

---

# 通讯协议

通讯协议	1
1 格式说明	3
1.1 TCP 格式	3
1.1.1 下行数据	3
1.1.2 上行数据	3
1.2 UDP 格式	3
1.3 应用数据	4
2 无线升级命令	4
2.1 更新请求，上行命令为 0x5501	4
2.2 更新应答，下行命令为 0xDD01	4
2.3 终端对下行更新应答的应答。上行命令为 0x5502	5
2.4 中心下发窗口数据，下行命令 0xDD03	5
2.5 终端对窗口数据的应答，上行命令 0x5503	5
2.6 查询终端接收情况，下行命令 0xDD04	5
2.7 终端应答接收情况，上行命令 0x5504	6
2.8 停止此次升级。下行命令 0xDD05	6
2.9 停止升级应答，上行命令 0x5505	6
2.10 心跳命令，上行命令 0x55FF	6
2.11 心跳命令应答，下行命令 0xDDFF	6
3 无线升级配置	6

---

3.1 中心查询终端软件版本，下行命令 0xD035.....	6
3.2 终端应答中心查询软件版本，上行命令 0x5035.....	7
3.3 中心配置无线下载，下行命令 0xD030.....	7
3.4 终端应答无线下载配置，上行命令 0x5030.....	7
4 远程升级流程图.....	8
4.1 触发远程升级.....	8
4.2 远程升级.....	9
4.3 查询升级情况.....	9

---

文档版本	时间	作者	说明
0001	2011.12.31	林兴发	远程升级协议
0002	2012.12.20	林兴发	LED 控制卡在注册包中 增加 IMEI 号
0003	2014.3.28	林兴发	增加 MD5 校验
0004	2014.4.14	郑启枣	注册包增加扩展 ID
0004	2015.02.02	郑启枣	增加 DD01 报文注释, 应用程序长度

---

## 1 格式说明

下行数据：指中心下发给终端的数据

上行数据：指终端上发给终端的数据

### 1.1 TCP 格式

#### 1.1.1 下行数据

起始	版本 高	版本 低	应用 数据 长度 高	应用 数据 长度 低	应用 数据	数据 校验	结束 字节
1 字 节	1 字 节	1 字 节	1 字 节	1 字 节	根据 数据 长度	1 字 节	1 字 节

1. 起始字节为: 0x7E
2. 版本: 两个字节自定义, 版本 0002
3. 应用数据长度: 数据内容的长度
4. 应用数据: 收到的数据内容。
5. 数据校验: 收到的数据 (除起始, 结束与本身校验字节) 累加和。
6. 结束字节: 0x7E。
7. 除起始字节与结束字节, 在其它字段里出现 7E 转义为 7D 01, 7D 转义为 7D 02

#### 1.1.2 上行数据

起始	版本 高	版本 低	应用 数据 长度 高	应用 数据 长度 低	应用 数据	数据 校验	结束 字节
----	---------	---------	---------------------	---------------------	----------	----------	----------

1 字节	根据数据长度	1 字节	1 字节				
------	------	------	------	------	--------	------	------

## 1.2 UDP 格式

同 TCP 格式

## 1.3 应用数据

ID 号	命令字节	数据长度	数据
4 个字节	2	2	数据内容

ID 号： 表示设备的表示

数据长度： 表示数据内容长度

## 2 无线升级命令

本协议是窗口方式升级程序，所以中心在更新请求的应答中下发的窗口大小，中心必须保证每次下发的窗口都是这个窗口大小。

### 2.1 更新请求，上行命令为 0x5501

登录就发送这条命令，到一顶次数就认为登录失败。

字段	长度	说明
数据内容长度	2	以下参数的总长度
应用程序类型	1	0 表示 APP 程序，1 表示 BOOT 程序
断点	4	程序已经更新的字节数
应答方式	1	0x00 表示一一应答。0x01 表示窗口应答
窗口最大帧数	1	一个窗口最大帧数。不超过 16

需要更新的版本	40	需要更新版本，不够 40 个字节补空格
设备版本长度	1	设备版本长度
设备版本	根据设备版本长度	设备的当前版本号
MD5	32	暂定 32 个字节，如果断点为 0 就不需要判断。
扩展 ID	16	不足 16 个字节请补零

## 2.2 更新应答，下行命令为 0xDD01

字段	长度	说明
数据内容长度	2	以下参数的总长度
应答类型	1	01 表示需要更新 02 表示无需更新 03 表示找不到更新的版本号 04 表示断点错误 05 表示 MD5 出错，程序重新开始
需要更新后带如下字段		上个字节 01 或 05
窗口的帧号	2	窗口的起始帧号。(从 0 开始)
窗口的大小	1	最大 16 个帧数据位一个窗口，但是由于终端 RAM 的限制，本这次协议就取 4 个帧数据。
窗口每一帧的最大长度	2	取窗口 4 帧中的最大程序长度。
程序总长度	4	应用程序的总长度。 (注：长度=升级文件长度+1，其中 1 表示为一个字节累加和检验值)
MD5	32	暂定 32 个字节

### 2.3 终端对下行更新应答的应答。上行命令为 0x5502

字段	长度	说明
数据内容长度	2	以下参数的总长度，即长度为 1
应答类型	1	00 表示失败(中心收到次命令后，下发停止此次升级)  01 表示成功

### 2.4 中心下发窗口数据，下行命令 0XDD03

程序的最后一帧的最后一个字节请带所有应用程序的累加和的校验。

字段	长度	说明
数据内容长度	2	以下参数的总长度
窗口的帧号	2	当前数据对应的窗口帧号
程序内容	数据内容长度减去窗口帧号	要升级的程序内容。如果不是最后一帧数据（最后一帧长度取实际长度），取 1024 字节。

### 2.5 终端对窗口数据的应答，上行命令 0x5503

中心收到应答，且应答内容为 00H, 02H 或 03，中心要下发对应的停止此次升级的命令。

字段	长度	说明
数据内容长度	2	以下参数的总长度
应答类型	1	00H 表示程序校验失败  01H 表示成功  02H 表示写 FLASH 出问题，系统不升级。  03H 表示升级成功。

		04H 表示需要重发这个窗口数据
窗口的帧号	2	窗口起始帧号

## 2.6 查询终端接收情况，下行命令 0xDD04

字段	长度	说明
数据内容长度	2	无参数，长度为 00

## 2.7 终端应答接收情况，上行命令 0x5504

应答与 0x5503 一样。

字段	长度	说明
数据内容长度	2	以下参数的总长度
窗口的帧号	2	窗口起始帧号

## 2.8 停止此次升级。下行命令 0xDD05

字段	长度	说明
数据长度	2	无参数，所以长度为 01
停止原因	1	01H 表示升级成功 02H 表示 FLASH 出问题 03H 表示其他原因停止

## 2.9 停止升级应答，上行命令 0x5505

字段	长度	说明
数据长度	2	无参数，所以长度为 00

## 2.10 心跳命令，上行命令 0x55FF

字段	长度	说明
数据长度	2	无参数，所以长度为 00

## 2.11 心跳命令应答，下行命令 0xDDFF

字段	长度	说明
数据长度	2	无参数，所以长度为 00

# 3 无线升级配置

## 3.1 中心查询终端软件版本，下行命令 0xD035

字段	长度(字节)	说明
数据内容长度	2	无参数，所以长度为 00

## 3.2 终端应答中心查询软件版本，上行命令 0x5035

字段	长度	字段描述
数据长度 2	2	以下字段长度，共 80 个字节
APP 版本	40	终端 APP 程序的版本号，不够字节数补空格
BOOT 版本	40	终端 BOOT 程序的版本号，不够字节数补空格

## 3.3 中心配置无线下载，下行命令 0xD030

字段	长度	字段描述
数据长度 2	2	以下参数的总长度，共 92 字节

属性	1	<p>X111X111 (X 为保留位)</p> <p>Bit7, bit3: 保留</p> <p>bit6 : 1. 压缩模式下载; 0. 非压缩模式下载</p> <p>bit5 : 1. 立即下载; 0. 不立即下载 (由时间限制)</p> <p>bit4 : 1. 擦除参数区; 0. 不擦除参数区</p> <p>bit2~bit0: 组合如下:</p> <p style="padding-left: 40px;">0x00 应用程序下载</p> <p style="padding-left: 40px;">0x01 BOOT 程序下载</p> <p>其他组合保留待扩展</p>
模式	1	0x00 TCP, 0x01 UDP
应答方式	1	0x00 表示一一应答。0x01 表示窗口应答
窗口最大帧数	1	一个窗口最大帧数。最大 16, 此次协议不超过 4
APN	20	(暂无此功能) 字符串不够字节数请补空格, 比如: " cmnet"
IP	20	字符串不够字节数请补空格, 比如: " 119.75.217.56"
PROT	5	字符串不够字节数请补空格, 比如: " 20"
新版本长度	1	传输格式 HEX 取值范围 $1 \leq N \leq 40$
NEW_VE R	40	版本字段, ascii 格式, 不足填充格

时间范围	4	<p>(暂无此功能): [时间 1] + [时间 2], 由 bit5 控制</p> <p>含义: 设备在此时间段内可申请下载程序</p> <p>字段: H,M , 采用 24 小时制</p> <p>传输格式: hex 时间格式: 北京时间</p> <p>取值范围: 00:00 ~~23:59</p>
------	---	---

### 3.4 终端应答无线下载配置, 上行命令 0x5030

字段	长度	字段描述
应答类型	1	应答类型: 00H 失败 01H 成功 02H 版本不是最新

## 4 远程升级流程图

### 4.1 触发远程升级

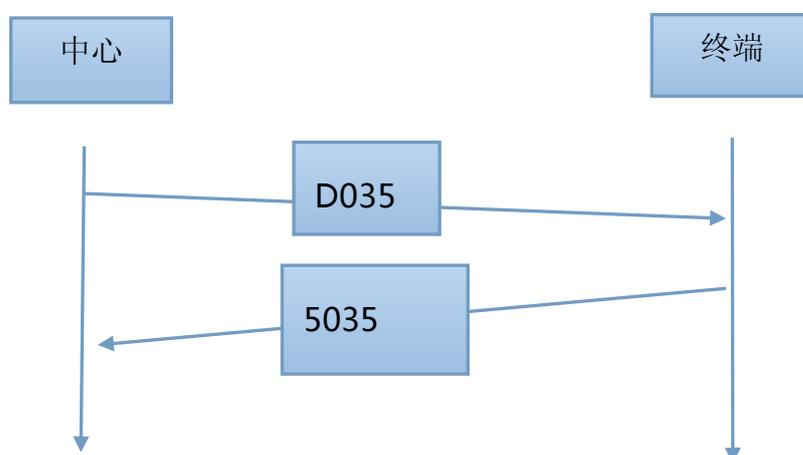


图 4-1

## 4.2 远程升级

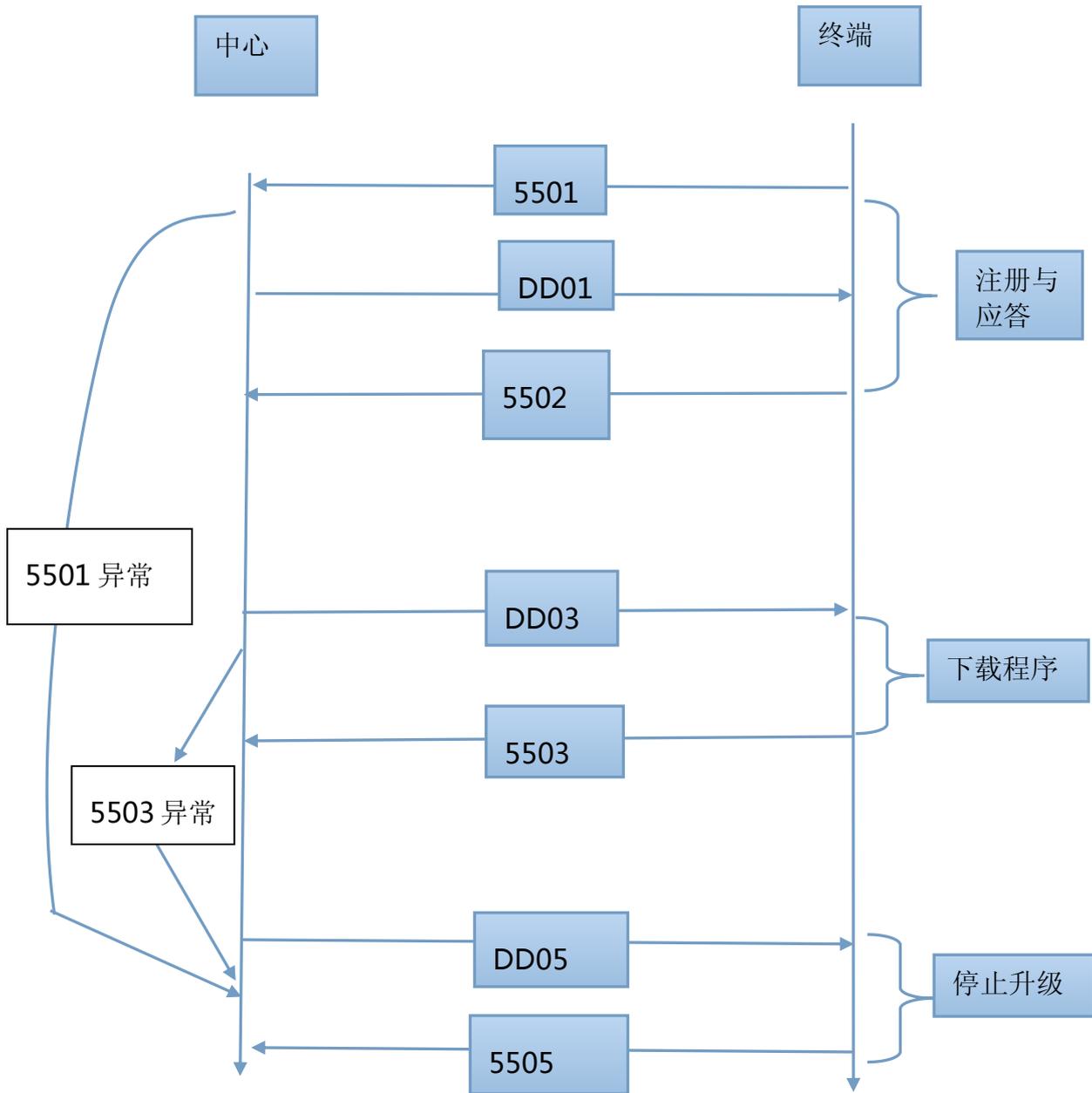


图 4-2

---

### 4.3 查询升级情况

