**G805G CAT1设备TCP协议**

**需要服务器回复的包有，F0登录包（回复格式有要求），F9心跳包（回复格式没要求）否则会数据不正常**

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 修订人 | 修订日期 | 修订描述 |
| V1.0 |  | 2024-10-26 | 目录整理，协议按型号区分,新增设备使用说明 |
| V1.1 |  | 2024-11-14 | 增加上行指令：设备充电状态（需下行开启充电开机才会上报）增加下行指令：设备休眠控制，设备充电状态开关机控制，设备蓝牙广播开关控制，设备按键关机功能开关 |
| V1.2 |  | 2024-11-19 | 增加下行指令：切换长短连接模式 |
| V1.3 |  | 2025-03-19 | 增加并包上报情况说明 |

目录

1.综述 1

2. 设备使用说明 1

2.1 设备功能与使用说明 1

2.2 设备默认上报逻辑 2

2.3 设备下行说明 3

3.协议数据包结构 4

3.1.数据头 5

3.2.报文标示符(Message ID) 5

3.3.Token生成机制 5

3.4.有效负载(Payload) 5

3.5.校验和(Checksum) 6

4.messages报文 7

4.1连接相关 7

4.1.1 LNK-LIN (0xF0)请求连接（TCP专用） 7

4.1.2 LNK-RPL(0xF1) 连接回复（TCP专用）-重要 8

4.1.3新心跳包协议(0xF9)-重要 9

4.1.4心跳包协议(0xF6)（以前设备用，不会和F9同时出现） 10

4.2定位相关上报 11

4.2.1GPS/ BDS位置上报：定位数据上报(0x03) 11

4.2.2 wifi和基站信息上传(0xA4 改进版) 12

4.2.3蓝牙定位信息(LBE Location)（MsgId=0xD6） 14

4.3 报警相关上报 16

4.3.1报警数据上传(0x02) 16

4.3.2 报警数据上传(0x21)(02的补充) 17

4.4设备信息及状态上报 18

4.4.1软件版本和型号上传（0XBB）----以前设备使用可不解析 18

4.4.2 SIM卡的ICCID上传(0xF3) 19

4.4.3状态参数上报(MSGID=0xA9)---可不用解析 19

4.4.4设备状态(0xE9)（以前设备无） 20

4.4.5设备充电状态上传(0xC3) 21

4.5 下行反馈上报 22

4.5.1下行反馈(MSGID=0xC0) 22

5.设置 24

5.1下行 24

5.1.1设置周期上传（0x17） 24

5.1.2设置-综合（见详细说明--重要下行）（0XCE） 25

5.1.3域名设置(0xC3)（TCP专用-以前设备无此功能） 27

#

# **1.**综述

本协议合适于4G CAT1设备，目前支持G805G等产品。

* 使用32位的数据头进行同步和终端识别；
* 使用低开销的校验算法实现校验保护；
* 使用报文标示符来标示不同的报文。
* 此协议为通用协议，需根据实际上报进行解析
* 设备上报的时间为UTC时间
1. **设备使用说明**

**2.1 设备功能与使用说明**

 通用版本：

1. 开机：

第一次使用前请充满电，充电自动开机，充电中灯效：红灯闪烁，充满电灯效：绿灯长亮，

手动开机：长按SOS按键5秒以上，开机灯效：红绿灯光交替闪烁，语音提示“欢迎使用智能物联网终端”

1. 关机：

 充电：自动关机

手动关机：关机：长按SOS按键15秒以上，灯闪烁后熄灭，语音提示“请注意设备主动关机”

低电关机：语音提示“请注意，设备电量不足关机”

1. 状态灯效：

 设备电量低：红灯闪烁，语音提示”设备电量低，请及时充电”

1. SOS功能:

 触发方式：触发后设备不进休眠，长按按钮5s，红灯闪烁后松开，红灯长亮，语音提示“进入报警模式”

 取消方式：红灯长亮下，长按按钮5秒红灯闪烁后松开，取消SOS报警，语音提示“关闭报警模式”。

1. 入网状态：

 未入网：短按一下sos按键，灯效为红灯

 已入网：短按一下sos按键，灯效为绿灯

1. 设备休眠：

 触发条件：设备20分钟一动不动，进入休眠模式，不上报数据

**2.2 设备默认上报逻辑**

通用版本：

1. 连接相关上报

 F0请求：设备是短链接的，会按定位上报频率请求连接

 F9/F6：心跳包上报，跟着定位报文一起上报

1. 定位相关上报

 gps/wifi/蓝牙信标：默认上报频率10分钟，默认定位优先级：wifi>gps，wifi定位优先，定位不到切换gps

1. 报警相关上报

 SOS报警(0x02)：使用者主动触发,触发方式见下一节

 SOS取消(0x02)：使用者主动触发取消,触发方式见下一节

 关机报警(0x02)：设备主动关机或低电关机,触发方式见下一节

 低电量报警(0x02)：设备当前 电量等级 小于等于0时触发

1. 设备信息及状态上报

 软件版本和型号(BB)/状态参数(A9)：开机会上报一笔

 SIM卡ICCID(F3)：开机上报一笔

 设备状态(E9):开机上报一笔，有上报频率有更改时上报一笔

充电状态(C3):充电开机状态会上报，关机状态不会上报

1. 下行反馈

 下行反馈(C0):服务器下行指令设备收到后上报，注意，短链接设备，下行指令在设备上报的时候设备才接收下行指令

注：设备上报有并包上报的情况，也就是一个数据包里面含有多个完整的报文，注意不要遗漏，报文为完整报文，不会出现中间断开在下一个数据包的现象

Eg:bdbdbdbdd6000119a9cf610445270387bf452708a1bc44279d18b74427e518b7f9bdbdbdbdf9010000006400002800000019a9cf61ca

此数据包里含有(0xD6)蓝牙定位和(0xF9)电量信号的报文

(0xD6)蓝牙定位:bdbdbdbdd6000119a9cf610445270387bf452708a1bc44279d18b74427e518b7f9

(0xF9)电量信号:bdbdbdbdf9010000006400002800000019a9cf61ca

**2.3 设备下行说明**

通用版本

1. 设备定位上报频率下发(0x17)：

默认上报频率10分钟，最低1分钟，下行指令设备收到后，设备按下发指令的时间段和频率

上报数据，时间段外按默认上报频率上报，如：00：00-18：00 5分钟定位上报，那么

时间段外按默认10分钟上报频率上报

1. 设备定位优先级下发(0xCE01):

 默认定位优先级wifi>gps,定位优先级如：wifi>gps>蓝牙信标，则wifi定位不到切换

gps,gps定位不到切换蓝牙信标，当定位成功时，不会切换下个定位优先级产生定位

1. 修改ip和端口指令下发(0xC3):

 默认通用版本指向为智慧云平台：118.178.184.219:8825,如需更改，可咨询相关对接人员或访问官网

1. 蓝牙广播开关下发(0xCE05):

 默认为开启状态，关闭后设备不进行蓝牙广播

1. 按键关机开关指令下发(0xCE16):

 默认设备可通过按键进行关机，下行关闭后设备不能通过按键进行关机

1. 控制设备触发休眠开关下发(0xCE18):

 默认为开启状态，设备40分钟不动进入休眠，下行关闭后，设备不进休眠

1. 控制设备充电开关机状态(0xCE21):

 默认充电为关机状态，下行开启后，设备充电不关机，设备上报充电状态

(8)按键触发sos启动开关(0xCE19)

 默认为开启状态，长按按键触发，关闭后，长按按键不会触发上报sos

(9)长连接短连接模式切换(0xCE22)

 默认为短连接，下行切换长连接指令，设备收到后重启变为长连接，注意长连接模式功耗会变大，默认状态每4分钟上报一次心跳包(0xF9)

# **3.**协议数据包结构

一条基本的协议数据包结构如图1所示：



图**1** 协议数据包结构图

## **3.1.**数据头

每个数据包均以4个字节的Header或者token开头（在某些回复报文中，timestamp代替）：

目前欧孚设备上传token固定为BDBDBDBD

* Header: 0xBD 0xBD0xBD0xBD；
* Timestamp: 32bits，由服务器产生

## **3.2.**报文标示符(Message ID)

 MessgeId 代表的内容如第3章。

 TCP每次链接的时候设备端都会先上报0xF0 报文，里面有设备唯一标识符IMEI，服务器端需要记录该imei作为标识。并回复0xf1报文，设备端才会认为此链接成功，否则会断开链接

## **3.3.**Token生成机制

目前固定为BDBDBDBD

## **3.4.**有效负载(Payload)

我们下面的payload 指的是协议中除了head token及校验码外的有效正文内容。后面加注的是正文长度。

有效负载中所用的数据格式如下表所示：

【U-unsigned；I-signed；X-bitfield；数字-所占字节数】

以下协议中使用除ch，u8，i8，x8外 都采用小端优先

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Short** | **peTypeType** | **Size(Bytes)** | **Min/max** | **Resolution** | **说明** |
| CH | ASCII/ISO 8859.1 | 1 | - | - | 字符 |
| u8 | Unsigned Char | 1 | 0..255 | 1 | 无符号短整形 |
| i8 | Signed Char | 1 | -128..127 | 1 | 短整形 |
| x8 | Bitfield | 1 | - | - | 位（bit） |
| u16 | Unsigned Short | 2 | 0..65，535 | 1 | 无符号整形 |
| i16 | Unsigned Short | 2 | -32,768..32,767 | 1 | 整形 |
| x16 | Bitfield | 2 | - | - | 位（bit）2 |
| u32 | Unsigned Long | 4 | 0..4,294,967,295 | 1 | 无符号长整形 |
| i32 | Signed Long | 4 | -2,147,483,648..2,147,483,647 | 1 | 长整形 |
| u64 | Uint64\_t | 8 | 0..18,446,744,073,709,551,616 | 1 | 无符号64位长整形 |
| float | float | 4 | -3.44\*10e38..3.4\*10e38 | - | 浮点型 |

## **3.5.**校验和(Checksum)

校验和所加内容包括payload，如图1所示。其算法如下所示，其中Buffer[N]表示需要累加的数据。

Ck\_sum = 0

For(i=0; i<N; i++)

{

ck\_sum = ck\_sum + Buffer[i]

ck\_sum = ck\_sum % 0x100

}

ck\_sum = 0xFF – ck\_sum

Return ck\_sum

其中，ck\_sum不能超过0xFF，故每次循环之后都要模0x100后取余。

# **4.**messages报文

## 4.1连接相关

### 4.1.1 LNK-LIN (0xF0)请求连接（TCP专用）

|  |  |
| --- | --- |
| Message | LNK-LIN |
| Description | Terminal requests to log into the terminal server through IMEI number |
| Firmware | 　 |
| Direction | Terminal => Terminal Server |
| Payload length | 10bytes |
| Message structure | Header | Message ID | Payload | Checksum |
| 0xBD 0xBD 0xBD 0xBD | 0xF0 | See below | CK\_sum |

Payload contents

BDBDBDBD F0 868DBA353D1003006C67 F6

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte Offset | Format | Name | Scale | Unit | Drscription |
| 8 | u64 | IMEI | 1 | - | IMEI number（小端模式） |
| 2 | x16 | version |  | - | Bitfield see below |

请求一定得有0XF1报文（具体格式见下一节）回复，否则登录失败

例：bdbdbdbdf09b51731bc61603000014 （imei是869465050010011）

BDBDBDBD：4个字节消息头

F0：消息id

9b51731bc6160300：imei number (小端模式)，imei 十进制是869465050010011，十六进制就是0x000316C6 1B73 519B, 小端模式即9b51731bc6160300

6C67：version

F6：校验码

tcp每次创建一个新的连接的时候会先上报F0 请求，f0里带imei，然后服务器记录下这个imei, 之后这个链接里所有的数据都是这个imei的

### 4.1.2 LNK-RPL(0xF1) 连接回复（TCP专用）-重要

|  |  |
| --- | --- |
| Message | LNK-RPL |
| Description |  |
| Firmware | 　 |
| Direction | Terminal <= Terminal Server |
| Payload length | 4 bytes |
| Message structure | Header | Message ID | Payload | Checksum |
| Timestamp(unix) | 0xF1 | See below | CK\_sum |

Payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte Offset | Format | Name | Scale | Unit | Drscription |
| 4 | u32 | Token | 1 | - | Token:固定为BDBDBDBD |

例：28D4DE55F1BDBDBDBDEB

回复需在当前通道回复

前面4个字节为时间戳，设备端根据此同步时间，所以必须为正确的时间戳值，小端模式，回复是一个字节一个字节回复，如：BD算一个字节

时间戳 是指当前时间距离1970-1-1 0点的秒数或者毫秒数 毫秒数在java里好转换一点 我们协议用的是秒数 长整形 我们采用小端优先的方式 就变成了当前这种样式 28D4DE55 --》55 DE D4 28 是其实际值 然后把这个值转成长整形 这个值加上1970-1-1 0点就是当前时间数

例子：时间戳 = 07FD8860真实值 6088FD07 =1619590407秒 这个是以1970-01-01 00:00:00 加上

1619590407 秒，就是设备上报时间：2021/4/28 6:13:27

### 4.1.3新心跳包协议(0xF9)-重要

终端连上服务器后，固定间隔周期上传服务器心跳包

|  |  |
| --- | --- |
| Message | MSG\_HTB\_UPL |
| Decription | 心跳 |
| Firmware | -/- |
| Payload Length | 15 bytes |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xF9 | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 1 | U8 | Bat\_type |  |  | 电量类型0：4级制1：5级制2：百分比3：电压值 |
| 2 | u16 | Bat\_volt |  | -/- | 电量值如果Bat\_type为0：则电量值范围为0-3（0为25%，3为100%）如果Bat\_type为1：则电量值范围为0-4（0为20%，4为100%）如果Bat\_type为2：则电量值范围为0-100 |
| 1 | U8 | Signal\_type |  |  | 信号类型0：百分比  1：5级制2：CSQ值 |
| 2 | I16 | Signal\_strength |  |  | 信号强度 |
| 1 | U8 | Other\_type |  |  | 扩展类型0：全量记步 1：增量记步2：震动 |
| 4 | U32 | Num |  |  | 扩展值 |
| 4 | U32 | Timestamp | -/- | -/- | utc时间戳 |

心跳包必须有回复 ，可以随便回复一个字节 ,比如0x01，设备端只要收到回复就认为链接还存在。

Eg：BDBDBDBDF301 可以固定回复这个

### 4.1.4心跳包协议(0xF6)（以前设备用，不会和F9同时出现）

终端连上服务器后，每隔固定间隔周期时间上传服务器心跳包 后面的版本都会带时间戳。

|  |  |
| --- | --- |
| Message | MSG\_HTB\_UPL |
| Decription | 心跳 |
| Firmware | -/- |
| Payload Length | 11 bytes  |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xF6 | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 2 | U16 | Bat\_volt |  | -/- | 电池电量格数 |
| 4 | U32 | Step\_num |  |  | 记步数据 |
| 1 | U8 | Signal\_strength |  |  | 信号强度 |
| 4 | U32 | Timestamp |  |  | 时间戳(补传时会在后面加时间戳) |

例：BDBDBDBDF6030000000000509C75FE6350

Bat\_volt=0 代表电池电量的百分比为百分之10

 Bat\_volt=1 代表电池电量的百分比为百分之30

 Bat\_volt=2 代表电池电量的百分比为百分之60

Bat\_volt=3 代表电池电量的百分比为百分之100

## 4.2定位相关上报

### 4.2.1GPS/ BDS位置上报：定位数据上报(0x03)

|  |  |
| --- | --- |
| Message | MSG\_UPL\_GPS |
| Decription | 回馈GPS/BDS定位数据 |
| Firmware | -/- |
| Payload Length | 23 bytes |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0x03 | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 8 | Double | lon |  | -/- | longitude |
| 8 | Double | lat |  | 　 | latitude |
| 1 | U8 | north\_south |  |  | /\*N or S\*/ |
| 1 | U8 | east\_west |  |  | /\*E or W\*/ |
| 1 | U8 | status |  |  | /\*A or V\*/ |
| 4 | U32 | Timestamp  |  |  | 时间戳 |

例如： BDBDBDBD03000000C0424C5E4000000000A5DC3C404E4541E62C616078

Lon: 000000C0424C5E40Lat: 00000000A5DC3C40 4E –N 45-E 41-A Time E62C6160

Lon:121.191574Lat: 28.861893

Status =A 表示信息内容准确。可以解析 为V可以放弃

GPS解析示例（JAVA）：

报文：DBDBDBDB037d9f84ac81815c40e766926b1d8936404e4541749d695f0b

//DBDBDBDB03 7d9f84ac81815c40 e766926b1d893640 4e 45 41 749d695f 0b

public static void main(String[] args){

 //报文7d9f84ac81815c40 实际值405c8181ac849f7d

Double.longBitsToDouble(Long.parseLong("405c8181ac849f7d",16))); //114.02353966666665

//报文e766926b1d893640 实际值4036891d6b9266e7

Double.longBitsToDouble(Long.parseLong("4036891d6b9266e7", 16))) ;//22.535605166666667

HexToStr(data.Substring(“4e”)); //N

HexToStr(data.Substring(“45”));//E

HexToStr(data.Substring(“41”));//AA表示数据"OK"，V表示一个警告

//报文 749d695f实际值 5f699d74

 Date date=new Date();

date.setTime(Long.parseLong(“5f699d74",16)\*1000);

SimpleDateFormatsdf = new SimpleDateFormat("yyyyMMddHHmmss");

System.out.println(sdf.format(date)); //2020-09-22 14:45:08

注：解析出来的gps经纬度为WGS-84坐标系，若地图使用百度高德等，坐标系需要转换

### 4.2.2 wifi和基站信息上传(0xA4 改进版)

|  |  |
| --- | --- |
| Message | EXT-CIU |
| Description | Cell information upload.Upload cell tower information for terminal server to compute location. |
| Firmware | 　 |
| Direction | Terminal -> Terminal Server |
| Payload length |  |
| Message structure | Header | Message ID | Payload | Checksum |
| Token | 0xA4 | See below | CK\_sum |

Payload contents:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Byte Offset** | **Format** | **Name** | **Scale** | **Unit** | **Description** |
| 4 | U32 | UtcTime |  |  | Search Time |
| 1 | u8 | Cell\_cnt | 1 | - | Number of cell info payload.Valid value:0~7 |
| 2 | u16 | Cell[0].MCC | - | - | mobile country code of cell[0] |
| 2 | u16 | Cell[0].MNC | - | - | mobile network code of cell[0] |
| 2 | u16 | Cell[0].LAC | - | - | Location area code of cell[0] |
| 4 | U32 | Cell[0].CELL\_ID | - | - | Cell id of cell[0] |
| 2 | i16 | Cell[0].RSSI | - | dbm | RSSI in dbm of cell[0] |
| … | 　 | 　 | 　 | 　 | 　 |
| 　2 | u16 | Cell[cell\_cnt-1].LAC | - | - | Location area code of cell[[cell\_cnt-1] |
| 　4 | U32 | Cell[cell\_cnt-1].CELL\_ID | - | - | Cell id of cell[[cell\_cnt-1] |
| 　2 | I16 | Cell[cell\_cnt-1].RSSI | - | dbm | RSSI in dbm of cell[[cell\_cnt-1] |
| 1 | U8 | Wifi\_cnt |  |  | Number 0f wifi |
| 1 | U8 | Wifi[0].bssid[0] |  |  |  |
| 1 | U8 | Wifi[0].bssid[1] |  |  |  |
| 1 | U8 | Wifi[0].bssid[2] |  |  |  |
| 1 | U8 | Wifi[0].bssid[3] |  |  |  |
| 1 | U8 | Wifi[0].bssid[4] |  |  |  |
| 1 | U8 | Wifi[0].bssid[5] |  |  |  |
| 4 | I32 | Wifi[0].rssi |  |  |  |
|  |  |  |  |  |  |
| 1 | U8 | Wifi[Wifi\_cnt-1].bssid[0] |  |  |  |
| 1 | U8 | Wifi[Wifi\_cnt-1].bssid[1] |  |  |  |
| 1 | U8 | Wifi[Wifi\_cnt-1].bssid[2] |  |  |  |
| 1 | U8 | Wifi[Wifi\_cnt-1].bssid[3] |  |  |  |
| 1 | U8 | Wifi[Wifi\_cnt-1].bssid[4] |  |  |  |
| 1 | U8 | Wifi[Wifi\_cnt].bssid[5] |  |  |  |
| 4 | I32 | Wifi[wifi\_cnt].rssi |  |  |  |

标注: 总计提供7个基站信息，即驻留的服务小区和邻近的6个小区。注：不是所有上报的报文都有基站信息，许多基站被加密，没有基站为正常情况

报文标示符(Message ID)

BDBDBDBDA468984C5F01CC010000C21871F543009E00078CBEBE1A8162C6FFFFFFC061180AF42AC1FFFFFF200BC726E000B6FFFFFFA8154DF6517EB2FFFFFFE005C5B1F824CCFFFFFFE8FCAFA02663AFFFFFFF6409805B2B9CAEFFFFFF94

最终取到经纬度数据还要参阅wifi定位关于A3和A2及A4协议解析的说明和高德wifi定位协议，如下：



### 4.2.3蓝牙定位信息(LBE Location)（MsgId=0xD6）

|  |  |
| --- | --- |
| Message | MSG\_HTB\_UPL |
| Decription | 上传标签 |
| Firmware | -/- |
| Payload Length | 1 bytes +n |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xD6 | 见下方定义 | CK\_sum |

Payload:

|  |  |  |  |
| --- | --- | --- | --- |
| Format | Name | Scale | Description |
| U8 | Type | 1 | 目前固定为0 (Fix value 0) |
| U8 | Total\_groups | 1 | 总组数,可能有多组信息,每组里可能有多个ibeacon (The total number of groups, there may be multiple groups of information, and there may be multiple ibeacons in each group) |
| Int32 | Utc | 4 | Utc时间戳 (the UTC timestamp of the first group) |
| U8 | Total\_PackCount | 1 | 当前时间的包总数 (the ibeacon’s count of the first group) |
| U16 | Major0 | 2 | Major |
| U16 | Minor0 | 2 | Minor |
| S8 | Rssi0 | 1 | Rssi |
| U16 | MajorN | 2 | Major |
| U16 | MinorN | 2 | Minor |
| S8 | RssiN] | 1 | Rssi |
| Int32 | Utc | 4 | Utc时间戳(UTC timestamp of the second group) |
| U8 | Total\_PackCount | 1 | 当前时间的包总数(the ibeacon’s count of current group) |
| U16 | Major0 | 2 | Major |
| U16 | Minor0 | 2 | Minor |
| S8 | Rssi0 | 1 | Rssi |
| U16 | MajorN | 2 | Major |
| U16 | MinorN | 2 | Minor |
| S8 | RssiN] | 1 | Rssi |

Example：

bdbdbdbdd60001be20315f0443271794ac43273094aa4327b956a54327fe94a56a

**bdbdbdbd - header**

**d6 - msgID**

**00 - type**

**01 -- 只有一组ibeacon数据（total groups of beacons data :1）**

be20315f -- 第一组beacon时间戳 ( the first group’s timestamp): 0x5f3120be=1597055166

04 --第一组 有4个beacon信息 （the beacon’s count of this group: 4 ）

4327 --- major : 0x2743 = 10051

1794--- minor: 0x9417 = 37911

ac--- rssi: 0xac = -84

4327 --- major: 0x2743 = 10051

3094--- minor:0x9430 = 37936

aa--- rssi:-86

4327 --- major: 0x2743 = 10051

b956--- minor:0x56b9 = 22201

a5--- rssi:-91

4327 --- major: 0x2743 = 10051

fe94--- minor:0x94fe=38142

a5--- rssi:-91

6a --校验码（checksum）

**4.3 报警相关上报**

### 4.3.1报警数据上传(0x02)

|  |  |
| --- | --- |
| Message | LNK-WRN |
| Description | Terminal uploads its warnings to terminal server. |
| Firmware | 　 |
| Direction | Terminal => Terminal Server |
| Payload length | 6 bytes |
| Message structure | Header | Message ID | Payload | Checksum |
| Token | 0x02 | See below | CK\_sum |

Payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte Offset | Format | Name | Scale | Unit | Drscription |
| 2 | x16 | Upl\_warn | - | - | Bitfield see below(小端优先) |
| 4 | U32 | Timestamp |  |  | 时间戳(补传时会在后面加时间戳) |
|  |  |  |  |  |  |

Bitfield WRN:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15 |  |  |  |  |  |  |  |  |  |  | 4 |  |  | 1 | 0 |

 下面提供对应的bit位为1时和当前报警的定义表。也可能多个报警同时存在。灰色为不支持

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| bit | Name | Description | Code | 调整后的16进制 | 十进制 |
| 14 | 跌落报警 | 跌落报警 | 1 | 4000 | 4\*4096=16384 |
| 8 | 设备佩戴 | 设备佩戴 | 7 | 0100 | 1\*256=256 |
| 7 | SOS 取消 | SOS 取消 | 8 | 0080 | 8\*16=128 |
| 6 | 震动报警 | 震动报警 | 9 | 0040 | 4\*16=64 |
| 5 | 久坐报警 | 久坐报警 | 10 | 0020 | 2\*16=32 |
| 4 | 摘掉设备 | 摘掉设备 | 11 | 0010 | 1\*16=16 |
| 3 | 开箱报警 | 开箱报警 | 12 | 0008 | 8 |
| 2 | 关机 | 关机 | 13 | 0004 | 4 |
| 1 | SOS |  | 14 | 0002 | 2 |
| 0 | 低电量 | 低电量 | 15 | 0001 | 1 |

BDBDBDBD02020007FD8860E7 真实值 0002—0000 0000 0000 0010 SOS报警，注意小端

时间戳 = 07FD8860真是值 6088FD07 =1619590407 这个是以1970-01-01 00:00:00 加上

1619590407 秒 就是设备上报时间 2021/4/28 6:13:27

02报警各自独立，相应位的状态在上下文非关联报警中不关联，只处理当前为1的位报警，进行相应处理即可。

**4.3.2 报警数据上传(0x21)(02的补充)**

|  |  |
| --- | --- |
| Message | LNK-WRN |
| Description | Terminal uploads its warnings to terminal server. |
| Firmware | 　 |
| Direction | Terminal => Terminal Server |
| Payload length | 8 bytes |
| Message structure | Header | Message ID | Payload | Checksum |
| Token | 0x21 | See below | CK\_sum |

Payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte Offset | Format | Name | Scale | Unit | Drscription |
| 2 | U16 | type |  |  | 报警类型 |
| 4 | U32 | Upl\_warn | - | - | Bitfield see below(小端优先) |
| 4 | U32 | Timestamp |  |  | 时间戳(补传时会在后面加时间戳) |
|  |  |  |  |  |  |

Alarm type =1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 | 设备充电中，已关机(固件需功能支持) |  | 29 | 0004 | 4 |
| 1 | 设备电量低，已关机(固件需功能支持) |  | 30 | 0002 | 2 |
| 0 | 设备主动关机(固件需功能支持) |  | 31 | 0001 | 1 |

BDBDBDBD21010001000000ECFFBE65DA

**4.4设备信息及状态上报**

### 4.4.1软件版本和型号上传（0XBB）----以前设备使用可不解析

|  |  |
| --- | --- |
| Message | MSG\_VERSION\_DATA |
| Decription | 设备版本号和型号上传，Terminal=>Terminal Server |
| Firmware | -/- |
| Payload Length | 2+N bytes |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xBB | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 1 | UINT8 | Version\_len | 必选 | / | 软件版本号长度 |
| N | S8[n] |  | 必选 |  | 软件版本号 |
| 1 | UINT8 | Model\_len | 可选 |  | 型号长度 |
| N | S8[n] |  | 可选 |  | 型号 |
| 可扩展 |  |  |  |  | 可扩展 |
|  |  |  |  |  |  |

### 4.4.2 SIM卡的ICCID上传(0xF3)

|  |  |
| --- | --- |
| Message | LNK-LIN |
| Description | The terminal reports iccid to the server .when it logs on first |
| Firmware | 　 |
| Direction | Terminal => Terminal Server |
| Payload length | 10bytes |
| Message structure | Header | Message ID | Payload | Checksum |
| 0xBD 0xBD0xBD0xBD | 0xF3 | See below | CK\_sum |
| Byte Offset | Format | Name | Scale | Unit | Drscription |
| 10 | 10\*U8 | ICCID | 1 | - | ICCID number |

如果iccid是89861118236001639994

报文：BDBDBDBDF389861118236001639994CC

### 4.4.3状态参数上报(MSGID=0xA9)---可不用解析

|  |  |
| --- | --- |
| Message | MSG\_HRD\_DATA |
| Decription | Terminal => Server  |
| Firmware | -/- |
| Payload Length | 6 bytes |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xA9 | 见下方定义 | CK\_sum |

1. payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 1 | u8 | TypeCnt | -/- | -/- | 类型数 |
|  |  |  |  |  | （预留 00） |
| 1 | u8 | Type | -/- | -/- | 类型1 |
| 1 | U8 | NameLen | -/- | -/- | 名称1长度 |
| n | N\*u8 | Name | -/- | -/- | 名称 |
| 1 | u8 | Type | -/- | -/- | 类型2 |
| 1 | U8 | NameLen | -/- | -/- | 类型2长度 |
| n | N\*u8 | Name | -/- | -/- | 名称 |
|  |  |  |  |  |  |

开机上报一条

类型规定 屏幕 系统（MCU 模组 传感器 wifi 屏幕 蓝牙 ）

代码 mcu 00 模组 01 传感器 02 依次扩展

 名称长度

BDBDBDBDA9 01 00 00---mcu版本号

125732303050475F4534322E57472E4D4C3238C8

### 4.4.4设备状态(0xE9)（以前设备无）

终端连上服务器后，开机上报一笔，有频率有变化时上报一笔

|  |  |
| --- | --- |
| Message | MSG\_HTB\_UPL |
| Decription | 设备状态 |
| Firmware | -/- |
| Payload Length | 15 bytes  |
| Message structure | Hearer | Message ID | Payload | Checksum　 |
| token | 0xE9 | 见下方定义 | CK\_sum |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |

Payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 |  |  |  |  | 默认--00 |
| 2 |  |  |  |  | 后面报文长度 |
| 1 |  |  |  |  | 定位上报频率00---默认未修改01---有下行时间段：只上报当前时间段的上报频率 |
| 2 |  |  |  |  | 频率00分钟如:0A00-- 10分钟1小时-->60分钟 |
| 1 |  |  |  |  | 健康上报频率00---默认未修改01---有下行时间段：只上报当前时间段的上报频率 |
| 2 |  |  |  |  | 频率00分钟如:0A00-- 10分钟1小时-->60分钟  |

Eg:BDBDBDBDE9 010A00 010A00 33

表示10分钟定位上报频率，10分钟健康采样上报频率，有下行时间段

注：若设备无健康上报功能或无定位上报功能，则健康上报频率和定位上报频率两个值会保持一致，表示设备上报频率

### 4.4.5设备充电状态上传(0xC3)

注：以前设备无此上报，默认充电为关机状态，最新版本固件才有，此报文只有在下行指令开启：充电开机，才会上报

|  |  |
| --- | --- |
| Message | MSG\_HRD\_DATA |
| Decription | 设备充电状态上传，Terminal=>Terminal Server 上行 |
| Firmware | -/- |
| Payload Length | 5 bytes |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xC3 | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 0 | U8 | Status | / | / | 0开始，1结束，2 充电满 |
| 1 | U32 | Timestamp |  |  | 时间戳(补传时会在后面加时间戳) |

 Eg:

 BDBDBDBDC301DB4D2F668A 设备结束充电

 BDBDBDBDC300DB4D2F668A 设备开始充电

 BDBDBDBDC302DB4D2F668A 设备已充满电

**4.5 下行反馈上报**

### 4.5.1下行反馈(MSGID=0xC0)

|  |  |
| --- | --- |
| Message | MSG\_HRD\_DATA |
| Decription | Terminal =>Server |
| Firmware | -/- |
| Payload Length | 1 +n bytes |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xC0 | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 1 | U8 | length | -/- |  | Message ID长度 |
| N | n\*U8 | type | -/- |  | N个Message ID |
|  |  |  |  |  |  |

此指令用于下行指令的反馈 ，返回前面收到的Message ID（可以是多个Message ID集体返回）

Eg:bdbd bdbd c001 1720

 bdbdbdbd--header

C0--Message ID

01 --ID长度

Type:17 表示设备收到Message ID为17的报文

20--checksum

# **5.设置**

## 5.1下行

### 5.1.1设置周期上传（0x17）

平台设置1~4个时段下发给终端，终端收到以后，在规定的时间段内上传数据

|  |  |
| --- | --- |
| Message | MSG\_NB\_SLT |
| Decription | 　下行 |
| Firmware | -/- |
| Payload Length | 28 bytes  |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0x17 | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Byte offset**  |  **Format**  |  **Name**  | **Scale**  |  **Unit**  | **Decription** |  |
| 1 | u8 | 　enable | -/- | -/- | 是否启用 | 　时间段1 |
| 1 | U16 | Interval |  |  | 时间间隔（分钟） |
| 1 | u8 | time\_start\_h | 　 | 　 | -时 |
| 1 | u8 | time\_start\_m | 　 | 　 | -分 |
| 1 | u8 | time\_end\_h | 　 | 　 | -时 |
| 1 | u8 | time\_end\_m | 　 | 　 | -分 |
| 1 | u8 | 　enable | -/- | -/- | 是否启用 | 时间段2 |
| 1 | U16 | Interval |  |  | 时间间隔（分钟） |
| 1 | u8 | time\_start\_h | 　 | 　 | -时 |
| 1 | u8 | time\_start\_m | 　 | 　 | -分 |
| 1 | u8 | time\_end\_h | 　 | 　 | -时 |
| 1 | u8 | time\_end\_m | 　 | 　 | -分 |
| 1 | u8 | 　enable | -/- | -/- | 是否启用 | 时间段3 |
| 1 | U16 | Interval |  |  | 时间间隔（分钟） |
| 1 | u8 | time\_start\_h | 　 | 　 | -时 |
| 1 | u8 | time\_start\_m | 　 | 　 | -分 |
| 1 | u8 | time\_end\_h | 　 | 　 | -时 |
| 1 | u8 | time\_end\_m | 　 | 　 | -分 |
| 1 | u8 | 　enable | -/- | -/- | 是否启用 | 时间段4 |
| 1 | U16 | Interval |  |  | 时间间隔（分钟） |
| 1 | u8 | time\_start\_h | 　 | 　 | -时 |
| 1 | u8 | time\_start\_m | 　 | 　 | -分 |
| 1 | u8 | time\_end\_h | 　 | 　 | -时 |
| 1 | u8 | time\_end\_m | 　 | 　 | -分 |

例如：

bd bd bd bd 17 01 03 00 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dd

0点到19点，每隔3分钟定位一次，时间段外按默认上报频率上报

BDBDBDBD17010A000000173B00000000000000000000000000000000000000000097

0-23：59（全天），每1隔10分钟定位一次

注：G805G通用版本是短链接设备，下行指令在设备上报的时候设备才接收下行指令

### 5.1.2设置-综合（见详细说明--重要下行）（0XCE）

|  |  |
| --- | --- |
| Message | MSG\_HRD\_DATA |
| Decription | 设置指令，Server => Terminal 下行 |
| Firmware | -/- |
| Payload Length | 4+n bytes |
| Message structure | Hearer | Message ID | Payload | Checksum |
| token | 0xCE | 见下方定义 | CK\_sum |

payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 0 | u8 | Type | -/- | -/- | 类型见下面 |
| 1 | u8 | Valid | -/- | -/- | 临时有效，一直有效 |
| 2 | U16 | Len | -/- | -/- | 后面的指令长度 |
| 4 | n |  | -/- | -/- | 正文 |
|  |  |  |  |  |  |

Type 01 定位 02 健康 03 报警（预留暂无） 04 本地存储（预留暂无）05蓝牙广播开关 06定位和健康数据上报开关 07 跌落报警开关 08 停留报警开关 后面也可扩展

Valid 00 一直有效 01 此次生效 02 关闭

Length 后面正文指令长度

正文指 ：020301

Type

01 定位功能 正文只能是 基本类01 --gps 02 --wifi 03 --蓝牙信标 04 – LBS基站 05 -- 125k 及以后扩展的基本类正文可以是 01或者010203 的组合 默认4g设备只有wifi，gps，蓝牙信标

如 010203时 表示用gps wifi 蓝牙信标;

示例：wifi定位优先（wifi>蓝牙>gps）：BDBDBDBDCE0100030002030133

gps定位优先（gps>wifi>蓝牙）： BDBDBDBDCE0100030001020333

蓝牙定位优先（需部署蓝牙信标，蓝牙>wifi>gps）:BDBDBDBDCE0100030003020133、

分析示例：wifi定位优先（wifi>蓝牙>gps）：BDBDBDBD CE 01 00 0300 020301 33

Type:01； Valid:00；length:0300;type:020301;checksum:33

05 蓝牙广播开关

00---开启 eg:BDBDBDBDCE0700000093

02---关闭 eg:BDBDBDBDCE0702000093

07 跌落报警开关

00---开启 eg:BDBDBDBDCE0700000093

02---关闭 eg:BDBDBDBDCE0702000093

16 下行是否能使用按键关机

00---开启 eg:BDBDBDBDCE1600000093

02---关闭 eg:BDBDBDBDCE1602000093

18 休眠功能开关

 00---开启，静止一段时间后进入休眠，不工作 eg:BDBDBDBDCE1800000093

02---关闭 静止状态或充电状态，也正常工作 eg:BDBDBDBDCE1802000093

19 按键触发sos报警开关

 00---开启 eg:BDBDBDBDCE1900000093

02---关闭 eg:BDBDBDBDCE1902000093

21 充电开机还是关机状态,非充电状态下发
00---开启 充电工作 eg:BDBDBDBDCE2100000093 (充电开机状态)
02---关闭 充电关机 eg:BDBDBDBDCE2102000093(充电关机状态)

22 长短连接模式切换

 00---长连接模式 eg:BDBDBDBDCE2200000093

 02---短连接模式，默认为短连接 eg:BDBDBDBDCE2202000093

注：短链接设备，下行指令在设备上报的时候设备才接收下行指令，收到后在下一个上报周期生效

### 5.1.3域名设置(0xC3)（TCP专用-以前设备无此功能）

|  |  |
| --- | --- |
| Message | MSG\_SET\_DOMAIN |
| Decription | 域名设置 下行  |
| Firmware | -/- |
| Payload Length | 52 bytes |
| Message structure | Hearer | Message ID | Payload | Checksum　 |
| token | 0XC3 | 见下方定义 | CK\_sum |

 payload contents

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte offset | Format | Name | Scale | Unit | Decription |
| 1 | U8 | Type |  |  | 下发类型 |
| 2 | U16 | Port |  |  | 端口号（2个字节） |
| 1 | U8 | Length |  |  | 长度 |
| N | U8 | Domainname |  |  | Type =1 IPv4 专用 Type=2 IPV6专用（ascii 编码）--暂不支持Type =3 域名专用（ascii 编码） |

说明 ：type =1 4字节 0F:12:34:4A

type=2 IPv6

Eg：BDBDBDBDC302792204 33

BDBDBDBD C3 01 7922 04 76B2B8DB 33

01 type=1 ipv4

1. --转大端--2279 --》转10进制 端口：8825

76B2B8DB --》转10进制118.178.184.219

33 checksum

注：G805G通用版本是短链接设备，下行指令在设备上报的时候设备才接收下行指令，下行指令修改ip和端口指向其他服务器后，设备将在其他服务器通信