

RTL8762E OTA User Guide

V1.0

2022/06/02

修订历史 (Revision History)

日期	版本	修改	作者	Reviewer
2021/06/22	V0.1	Draft version	Grace	
2022/06/02	V1.0	First release version	Arthur	Grace

Realtek Confidential

目 录

修订历史 (Revision History)	2
目 录	3
表目录	5
图目录	6
1 概述	7
1.1 功能介绍	7
1.2 相关重点内容	7
2 Flash 布局介绍	8
3 Image 格式	10
3.1 OTA Header Image 格式	10
3.2 其他 Image 格式	13
4 OTA 打包格式及工具	16
4.1 支持 Bank 切换	16
4.1.1 Flash 布局	16
4.1.2 打包工具使用步骤——切换 bank	18
4.2 不支持 Bank 切换	20
4.2.1 Flash 布局	20
4.2.2 打包工具使用步骤——不切换 bank	21
5 OTA 协议	23
5.1 DFU Service	23
5.2 OTA Service	25
5.2.1 OTA CMD	25
5.2.2 Device Mac	26
5.2.3 Patch Version	26
5.2.4 APP Version	26
5.2.5 Patch Extension Version	27
5.2.6 Test Mode	27
5.2.7 Device Info	27

5.2.8 Image Counter	29
5.2.9 Image Version.....	29
5.3 OTA 流程.....	31
5.3.1 多文件更新注意事项	33
6 参考文献.....	34

Realtek Confidential

表目录

表 2-1 Flash 空间分布和功能说明	8
表 2-2 Flash Segmentation	9
表 3-1 Fields of OTA Header.....	12
表 3-2 Fields of Image Header	13
表 4-1 Bank 切换 flash 布局示例.....	17
表 4-2 Bank 不切换 flash 布局示例.....	20
表 5-1 DFU opcode	24
表 5-2 OTA Characteristic	25
表 5-3 OTA CMD characteristics	26
表 5-4 Device Mac characteristics.....	26
表 5-5 Patch Version characteristic for RTL8762C/RTL8762E	26
表 5-6 APP Version characteristic for RTL8762C/RTL8762E	26
表 5-7 Patch Extension Version characteristic.....	27
表 5-8 Test Mode characteristics	27
表 5-9 Device info characteristic for RTL8762C/RTL8762E.....	27
表 5-10 Device info Format For RTL8762C/RTL8762E (OTA version = 1)	28
表 5-11 Image Counter Characteristics.....	29
表 5-12 Image Version characteristics	30

图目录

图 2-1 Flash 布局	8
图 2-2 OTA Bank 布局.....	9
图 3-1 OTA Header 结构.....	11
图 3-2 Image Header 结构	13
图 4-1 设置 Flash 布局并生成 OTA Header	18
图 4-2 编译 APP 文件.....	18
图 4-3 打包生成 Pack	19
图 4-4 配置 Flash Layout 并生成 OTA Header0.....	21
图 4-5 Pack OTA images with MP Pack Tool.....	22
图 5-1 OTA 不带 buffer check 流程	31
图 5-2 OTA buffer check 流程	32

1 概述

1.1 功能介绍

本文中 OTA（Over The Air）是指通过蓝牙的传输，对 RTL8762E 系列 Flash 中运行的 image 和 data 进行空中升级的技术。

1.2 相关重点内容

1. Flash 布局介绍
2. Image 格式和布局
3. OTA 打包格式及工具使用
4. OTA 协议

Realtek Confidential

2 Flash 布局介绍

RTL8762E 的 Flash 布局如图 2-1 所示，由 OEM Config，OTA Bank 0，OTA Bank 1，FLASH Transport Layer(FTL)，OTA TMP 以及 APP defined section 组成，访问起始地址为 0x800000。以上为简要说明，详细介绍请参考文档《RTL8762E Memory User Guide》第 5 章。

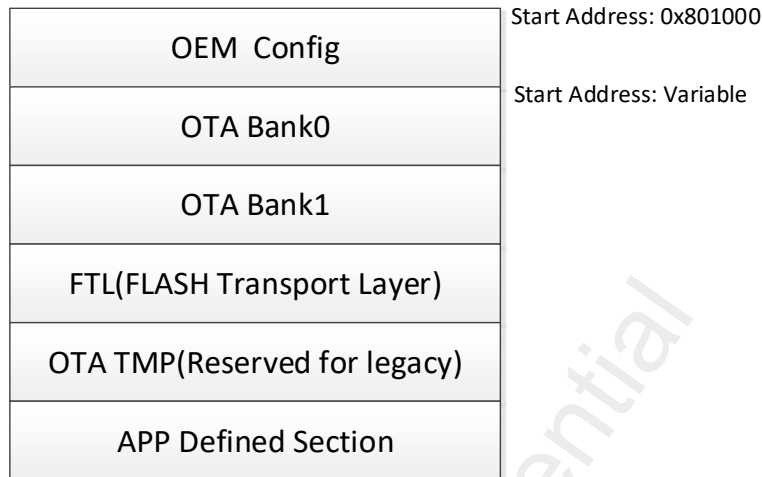


图 2-1 Flash 布局

Flash 中各个部分空间分布和功能说明如表 2-1 所示。

表 2-1 Flash 空间分布和功能说明

Memory Segment	Starting Address	Size(Bytes)	Functions
OEM Config	0x801000	0x1000	config 信息存储区域，包括蓝牙地址，AES Key，和用户可修改的 Flash 布局等内容。
OTA Bank0	可变 (OEM Config 里定义)	可变长度 (OEM Config 里定义)	不切换 Bank 方案，为数据和代码运行区，包括 OTA Header, Secure boot, Patch, Upperstack, APP, APP Data1, APP Data2, APP Data3, APP Data4, APP Data5, APP Data6。此 OTA 备份区为 OTA_TMP。 切换 Bank 模式，OTA Bank0 和 OTA Bank1 互为备份区。
OTA Bank1	可变	可变长度	切换 Bank 模式才存在，功能与大小和 Bank0 保持一致。
FTL	可变	可变长度	以逻辑地址访问 flash 的软件技术，可以按照 word 进行任意地址读写，用户无需关注 flash 物理层操作，同时也做到了损耗均衡。
OTA_TMP	可变	可变长度	不切换 Bank 模式下，作为 OTA 备份区使用，大小必须不小于 OTA Bank0 最大的 image 大小。
APP Defined Section	可变	可变长度	Flash 剩余未划分区域，用户可以自由使用。不受本文涉及的 OTA 方案的管控。

OTA bank 的布局如图 2-2 所示，各段描述说明如表 2-2 所示。

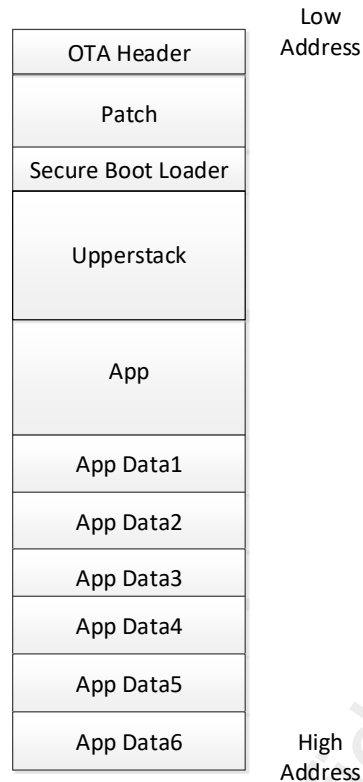


图 2-2 OTA Bank 布局

表 2-2 Flash Segmentation

Memory Segment	Starting Address	Size	Functions
OTA Header	由 OEM Config 定义决定	4KB	存放 OTA Header 的版本，BANK 中存在 image 的起始地址和大小
Secure Boot Loader	由 OTA Header 定义决定	Variable	启动过程中对代码安全级别检查的代码
Patch	由 OTA Header 定义决定	Variable	对 rom 中协议栈，系统的优化和扩展代码
Upperstack	由 OTA Header 定义决定	Variable	BLE HCI 以上协议栈部分
App	由 OTA Header 定义决定	Variable	开发方案的运行代码或者同时集成了 BLE HCI 以上协议栈部分
App Data1	由 OTA Header 定义决定	Variable	开发方案中使用的数据区
App Data2	由 OTA Header 定义决定	Variable	开发方案中使用的数据区
App Data3	由 OTA Header 定义决定	Variable	开发方案中使用的数据区
App Data4	由 OTA Header 定义决定	Variable	开发方案中使用的数据区
App Data5	由 OTA Header 定义决定	Variable	开发方案中使用的数据区
App Data6	由 OTA Header 定义决定	Variable	开发方案中使用的数据区

3 Image 格式

所有可能需要升级的 Image（OTA Header, Secure boot, Patch, Upperstack, APP, APP Data1, APP Data2, APP Data3, APP Data4, APP Data5, APP Data6）都是由一个 1KB 大小的 header 和 payload 部分组成。其中 OTA Header image 和其他 image 中的 header 部分略有差异。此文中除了 OTA Header image 外，其他所有可升级的 image 的 header 为 Image Header，下文分别说明。

3.1 OTA Header Image 格式

OTA Header image 是由 1KB 的 header 和 3KB 的 dummy payload 组成，OTA Header 由 MPTool 生成。其中 OTA Header Image 中的 header 各字段定义如[错误!未找到引用源。](#)所示。

Realtek Confidential

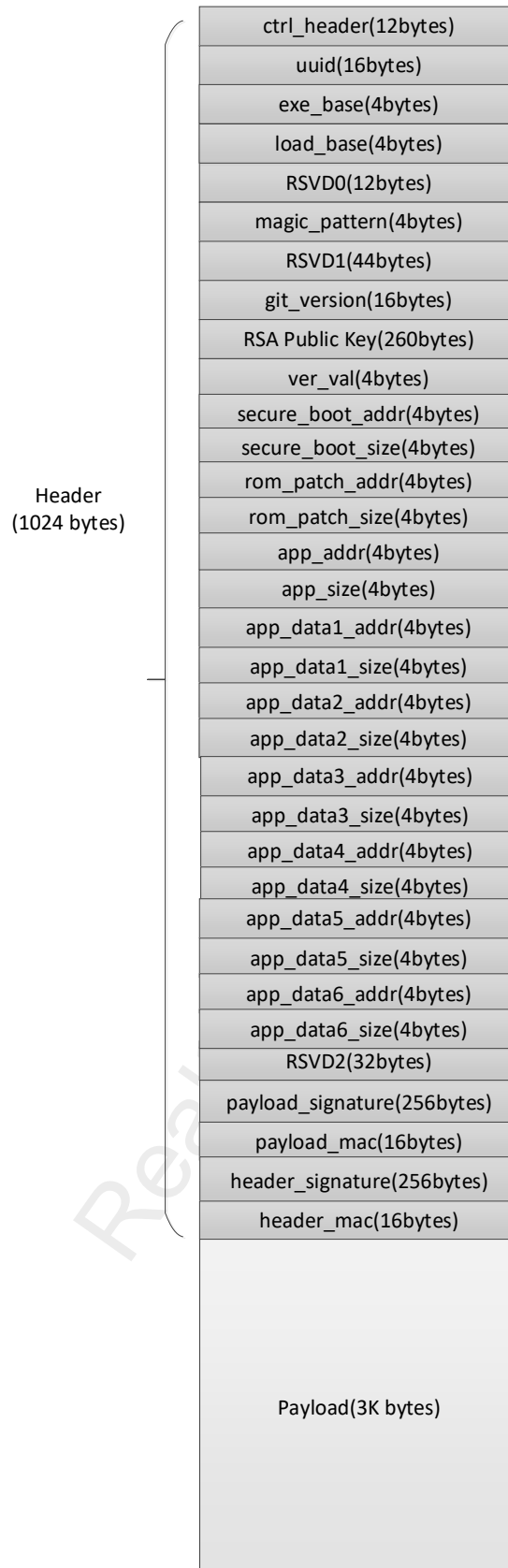


图 3-1 OTA Header 结构

OTA Header 中 header 部分与 OTA 相关字段含义如错误!书签自引用无效。所示。

表 3-1 Fields of OTA Header

Fields	Length(Byte)	Functions
ctrl_header	12	OTA Header 的控制信息
secure_boot_addr	4	Secure boot image 的起始地址
secure_boot_size	4	Secure boot image 的大小
rom_patch_addr	4	Rom patch image 的起始地址
rom_patch_size	4	Rom patch image 的大小
app_addr	4	App image 的起始地址
app_size	4	App image 的大小
app_data1_addr	4	App data1 的起始地址
app_data1_size	4	App data1 的大小
app_data2_addr	4	App data2 的起始地址
app_data2_size	4	App data2 的大小
app_data3_addr	4	App data3 的起始地址
app_data3_size	4	App data3 的大小
app_data4_addr	4	App data4 的起始地址
app_data4_size	4	App data4 的大小
app_data5_addr	4	App data5 的起始地址
app_data5_size	4	App data5 的大小
app_data6_addr	4	App data6 的起始地址
app_data6_size	4	App data6 的大小

3.2 其他 Image 格式

Patch、App 以及所有 App data 的 image 是由 1KB 的 image header 和对应的 payload 组成。Patch 和 App 的 image header 由编译链接生成，App data 的 image header 由 APP DATA 工具添加生成。其中 Image header 各字段定义如图 3-2 所示。

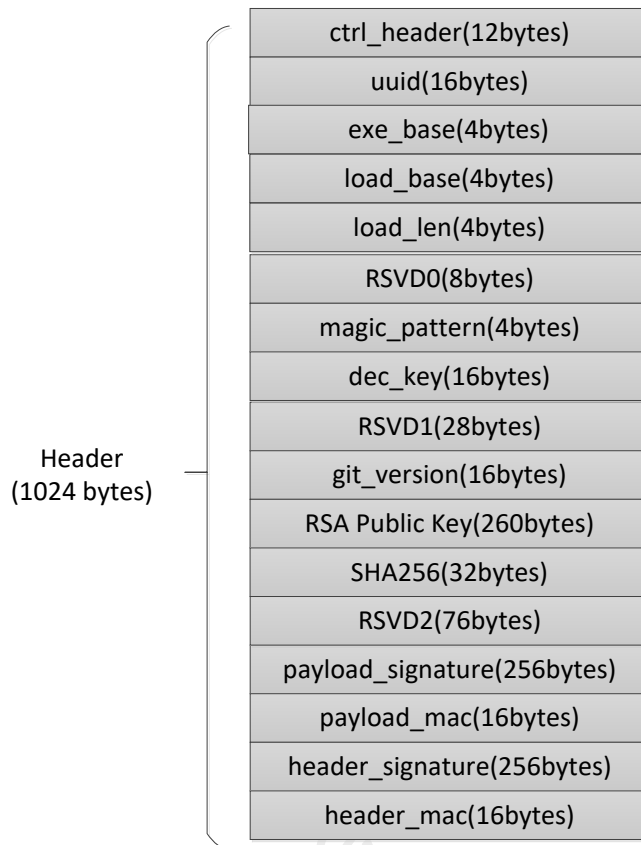


图 3-2 Image Header 结构

其中与 OTA 相关的字段表示的含义如表 3-2 所示。

表 3-2 Fields of Image Header

Fields	Length(Byte)	Functions
ctrl_header	12	Image Header 的控制信息
git_version	16	版本管理的信息字段

Image Header 中 **ctrl_header format** 如下：

```

1. typedef struct _IMG_CTRL_HEADER_FORMAT
2. {
3.     uint8_t ic_type;
4.     uint8_t secure_version;
5.     union

```

```

6.  {
7.    uint16_t value;
8.    struct
9.    {
10.        uint16_t xip: 1; // payload is executed on flash
11.        uint16_t enc: 1; // all the payload is encrypted
12.        uint16_t load_when_boot: 1; // load image when boot
13.        uint16_t enc_load: 1; // encrypt load part or not
14.        uint16_t enc_key_select: 3; // referenced to ENC_KEY_SELECT
15.        uint16_t not_ready : 1; //for copy image in ota
16.        uint16_t not_obsolete : 1; //for copy image in ota
17.        uint16_t integrity_check_en_in_boot : 1; // enable image integrity check in boot flow
18.        uint16_t rsvd: 6;
19.    };
20. } ctrl_flag;
21. uint16_t image_id;
22. uint16_t crc16;
23. uint32_t payload_len;
24. } T_IMG_CTRL_HEADER_FORMAT;

```

ic_type 表示 IC type，RTL8762E 的 ic type 值为 12，secure_version 表示启动安全检查 image 的版本。

image_id 标识不同的 image 类型，枚举如下，其中 SCCD，OCCD，FactoryCode 是不可以 OTA 升级的。

```

1. typedef enum
2. {
3.     SCCD      = 0x278D,
4.     OCCD      = 0x278E,
5.     FactoryCode = 0x278F,
6.     OTA       = 0x2790, /**< OTA header */
7.     SecureBoot = 0x2791,
8.     RomPatch   = 0x2792,
9.     AppPatch   = 0x2793,
10.    AppData1    = 0x2794,
11.    AppData2    = 0x2795,
12.    AppData3    = 0x2796,
13.    AppData4    = 0x2797,
14.    AppData5    = 0x2798,
15.    AppData6    = 0x2799,
16.    UpperStack  = 0x279a,
17.    IMAGE_MAX   = 0x279b,
18.    IMAGE_USER_DATA = 0xFFFE, /**<the image only support unsafe single bank ota*/
19. } T_IMG_ID;

```

相关说明:

1. payload_len 单位是字节, 表示 image 的大小, 不包括 1KB 的 image header;
2. crc16 表示进行 crc 校验还是 SHA256 校验, 如果不为 0 表示 crc 校验, 否则进行 SHA256 校验;
3. ctrl_flag 和 OTA 相关的位域只有 not_ready 和 not_obsolete:
 - 1) not_ready 表示 OTA 传输写入是否完成, 默认编译的 image 中 not_ready 为 0;
 - (1) 当 image 写到备份区时, 先将 not_ready 置 1, 直到升级传输完成, 且通过完整性校验后(CRC or SHA256), not_ready 才写为 0, 表示 image 已经 ready;
 - 2) not_obsolete 表示 image 是否废弃, 默认编译的 image 中 not_obsolete 为 1;
 - (1) 当支持 bank 切换时, not_obsolete 在 OTA 过程中无效;
 - (2) 当不支持 bank 切换时, OTA 升级完成后, 启动代码判断 not_ready 为 0 且 not_obsolete 为 1, 此时将 image 从 OTA_TMP 区域搬运到指定区域 (App/Patch/Appdata), 搬运成功后, 将 OTA_TMP 区 image 中 not_obsolete 写为 0;
4. Image Payload 中放置的是 Secure Boot/Patch/APP 的业务代码以及 APP Data 中的 raw data 部分。

4 OTA 打包格式及工具

OTA 有以下两种打包工具：

1. Flash Map Generate Tool: 生成 flash map. h 和 flash_map. ini。
 - 1) flash_map.h 需要放到工程同级目录下参与编译，生成 APP image;
 - 2) flash_map.ini 为 MP Pack Tool 和 MP Tool 的输入文件，需要保证 image 和设置的所有输出地址一致;
2. MP Pack Tool: 打包 OTA 文件。

4.1 支持 Bank 切换

4.1.1 Flash 布局

Bank 切换方案需要两个完全相同的 OTA bank 互为备份。该方案的优点是升级完成重启后，程序直接跳转到新的 Bank 运行，OTA 升级切换流程非常快。缺点是增加了比较多的 flash 开销，所以一般情况下选择 Bank 切换方案时，flash size 要比较大一点。

下面以 1M byte 的 flash 为例，介绍 Bank 切换方案。推荐的 Flash 布局如下表所示：

表 4-1 Bank 切换 flash 布局示例

1MB Flash 布局示例	大小（字节）	起始地址
1) Reserved	4K	0x00800000
2) OEM Header	4K	0x00801000
3) OTA Bank0	424K	0x00802000
a) OTA Header	4K	0x00802000
b) Secure boot loader	4K	0x0080D000
c) Patch code	40K	0x00803000
d) Upperstack code	144K	0x0080E000
e) APP code	232K	0x00832000
f) APP data1	0K	0x0086C000
g) APP data2	0K	0x0086C000
h) APP data3	0K	0x0086C000
i) APP data4	0K	0x0086C000
j) APP data5	0K	0x0086C000
k) APP data6	0K	0x0086C000
4) OTA Bank1 (大小必须和 OTA Bank0 相同)	424K	0x0086C000
a) OTA Header	4K	0x0086C000
b) Secure boot loader	4K	0x00877000
c) Patch code	40K	0x0086D000
d) Upperstack code	144K	0x00878000
e) APP code	232K	0x0089C000
f) APP data1	0K	0x008D6000
g) APP data2	0K	0x008D6000
h) APP data3	0K	0x008D6000
i) APP data4	0K	0x008D6000
j) APP data5	0K	0x008D6000
k) APP data6	0K	0x008D6000
5) FTL	16K	0x008D6000
6) OTA Temp	0K	0x008DA000
7) APP Defined Section	152K	0x008DA000

注意：Flash Layout 需要根据用户实际 image 和 data 的大小进行合理划分。

4.1.2 打包工具使用步骤——切换 bank

1. 使用 Flash Map Generate Tool 生成 flash map.ini、flash map.h、OTA Header0 和 OTA Header1 文件，具体如下图所示：

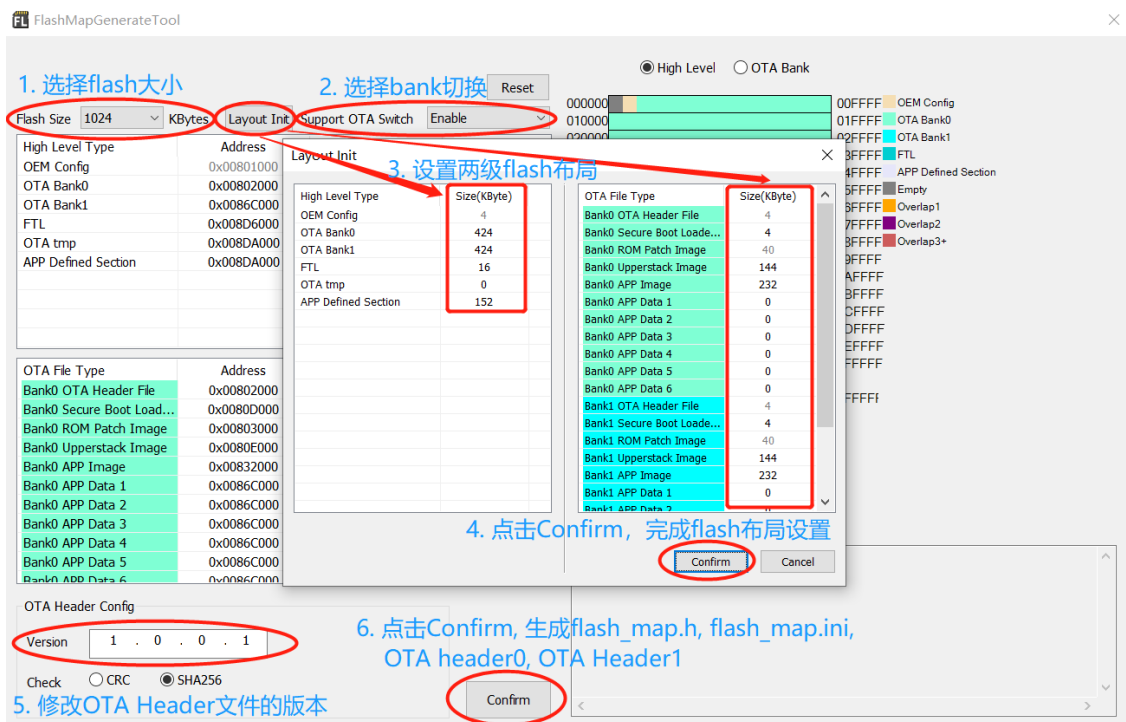


图 4-1 设置 Flash 布局并生成 OTA Header

注意：打包用的 OTA Header 版本号要比原来运行的版本号高，这样 OTA 升级完，新 bank 才能正常生效。

2. 将 flash_map.h 文件拷贝到工程文件同目录下，并用 keil 打开工程，编译链接生成 app MP sdk#####+version+MD5.bin 的文件供打包使用，具体如下图所示：

app.bin		2022/5/31 9:41	BIN 文件	38 KB
app.hex	版本号 MD5校验值	2022/5/31 9:41	HEX 文件	91 KB
app_MP_sdk_1.1.1.8_c03d956aec38b895df0a2b1d6761e7e862e305f0c.bin		2022/5/31 9:41	BIN 文件	39 KB
app-8cc2c6125eac81665842961751bb0ab3.bin		2022/5/31 9:41	BIN 文件	38 KB
app-8cc2c6125eac81665842961751bb0ab3.disasm		2022/5/31 9:41	DISASM 文件	1,802 KB
app-8cc2c6125eac81665842961751bb0ab3.trace		2022/5/31 9:41	TRACE 文件	12 KB
app.disasm		2022/5/31 9:41	DISASM 文件	1,802 KB
App.trace		2022/5/31 9:41	TRACE 文件	12 KB

图 4-2 编译 APP 文件

注意：切换 bank 的方案需要编译 OTA Bank0 和 OTA Bank1 的 image。Realtek 发布的 SDK 中，demo APP 工程默认编译的是 OTA Bank0 的 app image。编译 OTA Bank1 的 app image 需要将工程文件同目录下 mem_config.h 中的#define APP_BANK 修改为 1，具体代码如下：

1. `/** @brief set app bank to support OTA: 1 is ota bank1, 0 is ota bank0 */`
2. `#define APP_BANK 1`

3. 获取 OTA Bank1 的 patch 和 upperstack image;

注意: SDK 中发布的 secure boot, patch 和 upperstack Image 默认运行在 OTA Bank0, 如果选用了切换 bank 方案, 需要咨询 Realtek 对应发布运行在 OTA Bank1 的 secure boot, patch 和 upperstack Image。

4. 生成打包文件, 默认在软件同目录下生成 ImgPacketFile-xxxxxx.bin, 此文件为升级用的打包文件。

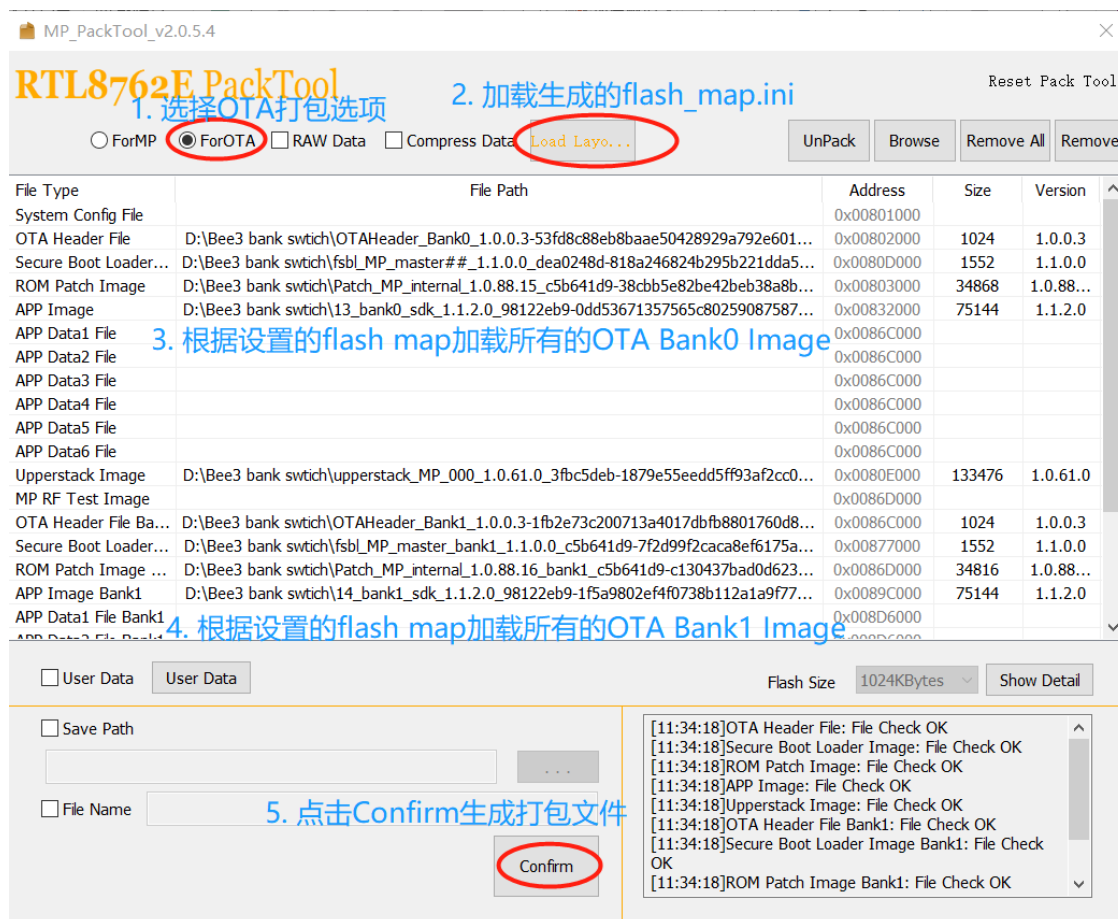


图 4-3 打包生成 Pack

注意事项:

- 1) OTA Header0 和 OTA Header1 都需要打包进 PACK (与不切换 Bank 模式不同);
- 2) Flash layout 中定义的内容都需要进行打包, 缺一不可;
- 3) 建议 Bank0 和 Bank1 一起打包进 PACK;
- 4) APPData 文件通过 SDK/tool/App DataTool 生成脚本生成, 具体参考《RTL8762E App DataTool User Guide》。

4.2 不支持 Bank 切换

4.2.1 Flash 布局

不切换 Bank 方案的 Flash layout 需注意以下三点：

1. OTA Bank1 区无需分配容量；
2. OTA Temp 区需要分配容量，且不小于 OTA Bank0 中容量最大的 image 大小。
故该方案优点是相对节约 Flash 空间。OTA 传输完成，重启 boot 程序会将 OTA Temp 区数据搬到 OTA Bank0 指定的 image 区域，再重启生效，所以相对增加了 OTA 升级完成的重启时间。
3. 在不切换 bank 方案中还支持组合 image 升级，该功能由 board.h 中宏定义 SUPPORT_TEMP_COMBINED_OTA 控制，默认打开。当使用组合 image 升级时，在将 image 数据写到 OTA temp 区时，会去计算 OTA temp 区剩余空间能否放下下一个需要写入的 image 文件，如果可以放下则继续将下一个 image 文件写入 OTA temp 区，当放不下时则再将 OTA Temp 区数据搬到 OTA Bank0 区域。组合升级的优点在于减少重启次数加快传输速率。

下面以 512K byte 的 flash 为例，介绍不切换 Bank 方案。推荐的 Flash 布局如下表所示：

表 4-2 Bank 不切换 flash 布局示例

512KB flash 示例布局	大小（字节）	起始地址
1) Reserved	4K	0x00800000
2) OEM Header	4K	0x00801000
3) OTA Bank0	340K	0x00802000
a) OTA Header	4K	0x00802000
b) Secure boot loader	4K	0x0080D000
c) Patch code	40K	0x00803000
d) Upperstack code	144K	0x0080E000
e) APP code	148K	0x00832000
f) APP data1	0K	0x00857000
g) APP data2	0K	0x00857000
h) APP data3	0K	0x00857000
i) APP data4	0K	0x00857000
j) APP data5	0K	0x00857000
k) APP data6	0K	0x00857000
4) OTA Bank1	0K	0x00857000
5) FTL	16K	0x00857000
6) OTA Temp	156K	0x0085B000
7) APP Defined Section	0K	0x00880000

注意：此处没有分配 APP data，Flash Layout，需要根据用户实际 image 和 data 的大小进行合理划分。

4.2.2 打包工具使用步骤——不切换 bank

1. 使用 Flash Map Generate Tool 生成 flash map.ini、flash map.h 和 OTA Header0 文件，具体如下图所示：

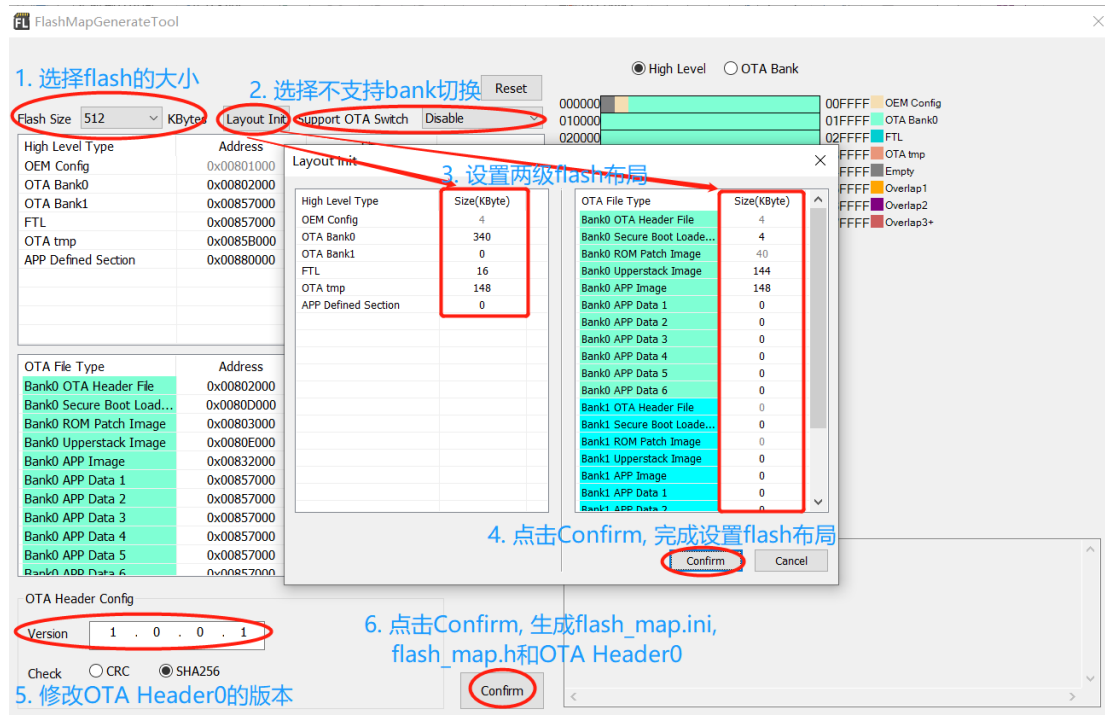


图 4-4 配置 Flash Layout 并生成 OTA Header0

注意：此处生成的 flash map.ini 需要和 MP 阶段使用的 flash map.ini 保持一致。

2. 将 flash_map.h 文件拷贝到工程文件同目录下，并用 keil 打开工程，编译链接生成 app_MP_sdk#####+version+MD5.bin 的文件供打包使用。

注意：不切换 Bank 方案只需要编译 OTA Bank0 的 image，配置见工程文件同目录下 mem_config.h 中的#define APP_BANK，具体代码如下

```
1. /** @brief set app bank to support OTA: 1 is ota bank1, 0 is ota bank0 */
2. #define APP_BANK 0
```

3. 打开 MP Pack Tool, 加载第一步生成的 flash_map.ini 文件, 并 load 相应 image 文件, 如下图所示:

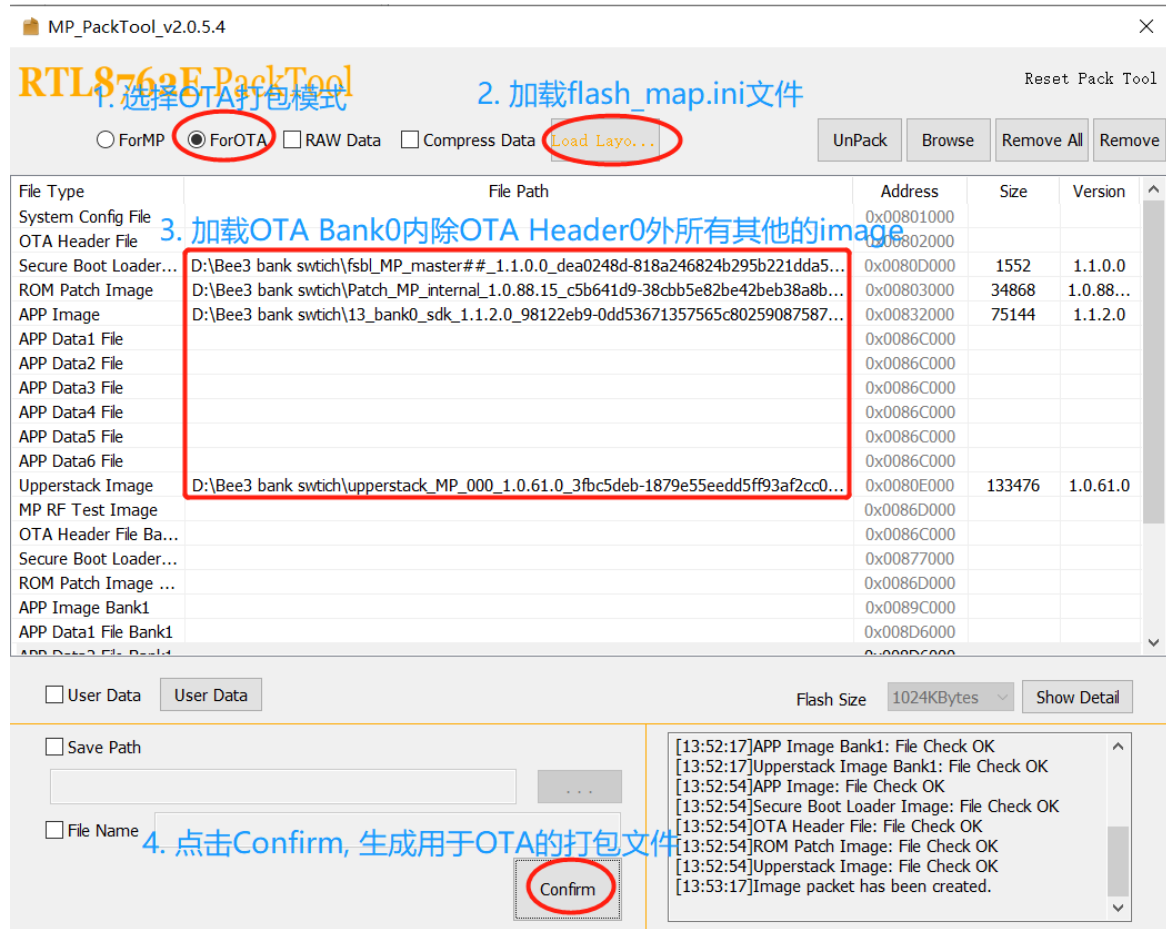


图 4-5 Pack OTA images with MP Pack Tool

注意事项:

- 1) OTA Header0 在不切换 Bank 方案时不需要打包进 PACK; (与切换 Bank 的模式不同)
- 2) Flash layout 中定义了 Secure boot loader Image 的内容, 如果没有新版本发布, 不建议打包;
- 3) 如果只需要更新 ROM Patch Image 或者 APP Image, 可只打包其中一个。

5 OTA 协议

5.1 DFU Service

DFU Service 的 uuid 为: { 0x12, 0xA2, 0x4D, 0x2E, 0xFE, 0x14, 0x48, 0x8e, 0x93, 0xD2, 0x17, 0x3C, **0x87, 0x62, 0x00, 0x00**}。

DFU Service 定义了两个 Characteristic:

1. Data Characteristic: 接受 image 的数据通道, 属性 write no response。
2. Control Point Characteristic: 接受控制指令的通道, 属性 write/notification。

Realtek Confidential

DFU Service 支持的 control point 如下表所示:

表 5-1 DFU opcode

Procedure	Requirement	Properties	Parameter Description	Applicable Response Value(s)	Response Parameter
Start DFU ①	M	Write	ic_type(UINT8) secure_version (UINT8) ctrl_flag.value(UINT16) image_id (UINT16) crc16((UINT16) payload_len (UINT32)	ARV	None
Receive FW image	M	Write	image_id (2byte-UINT16) nImageLength(4Byte-INT32)	ARV	None
Validate FW	M	Write	image_id (2byte-UINT16)	ARV	None
Activate Image and Reset	M	Write	None	None	None
Reset System	M	Write	None	None	None
Report Received Image Information	M	Write	image_id(UINT16)	ARV	origin_image_version (UINT32) cur_offset (UINT32)
Connection parameter update	M	Write	connIntervalMin(UINT16) connIntervalMax(UINT16) connLatency(UINT16) supervisionTimeout(UINT16)	ARV	None
Buffer check enable	M	Write	None	ARV	Max buffer size(UINT16) Mtu size(UINT16)
Buffer check size&crc	M	Write	mBufferSize(UINT16) mCrc(UINT16)	ARV	Next send offset(UINT32)
IC type	O	Write	None	ARV	ic_type(UINT8)
Copy Img②	M	Write	image_id(UINT16) destination_addr(UINT32) copysize(UINT32)	ARV	None

注意事项:

- 1) ①Start DFU 的参数为 img 的 ctrlheader, 在接受到 ctrlheader 后, 需要写进 flash 作为升级文件的一部分, 所以这 12 个 bytes 和数据的传输处理一样, 如果使能了 aes 加密, 在收到 Start DFU 参数后, 需要解密后再解析, 并写入 flash 中;
- 2) ②当升级 app data 时, 采用 Bank 切换方案, 判断 secure version 和 APP DATA version 相同, 可以使用这条命令, 直接复制原来 Bank 的内容到目的 Bank, 省去 OTA 传输环节;
- 3) 在数据传输时, 如果启用 buffer check, 则其大小必须为 $(16 * 2^n)$ bytes, 并且要小于等于 max buffer Size (Buffer check enable 命令返回)。如果支持 aes 加密, 每 16byte 都进行加密, 接收端收到数据后, 需要先对其解密。最后小于 16 byte 的部分没有加密发送。当收满 buffer check size 后, 再写入 flash;
- 4) 如果不启用 buffer check, 则需要一次发送 $20 * n (n=1,2,4,5,10)$ bytes, 直到接收端收满 2000bytes, 才能写入 flash, 最后一次则把文件收完就写入。如果支持 aes 加密, packet 数据中, 能被 16 整除的部分, 需要加密后发送, 余数小于 16 bytes 则不需要加密;

5.2 OTA Service

OTA Service 的 uuid 为: { 0x12, 0xA2, 0x4D, 0x2E, 0xFE, 0x14, 0x48, 0x8e, 0x93, 0xD2, 0x17, 0x3C, **0xFF**, **0xD0**, 0x00, 0x00 }。

OTA Service 定义了如下 Characteristics:

表 5-2 OTA Characteristic

Characteristic Name	Requirement	Mandatory Properties	Description
OTA CMD	M/O	WriteWithoutResponse	Refer to OTA CMD
Device Mac	M	Read	Refer to Device Mac
Patch Version	M	Read	Refer to Patch Version
App Version	M	Read	Refer to App Version
Patch Extension Version	O	Read	Refer to Patch Extension Version
Test Mode	O	WriteWithoutResponse	Refer to Test Mode
Device Info	M	Read	Refer to Device Info
Image Counter	O	WriteResponse	Refer to Image Counter
Image Version	M	Read	Refer to Image Version

5.2.1 OTA CMD

UUID: 0xFFD1

该特性是允许设备进入 OTA 模式的控制端点。

此命令用于进入 DFU mode，进入 DFU mode 部分的代码如下：

```
1. dfu_switch_to_ota_mode();
2. WDG_SystemReset(RESET_ALL_EXCEPT_AON, DFU_SWITCH_TO_OTA);
```

表 5-3 OTA CMD characteristics

Name	Field Requirement	Format	Value
OTA CMD	Mandatory	Uint8	1

5.2.2 Device Mac

UUID: 0xFFD2

该特性用来读取设备的 BDA（Bluetooth Device Address），用以和 OTA 模式中的扫描 BDA 进行比较。

表 5-4 Device Mac characteristics

Name	Field Requirement	Format	Value
Device Mac	Mandatory	Uint8*6	XX:XX:XX:XX:XX:XX

5.2.3 Patch Version

UUID: 0xFFD3

该特性用来读取设备的 patch 版本号，兼容 RTL8762A 版本，RTL8762C/RTL8762E 不推荐使用，其版本信息在 Image version 描述。

表 5-5 Patch Version characteristic for RTL8762C/RTL8762E

Name	Field Requirement	Format	Value
Patch Version	Mandatory	Uint32	0xNNNNNNNN

5.2.4 APP Version

UUID: 0xFFD4

该特性用来读取设备的 APP 版本号，兼容 RTL8762A 版本，RTL8762C/RTL8762E 不推荐使用，其版本信息在 Image version 描述。

表 5-6 APP Version characteristic for RTL8762C/RTL8762E

Name	Field Requirement	Format	Value
APP Version	Mandatory	Uint32	0xNNNNNNNN

5.2.5 Patch Extension Version

UUID: 0xFFD5

该特性用来读取设备的 patch extension 版本号，只有 RTL8762A 版本有，RTL8762C/RTL8762E 并没有此特性。

表 5-7 Patch Extension Version characteristic

Name	Field Requirement	Format	Value
Patch extension Version	Optional	Uint16	0xNNNN

5.2.6 Test Mode

UUID: 0xFFD8

该特性是允许设备退出测试模式的控制端点，写“1”则清除测试标志，并退出 MP 模式。

表 5-8 Test Mode characteristics

Name	Field Requirement	Format	Value
Test mode	Optional	Uint8	1

注意：此特性与 OTA 无关

5.2.7 Device Info

UUID: 0xFFFF1

该特性用来读取设备的固件基本信息，描述如下：

表 5-9 Device info characteristic for RTL8762C/RTL8762E

Name	Field Requirement	Format	Value
Device info	Mandatory	As Table 5-10	As Table 5-10

对于其他 BT SoC 系列芯片，特征值如下表所示：

表 5-10 Device info Format For RTL8762C/RTL8762E (OTA version = 1)

Form at	IC Type	Version	Secure Version	MODE	Max Buffer Size	temp_ba nk_size
Size	8bit	8bit	8bit	8bit	16bit	8bit
Value	RTL8763:4 RTL8762C:5 RTL8762E:12	Bit3~0: OTA version:0x1 Bit7~4: Reserved:0x0		Bit0	0xNNNN	0xNNNN
				0:normal mode 1:Support buffer check		
				Bit1		
				0:Aes flag not set 1:Aes flag Set		
				Bit2		
				0: Only encrypt first 16 bytes of OTA data in normal mode 1:Encrypt 16*N bytes of OTA date in normal mode	0xNNNN	0xNNNN
				Bit3		
				0: Disable Copy Image 1: Enable Copy Image		
				Bit4		
				0: Update one Image at a time 1: Update multiple Images at a time		

Format(Attach to above table)	Image Version Indicator 32bit																						
Value(Attach to above table)	0xNNNNNNNN																						
	Indications for each image version. Each indication uses 2 bits.																						
	00: image does not exist.																						
	01: image exists in bank0, OTA should update image for bank1.																						
	10: image exists in bank1, OTA should update image for bank0.																						
	11: image is standalone. OTA should update image for standalone.																						
	bit[1:0]: Image 0																						
	...																						
	bit[2N+1:2N]:Image N																						
	Image indicator for RTL8762C/RTL8762E is as below:																						
	<table border="1"> <tr> <td>Image 0</td><td>OTA Header Image</td></tr> <tr> <td>Image 1</td><td>Secure Boot Loader Image</td></tr> <tr> <td>Image 2</td><td>ROM Patch Image</td></tr> <tr> <td>Image 3</td><td>APP Image</td></tr> <tr> <td>Image 4</td><td>APP Data1 Image</td></tr> <tr> <td>Image 5</td><td>APP Data2 Image</td></tr> <tr> <td>Image 6</td><td>APP Data3 Image</td></tr> <tr> <td>Image 7</td><td>APP Data4 Image</td></tr> <tr> <td>Image 8</td><td>APP Data5 Image</td></tr> <tr> <td>Image 9</td><td>APP Data6 Image</td></tr> <tr> <td>Image 10</td><td>Upperstack Image</td></tr> </table>	Image 0	OTA Header Image	Image 1	Secure Boot Loader Image	Image 2	ROM Patch Image	Image 3	APP Image	Image 4	APP Data1 Image	Image 5	APP Data2 Image	Image 6	APP Data3 Image	Image 7	APP Data4 Image	Image 8	APP Data5 Image	Image 9	APP Data6 Image	Image 10	Upperstack Image
Image 0	OTA Header Image																						
Image 1	Secure Boot Loader Image																						
Image 2	ROM Patch Image																						
Image 3	APP Image																						
Image 4	APP Data1 Image																						
Image 5	APP Data2 Image																						
Image 6	APP Data3 Image																						
Image 7	APP Data4 Image																						
Image 8	APP Data5 Image																						
Image 9	APP Data6 Image																						
Image 10	Upperstack Image																						

5.2.8 Image Counter

UUID: 0xFFFF2

该特性为写入响应，告知设备接下来有多少个 image 文件需要写入。

表 5-11 Image Counter Characteristics

Name	Field Requirement	Format	Value
Image Counter	Optional	Uint8	0xNN

5.2.9 Image Version

UUID: 0xFFE0~FFEF

该特性为读取设备的 image 版本。

每个 image 版本占用 4 bytes，由于受默认 MTU size（20 bytes）的限制，当 image 数量大于 5 时，需

要下一定义的特性 (UUID: 0xFFE0~FFEF) 去读取接下来的 image 版本。设备的 image 版本数量通过 Image Version Indicator 去识别, 在 Device Info (0xffff1) 中定义。

表 5-12 Image Version characteristics

Name	Field Requirement	Format	Value
Image Version	mandatory	Uint32*N	

Realtek Confidential

5.3 OTA 流程

OTA 流程分为 buffer check 和不带 buffer check 两个，具体流程如下图所示：

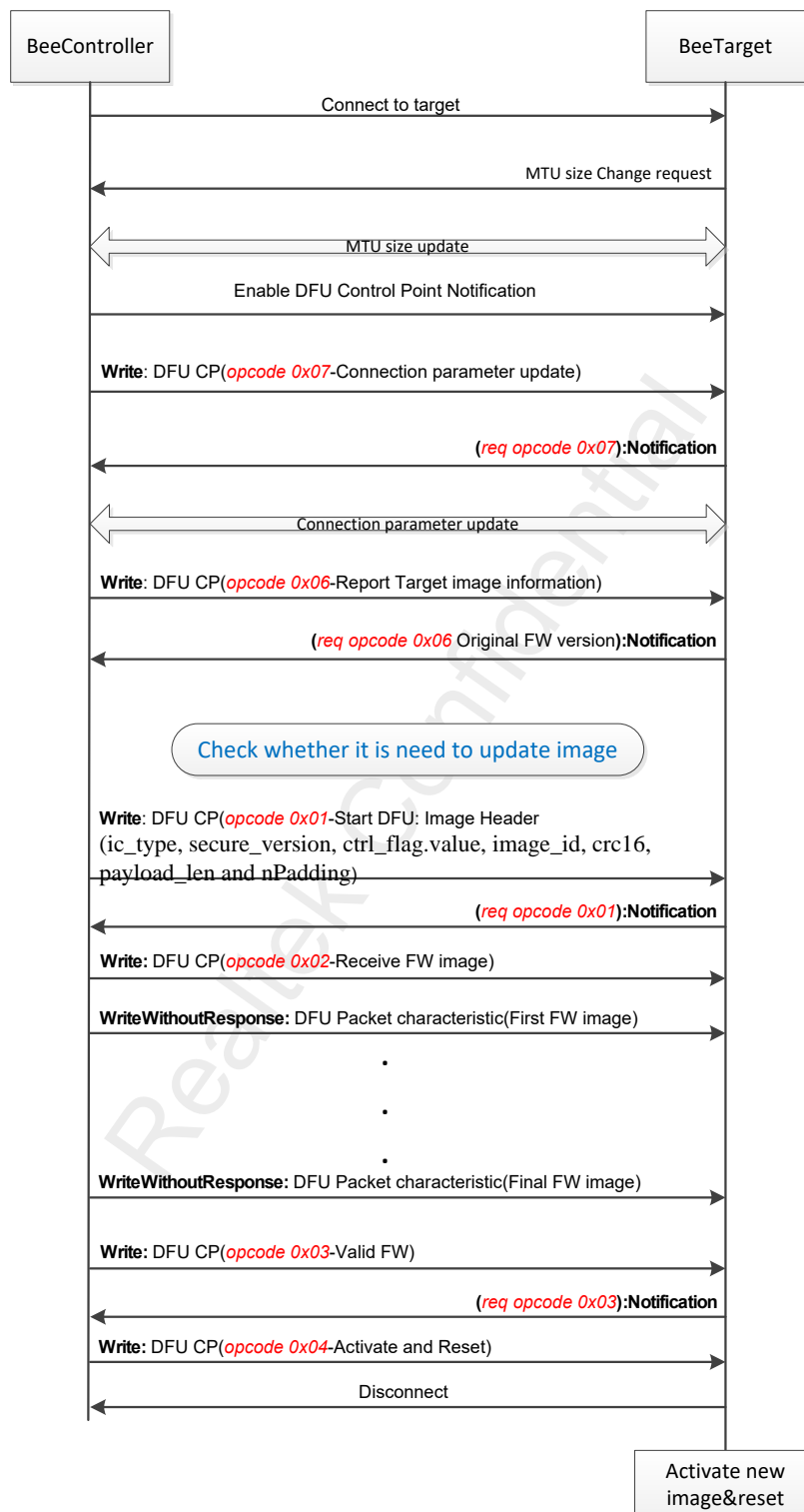


图 5-1 OTA 不带 buffer check 流程

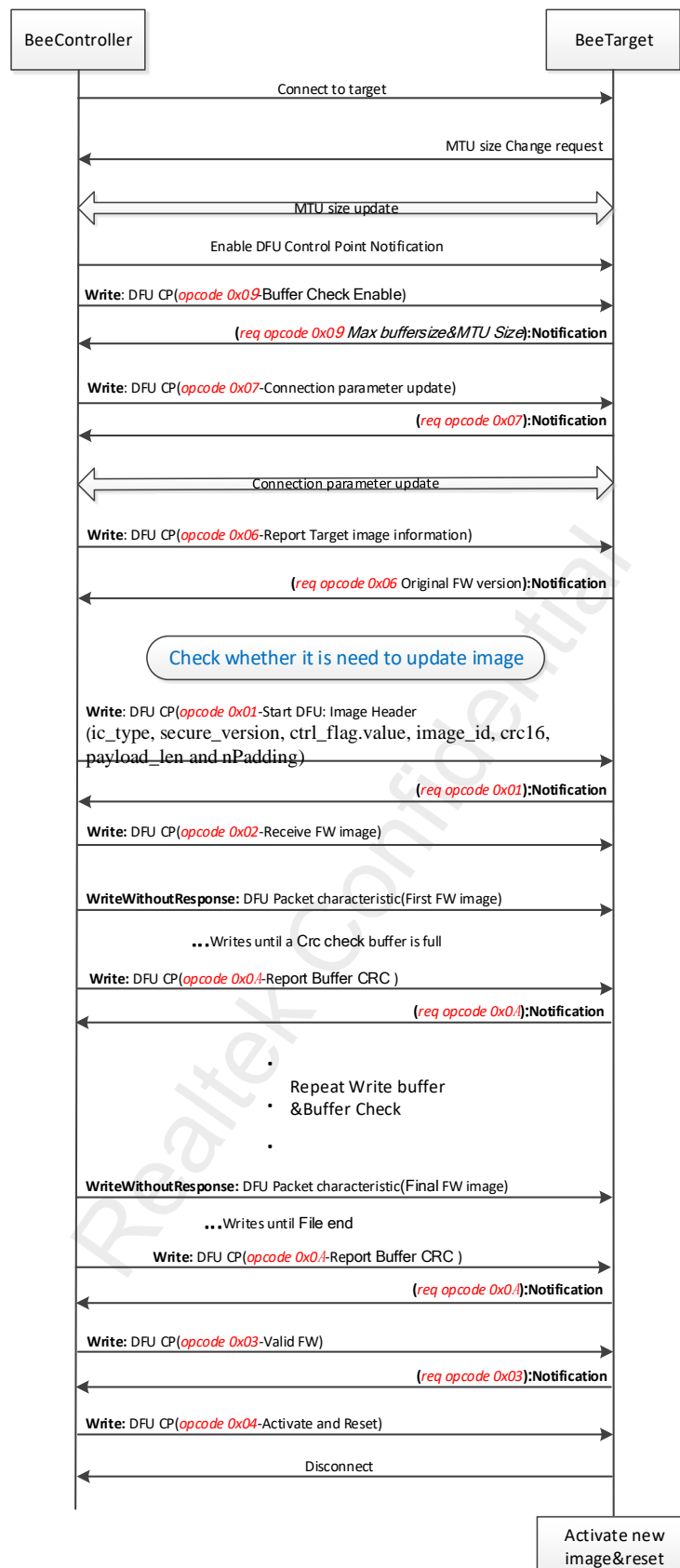


图 5-2 OTA buffer check 流程

5.3.1 多文件更新注意事项

1. Bank 不切换方案，当打包待升级文件中包含 Patch、APP 或者 APP DATA，需要一个文件升级验证成功，重启生效之后，再升级下一个文件；
2. Bank 切换方案，当打包待升级文件中包含 OTA Header、Patch、APP 或者 APP DATA，需要一个文件升级验证成功，再升级验证下一个文件。等所有文件都升级验证成功后，才能进行重启，否则本次升级无效。具体原因是切换 Bank 的方案，需要 bank 区所有文件都一起生效，才能正常运行。

Realtek Confidential

6 参考文献

- [1]. 《RTL8762E Memory User Guide》

Realtek Confidential