

一、 修订历史

版本	修改内容	日期	作者
V1.0	创建初版	2020-11-19	XT
V2.0	优化协议格式	2020-12-19	XT
V3.0	增加CRC校验	2022-5-10	Milo

二、 概述

1. 编写目的

描述 NB 设备与移动 OneNet、电信 AEP (CTWING) 的数据通信格式及方法，方便产品的开发。

2. 开发环境

- (1) 基于中国移动 OneNet、中国电信 AEP (CTWING)
- (2) 支持 LWM2M 通讯协议

三、 帧数据格式定义

字段	Header	Version	Cmd	dataLen	data	CRC+Tail
含义	帧头	协议版本	命令位	数据长度	数据	校验位+帧尾
长度	2 字节	1 字节	1 字节	1 字节	N	2 + 3 字节

- ◆ 帧头：2 字节，固定为 0x4B57
- ◆ 数据长度：1 字节，数据内容的字节数
- ◆ 数据内容：根据不同设备类型而定
- ◆ 帧格式是：以十六进制数形式的字符串上报
- ◆ 校验位：2字节，本协议使用CRC16-XMODEM多项式 $x^{16}+x^{12}+x^5+1$

校验内容=（帧头+协议版本+命令位+数据长度+数据体），舍去16位(2字节)以上的进位位后所形成的2字节校验数

- ◆ 帧尾：3字节，固定为 0x494F54

帧格式是：以十六进制数格式上报

四、 协议版本对照表

版本	协议上传内容
V1.0	0x10
V2.0	0x20
V2.6	0x26

五、 命令集

命令类型	说明	备注
01	设备注册	设备→平台（设备第一次上电发送）
02	设备事件上报	设备→平台
03	指令下发	平台→设备
04	下发指令回复	设备→平台

六、 设备类型对照表

设备类型	类型值	备注
01	门磁	

02	燃气	
03	烟感	
04	手报（紧急按钮）	
05	一氧化碳	
06	温感	
07	声光	

七、 事件类型对照表

事件类型	事件名称	备注
01	心跳	
02	报警	
03	报警恢复	
04	防拆报警	
05	防拆报警恢复	
06	低电压	
07	低电压恢复	
08	传感器故障	
09	传感器故障恢复	
0A	测试报警	
0B	测试报警恢复	
0C	紧急报警	
0D	紧急报警恢复	
0E	温度报警	
0F	温度报警恢复	

八、 注册包上报说明

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	协议版本
Byte4	命令	0x01 (注册)	1	命令集
Byte5	数据长度	0x37	1	
Byte6	设备类型	0x01	1	设备类型
Byte7~byte 21	设备编号	0x383639393735303334343431303832 Imei : 869975034441082	15	16 进制 ascil
Byte22~Byt e36	IMSI	0x3436303131333313138373433373332 Imsi : 460113118743732	15	16 进制 ascil
Byte37~Byt e56	ICCID	0x3839383631313230323234303134333 938373632 ICCID : 89861120224014398762	20	16 进制 ascil
Byte57 Byte58 Byte59 Byte60	电池电压 CSQ 电池电量 程序版本	0x25 (3.7V) 0x15 0x64 (100%) 0x10(1.0)	4	
Byte61-62	校验位	0xXXXX	2	参考CRC说明
Byte63-65	尾部	0x494F54	3	

示例：				
4B5726013701383639393735303334343431303832343630313133313138373433373332				
383938363131323032323430313433393837363225156410E79C494F54				

九、 不同设备类型事件包上报说明

1. 门磁事件上报

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	协议版本
Byte4	命令	0x02（事件上报）	1	命令集
Byte5	数据长度	0x16	1	
Byte6	设备类型	0x01	1	设备类型
Byte7~byte21	设备编号	0x383639393735303334343431303832 Imei : 869975034441082	15	16 进制 ascii
Byte22	事件类型	0x01（心跳）	1	事件类型
Byte23	门磁状	0x00	1	00：门窗已关

	态			闭；01：门窗已打开
Byte24	电池电压	0xx	1	电池电压，0.1v 为单位。
Byte25	CSQ（信号强度）	0x15	1	值范围：0~31
Byte26	电池电量	0x64	1	
Byte27	版本	0x10	1	
Byte28-29	校验码	0XXXXX	2	
Byte30~byte32	尾部	0x494F54	3	
示例：4B5726021601383639393735303334343431303832010025156410A9EB494F54				

2. 燃气事件上报

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	协议版本
Byte4	命令	0x02（事件上报）	1	命令集
Byte5	数据长度	0x17	1	
Byte6	设备类型	0x02	1	设备类型

Byte7~byte21	设备编号	0x383639393735303334343431303832 Imei: 869975034441082	15	16 进制 ascil
Byte22	事件类型	0x01(心跳)	1	事件类型
Byte23	燃气浓度值	0x0A(10%LEL)	1	
Byte24	电池电压	0x25(3.7V)	1	电池电压， 0.1v 为单位。
Byte25	CSQ（信号强度）	0x15	1	值范围： 0~31
Byte26	百分比	0x64	1	
Byte27	阀门状态	00	1	01：阀开 0:关
Byte28	版本	0x10	1	
Byte29~Byte30	校验位	0XXXXX	2	
Byte31-33	尾部	0x494F54	3	

示例：4B5726021702383639393735303334343431303832010A2515640010C09D494F54

3. 烟感事件上报

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	协议版本
Byte4	命令	0x02（事件上报）	1	命令集

Byte5	数据长度	0x15	1	
Byte6	设备类型	0x03	1	设备类型
Byte7~byte21	设备编号	0x383639393735303334343431303832 Imei: 869975034441082	15	16 进制 ascil
Byte22	事件类型	0x01 (心跳)	1	事件类型
Byte23	电池电压	0xx	1	电池电压， 0.1v 为单位。
Byte24	CSQ（信号强度）	0x15	1	值范围： 0~31
Byte25	电量	00	1	
Byte26	版本	00	1	
Byte27-28	校验码	00	2	
Byte29~byte31	尾部	0x494F54	3	
示例：4B57260215033836393937353033343434313038320125156410D578494F54				

4. 手报（紧急按钮）事件上报

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版	0x26	1	协议版本

	本			
Byte4	命令	0x02（事件上报）	1	命令集
Byte5	数据长度	0x15	1	
Byte6	设备类型	0x04	1	设备类型
Byte7~byte21	设备编号	0x383639393735303334343431303832 Imei: 869975034441082	15	16 进制 ascil
Byte22	事件类型	0x01(心跳)	1	事件类型
Byte23	电池电压	0xx	1	电池电压， 0.1v 为单位。
Byte24	CSQ（信号强度）	0x15	1	值范围： 0~31
Byte25	电量	00	1	
Byte26	版本	0x10	1	
Byte27-28	校验码	00	2	
Byte29~byte31	尾部	0x494F54	3	
示例：4B5721021304383639393735303334343431303832016415494F54				

5. 一氧化碳（CO）事件上报

序号	名称	数据	字节数	说明
----	----	----	-----	----

Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x21	1	协议版本
Byte4	命令	0x02（事件上报）	1	命令集
Byte5	数据长度	0x16	1	
Byte6	设备类型	0x05	1	设备类型
Byte7~byte21	设备编号	0x383639393735303334343431303832 Imei: 869975034441082	15	16 进制 ascii
Byte22	事件类型	0x01（心跳）	1	事件类型
Byte23~Byte24	燃气浓度值	0x0064 (100PPM)	2	
Byte25	电池电压	0xx	1	电池电压， 0.1v 为单位。
Byte26	CSQ（信号强度）	0x15	1	值范围： 0~31
Byte27	电量	00	1	
Byte28	版本	00	1	
Byte29-30	校验码	00	2	
Byte31~byte33	尾部	0x494F54	3	

示例：4B572602160538363939373530333434343130383201006425156410E58A494F54

6. 温感事件上报

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	协议版本
Byte4	命令	0x02（事件上报）	1	命令集
Byte5	数据长度	0x16	1	
Byte6	设备类型	0x06	1	设备类型
Byte7~byte21	设备编号	0x383639393735303334343431303832 Imei: 869975034441082	15	16 进制 ascii
Byte22	事件类型	0x01（心跳）	1	事件类型
Byte23	温度值	0x14（20℃）	1	单位：℃
Byte24	电池电压	0xx	1	电池电压， 0.1v 为单位。
Byte25	CSQ（信号强度）	0x15	1	值范围：0~31
Byte26	电量	00	1	
Byte27	版本	0x10	1	

Byte28-29	校验码	00	2	
Byte30~byte33	尾部	0x494F54	3	
示例：4B5726021606383639393735303334343431303832011425156410359E494F54				

7. 声光事件上报

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	协议版本
Byte4	命令	0x02（事件上报）	1	命令集
Byte5	数据长度	0x15	1	
Byte6	设备类型	0x07	1	设备类型
Byte7~byte21	设备编号	0x383639393735303334343431303832 Imei: 869975034441082	15	16 进制 ascil
Byte22	事件类型	0x01（心跳）	1	事件类型
Byte23	电池电压	0xx	1	电池电压， 0.1v 为单位。
Byte24	CSQ（信号强度）	0x15	1	值范围： 0~31

Byte25	电量	00	1	
Byte26	版本	00	1	
Byte27-28	校验码	00	2	
Byte29~byte31	尾部	0x494F54	3	
示例：4B57260215073836393937353033343434313038320125156410B2C3494F54				

十、 指令下发

命令类型

命令类型	含义
01	消音
02	报警控制

1、消音下发（烟感）

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	默认
Byte4	命令	0x03（指令下发）	1	命令集
Byte5	数据长度	0x01	1	
Byte6	命令类型	0x01	1	命令类型
Byte7~Byte8	校验码	00	2	
Byte9~Byte11	尾部	0x494F54	3	
消音---示例：4B5726030101B1C3494F54				

2、报警控制 （声光）

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x10	1	默认
Byte4	命令	0x03 （指令下发）	1	命令集
Byte5	数据长度	0x01	1	
Byte6	命令类型	0x02	1	命令类型
Byte7	操作模式	0x00	1	00: 解除报警 01: 报警
Byte8~Byte12	校验位+尾部	CRC + 0x494F54	2+3	
报警控制 -- 示例：4B572603020201XX494F54				

十一、 指令下发结果回复

序号	名称	数据	字节数	说明
Byte1~ Byte2	头部	0x4B57	2	
Byte3	协议版本	0x26	1	和下行一致
Byte4	命令	0x04 （指令下发回复）	1	命令集
Byte5	数据长度	0x13	1	
Byte6~byte20	设备编号	0x383639393735303334343431303832 Imei: 869975034441082	15	16 进制 ascii

Byte21	命令 类型	0x01	1	命令类型
Byte22	执行 结果	0x01	1	01: 成功 02: 失败
Byte23~Byte24	操作 值	xx	2	命令没有操作 值则固定为 FFFF
Byte25~Byte29	crc+尾部	CRC+0x494F54	2+3	
示例: 4B572604133836393937353033343434313038320101FFFFxx494F54				

十二、 说明

- 1、 设备每次上电注册时需要发送一次注册包和心跳包;
- 2、 心跳时间为 24 小时上报一次

```

unsigned short CRC16_XMODEM(unsigned char *puchMsg, unsigned int usDataLen)
{
    unsigned short wCRCin = 0x0000;
    unsigned short wCPoly = 0x1021;
    unsigned char wChar = 0;
    while (usDataLen--)
    {
        wChar = *(puchMsg++);
        wCRCin ^= (wChar << 8);
        for (int i = 0; i < 8; i++)
        {
            if (wCRCin & 0x8000)
                wCRCin = (wCRCin << 1) ^ wCPoly;
            else
                wCRCin = wCRCin << 1;
        }
    }
    return (wCRCin);
}

```