**MQTT升级流程**

**1.Flash分区**

.MCU分为三个区，BOOT区(32K)，APP区(112K)和Backup区(108K)，Flag区(4K)

0x0803F000

0x08024000

0x08008000

0x08000000

BOOT区

APP区

Backup区

Flag区

**2.升级流程**

升级主题：/device id/update/信息机编号

版本主题：/device id/version/信息机编号

响应主题：/device id/ack/信息机编号

1. 设备端订阅升级主题，读取当前版本信息，向版本主题上报版本信息；

格式：1Byte

1. 需要升级时，服务端往该升级主题发送第一包数据

格式：1Byte(数据包序号)+1Byte(新固件版本号)+2Byte(固件总字节数)；

1. 设备端接收到第一包数据，成功擦写相应的Backup区大小后，向响应主题

上报响应信息

格式：1Byte 成功 上报‘c’ 失败上报 ‘e’；

1. 服务端将固件拆分为每包1K/2K/4K大小，向升级主题下发消息，最后一包不足1K/2K/4K时，直接下发；

格式：1Byte(数据包序号)+1K/2K/4K固件数据；

1. 设备端依次接收数据，同时写入Backup区，向响应主题上报响应信息

格式：1Byte 成功上报当前第几包数据 失败上报 ‘e’；

1. 设备端判断写入Flash的固件长度是否等于服务端下发的固件长度？并向响应主题上报响应信息

格式：1Byte 相等上报‘c’ 不等上报 ‘e’；

1. 相等时写入升级标志位，和固件版本信息，并向响应主题上报响应信息

格式：1Byte 成功上报‘c’ 失败上报 ‘e’；

1. 设备端重启，进入boot,判断升级标志位，满足，开始更新app区，否则执行旧APP
2. 设备端擦除app区代码，将Backup区拷贝到app区
3. 跳转到新app区，清除升级标位，执行用户程序

**备注：**

异常情况：

1. 下载中断电,由于未完成升级，没有写入升级标志位，再次上电时进入Boot区，会执行旧APP，不会更新APP。
2. 进入Boot,开始更新APP区时断电。由于未成功跳转到新APP区，没有清除升级标注位，再次上电时，会重新更新APP区，（Baukup区的代码没有擦除）

服务端功能要求：

1. 拆分固件数据，分包发送

格式：1Byte(数据包序号)+1Byte(新固件版本号)+2Byte(固件总字节数)；

1Byte(数据包序号)+1K/2K/4K固件数据

1. 当收到设备端返回的‘e’信息时，从第一包数据开始重新发送。