SRWF-609通信协议

Version 1.0

|  |  |
| --- | --- |
| 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 |  | 2015.9.13 |  |
|  |  | 20190806 | 1. 读取NB入网信息及状态 2. 北京水表参数设置与读取 3. NB表端与平台数据交互 4. Tag List |
|  |  | 20190814 | 增加基础信息读取命令 |
|  |  | 20191106 | 更改付费信息 |
|  |  | 20191120 | 增加命令字0X3C及注释24 |
|  |  |  |  |
|  |  |  |  |

目录

[修改历史 2](#_Toc24476162)

[1. NB-IOT通讯网络结构图 6](#_Toc24476163)

[2. UART端口 6](#_Toc24476164)

[3. 协议的格式 7](#_Toc24476165)

[协议格式 7](#_Toc24476166)

[注释1：报文标识 7](#_Toc24476167)

[注释2：设备类型 7](#_Toc24476168)

[注释3：TLV格式说明 8](#_Toc24476169)

[注释4：Tag List 8](#_Toc24476170)

[注释5：预留 11](#_Toc24476171)

[注释6：脉冲系数 11](#_Toc24476172)

[注释7：表读数的数据格式 11](#_Toc24476173)

[注释8：信号强度下行注释 12](#_Toc24476174)

[注释9：信号强度上行注释 12](#_Toc24476175)

[注释10：数据包中的符号说明 12](#_Toc24476176)

[注释13：告警状态、阀状态和EEPROM状态 12](#_Toc24476177)

[注释14：返回的操作代码一般含义 13](#_Toc24476178)

[注释15：通讯协议中的存储格式约定 14](#_Toc24476179)

[注释17：串口传给透传模块的RF发射数据格式 14](#_Toc24476180)

[注释18：对于RF应答数据过长的处理 14](#_Toc24476181)

[注释19：表端功能使能位定义 14](#_Toc24476182)

[注释20：预付费用量信息 15](#_Toc24476183)

[注释21：阶梯结算价目表 15](#_Toc24476184)

[注释22：写入充值数据 16](#_Toc24476185)

[注释23：写入结算价目表 16](#_Toc24476186)

[4. NB-IOT无线通信数据（包括红外/蓝牙通讯命令） 17](#_Toc24476187)

[4.1. NB终端和平台交互 17](#_Toc24476188)

[4.2. NB主动上传/下发的数据包格式（命令字：0XA1） 21](#_Toc24476189)

[4.3. 读取NB主动上报的数据： 0x01 22](#_Toc24476190)

[4.4. 读取冻结数据格式 0x02 25](#_Toc24476191)

[4.5. 开关阀指令 0x03 26](#_Toc24476192)

[4.6. 读表端参数配置信息 0x04 27](#_Toc24476193)

[4.7. 清异常命令 0x05 27](#_Toc24476194)

[4.8. 设置用量及脉冲系数 0x06 28](#_Toc24476195)

[4.9. 测试命令 0x07 28](#_Toc24476196)

[4.10. 设置系统功能使能状态 0x08 32](#_Toc24476197)

[4.11. 读模块发射、接收，阀控，磁干扰次数等命令 0x09 32](#_Toc24476198)

[4.12. 清除反转计量数据命令 0x0A 33](#_Toc24476199)

[4.13. 读系统功能使能状态 0x0B 33](#_Toc24476200)

[4.14. 详见：注释19：表端运行参数位定义 33](#_Toc24476201)

[4.15. 设置定时定量上传参数命令 0x0C 33](#_Toc24476202)

[4.16. 设置/读取NB水表的IP+端口+协议类型(Coap/UDP)： 0x0D 34](#_Toc24476203)

[4.17. 读取/设置NB水表的运营商识别码： 0x0E 35](#_Toc24476204)

[4.18. 读取NB水表的CCID+IMEI： 0x0F 36](#_Toc24476205)

[4.19. 读取NB入网信息及状态： 0x10 37](#_Toc24476206)

[4.20. 读取价目表 0x11 38](#_Toc24476207)

[4.21. 设置价目表 0x12 38](#_Toc24476208)

[4.22. 读取时钟 0x13 39](#_Toc24476209)

[4.23. 设置时钟 0x14 39](#_Toc24476210)

[4.24. 下发预缴金额 0x15 40](#_Toc24476211)

[4.25. 读取预缴金额 0x16 40](#_Toc24476212)

[4.26. 设置剩余金额报警限值，关阀限值0x17 41](#_Toc24476213)

[4.27. 读取剩余金额报警限值，关阀限值0x18 41](#_Toc24476214)

[4.28. 读取命令的记录数据0x19 42](#_Toc24476215)

[4.29. 读取模块的基础信息0x1A 42](#_Toc24476216)

[4.30. 读预付费用量信息 0x1B 43](#_Toc24476217)

[4.31. 预留 0x1C 43](#_Toc24476218)

[4.32. 设置密钥 0x1D 43](#_Toc24476219)

[4.33. 读预缴费历史记录 0x1E 44](#_Toc24476220)

[4.34. 预留 0x1F 45](#_Toc24476221)

[4.35. 预留 0x20 45](#_Toc24476222)

[4.36. 设置参考用量 0x21 45](#_Toc24476223)

[4.37. 读取读取参考用量 0x22 45](#_Toc24476224)

[4.38. 预留 0x23 47](#_Toc24476225)

[4.39. 预留 0x24 47](#_Toc24476226)

[4.40. 预留 0x25 47](#_Toc24476227)

[4.41. 北京水表参数设置与读取： 0x26 47](#_Toc24476228)

[4.42. 预留 0x27 50](#_Toc24476229)

[4.43. 预留 0x28 50](#_Toc24476230)

[4.44. 预留 0x29 50](#_Toc24476231)

[4.45. 预留 0x2A 50](#_Toc24476232)

[4.46. 预留 0x2B 50](#_Toc24476233)

[4.47. 预留 0x2C 50](#_Toc24476234)

[4.48. 预留 0x2D 50](#_Toc24476235)

[4.49. 预留 0x2E 50](#_Toc24476236)

[4.50. 预留 0x2F 50](#_Toc24476237)

[5. UART表端模块测试系统通讯协议（软件校准RF参数） 50](#_Toc24476238)

[5.1. 协议格式 50](#_Toc24476239)

[5.2. 注释19，命令字详解（数据域低字节在前，高字节在后） 51](#_Toc24476240)

[5.3. 注释20，读取设置基准频率和发射功率 52](#_Toc24476241)

[5.4. 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) 52](#_Toc24476242)

[5.5. 注释23：设置NB-IOT水气表端模块运行参数的数据域结构 53](#_Toc24476243)

[5.6. 实例数据解析 55](#_Toc24476244)

[6. 表端的数据存储 64](#_Toc24476245)

[6.1. NB-IOT水表EEPROM的存储结构（存储空间：4Kbyte） 64](#_Toc24476246)

[7. BootLoader说明 70](#_Toc24476247)

[7.1. 协议说明 70](#_Toc24476248)

[7.2. 升级协议 70](#_Toc24476249)

[7.3. 升级步骤 70](#_Toc24476250)

[7.4. 通知系统开始升级（0x70） 73](#_Toc24476251)

[7.5. 通知系统开始升级（0x71） 74](#_Toc24476252)

[7.6. 开始发射升级数据，并写FLASH（0x72） 75](#_Toc24476253)

[7.7. 查询升级状态（0x73） 75](#_Toc24476254)

[7.8. 查询升级状态（0x74） 76](#_Toc24476255)

[8. .AAES128加密算法 77](#_Toc24476256)

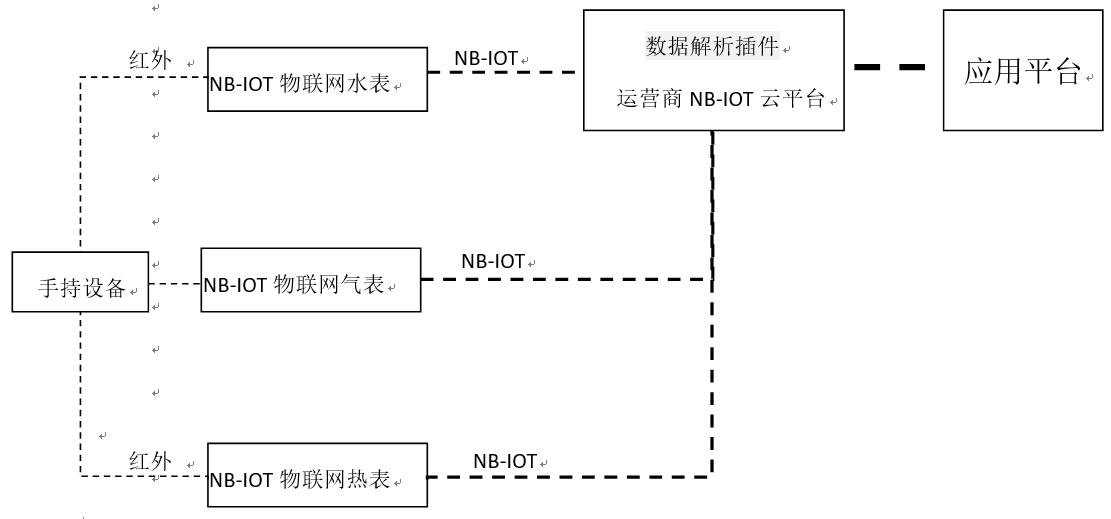
[8.1. 算法简介 77](#_Toc24476257)

[8.2. 算法实现 77](#_Toc24476258)

[8.3. 代码说明 78](#_Toc24476259)

[8.4. CRC算法说明 79](#_Toc24476260)

# NB-IOT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** |
| 0 | 起始帧 | 2 |  | 0xD30x91 |
| 1 | 包长 | 2 |  | 2到13的数据长度 |
| 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 | AES128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 | 保留 | 1 | 预留,默认0 |
| 7 | 保留 | 1 | 预留,默认0 |
| 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，根据TLV数据格式编制 |
| 10 | 预留 | 1 | 预留,默认0 |
| 11 | 预留 | 1 | 预留,默认0 |
| 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 |

## 注释1：报文标识

|  |  |  |  |
| --- | --- | --- | --- |
| 占用位 | 用途 | 默认值 | 含义 |
| Bit0- Bit3 | 预留 | 0 | 预留 |
| Bit 4 | 是否需要回执 | 0 | 0：不需回执; 1: 需要回执 |
| Bit 5 | 密标志 | 0 | 0:非加密； 1: 加密（AES128加密） |
| Bit 6 | 帧类型 | 0 | 0 : 数据帧; 1：应答帧 |
| Bit7 | 数据方向 | 1 | 0 : 下行; 1：上行 |

## 注释2：设备类型

数据发出者的设备类型

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **北京四表设备类型定义** | | | | | |
| **NO** | **基表厂家** | **厂家代码** | **传感器类别** | **设备类型** |  |
| 1 | 杭州竞达  /民生仪表 | 0 | 双霍尔脉冲水表 | 0X10 |  |
| NB霍尔水表 | 0X20 |  |
|  |  |  |
| 民生NB 2霍尔水表 | 0X50 |  |
| 民生NB 3霍尔水表 | 0X60 |  |
| 民生NB无磁水表 | 0X70 |  |
| 2 | 江西三川 | 1 | 四位光点水表 | 0X11 |  |
| 一位光点水表 | 0X21 |  |
| 无磁水表 | 0X31 |  |
| NB无磁水表 | 0X41 |  |
| 3 | 丹东思凯 | 2 |  | 0X12 |  |
| 4 | 京兆公司 | 3 |  | 0X13 |  |
| 5 | 宁波水表 | 4 | 宁波干式光电水表 | 0X14 |  |
| 宁波湿式光电水表 | 0X24 |  |
| 宁波无磁水表 | 0X34 |  |
| NB无磁水表 | 0X44 |  |
| 6 | 杭州山科 | 5 | 厚膜直读水表 | 0X15 |  |
| 无磁水表 | 0X25 |  |
| NB无磁水表 | 0X35 |  |
| 7 | 山东高翔 | 6 | 霍尔脉冲水表 | 0X16 |  |
| NB无磁水表 | 0X26 |  |
| 8 | 广州兆基 | 7 | 兆基湿式卧式光电水表 | 0X17 |  |
| 兆基湿式立式光电水表 | 0X27 |  |
| NB无磁水表 | 0X37 |  |
| 9 | 北京京源水 | 8 | 无磁水表 | 0X18 |  |
| NB无磁水表 | 0X28 |  |
| 10 | 宁波东海 | 9 | 双干簧管水表 | 0X19 |  |
| NB无磁水表 | 0X29 |  |

## 注释3：TLV格式说明

数据域数据项根据TLV格式编制，其格式如下

|  |  |  |
| --- | --- | --- |
| **字段** | **数据类型** | **描述** |
| **Tag(标签)** | **1Byte** | **标签** |
| **Length（长度）** | **1Byte** | **长度** |
| **Value（数值）** | **Byte[n]** | **N字节数据** |

## 注释4：Tag List

表端和平台交互使用到的标签：

|  |  |  |
| --- | --- | --- |
| **字段（Tag值）** | **数据类型** | **描述** |
| **0x00** | **1Byte** | **Tag\_RealTimeData实时数据** |
| **0x01** | **1Byte** | Tag\_FrozenData冻结数据 |
| **0x02** | **1Byte** | Tag\_PreValue读取预付费信息 |
| **0x03** | **1Byte** | Tag\_PriceTable读取结算价目表 |
| **0x04** | **1Byte** | Tag \_PlatIP读取平台IP |
| **0x05** | **1Byte** | Tag \_ReadPara读取系统参数信息 |
| **0x06** | **1Byte** |  |
| **0x07** | **1Byte** | Tag\_SoftWare水表模组程序版本 |
| **0x08** | **1Byte** | Tag\_NbModeNB模组类型 |
| **0x09** | **1Byte** | Tag\_NbSoftWareNB模组程序版本 |
| **0x0a** | **1Byte** | Tag\_ManufactureId厂商代码 |
| **0x0b** | **1Byte** | Tag\_NB\_RSRP |
| **0x0c** | **1Byte** | Tag\_NB\_TotalPower |
| **0x0d** | **1Byte** | Tag\_NB\_TxPower |
| **0x0e** | **1Byte** | Tag\_NB\_TxTime |
| **0x0f** | **1Byte** | Tag\_NB\_RxTime |
| **0x10** | **1Byte** | Tag\_NB\_CELLID |
| **0x11** | **1Byte** | Tag\_NB\_ECL |
| **0x12** | **1Byte** | Tag\_NB\_SNR |
| **0x13** | **1Byte** | Tag\_NB\_EARFCN |
| **0x14** | **1Byte** | Tag\_NB\_PCI |
| **0x15** | **1Byte** | Tag\_NB\_RSRQ |
| **0x16** | **1Byte** | Tag\_NB\_OperatorMode |
| **0x17** | **1Byte** | Tag\_WaringState |
| **0x18** | **1Byte** | Tag\_Option |
| **0x19** | **1Byte** | Tag\_ValveState |
| **0x1a** | **1Byte** | Tag\_Battery |
| **0x1b** | **1Byte** | Tag\_Temperature |
| **0x1c** | **1Byte** | Tag\_Protocol |
| **0x1d** | **1Byte** |  |
| **0x1e** | **1Byte** |  |
| **0x1f** | **1Byte** |  |
| **0x20** | **1Byte** | Tag\_ACK |
| **0x21** | **1Byte** | Tag\_OP\_ValveControl |
| **0x22** | **1Byte** | Tag\_OP\_PreValue写入预付费信息 |
| **0x23** | **1Byte** | Tag\_OP\_PriceTable写入结算价目表 |
| **0x24** | **1Byte** | 读模块预缴用量和参考用量数据 |
| **0x25** | **1Byte** | 下发模块预缴用量和参考用量数据 |
| **0x26** | **1Byte** | 设置剩余用量报警限值，关阀限值 |
| **0x27** | **1Byte** | 读取系统功能使能状态 |
| **0x28** | **1Byte** | 设置系统功能使能状态 |
| **0x29** | **1Byte** | 清除表端异常 |
| **0x2A** | **1Byte** | Tag \_OP\_PlatIP设置IP+端口+模式 |
| **0x2B** | **1Byte** | Tag \_SetPara设置系统参数信息 |
| **0x2C** | **1Byte** |  |
| **0x2D** | **1Byte** |  |
|  |  |  |

## 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 | 宁波无磁 |  |
| 10 | 山科无磁 |  |
|  |  | 11 | 东海无磁 |  |
|  |  | 12 | 三川无磁 |  |
|  |  | 13 |  |  |
|  |  | 14 | 山东高翔无磁 |  |

## 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

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | 总长 | 105 | |
| 段标识 | 段大小 | 段说明 |
| 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 |
| 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 | |

实时数据格式

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | 总长 | 6 | |
| 段标识 | 段大小 | 段说明 |
| 水表实时用量数据 | 6 | |  |  |  | | --- | --- | --- | | 项目 | 长度 | 注释 | | 4字节整数值(uint32) | 4 | 低字节在前 | | 2字节  (uint16) | 15bits | Bit14-Bit0:小数值，千分制小数 | | 1bit | Bit15:负数符号 | |

## 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 | NB下行时的信号强度 |

## 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 | NB上行时的信号强度 |

## 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
5. 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
6. 在RF通讯协议中的格式: 4字节的整数、 2字节的小数
7. 日期、时间按年、月、日、时、分、秒的Bcd码格式存储
8. 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 | X |
| 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 | 4 |  |
| 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 | 4 | 4 |
| 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 | 4 | float |
| 2 | 剩余金额 | 4 | Float |
| 3 | 执行阶梯 | 1 |  |
| 4 | 期初表底数 | 6 | 4整数2小数 |
| 5 | 校验码 | 2 | 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终端和平台交互

### 命令简介：

表端上报到平台的数据，分为周期数据（数据类型0x01）和实时数据（数据类型0x00），命令字：0x01。数据包均需要平台应答确认。

### 表端上行命令：

#### 表端上行周期数据：

NB 水表在产生完整的冻结数据后，会进行 24 小时的周期上报。

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | TAG | 段说明 |
| FrozenData | 冻结数据 | 0x01 | 共 105 字节，详见注释7“冻结数据格式” |
| WaringState | 报警状态 | 0x17 | 告警状态字 1、告警状态字 2.详见注释13 |
| ValveState | 阀门状态 | 0x19 | 详见注释13 |
| Battery | 电池电压 | 0x1A | 16 进制直接表示，如 0x24->3.6V |
| Temperature | 环境温度 | 0x1B | 16 进制直接表示，如 0x16->22℃ |
| Protocol | 应用层协议版本号 | 0x1C | 2字节 |
| PreValue | 预付费用量信息 | 0x02 | 共 38 字节，详见注释20 |
| Pricetable | 价目表 | 0x03 | 共 45 字节，详见注释23 |
| SignalPower | 信号强度 | 0x0B |  |
| TotalPower | 总功率 | 0x0C |  |
| TxPower | 发射功率 | 0x0D |  |
| TxTime | 发射时间 | 0x0E |  |
| RxTime | 接收时间 | 0x0F |  |
| CELLID | 小区 ID | 0x10 |  |
| ECL | 信号覆盖等级 | 0x11 |  |
| SNR | 信噪比 | 0x12 |  |
| EARFCN | 频点号 | 0x13 |  |
| PCI | 扇区标识 | 0x14 |  |
| RSRQ | 参考信号 | 0x15 |  |
| OPEARTORMODE | 操作模式 | 0x16 |  |

设备上传完整的主动周期上报数据，表格内是数据域逐个字段解析的结果  
D391D90093000100B502898603174220500449370000086948703002071201690000000000000  
0000000000000000000000000000000000000000000000000000000000000000000000000000000  
0000000000000000000000000000000000000000000000000000000000000000000000000000000  
000000000000000000000000000000000000000170200001901011A01241B01171C020100020003  
000B025B800C0250800D0217000E04040200000F04800A00001005D2AC160B0011010012022E001  
305CA090000001402CA0015020C801601040000FDCA16

|  |  |  |  |
| --- | --- | --- | --- |
| Tag | Length | Value(16 进制码流) | 说明 |
| 0x01 | 0x69 | 00000000………0000000000000 | FrozenData |
| 0x17 | 0x02 | 0000 | WaringState |
| 0x19 | 0x01 | 01 | ValveState |
| 0x1A | 0x01 | 24 | Battery |
| 0x1B | 0x01 | 17 | Temperature |
| 0x1C | 0x02 | 0100 | Protocol |
| 0x02 | 0 | PreValue |  |
| 0x03 | 0 | Pricetable |  |
| 0x0B | 0x02 | 5B80 | RSRP |
| 0x0C | 0x02 | 5080 | TotalPower |
| 0x0D | 0x02 | 1700 | TxPower |
| 0x0E | 0x04 | 04020000 | TxTime |
| 0x0F | 0x04 | 800A0000 | RxTime |
| 0x10 | 0x05 | D2AC160B00 | CELLID |
| 0x11 | 0x01 | 00 | ECL |
| 0x12 | 0x02 | 2E00 | SNR |

|  |  |  |  |
| --- | --- | --- | --- |
| 0x13 | 0x05 | CA09000000 | EARFCN |
| 0x14 | 0x02 | CA00 | PCI |
| 0x15 | 0x02 | 0C80 | RSRQ |
| 0x16 | 0x01 | 04 | OPEARTORMODE |
|  |  |  |  |

#### 表端上行实时数据：

当 NB 水表被触发时，发送完整的实时数据上报帧。

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 变长 |
| 段序号 | 段标识 | TAG | 段说明 |
| RealTimeData | 实时数据 | 0x00 | 详见注释7 |
| ManufactureId | 厂商代码 | 0x0A | “SR” |
| SoftWare | 水表软件版 本 | 0x07 | “SRWF-N609-NH01A-SR-CTCC-20190506-Vt1.07” |
| NbModule | NB 模组类型 | 0x08 | “NH01A” |
| NbSoftWare | NB 模组软件 版本 | 0x09 | “100C10B200SP1” |
| WaringState | 报警状态 | 0x17 | 告警状态字 1、告警状态字 2.详见注释13 |
| ValveState | 阀门状态 | 0x19 | 详见注释13 |
| Battery | 电池电压 | 0x1A | 16 进制直接表示，如 0x24->3.6V |
| Temperature | 环境温度 | 0x1B | 16 进制直接表示，如 0x16->22℃ |
| SignalPower | 信号强度 | 0x0B |  |
| TotalPower | 总功率 | 0x0C |  |
| TxPower | 发射功率 | 0x0D |  |
| TxTime | 发射时间 | 0x0E |  |
| RxTime | 接收时间 | 0x0F |  |
| CELLID | 小区 ID | 0x10 |  |
| ECL | 信号覆盖等 级 | 0x11 |  |
| SNR | 信噪比 | 0x12 |  |
| EARFCN | 频点号 | 0x13 | EARFCN |
| PCI | 扇区标识 | 0x14 | PCI |
| RSRQ | 参考信号 | 0x15 | RSRQ |
| OPEARTORMODE | 操作模式 | 0x16 | OPEARTORMODE |

数据被触发后，上传完整的实时数据上报帧，表格内是数据域逐个字段的解析的结果  
 D391B20093000100B502898603174520416343480000086948703002071200060000000000000  
A0253520728535257462D4E3630392D4E483031412D53522D435443432D32303139303530362D56  
74312E30372008054E48303141090D31303043313042323030535031170200001901011A01241B0  
1180B0259800C0252800D0217000E04610200000F04AF0D00001005D2AC160B0011010012022E00  
1305CA090000001402CA0015020C801601040000260616

|  |  |  |  |
| --- | --- | --- | --- |
| Tag | Length | Value(16 进制码流) | 说明 |
| 0x00 | 0x06 | 000000000000 | RealTimeData |
| 0x0A | 0x02 | 5352 | ManufactureId |
| 0x07 | 0x28 | 535257462D4E3630392D4E483031412D53522D43 5443432D32303139303530362D5674312E303720 | SoftWare |
| 0x08 | 0x05 | 4E48303141 | NbModule |
| 0x09 | 0x0D | 31303043313042323030535031 | NbSoftWare |
| 0x17 | 0x02 | 0000 | WaringState |
| 0x19 | 0x01 | 01 | ValveState |
| 0x1A | 0x01 | 24 | Battery |
| 0x1B | 0x01 | 18 | Temperature |
| 0x0B | 0x02 | 5980 | RSRP |
| 0x0C | 0x02 | 5280 | TotalPower |
| 0x0D | 0x02 | 1700 | TxPower |
| 0x0E | 0x04 | 61020000 | TxTime |
| 0x0F | 0x04 | AF0D0000 | RxTime |
| 0x10 | 0x05 | D2AC160B00 | CELLID |

|  |  |  |  |
| --- | --- | --- | --- |
| 0x11 | 0x01 | 00 | ECL |
| 0x12 | 0x02 | 2E00 | SNR |
| 0x13 | 0x05 | CA09000000 | EARFCN |
| 0x14 | 0x02 | CA00 | PCI |
| 0x15 | 0x02 | 0C80 | RSRQ |
| 0x16 | 0x01 | 04 | OPEARTORMODE |

### 平台应答确认命令：

同一次交互中，该命令的任务号必须和上行命令任务号保持一致。当平台有其他命令需要下发时，应同此应答一起下发，同时表端会应答给给平台，供平台确认命令下成功，本次交互结束；当平台无其他命令下发时，只下发应答，表端不再发应答包给平台，本次交互结束。

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | Tag | 段说明 |
| 1 | 平台应答返回 | 0x20 | 可能的Vlaue如下  OxAA:操作成功  0xAB：操作失败  0xAE：数据包格式错误或无法识别的命令  0XD5：校验码错误  0Xd7：未知错误 |
| 2 | 阀控命令 | 0x21 | 可根据实际需要决定是否下发次命令  （0x00:关阀 0x01:开阀） |
| 3 | 写入预付费信息 | 0x02 | 可根据实际需要决定是否下发次命令 |
| 4 | 写入结算价目表 | 0x03 | 可根据实际需要决定是否下发次命令 |
| … | ….. | …… | 更多命令见注释4 |

### 表端应答确认命令：

同一次交互中，该命令的任务号必须和上行命令任务号保持一致。当平台有命令需要下发时，表端会应答给平台，供平台确认命令下成功，本次交互结束；当平台无其他命令下发时，表端不再发应答包给平台，本次交互结束。

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 1 |
| 段序号 | 段标识 | Tag | 段说明 |
| 1 | 表端应答返回 | 0x20 | 可能的Vlaue如下  OxAA:操作成功  0xAB：操作失败  0xAE：数据包格式错误或无法识别的命令  0XD5：校验码错误  0Xd7：未知错误 |

## 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 YY MM 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：

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

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

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。  0xA0 应答数据帧  0xA1 命令数据帧 |
| 1 | 当前时间 | 7 | YY YY MM 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 | 1 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 标识 | 1 | 失败 0xAB |
| 或 |  |  |  |
| 0 | 标识 | 1 | 成功 0XAA |
| 1 | 用量 | 6 |  |
| 2 | 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

## 设置/读取NB水表的IP+端口+协议类型(Coap/UDP)： 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 | 协议类型 | 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：

### 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NB水表的CCID+IMEI： 0x0F

### 命令简介：

广播指令D4 D4D4D4D4D4 D4D4D4D4, 通过UART/红外读取模块的IMEI和CCID

### 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NB入网信息及状态： 0x10

### 命令简介：

### 下行命令：空数据域

### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 长度34byte |
| 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 YY MM 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} |
| 3 | 阶梯周期ti | 1 | 0：年 1：半年 2：季度 3：月 |
| 4 | 阶梯价目版本号 | 1 |  |

### 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 | 阶梯周期 | 1 | 0：年 1：半年 2：季度 3：月 |
| 3 | 阶梯价目版本号 | 1 | 从0开始递增 |
| 4 | 动态密码 | 6 | 动态密码是用来检查数据的合法信息（0x11,0x22,0x33,0x44,0x55,0x66）低位在前 |
| 5 | 校验码 | 2 | 校验码 |

### 上行命令：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 标志位 | 1 | 0xAA 成功 0XAB 失败 |
| 1 | 失败标志 | 1 | BIT0: 小数点超限  BIT1: 设置执行价格日期错误  BIT2: 写EEPROM错误  BIT3: 阶梯价目表非法  BIT4: CRC错误 |
| 2 | 状态 | 1 | 0：还未设价格表 1: 单一价格;2:阶梯价格 |

### 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 | |

### 实例数据

## 下发预缴金额 0x15

### 下行

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 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 | 预缴金额 | 4 | Float |
| 2 | 剩余金额 | 4 | Float |
| 3 | 动态充值密码 | 6 | 动态密码是用来检查数据的合法信息（0x11,0x22,0x33,0x44,0x55,0x66）低位在前 |
| 4 | 校验码 | 2 | 校验码 |

### 上行：返回当前充值信息

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | 10 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功;0xBB: 已充过值; 0xAB：操作失败 |
| 1 | 充值序号 | 2 | 1字节的充值网点+1字节的充值序号 |
| 2 | 充值额 | 4 | float |
| 3 | 剩余金额 | 4 | float |

## 读取预缴金额 0x16

### 下行空

### 上行

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 操作状态 | 1 | 0xAA：操作成功; 0xAB：还未充值 |
| 1 | 充值序号 | 2 | 1字节的充值网点+1字节的充值序号 |
| 2 | 充值额 | 4 | float |
| 3 | 剩余金额 | 4 | float |

## 设置剩余金额报警限值，关阀限值0x17

### 下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类别 | 1 | 0：报警限值；1：透支用量数值 |
| 1 | 报警限值 | 4 | 小于限量值蜂鸣报警 |
| 或 |  |  |  |
| 1 | 透支用量数值 | 4 | 透支用量数值可以是负数，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 |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 标志位 | 1 | 0xAA：操作成功0xAB：操作失败 |
| 1 | 失败类型 | 1 | BIT0: 报警值大于关阀值  BIT1: 关阀值小于彻底关阀值  BIT2: 报警值不合理（大于10元）  BIT3: 设置类别错误 |

## 读取剩余金额报警限值，关阀限值0x18

### 下行：空数据域

### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 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 | 4 | 小于限量值蜂鸣报警 |
| 2 | 透支用量数值 | 4 | 小于金额关阀 |

## 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：

## 读取模块的基础信息0x1A

### 命令说明：

本命令为只读命令,可通过红外或者NB读取.

### 下行：空数据域

### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据ID | 字段 | 数据类型 | 描述及要求 |
| 0 | IMEI号 | BYTE[10] | 20位CCID号，用ASCII码表示 |
| 1 | CCID号 | BYTE[10] |  |
| 2 | IMSI | BYTE[8] |  |
| 3 | 设备出厂编号 | BYTE[5] | YYMMDDXXXX |
| 4 | 设备类型 | BYTE[1] |  |
| 5 | NB软件版本 | BYTE[13] |  |
| 6 | 方案版软件版本 | BYTE[39] |  |
| 7 | 终端时钟 | BYTE[6] | YYMMDDHHMMSS |
| 8 | 终端IP+端口+协议类型 | BYTE[7] |  |
| 9 | 当前入网状态 | BYTE[1] |  |
| 3 |  |  |  |
| 4 |  |  |  |

## 设置\读取NB频点 0x1B

### 命令说明

此命令用于设置/读取模块的频点。

### 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 | 设置类型 | 1 | 0 | 0：读取  1：设置 |
| 1 | 频点1 | 2 | 0 | uint16 |
| 2 | 频点2 | 2 | 0 | uint16 |
| 3 | 频点3 | 2 | 0 | uint16 |

### 设置下行应答：

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

### 读取下行:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

### 读取下行应答：返回设置后的信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | 频点1 | 2 |  | uint16 |
| 2 | 频点2 | 2 |  | uint16 |
| 3 | 频点3 | 2 |  | uint16 |
| 4 | 操作结果 | 1 |  | 返回的操作结果 0xAA或0xAB |

## 读预缴费历史记录 0x1C

### 命令说明：

**本命令可读取最近10次的缴费记录历史信息**

### 下行：空数据域

### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | X |
| 段序号 | 段标识 | 段大小 | 段说明 |
|  | 历史累计总用量 | 4 | Float类型 |
|  | 历史累计总金额 | 4 | Float类型 |
| 0 | 预缴时间1 | 5 | YY YY MM DD HH |
| 1 | 充值序号1 | 2 | 1字节的充值网点+1字节的充值序号 |
| 2 | 预缴金额1 | 4 | 单位分 |
| 3 | 预缴时间2 | 5 | YY YY MM DD HH |
| 4 | 充值序号2 | 2 | 1字节的充值网点+1字节的充值序号 |
| 5 | 预缴金额2 | 4 | 单位分 |
| 6 | 预缴时间3 | 5 | YY YY MM DD HH |
| 7 | 充值序号3 | 2 | 1字节的充值网点+1字节的充值序号 |
| 8 | 预缴金额3 | 4 | 单位分 |
| 9 | 预缴时间4 | 5 | YY YY MM DD HH |
| 10 | 充值序号4 | 2 | 1字节的充值网点+1字节的充值序号 |
| 11 | 预缴金额4 | 4 | 单位分 |
| 12 | 预缴时间5 | 5 | YY YY MM DD HH |
| 13 | 充值序号5 | 2 | 1字节的充值网点+1字节的充值序号 |
| 14 | 预缴金额5 | 4 | 单位分 |
| 15 | 预缴时间6 | 5 | YY YY MM DD HH |
| 16 | 充值序号6 | 2 | 1字节的充值网点+1字节的充值序号 |
| 17 | 预缴金额6 | 4 | 单位分 |
| 18 | 预缴时间7 | 5 | YY YY MM DD HH |
| 19 | 充值序号7 | 2 | 1字节的充值网点+1字节的充值序号 |
| 20 | 预缴金额7 | 4 | 单位分 |
| 21 | 预缴时间8 | 5 | YY YY MM DD HH |
| 22 | 充值序号8 | 2 | 1字节的充值网点+1字节的充值序号 |
| 23 | 预缴金额8 | 4 | 单位分 |
| 24 | 预缴时间9 | 5 | YY YY MM DD HH |
| 25 | 充值序号9 | 2 | 1字节的充值网点+1字节的充值序号 |
| 26 | 预缴金额9 | 4 | 单位分 |
| 27 | 预缴时间10 | 5 | YY YY MM DD HH |
| 28 | 充值序号10 | 2 | 1字节的充值网点+1字节的充值序号 |
| 29 | 预缴金额10 | 4 | 单位分 |

## 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: |

## 读预付费用量信息 0x1E

### 命令说明：

读取目前**期初表底数**、**期初预付费余额、本期目前读数**、**本期目前用量、本期目前预付费余额、本期剩余用量、本期最大剩余用量**和**当前计费价格**

### 下行：空数据域

### 上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 | X |
| 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 | 4 |  |
| 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 | 4 | 4 |
| 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 |

## 预留 0x1F

## 预留0x20

## 预留 0x21

## 预留 0x22

## 预留 0x23

## 预留 0x24

## 预留 0x25

## 北京水表参数设置与读取： 0x26

### 命令说明

此命令用于设置/读取北京水表的参数。

### 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 | 设备类型 | 1 | 0X41 | 江西三川NB无磁： 0X41  宁波NB无磁： 0x44  杭州山科NB无磁： 0x35  宁波东海NB无磁： 0x2a  北京京源NB无磁： 0x2b |
| 2 | 水表出厂表号信息 | 7 |  | BCD码 |
| 3 | 过流告警阈值 | 4 |  | 单位L/H |
| 4 | 持续过流时间 | 1 | 1 | 默认值：1 单位分钟 |
| 5 | 反流告警阀值 | 4 |  | 单位L/h，默认DN15mm：40L/h、DN20mm：64 L/h、DN25mm：126L/h，可设置。 |
| 6 | 持续反流告警时间 | 1 | 1 | 单位1分钟，可设置。 |
| 7 | 电压告警阀值 | 2 |  | 单位0.01V |
| 8 | 服务器地址 | 6 |  | 16进制  例如：  NB-IOT的IP+连接端口：  121.43.175.222,5683  IP第1个字节：79  IP第2个字节：2B  IP第3个字节：AF  IP第4个字节：DE  连接端口2个字节：3316 |
| 9 | APN信息 | 6 |  | 运营商APN ASCII |
| 10 | 上报重连次数 | 1 |  | 默认2次，可设置0-4次。 |
| 11 | 周期上报离散起始时间+结束时间+估长 | BYTE[6+6+1] |  | 时间格式为YYMMDDHHMMSS  估长默认10秒，可设置T（1-6）×10秒 |
| 12 | 终端启停设置 | 1 |  | 1启用 0停用 |
| 13 | 周期上报频率 | 1 |  | 默认24小时，可设置1-24小时 |
| 14 | 密集上报起始时间点 | 1 |  | 十六进制，单位小时，设置起始整点，当天有效 |
| 15 | 周期采样间隔 | 1 |  | 单位：30分钟，1~48可设置，默认为1 |
| 16 | 上报重连等待时间 | 1 |  | 20分钟（固化，不可修改） |
| 17 | 密集采样间隔 | 1 |  | 默认5分钟（固化，不可修改） |
| 18 | KEY | 16 |  | AES加解密的KEY,ASCII（固化，不可修改） |
|  |  |  |  |  |

### 设置下行应答：

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

### 读取下行:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

### 读取下行应答：返回设置后的信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | CCID号 | 10 |  | BCD |
| 2 | 设备类型 | 1 | 0X41 | 详细信息见注释2 |
| 3 | 水表出厂表号信息 | 7 |  | BCD码 |
| 4 | 终端时钟 | 6 |  | BCD (YYMMDDHHMMSS) |
| 5 | 终端软件版本 | 1 |  | 16进制 |
| 6 | 过流告警阈值 | 4 |  | 单位L/H |
| 7 | 持续过流时间 | 1 | 1 | 默认值：1 单位分钟 |
| 8 | 反流告警阀值 | 4 |  | 单位L/h，默认DN15mm：40L/h、DN20mm：64 L/h、DN25mm：126L/h，可设置。 |
| 9 | 持续反流告警时间 | 1 | 1 | 单位1分钟，可设置。 |
| 10 | 电压告警阀值 | 2 |  | 单位0.01V |
| 11 | 服务器地址 | 6 |  | 16进制  例如：  NB-IOT的IP+连接端口：  121.43.175.222,5683  IP第1个字节：79  IP第2个字节：2B  IP第3个字节：AF  IP第4个字节：DE  连接端口2个字节：3316 |
| 12 | APN信息 | 6 |  | 运营商APN ASCII |
| 13 | 上报重连次数 | 1 |  | 默认2次，可设置0-4次。 |
| 14 | 周期上报离散起始时间+结束时间+估长 | BYTE[6+6+1] |  | 时间格式为YYMMDDHHMMSS  估长默认10秒，可设置T（1-6）×10秒 |
| 15 | 终端启停设置 | 1 |  | 1启用 0停用 |
| 16 | 周期上报频率 | 1 |  | 默认24小时，可设置1-24小时 |
| 17 | 密集上报起始时间点 | 1 |  | 设置起始整点，当天有效 |
| 18 | 周期采样间隔 | 1 |  | 单位：30分钟，1~48可设置，默认为1 |
| 19 | 上报重连等待时间 | 1 |  | 20分钟（固化，不可修改） |
| 20 | 密集采样间隔 | 1 |  | 默认5分钟（固化，不可修改） |
| 21 | KEY | 16 |  | AES加解密的KEY,ASCII（固化，不可修改） |

## 预留 0x27

## 预留 0x28

## 预留 0x29

## 预留 0x2A

## 预留 0x2B

## 预留 0x2C

## 预留 0x2D

## 预留 0x2E

## 预留 0x2F

# 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 |

## 注释24：设置北京NB水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 |
| 34 | 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 |
| 35 | 69 | 报警状态标志位 | 2 |  | 0 | 清空所有报警状态位 |
| 36 | 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 |
| 37 | 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 |
| 38 | 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 |
| 39 | 74 | 预留 | 10 |  |  |  |
| 40 | 84 | CCID号 | 10 |  |  | BCD |
| 42 | 94 | 水表出厂表号信息 | 7 |  |  | BCD码 |
| 44 | 101 | 终端软件版本 | 1 |  |  | 16进制 |
| 45 | 102 | 过流告警阈值 | 4 |  |  | 单位L/H |
| 46 | 106 | 持续过流时间 | 1 |  |  | 默认值：1 单位分钟 |
| 47 | 107 | 反流告警阀值 | 4 |  |  | 单位L/h，默认DN15mm：40L/h、DN20mm：64 L/h、DN25mm：126L/h，可设置。 |
| 48 | 111 | 持续反流告警时间 | 1 |  |  | 单位1分钟，可设置。 |
| 49 | 112 | 电压告警阀值 | 2 |  |  | 单位0.01V |
| 51 | 114 | APN信息 | 6 |  |  | 运营商APN ASCII |
| 52 | 120 | 上报重连次数 | 1 |  |  | 默认2次，可设置0-4次。 |
| 53 | 121 | 周期上报离散起始时间+结束时间+估长 | BYTE[6+6+1] |  |  | 时间格式为YYMMDDHHMMSS  估长默认10秒，可设置T（1-6）×10秒 |
| 54 | 134 | 终端启停设置 | 1 |  |  | 1启用 0停用 |
| 55 | 135 | 周期上报频率 | 1 |  |  | 默认24小时，可设置1-24小时 |
| 56 | 136 | 密集上报起始时间点 | 1 |  |  | 设置起始整点，当天有效 |
| 57 | 137 | 周期采样间隔 | 1 |  |  | 单位：30分钟，1~48可设置，默认为1 |
| 58 | 138 | 上报重连等待时间 | 1 |  |  | 20分钟（固化，不可修改） |
| 59 | 139 | 密集采样间隔 | 1 |  |  | 默认5分钟（固化，不可修改） |
| 60 | 140 | KEY | 16 |  |  | AES加解密的KEY,ASCII（固化，不可修改） |
| 61 | 156 | 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IMEI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 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 01 55 AA B6 16

**RXD:** D3 91 1E 00 C0 01 3B FB 9F 02 08 69 48 70 30 00 64 06 19 21 68 00 10 66 00 00 01 AA 55 AA DC 16

#### 打开NB入网模式【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 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 02 55 AA 52 16

**RXD:**D3 91 1E 00 C0 01 3B FB 9F 02 08 69 48 70 30 00 77 76 19 21 68 00 10 66 00 00 02 AA 55 AA 4F 16

#### 退出NB入网测试模式【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 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 07 55 AA 67 16

**RXD:**D3 91 1E 00 C0 01 3B FB 9F 02 08 69 48 70 30 00 77 76 19 21 68 00 10 66 00 00 07 AA 55 AA CE 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 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 07 55 AA 1F 16

**RXD:**

#### 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 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 02 55 AA EB 16

**RXD:**

#### 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 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 0A 55 AA 77 16

**RXD:**D3 91 1E 00 C0 01 3B FB 9F 02 08 69 48 70 30 00 64 06 19 21 68 00 10 66 00 00 0A AA 55 AA 48 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 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 02 55 AA A4 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：休眠电流符合要求  BIT1：NB入网成功，信号强度符合要求  BIT2：预留  BIT3：预留  BIT4：预留  BIT5：预留  BIT6：阀控电路测试OK  BIT7：计量电路测试OK  BIT8：LCD测试OK  BIT9：预留 |

##### 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 1F 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 0C 00 00 55 AA7F 16

**TXD:** 55 55 D3 91 1F 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 0C 01 01 55 AA5B 16

**RXD:**D3 91 1E 00 C0 01 3B FB 9F 02 08 69 48 70 30 00 77 76 19 21 68 00 10 66 00 00 0C AA 55 AA 5A 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：休眠电流符合要求  BIT1：NB入网成功，信号强度符合要求  BIT2：预留  BIT3：预留  BIT4：预留  BIT5：预留  BIT6：阀控电路测试OK  BIT7：计量电路测试OK  BIT8：LCD测试OK  BIT9：预留 |

##### 实例数据：

**TXD:**55 55 D3 91 1D 00 10 01 3B FB 9F 02 19 21 68 00 10 66 00 00 D4 D4D4D4D4D4D4D4 0D 55 AA0D 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

### 北京水表表端运行参数设置/读取（命令字：0x3C）

#### 功能简介：

1. 模块在生产时设置/读取模块的ID号和相关运行参数。

#### 设置下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类型 | 1 | 0:读取  1:设置 |
| 1 | 运行参数 |  | 详见注释24：设置表端模块运行参数的数据域结构 |

#### 设置上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

#### 读取下行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类型 | 1 | 0:读取  1:设置 |

#### 读取上行：

|  |  |  |  |
| --- | --- | --- | --- |
| 数据域结构 | | 总长 |  |
| 段序号 | 段标识 | 段大小 | 段说明 |
| 0 | 设置类型 | 1 | 0:读取  1:设置 |
| 1 | 运行参数 |  | 详见注释24：设置表端模块运行参数的数据域结构 |

# 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）

## 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

变量值在传输及存储均为低字节在前，高字节在后。

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。

广播升级程序的设备为手持机或集中器。

被升级设备为表具。

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。

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：

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：

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。

}