

FR801xH OTA 升级流程

前提：蓝牙连接上

注：1、x 为任意值

- 2、image_size 为 FR801xH 软件大小，可在软件中设置，如 0x19000 为 100K
- 3、packet_len 为传升级数据每一包的长度，包长根据交互 MTU 的长度来定
- 4、通讯 UUID:
Service UUID:
0x02,0xF0,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xFE,0x00
TX(APP->DEV)
0x02,0xF0,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xFF,0x01
RX(DEV->APP)
0x02,0xF0,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xFF,0x02
- 5、通讯命令格式:

APP->DEV

cmd head		操作内容
Opcode(1 字节)	len(2 字节)	根据实际命令定义
命令字,对应不同的指令	操作内容中所有数据的长度	

DEV->APP

Rsp head			操作内容
结果(1 字节)	opcode(1 字节)	len(2 字节)	根据实际命令来定义
0: ok; 1: fail	对应 app 下发的命令	操作内容中所有数据的长度	

- 6、命令字定义(下面没有写出来的命令定义可以不用关注):
 - 0x01: 获取设备当前升级程序的 flash 起始地址，App 需要记录下来，ota 升级是 A/B 乒乓式升级，A 区域是从 0 地址起始的区域，B 区域是从 image_size 起始的区域 (image_size 是设备端软件根据实际需要大小设定，比如实际软件大小是 90K，预留 10K 空间，所以设置 iamge_size 大小为 100K，则 B 区域是从 100K-200K 的 flash 空间);
 - 0x02: 获取设备当前的软件版本号，升级前可以读取，设备端软件可以将该版本号配置成发布的软件版本号，便于 APP 获取对比;
 - 0x03: 擦除命令，每次擦除 4K(0x1000)空间，app 根据实际软件大小，依次累加地址擦除，直至需要升级的 bin 文件大小的空间被擦除完;
 - 0x05: 写数据命令，该命令即用于 bin 文件数据传输，每次传输的长度由 APP 根据实际连接交互的 mtu 长度来定。每传输一包数据地址偏移累加上传输的数据长度，用于下一次写命令传输，直至升级的 bin 文件完全传输完成;
 - 0x09: 重启指令，bin 文件传输完成之后，发送该命令通知设备升级完成并重启，命令附带 bin 文件去掉开始的 256 字节头数据之后的 CRC 校验值，设备收到该命令之后先会做 CRC 校验，之后再重启;

步骤 1: 手机 APP 获取设备软件版本号, 按需要选择是否发送该命令

App 发送指令至设备, 命令 0x02

cmd head		操作内容
opcode(1 字节)	len(2 字节)	无实际意义(4 字节)
0x02	0x0004	x(任意值)

设备回复指令至 App

Rsp head			操作内容
结果(1 字节)	opcode(1 字节)	len(2 字节)	Version(软件版本号)
0: ok; 1: fail	0x02	0x0004	如 0x00000001

步骤 2: 手机 APP 获取设备当前升级程序的存储起始地址

App 发送指令至设备, 命令 0x01

cmd head		操作内容
opcode(1 字节)	len(2 字节)	无实际意义(4 字节)
0x01	0x0004	x(任意值)

设备回复指令至 App

Rsp head			操作内容
结果(1 字节)	opcode(1 字节)	len(2 字节)	base_addr(4 字节)
0: ok; 1: fail	0x01	0x0004	0 或 image_size, 升级文件写入 flash 的 起始地址

步骤 3: APP 发命令让设备擦除升级所需要的地址空间

App 发送指令至设备, 命令 0x03

cmd head		操作内容
opcode(1 字节)	len(2 字节)	base_addr(4 字节)
0x03	0x0004	从起始地址开始(0 或者 image_size), 每次地址都加 4096,直到 bin 文件所需的 空间都被擦除。

设备回复指令至 App

Rsp head			操作内容
结果(1 字节)	opcode(1 字节)	len(2 字节)	base_addr(4 字节)
0: ok; 1: fail	0x03	0x0004	APP 命令里的擦除地址

注意：循环擦除步骤，直到要烧录文件所需的空间地址全部被擦除

步骤 4：传升级数据

App 发送指令至设备，命令 0x05

cmd head		操作内容		
opcode(1 字节)	len(2 字节)	base_addr(4 字节)	len(2 字节)	data
0x05	操作内容里面数据的总长度 packet_len+6	填写入的地址，从 0x0 或 image_size 开始，每次写 packet_len 个字节，注意地址每次加 packet_len	packet_len 由 app 根据实际连接交互的 mtu 大小来定	packet_len 个长度的升级文件的数据

设备回复指令至 App

Rsp head			操作内容	
结果(1 字节)	opcode(1 字节)	len(2 字节)	base_addr(4 字节)	len(2 字节)
0: ok; 1: fail	0x05	0x0006	APP 命令里的写数据的地址	APP 命令里写入数据的长度(packet_len)

注意：循环写数据步骤，直到要烧录文件的数据全部被写入

步骤 5：升级结束，重启

App 发送指令至设备，命令 0x09

cmd head		操作内容	
opcode(1 字节)	len(2 字节)	bin_length(4 字节)	CRC(4 字节)
0x09	0x0008	升级文件的实际长度	升级文件去掉头部的 256bytes 之后的 CRC 校验值

设备收到指令后做 CRC 校验并重启!

说明:

1: 擦除命令 0x03, ble 的回复包里, “收到 cmd 里的擦除地址”, 指的是 app 传过来的擦除地址, 这里原样返回;

2: 擦除命令 0x03 的结束条件是 app 端去判断升级文件的大小, 然后以这个文件大小作为阈值判断什么时候结束;

3: bin 文件的 0x58 字节开始, 4 个字节是{0x51, 0x52, 0x52, 0x51}, 可用于判断升级文件是有效的, 升级之前 app 可以检查一下;

4: 2 字节和 4 字节均为小端模式, 注意字节顺序;

5: 以上升级步骤适合上海富芮坤蓝牙;