉太 | 2016-10-12 | 增加模块工作时间段功能 |
|  | 张吉太 | 2017-02-12 | 修改冻结数据数据结构 |
|  | 张吉太 | 2017-02-21 | 增加RF修改表ID的功能 |
|  | 张吉太 | 2017-09-04 | 数据帧的CRC8修改为CRC16 |
|  | 张吉太 | 2017-11-29 | 在集中器应答ACK中增加设置命令 |
|  | 张吉太 | 2019-03-11 | 增加NB相关命令 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 目录

1 系统通讯网络结构图 7

2 UART端口 7

3 协议的格式 8

包结构 **错误!未定义书签。**

注释1：报文标识 8

注释2：设备类型 9

注释3：路径级数以及当前位置 9

注释4：传输路径注释 10

注释5：计量传感器类型及信道（长度：1byte） 11

注释6：脉冲系数 11

注释7：表读数的数据格式 12

注释8：信号强度下行注释 14

注释9：信号强度上行注释 14

注释10：数据包中的符号说明 14

注释11：表ID的Bcd码说明 15

注释12：各类设备的Bcd编码规则 15

注释13：告警状态、阀状态和EEPROM状态 16

注释14：返回的操作代码一般含义 18

注释15：通讯协议中的存储格式约定 19

注释16：运营商编号在RF通讯的作用和用法 19

注释17：串口传给透传模块的RF发射数据格式 21

注释18：对于RF应答数据过长的处理 22

注释19：表端功能使能位定义 22

4 协议的表端无线命令列表 23

详见注释7：表读数的数据格式(默认0) 23

4: 报警上传数据 **错误!未定义书签。**

详见注释7：读冻结数的数据格式 25

A.读正转数据：01 25

默认：0 25

详见注释7：读冻结数的数据格式 25

A.读正转数据：01 25

详见：注释19：表端运行参数位定义 35

详见：注释7：表读数的数据格式中的定时定量数据格式。 53

5 协议的集中器、中继器无线命令列表 54

5.1. 读取集中器版本信息 0x40 54

5.2. 读取集中器ID 0x41 54

5.3. 写入集中器ID 0x42 54

5.4. 读集中器时钟 0x43 55

5.5. 写集中器时钟 0x44 55

5.6. 读GPRS参数 0x45 56

5.7. 写GPRS参数 0x46 57

5.8. 读GPRS信号强度 0x47 57

5.9. 集中器初始化 0x48 58

5.10. 读集中器工作模式参数 0x49 59

5.11. 写集中器工作模式参数 0x4A 60

5.12. 集中器请求时间 0x4B 61

5.13. 集中器重新启动 0x4C 62

5.14. 集中器数据转发 0x4D 62

5.15. 读设备档案数量 0x50 63

5.16. 读设备档案信息 0x51 63

5.17. 写设备档案信息 0x52 64

5.18. 删除设备档案信息 0x53 65

5.19. 修改设备档案信息 0x54 66

5.20. 读设备自定义路由信息 0x55 66

5.21. 写设备自定义路由信息 0x56 67

5.22. 批量读设备自定义路由信息 0x57 68

5.23. 批量写设备自定义路由信息 0x58 69

5.24. 定时定量数据主动上传 0x61 70

5.25. 冻结数据主动上传 0x62 71

5.26. 读集中器中的定时定量数据 0x63 72

5.27. 读集中器中的冻结数据 0x64 72

5.28. 批量读集中器中的定时定量数据 0x65 73

5.29. 批量读集中器中的冻结数据 0x66 74

5.30. 集中器程序升级0xF1 75

5.31. 集中器监控控制0xF2 76

5.32. EEPROM存储区检查0xF3 76

6 UART表端模块测试系统通讯协议（软件校准RF参数） 54

7 表端的数据存储 94

水表EEPROM的存储结构（存储空间：4Kbyte） 94

8 BootLoader说明 99

8.1 协议说明 99

8.2 升级协议 100

8.3 升级步骤 100

高字节气表电压值，低字节水表电压值 103

(37+3个空格) 103

程序版本的CRC16，程序接收数据包时使用 103

低字节在前 103

RXD信道，默认3信道 103

高字节气表电压值，低字节水表电压值 104

(37+3个空格) 104

程序版本的CRC16，程序接收数据包时使用 104

低字节在前 104

RXD信道，0或1 104

低字节在前 105

低字节在前 105

8.4 广播升级步骤 107

9 通讯网络的特点 107

9.1 集中管理，维护方便 107

9.2 简单有保障 108

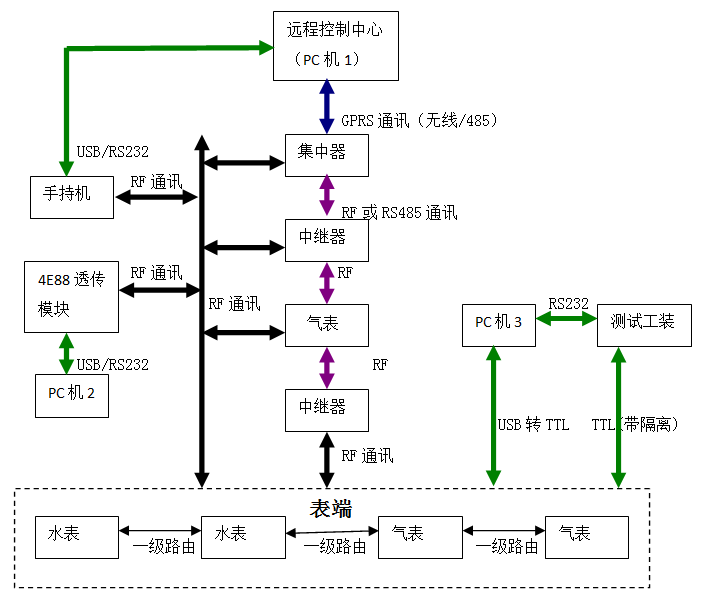
9.3 组网过程 108

9.4 表端的主动上报数据 108

9.5 表端的主要接收命令 109

9.6 网内各类设备通信频率 109

# 系统通讯网络结构图



# UART端口

表端UART设置：9600bps、数据位：8、偶校验、停止位：1

主机UART设置：9600bps、数据位：8、偶校验、停止位：1

# 协议的格式

## 协议格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **字节** |  | **说明** |
| 重复N次 | 前导码 | 24 |  | 24字节前导码 |
| 表ID短地址 | 2 |  | 接收者地址的CRC16 |
| 0 | 同步码 | 2 |  | 0xD30x91 |
| 1 | 包长 | 2 |  | **低12位存储包长：最大值4095**  **高4：预留** |
| 2 | 报文标识 | 1 | 详细注释**1**‘报文标识注释’ |
| 3 | 任务号 | 1 | 包序号，两者之间通信，发送方自累计，广播包用来源方的任务号，中间不变更,自组网用 |
| 4 | 命令字 | 1 | 加密区域 | 通信命令标识符 |
| 5 | 设备类型 | 1 | 命令发起方的设备类型，详见注释**2**‘设备类型注释’ |
| 6 | 生命周期 | 1 | bit0- bit 3:低四位存储生命周期，最大15，过一个路由器减一，为零后丢弃。  bit4- bit7:指定应答方回复的信道，  数据上行时：指集中器ACK应答信道，默认：8信道  数据下行时：指集中器指定表上报的信道，默认：3信道，当自动信道功能打开时启用。 |
| 7 | 路径信息 | 1 | 详见注释**3**：‘路径级数以及当前位置’ |
| 8 | 传输路径 | 6\*n | 详见注释**4**：‘传输路径注释’，最高3级 |
| 9 | 数据域 | N | 变长，内容与命令有关。 |
| 10 | 下行信号强度 | 1 | 详见注释**5**：‘信号强度下行注释’ |
| 11 | 上行信号强度 | 1 | 详见注释**6**：‘信号强度上行注释’ |
| 12 | 校验字 | 2 |  | 1到11数值的CRC16校验 |
| **13** | **结束符** | **1** | **数据帧结束标识符0x16** |
| 14 | 导言长度标识 | 1 | **主机识别码** | 0x1E: 表示主机需要向空中发送30轮唤醒导言+CRC16 |
| 15 | TX通讯信道 | 1 | 默认信道为：3 |
| 16 | RX通讯信道 | 1 | 默认：25（兼容老集中器时用） |

## 注释1：报文标识

|  |  |  |
| --- | --- | --- |
| 占用位 | 用途 | 含义 |
| Bit0 | CRC校验标志位 | 0：CRC8校验；1：CRC16校验 |
| Bit1 | 地址长度标志位 | 0：ID长度为6字节，1：ID长度为8字节 |
| Bit2 | 接收方休眠 | 0:不休眠。1:休眠设备，需要唤醒 |
| Bit3 | 发送方休眠 | 0:不休眠。1:休眠设备，需要唤醒 |
| Bit 4 | 是否需要回执 | 0：不需回执; 1: 需要回执 |
| Bit 5 | 密标志 | 0:非加密； 1: 加密（AES128加密） |
| Bit 6 | 帧类型 | 0 :命令帧; 1：应答帧 |
| Bit7 | 数据方向 | 0 :下行; 1：上行 |

## 注释2：设备类型

原始数据发出者的设备类型，如抄表命令的发起者。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备编码** | | **设备名称** | | **设备大类** |
| 0x1X | 冷水表 | RF水表 | 0x10 | 居民水表（包括口径：Φ15、Φ20、Φ25、） |
| GPRS水表 | 0x11 | 居民水表（包括口径：Φ15、Φ20、Φ25、） |
| NB-IOT水表 | 0x12 | 居民水表（包括口径：Φ15、Φ20、Φ25、） |
| 0x2X | 热水表 | RF热水表 | 0x20 |  |
| NB-IOT水表 | 0x21 | 热水表（包括口径：Φ15、Φ20、Φ25、） |
| 0x3X | 燃气表 | RF气表 | 0x30 | 居民气表（包括口径：Φ15、Φ20、Φ25、） |
| GPRS气表 | 0x31 | 居民气表（包括口径：Φ15、Φ20、Φ25、） |
| NB-IOT水表 | 0x32 | 居民气表（包括口径：Φ15、Φ20、Φ25、） |
| 0x4X | 电表 | 电表 | 0x40 | 电表 |
|  |  |  |  |  |
| 0x5x | 透传 | 水处理设备 | 0X50 | 串口通信的设备类型 |
| 变频器 | 0X50 |  |
| 0xFx | 0xF9 | USB |  | 有线数据 |
| 0xFA | 上位机器 |  | PC调试软件 |
| 0xFB | UART串口 |  | 串口，有线数据 |
| 0xFC | 集中器 |  | 集中器 |
| 0xFD | 中继器 |  | 中继器 |
| 0xFE | 手持 |  | 手持 |

## 注释3：路径级数以及当前位置

|  |  |  |  |
| --- | --- | --- | --- |
| NO |  | 项目 | 说明 |
|  | Bit0、Bit 1、Bit 2、Bit3 | 路径级数 | 路径的级数，最小值为2 |
| Bit4、Bit5、Bit6、 Bit7 | 当前位置 | 发件人在全路径中的位置，以0开始编号 |

## 注释4：传输路径注释

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 路由长度 | 级数 | 备注 |
| 0 | 1到6 | 来源地址（命令发起人ID） | “控制字”中低四位表示路由级数（最大为3级），路由级数为2时，域中只有发起人ID和终端ID。  数据域里的ID，为全路径ID,先后排序为：命令发起人ID🡺路由ID1🡺路由ID2🡺  。。。🡺终端ID |
| 1 | 7到12 | 指定1级路由ID |
| 2 | 13到18 | 指定2级路由ID |
| 3 | 19到24 | 指定3级路由ID |
| 4 | 15到30 | 目标端地址（终端ID） |

对于表端上传来说：传输路径是指存储的路径或下发包中路径的反向路径, 当前位置位置为0。

对于中继器、集中器来说，传输路径要分是来路由路径还是不带路由路径，我们目前是带路由路径的全路径。

## 注释5：计量传感器类型及信道（计量传感器类型长度：1byte，信道长度：1byte）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NO | | 编号 | 类型 | 备注3 |
| 1 | 计量传感器类型  （1byte） | 0 | 单干簧管传感器/霍尔传感器 |  |
| 1 | 双干簧管传感器/霍尔传感器 |  |
| 2 | 三干簧管传感器/霍尔传感器 |  |
| 3 | 骏普4位光电直读传感器 | 三川 |
| 4 | 厚膜直读表头 | 山科 |
| 5 | 骏普1位光电直读传感器 | 三川 |
| 6 | 188协议光电直读 | 宁波水表 |
| 7 | 188协议无磁直读 | 宁波水表 |
| 8 | 2霍尔竟达传感器 | 杭州竟达 |
| 9 |  |  |
| 10 |  |  |

**系统信道定义**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 信道组 | 网络信道 | | 表端信道 | | | | 信道组说明 |
| 扩频因子 | 频率(MHz) | 扩频因子 | | 频率(MHz) | |
| Rx | Tx | RX | TX |
| 0 | Rx/Tx:9 | 488.7 | 9 | 11 | 490.39 | 495.5 | 公共信道组 |
| 1 | Rx/Tx:9 | 488.5 | 9 | 11 | 491.17 | 495.72 | 工作信道组 |
| 2 | Rx/Tx:9 | 488.3 | 9 | 11 | 491.95 | 495.94 |
| 3 | Rx/Tx:9 | 488.1 | 9 | 11 | 492.73 | 496.16 |
| 4 | Rx/Tx:9 | 487.9 | 9 | 11 | 493.51 | 496.38 |
| 5 | Rx/Tx:9 | 487.7 | 9 | 11 | 494.29 | 496.6 |
| 6 | Rx/Tx:9 | 487.5 | 9 | 11 | 495.07 | 496.82 |
| 7 | Rx/Tx:9 | 487.3 | 9 | 11 | 499.58 | 497.04 |
| 8 | Rx/Tx:9 | 487.1 | 9 | 11 | **500.36** | **497.26** |
| **509.48** |
| 9 | Rx/Tx:9 | 486.9 | 9 | 11 | 501.14 | 497.48 |
| A | Rx/Tx:9 | 486.7 | 9 | 11 | 501.92 | 497.7 |
| B | Rx/Tx:9 | 486.5 | 9 | 11 | 502.70 | 497.92 |
| C | Rx/Tx:9 | 486.3 | 9 | 11 | 503.48 | 498.14 |
| D | Rx/Tx:9 | 486.1 | 9 | 11 | 504.26 | 498.36 |
| E | Rx/Tx:9 | 485.9 | 9 | 11 | 505.04 | 498.58 |
| F | Rx/Tx:9 | 485.7 | 9 | 11 | 505.82 | 498.8 |
| **10** |  |  | **7** | **8** | 491.46 | 490.25 | RF升级信道 |

◆**自动信道：**打开模块的自动信道功能，模块会根据表ID最后1位设置自己的通讯信道，对应信道如下：

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 示例表号 | 表端信道号 | 注释 |
| 1 | 10171114000**0** | 0 | 对应频率见表端信道 |
| 2 | 10171114000**1** | 1 | 对应频率见表端信道 |
| 3 | 10171114000**2** | 2 | 对应频率见表端信道 |
| 4 | 10171114000**3** | 3 | 对应频率见表端信道 |
| 5 | 10171114000**4** | 4 | 对应频率见表端信道 |
| 6 | 10171114000**5** | 5 | 对应频率见表端信道 |
| 7 | 10171114000**6** | 6 | 对应频率见表端信道 |
| 8 | 10171114000**7** | 7 | 对应频率见表端信道 |
| 9 | 10171114000**8** | 8 | 对应频率见表端信道 |
| 10 | 10171114000**9** | 9 | 对应频率见表端信道 |

## 注释6：脉冲系数

0 - 1个脉冲一方（吨）

1 - 10个脉冲一方（吨）

2 - 100个脉冲一方（吨）

3 - 1000个脉冲一方（吨）

## 注释7：表读数的数据格式

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 表类型 | 格式类型 | 序号 | 数据段名称 | 大小 | 实时数据长度：20 |
| 说明 |
| 水气表 | 抄表时返回的数据、定时定量上传的数据，故障告警数据  **实时0** | 1 | 正转用量 | 6 | 4位整数，2字节小数，  **如：FF 98 00 00 F4 01==》》39167.5** |
| 2 | 反转用量 | 6 |  |
| 3 | 报警状态 | 2 | 告警状态字1，告警状态字2 |
| 4 | 阀状态 | 1 |  |
| 5 | 电池电压 | 1 | >= 0xF0,表示备用电池供电  **10进制直接表示，如36**🡺3.6V |
| 6 | 模块的当前环境温度 | 1 | 模块的当前环境温度。0x16 ==>> 22℃ |
| 7 | SNR | 1 | Bit7为0：**其Bit0—Bit6的值为正数，如0x0A ==>>10**  Bit7为1：**其Bit0—Bit6的值为负数，如0x8A ==>> -10** |
| 8 | 抄表信道和上报信道 | 1 | 户表模块抄表信道和上报信道，默认：0x33  高字节bit7---bit4：抄表通讯信道  低字节bit3---bit0：主动上报信道，自动信道功能打开时，该信道是集中器分配的，关闭时该信道默认和抄表信道一致。 |
| 9 | 当前协议的版本号 | 1 | 版本号从0开始，255结束 |
| 冻结数据格式  **01** | 1 | 冻结数据的起始序号 | 1 | Bit7——Bit0：定义如下：  0：代表倒数第一天1天冻结数据  1：代表倒数第一天2天冻结数据  2：代表倒数第一天3天冻结数据  3：代表倒数第一天4天冻结数据  4：代表倒数第一天5天冻结数据  5：代表倒数第一天6天冻结数据  6：代表倒数第一天7天冻结数据  7：代表倒数第一天8天冻结数据  8：代表倒数第一天9天冻结数据  9：代表倒数第一天10天冻结数据 |
| 6 | 冻结的用量数据 | 104 | 单次上传1天冻结数据  数据格式如下：   |  |  |  | | --- | --- | --- | | 项目 | 长度 | 注释 | | 4byte时间信息 | 4 | 月、日、时、分 | | 6byte0：00累计用量数据 | 6 | 全字节累计用量 | | 0：00到0：30的增量 | 2 | 低字节在前,最小单位L | | 0：30到1：00的增量 | 2 | | 1：00到1：30的增量 | 2 | | 1：30到2：00的增量 | 2 | | 2：00到2：30的增量 | 2 | | 。。。。 | 2 | | 23：00到23：30的增量 | 2 | |
| 7 | 报警状态 | 2 | 告警状态字1，告警状态字2 |
| 8 | 阀状态 | 1 |  |
| 9 | 电池电压 | 1 | >= 0xF0,表示备用电池供电  **10进制直接表示，如36**🡺3.6V |
| 10 | 模块的当前环境温度 | 1 | 模块的当前环境温度。0x16 ==>> 22℃ |
| 11 | SNR | 1 | Bit7为0：**其Bit0—Bit6的值为正数，如0x0A ==>>10**  Bit7为1：**其Bit0—Bit6的值为负数，如0x8A ==>> -10** |
| 12 | RXD信道和TXD信道 | 1 | 户表模块抄表信道和上报信道，默认：0x33  高字节bit7---bit4：抄表通讯信道  低字节bit3---bit0：主动上报信道，自动信道功能打开时，该信道是集中器分配的，关闭时该信道默认和抄表信道一致。 |
| 13 | 当前协议的版本号 | 1 | 版本号从0开始，255结束 |
| 热量表 | 待定 |  |  |  |  |
| 电表 | 待定 |  |  |  |  |
|  |  |  |  |  |  |
| 水处理  设备 | 0x80 |  | 状态上报标志 |  |  |
| 0x81 |  | 报警上报标志 |  |  |
| 变频器 | 0x82 |  | 状态上报标志 |  |  |
| 0x83 |  | 报警上报标志 |  |  |
| 集中器应答ACK | 0xA0 |  | 应答数据标志， | 24+n | 集中器收到上报数据后，回应的应答数据标志。 |
| 集中器应答命令帧 | 0xA1 |  | 功能设置数据帧标志 | 24+n | 集中器收到上报数据后，下发设置命令，此命令需要表端应答。 |
|  |  |  |  |  |  |

## 注释8：信号强度下行注释

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 长度 | 项目 | 备注 |
| 1 | 1字节 | 信号强度下行 | 主机下发的命令，用16进制表示（0X20=>> -32dBm）  当路由抄表时信号强度为：与表通讯的路由器，它们之间通讯信号强度 |

## 注释9：信号强度上行注释

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 长度 | 项目 | 备注 |
| 1 | 1字节 | 信号强度上行 | 终端返回的命令，用16进制表示（0X20=>> -32dBm）  当路由抄表时信号强度为：与表通讯的路由器，它们之间通讯信号强度 |

## 注释10：数据包中的符号说明

|  |  |
| --- | --- |
| **符号** | **含义** |
| TL TL | 包长 |
| TN | 任务号 |
| XX | 校验字 |
| AC | 报文标识 |
| LL | 数据域长度 |
| CD | 命令字(CD宏可以减少命令字的重排带来的变动) |
| DV | 设备类型 |
| RV | 控制字2 |
| R1 | 信号强度下行 |
| R2 | 信号强度上行 |
| 00 01 00 00 00 SR | 发件人地址 |
| 00 01 00 00 00 DE | 收件人地址 |
| 00 00 01 00 00 00 FN | 目标地址 |

## 注释11：表ID的Bcd码说明

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO | 类型 | 长度 | 关键字 | 短地址 | 注释 |
| 1 | 表具ID【高字节在前) | 6字节 |  |  | 压缩BCD码 |
| 2 | 无效ID | 6字节 | FF FFFFFFFFFF |  |  |
| 3 | 广播地址ID | 6字节 | D4 D4D4D4D4D4 | 0xBECF | 广播组网时使用 |
| 4 | 主动上传时的默认集中器地址 | 6字节 | D5 D5D5D5D5D5 |  | 表中未保存集中器ID |
| 5 | 广播抄表和升级时的广播ID | 6字节 | D6 D6D6D6D6D6 |  | 广播时的表端ID |
| 6 | 主控模块地址 | 6字节 | D7 D7D7D7D7D7 |  | UART有线通信 |
| 7 |  |  |  |  |  |

为确保广播地址对应的CRC16的唯一，广播地址对应的CRC16 为：0xBECF, 同时修改CRC16的算法，值为0xBECF并且不是广播地址的CRC16减一。

## 注释12：各类设备的Bcd编码规则

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备大类 | 年 | 月 | 日 | 自动编号 |
| BT | YY | MM | DD | XXXX |

BT的内容可根据需要设置，后5个字节作为设备的标识ID.

BT的设置：

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 电池供电下的编码 | | 交流供电下的编码 |
| 冷水表 | 0x10 | RF户表 | / |
| 0X11 | GPRS户表 |  |
| 热水表 | 0x20 | RF户表 | / |
| 0x21 | GPRS户表 |  |
| 气表 | 0x30 | RF户表 |  |
| 0x31 | GPRS户表 |  |
| 路由器 | 0x40 | 电池供电中继器 | / |
| 0x41 | AC220供电中继器 |  |
| 手持 | 0x50 |  |  |
| 集中器 | 0x60 |  | / |
| 上位机器 | 0x70 |  | / |
| 空类型 | 0x00 |  | 0x00 |

## 注释13：告警状态、阀状态和EEPROM状态

|  |  |  |
| --- | --- | --- |
| 2个字节 | 表告警状态 | 告警状态字1：  Bit0：干簧管故障  Bit1：阀门故障  Bit2：水表传感器线断开  Bit3：电池欠压  Bit4：预留  Bit5：磁干扰标志  Bit6：光电直读表坏  Bit7：光电直读表被强光干扰  告警状态字2：GASMETER  Bit0：水表反转  Bit1：水表被拆卸  Bit2：水表被垂直安装  Bit3： EEPROM异常  Bit4：煤气泄漏  Bit5：欠费标志  Bit6-7：预留 |
| 1个字节 | 阀状态  及  LCD故障提示 | **BIT0、BIT1位：**  00：阀门故障  01：开阀  10：关阀  11：阀门未知  **BIT2位：**预留  **BIT3位：**预留  **BIT4～BIT7位功能定义如下：**  E0（Error 0）:预付费功能未打开。在预付费功能关闭状态下，按显示按键LCD屏在应缴金额、剩余、用气价格显示E0提示符。  E1（Error1）: 预留 |
| 1字节 | 电池电压 | **10进制直接表示，如36**🡺3.6V |

## 注释14：返回的操作代码一般含义

|  |  |
| --- | --- |
| **返回代码** | **信息** |
| 0xAA | 操作成功 |
| 0xAB | 操作失败 |
| 0xAC | 通讯失败 |
| 0xAD | 命令下达成功 |
| 0xAE | 数据包格式错误或无法识别的命令 |
| 0xAF | 时间异常 |
| 0xBA | 对象不存在 |
| 0xBB | 对象重复 |
| 0xBC | 对象已满 |
| 0xBD | 参数错误 |
| OxCC | 超时错误 |
| OxCD | 单轮运行超时错误 |
| OxCE | 正在执行 |
| OxCF | 操作已处理 |
| OxD0 | 已应答 |
| OxD1 | 抄取表数据错误 |
| OxD2 | 没有此项功能 |
| OxD3 | 网络未注册或节点无法识别 |
| OxD4 | 网络用户码错误 |
| OxD5 | 校验码错误 |
| OxD6 | 数据禁止访问 |
| OxD7 | 未知错误 |
| OxD8 |  |

## 注释15：通讯协议中的存储格式约定

无特别声明情况下按如下约定存储：

1. 所有的数字都按16进制存储
2. 所有整数都按低字节在前，高字节在后的顺序存储
3. 前导码中CRC16（2字节）以及数据包中的包长（2字节）按整数格式存储
4. 用量

在EEPROM的存储格式: 一个32位的整数 = 用量整数 \* 脉冲系数 +用量小数

在RF通讯协议中的格式: 4字节的整数、 2字节的小数

1. 日期、时间按年、月、日、时、分、秒的Bcd码格式存储
2. 设备号是按设备号的顺序存储的

注：

上位机软件或手持机软件在收到数据包后，要将信息以适当的方式展现出来。

没有特别说明表端的存储格式也是按上述约定存储的，除了时间、日期。

## 注释16：运营商编号在RF通讯的作用和用法

### 运营商编号在RF通讯的作用

为了防止其他运营商设备发出的RF命令不能操纵本运营商的设备，特将本运营商编号作为键值加工RF的报文数据，接收方只有知道关键值才能正确解包。**本运营商上所有设备的运营商编号都必须设为一致。**

### 发送端的数据组织步骤

组装报文🡪加密报文数据域(根据需要) 🡪根据运营商编号加密报文(从报文标识后加密)

|  |
| --- |
| 示例代码1 |
| packBuffer = GenDataPacket(...); // 组织报文数据,根据需要，报文的数据数据域数据可能要加密  // carrierNo设备上存储的运营商编号  rawPackLen = GetPackLength(packBuffer);  rf.txCrc16 = comCalCRC16(packBuffer+14,6);  packLen = GetPackLength(packBuffer);  if( pTask->u8DataBuffer[PACKIDX\_CmdID] != 0x21 ) // 不是‘设置运营商编号’命令要加工(亦或)报文  CarrierXorPacket(packBuffer,carrierNo,0,true);  else  Pack\_SetCarrierNotXOR(packBuffer,1); // 参看‘报文标识’描述  rf.packLength = newPackLen; // 新的要发射的报文长度 |

### 接收端的数据解包步骤

根据运营商编号解密报文(从报文标识后加密) 🡪解密报文数据域(根据需要) 🡪得到原始报文

|  |
| --- |
| 示例代码2 |
| uint8 decodedLen,tmpBuf[PHY\_DECODE\_UNIT\_24],decodedBuf[RF\_BUFFER\_SIZE];  uint16 lengthOut;  uint8 xorRs;  if( Pack\_GetCarrierNotXOR(decodedBuf[2]) == 0 ) // 需要异或  {  xorRs = CarrierXorPacket(decodedBuf,carrierNo,lengthOut,false);  if( xorRs != 0 ) // 报文不合法  {  // RFRxStop();  // DestroyTask(pTask);  return;  }  }  if( !(memcmp(myDeviceID,decodedBuf+lastBcdPos,LONG\_ADDR\_SIZE) == 0  || bcdIsBrodcast(decodedBuf+lastBcdPos) ) ) // 不是发给自己的报文，终止接收  {  // RFRxStop();  // DestroyTask(pTask);  return;  }  RFRxStop();  ....  PackDisposal(decodedBuf); // 处理报文  .... |

上述事例中涉及到运营商编号作为键值加工的函数：CarrierXorPacket, Pack\_SetCarrierNotXOR, Pack\_GetCarrierNotXOR可参见6009 工程中‘msgpack.h’和‘msgpack.C’

## 注释17：串口传给透传模块的RF发射数据格式

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| D3 91 | 数据报文正文 | 1个字节的导言组数 | 1个字节的主机TX信道号 |

## 注释18：对于RF应答数据过长的处理

由于RF发射包的长度控制在255个字节以内，报文有效正文的长度也受到限制。出于保护RF安全发射和数据的完整性，对于返回数据过长的请求（非分包传递请求命令），系统的RF应答正文只有一个字节：格式错误（0xAE）。

## 注释19：表端功能使能位定义

|  |  |  |
| --- | --- | --- |
| NO | 功能描述 | 备注 |
| 0 | Bit0：开启磁干扰关阀功能 |  |
|  | Bit1：开启主动上报的数据帧加密功能 |  |
|  | Bit2：开启/关闭防拆卸和垂直安装检测功能 |  |
|  | Bit3：打开LORAWAN模块发射 | LORAWAN模块的打开或关闭 |
|  | Bit4：开启/关闭主动告警/主动上传 | 打开/关闭,表端告警,定时定量 |
|  | Bit5：开启主动上报冻结数据 |  |
|  | Bit6：开启/关闭透支关阀功能 |  |
|  | Bit7：开启预付费功能 |  |
|  | Bit0：**打开自动信道分配功能** | 模块根据表号的最后一位分配相应信道。 |
|  | Bit1：开启/关闭防锈功能 |  |
|  | Bit2：开启掉电关阀功能 |  |
|  | Bit3：启用RF休眠策略 | 打开关闭实时通讯功能 |
|  | **Bit4:预留** |  |
|  | Bit5: 是否检测煤气泄露 |  |
|  | **Bit6:预留** |  |
|  | Bit7:开启/关闭流速控制 |  |

## 注释20：预付费用量信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 38 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 期初表底数 | 6 | 4整数2小数 |
| 1 | 期初预付费余额 | 3 | 2整数1小数 |
| 2 | 目前读数 | 6 | 4整数2小数 |
| 3 | 本期目前用量 | 6 | 4整数2小数 |
| 4 | 目前预付费余额 | 3 | 2整数+1小数 |
| 5 | 剩余用量 | 6 | 4整数2小数 |
| 6 | 本期最大剩余用量 | 6 | 4整数2小数 |
| 7 | 当前计费价格 | 2 | 1整数+1小数 |

## 注释21：阶梯结算价目表

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 45 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 状态 | 1 | 0：还未设价格表 1: 单一价格;2:阶梯价格 |
| 1 | 价格执行日期 | 4 |  |
| 2 | 阶梯价格 | 4\*10 | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |

## 注释22：写入充值数据

**备注：**数据域中的内容是要加密的,充值序号是防止多次充值的

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6/11 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 充值序号 | 2 | 1字节的充值网点+1字节的充值序号 |
| 1 | 充值额 | 3 | 单位：分（可以为负，【1】的第23位为1表示负数） |
| 2 | 动态充值密码 | 6 | 动态充值密码是用来数据的合法信息 |
| 3 | 校验码 | 1 | 校验码 |

## 注释23：写入结算价目表

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段说明 | 段标识 | 段大小 |  |
| 0 | 价格执行日期 | 4 | YY YY MM DD |
| 1 | 阶梯价格 | 4\*10 | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |
| 2 | 动态充值密码 | 6 | 动态充值密码是用来数据的合法信息 |
| 3 | 校验码 | 1 | 校验码 |

# NB-IOT无线通信数据（包括红外/蓝牙通讯命令）

### NB主动上报数据格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | 同步码 | 2 |  | 0xD30x91 |
| 1 | 包长 | 2 |  | **低12位存储包长：最大值4095**  **高4：预留** |
| 2 | 报文标识 | 1 | 详细注释**1**‘报文标识注释’ |
| 3 | 任务号 | 1 | 包序号，发送方自累计，最大255 |
| 4 | 命令字 | 1 | 加密区域 | 通信命令标识符 |
| 5 | 设备类型 | 1 | 命令发起方的设备类型，详见注释**2**‘设备类型注释’ |
| 6 | 生命周期 | 1 | 预留 |
| 7 | 路径信息 | 1 | 预留 |
| 8 | SIM卡的CCID | 10 | 10byte:CCID，压缩BCD |
| NB模块的IMEI | 10 | 10byte:IMEI，压缩BCD |
| 9 | 数据域 | N | 变长，内容与命令有关。 |
| 10 | 下行信号强度 | 1 | 预留 |
| 11 | 上行信号强度 | 1 | 预留 |
| 12 | 校验字 | 2 |  | 1到11数值的CRC16校验 |

### NB心跳包的数据格式（命令字：0xA0）

#### 命令简介：

* + - 1. 读NB当前入网信息和入网状态

#### 心跳包数据格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 长度30 byte |
| 段序号 | 段标识 | 段大小 | 段说明， |
| 0 | Battery | 1 | Battery voltage |
| 1 | Signal power | 2 | **signal power in centibels（**高位为1为负数**）** |
| 2 | Total power | 2 | **total power in centibels（**高位为1为负数**）** |
| 3 | TX power | 2 | **current Tx power level in centibels** |
| 4 | TX time | 4 | **total Tx time since last reboot in millisecond** |
| 5 | RX time | 4 | **total Rx time since last reboot in millisecond** |
| 6 | Cell ID | 5 | **last cell ID** |
| 7 | ECL | 1 | **last ECL value** |
| 8 | SNR | 2 | **last snr value（**高位为1为负数**）** |
| 9 | EARFCN | 5 | **last earfcn value** |
| 10 | PCI | 2 | **last pci value** |
| 11 | RSRQ | 2 | **rsrq in centibels（**高位为1为负数**）** |
| 12 | OPERATOR  MODE | 1 |  |
| 13 | RegisterState | 1 | 0：入网失败（入网失败，上述入网信息全为0）  1:入网成功 |

实例数据：

Signal power:-936

Total power:-845

TX power:230

TX time:978

RX time:5377

Cell ID:186035666

ECL:1

SNR:3

EARFCN:2506

PCI:259

RSRQ:-137

OPERATOR MODE:4

数据域数据：

53 69 67 6E 61 6C 20 70 6F 77 65 72 3A 2D 39 33 360D 0A 54 6F 74 61 6C 20 70 6F 77 65 72 3A 2D 38 34 35 0D 0A 54 58 20 70 6F 77 65 72 3A32 33 30 0D 0A 54 58 20 74 69 6D 65 3A39 37 38 0D 0A 52 58 20 74 69 6D 65 3A35 33 37 370D 0A 43 65 6C 6C 20 49 44 3A31 38 36 30 33 35 36 36 36 0D 0A 45 43 4C 3A310D 0A 53 4E 52 3A330D 0A 45 41 52 46 43 4E 3A32 35 30 360D 0A 50 43 49 3A32 35 39 0D 0A 52 53 52 51 3A2D 31 33 370D 0A 4F 50 45 52 41 54 4F 52 20 4D 4F 44 45 3A34

原始数据报文：

### NB主动上传/下发的数据包格式（命令字：0XA1）

#### 命令简介：

#### 表端上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 当前的数据格式编号 | 1 | 1. 实时数据，表端主动上传标志 2. 冻结的数据，表端主动上传标志 3. 预留 4. 定时上传数据，表端主动上传标志 5. 定量上传数据，表端主动上传标志 6. 报警上传定时定量数据，表端主动上传标志 7. 报警上传冻结数据，表端主动上传标志 |
| 1 | 表端数据 | N | 详见注释7：表读数的数据格式 |
| 2 | 表端预付费用量信息 | N | 注释20：预付费用量信息 |
| 3 | 表端价目表 | N | 注释21：阶梯结算价目表 |
| 4 | 预留 | 15 | 预留 |
| 5 | Battery | 1 | Battery voltage |
| 6 | Signal power | 2 | **signal power in centibels（**高位为1为负数**）** |
| 7 | Total power | 2 | **total power in centibels（**高位为1为负数**）** |
| 8 | TX power | 2 | **current Tx power level in centibels** |
| 9 | TX time | 4 | **total Tx time since last reboot in millisecond** |
| 10 | RX time | 4 | **total Rx time since last reboot in millisecond** |
| 11 | Cell ID | 5 | **last cell ID** |
| 12 | ECL | 1 | **last ECL value** |
| 13 | SNR | 2 | **last snr value（**高位为1为负数**）** |
| 14 | EARFCN | 5 | **last earfcn value** |
| 15 | PCI | 2 | **last pci value** |
| 16 | RSRQ | 2 | **rsrq in centibels（**高位为1为负数**）** |
| 17 | OPERATOR  MODE | 1 |  |

#### 平台下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长：长度可 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 1 | 系统当前时间 | 7 | YY YYMM DD HH MM SS，用于校准户表时钟 |
| 2 | 下发预付费金额 | N | 注释22：写入充值数据 |
| 3 | 下发结算价目表 | N | 注释23：写入结算价目表 |
| 4 | 下发命令 | 1 | 协议的表端无线命令列表，  此字节值为0时，命令内容长度为空。 |
| 5 | 命令内容 | N | 见命令内容 |

### 读取NB主动上报的数据： 0x01

#### 命令简介：

* + - 1. 读用户用量：上位机实时读户表数据时使用的命令格式，数据域长度可以为1或24
      2. 集中器下发的应答帧和命令帧：终端户表定时定量上传数据时，主机接收成功后的应答数据格式
      3. 下发剩余用量和剩余价格：主机主动下发当前剩余用量和结算价格的数据格式。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长：长度可为1或24或24+N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读取的数据格式编号 | 1 | 详见注释7：表读数的数据格式(默认0) 集中器应答表主动上传数据时。   * + - 1. 0xA0 应答数据帧       2. 0xA1 命令数据帧 |
| 1 | 当前时间 | 7 | YY YYMM DD HH MM SS，用于校准户表时钟 |
| 2 | 预缴用量 | 6 | 根据用户缴费金额和单价计算出来的可用数据 |
| 3 | 参考起始用量 | 6 | 后台服务器在计算剩余用量时使用的户表当前累计参考量。 |
| 4 | 主动上传的时隙号 | 2 | 低字节在前，高字节在后  表端主动上报的时隙编号，表端根据此时隙编号上报数据 |
| 5 | 总表数据 | 2 | 低字节在前，高字节在后。此集中器下的总表数量 |
| 6 | 操作命令 | 1 | 相关命令见“4.协议的表端无线命令列表”0：没有操作命令 |
| 7 | 数据长度 | 1 | 值范围：≤15 |
| 8 | 数据内容 | N | 数据总长度≤8byte  根据命令字，随机变化，内容见“操作命令注释” |

带有RTC时钟的表端在收到数据后，可根据数据包中的时间校准时钟。

操作命令（下行）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能 | 说明 | 长度 | 注释:所有扩展命令总长度≤8byte |
| 1 | 设置信道 | 操作命令 | 1 | 值为：1 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 信道号 | 1 | Bit7:为1时设置信道，低7bit为信道号 |
| 2 | 打开自动信道 | 操作命令 | 1 | 值为：2 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 设置字 | 1 | Bit7:为0时，关闭自动信道功能  Bit7:为1时，打开自动信道功能 |
| 3 | 阀控 | 操作命令 | 1 | 值为：3 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 状态字 | 1 | 低四位：01：开阀；02：关阀 |
| 4 | 下发当前结算价格 | 操作命令 | 1 | 值为：4 |
| 数据长度 | 1 | 值为：4 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 结算价格 | 2 | 低位在前，高位在后  如：0x35 0x02 ==>> 2.35元 |
| 5 | 打开关闭实时抄表功能 | 操作命令 | 1 | 值为：2 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 设置字 | 1 | Bit7:为0时，关闭自动信道功能  Bit7:为1时，打开自动信道功能 |
| 6 |  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 当前的数据格式编号 | 1 | 1. 实时数据，表端主动上传标志 2. 冻结的数据，表端主动上传标志 3. 预留 4. 定时上传数据，表端主动上传标志 5. 定量上传数据，表端主动上传标志 6. 报警上传定时定量数据，表端主动上传标志 7. 报警上传冻结数据，表端主动上传标志 |
| 1 | 表端数据 | N | 详见注释7：表读数的数据格式 |
| 2 | Battery | 1 | Battery voltage |
| 3 | Signal power | 2 | **signal power in centibels（**高位为1为负数**）** |
| 4 | Total power | 2 | **total power in centibels（**高位为1为负数**）** |
| 5 | TX power | 2 | **current Tx power level in centibels** |
| 6 | TX time | 2 | **total Tx time since last reboot in millisecond** |
| 7 | RX time | 2 | **total Rx time since last reboot in millisecond** |
| 8 | Cell ID | 5 | **last cell ID** |
| 9 | ECL | 1 | **last ECL value** |
| 10 | SNR | 2 | **last snr value（**高位为1为负数**）** |
| 11 | EARFCN | 5 | **last earfcn value** |
| 12 | PCI | 2 | **last pci value** |
| 13 | RSRQ | 2 | **rsrq in centibels（**高位为1为负数**）** |
| 14 | OPERATOR  MODE | 1 |  |

操作命令（上行）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能 | 说明 | 长度 | 注释:所有扩展命令总长度≤8byte |
| 1 | 设置信道 | 操作命令 | 1 | 值为：1 |
| 操作结果 | 1 | 0xAA或0XAB |
| 信道号 | 1 | 低四位：上报信道  高四位：当前通信信道 |
| 2 | 打开自动信道 | 操作命令 | 1 | 值为：2 |
| 操作结果 | 1 | 0xAA或0XAB |
| 使能状态 | 2 | 见：“注释19” |
| 3 | 阀门控制 | 操作命令 | 1 | 值为：3 |
| 操作结果 | 1 | 0xAA或0XAB |
| 命令状态 | 1 | 见阀控状态 |
| 4 | 下发当前结算价格 | 操作命令 | 1 | 值为：4 |
| 操作结果 | 1 | 0xAA或0XAB |
| 当前结算价格 | 2 | 低位在前，高位在后  如：0x35 0x02 ==>> 2.35元 |
| 5 | 打开关闭实时抄表功能 | 操作命令 | 1 | 值为：2 |
| 操作结果 | 1 | 0xAA或0XAB |
| 使能状态 | 2 | 见：“注释19” |
| 6 |  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### 实例数据：

#### 注意事项：

当下发的剩余用量中参考起始用量大于表端累计用量时，表端模块返回的数据中，数据域只有一个0xAC，表示：剩余用量下发非法

### 读取NB心跳包的数据格式 0x02

#### 命令简介：

#### 冻结时间从0点开始，每隔30分钟冻结一次数据，每天冻结48条，10天滚动存储。

#### 每次只上传一天的数据。

#### 当读取的冻结数据时整数位为0xFF 0x FF 0x FE时，表示累计用量已达到最大值。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长：长度可为2或9 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读取的数据格式编号 | 1 | 详见注释7：读冻结数的数据格式A.读正转数据：01 B. 读反转数据：02 |
| 1 | 当前时间 | 7 | YY YY MM DD HH MM SS |
| 2 | 要读取的冻结数据起始序号 | 1 | 默认：0 详见注释7：读冻结数的数据格式 |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1或N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读取的数据格式编号 | 1 | 详见注释7：读冻结数的数据格式A.读正转数据：01 B. 读反转数据：02 |
| 1 | 冻结数据 | N | 详见注释7：表读数的数据格式 |

#### 实例数据

### 开关阀指令 0x03

#### 命令简介：

强制或正常开关阀，强制开关阀时，在动阀时不检测到位信号、磁干扰标识、欠压标志和当前的阀门状态。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 强制还是正常开关阀标志 | 1 | 01: 强制；00：正常 |
| 1 | 开阀还是关阀标志 | 1 | 01：开阀；00：关阀 |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 开关成功标志 | 1 | 0xAA：开/关阀成功,  0xAB：开/关阀失败  0xAD：表端接收命令成功 |
| 1 | 阀控失败的原因 | 2 | **低字节在前，高字节在后**  Bit0： 电池欠压  Bit1： 磁干扰中  Bit2：Adc正在工作  Bit3： 阀门正在运行中  Bit4： 阀门故障  Bit5： RF正在工作  Bit6：任务申请失败  Bit7：等待按键开阀  Bit8：当前阀门已经到位  Bit9：设备类型错误  Bit10：time 申请失败  Bit11：系统欠费  Bit12：  Bit13：  Bit14：  Bit15： |

#### 实例数据

### 读表端参数配置信息 0x04

#### 命令简介：

读表端运行时的相关参数值

#### 下行：空数据域

#### 上行数据：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 164 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 参数 | **164字节** | 注释22：数据域结构 |

### 清异常命令 0x05

#### 命令简介：

此命令可以一次性的清除模块告警信息

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 0 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 数据域空 |  |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作结果 | 1 | 详见：注释14：返回的操作代码一般含义 |

#### 实例数据

### 设置用量及脉冲系数 0x06

#### 命令简介：

略

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 用量 | 6 |  |
| 1 | 脉冲系数 | 1 | 0：脉冲系数为1  1：脉冲系数为10  2：脉冲系数为100  3：脉冲系数为1000 |

#### 上行命令

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7或1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 用量的 | 6 |  |
| 1 | 脉冲系数 | 1 |  |

#### 实例数据

### 测试命令 0x07

#### 命令简介

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令字 | 1 | 详见：**子命令字列表** |

#### 子命令字列表

|  |  |  |
| --- | --- | --- |
| 子命令字 | 参数说明 | 上行数据 |
| 0x01 | 读Debug信息 | 注释7：表读数的数据格式 |
| 0x02 | 清Debug信息 | 返回操作状态  **详见注释14：返回的操作代码一般含义** |
| 0x03 | 读取NB模组心跳包信息 | 数据格式相见0xA1命令 |
| 0x04 | 表端重启 | 返回操作状态  **详见注释14：返回的操作代码一般含义** |
| 0x05 | 读表端实时温度 | 一个字节的温度（可以是负数）  Bit7为0：表示bit0―bit6数据为正温度  Bit7为1：表示bit0―bit6数据为负温度  当表端检测温度错误时返回**0xff** |
| 0x07 | 读取系统实时电压 | 表端接收到此命令后，立刻检测电池电压，检测后返回其值 |
| 0x08 |  |  |
| 0x09 | 设置阀门过流电流值，超时时间 | 操作后返回其值  过流电流值： 1 个字节，单位：mA，为0 表示不设置  超时时间: 2 个字节，低字节在前，单位：ms,为0 表示不设置 |
| 0x0A |  |  |
| 0x0B |  |  |
| 0x0C | LED屏测试 | 0 SetLcdStatus(false)   1. SetLcdStatus(true)   2 ClearLcd   1. + 6个字节的数字显示数字   注：此命令为UART命令 |
| 0x0D | 设置流速控制 | 过大值(2, 方/每小时) 持续时间(1,分钟) 过小值(1,方/每100小时) 持续时间(1,小时) |
| 0x0E |  | 1字节的路径级数  6:N字节的理由表ID |
| 0x0F |  |  |
| 0x10 |  |  |
| 0x11 |  |  |
| 0x12 |  |  |
| 0x13 |  |  |
| 0x14 |  |  |
| 0x15 |  |  |
| 0x16 |  |  |
| 0x17 |  |  |
| 0x18 |  |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1+N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令字 | 1 | 详见：**子命令字列表** |
| 1 | 相关数据 | N | 详见：**子命令数据格式解析**中的相关命令格式注释 |

#### 子命令数据格式解析

##### Debug信息数据格式

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 项目名称 | 总长: | |
| 长度 | 注释 |
| 1 | 模块的发射总次数RF | 2 | 低字节在前 |
| 2 | 模块的接收总次数 | 2 |  |
| 3 | 模块的开/关阀门总次数 | 2 |  |
| 4 | 模块受到的磁干扰总次数 | 1 |  |
| 5 | EEPROM 写次数, 低字节在前 | 4 |  |
| 6 | 系统48小时复位次数 | 2 |  |
| 7 | 系统进入初始化次数 | 2 |  |
| 8 | 系统完成初始化次数 | 2 |  |
| 9 | 系统长时间不喂狗导致的初始化 | 2 |  |
| 10 | CDA检测信号超过100MS的次数 | 2 |  |
| 11 | 在检测到CDA信号后的接收超时次数 | 2 |  |
| 12 | A干簧管闭合的总脉冲数 | 2 |  |
| 13 | B干簧管闭合的总脉冲数 | 2 |  |
| 14 | ID校验错误 | 1 |  |
| 15 | 收到非法命令字 | 1 |  |
| 16 | 申请定时器失败 | 1 |  |
| 17 | 申请定时器失败的命令字 | 5 | 最多记录5条命令,滚动存储 |
| 18 | 申请任务失败 | 1 |  |
| 19 | 申请任务失败的命令字 | 5 | 最多记录5条命令,滚动存储 |
| 20 | 申请内存失败 | 1 |  |
| 21 | 申请内存失败的任务类型 | 5 |  |
| 22 | 零时数据A | 1 |  |
| 23 | 零时数据B | 1 |  |
| 24 | 零时数据C | 1 |  |
| 25 | 零时数据D | 1 |  |
| 26 | 零时数据E | 1 |  |
| 27 | 零时数据F | 1 |  |
| 28 | 零时数据G | 1 |  |
| 29 | 零时数据H | 1 |  |
| 30 | 零时数据I | 1 |  |
| 31 | 零时数据J | 1 |  |

##### RF设置表ID数据格式

简介：

1. 每次在设定模块ID前，必须读取”参数配置信息”来获取40byte的软件版本号。
2. RF更改模块ID时，必须携带目标设备的软件版本号。
3. 每次系统冷启动后的1分钟内为ID更改窗口。

下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 1 | 扩展命令值 | 1 | 0X10 |
| 2 | 软件版本号 | 40 |  |
| 3 | 新表地址 | 6 |  |

上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 1 | 扩展命令值 | 1 | 0X10 |
| 2 | 操作状态 | 1 | 0XAA:操作成功，0XAB:操作失败， |
| 3 | 设备地址 | 6 |  |

### 设置系统功能使能状态 0x08

#### 命令简介：

对户表模块的相关功能进行打开或关闭动作

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 第1个标志位上的值 | 1 | 0:关闭功能；1：开启功能； 2：不处理 |
| …. |  |  |  |
| 15 | 第15个标志位上的值 | 1 | 0:关闭功能；1：开启功能； 2：不处理 |
| 表端运行参数占两个字节，具体定义如下： | | | |
|  | 标志位1 | 1 | 注释19：表端功能使能位定义的低8位 |
|  | 标志位2 | 1 | 注释19：表端功能使能位定义的高8位 |

#### 上行命令：返回操作状态

#### 实例数据

### 读模块发射、接收，阀控，磁干扰次数等命令 0x09

#### 命令简介：

读表具的块发射次数，接收次数，开关阀次数命令、磁干扰次数

#### 下行命令：空数据域

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 发射次数 | 2 |  |
| 1 | 接收次数 | 2 |  |
| 2 | 开关阀次数 | 2 |  |
| 3 | 磁干扰次数 | 1 |  |

#### 实例数据

### 清除反转计量数据命令 0x0A

#### 命令简介：

清除表具的反转用量数据

#### 下行：空数据域

#### 上行：清除后的反转读数

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6或1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 反转读数 | 6 |  |

#### 实例数据

### 读系统功能使能状态 0x0B

#### 命令说明：

#### 下行：空数据域

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 功能使能状态 | 2 | 详见：注释19：表端运行参数位定义 |

#### 实例数据

### 设置定时定量上传参数命令 0x0C

#### 命令简介：

设置表端定时上传的时间间隔(天)和定量上传的数量间隔(方、吨),间隔为0表示不定时定量上传数据。

#### 下行数据：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2/3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类别 | 1 | 0：定时间隔；1：定量间隔：2：定时+定量 |
| 1 | 定时时间间隔 | 1 | 单位：小时，值为0关闭此功能 |
| 或 |  |  |  |
| 1 | 定量数量间隔 | 1 | 单位：m³，值为0关闭此功能 |
| 或 |  |  |  |
| 1 | 定时时间间隔 | 1 | 单位：小时 |
| 2 | 定量数量间隔 | 1 | 单位：m³ |

#### 上行：返回设置后的参数

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 定时上传的时间间隔 | 1 | 单位：小时 |
| 1 | 定量上传的数量间隔 | 1 | 单位：m³ |

#### 实例数据

### 读取/设置NB水表IP+端口+模式： 0x0D

#### 命令说明：

1. 设置NB模组的IP+端口+模式，

#### 设置下行

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |  |
| 段序号 | 段标识 | 段大小 | 默认值 | 段说明 |
| 0 | 数据类型 | 1 | 0 | 0：读取  1：设置 |
| 1 | 工作模式 | 1 | 0 | 0xA0：Coap  0xA1：UDP |
| 2 | IP第1个字节 | 1 | 79 | 16进制  NB-IOT的IP+连接端口：  121.43.175.222,5683 |
| 3 | IP第2个字节 | 1 | 2B |
| 4 | IP第3个字节 | 1 | AF |
| 5 | IP第4个字节 | 1 | DE |
| 6 | 连接端口 | 2 | 16 |
| 33 |

#### 设置上行：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |  |
| 段序号 | 段标识 | 段大小 | 默认值 | 段说明 |
| 0 | 数据类型 | 1 | 0 | 0：读取  1：设置 |
| 1 | 工作模式 | 1 | 0 | 0xA0：Coap  0xA1：UDP |
| 2 | IP第1个字节 | 1 | 79 | 16进制  NB-IOT的IP+连接端口：  121.43.175.222,5683 |
| 3 | IP第2个字节 | 1 | 2B |
| 4 | IP第3个字节 | 1 | AF |
| 5 | IP第4个字节 | 1 | DE |
| 6 | 连接端口 | 2 | 16 |
| 33 |
| 7 | 操作结果 | 1 |  | 0xAA:操作成功  0xAB:操作失败 |

### 读取/设置NB水表的运营商识别码： 0x0E

#### 命令说明：

1.

#### 设置下行

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |  |
| 段序号 | 段标识 | 段大小 | 默认值 | 段说明 |
| 0 | 数据类型 | 1 | 0 | 0：读取  1：设置 |
| 1 | SIM卡类型 | 4 | 46001000 | 默认高位在前  NB-IOT时：46001000  中国国家码 460  中国移动 04  中国联通 01  中国电信 11 |
| 2 | 通信频段 | 1 | 8 | 中国电信：5  中国移动：8  中国联通：8或3 |

#### 设置上行：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |  |
| 段序号 | 段标识 | 段大小 | 默认值 | 段说明 |
| 0 | 数据类型 | 1 | 0 | 0：读取  1：设置 |
| 1 | SIM卡类型 | 4 | 46001000 | 默认高位在前  NB-IOT时：46001000  中国国家码 460  中国移动 04  中国联通 01  中国电信 11 |
| 2 | 通信频段 | 1 | 8 | 中国电信：5  中国移动：8  中国联通：8或3 |
| 3 | 操作结果 | 1 |  | 0xAA:操作成功  0xAB:操作失败 |

### 读取/设置模块的IMEI： 0x0F

#### 命令说明：

1.

#### 设置下行

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |  |
| 段序号 | 段标识 | 段大小 | 默认值 | 段说明 |
| 0 | 数据类型 | 1 | 0 | 0：读取（IMEI+ICCID）  1：设置IMEI  2：设置ICCID |

#### 设置上行：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |  |
| 段序号 | 段标识 | 段大小 | 默认值 | 段说明 |
| 0 | 数据类型 | 1 | 0 | 0：读取（IMEI+ICCID）  1：设置IMEI  2：设置ICCID |
| 1 | ICCID | 10 |  | 10byte:CCID，压缩BCD |
| 2 | IMEI | 10 |  | 10byte:IMEI，压缩BCD |
| 3 | 操作结果 | 1 |  | 0xAA:操作成功  0xAB:操作失败 |

### 读取NB入网信息及状态： 0x10

#### 4.19.1命令简介：

* + - 1. 读NB当前入网信息和入网状态

#### 4.19.2下行命令：空数据域

#### 4.19.3上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 长度30 byte |
| 段序号 | 段标识 | 段大小 | 段说明， |
| 0 | Battery | 1 | Battery voltage |
| 1 | Signal power | 2 | **signal power in centibels（**高位为1为负数**）** |
| 2 | Total power | 2 | **total power in centibels（**高位为1为负数**）** |
| 3 | TX power | 2 | **current Tx power level in centibels** |
| 4 | TX time | 4 | **total Tx time since last reboot in millisecond** |
| 5 | RX time | 4 | **total Rx time since last reboot in millisecond** |
| 6 | Cell ID | 5 | **last cell ID** |
| 7 | ECL | 1 | **last ECL value** |
| 8 | SNR | 2 | **last snr value（**高位为1为负数**）** |
| 9 | EARFCN | 5 | **last earfcn value** |
| 10 | PCI | 2 | **last pci value** |
| 11 | RSRQ | 2 | **rsrq in centibels（**高位为1为负数**）** |
| 12 | OPERATOR  MODE | 1 |  |
| 13 | RegisterState | 1 | 0：入网失败（入网失败，上述入网信息全为0）  1:入网成功 |

### 读取价目表 0x11

#### 命令简介：

读取某一天开始执行的价格表

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 时间点 | 4 | YY YYMM DD, 年月日的BCD码 |

备注：数据域可以是空或者是个日期, 数据域长度为0表示读取目前执行的价格表,否者表示读取自这个日期开始执行的价格表.

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 状态 | 1 | 0：还未设价格表 1: 单一价格;2:阶梯价格 |
| 1 | 价格执行日期 | 4 |  |
| 2 | 单一价格 | 2 | 价格整数部分+价格小数备份 |
| 或 |  |  |  |
| 2 | 阶梯价格 | 4N | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |

#### 实例数据

### 设置价目表 0x12

#### 命令说明：

数据域的内容是加密的

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段说明 | 段标识 | 段大小 |  |
| 0 | 价格执行日期 | 4 | YY YY MM DD |
| 1 | 单一价格 | 2 |  |
| 或 |  |  |  |
| 1 | 阶梯价格 | 4N | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |
| 2 | 校验码/动态密码 | 1/6 | 校验码/动态密码是用来检查数据的合法信息 |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1/4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 状态 | 1 | 低4位：  0：还未设价格表 1: 单一价格;2:阶梯价格  高4位:  1: 设置的价格执行日期错误 |
| 1 | 价格执行日期 | 4 |  |
| 2 | 单一价格 | 2 | 价格整数部分+价格小数备份 |
| 或 |  |  |  |
| 2 | 阶梯价格 | 4N | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |

#### 实例数据

### 读取时钟 0x13

#### 命令简介：

读取某表的RTC时间

#### 下行：空数据域

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7（BCD码） |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 当前时间 | 7 | YY YY MM DD HH MM SS |

#### 实例数据

### 设置时钟 0x14

#### 命令说明：

上位机可选择逐个校时当个表具。

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 当前时间 | 7 |  |

#### 上行：返回确认帧

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 | | 2 | |
| 段说明 | 段标识 | | 段大小 | | 1或2 | |
| 0 | 操作状态 | | 1 | | 0xAA：操作成功； 0xAB：操作失败 | |
| 1 | 错误类型 | | 1 | | BIT0:参考起始用量不合法  BIT1:设置的预缴用量未达到开阀门限  BIT2: | |

#### 实例数据

### 读模块预缴用量和参考用量数据0x15

#### 命令说明：

读最近一次的下发剩余用量

#### 下行：空数据域

#### 上行：返回最近一次收到的剩余用量和参考用量

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 12 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 1 | 预缴用量 | 6 | 单位：㎥ |
| 2 | 参考起始用量 | 6 | 单位：㎥ |

#### 实例数据

### 下发模块预缴用量和参考用量数据0x16

#### 命令说明：

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 12（数据域中的内容是要加密的） |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 0 | 预缴用量 | 6 |
| 1 | 1 | 参考起始用量 | 6 |

#### 上行：返回当前充值信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1或2（数据域中的内容是要加密的） |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功; 0xAE：数据非法 |
| 1 | 数据非法类型 | 1 | BIT0:参考起始用量不合法  BIT1:设置的预缴用量未达到开阀门限  BIT2:  BIT3:  BIT4: |

#### 实例数据

### 读剩余用量报警限值，透支用量数值 0x17

#### 命令说明：

#### 下行：空数据域

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1/4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 标志位 | 1 | 0xAB：操作失败 |
| 或 |  |  |  |
| 0 | 标志位 | 1 | 0xAA：操作成功 |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 1 | 透支用量数值 | 2 | 透支用量数值可以是负数，高一位为1 表示负数 |

#### 实例数据

### 设置剩余用量报警限值，关阀限值 0x18

#### 命令说明：

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2/3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类别 | 1 | 0：报警限值；1：关阀限值：2：报警限值+关阀限值 |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 或 |  |  |  |
| 1 | 关阀限值 | 2 | 关阀限值可以是负数，高一位为1 表示负数 |
| 或 |  |  |  |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 2 | 关阀限值 | 2 | 关阀限值可以是负数，高一位为1 表示负数 |

#### 上行：返回设置后的值

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2/4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 标志位 | 1 | 0xAB：操作失败 |
| 1 | 失败类型 | 1 | BIT0:  BIT1:  BIT2: |
| 或 |  |  |  |
| 0 | 标志位 | 1 | 0xAA：操作成功 |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 1 | 关阀限值 | 2 | 关阀限值可以是负数，高一位为1 表示负数 |

#### 实例数据

### 读取命令的记录数据0x19

#### 命令说明：

读取表端记录的历史控阀命令。包括4byte（月，日，时，分）时间+ 1byte操作类型+ 1byte开/关阀类型

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读的数据类型 | 1 | 0：阀门【目前只有操作阀门命令的记录】  1：组网  2：抄表 |

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读的数据类型 | 1 |  |
| 1 | 执行的日期 | 4 | 月，日，时，分 |
| 2 | 操作类型 | 1 | 0：RF命令  1：磁干扰  2：掉电  3：上电  4：防锈 |
| 3 | 开/关阀类型 | 1 | 0：开阀动作  1：关阀动作 |

#### 实例数据：

### RAM/EEPROM数据读取命令 0x1A（手持器或调试软件功能）

#### 命令说明：

特殊的内容是不允许读出的，如DES密钥，要检查读出位置和读出长度是否有效或合法

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | EEPROM/RAM标志 | 1 | 0: Ram,1:EEPROM |
| 1 | 起始地址 | 2/4 | 对于集中器命令长度为4 |
| 2 | 要读出的字节数 | 1 |  |

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4+N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | AA:成功；AB：失败 |
| 1 | EEPROM/RAM标志 | 1 | 0: Ram,1:EEPROM |
| 2 | 起始地址 | 2/4 | 对于集中器命令长度为4 |
| 3 | 要读出的字节数 | 1 |  |
| 4 | 读出的数据 | N |  |

### 读取/设置模块抄表和上报信道 0x1B

#### 命令说明：

1. 通过RF的方式设置模块实时抄表的上报信道，

#### 设置下行

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 3或2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类别 |  | 0：读取和设置实时抄表和主动上传信道  ~~1：读取和设置集中器应答信道~~ |
| 1 | 实时抄表信道 | 1 | Bit7：0 读信道号  Bit7：1 写信道号  Bit0—Bit6：值范围见注释5：计量传感器类型及信道 |
| 2 | 主动上传信道 | 1 | Bit7：0 读信道号  Bit7：1 写信道号  Bit0—Bit6：值范围见注释5：计量传感器类型及信道 |

#### 设置上行：操作结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | | 总长 | 2 |
| 段序号 | 段标识 | | 段大小 | 段说明 |
| 0 | RXD | | 1 | 实时抄表信道Bit0—Bit6：  值范围见注释5：计量传感器类型及信道 |
| 1 | TXD | | 1 | 实时抄表信道Bit0—Bit6：  值范围见注释5：计量传感器类型及信道 |
| 或 | | | | |
| 0 | 操作结果 | 1 | | AB，操作失败 |
| 1 | 错误类型 | 1 | | BIT0:  BIT1:  BIT2: |

### 设置密钥 0x1D

#### 命令说明：

向某一表具下发AES128密钥

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 密钥内容 | 16 | 128位的密钥数据 |

#### 上行：返回操作结果

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0:  BIT1:  BIT2: |

### 预留 0x1E （内部命令）

**命令说明：**

这是一个表具自下而上的入网过程。应用场景是网络已组网，不想再重新组建所有网络，只想重建局部关系，入网的条件有两种：a. 表具收到广播抄表、校时等命令，但表具本身还未入网 b手持器对这个表具的入网邀请。

表具向周围中继器、集中器广播入网申请，中继器、集中器在收到后向表具回复连接信息，表具将这些信息分别沿这几个连接点发送入网信息到集中器，信息经过表具直接相连的中继器时表具Bcd码将被记录在中继器的EEPROM中，信息到集中器后，集中器将记录表具信息以及表具和中继器的连接信息。

#### 向中继器、集中器广播的数据：

空数据域

#### 中继器、集中器给表具回的连接信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备号 | 6 |  |
| 1 | 设备类型 | 1 | 中继器还是集中器 |

#### 表具将上面收到的信息中的下行Rssi值填好后发给集中器

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 10 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备号 | 6 |  |
| 1 | 设备类型 | 1 | 中继器还是集中器 |
| 2 | 设备所在层数 | 1 |  |
| 3 | 下行Rssi | 1 |  |
| 4 | 上行Rssi | 1 |  |

#### 集中器给表具回一两条从表具到集中器的全路径信息

这个命令可在集中器第一收到自主入网信息后的5分钟是向表具发出

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 | | 10 |
| 段序号 | 段标识 | 段大小 | | 段说明 |
| 0 | 设备的入网层号 | 1 | |  |
| 1 | 路径条数 | 1 | |  |
| 2 | 单个路径的级数 | 1 | 一两条路径 |  |
| 3 | 单个路径的全路径信息 | N |  |

### 预留 0x1F

**命令说明：**

对于后加入的中继器或表具，为了这个新加的设备能立刻入网，操作人员可以通过手抄器发‘邀请设备入网’命令，表具或中继器接收到命令后立即自主入网，入网结束后给发送方发操作结果。

**下行：空数据域**

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作结果 | 1 | 0xCF：操作已处理 |

### 读取/设置RF休眠策略 0x20

#### 命令说明：

**为了更好地节省表端用电量，RF的休眠策略:**

|  |  |  |  |
| --- | --- | --- | --- |
| **时段名称** | **时间** | **RF作息规律** | **备注** |
| RF工作时段 | 按日按月：1byte  起始时间：1byte  工作时长：1byte | 遇见干扰后自动跳频 | 模块主动上报时带RX，TX信道号 |
| 默认值 | 按日按月：0  起始时间：0  工作时长：24 | RF一直为工作状态 | 全天候工作 |

#### 设置下行/读取上行：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1/4 | |
| 段说明 | 段标识 | 段大小 | 段说明 |  |
| 0 | 读写标志 | 1 | BIT7: 0 读  BIT7: 1 写 |  |
| 1 | 按日按月标志： | 1 | BIT7: 0 按日执行BIT7: 1 按月执行 | 代表“RF侦听起始时间”代表的是小时还是日期 |
| 2 | 起始时间： | 1 | 值范围：0到24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
| 3 | 工作时长： | 1 | 值范围：0到24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |

#### 读取下行: 空数据域

#### 设置上行：返回设置后的信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0: 起始时间超限  BIT1: 工作时长超限  BIT2: 按日按月标志错误  BIT3: 其它设置的值不合法 |

### 预留 0x21

**命令说明：**

数据要加密传输

设置透传模块的运营商编号的命令时路径级数为1(长度为6字节)

**设置下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 运营商编号 | 4 |  |

**设置上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0:  BIT1:  BIT2: |

### 预留 0x22

**命令说明：**

下表具上传路径信息。一般是组网或自主入网系统自动调用，也可手持设置。

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 节点所在级数 | 1 |  |
| 1 | 路径长度 | 1 | M个，M<=3 |
| 2 | 路径信息 | 6N |

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0:  BIT1:  BIT2: |

### 预留 0x23

**命令说明：**

表具或中继重启后若时间非法，向集中器请求时间服务。

**上行：**启动定时上报功能来获取时间，详见0X01命令

**下行：**户表模块通过获取集中器应答帧携带的时间来校时，详见0X01命令

### 预留 0x25

**命令说明**

此命令是把抄表链路上的所有路由表用量数据全部一并读取回来。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 表号 | 6 |  |
| 1 | 要收集的数据 | 6 | 详见：注释7：表读数的数据格式 中的定时定量数据格式。 |

将沿途中继的表读数都读入进来.

# LORA表端无线命令列表

### 读用户用量、主机应答定时定量上传、下发剩余用量和剩余价格的指令： 0x01

#### 命令简介：

* + - 1. 读用户用量：上位机实时读户表数据时使用的命令格式，数据域长度可以为1或24
      2. 集中器下发的应答帧和命令帧：终端户表定时定量上传数据时，主机接收成功后的应答数据格式
      3. 下发剩余用量和剩余价格：主机主动下发当前剩余用量和结算价格的数据格式。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长：长度可为1或24或24+N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读取的数据格式编号 | 1 | 详见注释7：表读数的数据格式(默认0) 集中器应答表主动上传数据时。   * + - 1. 0xA0应答数据帧       2. 0xA1命令数据帧 |
| 1 | 当前时间 | 7 | YY YYMM DD HH MM SS，用于校准户表时钟 |
| 2 | 预缴用量 | 6 | 根据用户缴费金额和单价计算出来的可用数据 |
| 3 | 参考起始用量 | 6 | 后台服务器在计算剩余用量时使用的户表当前累计参考量。 |
| 4 | 主动上传的时隙号 | 2 | 低字节在前，高字节在后  表端主动上报的时隙编号，表端根据此时隙编号上报数据 |
| 5 | 总表数据 | 2 | 低字节在前，高字节在后。此集中器下的总表数量 |
| 6 | 操作命令 | 1 | 相关命令见“4.协议的表端无线命令列表”0：没有操作命令 |
| 7 | 数据长度 | 1 | 值范围：≤15 |
| 8 | 数据内容 | N | 数据总长度≤8byte  根据命令字，随机变化，内容见“操作命令注释” |

带有RTC时钟的表端在收到数据后，可根据数据包中的时间校准时钟。

操作命令（下行）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能 | 说明 | 长度 | 注释:所有扩展命令总长度≤8byte |
| 1 | 设置信道 | 操作命令 | 1 | 值为：1 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 信道号 | 1 | Bit7:为1时设置信道，低7bit为信道号 |
| 2 | 打开自动信道 | 操作命令 | 1 | 值为：2 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 设置字 | 1 | Bit7:为0时，关闭自动信道功能  Bit7:为1时，打开自动信道功能 |
| 3 | 阀控 | 操作命令 | 1 | 值为：3 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 状态字 | 1 | 低四位：01：开阀；02：关阀 |
| 4 | 下发当前结算价格 | 操作命令 | 1 | 值为：4 |
| 数据长度 | 1 | 值为：4 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 结算价格 | 2 | 低位在前，高位在后  如：0x35 0x02 ==>> 2.35元 |
| 5 | 打开关闭实时抄表功能 | 操作命令 | 1 | 值为：2 |
| 数据长度 | 1 | 值为：3 |
| 特征字 | 2 | 特征字： 0xDA 0x26 |
| 设置字 | 1 | Bit7:为0时，关闭自动信道功能  Bit7:为1时，打开自动信道功能 |
| 6 |  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 当前的数据格式编号 | 1 | 1. 实时数据，表端主动上传标志 2. 冻结的数据，表端主动上传标志 3. 预留 4. 定时上传数据，表端主动上传标志 5. 定量上传数据，表端主动上传标志 6. 报警上传定时定量数据，表端主动上传标志 7. 报警上传冻结数据，表端主动上传标志 |
| 1 | 表端数据 | N | 详见注释7：表读数的数据格式 |
| 2 | Battery | 1 | Battery voltage |
| 3 | Signal power | 2 | **signal power in centibels（**高位为1为负数**）** |
| 4 | Total power | 2 | **total power in centibels（**高位为1为负数**）** |
| 5 | TX power | 2 | **current Tx power level in centibels** |
| 6 | TX time | 2 | **total Tx time since last reboot in millisecond** |
| 7 | RX time | 2 | **total Rx time since last reboot in millisecond** |
| 8 | Cell ID | 5 | **last cell ID** |
| 9 | ECL | 1 | **last ECL value** |
| 10 | SNR | 2 | **last snr value（**高位为1为负数**）** |
| 11 | EARFCN | 5 | **last earfcn value** |
| 12 | PCI | 2 | **last pci value** |
| 13 | RSRQ | 2 | **rsrq in centibels（**高位为1为负数**）** |
| 14 | OPERATOR  MODE | 1 |  |

操作命令（上行）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 功能 | 说明 | 长度 | 注释:所有扩展命令总长度≤8byte |
| 1 | 设置信道 | 操作命令 | 1 | 值为：1 |
| 操作结果 | 1 | 0xAA或0XAB |
| 信道号 | 1 | 低四位：上报信道  高四位：当前通信信道 |
| 2 | 打开自动信道 | 操作命令 | 1 | 值为：2 |
| 操作结果 | 1 | 0xAA或0XAB |
| 使能状态 | 2 | 见：“注释19” |
| 3 | 阀门控制 | 操作命令 | 1 | 值为：3 |
| 操作结果 | 1 | 0xAA或0XAB |
| 命令状态 | 1 | 见阀控状态 |
| 4 | 下发当前结算价格 | 操作命令 | 1 | 值为：4 |
| 操作结果 | 1 | 0xAA或0XAB |
| 当前结算价格 | 2 | 低位在前，高位在后  如：0x35 0x02 ==>> 2.35元 |
| 5 | 打开关闭实时抄表功能 | 操作命令 | 1 | 值为：2 |
| 操作结果 | 1 | 0xAA或0XAB |
| 使能状态 | 2 | 见：“注释19” |
| 6 |  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### 实例数据：

#### 注意事项：

当下发的剩余用量中参考起始用量大于表端累计用量时，表端模块返回的数据中，数据域只有一个0xAC，表示：剩余用量下发非法

### 读取冻结数据 0x02

#### 命令简介：

#### 冻结时间从0点开始，每隔30分钟冻结一次数据，每天冻结48条，10天滚动存储。

#### 每次只上传一天的数据。

#### 当读取的冻结数据时整数位为0xFF 0x FF 0x FE时，表示累计用量已达到最大值。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长：长度可为2或9 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读取的数据格式编号 | 1 | 详见注释7：读冻结数的数据格式A.读正转数据：01 B. 读反转数据：02 |
| 1 | 当前时间 | 7 | YY YY MM DD HH MM SS |
| 2 | 要读取的冻结数据起始序号 | 1 | 默认：0 详见注释7：读冻结数的数据格式 |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1或N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读取的数据格式编号 | 1 | 详见注释7：读冻结数的数据格式A.读正转数据：01 B. 读反转数据：02 |
| 1 | 冻结数据 | N | 详见注释7：表读数的数据格式 |

#### 实例数据

### 开关阀指令 0x03

#### 命令简介：

强制或正常开关阀，强制开关阀时，在动阀时不检测到位信号、磁干扰标识、欠压标志和当前的阀门状态。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 强制还是正常开关阀标志 | 1 | 01: 强制；00：正常 |
| 1 | 开阀还是关阀标志 | 1 | 01：开阀；00：关阀 |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 开关成功标志 | 1 | 0xAA：开/关阀成功,  0xAB：开/关阀失败  0xAD：表端接收命令成功 |
| 1 | 阀控失败的原因 | 2 | **低字节在前，高字节在后**  Bit0： 电池欠压  Bit1： 磁干扰中  Bit2：Adc正在工作  Bit3： 阀门正在运行中  Bit4： 阀门故障  Bit5： RF正在工作  Bit6：任务申请失败  Bit7：等待按键开阀  Bit8：当前阀门已经到位  Bit9：设备类型错误  Bit10：time 申请失败  Bit11：系统欠费  Bit12：  Bit13：  Bit14：  Bit15： |

#### 实例数据

### 读表端参数配置信息 0x04

#### 命令简介：

读表端运行时的相关参数值

#### 下行：空数据域

#### 上行数据：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 164 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 参数 | **164字节** | 注释22：数据域结构 |

### 清异常命令 0x05

#### 命令简介：

此命令可以一次性的清除模块告警信息

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 0 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 数据域空 |  |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作结果 | 1 | 详见：注释14：返回的操作代码一般含义 |

#### 实例数据

### 设置用量及脉冲系数 0x06

#### 命令简介：

略

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 用量 | 6 |  |
| 1 | 脉冲系数 | 1 | 0：脉冲系数为1  1：脉冲系数为10  2：脉冲系数为100  3：脉冲系数为1000 |

#### 上行命令

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7或1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 用量的 | 6 |  |
| 1 | 脉冲系数 | 1 |  |

#### 实例数据

### 测试命令 0x07

#### 命令简介

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令字 | 1 | 详见：**子命令字列表** |

#### 子命令字列表

|  |  |  |
| --- | --- | --- |
| 子命令字 | 参数说明 | 上行数据 |
| 0x01 | 读Debug信息 | 注释7：表读数的数据格式 |
| 0x02 | 清Debug信息 | 返回操作状态  **详见注释14：返回的操作代码一般含义** |
| 0x03 | 发射功率测试指令 | 返回操作状态  **详见注释14：返回的操作代码一般含义** |
| 0x04 | 表端重启 | 返回操作状态  **详见注释14：返回的操作代码一般含义** |
| 0x05 | 读表端实时温度 | 一个字节的温度（可以是负数）  Bit7为0：表示bit0―bit6数据为正温度  Bit7为1：表示bit0―bit6数据为负温度  当表端检测温度错误时返回**0xff** |
| 0x07 | 读取系统实时电压 | 表端接收到此命令后，立刻检测电池电压，检测后返回其值 |
| 0x08 | 清预缴用量和参考用量等值 |  |
| 0x09 | 设置阀门过流电流值，超时时间 | 操作后返回其值  过流电流值： 1 个字节，单位：mA，为0 表示不设置  超时时间: 2 个字节，低字节在前，单位：ms,为0 表示不设置 |
| 0x0A | 读运行商编号 | 4个字节运行商编号 |
| 0x0B | 清除入网标志 | 返回操作成功或失败标志  **详见注释14：返回的操作代码一般含义** |
| 0x0C | LED屏测试 | 0 SetLcdStatus(false)   1. SetLcdStatus(true)   2 ClearLcd   1. + 6个字节的数字显示数字   注：此命令为UART命令 |
| 0x0D | 设置流速控制 | 过大值(2, 方/每小时) 持续时间(1,分钟) 过小值(1,方/每100小时) 持续时间(1,小时) |
| 0x0E | 读取模块上报的路径信息 | 1字节的路径级数  6:N字节的理由表ID |
| 0x0F | 读取阀门操作的历史状态 | 模块最多存储5条历史动阀记录，记录所有控阀命令 |
| 0x10 | RF更改表ID | * + - 1. 每次上电后的1分钟内为设置窗口，且只有一次修改机会       2. 每次修改时必须携带程序的版本号 |
| 0x11 | 让LORAWAN模块进入BOOT模式 | 通过手抄器让lorawan模块进入升级功能(超时时间6分钟)。 |
| 0x12 | 读取LORAWAN模块的EUI | 通过手抄器读取lorawan模块的EUI |
| 0x13 | 清除LORAWAN的入网标志 | 通过手抄器清除lorawan模块的入网信息 |
| 0x14 | 切换模块的工作模式为LORAWAN | 正常情况下，模块的工作模式为四表集抄模式，收到切换命令后程序切换为6009模式。数据域密钥为0x5A, 0x5B, 0x5C, 0x5D, 0x5E, 0x5F, 0x60, |
| 0x15 | 水处理设备  下发相关的控制命令/ | 神源客户，下发相应的开门或关门命令到终端 |
| 0x16 | 变频器设备  下发的设置命令 | 设置变频器的工作频率 |
| 0x17 | 设置公司代码 | 2字节长度，默认是0x8021 |
| 0x18 | 设置表ID | 8字节长度， |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1+N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令字 | 1 | 详见：**子命令字列表** |
| 1 | 相关数据 | N | 详见：**子命令数据格式解析**中的相关命令格式注释 |

#### 子命令数据格式解析

##### Debug信息数据格式

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 项目名称 | 总长: | |
| 长度 | 注释 |
| 1 | 模块的发射总次数RF | 2 | 低字节在前 |
| 2 | 模块的接收总次数 | 2 |  |
| 3 | 模块的开/关阀门总次数 | 2 |  |
| 4 | 模块受到的磁干扰总次数 | 1 |  |
| 5 | EEPROM 写次数, 低字节在前 | 4 |  |
| 6 | 系统48小时复位次数 | 2 |  |
| 7 | 系统进入初始化次数 | 2 |  |
| 8 | 系统完成初始化次数 | 2 |  |
| 9 | 系统长时间不喂狗导致的初始化 | 2 |  |
| 10 | CDA检测信号超过100MS的次数 | 2 |  |
| 11 | 在检测到CDA信号后的接收超时次数 | 2 |  |
| 12 | A干簧管闭合的总脉冲数 | 2 |  |
| 13 | B干簧管闭合的总脉冲数 | 2 |  |
| 14 | ID校验错误 | 1 |  |
| 15 | 收到非法命令字 | 1 |  |
| 16 | 申请定时器失败 | 1 |  |
| 17 | 申请定时器失败的命令字 | 5 | 最多记录5条命令,滚动存储 |
| 18 | 申请任务失败 | 1 |  |
| 19 | 申请任务失败的命令字 | 5 | 最多记录5条命令,滚动存储 |
| 20 | 申请内存失败 | 1 |  |
| 21 | 申请内存失败的任务类型 | 5 |  |
| 22 | 零时数据A | 1 |  |
| 23 | 零时数据B | 1 |  |
| 24 | 零时数据C | 1 |  |
| 25 | 零时数据D | 1 |  |
| 26 | 零时数据E | 1 |  |
| 27 | 零时数据F | 1 |  |
| 28 | 零时数据G | 1 |  |
| 29 | 零时数据H | 1 |  |
| 30 | 零时数据I | 1 |  |
| 31 | 零时数据J | 1 |  |

##### RF设置表ID数据格式

简介：

1. 每次在设定模块ID前，必须读取”参数配置信息”来获取40byte的软件版本号。
2. RF更改模块ID时，必须携带目标设备的软件版本号。
3. 每次系统冷启动后的1分钟内为ID更改窗口。

下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 1 | 扩展命令值 | 1 | 0X10 |
| 2 | 软件版本号 | 40 |  |
| 3 | 新表地址 | 6 |  |

上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 1 | 扩展命令值 | 1 | 0X10 |
| 2 | 操作状态 | 1 | 0XAA:操作成功，0XAB:操作失败， |
| 3 | 设备地址 | 6 |  |

### 设置系统功能使能状态 0x08

#### 命令简介：

对户表模块的相关功能进行打开或关闭动作

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 第1个标志位上的值 | 1 | 0:关闭功能；1：开启功能； 2：不处理 |
| …. |  |  |  |
| 15 | 第15个标志位上的值 | 1 | 0:关闭功能；1：开启功能； 2：不处理 |
| 表端运行参数占两个字节，具体定义如下： | | | |
|  | 标志位1 | 1 | 注释19：表端功能使能位定义的低8位 |
|  | 标志位2 | 1 | 注释19：表端功能使能位定义的高8位 |

#### 上行命令：返回操作状态

#### 实例数据

### 读模块发射、接收，阀控，磁干扰次数等命令 0x09

#### 命令简介：

读表具的块发射次数，接收次数，开关阀次数命令、磁干扰次数

#### 下行命令：空数据域

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 发射次数 | 2 |  |
| 1 | 接收次数 | 2 |  |
| 2 | 开关阀次数 | 2 |  |
| 3 | 磁干扰次数 | 1 |  |

#### 实例数据

### 清除反转计量数据命令 0x0A

#### 命令简介：

清除表具的反转用量数据

#### 下行：空数据域

#### 上行：清除后的反转读数

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6或1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 反转读数 | 6 |  |

#### 实例数据

### 读系统功能使能状态 0x0B

#### 命令说明：

#### 下行：空数据域

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 功能使能状态 | 2 | 详见：注释19：表端运行参数位定义 |

#### 实例数据

### 设置定时定量上传参数命令 0x0C

#### 命令简介：

设置表端定时上传的时间间隔(天)和定量上传的数量间隔(方、吨),间隔为0表示不定时定量上传数据。

#### 下行数据：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2/3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类别 | 1 | 0：定时间隔；1：定量间隔：2：定时+定量 |
| 1 | 定时时间间隔 | 1 | 单位：小时，值为0关闭此功能 |
| 或 |  |  |  |
| 1 | 定量数量间隔 | 1 | 单位：m³，值为0关闭此功能 |
| 或 |  |  |  |
| 1 | 定时时间间隔 | 1 | 单位：小时 |
| 2 | 定量数量间隔 | 1 | 单位：m³ |

#### 上行：返回设置后的参数

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 定时上传的时间间隔 | 1 | 单位：小时 |
| 1 | 定量上传的数量间隔 | 1 | 单位：m³ |

#### 实例数据

### 广播寻址指令： 0x0F

#### 命令简介：

广播寻址指令, 搜寻附近的设备。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要搜索的设备类型 | 1 | 0：所有类型，  1：气表；  2：中继器；  4：集中器  8: 水表  16：电表  64：组网寻址  128：只搜未入网的设备 |
| 1 | 主动寻址的设备类型 | 1 | 值参看‘en\_DeviceType’ |
| 2 | 集中器地址 | 6 | 可选 |
| 3 | 要搜寻的设备号 | 6N | 可选, 若有这个段，必须有段2 |
| 4 | 户表应答门限（RSSI） | 1 | 拿此门限值和接收信号时产生的门限进行比对，大于这个值时返回信号。小于时不响应此命令。单位—dBm |

广播命令的目的地址是广播地址：D4 D4D4D4D4D4

户表应答门限（RSSI）:主机发出的广播命令，只有接收到广播命令时信号强度大于应答门限时，才返回应答帧，否则不响应。这样可以避免单获取一只表的ID时所有表都应答的问题。

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 8 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备号 | 6 |  |
| 1 | 设备类型 | 1 |  |

各个设备在收到广播信息后，要向发送方回复信息

#### 实例数据

### 读取价目表 0x11

#### 命令简介：

读取某一天开始执行的价格表

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 时间点 | 4 | YY YYMM DD, 年月日的BCD码 |

备注：数据域可以是空或者是个日期, 数据域长度为0表示读取目前执行的价格表,否者表示读取自这个日期开始执行的价格表.

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 状态 | 1 | 0：还未设价格表 1: 单一价格;2:阶梯价格 |
| 1 | 价格执行日期 | 4 |  |
| 2 | 单一价格 | 2 | 价格整数部分+价格小数备份 |
| 或 |  |  |  |
| 2 | 阶梯价格 | 4N | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |

#### 实例数据

### 设置价目表 0x12

#### 命令说明：

数据域的内容是加密的

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段说明 | 段标识 | 段大小 |  |
| 0 | 价格执行日期 | 4 | YY YY MM DD |
| 1 | 单一价格 | 2 |  |
| 或 |  |  |  |
| 1 | 阶梯价格 | 4N | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |
| 2 | 校验码/动态密码 | 1/6 | 校验码/动态密码是用来检查数据的合法信息 |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1/4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 状态 | 1 | 低4位：  0：还未设价格表 1: 单一价格;2:阶梯价格  高4位:  1: 设置的价格执行日期错误 |
| 1 | 价格执行日期 | 4 |  |
| 2 | 单一价格 | 2 | 价格整数部分+价格小数备份 |
| 或 |  |  |  |
| 2 | 阶梯价格 | 4N | N组{ 一个字节单价整数+一个字节单价小数+ 2个字节的限量} |

#### 实例数据

### 读取时钟 0x13

#### 命令简介：

读取某表的RTC时间

#### 下行：空数据域

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7（BCD码） |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 当前时间 | 7 | YY YY MM DD HH MM SS |

#### 实例数据

### 设置时钟 0x14

#### 命令说明：

上位机可选择逐个校时当个表具。

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 当前时间 | 7 |  |

#### 上行：返回确认帧

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 | | 2 | |
| 段说明 | 段标识 | | 段大小 | | 1或2 | |
| 0 | 操作状态 | | 1 | | 0xAA：操作成功； 0xAB：操作失败 | |
| 1 | 错误类型 | | 1 | | BIT0:参考起始用量不合法  BIT1:设置的预缴用量未达到开阀门限  BIT2: | |

#### 实例数据

### 读模块预缴用量和参考用量数据0x15

#### 命令说明：

读最近一次的下发剩余用量

#### 下行：空数据域

#### 上行：返回最近一次收到的剩余用量和参考用量

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 12 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 1 | 预缴用量 | 6 | 单位：㎥ |
| 2 | 参考起始用量 | 6 | 单位：㎥ |

#### 实例数据

### 下发模块预缴用量和参考用量数据0x16

#### 命令说明：

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 12（数据域中的内容是要加密的） |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 0 | 预缴用量 | 6 |
| 1 | 1 | 参考起始用量 | 6 |

#### 上行：返回当前充值信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1或2（数据域中的内容是要加密的） |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功; 0xAE：数据非法 |
| 1 | 数据非法类型 | 1 | BIT0:参考起始用量不合法  BIT1:设置的预缴用量未达到开阀门限  BIT2:  BIT3:  BIT4: |

#### 实例数据

### 读剩余用量报警限值，透支用量数值 0x17

#### 命令说明：

#### 下行：空数据域

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1/4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 标志位 | 1 | 0xAB：操作失败 |
| 或 |  |  |  |
| 0 | 标志位 | 1 | 0xAA：操作成功 |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 1 | 透支用量数值 | 2 | 透支用量数值可以是负数，高一位为1 表示负数 |

#### 实例数据

### 设置剩余用量报警限值，关阀限值 0x18

#### 命令说明：

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2/3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类别 | 1 | 0：报警限值；1：关阀限值：2：报警限值+关阀限值 |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 或 |  |  |  |
| 1 | 关阀限值 | 2 | 关阀限值可以是负数，高一位为1 表示负数 |
| 或 |  |  |  |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 2 | 关阀限值 | 2 | 关阀限值可以是负数，高一位为1 表示负数 |

#### 上行：返回设置后的值

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2/4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 标志位 | 1 | 0xAB：操作失败 |
| 1 | 失败类型 | 1 | BIT0:  BIT1:  BIT2: |
| 或 |  |  |  |
| 0 | 标志位 | 1 | 0xAA：操作成功 |
| 1 | 报警限值 | 1 | 小于限量值蜂鸣报警 |
| 1 | 关阀限值 | 2 | 关阀限值可以是负数，高一位为1 表示负数 |

#### 实例数据

### 读取命令的记录数据0x19

#### 命令说明：

读取表端记录的历史控阀命令。包括4byte（月，日，时，分）时间+ 1byte操作类型+ 1byte开/关阀类型

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读的数据类型 | 1 | 0：阀门【目前只有操作阀门命令的记录】  1：组网  2：抄表 |

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 要读的数据类型 | 1 |  |
| 1 | 执行的日期 | 4 | 月，日，时，分 |
| 2 | 操作类型 | 1 | 0：RF命令  1：磁干扰  2：掉电  3：上电  4：防锈 |
| 3 | 开/关阀类型 | 1 | 0：开阀动作  1：关阀动作 |

#### 实例数据：

### RAM/EEPROM数据读取命令 0x1A（手持器或调试软件功能）

#### 命令说明：

特殊的内容是不允许读出的，如DES密钥，要检查读出位置和读出长度是否有效或合法

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | EEPROM/RAM标志 | 1 | 0: Ram,1:EEPROM |
| 1 | 起始地址 | 2/4 | 对于集中器命令长度为4 |
| 2 | 要读出的字节数 | 1 |  |

#### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4+N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | AA:成功；AB：失败 |
| 1 | EEPROM/RAM标志 | 1 | 0: Ram,1:EEPROM |
| 2 | 起始地址 | 2/4 | 对于集中器命令长度为4 |
| 3 | 要读出的字节数 | 1 |  |
| 4 | 读出的数据 | N |  |

### 读取/设置模块抄表和上报信道 0x1B

#### 命令说明：

1. 通过RF的方式设置模块实时抄表的上报信道，

#### 设置下行

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 3或2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类别 |  | 0：读取和设置实时抄表和主动上传信道  ~~1：读取和设置集中器应答信道~~ |
| 1 | 实时抄表信道 | 1 | Bit7：0 读信道号  Bit7：1 写信道号  Bit0—Bit6：值范围见注释5：计量传感器类型及信道 |
| 2 | 主动上传信道 | 1 | Bit7：0 读信道号  Bit7：1 写信道号  Bit0—Bit6：值范围见注释5：计量传感器类型及信道 |

#### 设置上行：操作结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | | 总长 | 2 |
| 段序号 | 段标识 | | 段大小 | 段说明 |
| 0 | RXD | | 1 | 实时抄表信道Bit0—Bit6：  值范围见注释5：计量传感器类型及信道 |
| 1 | TXD | | 1 | 实时抄表信道Bit0—Bit6：  值范围见注释5：计量传感器类型及信道 |
| 或 | | | | |
| 0 | 操作结果 | 1 | | AB，操作失败 |
| 1 | 错误类型 | 1 | | BIT0:  BIT1:  BIT2: |

### 设置密钥 0x1D

#### 命令说明：

向某一表具下发AES128密钥

#### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 密钥内容 | 16 | 128位的密钥数据 |

#### 上行：返回操作结果

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0:  BIT1:  BIT2: |

### 表具自主入网 0x1E （内部命令）

**命令说明：**

这是一个表具自下而上的入网过程。应用场景是网络已组网，不想再重新组建所有网络，只想重建局部关系，入网的条件有两种：a. 表具收到广播抄表、校时等命令，但表具本身还未入网 b手持器对这个表具的入网邀请。

表具向周围中继器、集中器广播入网申请，中继器、集中器在收到后向表具回复连接信息，表具将这些信息分别沿这几个连接点发送入网信息到集中器，信息经过表具直接相连的中继器时表具Bcd码将被记录在中继器的EEPROM中，信息到集中器后，集中器将记录表具信息以及表具和中继器的连接信息。

#### 向中继器、集中器广播的数据：

空数据域

#### 中继器、集中器给表具回的连接信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备号 | 6 |  |
| 1 | 设备类型 | 1 | 中继器还是集中器 |

#### 表具将上面收到的信息中的下行Rssi值填好后发给集中器

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 10 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备号 | 6 |  |
| 1 | 设备类型 | 1 | 中继器还是集中器 |
| 2 | 设备所在层数 | 1 |  |
| 3 | 下行Rssi | 1 |  |
| 4 | 上行Rssi | 1 |  |

#### 集中器给表具回一两条从表具到集中器的全路径信息

这个命令可在集中器第一收到自主入网信息后的5分钟是向表具发出

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 | | 10 |
| 段序号 | 段标识 | 段大小 | | 段说明 |
| 0 | 设备的入网层号 | 1 | |  |
| 1 | 路径条数 | 1 | |  |
| 2 | 单个路径的级数 | 1 | 一两条路径 |  |
| 3 | 单个路径的全路径信息 | N |  |

### 邀请设备入网 0x1F

**命令说明：**

对于后加入的中继器或表具，为了这个新加的设备能立刻入网，操作人员可以通过手抄器发‘邀请设备入网’命令，表具或中继器接收到命令后立即自主入网，入网结束后给发送方发操作结果。

**下行：空数据域**

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作结果 | 1 | 0xCF：操作已处理 |

### 读取/设置RF休眠策略 0x20

#### 命令说明：

**为了更好地节省表端用电量，RF的休眠策略:**

|  |  |  |  |
| --- | --- | --- | --- |
| **时段名称** | **时间** | **RF作息规律** | **备注** |
| RF工作时段 | 按日按月：1byte  起始时间：1byte  工作时长：1byte | 遇见干扰后自动跳频 | 模块主动上报时带RX，TX信道号 |
| 默认值 | 按日按月：0  起始时间：0  工作时长：24 | RF一直为工作状态 | 全天候工作 |

#### 设置下行/读取上行：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1/4 | |
| 段说明 | 段标识 | 段大小 | 段说明 |  |
| 0 | 读写标志 | 1 | BIT7: 0 读  BIT7: 1 写 |  |
| 1 | 按日按月标志： | 1 | BIT7: 0 按日执行BIT7: 1 按月执行 | 代表“RF侦听起始时间”代表的是小时还是日期 |
| 2 | 起始时间： | 1 | 值范围：0到24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
| 3 | 工作时长： | 1 | 值范围：0到24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |

#### 读取下行: 空数据域

#### 设置上行：返回设置后的信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0: 起始时间超限  BIT1: 工作时长超限  BIT2: 按日按月标志错误  BIT3: 其它设置的值不合法 |

### 设置运营商编号 0x21

**命令说明：**

数据要加密传输

设置透传模块的运营商编号的命令时路径级数为1(长度为6字节)

**设置下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 4 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 运营商编号 | 4 |  |

**设置上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0:  BIT1:  BIT2: |

### 路径下发命令 0x22

**命令说明：**

下表具上传路径信息。一般是组网或自主入网系统自动调用，也可手持设置。

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 节点所在级数 | 1 |  |
| 1 | 路径长度 | 1 | M个，M<=3 |
| 2 | 路径信息 | 6N |

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段说明 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功； 0xAB：操作失败 |
| 1 | 错误类型 | 1 | BIT0:  BIT1:  BIT2: |

### 请求时间服务命令 0x23

**命令说明：**

表具或中继重启后若时间非法，向集中器请求时间服务。

**上行：**启动定时上报功能来获取时间，详见0X01命令

**下行：**户表模块通过获取集中器应答帧携带的时间来校时，详见0X01命令

### 读一串表数据 0x25

**命令说明**

此命令是把抄表链路上的所有路由表用量数据全部一并读取回来。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 16N |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 表号 | 6 |  |
| 1 | 要收集的数据 | 6 | 详见：注释7：表读数的数据格式 中的定时定量数据格式。 |

将沿途中继的表读数都读入进来.

# 协议的集中器、中继器无线命令列表

## 读取集中器版本信息 0x40

**命令说明**

此命令用于获取集中器的软件版本、硬件版本和协议版本。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 程序版本 | 2 |  |
| 1 | 硬件版本 | 2 |  |
| 2 | 协议版本 | 2 |  |

## 读取集中器ID 0x41

**命令说明**

此命令用于获取集中器的ID编号.

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 集中器ID的BCD码 | 6 |  |

## 写入集中器ID 0x42

**命令说明**

此命令用于设置集中器的ID编号.

注意：

* 集中器ID不可以和表具档案的ID重复；
* 本指令只能通过串口或USB接口通过物理连接到集中器主板上设置，不能通过GPRS或RF通道设置；
* 如果设置成和原ID不同的ID值，集中器会在5秒钟后重新启动。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 集中器ID的BCD码 | 6 |  |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 操作状态见注释14. |

## 读集中器时钟 0x43

**命令说明**

此命令用于读取集中器内的实时时钟。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 集中器时钟 | 7 | 格式为：YY YY MM DD HH MM SS |

## 写集中器时钟 0x44

**命令说明**

此命令用于设置集中器内的实时时钟。

注意：

* 当设置的时钟和集中器内的时钟相差24小时以上时，要连续设置3次，集中器才会接受新的时钟值。
* 写实时时钟可能会导致集中器执行数据补抄或数据上传任务，前提是满足了数据补抄或数据上传的触发条件。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 时钟数据 | 7 | 格式为：YY YY MM DD HH MM SS |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 操作状态见注释14. |

## 读GPRS参数 0x45

**命令说明**

此命令用于读取集中器中的Gprs参数设置。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 0/2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 首选DSC IP(4)+首选 DSC PORT(2) +备用DSC IP(4)+备用DSC PORT(2)+GPRS心跳包时间间隔 (1) | 13 | 信息输出类型：保留  Gprs心跳包时间间隔单位为10秒 |
| 1 | APN长度+APN+用户名长度+用户名+密码长度+密码 | 3+N |  |

## 写GPRS参数 0x46

**命令说明**

此命令用于写入集中器中的Gprs参数设置。

注意：

写入新的GPRS参数后，集中器将会在10秒钟内重启，并且以新的GPRS参数设置连接服务器。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 0/2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 首选DSC IP(4)+首选 DSC PORT(2) +备用DSC IP(4)+备用DSC PORT(2)+GPRS心跳包时间间隔(1) | 13 | 信息输出类型：保留  Gprs心跳包时间间隔单位为10秒 |
| 1 | APN长度+APN+用户名长度+用户名+密码长度+密码 | 3+N |  |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 操作状态见注释14. |

## 读GPRS信号强度 0x47

**命令说明**

此命令用于读取Gprs的信号强度。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 信号强度 | 1 | 16进制：  0：小于等于-113dBm  1：-111dBm  2……30：-109dBm……-53dBm  31：大于等于-53dBm  99：未知或不可测 |
| 1 | 联机状态 | 1 | 0：离线，1：在线 |
| 2 | IMSI长度 | 1 | IMSI的长度 |
| 3 | IMSI内容 | N | ASCII码格式 |
| 4 | GMM长度 | 1 | 模块型号长度 |
| 5 | GMM内容 | N | 模块型号，ASCII码格式 |

## 集中器初始化 0x48

**命令说明**

此命令用于格式化集中器。

注意：此操作过程需耗费较长时间。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作类别 | 1 | 0：清除所有表档案、中继档案,自定义路径等  1：清空所有抄到的表数据，即清空EEPROM |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作类别 | 1 | 0：清除所有表档案、中继档案,自定义路径等  1：清空所有抄到的表数据，即清空EEPROM |
| 1 | 操作状态 | 1 | 操作状态见注释14. |

## 读集中器工作模式参数 0x49

**命令说明**

此命令用于读取集中器的一些工作参数。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 工作类型 | 1 | 0：定时定量数据；1：冻结数据；其他：无效 |
| 1 | 工作参数 | 1 | Bit7：数据补抄控制位，1为打开；0为关闭  Bit6：数据上传控制位，1为上传；0为关闭  Bit5-Bit0：保留 |
| 2 | 数据上传时间点 | 1 | BCD格式。在此时间点之前，数据量每够一包上传一次；在此时间点之后，收到表具数据即上传。 |
| 3 | 数据补抄日期 | 4 | 第一个字节：  Bit7：保留  Bit6-Bit0:代表日期1日到7日；  第二个字节：  Bit7-Bit0：代表日期8日到15日  第三个字节：  Bit7-Bit0：代表日期16日到23日  第四个字节：  Bit7-Bit0：代表日期24日到31日 |
| 4 | 数据补抄时间点 | 1 | BCD格式，数据补抄的时间，在此时间之后，集中器将对未抄到的表具数据进行主动补抄。 |
| 5 | 数据补抄的次数 | 1 | 数据补抄失败时重复补抄的次数，最大值为10。 |

## 写集中器工作模式参数 0x4A

**命令说明**

此命令用于设置集中器的工作参数。

注意：

* 修改集中器的工作类型后，集中器会在10秒钟内重启，并按新的工作类型工作；但只修改工作类型以外的参数时，集中器不会重启；
* 修改集中器工作类型后，集中器重启后有效；修改其他参数时，会在5秒钟到10分钟之内生效；
* 工作类型的修改必须在串口或USB口等有线连接的方式下进行，其他方式无法修改。但是可以修改除工作类型外的其他参数；
* 工作类型修改以后会造成大部分已抄到数据的丢失，必须重新补抄才可以；
* 工作类型必须和集中器表档案的工作类型一致，否则会出现工作异常。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 工作类型 | 1 | 0：定时定量数据；1：冻结数据；其他：无效 |
| 1 | 工作参数 | 1 | Bit7：数据补抄控制位，1为打开；0为关闭  Bit6：数据上传控制位，1为上传；0为关闭  Bit5-Bit0：保留 |
| 2 | 数据上传时间点 | 1 | BCD格式。在此时间点之前，数据量每够一包上传一次；在此时间点之后，收到表具数据即上传。 |
| 3 | 数据补抄日期 | 4 | 第一个字节：  Bit7：保留  Bit6-Bit0:代表日期1日到7日；  第二个字节：  Bit7-Bit0：代表日期8日到15日  第三个字节：  Bit7-Bit0：代表日期16日到23日  第四个字节：  Bit7-Bit0：代表日期24日到31日 |
| 4 | 数据补抄时间点 | 1 | BCD格式，数据补抄的时间，在此时间之后，集中器将对未抄到的表具数据进行主动补抄。 |
| 5 | 数据补抄的次数 | 1 | 数据补抄失败时重复补抄的次数，最大值为10。 |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 操作状态见注释14. |

## 集中器请求时间 0x4B

**命令说明**

此命令用于集中器向服务器请求当前的时间。

**上行**：空数据域

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 时钟数据 | 7 | 格式为：YY YY MM DD HH MM SS |

## 集中器重新启动 0x4C

**命令说明**

此命令用于重新启动集中器设备，集中器将在5秒钟内重新启动。

**下行**：空数据域

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 操作状态见注释14. |

## 集中器数据转发 0x4D

**命令说明**

此命令用于将数据通过集中器转发给目标节点，集中器到目标节点的路径由集中器负责组织。

注意：如果目标节点不存在于集中器的档案列表中，则不转发。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 命令字 | 1 | 集中器需要转发的命令 |
| 1 | 目标节点地址 | 6 | 接收该数据的目标节点地址 |
| 2 | 转发的数据 | N | 转发的数据 |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 命令字 | 1 | 集中器需要转发的命令 |
| 1 | 目标节点地址 | 6 | 接收该数据的目标节点地址 |
| 2 | 转发的结果 | 1 | 见注释14. |
| 2 | 转发的应答数据 | N | 目标节点的应答数据（包含下行场强和上行场强） |

## 读设备档案数量 0x50

**命令说明**

此命令用于读取集中器中所有档案数量，不分设备类型。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备类型 | 1 | 见注释2，当为全FF时表示全部设备的数量 |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备类型 | 1 | 见注释2，当为全FF时表示全部设备的数量 |
| 1 | 档案数量 | 2 | 16进制，低字节在前，高字节在后 |

## 读设备档案信息 0x51

**命令说明**

此命令按照条件读取集中器中的设备信息。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备类型 | 1 | 见注释2，当为全FF时表示全部设备的数量 |
| 1 | 起始序号 | 2 | 本次读取的起始节点序号，16进制，低字节在前，高字节在后。 |
| 2 | 读取的数量 | 1 | 本次读取的数量，16进制。 |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 节点总数量 | 2 | 集中器中所有该设备类型节点的总数量，低字节在前，高字节在后，当下行设备类型为FF时表示全部节点的数量 |
| 1 | 本次应答的数量 | 1 | 本次应答的节点数量 |
| 2 | N个节点的信息 | 8N | 8个字节为一组：  1-6：字节为节点的地址（BCD码）  7：设备类型，见注释2设备类型  8：最后一次抄表的结果0-失败，1-成功，2-未知 |

## 写设备档案信息 0x52

**命令说明**

此命令按照条件向集中器写入设备信息。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置节点的数量 | 1 | 本次设置节点的数量 |
| 1 | 最后一包标识 | 1 | 1: 最后一包；0：非最后一包 |
| 2 | N个节点的信息 | 8N | 8个字节为一组：  1-6：字节为节点的地址（BCD码）  7：设备类型，见注释2设备类型  8：最后一次抄表的结果1-成功，0-失败，默认为0 |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置节点的数量 | 1 | 本次设置节点的数量 |
| 1 | 设备的BCD码6字节 | 7N | N可通过总包长算出 |
| 操作状态1字节 | 见注释14 |

## 删除设备档案信息 0x53

**命令说明**

此命令将集中器中对应的设备档案删除。

注意：删除设备档案信息在删除此设备的同时，也会将以此设备为路由节点的路径全部删除，请谨慎操作。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | N个设备BCD码 | 6N | N可通过总包长算出 |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备BCD码6字节 | 7N | N可通过总包长算出 |
| 操作状态1字节 |  |

## 修改设备档案信息 0x54

**命令说明**

此命令将修改设备的ID号码或者设备类型。

注意：修改设备档案信息时，以此设备为路由的路径信息也会一并修改。

**下行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 13 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 原表号 | 6 |  |
| 1 | 新表号 | 6 |  |
| 2 | 设备类型 | 1 | 参见注释2：设备类型 |

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作的状态 | 1 | 见注释14 |

## 读设备自定义路由信息 0x55

**命令说明**

此命令从集中器中读取指定设备的自定义路由信息。

**下行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备BCD码 | 6 |  |

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 见注释14 |
| 1 | 设备BCD码 | 6 |  |
| 2 | 设备类型 | 1 | 见注释2 |
| 3 | 路径1的节点数量 | 1 | 不包括集中器和设备两个节点，为0时表示不存在此路径 |
| 4 | 路径1的信息 | 6N | 中继节点的地址列表，靠近集中器的地址写在前面，靠近目标节点的地址写在后面 |
| 5 | 路径2的节点数量 | 1 | 不包括集中器和设备两个节点，为0时表示不存在此路径 |
| 6 | 路径2的信息 | 6N | 中继节点的地址列表，靠近集中器的地址写在前面，靠近目标节点的地址写在后面 |

## 写设备自定义路由信息 0x56

**命令说明**

此命令将指定设备的自定义路由信息写入集中器中。

注意：当路径的节点数量为0时表示不存在这条路径，两条路径的数量都为0时，表示该节点不存在自定义路由信息。

**下行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备BCD码 | 6 | BCD码格式 |
| 1 | 路径1的节点数量 | 1 | 不包括集中器和表具两个节点 |
| 2 | 路径1的信息 | 6N | 中继节点的地址列表，靠近集中器的地址写在前面，靠近目标节点的地址写在后面 |
| 3 | 路径2的节点数量 | 1 | 不包括集中器和表具两个节点 |
| 4 | 路径2的信息 | 6N | 中继节点的地址列表，靠近集中器的地址写在前面，靠近目标节点的地址写在后面 |

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 7 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备BCD码 | 6 |  |
| 1 | 操作状态 | 1 | 见注释14 |

## 批量读设备自定义路由信息 0x57

**命令说明**

此命令批量读取设备的自定义路由信息。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 定长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 起始序号 | 2 | 本次读取的起始节点序号，16进制，低字节在前，高字节在后。 |
| 1 | 读取的数量 | 1 | 本次读取的数量，最大为10. |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 节点总数量 | 2 | 包括表具节点和路由节点 |
| 1 | 本次读取的数量 | 1 |  |
| 2 | 自定义路由信息 | N | 包括N个如下列表的自定义路由信息   |  |  | | --- | --- | | 类别 | 长度 | | 设备BCD码 | 6 | | 设备类型 | 1 | | 路径1的节点数量X | 1 | | 路径1的信息 | 6X | | 路径2的节点数量Y | 1 | | 路径2的信息 | 6Y |   其中：  设备类型见注释2；  路径节点数量不包括集中器和表具两个节点，为0时表示不存在此路径；  中继节点的地址列表，靠近集中器的地址写在前面，靠近目标节点的地址写在后面； |

## 批量写设备自定义路由信息 0x58

**命令说明**

此命令批量写入设备的自定义路由信息。写入的时候集中器会对路由信息进行检查，如果路由信息出错，则不会写入，还是保留原有的路由信息。

**下行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 自定义路由信息 | N | 包括N个如下列表的自定义路由信息   |  |  | | --- | --- | | 类别 | 长度 | | 设备BCD码 | 6 | | 路径1的节点数量X | 1 | | 路径1的信息 | 6X | | 路径2的节点数量Y | 1 | | 路径2的信息 | 6Y |   其中：  设备类型见注释2；  路径节点数量不包括集中器和表具两个节点，为0时表示不存在此路径；  中继节点的地址列表，靠近集中器的地址写在前面，靠近目标节点的地址写在后面； |

**上行**：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备BCD码 | 7N | N可通过总包长算出 |
| 操作状态1字节 | 见注释14 |

## 定时定量数据主动上传 0x61

**命令说明**

此命令由集中器发起，向服务器上传定时定量或者实时数据。本指令必须在主动上传功能打开的条件下有效。

**上行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 上传的数量 | 1 |  |
| 1 | 上传的数据 | N | 设备长地址+接收时的时间（格式为YYYYMMDDHH）+定时定量数据（格式见注释7）,当数据全为0时表示未抄到数据或数据格式错误； |

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作的状态 | 1 | 见注释14 |

## 冻结数据主动上传 0x62

**命令说明**

此命令由集中器发起，向服务器上传冻结数据。本指令必须在主动上传功能打开的条件下有效。

**上行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 上传的数量 | 1 |  |
| 1 | 上传的数据 | N | 设备长地址+冻结数据（格式见注释7）, 当数据全为0时表示未抄到数据或数据格式错误； |

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作的状态 | 1 | 见注释14 |

## 读集中器中的定时定量数据 0x63

**命令说明**

此命令由服务器发起，读取集中器中指定单个设备的定时定量数据。

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备BCD码 | 6 | 设备长地址 |

**上行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 30 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作的状态 | 1 | 见注释14 |
| 1 | 设备BCD码 | 6 | 设备长地址 |
| 2 | 时间+定时定量数据+下行上行信号强度 | 27 | 接收时的时间（格式为YYYYMMDDHH）+定时定量数据（格式见注释7）+下行上行信道强度，当数据全为0时表示未抄到数据或数据格式错误 |

## 读集中器中的冻结数据 0x64

**命令说明**

此命令由服务器发起，读取集中器中指定单个设备的冻结数据。

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 6 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设备BCD码 | 6 | 设备长地址 |

**上行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 82 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作的状态 | 1 | 见注释14 |
| 1 | 设备BCD码 | 6 | 设备长地址 |
| 2 | 冻结数据 | 89 | 冻结数据（格式见注释7）+下行上行信号强度，当数据全为0时表示未抄到数据或数据格式错误 |

## 批量读集中器中的定时定量数据 0x65

**命令说明**

此命令由服务器发起，读取集中器中指定序号开始，指定数量的定时定量数据。

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 起始序号 | 2 | 本次读取的起始节点序号，16进制，低字节在前，高字节在后。 |
| 1 | 读取的数量 | 1 | 本次读取的数量，最大为10. |

**上行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 节点总数量 | 2 | 包括表具节点和路由节点 |
| 1 | 本次读取的数量N | 1 | 1 |
| 2 | 定时定量数据 | N | 包括N个如下列表的定时定量数据   |  |  | | --- | --- | | 类别 | 长度 | | 操作的状态 | 1 | | 设备BCD码 | 6 | | 时间+定时定量数据+ | 27 | | 下行上行信号强度 | 2 |   其中：  操作的状态见注释14；  时间的格式为YYMMDD；  定时定量数据（格式见注释7）+下行上行信号强度，当数据全为0时表示未抄到数据或数据格式错误； |

## 批量读集中器中的冻结数据 0x66

**命令说明**

此命令由服务器发起，读取集中器中指定序号开始，指定数量的冻结数据。

**下行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 起始序号 | 2 | 本次读取的起始节点序号，16进制，低字节在前，高字节在后。 |
| 1 | 读取的数量 | 1 | 本次读取的数量，最大为10. |

**上行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 节点总数量 | 2 | 包括表具节点和路由节点 |
| 1 | 本次读取的数量N | 1 | 1 |
| 2 | 冻结数据 | N | 包括N个如下列表的定时定量数据   |  |  | | --- | --- | | 类别 | 长度 | | 操作的状态 | 1 | | 设备BCD码 | 6 | | 冻结数据 | 113 | | 下行上行信号强度 | 2 |   其中：  操作的状态见注释14；  冻结数据（格式见注释7）+下行上行信号强度（2），当数据全为0时表示未抄到数据或数据格式错误； |

## 集中器程序升级0xF1

**命令说明**

升级数据必须按顺序发送，集中器在收到写入地址为0时会擦除程序升级代码区，当收到的“写入地址+本包升级代码长度>=升级代码总长度”时，会进行Crc校验计算，成功则升级重启。

升级文件中如果含有"6009\*Boot"，表示有boot在里面，不能升级；升级文件中必须有"SRWF-"且在这个字符串后50个字节之内必须出现"Vsp"字符为合法升级文件。PC机可以读出这个字符串作为软件的版本信息，如"SRWF-6009-SR-20151008-Vsp0.10" 。

升级可以通过本地Debug端口（串口通讯）、本地USB端口(USB通讯)、无线手持机（RF通讯）、远程服务器（Gprs通讯）实行APP状态下升级，也可以通过本地Debug端口（串口通讯）实行BOOT状态下升级。

**下行**:

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 0/2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | CRC16 | 2 | 升级代码所有字节的CRC16计算值 |
| 1 | 写入地址 | 4 | 本包升级数据写入Flash的偏移地址（从0开始） |
| 2 | 升级代码总长度 | 4 | 升级代码总的字节数 |
| 3 | 本包升级代码长度 | 2 | 本数据包中升级代码的长度，必须为偶数 |
| 4 | 升级代码 | N | 升级代码数据 |

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 0/2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | CRC16 | 2 | 升级代码所有字节的CRC16计算值 |
| 1 | 写入地址 | 4 | 本包升级数据写入Flash的偏移地址（从0开始） |
| 2 | 操作结果 | 1 | 成功、失败或参数错误 |

## 集中器监控控制0xF2

**命令说明**

此功能用于监控集中器的监控数据，目前只有Gprs模块连接状态数据。但是，不能保证会输出所有的监控数据。上电后默认的输出通道是串口，如果串口没有输出，请刷新一下集中器的配置。

当使用RF模块进行调试的时候，不会有Gprs连接信息数据输出。

**下行**:

此命令无下行数据。

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 监控数据的类型 | 1 | 0：Gprs连接数据  其他保留 |
| 1 | 监控数据 | N |  |

## EEPROM存储区检查0xF3

**命令说明**

本命令用于检查存储数据的Eeprom是否已经损坏，该指令运行需要的时间较长，在运行期间尽量不要有数据通信。正常检查完毕后，原始的存储数据不会丢失。

注意：上行数据中的Eeprom种类并不是硬件上的容量，而是软件上定义的容量；

**下行**:空数据域

**上行：**

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 0/2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作结果 | 1 | 见注释14 |
| 1 | Eeprom种类 | 1 | 0：容量为64K字节的存储器  1：容量为128K字节的存储器 |
| 2 | 错误位置 | 4 | 当操作结果为错误时，本字段标记处发生错误的开始位置，低字节在前，高字节在后 |

# UART表端模块测试系统通讯协议（软件校准RF参数）

### 协议格式

|  |  |  |  |
| --- | --- | --- | --- |
| **NO** | **项目名称** | **字节** | **说明** |
|  | 前导码 | 2 | 0x55, 0x55 |
| 0 | 同步字 | 2 | 0xd3、0x91 |
| 1 | 包长 | 2 | 1到13（最后一个字段）的总长度，低字节在前 |
| 2 | 报文标识 | 1 | 0x10：PC下发命令  0xC0：表端返回命令 |
| 3 | 任务号 | 1 | 0 |
| 4 | 命令字 | 1 | 见相关命令字 |
| 5 | 设备类型 | 1 | 0xFB |
| 6 | 生命周期 | 1 | 0 |
| 7 | 路径信息 | 1 | 0x02 |
| 8 | 传输路径 | 12 | 0x55、0x55、0x55、0x55 、0x55、0x55  要设置的表ID,从高-低 |
| 9 | 数据域 | n | 详见注释22 |
| 10 | 下行信号强度 | 1 | 0x55 |
| 11 | 上行信号强度 | 1 | 0xAA |
| 12 | 校验字 | 1 | 1到11数值的CRC8校验，详见“注释12，CRC8校验” |
| 13 | 结束符 | 1 | 0x16 |

### 注释19，命令字详解（数据域低字节在前，高字节在后）

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 命令字 | 注释 | |
| 1 | 0x3A | 1. **读取模块运行参数**（包括表ID+程序版本号+相关运行参数）总长度：124byte 2. 高字节在前，低字节在后 | |
| 2 | 0x3B | 1. **设置模块为休眠、接收、发射模式、读取模块的基准频率和发射功率、退出测试模式** 2. **数据域：** 3. **休眠电流测试：** 4. **进入发射状态：** 5. **读取基准频率和发射功率：** 6. **设置基准频率和发射功率：** 7. **进入接收模式：** 8. **读取模块接收误码率：** 9. **退出RF测试模式:** 10. **开关阀门测试开始** 11. **读取阀门测试结果** 12. **测试计量电路状态** 13. **测试LCD硬件状态** 14. **读取模块的测试标志** 15. **写模块的测试状态** 16. 休眠时：RF载波侦听模式关闭，RF射频芯片深度休眠 | |
| 3 | 0x3C | LORAWAN模块通讯相关命令 | 子命令0X01: LORAWAN入网成功命令 |
| 子命令0X02: LORAWAN模块数据发射完成，请求掉电处理数据帧 |
| 子命令0X03:接收来自LORAWA模块发出的设置指令 |
| 子命令0X04:给LORAWAN模块持续供电 |
| 子命令0X05:给LORAWAN模块断电 |
| 子命令0X06:让LORAWAN进入BOOT模式 |
| 子命令0X07:读LORAWAN模块的EUI |
| 子命令0X08:清LORAWAN模块的入网信息 |
| 子命令0X09:设置LORAWAN模块的**DEVEUI、APPEUI、appkey编号** |
|  |
| NB-IOT模块通讯相关命令 | 子命令0X10: NB-IOT入网成功 |
| 子命令0X11: NB-IOT的UART数据接收正常 |
| 子命令0X12: NB-IOT的UART数据校验错误 |
| 子命令0X13: NB-IOT数据发射完成，请求断电处理 |
|  |
|  |
|  |
| **数据透传命令** | 子命令0X20: 串口下发的控制命令帧 |
| 子命令0X21: 串口下发的读取终端状态的命令帧 |
| 子命令0X22: 串口收到终端故障告警数据帧 |
| 子命令0X23: 设置变频器频率 |
| 子命令0X24: 读变频器参数 |
| 4 | 0x3D | 设置命令  （bit7:1） | 子命令0X81：设置模块的ID号, 客户使用功能 |
| 子命令0X82：设置模块的RXD信道 |
|  |
|  |
| 读取命令  （bit7:0） |  |
|  |
|  |
|  |
| 5 | 0x3E | **预留** | |
| 6 | 0x3F | **设置表端运行参数命令** | |

### 注释20，读取设置基准频率和发射功率

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 项目 | 占用字节长度 | 注释 |
| 0 | 基准接收频率 | 3byte | T0 T1 T2，低字节在前，高字节在后,单位为：KHZ |
| 1 | RF输出功率 | 1byte | RF芯片的输出功率, 0到20自然数，单位：dBm |

### 注释21，读取模块接收误码率(总电平错误数/总脉冲个数=误码率)

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 项目 | 占用字节长度 | 注释 |
| 0 | 模块接收的总脉冲个数 | 4byte | T0 T1 T2 T3，低字节在前，高字节在后 |
| 1 | 接收电平总错误数 | 4byte | T0 T1 T2 T3，低字节在前，高字节在后 |

### 注释22：设置LORA水气表端模块运行参数的数据域结构

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **NO** | **地址DEC** | **总长度:** | **上传长度: 124 byte下发长度: 84byte** | | | |
| **内容** | **长度** | **单位** | **默认值** | **说明** |
| 0 | 0 | 表类型 | 1 |  | 0x10 | 参见设备类型定义 |
| 1 | 1 | 脉冲系数 | 1 |  | 1 | 注释6：脉冲系数 |
| 2 | 2 | 磁干扰开阀时间 | 1 | 1秒 | 50 |  |
| 3 | 3 | 计量脉冲最小闭合时间 | 1 | 1毫秒 | 100 |  |
| 4 | 4 | 开关阀时间 | 2 | 1毫秒 | 12000 | 最大65535mS |
| 5 | 6 | 过流阀值 | 1 | 单位：mA | 150 |  |
| 6 | 7 | 电池电压类型 | 1 |  | 0 | B1B0: 01 – 6V 00 – 3.6V |
| 7 | 8 | 定时上传时间间隔 | 1 | 小时 | 120 | 默认：120，值为0关闭此功能 |
| 8 | 9 | 定量上传数量间隔 | 1 | M³ | 2 | 默认：2，值为0关闭此功能 |
| 9 | 10 | 每天定时定量最大上传次数 | 1 |  | 3 | 0：定时定量关闭，当设定的上报数据大于250时，即上报不受限制 |
| 10 | 11 | 计量传感器类型 | 1 |  | 0x01 | 注释5：计量传感器类型及信道 |
| 11 | 12 | **基准接收频率** | 3 |  | 470000 |  |
| 12 | 15 | **接收信道** | 1 |  | 0x63 | 注释5：计量传感器类型及信道  Bit0---bit3:载波侦听信道  值范围见注释5：  Bit4---bit7:集中器应答信道  值范围见注释5： |
| 13 | 16 | **发射信道** | 1 |  | 9 | 值范围见注释5： |
| 14 | 17 | **发射功率** | 1 |  | Ox14 | 0到20自然数，单位：dBm |
| 15 | 18 | 水表防锈定时间隔 | 1 | **天** | **10** | 默认10天 |
| 16 | 19 | 系统调试级别 | 1 |  | 0 | 为0表示不输出调式信息 |
| 17 | 20 | 运营商编号 | 4 |  | 11223344 | 默认高位在前 |
| 18 | 24 | 出厂/RF设定的系统时间 | 7 |  | 当前系统时间 | YY YY MM DD HH MM SS |
| 19 | 31 | 预留 | 1 |  |  |  |
| 20 | 32 | 预留 | 1 |  |  |  |
| 21 | 33 | 预留 | 1 |  |  |  |
| 22 | 34 | 预留 | 1 |  |  |  |
| 23 | 35 | 剩余用量报警限值 | 1 |  |  |  |
| 24 | 36 | 剩余用量关阀值 | 2 |  | 0 | 低位在前  BIT 15：为0 表示负数  BIT 15：为1 表示负数 |
| 25 | 38 | 预缴费量数  （后台下发的值） | 6 |  | 0 |  |
| 26 | 44 | 参考起始用量 | 6 |  | 0 |  |
| 27 | 50 | 模块测试状态 | 2 |  | 0 | **低字节在前，高字节在后**  BIT0：休眠电流测试OK  BIT1：频率测试OK  BIT2：功率测试OK  BIT3：发射功率测试OK  BIT4：接收灵敏度测试OK  BIT5：接收电流测试OK  BIT6：阀控电路测试OK  BIT7：计量电路测试OK  BIT8：LCD测试OK  BIT9： |
|  | 52 | 预留 | 2 |  | 0 |  |
|  | 54 | **正转用量** | 6 |  | 0 |  |
|  | 60 | 反转用量 | 6 |  | 0 |  |
|  | 66 | 阀状态 | 1 |  | 00 | 阀状态默认值：0x00 |
|  | 67 | 功能使能状态 | 2 |  | 0x0210 | 注释18：表端运行参数位定义，抵字节在前 |
|  | 69 | 报警状态标志位 | 2 |  | 0 | 清空所有报警状态位 |
|  | 71 | 按日按月设置 | 1 |  | 0 | 代表“RF侦听起始时间”代表的是小时还是日期 |
|  | 72 | RF侦听起始时间 | 1 |  | 0 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
|  | 73 | RF侦听工作时长 | 1 |  | 24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
|  | 74 | 预留 | 10 |  |  |  |
| 33 | 84 | 模块软件版本号 | 40 |  | 0 | RF: 数据长度124。  软件版本号：ASCII |

### 注释23：设置NB-IOT水气表端模块运行参数的数据域结构

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **NO** | **地址DEC** | **总长度:** | **上传长度: 124 byte下发长度: 84 byte** | | | |
| **内容** | **长度** | **单位** | **默认值** | **说明** |
| 0 | 0 | 表类型 | 1 |  | 0x10 | 参见设备类型定义 |
| 1 | 1 | 脉冲系数 | 1 |  | 1 | 注释6：脉冲系数 |
| 2 | 2 | 磁干扰开阀时间 | 1 | 1秒 | 50 |  |
| 3 | 3 | 计量脉冲最小闭合时间 | 1 | 1毫秒 | 100 |  |
| 4 | 4 | 开关阀时间 | 2 | 1毫秒 | 12000 | 最大65535mS |
| 5 | 6 | 过流阀值 | 1 | 单位：mA | 150 |  |
| 6 | 7 | 电池电压类型 | 1 |  | 0 | B1B0: 01 – 6V 00 – 3.6V |
| 7 | 8 | 定时上传时间间隔 | 1 | 小时 | 120 | 默认：120，值为0关闭此功能 |
| 8 | 9 | 定量上传数量间隔 | 1 | M³ | 2 | 默认：2，值为0关闭此功能 |
| 9 | 10 | 每天定时定量最大上传次数 | 1 |  | 3 | 0：定时定量关闭，当设定的上报数据大于250时，即上报不受限制 |
| 10 | 11 | 计量传感器类型 | 1 |  | 0x01 | 注释5：计量传感器类型及信道 |
| 11 | 12 | **IP的第1个字节** | 1 | 16进制 | 79 | NB-IOT的IP+连接端口：  121.43.175.222,5683 |
| 12 | 13 | **IP的第2个字节** | 1 | 16进制 | 2B |
| 13 | 14 | **IP的第3个字节** | 1 | 16进制 | AF |
| 14 | 15 | **IP的第4个字节** | 1 | 16进制 | DE |
| 15 | 16 | **服务器连接端口** | 1 | 16进制 | 33 |
| 16 | 17 | 1 | 16进制 | 16 |
| 17 | 18 | 水表防锈定时间隔 | 1 | **天** | **10** | 默认10天 |
| 18 | 19 | 系统调试级别 | 1 |  | 0 | 为0表示不输出调式信息 |
| 19 | 20 | 运营商编号/SIM卡类型 | 4 |  | 46001000 | 默认高位在前  LORA时：11223344  NB-IOT时：46001000 |
| 20 | 24 | 出厂/RF设定的系统时间 | 7 |  | 当前系统时间 | YY YY MM DD HH MM SS |
| 21 | 31 | 通信频段 | 1 |  | 8 | 中国电信：5  中国移动：8  中国联通：8或3 |
| 22 | 32 | NB连接方式 | 1 |  | 2 | 1：COAP  2：UDP |
| 23 | 33 | 预留 | 1 |  |  |  |
| 24 | 34 | 预留 | 1 |  |  |  |
| 25 | 35 | 剩余用量报警限值 | 1 |  |  |  |
| 26 | 36 | 剩余用量关阀值 | 2 |  | 0 | 低位在前  BIT 15：为0 表示负数  BIT 15：为1 表示负数 |
| 27 | 38 | 预缴费量数  （后台下发的值） | 6 |  | 0 |  |
| 28 | 44 | 参考起始用量 | 6 |  | 0 |  |
| 29 | 50 | 模块测试状态 | 2 |  | 0 | **低字节在前，高字节在后**  BIT0：休眠电流测试OK  BIT1：频率测试OK  BIT2：功率测试OK  BIT3：发射功率测试OK  BIT4：接收灵敏度测试OK  BIT5：接收电流测试OK  BIT6：阀控电路测试OK  BIT7：计量电路测试OK  BIT8：LCD测试OK  BIT9： |
| 30 | 52 | 预留 | 2 |  | 0 |  |
| 31 | 54 | **正转用量** | 6 |  | 0 |  |
| 32 | 60 | 反转用量 | 6 |  | 0 |  |
| 33 | 66 | 阀状态 | 1 |  | 00 | 阀状态默认值：0x00 |
|  | 67 | 功能使能状态 | 2 |  | 0x0210 | 注释18：表端运行参数位定义，抵字节在前 |
|  | 69 | 报警状态标志位 | 2 |  | 0 | 清空所有报警状态位 |
|  | 71 | 按日按月设置 | 1 |  | 0 | 代表“RF侦听起始时间”代表的是小时还是日期 |
|  | 72 | RF侦听起始时间 | 1 |  | 0 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
|  | 73 | RF侦听工作时长 | 1 |  | 24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
|  | 74 | 预留 | 10 |  |  |  |
| 33 | 84 | 模块软件版本号 | 40 |  | 0 | RF: 数据长度124。  软件版本号：ASCII |

### 实例数据解析

#### 读取模块ID号和相关参数（命令字：0x3A）

##### 功能简介：

1. 此命令可读出UART设置的所有运行参数，包括表ID和程序版本号

##### 下行命令：

1. 空数据域

##### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 模块运行参数 | 84 | 详见注释22 |
| 1 | 程序版本号 | 40 | 数据格式：ASCII |

##### 实例数据：

1. **TXD:** 55 55 D3 91 18 00 10 00 3A FA 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 55 AA 3E 16 1E 03 19
2. **RXD:** D3 91 94 00 C0 00 3A FA 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 10 01 32 64 E0 2E 96 00 78 02 03 31 F0 2B 07 83 09 F0 0A 00 11 22 33 44 20 16 07 15 17 48 01 00 03 02 01 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F2 04 00 00 64 00 00 00 00 00 00 00 8A 31 02 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 52 57 46 2D 36 30 30 39 41 2D 44 45 2D 42 44 44 41 42 32 30 2D 32 30 31 36 30 37 32 31 2D 56 74 30 2E 30 37 20 20 20 AA AA FA 16

#### 测试模块射频参数（命令字：0x3B）

##### 休眠电流测试【命令字: 0x01】：

###### 功能简介：

1. 模块收到此命令后进入深度休眠状态，系统关闭RFIC

2. 模块在收到命令并返回应答数据后，关闭UART, 复位解除

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令字0x01 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令字0x01 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA（成功）或0xAB（失败） |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D401 55 AAF6 16

**RXD:** D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 01 AA 55 AA 49 16

##### 切换为发射模式【命令字: 0x02】：

###### 功能简介：

1. 模块收到此命令后进入发射模式

2。在此模式下可以更改模块的发射功率和中心频点。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x02 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| -0 | 子命令 | 1 | 命令0x02 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 02 55 AA 12 16

**RXD:**D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 02 AA 55 AA C1 16

##### 读取基准频率和发射功率【命令字: 0x03】：

###### 功能简介：

1. 读取模块当前执行的发射功率和中心频率

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x03 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2或6 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x03 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |
| 2 | 当前基准频率 | 3 | 基准频率。单位为：KHZ，低位在前，高在后 |
| 3 | 当前发射功率 | 1 | 发射功率。0到20自然数，单位：dBm |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 03 55 AA B9 16

**RXD:** D3 91 1E 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 03 AA F0 2B 07 14 55 AA 9f 16

##### 设置基准频率和发射功率【命令字: 0x04】：

###### 功能简介：

1. 设置模块的中心频点和发射功率，

2. 模块每设置一次系统频率和功率，系统主动复位一次，执行新设置的中心频率和功率。±

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x04 |
| 1 | 当前基准频率 | 3 | 基准频率, 单位为：KHZ，低位在前，高在后 |
| 2 | 当前发射功率 | 1 | 发射功率，0到20自然数，单位：dBm |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2或3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x04 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |
| 2 | 错误类型 | 1 | Bit0：设置的中心频率大小越界  Bit1：中心频率写EEPROM错误  Bit2：功率写EEPROM错误  Bit3： |

###### 实例数据：

\*\*\*\*\*470Mhz/20dBm

**TXD:**55 55 D3 91 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 04 F0 2B 07 1455 AA B8 16

**RXD:**D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 04 AA 55 AA C8 16

\*\*\*\*\*470.500Mhz/20dBm

**TXD:**55 55 D3 91 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D404 E4 2D 07 14 55 AA A3 16

**RXD:** D3 91 1B 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 04 AB 01 55 AA 60 16

\*\*\*\*\*470.02Mhz/20dBm

**TXD:**55 55 D3 91 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 04 04 2C 07 14 55 AA 47 16

**RXD:**D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 04 AA 55 AA C8 16

\*\*\*\*\*470Mhz/16dBm

**TXD:**55 55 D3 91 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 04 F0 2B 07 1055 AA 26 16

**RXD:**D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 04 AA 55 AA C8 16

##### 切换为接收模式【命令字: 0x05】：

###### 功能简介：

1. 模块收到此命令后进入接收模式

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x05 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x05 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D405 55 AA 68 16

**RXD:** D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 05 AA 55 AA 47 16

##### 读取模块接收误码率【命令字: 0x06】：

###### 功能简介：

1. 模块在没有接信号发生器是，读取的“总脉冲数”和“总错误数”都为0.

2. 误码率 = 总错误数 / 总脉冲数

3. 每次读取误码率后其“总脉冲数”和“总错误数”自动归0

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x06 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2或10 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x06 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |
| 2 | 总脉冲数 | 4 | 模块接收的总脉冲个数 |
| 3 | 总错误数 | 4 | 接收电平总错误数，  误码率 = 总错误数 / 总脉冲数 |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 06 55 AA 8C 16

**RXD:** D3 91 22 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 06 AA 00 00 00 00 00 00 00 00 55 AA 02 16

##### 退出RF测试模式【命令字: 0x07】：

###### 功能简介：

1. RF参数测试完成后退出测试模式。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x07 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x07 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D40755 AA 27 16

**RXD:** D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 07 AA 55 AA 40 16

##### 阀门测试开始【命令字: 0x08】：

###### 功能简介：

1. 模块收到此命令后开始执行开关阀门动作，开和关分别执行一次。

2. 执行完后才响应读取阀门测试结果命令。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x08 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x08 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 08 55 AA 78 16

**RXD:**D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 08 AA 55 AA DA 16

##### 读取阀门测试结果【命令字: 0x09】：

###### 功能简介：

1. 模块收到此命令后进入发射模式

2. 进入测试模式后，PC只需要发一次"“读测试结果命令”之后进入等待状态，表端执行完阀门后返回应答数据帧，告知测试的结果。

3. 表端在收到“读测试结果命令”后任务挂起，等阀门执行完后再执行读测试结果命令，然后回送阀门的测试结果。如果失败并告知其失败的原因。

4. 测试系统需要解析出错误失败原因。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x09 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2或3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x09 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |
| 2 | 操作结果 | 1 | Bit0为0时：开阀门异常  Bit1为0时：关阀门异常  Bit2：测试未完成  Bit3：阀门测试不通过 |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 09 55 AA D3 16

**RXD:** D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 09 AA 55 AA 55 16

**RXD:** D3 91 1B 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 09 AB 00 55 AA 27 16

##### 测试计量电路硬件状态【命令字: 0x0A】：

###### 功能简介：

1. 模块收到命令后回送测试结果，如果失败会告知失败的原因。

2, 测试系统需要显示失败的原因。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x0A |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2或3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x0A |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |
| 2 | 错误类型 | 1 | Bit0：CHC 硬件电路故障  Bit1：CHB 硬件电路故障  Bit2：CHA 硬件电路故障 |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D40A55 AA 37 16

**RXD:**D3 91 1B 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 0A AB 07 55 AA 13 16

##### 测试LCD硬件电路状态【命令字: 0x0B】：

###### 功能简介：

1. 模块收到此命令后进入发射模式

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x0B |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x0B |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 0B 55 AA52 16

**RXD:**

##### 写模块各功能的测试状态【命令字: 0x0C】：

###### 功能简介：

1. 本字节记录了模块各个功能的测试状态。

2. 本字节的所有内容都是由测试系统写入的。

3. 测试在退出测试模式前写入此值。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 3 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x0C |
| 1 | 操作结果 | 2 | **低字节在前，高字节在后**  BIT0：休眠电流测试OK  BIT1：频率测试OK  BIT2：功率测试OK  BIT3：发射电流测试OK  BIT4：接收灵敏度测试OK  BIT5：接收电流测试OK  BIT6：阀控电路测试OK  BIT7：计量电路测试OK  BIT8：LCD测试OK  BIT9： |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x0C |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |

###### 实例数据：

**TXD:** 55 55 D3 91 1B 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 0C00 00 55 AA28 16

**TXD:** 55 55 D3 91 1B 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 0C01 01 55 AA C3 16

**RXD:** D3 91 1A 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 0C AA 55 AA D4 16

##### 读模块各功能的测试状态【命令字: 0x0D】：

###### 功能简介：

1. 本字节记录了模块各个功能的测试状态，

2. 本字节的所有内容都是由测试系统写入的。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 下发命令0x0D |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2或4 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令0x0D |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |
| 1 | 操作结果 | 2 | **低字节在前，高字节在后**  BIT0：休眠电流测试OK  BIT1：频率测试OK  BIT2：功率测试OK  BIT3：发射电流测试OK  BIT4：接收灵敏度测试OK  BIT5：接收电流测试OK  BIT6：计量电路测试OK  BIT7：阀控电路测试OK  BIT8：LCD测试OK  BIT9： |

###### 实例数据：

**TXD:** 55 55 D3 91 19 00 10 01 3B FB 9F 02 19 21 68 00 10 66 D4 D4D4D4D4D4 0D 55 AA 83 16

**RXD:** D3 91 1C 00 C0 01 3B FB 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 0D AA 01 01 55 AA A7 16

#### 测试模块射频参数（命令字：0x3D）

##### 设置模块ID号【命令字: 0x81】：

###### 功能简介：

本功能通过UART设置模块ID号。

方便客户更改模块ID

新表号从协议数据帧的目标ID里面取

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令字0x81 |
| 1 | 操作密钥 | 7 | 0x5A, 0x5B, 0x5C, 0x5D, 0x5E, 0x5F, 0x60, |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令字0x01 |
| 1 | 操作结果 | 1 | 返回的操作结果 0xAA（成功）或0xAB（失败） |

###### 实例数据：

**TXD:**

**RXD:**

##### 设置模块RXD信道【命令字: 0x82】：

###### 功能简介：

本功能通过UART设置模块的接收信道。

新主机模块的默认信道为3（固定不可设置）和8信道。

###### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令字0x02, 读取信道号，此时默认信道号为00 |
| 命令字0x82, 设置信道号 |
| 1 | 操作密钥 | 7 | 0x5A, 0x5B, 0x5C, 0x5D, 0x5E, 0x5F, 0x60, |
| 2 | 信道号 | 1 | 设置接收的2个信道号，   * + - 1. bit4—bit7位：固定为3，       2. bit0—bit3位：当前接收信道号。 |

###### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 2 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 子命令 | 1 | 命令字0x02 |
| 1 | 操作结果 |  |  |
| 2 | 信道号 | 1 | 当前接收的2个信道号，   * + - 1. bit4—bit7位：固定为3，       2. bit0—bit3位：当前接收信道号。 |

###### 实例数据：

**TXD:**

**RXD:**

#### 设置表端运行参数命令（命令字：0x3F）

##### 功能简介：

1. 模块在生产时设置模块的ID号和相关运行参数。

##### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 序号 | 段标识 | 段大小 | 段说明 |
| 0 | 运行参数 | 84 | 详见注释22：设置表端模块运行参数的数据域结构 |

##### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作结果 | 1 | 返回的操作结果 0xAA或0xAB |

##### 实例数据：

**TXD:**55 55 D3 91 6C 00 10 00 3F FA 9F 02 19 21 68 00 10 66 01 16 04 19 00 03 10 01 32 64 E0 2E AA 00 78 02 03 31 F0 2B 07 83 09 F0 0A 00 11 22 33 44 20 16 07 25 11 59 19 00 03 02 01 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA 93 16 1E 03 19

RXD: D3 91 19 00 C0 00 3F FA 9F 02 01 16 04 19 00 03 19 21 68 00 10 66 AA 00 00 FE 16

# 表端的数据存储

没有特别说明，都以HEX 方式存储, 整数存储都是低字节再前，高字节在后；整数和小数的存储一般是整数在前，小数在后。**日期的存储格式**: 3个字节:（ YYYYY\*16+MM) , DD

**时间的存储格式**: 3个字节日期{（ YYYYY\*16+MM) , DD } + 3 个字节的时分秒 { HH MM SS }

**大概时间的存储格式**：4个字节 ((((YYYY-2000)\*16+MM)\*32+DD)\*32+HH)\*64+MM

**短日期的存储格式**：2个字节（YY : 7; MM:4; DD: 5）

# LORA水表EEPROM的存储结构（存储空间：4Kbyte）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **相对地址** | **内容** | **长度byte** | **Buf位置** | **单位** | **1. 系统基本运行参数：1024 byte。**  **2. 冻结数据占用空间：2816 byte。** |
| 00 | 表ID | 6 | **0** |  | 从高-低，  当长度大于12位时存储地址改为为84 |
| 表类型 | 1 | **6** |  | 参见设备类型定义 |
| 脉冲系数 | 1 | **7** |  | 单位：个脉冲/方(吨)(注：可选4个值：0,1,2,3(分别为1个10个100个1000脉冲一方) |
| 磁干扰开阀时间 | 1 | **8** | 1秒 | 磁干扰消失后延时开阀的时间 |
| 计量脉冲最小闭合时间 | 1 | **9** | 1毫秒 | 干簧管的最短闭合脉宽 |
| 开关阀时间 | 2 | **10** | 1毫秒 | 阀超时门限 |
| 过流阀值 | 1 | **12** | 单位：mA |  |
| 电池电压类型 | 1 | **13** |  | B1B0:  00 – 3.6V  01 – 6V  10 – 4.5V |
| 定时上传时间间隔 | 1 | **14** | 小时 | 0,不定时上传 |
| 定量上传数量间隔 | 1 | **15** | 方/吨 | 0,不定时上传 |
| 每天定时定量最大上传次数 | 1 | **16** |  | 默认:3，  0：定时定量关闭，当设定的上报数据大于250时，即上报不受限制 |
| 计量传感器类型 | 1 | **17** |  | 注释5：计量传感器类型及信道 |
| **基准接收频率** | 3 | **18** |  | 校准系统中心频率使用，系数：1000  接收频率 = **基准接收频率 x** 1000 |
| **接收信道** | 1 | **21** |  | 注释5：计量传感器类型及信道  Bit0---bit3:载波侦听信道  值范围见注释5：  Bit4---bit7:集中器应答信道  值范围见注释5： |
| **发射信道** | 1 | **22** |  | 值范围见注释5：  默认9信道, |
| **发射功率** | 1 | **23** |  | 0到20自然数，单位：dBm |
| 水表防锈定时间隔 | 1 | **24** | **天** | 默认：10天 |
| 系统调试级别 | 1 | **25** |  | 为0表示不输出调式信息 |
| 运营商编号 | 4 | **26** |  | 默认：11223344 |
| CRC8校验 | 1 | **30** |  | 1到29的数据校验 |
| SUM校验 | 1 | **31** |  |  |
| 32 | 出厂/RF设定的系统时间 | 7 | **32** |  | 出厂/RF设定的原始时间 |
| 预留 | 1 | **39** |  |  |
| 预留 | 1 | **40** |  |  |
| 预留 | 1 | **41** |  |  |
| 预留 | 1 | **42** |  |  |
| 剩余用量报警限值 | 1 | **43** |  | 增值提示 |
| 剩余用量关阀值 | 2 | **44** |  | BIT 15：为0表示负数  BIT 15：为1 表示负数 |
| 模块剩余的可用量数  （后台下发的值） | 6 | **46** |  | **户表依靠这个值，来决定是否报警和关闭阀门** |
| 参考起始用量 | 6 | **52** |  | 计算剩余用量时使用的当前累计参考量。 |
| 预留 | 2 | **58** | 0 |  |
| 预留 | 2 | **60** |  |  |
| CRC8校验 | 1 | **62** |  | 32到61的数据校验 |
| SUM校验 | 1 | **63** |  |  |
| 64 | **正转用量** | 6 | **64** |  | 参见 |
| 反转用量 | 6 | **70** |  |  |
| 阀状态 | 1 | **76** |  | **B0,B1:阀门当前状态**  B2,B3: 阀门期望的背景值  B4:正处于磁干扰过程中标志  B5:磁干扰消失后等待延时再动阀的过程中，延时到了后再视磁干扰前阀门状态另行处理。默认值：**0**  **B6,B7: 阀门原始状态，只有RF可以更改其状态。默认为关状态**  00：阀门故障  01：开阀  10：关阀  11：阀门未知 |
| 功能使能状态 | 2 | **77** |  | 参见’注释19：表端运行参数位定义’ |
| 报警状态标志位 | 2 | **79** |  | 默认0 |
| 按日按月设置 | 1 | **81** | 0 | 代表“RF侦听起始时间”代表的是小时还是日期 |
| RF侦听起始时间 | 1 | **82** | 0 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
| RF侦听工作时长 | 1 | **83** | 24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
| 20位表端ID | 10 | **84** | 0 | 表端ID，最大20位 |
| CRC8校验 | 1 | **94** |  | 64到93的数据校验 |
| SUM校验 | 1 | **95** |  |  |
| 96 | 内存紊乱校验区 | 7 | **96** |  | 7个固定的值，用来比较内存是否紊乱 |
| SUM校验 | 1 | **103** |  |  |
| 104 | 集中器号 | 6 | **104** |  | 所属集中器号 |
| 预留 | 1 | **110** |  |  |
| SUM校验 | 1 | **111** |  |  |
| 112 | 正转用量备份区1 | 6 | **112** |  |  |
| 预留 | 1 | **118** |  |  |
| SUM校验 | 1 | **119** |  |  |
| 120 | 反转用量备份区1 | 6 | **120** |  |  |
| 预留 | 1 | **126** |  |  |
| SUM校验 | 1 | **127** |  |  |
| 128 | 路由路径长度 | 1 | **128** |  | 第一条路径长度 |
| 第一条路由路径 | 30 | **129** |  | 6\*5=30，最大支持5级路径 |
| SUM校验 | 1 | **159** |  |  |
| 160 | 路由路径长度 | 1 | **160** |  | 第二条路径长度 |
| 第二条路由路径 | 30 | **161** |  | 6\*5=30，最大支持5级路径 |
| SUM校验 | 1 | **191** |  |  |
| 192 | 密钥长度 | 1 | **192** |  | 默认长度：16byte |
| 表端密钥 | 16 | **193** |  | AES128加密使用 |
| 保留 | 6 | **209** |  |  |
| SUM校验 | 1 | **215** |  |  |
| 216 | 正转用量 备份区2 | 6 | **216** |  |  |
| 预留 | 1 | **222** |  |  |
| SUM校验 | 1 | **223** |  |  |
| 224 | 反转用量 备份区2 | 6 | **224** |  |  |
| 预留 | 1 | **230** |  | OPERATORSNUMBER |
| SUM校验 | 1 | **231** |  |  |
| 232 | 发射次数 | 2 | **232** |  | 默认：0 |
| 接收次数 | 2 | **234** |  | 默认：0 |
| 开关阀次数 | 2 | **236** |  | 默认：0 |
| 磁干扰次数 | 1 | **238** |  | 默认：0 |
| SUM校验 | 1 | **239** |  | ,**需要初始化EEPROM** |
| 240 | 预留 | 3 | **240** |  |  |
| 计量增加的脉冲数 | 1 | **243** | MAX: 255 | DB\_TON\_PULSE |
| 计量传感器两个状态间的次数 | 1 | **244** |  | A\_TO\_B\_TIME |
| 计量传感器所期望的下个状态值 | 1 | **245** |  | DB\_PULSE\_NEXT\_PTR |
| 正反转标志 | 1 | **246** |  | AWAKENING |
| SUM校验 | 1 | **247** |  |  |
| 248 | 掉电前的系统时间 | 7 | **248** |  | 系统掉电要保存的数据 |
| SUM校验 | 1 | **255** |  |  |
| 256 | EEPROM写次数 | 4 | **256** |  | 低字节在前，高字节在后 |
| 预留 | 27 | **260** |  |  |
| SUM校验 | 1 | **287** |  |  |
| 288 | 定时上传的时隙号 | 2 | **288** |  | 低字节在前，高字节在后  只有冻结上传时才用到时隙号 |
| 单位系统下的总表数 | 2 | **290** |  | 低字节在前，高字节在后  此集中器下的设备数量总和 |
| 测试系统的测试状态 | 2 | **292** | 0 | 保存测试系统下发的各个表端测试项目的测试状态。  默认为0：表示各个功能模块未测试成功 |
| 预留 | 1 | **294** |  |  |
| SUM校验 | 1 | **295** |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **冻结数据存放区（占用空间2816 byte）：**   * + - 1. **系统每间隔30分钟冻结一次数据**       2. **每次只能抄取一天的数据**       3. **11天滚动存储。**       4. **数据长度为4byte起始时间 + 100byte冻结数据+1byte写标志位 +1byte段号 + 1byte数据CRC8校验** | | | | | |
| 1280 | **4byte时间信息** | 4 |  | 存储区1  开始 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |
| 2656 | **4byte时间信息** | 4 |  | 存储区1  结束 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |
| 2688 | **4byte时间信息** | 4 |  | 备份区  开始 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |
| O4064 | **4byte时间信息** | 4 |  | 备份区  结束 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |

# NB-IOT水表EEPROM的存储结构（存储空间：4Kbyte）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **相对地址** | **内容** | **长度byte** | **Buf位置** | **单位** | **1. 系统基本运行参数：1024 byte。**  **2. 冻结数据占用空间：2816 byte。** |
| 00 | 表ID | 6 | **0** |  | 从高-低，  当长度大于12位时存储地址改为为84 |
| 表类型 | 1 | **6** |  | 参见设备类型定义 |
| 脉冲系数 | 1 | **7** |  | 单位：个脉冲/方(吨)(注：可选4个值：0,1,2,3(分别为1个10个100个1000脉冲一方) |
| 磁干扰开阀时间 | 1 | **8** | 1秒 | 磁干扰消失后延时开阀的时间 |
| 计量脉冲最小闭合时间 | 1 | **9** | 1毫秒 | 干簧管的最短闭合脉宽 |
| 开关阀时间 | 2 | **10** | 1毫秒 | 阀超时门限 |
| 过流阀值 | 1 | **12** | 单位：mA |  |
| 电池电压类型 | 1 | **13** |  | B1B0:  00 – 3.6V  01 – 6V  10 – 4.5V |
| 定时上传时间间隔 | 1 | **14** | 小时 | 0,不定时上传 |
| 定量上传数量间隔 | 1 | **15** | 方/吨 | 0,不定时上传 |
| 每天定时定量最大上传次数 | 1 | **16** |  | 默认:3，  0：定时定量关闭，当设定的上报数据大于250时，即上报不受限制 |
| 计量传感器类型 | 1 | **17** |  | 注释5：计量传感器类型及信道 |
| IP的第1个字节 | 1 | **18** | **1个字节** | NB-IOT的IP+连接端口：  121.43.175.222,5683 |
| IP的第2个字节 | 1 | **19** | **1个字节** |
| IP的第3个字节 | 1 | **20** | **1个字节** |
| IP的第4个字节 | 1 | **21** | **1个字节** |
| 服务器连接端口 | 2 | **22** | **2个字节** |
| 水表防锈定时间隔 | 1 | **24** | **天** | 默认：10天 |
| 系统调试级别 | 1 | **25** |  | 为0表示不输出调式信息 |
| SIM卡类型 | 4 | **26** |  | 默认：46001000 |
| CRC8校验 | 1 | **30** |  | 1到29的数据校验 |
| SUM校验 | 1 | **31** |  |  |
| 32 | 出厂/RF设定的系统时间 | 7 | **32** |  | 出厂/RF设定的原始时间 |
| NB通信频段 | 1 | **39** |  | 中国电信：Ｂ5【850 MHz】  中国移动：Ｂ8【900 MHz】  中国联通：Ｂ8或Ｂ3【1800 MHz】 |
| NB连接方式 | 1 | **40** |  | 0：COAP  1：UDP |
| 预留 | 1 | **41** |  |  |
| 预留 | 1 | **42** |  |  |
| 剩余用量报警限值 | 1 | **43** |  | 增值提示 |
| 剩余用量关阀值 | 2 | **44** |  | BIT 15：为0表示负数  BIT 15：为1 表示负数 |
| 模块剩余的可用量数  （后台下发的值） | 6 | **46** |  | **户表依靠这个值，来决定是否报警和关闭阀门** |
| 参考起始用量 | 6 | **52** |  | 计算剩余用量时使用的当前累计参考量。 |
| 预留 | 2 | 58 | 0 |  |
| 预留 | 2 | **60** |  |  |
| CRC8校验 | 1 | **62** |  | 32到61的数据校验 |
| SUM校验 | 1 | **63** |  |  |
| 64 | **正转用量** | 6 | **64** |  | 参见 |
| 反转用量 | 6 | **70** |  |  |
| 阀状态 | 1 | **76** |  | **B0,B1:阀门当前状态**  B2,B3: 阀门期望的背景值  B4:正处于磁干扰过程中标志  B5:磁干扰消失后等待延时再动阀的过程中，延时到了后再视磁干扰前阀门状态另行处理。默认值：**0**  **B6,B7: 阀门原始状态，只有RF可以更改其状态。默认为关状态**  00：阀门故障  01：开阀  10：关阀  11：阀门未知 |
| 功能使能状态 | 2 | **77** |  | 参见’注释19：表端运行参数位定义’ |
| 报警状态标志位 | 2 | **79** |  | 默认0 |
| 按日按月设置 | 1 | **81** | 0 | 代表“RF侦听起始时间”代表的是小时还是日期 |
| RF侦听起始时间 | 1 | **82** | 0 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
| RF侦听工作时长 | 1 | **83** | 24 | 按日时：值代表的是小时，0到24  按月时：值代表的是日期，0到28 |
| 20位表端ID | 10 | **84** | 0 | 表端ID，最大20位 |
| CRC8校验 | 1 | **94** |  | 64到93的数据校验 |
| SUM校验 | 1 | **95** |  |  |
| 96 | 内存紊乱校验区 | 7 | **96** |  | 7个固定的值，用来比较内存是否紊乱 |
| SUM校验 | 1 | **103** |  |  |
| 104 | 集中器号 | 6 | **104** |  | 所属集中器号 |
| 预留 | 1 | **110** |  |  |
| SUM校验 | 1 | **111** |  |  |
| 112 | 正转用量备份区1 | 6 | **112** |  |  |
| 预留 | 1 | **118** |  |  |
| SUM校验 | 1 | **119** |  |  |
| 120 | 反转用量备份区1 | 6 | **120** |  |  |
| 预留 | 1 | **126** |  |  |
| SUM校验 | 1 | **127** |  |  |
| 128 | 路由路径长度 | 1 | **128** |  | 第一条路径长度 |
| 第一条路由路径 | 30 | **129** |  | 6\*5=30，最大支持5级路径 |
| SUM校验 | 1 | **159** |  |  |
| 160 | 路由路径长度 | 1 | **160** |  | 第二条路径长度 |
| 第二条路由路径 | 30 | **161** |  | 6\*5=30，最大支持5级路径 |
| SUM校验 | 1 | **191** |  |  |
| 192 | 密钥长度 | 1 | **192** |  | 默认长度：16byte |
| 表端密钥 | 16 | **193** |  | AES128加密使用 |
| 保留 | 6 | **209** |  |  |
| SUM校验 | 1 | **215** |  |  |
| 216 | 正转用量 备份区2 | 6 | **216** |  |  |
| 预留 | 1 | **222** |  |  |
| SUM校验 | 1 | **223** |  |  |
| 224 | 反转用量 备份区2 | 6 | **224** |  |  |
| 预留 | 1 | **230** |  | OPERATORSNUMBER |
| SUM校验 | 1 | **231** |  |  |
| 232 | 发射次数 | 2 | **232** |  | 默认：0 |
| 接收次数 | 2 | **234** |  | 默认：0 |
| 开关阀次数 | 2 | **236** |  | 默认：0 |
| 磁干扰次数 | 1 | **238** |  | 默认：0 |
| SUM校验 | 1 | **239** |  | ,**需要初始化EEPROM** |
| 240 | 预留 | 3 | **240** |  |  |
| 计量增加的脉冲数 | 1 | **243** | MAX: 255 | DB\_TON\_PULSE |
| 计量传感器两个状态间的次数 | 1 | **244** |  | A\_TO\_B\_TIME |
| 计量传感器所期望的下个状态值 | 1 | **245** |  | DB\_PULSE\_NEXT\_PTR |
| 正反转标志 | 1 | **246** |  | AWAKENING |
| SUM校验 | 1 | **247** |  |  |
| 248 | 掉电前的系统时间 | 7 | **248** |  | 系统掉电要保存的数据 |
| SUM校验 | 1 | **255** |  |  |
| 256 | EEPROM写次数 | 4 | **256** |  | 低字节在前，高字节在后 |
| 预留 | 27 | **260** |  |  |
| SUM校验 | 1 | **287** |  |  |
| 288 | 定时上传的时隙号 | 2 | **288** |  | 低字节在前，高字节在后  只有冻结上传时才用到时隙号 |
| 单位系统下的总表数 | 2 | **290** |  | 低字节在前，高字节在后  此集中器下的设备数量总和 |
| 测试系统的测试状态 | 2 | **292** | 0 | 保存测试系统下发的各个表端测试项目的测试状态。  默认为0：表示各个功能模块未测试成功 |
| 预留 | 1 | **294** |  |  |
| SUM校验 | 1 | **295** |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **冻结数据存放区（占用空间2816 byte）：**   1. **系统每间隔30分钟冻结一次数据** 2. **每次只能抄取一天的数据** 3. **11天滚动存储。** 4. **数据长度为4byte起始时间 + 100byte冻结数据+1byte写标志位 +1byte段号 + 1byte数据CRC8校验** | | | | | |
| 1280 | **4byte时间信息** | 4 |  | 存储区1  开始 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |
| 2656 | **4byte时间信息** | 4 |  | 存储区1  结束 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |
| 2688 | **4byte时间信息** | 4 |  | 备份区  开始 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |
| 4064 | **4byte时间信息** | 4 |  | 备份区  结束 | **【月、日、时、分】** |
| **6byte0：00累计用量数据** | 6 |  | **0点累计用量数据, 最小单位L** |
| **0：00到0：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **0：30到1：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：00到1：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1：30到2：00的增量** | 2 |  | **低字节在前,最小单位L** |
| **2：00到2：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **。。。。** | 2 |  | **低字节在前,最小单位L** |
| **23：00到23：30的增量** | 2 |  | **低字节在前,最小单位L** |
| **1byte段号** | **1** |  | **取值范围为0到10** |
| **1byte写标志位** | 1 |  |  | **BIT7: OxD3新数据，0老数据** |
| **1byte数据CRC8校验** | 1 |  | **低字节在前** |
| SUM校验 | 1 |  |  |  |

# BootLoader说明



## 协议说明

* + 1. 变量值在传输及存储均为低字节在前，高字节在后。
    2. 引导程序可以将程序跳转至升级程序和应用程序。引导程序和升级程序在一个程序体中，应用程序在另一个程序体中。
    3. 广播升级程序的设备为手持机或集中器。
    4. 被升级设备为表具。
    5. 表端模块升级程序在FLASH 0x4000~0x67ff, 共10KB。表端模块应用程序在FLASH 0x6800~0x13fff, 共54KB。表端EEPROM 4KB用作长期存储信息。除此，表端INFORMATION FLASH 0x1800 存储版本号等信息，可供应用程序和升级程序使用。
    6. 表端升级程序的128字节的INT VECTOR存储在应用程序的FLASH 0x7880处，供升级时使用。

## 升级协议

### 同6009通讯协议。

### 升级命令

|  |  |  |  |
| --- | --- | --- | --- |
| NO | 命令字 | 适用对象 | 注释 |
| 0 | 0x70 | APP命令 | 通知APP跳转到BOOT |
| 1 | 0x71 | BOOT | 开始升级，并擦除FLASH |
| 2 | 0x72 | BOOT | 开始接收升级包数据 |
| 3 | 0x73 | BOOT | 查询缺包状态 |
| 4 | 0x74 | APP命令 | 查询升级状态 |

## 升级步骤

### 逐个发送升级命令帧

向升级设备(表具命令0x70）发送升级命令帧。根据命令帧判断是否要进入boot。若条件满足则跳转到升级程序，等待升级。否则不升级，将不升级状态写入特定FLASH。若设备升级，做以下操作：

1. 保存数据信息到EEPROM，保存数据到FLASH
2. 关阀（若设备为表具）
3. 擦掉应用程序复位向量地址的内容和存放CRC16的内容
4. 复位后升级

### 升级流程

IAR生成TXT文件

txt转换成BIN文件

表端模块校验版本号,电池电压,SNR和RSSI，校验不通过

手抄器或PC通知系统跳转到boot（0X70）

表端模块校验版本号,电池电压,SNR和RSSI，RXD通信的信道号（0X71）

主机发射升级包数据（0x72）

缺包

查询升级状态（0x73）

结束升级

APP查询升级状态（0x74）

### TXT和BIN文件格式

#### TXT格式

|  |  |  |
| --- | --- | --- |
| NO | 说明 | 注释 |
| 1 | 0x1800开始的数据区， | 数据传递区，占用空间128byte |
| 2 | 0x700开始的APP数据区 | APP升级数据  主机不带导言发射升级包，每包固定长度（24+134）， |
| 3 | 0xFF80开始的中断向量数据区 |
| 4 | q结束标志 |  |

示例数据如：

|  |
| --- |
| 0x1800  XX XXXXXXXXXXXXXXXXXXXXXXXX XX.........  0x700  XX XXXXXXXXXXXXXXXXXXXXXXXX XX.........  0xFF80  XX XXXXXXXXXXXXXXXXXXXXXXXX XX.........  q |

#### bin格式

|  |  |  |
| --- | --- | --- |
| NO | 说明 | 注释 |
| 1 | 长度为128byte固定长度的数据传递区，不足时转换器补0 | 数据传递区，占用空间128byte |
| 2 | APP数据区 | APP升级数据  主机不带导言发射升级包，每包固定长度（24+134），转换器过滤掉0xFF.之后填充n个OXFF，APP数据区大小为128的整数倍 |

示例数据如：

|  |  |
| --- | --- |
| XX XXXXXXXXXXXXXXXXXXXXXXXX XX......... | 固定长度128byte |
| XX XXXXXXXXXXXXXXXXXXXXXXXX XX......... | APP数据区，每次发射128byte |

### @1800区数据域（占用空间大小128byte）

|  |  |  |  |
| --- | --- | --- | --- |
| 相对地址 | 内容 | 占用字节大小 | 备注 |
| 0 | 版本信息 | 40 | 40 (37+3个空格) |
| 40 | 将要升级的代码的总包数 | 2 |  |
| 42 | 程序代码的CRC16校验值,  2个26K 的CRC16  1个52K 的CRC16 | 6 | TXT转BIN软件产生此CRC16校验值，并放在此位置（低字节在前）， |
| 48 | 无线升级失败的原因 | 1 | Bit0：电池电压<5.0V  Bit1：电池电压<3.4V  Bit2：SNR< 0  Bit3：RSSI< 100  Bit4：版本号相同  Bit5：版本号错误，软硬件不配套  Bit6/Bit7：预留 |
| 49 | 表ID号 | 6 |  |
| 55 | 设备类型 | 1 |  |
| 56 | RF收发频率，3byte  信道带宽，1byte  扩频因子，1byte | 5 |  |
| 61 | RXD信道号 | 1 | 默认1：值范围，0或1 |
| 62 | 水表电池电压 | 1 | 默认：3.4 |
| 63 | 气表电池电压 | 1 | 默认：5 |
| 64 | 信噪比 | 1 | 默认：0 |
| 65 | 信号强度 | 1 | 默认：100 |
| 66 | 升级状态 | 1 | Bit0：未开始升级，  Bit1：当前为缺包等待状态  Bit2：程序已经升级完成  Bit3：程序体的CRC16校验错误  Bit4：程序版本号CRC16检验错误  Bit5：总包数错误 |
| 67 | 新程序版本CRC16 | 2 | 将要RF升级的新程序版本CRC16 |
| 69 | 预留 | 58 |  |

### 通知系统开始升级（0x70）

#### 命令简介：

* + - 1. 在APP中，系统以下发命令中的数据内容为条件判断当前是否具备升级条件，具备升级条件后。程序跳转到boot区

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明，相关数值见@1800区数据域 |
| 0 | 电池电压门限 | 2 | 高字节气表电压值，低字节水表电压值 |
| 1 | RSSI门限 | 2 | 高字节SNR，低字节RSSI |
| 2 | 应用程序版本 | 40 | (37+3个空格) |
| 3 | 应用程序版本CRC16 | 2 | 程序版本的CRC16，程序接收数据包时使用 |
| 4 | 总包数 | 2 | 低字节在前 |
| 5 | 2个26K的CRC16  一个54K的CRC16 | 6 |  |
| 6 | 指定通信信道 | 1 | RXD信道，默认3信道 |
| 7 | 预留 | 7 |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 无法无线升级的原因 | 1 | **如果值为0，条件都满足可以升级**  Bit0：5.0V电池电压  Bit1：3.4V电池电压  Bit2：SNR  Bit3：RSSI  Bit4：版本号相同  Bit5：版本号CRC16错误  /Bit6/Bit7：预留 |
| 1 | 当前APP版本号 | 40 | **(37+3个空格)** |

### 通知系统开始升级（0x71）

#### 命令简介：

* + - 1. 在boot中，系统以下发命令中的数据内容为条件判断当前是否具备升级条件，具备升级条件后擦除FLASH，开始接收数据包。

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明，相关数值见@1800区数据域 |
| 0 | 电池电压门限 | 2 | 高字节气表电压值，低字节水表电压值 |
| 1 | RSSI门限 | 2 | 高字节SNR，低字节RSSI |
| 2 | 应用程序版本 | 40 | (37+3个空格) |
| 3 | 应用程序版本CRC16 | 2 | 程序版本的CRC16，程序接收数据包时使用 |
| 4 | 总包数 | 2 | 低字节在前 |
| 5 | 2个26K的CRC16  一个54K的CRC16 | 6 |  |
| 6 | 指定通信信道 | 1 | RXD信道，0或1 |
| 7 | 预留 | 7 |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 无法无线升级的原因 | 1 | **如果值为0，条件都满足可以升级**  Bit0：50V电池电压  Bit1：34V电池电压  Bit2：SNR  Bit3：RSSI  Bit4：版本号  Bit5：版本号CRC16错误  /Bit6/Bit7：预留 |
| 1 | 当前APP版本号 | 40 | **(37+3个空格)** |

#### 实例数据

### 开始发射升级数据，并写FLASH（0x72）

#### 命令简介：

* + - 1. 在boot中使用

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明，相关数值见@1800区数据域 |
| 0 | 包序号 | 2 | 低字节在前 |
| 1 | 版本号CRC16 | 2 | 低字节在前 |
| 2 | 程序体 | 128 |  |
| 3 | 程序体的CRC16 | 2 |  |
|  |  |  |  |

#### 上行命令：不应答

#### 实例数据

### 查询升级状态（0x73）

#### 命令简介：

在boot中

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明，相关数值见@1800区数据域 |
| 0 | 总包数 | 2 |  |
| 1 | 版本号CRC16 | 2 |  |
| 2 |  |  |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 升级状态 | 1 | Bit0：未开始升级，  Bit1：当前为缺包等待状态  Bit2：程序已经升级完成  Bit3：程序体的CRC16校验错误  Bit4：程序版本号CRC16检验错误  Bit5：总包数错误 |
|  | 当前程序的版本 | 40 |  |
|  | 缺包数 | 52 | 低字节在前，上位机显示具体的包号。 |
| 1 |  |  | 0x7000~0x14000（52KByte）  注：MM = 52\*1024/128/8=52（1包128字节）  例如，总包数为12，MM=2字节  1代表不缺包，0代表缺包，黑色部分无意义 |

#### 实例数据

### 查询升级状态（0x74）

#### 命令简介：

在APP中

#### 下行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明，相关数值见@1800区数据域 |
| 0 | 总包数 | 2 |  |
| 1 | 版本号CRC16 | 2 |  |
| 2 |  |  |  |

#### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 升级状态 | 1 | Bit0：未开始升级，  Bit1：当前为缺包等待状态  Bit2：程序已经升级完成  Bit3：程序体的CRC16校验错误  Bit4：程序版本号CRC16检验错误  Bit5：总包数错误 |
|  | 当前程序的版本 | 40 |  |

## 广播升级步骤

# .AAES128加密算法



## 算法简介

**高级加密标准**（英语:**Advanced Encryption Standard**，缩写:**AES**），在密码学中又称**Rijndael加密法**，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的DES，已经被多方分析且广为全世界所使用。经过五年的甄选流程，高级加密标准由美国国家标准与技术研究院（NIST）于2001年11月26日发布于FIPS PUB 197，并在2002年5月26日成为有效的标准。2006年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

不同于它的前任标准DES，Rijndael使用的是代换-置换网络，而非Feistel架构。AES在软件及硬件上都能快速地加解密，相对来说较易于实作，且只需要很少的存储器。作为一个新的加密标准，目前正被部署应用到更广大的范围。

## 算法实现

AES加密过程是在一个4×4的字节矩阵上运作，这个矩阵又称为“状态（state）”，其初值就是一个明文区块（矩阵中一个元素大小就是明文区块中的一个Byte）。（Rijndael加密法因支持更大的区块，其矩阵行数可视情况增加）加密时，各轮AES加密循环（除最后一轮外）均包含4个步骤:

1. AddRoundKey — 矩阵中的每一个字节都与该次轮秘钥（roundkey）做XOR运算。每个子密钥由密钥生成方案产生。
2. SubBytes — 通过个非线性的替换函数，用查找表的方式把每个字节替换成对应的字节。
3. ShiftRows — 将矩阵中的每个横列进行循环式移位。
4. MixColumns — 为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每列的四个字节。

最后一个加密循环中省略MixColumns步骤，而以另一个AddRoundKey取代。

使用该算法时，首先会生成128位 MD5值，再将该MD5只作为真实的加密密钥。

加密时，明文长度必须是8字节，因此会将输入明文分割成多干个8字节的段，再将每段明文分别加密，加密密文会按照原有顺序连接在一起。如果密文长度是8字节的倍数，则在其后加上“80H 00H00H00H00H00H00H00H”。当最后的数据块长度不足8个字节，则在其后加上“80H” 如仍没有达到8个字节长度，则在其后加入“00H”，知道长度达到8个字节。

解密密钥与加密密钥一致，同样是采用分段解密方式，最后一块数据内容自动判断有效数据长度后，会将所有明文按照原有顺序连接在一起后输出。并去除加密时程序自动增加的补码。

## 代码说明

使用本算法需调用3个接口函数，分别为:

1. **用户提供的密钥MD5生成函数接口，原型如下:**

void librad\_md5\_calc(uint32 \*output, uint8 \*input, uint16inputlen)。

\*output// 存放密钥md5值的变量，长度为16Byte

\*input // 用户密钥，可为任意长度

inputlen // 密钥长度

1. **加密函数接口，原型如下:**

uint8 EncryptPackDataSeg(uint8 \*packBuf, const uint32 \*key,uint8 \*newPack)。

\*packBuf//源数据,

\*key //实际密钥,128bit密钥

\*newPack//加密后的新数据，长度为8的倍数

说明:该函数会自动增加80H 00H等方式将源数据补齐，函数返回0时表示加密成功

1. **解密函数接口，原型如下:**

uint8 DecryptPackDataSeg(uint8 \*packBuf, const uint32 \*key, uint8 \*newPack)。

\*packBuf//源数据

\*key //实际密钥,128bit密钥

\*newPack//解密后的新数据

说明:该函数会自动按规则将填补的80H 00H等数据去除，函数返回0时表示解密成功

# .CRC算法说明



## . CRC8代码

uint8 comCalCRC8(const uint8 \*dataBuf,uint16 dataLen)

{

uint8 i,cCrc=0。

while(dataLen--)

{

cCrc^=\*dataBuf。

for(i=0。i<8。i++)

{

if(cCrc&0x01)

{

cCrc>>=1。

cCrc^=0x8c。

}

else

{

cCrc>>=1。

}

}

dataBuf++。//next data

}

return cCrc。

}

## . CRC16代码

#define CRC\_POLY 0x8408

uint16 comPureCalCRC16(const uint8 \*pucBuf, uint16 uwLength)

{

uint16 uiCRCValue=0xFFFF。

uint8 ucLoop。

uint8\* pu8Buf = (uint8 \*)pucBuf。

while(uwLength--)

{

uiCRCValue ^= \*pu8Buf++。

for(ucLoop=0。ucLoop<8。ucLoop++)

{

if(uiCRCValue& 0x0001)

{

uiCRCValue>>= 1。

uiCRCValue ^= CRC\_POLY。

}

else

{

uiCRCValue>>= 1。

}

}

}

uiCRCValue ^= 0xFFFF。

return uiCRCValue。

}