USB-IAP通讯协议

通讯协议

- 传输介质单包传输长度是有限的，例如**WINUSB**的**MPS**为**64**，即单包最大**64**字节，所以要实现任意长度的应用数据传输，则需要进行分包和组包，可以在**传输层**实现分包和组包操作；
- 为了将升级文件传输到芯片，还需要做一套IAP应用协议，按照指定的格式将数据依次传输到芯片，并存储到flash中；

1. 应用包格式

1.1 主机发送包格式

CMD	Length	Payload	CRC
命令	长度	参数值	校验值

- **各字段含义：**

序号	字段	字节数	说明
1	**CMD**	1	请求命令
2	**Length**	2	payload长度，**小端模式**。
3	**Payload**	**Length**	payload数据内容，不同命令数据内容不同；长度为0时，此项不存在；
4	**CRC**	2	CRC校验（**小端模式**）： 多项式= 1021 CRC-16/X25 ，初值0xFFFF，**CRC-16(Modbus)**； 校验对象：CMD+Length+DATA 例如： 如下十六进制数据计算的CRC值为**0x786C**： 11 22 33 44 44 44 44 45 44 44 45 63 46 34 56 34 3D DD DE DD EC F4 00 22 22 22 22 22 22 22 22 22 可通过如下网址的工具验证：

			https://www.23bei.com/tool/59.html

1.2 从机返回包格式

CMD	ErrCode	rspCmd	Length	Payload	CRC
命令	错误码	响应命令	长度	参数值	校验值

- **各字段含义：**

序号	字段	字节数	说明
1	**CMD**	1	应答命令
2	**ErrCode**	1	错误码，代表本次命令执行情况。
3	**rspCmd**	1	响应命令，针对哪一条指令进行的响应； **当下发CMD值错误时，这里也会填充下发命令字段对应值，原路返回。**
4	**Length**	2	payload长度，小端模式。
5	**Payload**	**Length**	数据内容，不同命令数据内容不同；长度为0时，此项不存在；
6	**CRC**	2	CRC校验（小端模式）： 与下发命令的CRC计算方法相同，此处不再赘述。

2. IAP命令列表

2.1 主机发送给从机的命令

序号	CMD值	HEX	说明

1	IAP_CMD_START	0xA0	启动IAP升级，发送header数据给设备；设备在接收到该指令后，需校验header，如果正常，则准备好升级，并返回成功应答给主机，如果校验header不满足升级条件，返回相应的错误状态给主机。
2	IAP_CMD_FLASH_WRITE	0xA1	主机发送写flash命令，将BIN文件的一块数据发到设备，设备需要校验数据，并将数据存储到flash，当发生错误时，设备需要返回错误码给主机，如果操作成功，则返回成功应答给主机； 如果设备检测到是最后一块儿数据，则会校验所有传输的升级数据，如果CRC与header中的CRC一致，则会返回成功，否则也会返回错误，表明本次升级失败；
3	IAP_CMD_FLASH_READ	0xA2	主机发送读flash命令，设备需根据主机列出的偏移地址获取指定长度的数据，并返回给手机，如果发生故障，则返回错误应答码；
4	IAP_CMD_REBOOT	0xA3	主机发送重启设备的命令，设备会返回应答，并在主机指定的时间后重启设备；
5	IAP_CMD_SWITCH_APP	0xA4	主机发送切换到新程序的命令，设备会跳转到新程序执行，一般用不到该命令，因为设备升级完重启后则自动启动了新程序；【只有在BOOT中才会处理该命令，APP中不处理该命令】
6	IAP_CMD_SWITCH_BOOT	0xC0	主机发送切换到BOOT程序的命令，设备会从APP程序跳转到BOOT程序，并等待升级；【只有APP程序中才会处理该命令，BOOT中不处理该命令】

2.2 从机返回给主机的命令

序号	CMD值	HEX	说明
1	IAP_CMD_ACK	0xB0	这是从机给主机发送的应答指令包，用于指明上一条指令的执行情况，并将执行状态返回；

2. 命令解析

2.1 启动升级 [IAP_CMD_START]

- **主机发送格式**

CMD	Length	Payload	CRC
0xA0	0x0080	128字节header数据	校验值

- **设备应答格式**
  - 见下方从机通用应答命令[**IAP_CMD_ACK**]介绍，payload为0。
- 指令依赖关系：
  - **未成功收到此指令，无法执行FLASH的读写操作；**

2.2 写入数据 [IAP_CMD_FLASH_WRITE]

- **主机发送格式**

CMD	Length	Payload	CRC
0xA1	**块号**字段长度+ **偏移地址**字段长度+ **块数据**字段长度	1. **块号**：2字节，从0x0000到0xFFFF，**最后一块儿的块号必须为0xFFFF**，且最后一块儿的数据长度可以小于等于**BLOCK_SIZE**，其余块儿长度必须为**BLOCK_SIZE**，**BLOCK_SIZE**由IAP包**header**特定字段决定； 2. **偏移地址**：4字节，每块的偏移地址为：块号*BLOCK_SIZE，最后一块儿除外； 3. **块数据**：BIN文件分块数据，除了最后一块儿，大小均为**BLOCK_SIZE；**	校验值

- **设备应答格式**
  - 见下方从机通用应答命令[**IAP_CMD_ACK**]介绍，payload为0。
- **指令依赖关系：**
  - **未成功收到IAP_CMD_START指令，无法执行FLASH的读写操作；**

2.3 读取数据 [IAP_CMD_FLASH_READ]

特别提醒：预留这个接口是不安全的，开发完协议后在程序里关掉

- **主机发送格式**

CMD	Length	Payload	CRC
0xA2	0x0006	1. **偏移地址**：4字节，**小端模式**，代表读取数据的偏移地址，地址范围不能超过header中（**BLOCK_SIZE***总块数）的值，其中**BLOCK_SIZE**由IAP包header特定字段决定； 2. **获取数据大小**：2字节，**小端模式**，代表主机想获取数据的长度，一次获取不能超过**BLOCK_SIZE；**	校验值

- **设备应答格式**
  - 见下方从机通用应答命令[**IAP_CMD_ACK**]介绍，payload不为0，格式如下：

Payload	1. **偏移地址**：4字节，**小端模式**，代表偏移地址，与主机请求的地址相同，地址范围不超过header中（**BLOCK_SIZE***总块数）的值，其中**BLOCK_SIZE**由IAP包header特定字段决定； 2. **返回数据大小（size）**：2字节，**小端模式**，代表返回flash数据的长度，与主机下发的长度相同，一次返回不超过**BLOCK_SIZE；** 3. **FLASH数据**：此项数据长度为**size**；

- **指令依赖关系：**
  - **未成功收到IAP_CMD_START指令，无法执行FLASH的读写操作；**

2.4 重启设备 [IAP_CMD_REBOOT]

- **主机发送格式**

CMD	Length	Payload	CRC
0xA3	0x0002	1. 延迟复位毫秒数：2字节，范围：0~1000	校验值

- **设备应答格式**
  - 见下方从机通用应答命令[**IAP_CMD_ACK**]介绍，payload为0。

2.5 切换到新程序 [IAP_CMD_SWITCH_APP]

- **主机发送格式**

CMD	Length	Payload	CRC

0xA4	2字节	1. 延迟切换毫秒数：2字节，范围：0~1000	校验值

- **设备应答格式**
  - 见下方从机通用应答命令[**IAP_CMD_ACK**]介绍，payload为0。

2.6 从机通用应答命令[IAP_CMD_ACK]

CMD	ErrCode	rspCmd	Length	Payload	CRC
0xB0	**错误码**，1字节，表明本次指令执行情况，详见下方命令错误码表	**响应命令**，1字节，与接收到的命令字字段相同，即使接收到不合法的命令字段，填到这里；	根据下发命令不同而不同，当下发命令不在有效命令列表时，此项固定为0x0000；	根据下发命令不同而不同，详见每个命令的介绍。当Length为0是此项不存在。	校验值

2.7 切换到BOOT程序[IAP_CMD_SWITCH_BOOT]

- **主机发送格式**

CMD	Length	Payload	CRC
0xC0	2字节	1. 延迟切换毫秒数：2字节，范围：0~1000	校验值

- **设备应答格式**
  - 见从机通用应答命令[**IAP_CMD_ACK**]介绍，payload为0。

2. 命令错误码表

错误码	含义
0x00	**操作成功**
0xE0	**未知CMD**
0xE1	**Length错误**
0xE2	**CRC错误**

0xE3	块号错误
0xE4	块大小错误
0xE5	写入偏移地址错误
0xE6	读取偏移地址错误
0xE7	参数错误
0xE8	FLASH操作失败
0xE9	状态不满足，例如未发送header就操作write等
0xF0	HEADER信息错误：升级标记不匹配
0xF1	HEADER信息错误：芯片代号错误
0xF2	HEADER信息错误：项目代号错误
0xF3	HEADER信息错误：硬件版本格式不正确，应为：Vx.y.z（x,y,z必须0~9字符）
0xF4	HEADER信息错误：软件版本格式不正确，应为：Vx.y.z（x,y,z必须0~9字符）
0xF5	HEADER信息错误：校验类型不支持，或者校验值长度不对；
0xF6	HEADER信息错误：块大小不在有效范围，或总升级字节数超过可存储区。
0xF7	HEADER信息错误：升级类型暂不支持；
0xF8	HEADER信息错误：加密信息有误：例如加密类型不支持，或加密数据长度错误等；