

## master端OTA说明

### 1.master端OTA的处理流程为:

- 1) master直连需要OTA的设备，之后通过扫描直连设备的Service与Characteristic，获取到UUID为"00010203-0405-0607-0809-0A0B0C0D2B12"的Characteristic就是OTA的特征。
- 2) 获取设备当前firmware版本号，决定是否要做OTA更新（或者服务器端自己维护版本信息）。获取版本号操作是，对OTA的特征写两个字节的的数据0xff00，如下图所示。（设备端暂时没有响应此命令）

Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
L2CAP-S	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue	0xF00021	-38	OK
	2	1	0	0	9	0x0005	0x0004	0x52	0x000D	00 FF			

- 3) 向设备的OTA特征写一个OTA start命令0xff01，通知设备进入OTA模式，如下图所示。

Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
L2CAP-S	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue	0xF00006	-38	OK
	2	1	0	1	9	0x0005	0x0004	0x52	0x000D	01 FF			

- 4) 读取新的firmware文件到master内存中，对firmware数据按照16字节的长度进行截取，组成一个个20字节长度的OTA数据包。OTA data的格式如下，有效数据为20字节，前2个字节放index，index从0开始进行累加，紧跟16个字节为有效的firmware数据，最后2个字节是前18个字节数据的CRC计算值。

注意，如果firmware最后一笔数据不是16字节对齐，需要将剩余的部分按0xff补对齐，计算CRC的时候需要将补充的数据计算进去。

根据上面的格式组成了OTA数据包，然后master向设备的OTA特征发送write OTA数据包的命令。

连续写入8个OTA数据包后，对设备的OTA特征发送read命令并等待read\_response，收到read\_response后重复“写入8个OTA数据包read一次”这个步骤。Read命令的作用是防止手机的TX buffer溢出，如果master不是手机可以考虑取消read做法。

OTA start数据包、index=0数据包、index=1数据包如下图：

Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
L2CAP-S	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	2	1	0	1	9	0x0005	0x0004	0x52	0x000D	01 FF	0xF00006	-38	OK
Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
Empty PDU	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	1	1	1	0	0	0x00047	0x0004				0xF00047	-38	OK
Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
L2CAP-S	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	2	0	1	1	27	0x0017	0x0004	0x52	0x000D	00 00 0E 80 56 32 2E 35 5D 01 4B 4E 4C 54 90 01 88 00 B2 0C	0xF00006	-38	OK
Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
Empty PDU	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	1	0	0	0	0	0xF00043	0x0004				0xF00043	-38	OK
Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
L2CAP-S	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	2	1	0	0	27	0x0017	0x0004	0x52	0x000D	01 00 5E 80 00 00 00 00 00 00 44 0C 02 00 00 00 00 00 D0 01	0xF00016	-38	OK

- 5) master端发送OTA数据包完成后，向设备的OTA特征写一个OTA end命令，通知设备OTA数据已经发送完成，设备端会自动升级并重启。OTA end命令如下，有效数据为8字节，前2个字节为0xff02，紧跟2个字节为新firmware的最大index值，最后2个字节为index的取反值。

最后一个OTA数据包、OTA end数据包如下图：

Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
L2CAP-S	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	2	1	0	1	27	0x0017	0x0004	0x52	0x000D	C4 20 DF 3C 33 10 FF FF FF FF FF FF FF FF FF FF 69 78	0xF00008	-38	OK
Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
Empty PDU	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	1	1	1	0	0	0xF00043	0x0004				0xF00043	-38	OK
Data Type	Data Header					L2CAP Header		ATT_Write_Command			CRC	RSSI (dBm)	FCS
L2CAP-S	LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	AttHandle	AttValue			
	2	0	1	0	13	0x0009	0x0004	0x52	0x000D	02 FF C4 20 3B DE	0xF00013	-38	OK

- 6) 设备端收到OTA end命令后会自动升级并重启。master端重连设备成功则提示OTA成功。

## 2.master端OTA流程图，如下：

