EZVIZ IOT
BLE 点对点协议（V1.0）

目录

1. 简介

随着萤石 IOT 生态的开放， 需要制定 BLE 设备通讯规范，消除 BLE 设备通讯流程中的歧义性、多样性。

本文档用于规范化萤石 IOT 生态下 BLE 设备的通讯协议，使 BLE 设备可以被萤石互联 APP 进行发现、配网、连接、控制。

2. BLE 广播包

2.1 数据格式

广播包的接入地址为 0x8e89bed6，根据 PDU type 分为 ADV_IND、SCAN_REQ、SCAN_RSP 等。

ADV_IND 和 SCAN_RSP 数据格式包含 Advertising Address 和 data，如下图 1 所示：

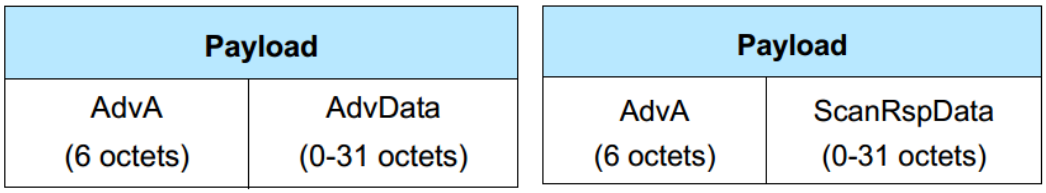


图 1 广播包格式

data 的具体数据格式如下图 2 所示：

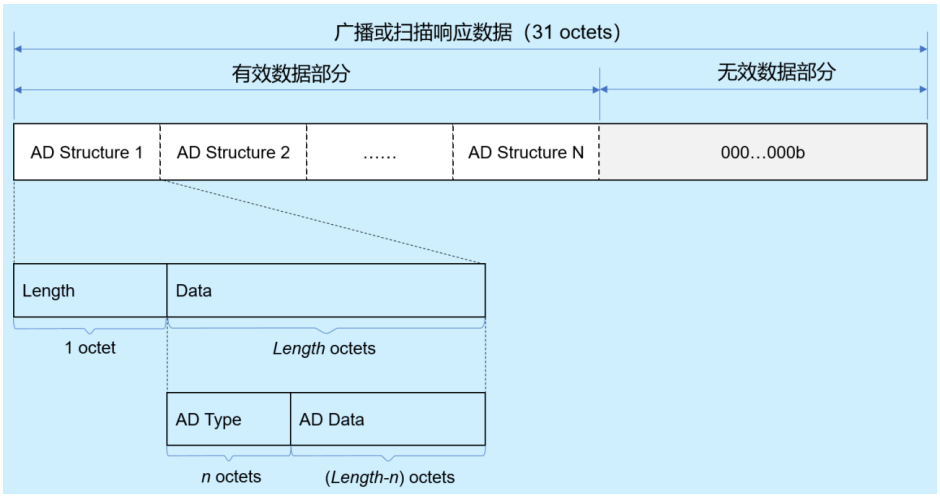


图 2 adv data 具体数据格式

每个包都是 31 字节，数据包中分为有效数据（significant）和无效数据（non-significant）两部分。

有效数据部分：包含若干个广播数据单元，称为 AD Structure 。如图所示，AD Structure 的组成是：

- 长度 Len ，表示这个 AD Structure 的长度（除去 Len 本身 1）
- 类型 AD Type：标记这段广播数据代表什么，如设备名、uuid 等。当 AdType == 0x09 时，数据 AD data 内容为设备显示名称。例如：广播名称：EZAAAAAA-XNNNNNNNNNN
- 数据 AD data

无效数据部分：广播包的长度必须是 31 个 byte，如果有效数据部分不到 31 字节，剩下的就用 0 补全。这部分的数据是无效的。

2.2 主动广播包

主动广播包的 PDU Type 为 0x3，设备激活时，通过广播表明自己的存在。

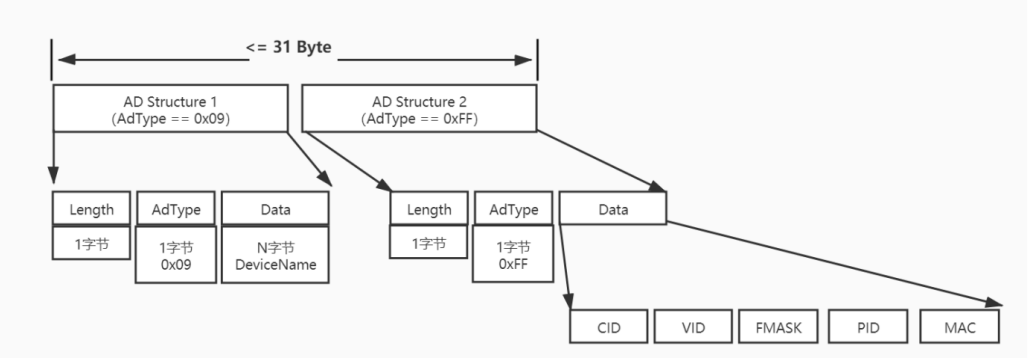
手机直连设备目前暂未使用该内容，建议跟 SCAN 响应包（PDU Type: SCAN_RSP）保持一致。

2.3 扫描响应包

手机直连设备采用主动扫描，即手机主动发起扫描请求（SCAN_REQ），设备接收到扫描请求之后，响应请求（SCAN_RSP，PDU Type: 0x4）。

萤石 BLE 设备响应包包中分为两块有效数据：AD Structure（AdType == 0x09） 和 AD Structure（AdType == 0xFF）。

AD Structure（AdType == 0x09)	AD Structure（AdType == 0xFF)
12字节 （BLE设备的显示名称)	19字节 （BLE设备的描述信息)



AD Structure（AdType == 0x09）数据格式解析：

- Length：广播帧的长度， （1 字节）
- AdType：广播帧类型，固定为 0x09 （1 字节）
- DeviceName：广播设备名称，（10 字节）

AD Structure（AdType == 0xFF）数据格式解析：

- Length： （1 字节）广播帧的长度，
- AdType：（1 字节）广播帧类型，固定为 0xFF
- CID： （2 字节）Company Identifiers，0x455A 为萤石公司编码 （EZ 的 ASCll 码）
- VID： （1 字节）蓝牙规范版本号和 Subtype 类型

  bit3～0 ： 当前版本号为 1，值为 0b0001

  bit7～4 ： 0b1000：蓝牙基础类型，mesh 设备 AIS 广播使用此类型

  0b1001：蓝牙 Beacon 类型

  0b1010：蓝牙语音类型

  0b1011：蓝牙 GATT 类型，接入的 BLE 品类设备使用此类型

- FMASK：（1 字节）SDK 提供能力 Function Mask，比如安全、OTA、蓝牙版本、安全广播等，如下图所示：

Bit序	功能说明
1~0	蓝牙版本，00：BLE4.0； 01：BLE4.2；10：BLE5.0；11：BLE5.0以上
2	0：不支持OTA；1：支持OTA
4~3	0：不进行安全认证； 1：进行在线安全认证，2：进行离线安全认证
5	0：一型一密；1：一机一密
6	配网标识，0：未配网；1：已配网
7	保留

注：**1、萤石默认采用一机一密（license 认证）。**

2、配网标识在主动广播包中使用，在扫描响应包中默认为 0

- PID： （6 字节）产品 Product ID，由萤石平台颁发
- MAC： （6 字节）蓝牙设备的 MAC 地址，唯一设备地址。

3. 数据传输规范

3.1 数据格式

不同的蓝牙版本下，支持的数据长度存在差异，当一包数据超过最大长度时，蓝牙无法一次完成数据的传送，所以在发送长数据包时，需要发送时拆包，接收时组包。本协议约定一包数据传输的有效数据长度如下表所示。

BLE 版本	Payload 最大数据长度（Byte）
4.0	20
4.2	244
5.0	244

其中一包数据支持格式如下图所示。

Header	Length	Frame control	SourceMAC	Destination MAC	GroupID	Total fragment	Current fragment	Sequence number	CMD Type	Payload	CRC8
2 Byte	1 Byte	2 Byte	8 Byte	8 Byte	1 Byte	2 Byte	2 Byte	1 Byte	2 Byte	N Byte	1 Byte

帧结构由（Header）、帧控（Frame control）、帧长（Length）、帧序号（Sequence number）、命令类型（CMD Type）、有效数据（Payload）、校验和（CRC8）等部分组成。

数据格式详细定义参考附录 A。

3.2 传输服务与 Characteristics

接入萤石 IOT 平台的设备，需要遵循萤石 IOT 自定义的蓝牙服务与 Characteristics。

- 萤石服务声明为 Primary Service，Service UUID 为 0xFCCC。
- 萤石服务包含以下 5 个 Characteristics。

Characteristics 名称	Characteristics UUID	是否必选	属性	许可权限
Read Characteristics	0xFED4	是	Read	Read
Write Characteristics	0xFED5	是	Read 或 Write	Write
Indicate Characteristics	0xFED6	是	Read 或 Indicate	None
WriteWithNoRsp Characteristics	0xFED7	是	Read 或 Write with No Response	Write
Notify Characteristics	0xFED8	是	Read 或 Notify	None

4. 设备接入认证

安全认证主要用于设备和手机以及网关之间互相校验身份，应用于安全性要求较高的设备或场景，安全认证需要依赖云端能力。使用安全认证的设备，需要将广播的 FMSK 第三个 Bit 位置为 0b01。

手机或者网关在每次连接的时候，会进行安全认证流程。安全认证通过后，手机和

设备的数据传输会通过密文传输。

具体交互流程参考附录 A 中设备接入认证章节。

附录 A

BLE 二进制协议

1. 说明

本二进制协议配合萤石 BLE GATT 协议，封装在 GATT 协议的 payload 中，用于 GATT 设备与手机 APP 交互。

2. 帧结构说明

完整的帧结构如下图所示：

Header	Length	Frame control	SourceMAC	Destination MAC	GroupID	Total fragment	Current fragment	Sequence number	CMD Type	Payload	CRC8
2 Byte	1 Byte	2 Byte	8 Byte	8 Byte	1 Byte	2 Byte	2 Byte	1 Byte	2 Byte	N Byte	1 Byte

帧结构由（Header）、帧控（Frame control）、帧长（Length）、帧序号（Sequence number）、命令类型（CMD Type）、有效数据（Payload）、校验和（CRC8）等部分组成。

2.1 Header

Header 占用 2 个字节，取值固定为 0x55AA。

2.2 Length

Length 占用 1 字节，包含范围为从 frame control 到 CRC8。

2.3 Frame control

帧控占用两个字节，具体划分如下图所示：

opcode	reserved	Source mac include	Destination mac include	Group ID include	Fragment Flag	reserved
3 bit	1 bit	1 bit	1 bit	1 bit	1 bit	8 bit

帧控主要由帧控制码、部分可选字段 flag、协议版本、保留字段等部分组成。

2.3.1 Opcode

opcode 用于指示数据帧的读、写、上报等操作，具体对应关系如下表所示。

如使用定义的 BLE Characteristics，此处可选择为 0b000。

Opcode	Description
0b000	不生效，由 BLE Characteristics 确定数据读写方向

2.3.2 Source mac include

用于指示帧内容中是否包含 source mac，0 表示不包含 source MAC 地址；1 表示包含固定的 source MAC 地址，MAC 地址占用 8 字节。

2.3.3 Destination mac include

用于指示帧内容中是否包含 destination mac，0 表示不包含 destination MAC 地址；1 表示包含固定的 destination MAC 地址，MAC 地址占用 8 字节。

2.3.4 Group ID include

用于指示帧内容中是否包含分组 ID，0 表示不包含分组 ID；1 表示包含分组 ID，内容占用 1 字节。

2.3.5 Fragment Flag

用于指示帧内容中是否包含分片包信息，0 表示不包含分片信息；1 表示包含分片，内容占用 4 字节。

2.4 Source MAC

数据发起的源节点 MAC 地址。

2.5 Destination MAC

数据接收节点的 MAC 地址。

2.6 Group ID

设备分组 ID。

2.7 Total fragment

分片数据包的总大小，占用 2 字节，最大可分为 65535 个包。

2.8 Current fragment

当前分片数据包的编号，占用 2 字节。

2.9 Sequence number

发送的应用层数据的序号，从 0 开始计数，发送新的帧累加，累加溢出后，继续从 0 开始，占用 1 字节。

响应包的 sequence 与对应配置操作的 sequence 是相呼应的。比如打开灯操作对应的 sequence 为 10，开灯结果返回时对应的 sequence 也为 10。

2.10 Cmd type

功能命令，见后面详细定义，占用 2 字节。

2.11 Payload

对应 Cmd type 的数据，见后面详细定义。

2.12 CRC8

CRC8 取值为 frame control 到 Payload 相加值的最低字节，各字节累加和模 256。

3. CMD 类型

Cmd 用于指示一个具体功能操作。当需要向对端赋予数据时，选择写操作，当需要向对端获取数据时，选择读操作。

部分功能定义如下表所示：

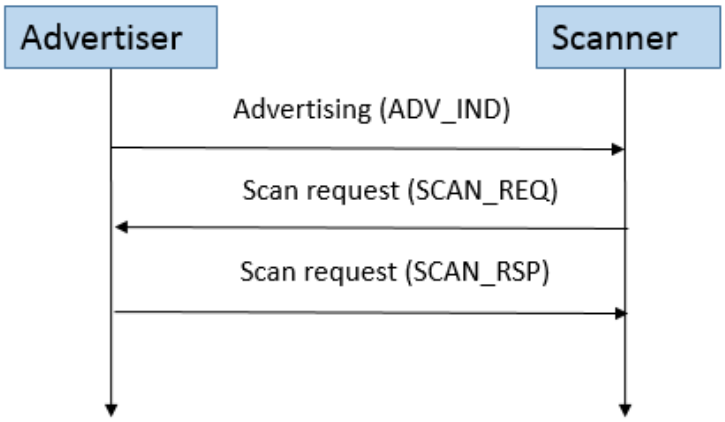
类型	索引	对应 Characteristics 发送/回复	说明
基础功能	0x0000		Reserved
	0x0001	0xFED7/0xFED8	获取设备协议版本号，并回复结果
	0x0002	0xFED7/0xFED8	获取设备固件版本号，并回复结果
	0x0003	0xFED5	恢复出厂设置
	0x0004	0xFED5	设备重启
	0x0005	0xFED7/0xFED8	获取 device name，并回复结果
OTA 升级	0x0300		Reserved
	0x0302	0xFED5	通知设备进入升级模式
	0x0303	0xFED7	向设备发送 OTA 数据
	0x0304	0xFED7/0xFED8	通知设备执行升级，并回复结果
设备接入认证	0x2000		Reserved
	0x2001	0xFED7/0xFED8	APP 获取设备相关信息
	0x2002	0xFED5	APP 发送随机数到设备
	0x2003	0xFED6	设备发送密钥到 APP
	0x2004	0xFED5	APP 下发校验到设备
	0x2005	0xFED6	设备返回认证结果
物模型操作	0x8000		Reserved
	0x8001	0xFED8	属性上报
	0x8002	0xFED7/0xFED8	属性下发，并回复结果
	0x8003	0xFED7/0xFED8	属性获取，并回复结果

4. CMD 数据格式

4.1 设备扫描

4.1.1 交互流程

设备发现阶段交互如下图所示，其中设备作为 advertiser，手机端作为 scanner。



4.1.2 数据交互

假设当前设备为 GATT 设备，MAC 地址为 6f:00:12:35:44:19，设备名称为“EZVIZ GATT”，蓝牙版本为 BLE4.2，支持 OTA，需要进行在线认证，一机一密。具体数据展示如下：

数据块	数据区域	子区域	字节	数据	说明
AD Structure 1	Length		1	0B	
	ADtype		1	09	BLE 规范，固定为 0x09
	Data		10	54 54 41 47 20 5A 49 56 5A 45	devname 最大允许 10 字节，“EZVIZ GATT”小端表示
AD Structure 2	Length		1	0F	
	ADtype		1	FF	BLE 规范，固定为 0xFF
	Data	CID	1	5A 45	0x455A 为萤石公司编码
		VID	1	B1	当前版本版本为 1，值为 0b0001 GATT 类型：0b1011
		FMASK	1	2D	1、版本 BLE4.2，0b01 2、支持 OTA，0b1 3、进行在线安全认证，0b01 4、一机一密，0b1 5、默认为未配网，0b0
		PID	6	66 55 44 33 22 11	固定 6 字节，假设 0x112233445566
		MAC	6	19 44 35 12 00 6F	假设为 MAC 地址为 6f:00:12:35:44:19

因此 ADV_IND 对应的 payload 共 36 字节，共如下：

19 44 35 12 00 6F 0B 09 54 54 41 47 20 5A 49 56 5A 45 0F FF 5A 45 B1 2D 66 55 44 33 22 11 19 44 35 12 00 6F

SCAN_REQ 数据格式无自定义数据，按照 BLE 规范执行。

SCAN_RSP 对应的 payload 与 ADV_IND 一致，如下：

19 44 35 12 00 6F 0B 09 54 54 41 47 20 5A 49 56 5A 45 0F FF 5A 45 B1 2D 66 55 44 33 22 11 19 44 35 12 00 6F

4.2 设备基本操作

4.2.1 CMD（0x0001）获取协议版本

协议版本是指二进制协议版本。

4.2.1.1 发送

ATT value：AA 55 06 00 00 00 01 00 01

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	06	
Frame control	2	00 00	
Sequence number	1	00	帧序号
Cmd type	2	01 00	0x0001
CRC8	1	01	

4.2.1.2 回复

ATT value：AA 55 08 00 00 00 01 00 01 00 02

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	08	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	01 00	0x0001
Payload	2	01 00	协议版本号，占用两个字节，目前为 0x01
CRC8	1	02	

4.2.2 CMD（0x0002）获取固件版本号

固件版本格式为 Vx.y.z build YYMMDD，x/y/z/YY/MM/DD 分别用一个字节表示，比如 V1.1.3 build 210825，表示为 0x01 01 03 15 08 19。

4.2.2.1 发送

ATT value：AA 55 06 00 00 00 02 00 02

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA

Length	1	06	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	02 00	0x0002
CRC8	1	02	

4.2.2.2 回复

ATT value：AA 55 0C 00 00 00 02 00 19 08 15 03 01 01 3D

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	0C	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	02 00	0x0002
Payload	6	19 08 15 03 01 01	假设版本为 V1.1.3 build 210825
CRC8	1	3D	

4.2.3 CMD（0x0003）恢复出厂设置

4.2.3.1 发送

ATT value：AA 55 06 00 00 00 03 00 03

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	06	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	03 00	0x0003
CRC8	1	03	

4.2.3.2 回复

ATT value：AA 55 07 00 00 00 03 00 01 04

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	03 00	0x0003

Payload	1	01	err code ：0x00 配置成功,0x01 配置失败
CRC8	1	04	

4.2.4 CMD（0x0004）设备重启

4.2.4.1 发送

ATT value：AA 55 06 00 00 00 04 00 04

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	06	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	04 00	0x0004
CRC8	1	04	

4.2.4.2 回复

ATT value：AA 55 07 00 00 00 04 00 01 05

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	04 00	0x0004
Payload	1	01	err code ：0x00 配置成功,0x01 配置失败
CRC8	1	05	

4.2.5 CMD（0x0005）获取 device name

设备名称以字符表示，例如“ercbcvne”，表示为 0x65 72 63 62 63 76 6E 65。

4.2.5.1 发送

ATT value：AA 55 06 00 00 00 05 00 05

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	06	
Frame control	2	00 00	
Sequence number	1	00	

Cmd type	2	05 00	0x0005
CRC8	1	05	

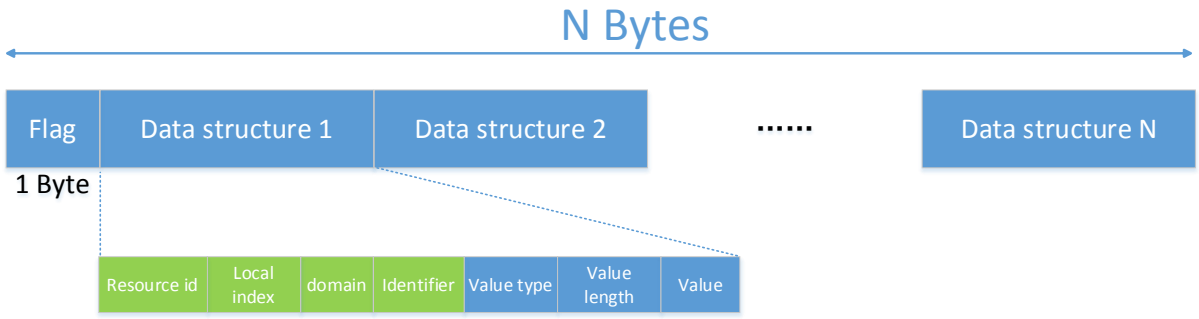
4.2.5.2 回复

ATT value： AA 55 0E 00 00 00 05 00 65 6E 76 63 62 63 72 65 4D

Name	**字节**	**数据**	**说明**
Header	1	AA 55	固定为 0x55AA
Length	1	0E	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	05 00	0x0005
Payload	8	65 6E 76 63 62 63 72 65	“ercbcvne”
CRC8	1	4D	

4.3 物模型数据格式

数据格式包含 1 字节 flag 和数据块如下图所示，其中数据块可以包含多个。



4.3.1 Flag 格式

Flag 占用 1 字节，用于指示 domain、localindex、resourceid、identifier 等字段是否包含在后面数据块中。

Bit	**Name**	**Description**
0	Resourceid include	0 表示不包含，1 表示包含
1	Localindex include	0 表示不包含，1 表示包含
2	Domain include	0 表示不包含，1 表示包含
3	Identifier include	0 表示不包含，1 表示包含
4-7	reserved	

4.3.2 物模型数据格式

协议区域	Name	必备 / 可选	Description
1	Resourceid	可选（flag 指定）	2 字节
2	Localindex	可选（flag 指定）	2 字节
3	Domain	可选（flag 指定）	2 字节
4	Identifier	可选（flag 指定）	2 字节
5	Value type	必备	数据类型，0：bool；1：int；2：double；3：string；4：array；5：object
6	Value length	必备	数据长度
7	Value	必备	具体数据

4.3.3 CMD（0x8001）属性上报

属性上报是指设备当有状态变化时，如有 APP 连接时，主动上报到 APP。

4.3.3.1 发送

ATT value：AA 55 12 00 00 00 01 80 AA 01 01 EF CD AB 90 78 56 34 12 0F 47

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	12	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	01 80	0x8001
Payload	12	AA 01 01 EF CD AB 90 78 56 34 12 0F	Flag：0x0F Domain：0x1234 Localindex：0x5678 Resourceid：0x90AB Identifier：0xCDEF Value type：0x01 Value length：0x01 Value ：0xAA
CRC8	1	47	

4.3.3.2 回复

ATT value：AA 55 12 00 00 00 01 80 00 01 01 EF CD AB 90 78 56 34 12 0F 9D

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	12	
Frame control	2	00 00	
Sequence number	1	00	

Cmd type	2	01 80	0x8001
Payload	12	00 01 01 EF CD AB 90 78 56 34 12 0F	Flag：0x0F Domain：0x1234 Localindex：0x5678 Resourceid：0x90AB Identifier：0xCDEF Value type：0x01 Value length：0x01 Value（errcode） ：00 0x00 配置成功,0x01 配置失败
CRC8	1	9D	

4.3.4 CMD（0x8002）属性下发

属性下发是指当 APP 连接到设备时，APP 修改设备的相关状态。

4.3.4.1 发送

ATT value：AA 55 12 00 00 00 02 80 88 01 01 EF CD AB 90 78 56 34 12 0F 26

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	12	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	02 80	0x8002
Payload	12	88 01 01 EF CD AB 90 78 56 34 12 0F	Flag：0x0F Domain：0x1234 Localindex：0x5678 Resourceid：0x90AB Identifier：0xCDEF Value type：0x01 Value length：0x01 Value ： 0x88
CRC8	1	26	

4.3.4.2 回复

ATT value：AA 55 12 00 00 00 02 80 00 01 01 EF CD AB 90 78 56 34 12 0F 9E

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	12	

Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	02 80	0x8002
Payload	12	00 01 01 EF CD AB 90 78 56 34 12 0F	Flag：0x0F Domain：0x1234 Localindex：0x5678 Resourceid：0x90AB Identifier：0xCDEF Value type：0x01 Value length：0x01 Value（errcode） ：0x00 0x00 配置成功,0x01 配置失败
CRC8	1	9E	

4.3.5 CMD（0x8003）属性获取

属性获取是指当 APP 连接到设备时，主动读取设备中的相关状态属性。

4.3.5.1 发送

ATT value：AA 55 1F 00 00 00 03 80 03 00 03 10 78 56 34 12 02 00 02 10 78 56 23 12 01 00 01 10 89 56 34 12 0F 0A

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	1F	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	03 80	0x8003
Payload	25	03 00 03 10 78 56 34 12 02 00 02 10 78 56 23 12 01 00 01 10 89 56 34 12 0F	Flag：0x0F Domain：0x1234 Localindex：0x5678 Resourceid：0x1001 Identifier：0x0001 Domain：0x1234 Localindex：0x5678 Resourceid：0x1002 Identifier：0x0002 Domain：0x1234 Localindex：0x5678 Resourceid：0x1003 Identifier：0x0003

CRC8	1	0A	

4.3.5.2 回复

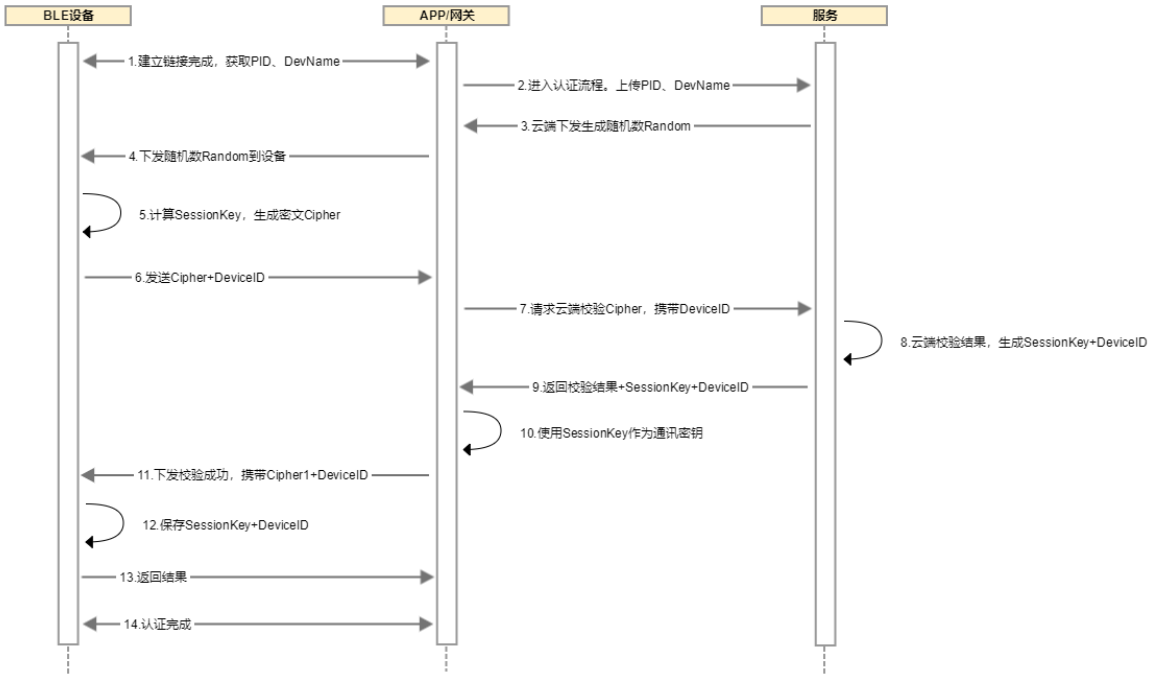
ATT value：AA 55 2B 00 00 00 02 80 33 33 02 01 03 00 03 10 89 56 34 12 22 22 02 01 02 00 02 10 78 56 34 12 11 11 02 01 01 00 01 10 89 56 34 12 0F 00

Name	字节	数据	说明
Header	1	AA 55	
Length	1	2B	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	02 80	0x8003
Payload	37	33 33 02 01 03 00 03 10 89 56 34 12 22 22 02 01 02 00 02 10 78 56 34 12 11 11 02 01 01 00 01 10 89 56 34 12 0F	Flag：0x0F Domain：0x1234 Localindex：0x5678 Resourceid：0x1001 Identifier：0x0001 Value type：0x01 Value length：0x02 Value ： 0x1111 Domain：0x1234 Localindex：0x5678 Resourceid：0x1002 Identifier：0x0002 Value type：0x01 Value length：0x02 Value ： 0x2222 Domain：0x1234 Localindex：0x5678 Resourceid：0x1003 Identifier：0x0003 Value type：0x01 Value length：0x02 Value ： 0x3333
CRC8	1	00	

4.4 GATT 设备接入认证

4.4.1 认证交互流程

BLE 设备通过 GATT 连接到手机 APP 时，认证交互如下图所示：



流程图中部分变量对应的信息如下表所示。

数据字段	名词解释	长度(Byte)	示例
Cipher	认证的密文，Cipher = $AES128_{MasterKey\_Key}$(Random)	16	
Cipher1	认证的密文，Cipher1 = $AES128_{MasterKey\_Key}$(DevName)	16	
DeivceID	设备首次上线时服务颁发的 UUID（需要永久固化 devid，维修和恢复出厂设置都不能擦除。）	32	"RkYmtqD3900QGwW 8te7sPhwwBfxSpr8="
DevName	三元组的 deviceName	12	"ASK6IYFB16V4"
PID	三元组的 ProductKey	6	0x010203040506
Secret	三元组的 deviceLicense	22	"fUUVVg764BeNppujf Hsd8Y"
Random	随机数	16	"drfiHgbsvomOieog"
Session	本次和设备通讯的会话密钥，MD5(Random,PID,DevName,Secret)	16	

4.4.2 CMD（0x2001）APP 获取设备信息

在建立连接之后，APP 向设备发送读请求，获取设备 PID 和 DevName。

Payload 以 TLV 格式组成，具体定义如下表所示。

Name	字节数	Description
Type	1	0x01：PID

		0x02：DevName
Length	1	
Value	N	PID： 16 进制表示，例如为 0x11 22 33 44 55 66 DevName：字符表示，例如 C0123456789A，表示为 0x43 30 31 32 33 34 35 36 37 38 39 41

4.4.2.1 发送

ATT value：AA 55 06 00 00 00 01 20 21

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	06	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	01 20	
CRC8	1	21	

4.4.2.2 回复

ATT value：AA 55 1C 00 00 00 01 20 41 39 38 37 36 35 34 33 32 31 30 43 0C 02 66 55 44 33 22 11 06 01 2C

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	1C	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	01 20	
Payload	22	41 39 38 37 36 35 34 33 32 31 30 43 0C 02 66 55 44 33 22 11 06 01	Type：0x01 Length：0x06 Value：0x11 22 33 44 55 66 Type：0x02 Length：0x0C Value：0x43 30 31 32 33 34 35 36 37 38 39 41
CRC8	1	2C	

4.4.3 CMD（0x2002）APP 下发随机数

APP 向设备发送随机数，随机数由 APP 产生，以字符形式表示。

4.4.3.1 发送

ATT value：AA 55 16 00 00 00 02 20 67 6F 65 69 4F 6D 6F 76 73 62 67 48 69 66 72 64 90

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	16	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	02 20	
Payload	16	67 6F 65 69 4F 6D 6F 76 73 62 67 48 69 66 72 64	例如："drfiHgbsvomOieog" Value：0x64 72 66 69 48 67 62 73 76 6F 6D 4F 69 65 6F 67
CRC8	1	90	

4.4.3.2 回复

ATT value：AA 55 07 00 00 00 02 20 01 23

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	02 20	
Payload	1	01	Value(err code) ： 0x00 成功,0x01 失败
CRC8	1	23	

4.4.4 CMD（0x2003）设备发送密钥

设备端发送数据到 APP，包含 cipher 和 device ID。其中 cipher 生成步骤如下：

1、 首先由 Random、PID、DevName、Secret 通过 MD5 加密生成 Sessionkey。

MD5(drfiHgbsvomOieogqazxswASK6IYFB16V4fUUVVg764BeNppujfHsd8Y)

Name	字节	数据	说明
Random	16	drfiHgbsvomOieog	
PID	6	qazxsw	
DevName	12	ASK6IYFB16V4	
Secret	22	fUUVVg764BeNppujfHsd8Y	
Sessionkey	16	4E8FD966C03FAF7F2EB7AEA13911F094	16 字节，32 个可见字符

2、 然后 Sessionkey 通过 AEC128_ECB（no padding）生成 cipher。

Name	字节	数据	说明
Sessionkey	16	4E8FD966C03FAF7F2EB7AEA13911F094	作为密码
Random	16	drfiHgbsvomOieog	加密文本
cipher	16	cd562e5164973b1f552e5bfde7510318	16 进制表示

Payload 以 TLV 格式组成，具体定义如下表所示。

Name	字节数	Description
Type	1	0x01：cipher 0x02：device ID
Length	1	
Value	N	cipher： 16 进制表示，例如为 0xcd 56 2e 51 64 97 3b 1f 55 2e 5b fd e7 51 03 18 device ID：字符表示，例如 RkYmtqD3900QGwW8te7sPhwwBfxSpr8=，表示为 0x52 6b 59 6d 74 71 44 33 39 30 30 51 47 77 57 38 74 65 37 73 50 68 77 77 42 66 78 53 70 72 38 3d

4.4.4.1 发送

ATT value：AA 55 3A 00 00 00 03 20 3D 38 72 70 53 78 66 42 77 77 68 50 73 37 65 74 38 57 77 47 51 30 30 39 33 44 71 74 6D 59 6B 52 20 02 18 03 51 E7 FD 5B 2E 55 1F 3B 97 64 51 2E 56 CD 10 01 84

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	3A	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	03 20	
Payload	52	3D 38 72 70 53 78 66 42 77 77 68 50 73 37 65 74 38 57 77 47 51 30 30 39 33 44 71 74 6D 59 6B 52 20 02 18 03 51 E7 FD 5B 2E 55 1F 3B 97 64 51 2E 56 CD 10 01	Type：0x01 Length：0x10 Value：0xcd 56 2e 51 64 97 3b 1f 55 2e 5b fd e7 51 03 18 Type：0x02 Length：0x20 Value：0x0x52 6b 59 6d 74 71 44 33 39 30 30 51 47 77 57 38 74 65 37 73 50 68 77 77 42 66 78 53 70 72 38 3d
CRC8	1	84	

4.4.4.2 回复

ATT value：AA 55 07 00 00 00 03 20 01 24

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	03 20	
Payload	1	01	Value(err code) ： 0x00 成功,0x01 失败
CRC8	1	24	

4.4.5 CMD（0x2004）APP 下发密钥校验结果

APP 发送数据到设备端，包含 cipher1 和 device ID。与设备端发送密钥（CMD 0x2003）方式一致。

Payload 以 TLV 格式组成，具体定义如下表所示。

Name	字节数	Description
Type	1	0x01：cipher 0x02：device ID
Length	1	
Value	N	cipher： 16 进制表示，例如为 0x00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF device ID：字符表示。 例如 RkYmtqD3900QGwW8te7sPhwwBfxSpr8=，表示为 0x52 6b 59 6d 74 71 44 33 39 30 30 51 47 77 57 38 74 65 37 73 50 68 77 77 42 66 78 53 70 72 38 3d

4.4.5.1 发送

ATT value：AA 55 3A 00 00 00 04 20 3D 38 72 70 53 78 66 42 77 77 68 50 73 37 65 74 38 57 77 47 51 30 30 39 33 44 71 74 6D 59 6B 52 20 02 FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00 10 01 58

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	3A	
Frame control	2	00 00	
Sequence number	1	00	

Cmd type	2	04 20	0x2004
Payload	52	3D 38 72 70 53 78 66 42 77 77 68 50 73 37 65 74 38 57 77 47 51 30 30 39 33 44 71 74 6D 59 6B 52 20 02 FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00 10 01	Type：0x01 Length：0x10 Value：0x00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF Type：0x02 Length：0x20 Value：0x0x52 6b 59 6d 74 71 44 33 39 30 30 51 47 77 57 38 74 65 37 73 50 68 77 77 42 66 78 53 70 72 38 3d
CRC8	1	58	

4.4.5.2 回复

ATT value：AA 55 07 00 00 00 04 20 01 25

Name	**字节**	**数据**	**说明**
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	04 20	0x2004
Payload	1	01	Value(err code) ： 0x00 成功,0x01 失败
CRC8	1	25	

4.4.6 CMD（0x2005）设备返回认证结果

4.4.6.1 发送

设备端返回认证结果

ATT value：AA 55 07 00 00 00 05 20 01 26

Name	**字节**	**数据**	**说明**
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	05 20	0x2005
Payload	1	01	Value(err code) ： 0x00 成功,0x01 失败
CRC8	1	26	

4.4.6.2 回复

APP 返回认证完成。

ATT value： AA 55 07 00 00 00 05 20 00 25

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	05 20	0x2005
Payload	1	00	Value(err code) ： 0x00 成功,0x01 失败
CRC8	1	25	

4.5 OTA 升级

4.5.1 交互流程

升级总共有以下几个步骤：

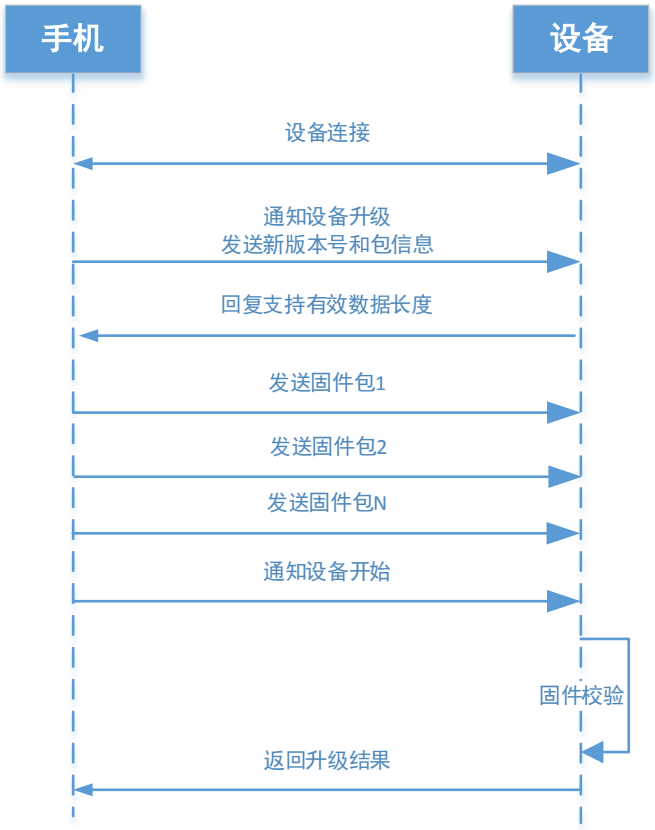
1、 手机 APP 通知设备有新固件可以升级，发送新固件版本号和固件大小信息，

2、 设备回应单包最大支持的数据长度。

3、 手机 APP 分片发送升级数据，直到发送结束。

4、 手机 APP 通知设备开始进行升级操作。

5、 设备对包进行校验后，返回校验结果，然后执行升级。



4.5.2 CMD（0x0301）通知进入升级模式

通知设备进入升级模式，包含新版本号、升级包大小。

Payload 以 TLV 格式组成，具体定义如下表所示。

Name	字节数	Description
Type	1	0x01：表示新版本号 0x02：升级包大小
Length	1	
Value	N	版本号：V1.1.3 build 210825，表示为 0x01 01 03 15 08 19。 升级包大小：1234567（0x12D687）

4.5.2.1 发送

ATT value：AA 55 13 00 00 00 03 20 87 D6 12 04 02 19 08 15 03 01 01 06 01 DA

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	13	
Frame control	2	00 00	

Sequence number	1	00	
Cmd type	2	01 03	0x0301
Payload	13	87 D6 12 04 02 19 08 15 03 01 01 06 01	Type：0x01 Length：0x06 Value：0x01 01 03 15 08 19 Type：0x02 Length：0x04 Value：0x12 D6 87
CRC8	1	DA	

4.5.2.2 回复

ATT value：AA 55 07 00 00 00 01 03 10 14

Name	**字节**	**数据**	**说明**
Header	1	AA 55	固定为 0x55AA
Length	1	09	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	01 03	0x0301
Payload	1	10	回复支持单包最大长度。 0 表示不支持升级。 假设支持最大 16 字节有效 payload
CRC8	1	14	

4.5.3 CMD（0x0302）向设备发送 OTA 数据

主动发送 OTA 数据，分为需要回复响应和不需要回复响应两种。

目前使用 WriteWithNoRsp Characteristics，所以不需要回复响应包。

4.5.3.1 发送

设备固件一般较大，需使用分片发送，此时需要将 frame control 中的 fragment flag 置为 1。以下构造了部分升级包数据：

包 1： ATT value：AA 55 18 00 01 5A 01 00 02 03 FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00 59

Name	**字节**	**数据**	**说明**
Header	1	AA 55	固定为 0x55AA
Length	1	18	

Frame control	2	00 01	报文分片,0x01 00
Total fragment	1	5A	总分片数,
Current fragment	1	00	当前分片序号
Sequence number	1	00	
Cmd type	2	02 03	0x0302
Payload	16	FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00	OTA 数据 0x00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
CRC8	1	59	

包 2： ATT value：AA 55 18 00 01 5A 02 01 02 03 FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00 5B

假设包大小为 1234567，每个包有效数据大小为 16 字节，因此最后一个包的数据长度为 7 字节。

包 5A： ATT value：AA 55 0F 00 01 5A 5A 59 02 03 01 02 03 04 05 06 07 2F

4.5.4 CMD（0x0303）通知设备执行升级

数据发送完成之后，通知设备进行升级操作，设备需要回复升级结果。

4.5.4.1 发送

ATT value：AA 55 06 00 00 00 03 03 06

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	06	
Frame control	2	00 00	
Sequence number	1	00	
Cmd type	2	03 03	0x0303
CRC8	1	06	

4.5.4.2 回复

ATT value：AA 55 07 00 00 00 03 03 00 06

Name	字节	数据	说明
Header	1	AA 55	固定为 0x55AA
Length	1	07	
Frame control	2	00 00	

Sequence number	1	00	
Cmd type	2	03 03	
Payload	1	00	err code：0x00 成功,0x01 失败
CRC8	1	06	