

ACM32WB15 芯片 内置蓝牙模块开发手册

版本: V1.0

日期: 2025-3-10



上海航芯电子科技有限公司

目录

目录.....	2
1. 概述.....	5
1.1. MCU 与蓝牙模块之间的信号	5
1.2. 蓝牙模块上电过程.....	5
2. HCI BOOT 流程.....	6
2.1. UART 通信配置.....	6
2.2. 硬件复位.....	6
2.3. 软件复位.....	6
2.4. 切换波特率	6
2.4.1. MCU 发送切换波特率命令	6
2.4.2. MCU 切换波特率.....	6
2.4.3. 确认波特率切换成功	6
2.5. 下载 patch.....	6
2.6. HCI BOOT 成功进入 HCI 通信阶段	7
3. HCI 通信协议.....	8
3.1. HCI 协议概述.....	8
3.2. UART 通信配置.....	8
3.3. 包格式.....	8
3.4. CMD 命令.....	8
3.4.1. CMD 命令汇总.....	8
3.4.2. HCI_CMD_SET_BT_ADDR (0x00, SPP).....	10
3.4.3. HCI_CMD_SET_BLE_ADDR (0x01, BLE_S).....	10
3.4.4. HCI_CMD_SET_VISIBILITY (0x02, SPP/BLE_S)	10
3.4.5. HCI_CMD_SET_BT_NAME (0x03, SPP).....	11
3.4.6. HCI_CMD_SET_BLE_NAME (0x04, BLE_S).....	11
3.4.7. HCI_CMD_SEND_SPP_DATA (0x05, SPP).....	11
3.4.8. HCI_CMD_SEND_BLE_DATA (0x09, BLE_M/S).....	12
3.4.9. HCI_CMD_STATUS_REQUEST (0x0B, SPP/BLE_S)	12
3.4.10. HCI_CMD_SET_PAIRING_MODE (0x0C, SPP).....	12
3.4.11. HCI_CMD_SET_PINCODE (0x0D, SPP).....	13
3.4.12. HCI_CMD_SET_UART_FLOW (0x0E, SPP/BLE_M/S)	13
3.4.13. HCI_CMD_SET_UART_BAUD (0x0F, SPP/BLE_M/S).....	13
3.4.14. HCI_CMD_VERSION_REQUEST (0x10, SPP/BLE_M/S)	14
3.4.15. HCI_CMD_BT_DISCONNECT (0x11, SPP).....	14
3.4.16. HCI_CMD_BLE_DISCONNECT (0x12, BLE_M/S)	14

3.4.17. HCI_CMD_BLE_SCAN (0x14, BLE_M).....	15
3.4.18. HCI_CMD_SET_NVRAM (0x26, SPP/BLE_M).....	15
3.4.19. HCI_CMD_CONFIRM_GKEY (0x28, SPP/BLE_M).....	16
3.4.20. HCI_CMD_SET_CREDIT_GIVEN (0x29, SPP).....	16
3.4.21. HCI_CMD_AUTO_ADV_SCAN (0x2A, BLE_S).....	16
3.4.22. HCI_CMD_POWER_REQ (0x2B, SPP/BLE_M/S).....	17
3.4.23. HCI_CMD_POWER_SET (0x2C, SPP/BLE_M/S).....	17
3.4.24. HCI_CMD_PASSKEY_ENTRY (0x30, BLE_S).....	17
3.4.25. HCI_CMD_LE_SET_PAIRING(0x33, BLE_S).....	18
3.4.26. HCI_CMD_LE_SET_ADV_DATA (0x34, BLE_S).....	19
3.4.27. HCI_CMD_LE_SET_SCAN_DATA (0x35, BLE_S).....	19
3.4.28. HCI_CMD_LE_SEND_CONN_UPDATE_REQ (0x36, BLE_S).....	19
3.4.29. HCI_CMD_LE_SET_ADV_PARM (0x37, BLE_S).....	20
3.4.30. HCI_CMD_LE_START_PAIRING (0x38, BLE_S).....	20
3.4.31. HCI_CMD_SET_TX_POWER (0x42, SPP/BLE_M/S).....	20
3.4.32. HCI_CMD_LE_CONFIRM_GKEY (0x48, BLE_S).....	21
3.4.33. HCI_CMD_REJECT_JUSTWORK (0x49, BLE_S).....	21
3.4.34. HCI_CMD_RESET_CHIP_REQ (0x51, SPP/BLE_M/S).....	21
3.4.35. HCI_CMD_LE_SET_FIXED_PASSKEY (0x61, BLE_S).....	22
3.4.36. HCI_CMD_DELETE_CUSTOMIZE_SERVICE (0x76, BLE_S).....	22
3.4.37. HCI_CMD_ADD_SERVICE_UUID (0x77, BLE_S).....	22
3.4.38. HCI_CMD_ADD_CHARACTERISTIC_UUID (0x78, BLE_S).....	23
3.4.39. HCI_CMD_BLE_CREATE_CONN (0x7B, BLE_M).....	23
3.4.40. HCI_TEST_CMD_CLOSE_LPM (0xFF, SPP/BLE_M/S).....	24
3.5. EVENT 事件.....	24
3.5.1. EVENT 事件汇总.....	24
3.5.2. HCI_EVENT_SPP_CONN_REP (0x00, SPP).....	25
3.5.3. HCI_EVENT_LE_CONN_REP (0x02, BLE_S).....	25
3.5.4. HCI_EVENT_SPP_DIS_REP (0x03, SPP).....	25
3.5.5. HCI_EVENT_LE_DIS_REP (0x05, BLE_S).....	26
3.5.6. HCI_EVENT_CMD_RES (0x06, SPP/BLE_M/S).....	26
3.5.7. HCI_EVENT_SPP_DATA_REP (0x07, SPP).....	26
3.5.8. HCI_EVENT_LE_DATA_REP (0x08, BLE_M/S).....	27
3.5.9. HCI_EVENT_STANDBY_REP (0x09, BLE_M/S).....	27
3.5.10. HCI_EVENT_STATUS_RES (0x0A, BLE_S).....	27
3.5.11. HCI_EVENT_NVRAM_REP (0x0D, BLE_S).....	28
3.5.12. HCI_EVENT_GKEY (0x0E, BLE_S).....	28

3.5.13. HCI_EVENT_INVALID_PACKET (0x0F, SPP/BLE_M/S)	28
3.5.14. HCI_EVENT_GET_PASSKEY (0x10, BLE_S).....	28
3.5.15. HCI_EVENT_LE_TK (0x11, BLE_S)	29
3.5.16. HCI_EVENT_LE_PAIRING_STATE (0x14, BLE_S)	29
3.5.17. HCI_EVENT_LE_ENCRYPTION_STATE (0x15, BLE_S)	29
3.5.18. HCI_EVENT_LE_GKEY (0x1D, BLE_S)	30
3.5.19. HCI_EVENT_UUID_HANDLE (0x29, BLE_S)	30
3.5.20. HCI_EVENT_SCAN_RES (0x2A, BLE_M).....	30
3.5.21. HCI_EVENT_SERVICE_RES (0x50, BLE_M)	31
3.5.22. HCI_EVENT_CHARACTER (0x51, BLE_M)	32
3.6. BLE 属性列表	32
4. 版本历史	34
5. 版权声明	35

1. 概述

ACM32WB15 芯片内置蓝牙模块，支持 BT3.0 模式 (BR) 以及 BLE5.2 标准协议，支持 SPP 协议，支持低功耗模式。

MCU 与蓝牙模块之间 UART 进行通信，通信协议采用 HCI 协议。

1.1. MCU 与蓝牙模块之间的信号

芯片引脚	MCU 信号	蓝牙模块信号	方向	描述
内部信号互联	PA9/UART1_TX	BT_RX	MCU 到蓝牙	串口发送信号
内部信号互联	PA10/UART1_RX	BT_TX	蓝牙到 MCU	串口接收信号
内部信号互联	PC6	BT_INT	蓝牙到 MCU	蓝牙模块输出的中断信号，暂未使用
内部信号互联	PC7	BT_LPM	MCU 到蓝牙	蓝牙模块低功耗模式控制，有效电平可配置
Pin 1		BT_NRST	外部输入	复位蓝牙模块，低电平有效，复位信号释放后，需要等待 100ms 左右，才能进行通信

1.2. 蓝牙模块上电过程

蓝牙模块上电或复位后，需要经过 HCI BOOT 流程，才能进入 HCI 通信阶段。

2. HCI BOOT 流程

2.1. UART 通信配置

HCI Boot 功能基于 UART 硬件接口。默认配置如下：

波特率：115200；数据位：8；停止位：1；校验位：无；流控：无

2.2. 硬件复位

蓝牙模块上电后，需要等待 100ms，才能接收 MCU 的命令。

硬件复位（BT_RST 输出 10ms 低脉冲）后，也需要等待 100ms，才能接收 MCU 的命令。

2.3. 软件复位

MCU 发送：HCI_CMD_BT_RESET (01 00 fc 00)

BT 回复：HCI_EVENT_COMMAND_COMPLETE (04 0E 04 01 00 FC 00)

2.4. 切换波特率

2.4.1. MCU 发送切换波特率命令

MCU 发送：HCI_CMD_BT_BAUD (01 02 fc 02 LL HH)

BT 无回复。

如后续使用默认波特率则可跳过此步骤。其中，LL 是 baud_param 的低 8bit，HH 是 baud_param 的高 8bit。

计算方法：

$\text{baud_param} = 24000000/\text{baudrate}$

例如：115200 波特率：

$\text{baud_param} = 24000000/115200 = 208 = 0xD0$

则发送 (01 02 fc 02 D0 00)

2.4.2. MCU 切换波特率

MCU 自行切换至设置的波特率。

2.4.3. 确认波特率切换成功

MCU 发送：HCI_CMD_BT_ECHO: (01 05 fc 00)

BT 回复：HCI_EVENT_COMMAND_COMPLETE (04 0E 04 01 05 FC 00)

2.5. 下载 patch

Patch 在发布时会打包成数组，Patch 中包含多条 HCI_CMD，MCU 只需逐条读出并从 UART 上发出即可。注意：发送每条 HCI_CMD 后 BT 都会回复 HCI_EVENT_COMMAND_COMPLETE，请等待收到此 Event 后再发送新的 CMD，以保证数据可靠性。

Patch 的结构如下:

```
Struct patch{
u16_t total_len;      //Patch 总长度, 包括 len0-cmdN 的长度
u8_t len0;           //cmd0 长度
u8_t cmd0[len0];     //cmd0 数据
u8_t len1;           //cmd1 长度
u8_t cmd1[len1];     //cmd1 数据
u8_t len2;           //cmd2 长度
u8_t cmd2[len2];     //cmd2 数据
...
...
...
u8_t lenN;           //cmdN 长度
u8_t cmdN[lenN];    //cmdN 数据
}
```

2.6. HCI BOOT 成功进入 HCI 通信阶段

3. HCI 通信协议

3.1. HCI 协议概述

MCU 和蓝牙模块之间的 UART 通信协称为 HCI 协议，格式类似于蓝牙标准 HCI 协议。

MCU 发送给模块的包称为 CMD (命令)，MCU 通过发送 CMD 来完成配置蓝牙、控制蓝牙连接、发送数据等操作。

模块发送给 MCU 的包称为 EVENT (事件)，模块通过发送 EVENT 来完成通知蓝牙状态变化、上报数据等操作。

模块接收到每个 CMD 后都会回复一个与之对应的 EVENT 作为回应 (通常为 HCI_EVENT_CMD_RES)。此机制应作为软件流控机制处理。即，MCU 发送 CMD 后应等待一个与之对应的 EVENT，收到此 EVENT 后再发送新的 CMD。

模块上电/复位初始化完成后会发送 HCI_EVENT_I_AM_READY 来通知 MCU 自己已经准备好可以开始工作。MCU 需要收到此 EVENT 后方可发送第一个 CMD。

HCI 包为小端传输，即低字节先传输。

MCU 通过 UART 发送数据前，必须保证“BT_LPM”信号为唤醒电平并保持 5ms 以上。发送完毕后方可切换为低功耗电平。

3.2. UART 通信配置

MCU 与蓝牙模块之间采用 UART 进行通信，默认配置如下：

波特率：115200；数据位：8；停止位：1；校验位：无；流控：无

3.3. 包格式

Byte0	Byte1	Byte2	Byte3~ Byte(length+3)
Packet Type	Opcode	Length	Payload
包类型	操作码	内容长度	内容

HCI 包结构如上表所示

- Packet Type: 包类型，0x01 表示 CMD，0x02 表示 Event
- Opcode: 操作码，指示不同 CMD 和 Event 指令
- Length: 内容长度
- Payload: 包内容

3.4. CMD 命令

3.4.1. CMD 命令汇总

CMD	Opcode	描述	支持协议
-----	--------	----	------

HCI_CMD_SET_BT_ADDR	0x00	设置 BT3.0 地址	SPP
HCI_CMD_SET_BLE_ADDR	0x01	设置 BLE 地址	BLE_S
HCI_CMD_SET_VISIBILITY	0x02	设置可发现和广播	BLE_S
HCI_CMD_SET_BT_NAME	0x03	设置 BT3.0 名称	SPP
HCI_CMD_SET_BLE_NAME	0x04	设置 BLE 名称	BLE_S
HCI_CMD_SEND_SPP_DATA	0x05	发送 BT3.0 数据	SPP
HCI_CMD_SEND_BLE_DATA	0x09	发送 BLE 数据	BLE_M/S
HCI_CMD_STATUS_REQUEST	0x0B	请求蓝牙状态	SPP/BLE_S
HCI_CMD_SET_PAIRING_MODE	0x0C	设置配对模式	SPP
HCI_CMD_SET_PINCODE	0x0D	设置配对码	SPP
HCI_CMD_SET_UART_FLOW	0x0E	设置 UART 流控	SPP/BLE_M/S
HCI_CMD_SET_UART_BAUD	0x0F	设置 UART 波特率	SPP/BLE_M/S
HCI_CMD_VERSION_REQUEST	0x10	查询模块固件版本	SPP/BLE_M/S
HCI_CMD_BT_DISCONNECT	0x11	断开 BT3.0 连接	SPP
HCI_CMD_BLE_DISCONNECT	0x12	断开 BLE 连接	BLE_M/S
HCI_CMD_BLE_SCAN	0x14	BLE 扫描广播	BLE_M
HCI_CMD_SET_NVRAM	0x26	下发 NVRAM 数据	SPP/BLE_M/S
HCI_CMD_CONFIRM_GKEY	0x28	Numeric Comparison 配对方式中对密钥的比较	SPP/BLE_M
HCI_CMD_SET_CREDIT_GIVEN	0x29	设置 Spp 流控	SPP
HCI_CMD_SET_ADV_DATA	0x2A	设置 ADV 数据	BLE_S
HCI_CMD_POWER_REQ	0x2B	查询模块电源电压	SPP/BLE_M/S
HCI_CMD_POWER_SET	0x2C	读取电源电压功能开	SPP/BLE_M/S
HCI_CMD_PASSKEY_ENTRY	0x30	输入 Passkey	BLE_S
HCI_CMD_LE_SET_PAIRING	0x33	设置配对模式	BLE_S
HCI_CMD_LE_SET_ADV_DATA	0x34	设置 adv 数据	BLE_S
HCI_CMD_LE_SET_SCAN_DATA	0x35	设置 scan 数据	BLE_S
HCI_CMD_LE_SEND_CONN_UPDATE_REQ	0x36	更新连接参数	BLE_S
HCI_CMD_LE_SET_ADV_PARM	0x37	设置广播参数	BLE_S
HCI_CMD_LE_START_PAIRING	0x38	开始配对	BLE_S
HCI_CMD_SET_TX_POWER	0x42	设置发射功率	SPP/BLE_M/S
HCI_CMD_LE_CONFIRM_GKEY	0x48	BLE Numeric Comparison 配对密钥确认	BLE_S
HCI_CMD_REJECT_JUSTWORK	0x49	拒绝 Justwork 配对方式	BLE_S
HCI_CMD_RESET_CHIP_REQ	0x51	复位芯片	SPP/BLE_M/S

HCI_CMD_LE_SET_FIXED_PASSKEY	0x61	设置固定的 passkey	BLE_S
HCI_CMD_DELETE_CUSTOMIZE_SERVICE	0x76	删除 BLE 非系统服务及特征	BLE_S
HCI_CMD_ADD_SERVICE_UUID	0x77	增加 BLE 自定义服务	BLE_S
HCI_CMD_ADD_CHARACTERISTIC_UUID	0x78	增加 BLE 自定义特征	BLE_S
HCI_CMD_BLE_CREATE_CONN	0x7b	LE 建立连接	BLE_M
HCI_TEST_CMD_CLOSE_LPM	0xFF	关闭 LPM	SPP/BLE_M/S

3.4.2. HCI_CMD_SET_BT_ADDR (0x00, SPP)

HCI_CMD_SET_BT_ADDR 用于设置 BT3.0 设备地址，操作码 0x00。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x00
Length	Byte2	0x06
Payload	Byte3~Byte8	BT3.0 地址 (小端格式)

3.4.3. HCI_CMD_SET_BLE_ADDR (0x01, BLE_S)

HCI_CMD_SET_BLE_ADDR 用于设置 BLE 设备地址，操作码 0x01。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x01
Length	Byte2	0x06
Payload	Byte3~Byte8	BLE 设备地址 (小端格式)

3.4.4. HCI_CMD_SET_VISIBILITY (0x02, SPP/BLE_S)

HCI_CMD_SET_VISIBILITY 用于设置蓝牙的可发现和广播状态，操作码 0x02。Payload 中 Bit0 表示 BT3.0 可发现 (可以被搜索)，Bit1 表示 BT3.0 可连接 (可以被连接)，没有特殊需求时这两位开关应设为同样值，即取为 00B 或 11B。Bit2 表示 BLE 可发现，BLE 在可发现状态下可以被搜索和连接，同时会发送 ADV 广播包。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x02
Length	Byte2	0x01
Payload	Byte3	Bit0: BT3.0 可发现 Bit1: BT3.0 可连接 Bit2: BLE 可发现 (ADV 广播)

3.4.5. HCI_CMD_SET_BT_NAME (0x03, SPP)

HCI_CMD_SET_BT_NAME 用于设置 BT3.0 的蓝牙设备名称，操作码为 0x03。命令长度根据蓝牙设备名称长度而定，最大长度为 32byte。蓝牙设备名称是以 ASCII 编码的字符串。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x03
Length	Byte2	0x01~0x20
Payload	Byte3 ~Byte (Length+3)	蓝牙设备名称

3.4.6. HCI_CMD_SET_BLE_NAME (0x04, BLE_S)

HCI_CMD_SET_BLE_NAME 用于设置 BLE 的蓝牙设备名称，操作码为 0x04。命令长度根据蓝牙设备名称长度而定，最大长度为 24byte。蓝牙设备名称是以 ASCII 编码的字符串。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x04
Length	Byte2	0x01~0x18
Payload	Byte3 ~Byte (Length+3)	蓝牙设备名称

3.4.7. HCI_CMD_SEND_SPP_DATA (0x05, SPP)

HCI_CMD_SEND_SPP_DATA 用于发送 BT3.0 数据 (SPP 协议)，操作码为 0x05。每个 SPP 数据包的长度小于等于 127 时可以达到最佳的数据吞吐率。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x05
Length	Byte2	0x01~0xFF (推荐小于 127)
Payload	Byte3 ~Byte (Length+3)	BT3.0 数据 (SPP 协议)

3.4.8. HCI_CMD_SEND_BLE_DATA (0x09, BLE_M/S)

HCI_CMD_SEND_BLE_DATA 用于发送 BLE 数据 (GATT 协议)，操作码为 0x09。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x09
Length	Byte2	0x01~0xFF
Payload	Byte3~Byte4	Attribute Handle, 默认 0x0E 0x00
	Byte5 ~Byte (Length+3)	BLE 数据 (GATT 协议)

3.4.9. HCI_CMD_STATUS_REQUEST (0x0B, SPP/BLE_S)

HCI_CMD_STATUS_REQUEST 用于请求蓝牙状态，操作码为 0x0B。

模块收到此命令后会回复 HCI_EVENT_STATUS_RES。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0B
Length	Byte2	0x00

3.4.10. HCI_CMD_SET_PAIRING_MODE (0x0C, SPP)

HCI_CMD_SET_PAIRING_MODE 用于设置 BT3.0 的配对方式，操作码为 0x0C。模块默认配对模式为 0x01 Just Work (SSP)。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
----	----	----

CMD	Byte0	0x01
Opcode	Byte1	0x0C
Length	Byte2	0x01
Payload	Byte3	0x00: pin code 0x01: just work 0x02: passkey 0x03: confirm

3.4.11. HCI_CMD_SET_PINCODE (0x0D, SPP)

HCI_CMD_SET_PINCODE 用于设置 BT3.0 的配对 PIN 码，操作码为 0x0D。模块默认配对 PIN 码为 0x30 0x30 0x30 0x30

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0D
Length	Byte2	0x01~0x10
Payload	Byte3~Byte(Length+2)	Pincode

3.4.12. HCI_CMD_SET_UART_FLOW (0x0E, SPP/BLE_M/S)

HCI_CMD_SET_UART_FLOW 用于设置 UART 流控，操作码为 0x0E。0x00 为关闭 UART 流控，0x01 为开启 UART 流控。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0E
Length	Byte2	0x01
Payload	Byte3	0x00: 关闭 UART 流控 0x01: 开启 UART 流控

3.4.13. HCI_CMD_SET_UART_BAUD (0x0F, SPP/BLE_M/S)

HCI_CMD_SET_UART_BAUD 用于设置 UART 波特率，操作码为 0x0F。UART 波特率默认为 115200，最大 1Mbps。设置波特率时将波特率数字用 ASCII 编码字符串输入。例如：设置 921600 波特率，完整的包为“01 0F 06 39 32 31 36 30 30”。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。此 回复将基于新波特率发送。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0F
Length	Byte2	0x01~0x07
Payload	Byte3	波特率 (ASCII 编码字符串)

3.4.14. HCI_CMD_VERSION_REQUEST (0x10, SPP/BLE_M/S)

HCI_CMD_VERSION_REQUEST 用于查询模块固件版本，操作码为 0x10。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x02，回复内容为固件版本号：1~65535。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x10
Length	Byte2	0x00

3.4.15. HCI_CMD_BT_DISCONNECT (0x11, SPP)

HCI_CMD_BT_DISCONNECT 用于断开 BT3.0 (SPP 协议) 连接，操作码为 0x11。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x11
Length	Byte2	0x00

3.4.16. HCI_CMD_BLE_DISCONNECT (0x12, BLE_M/S)

HCI_CMD_BT_DISCONNECT 用于断开 BLE 连接，操作码为 0x12。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01

Opcode	Byte1	0x12
Length	Byte2	0x00

3.4.17. HCI_CMD_BLE_SCAN (0x14, BLE_M)

用于开始扫描数据，操作码为 0x14。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容 02 06 02 14 00

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x14
Length	Byte2	0x01
Payload	Byte3	0x00：表示关闭扫描 0x01：表示开启扫描

3.4.18. HCI_CMD_SET_NVRAM (0x26, SPP/BLE_M)

该命令用于设置 NVRAM 数据。

蓝牙模块在掉电时需要保存一些数据，要求 MCU 开辟一块非易失存储器（如 FLASH）帮助模块保存数据，这段存储器称为 NVRAM。模块在需要保存数据时发送 HCI_EVENT_NVRAM_REP 将数据发至 MCU，MCU 则在上电后使用 HCI_CMD_SET_NVRAM 命令将数据发送给模块。MCU 不用关心模块存储数据的内容。

NVRAM 信息 34 字节一组，一共 5 组，共 170 字节。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x26
Length	Byte2	0xAA
Payload	Byte3~Byte172	NVRAM 数据(170Byte)

NVRAM 格式说明：

描述	位置	取值		
设备编号	Byte0	设备编号		
类型	Byte1	0x35	0x36	0x37
数据 1	Byte2~ Byte17	Master address (不足)	IRK	8byte:Ediv 8byte:IRK
数据 2	Byte18~Byte33	Long Term	Long Term	Long Term

*设备编号表示连接的先后顺序，最新(配对)连接或配对后再连(接的)设备，设备编号为(00,)其他设备编号依次是 01, 02, 03

3.4.19. HCI_CMD_CONFIRM_GKEY (0x28, SPP/BLE_M)

HCI_CMD_CONFIRM_GKEY 用于 Numeric Comparison 配对方式中对密钥的比较，收到 HCI_EVENT_GKEY 事件后返回。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x28
Length	Byte2	0x01
Payload	Byte3	0x00：密钥匹配 0x01：密钥不匹配

3.4.20. HCI_CMD_SET_CREDIT_GIVEN (0x29, SPP)

HCI_CMD_SET_CREDIT_GIVEN 用于设置 spp 流控(并非开启)，操作码为 0x29。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x29
Length	Byte2	0x01
Payload	Byte3	流控的增加值

3.4.21. HCI_CMD_AUTO_ADV_SCAN (0x2A, BLE_S)

HCI_CMD_AUTO_ADV_SCAN 用于设置 BLE ADV DATA。当 ADV Data 长度大于 31 字节 时，模块会将超出部分（按照 ADV Data 格式）放置在 Scan Resp Data 中。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x2A
Length	Byte2	0x01~0x3E
Payload	Byte3~ Byte(Length-3)	ADV Data

3.4.22. HCI_CMD_POWER_REQ (0x2B, SPP/BLE_M/S)

HCI_CMD_POWER_REQ 用于查询模块电源电压，操作码为 0x2b。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x02，回复内容为 2 个的 byte 的电压值。2 个 byte 为定点数，第一个 byte 为电压值的整数部分，第二个 byte 为电压值的小数部分，2 个 byte 都为十六进制。例 03 22 为 3.34V。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x2B
Length	Byte2	0x00

3.4.23. HCI_CMD_POWER_SET (0x2C, SPP/BLE_M/S)

HCI_CMD_POWER_SET 用于设置模块读取电源电压功能开关，操作码为 0x2C。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x2C
Length	Byte2	0x01
Payload	Byte3	0x00：关闭电压检测 0x01：开启电压检测

3.4.24. HCI_CMD_PASSKEY_ENTRY (0x30, BLE_S)

HCI_CMD_PASSKEY_ENTRY 用于输入 Passkey，操作码为 0x30。

例如手机上显示 779603，十进制数 779603 转换为 UINT32 的数为 0x000be553，大小端转换下，即 0x53 0xE5 0x0B 0x00

则应当发送的指令为：01 30 04 53 E5 0B 00。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x30
Length	Byte2	0x04
Payload	Byte3~Byte6	Passkey Data

3.4.25. HCI_CMD_LE_SET_PAIRING(0x33, BLE_S)

HCI_CMD_LE_SET_PAIRING 设置 BLE 配对模式。

模块收到此命令后会回复 HCI_EVENT_CMD_RES, 回复内容长度为 0x00 。

命令格式如下:

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x33
Length	Byte2	0x02
Payload	Byte3	0x00 (默认): LE_PAIRING_NONE: 不加密 0x01: LE_PAIRING_JUSTWORK: 加密, 用户不需要操作, NO MITM 0x02: LE_PAIRING_PASSKEY: 需要手机输入验证码并确认, 支持 MITM 0x81: LE_PAIRING_SECURE_CONNECT_JUSTWORK: 具有 SC 属性的加密, 用户不需要操作, NO MITM 0x82: LE_PAIRING_SECURE_CONNECT_NUMERIC: 具有 SC 属性数字比对的配对模式, 手机和设备显示确认码, 用户确认是否相同 0x83: LE_PAIRING_SECURE_CONNECT_PASSKEY: 具有 SC 属性的配对模式, 需要手机输入验证码并确认, 支持 MITM

加密相关返回的 EVENT:

1) LE_PAIRING_JUSTWORK:

先返回 HCI_EVENT_LE_PAIRING_STATE, 通知 MCU 配对状态,
再返回 HCI_EVENT_LE_ENCRYPTION_STATE 通知 MCU 加密状态,
最后再返回配对成功 HCI_EVENT_NVRAM_REP, 包含配对信息。

2) LE_PAIRING_PASSKEY:

先返回 HCI_EVENT_LE_TK, 包含输入 passkey 信息,
然返回 HCI_EVENT_LE_PAIRING_STATE 通知 MCU 配对状态,
再返回 HCI_EVENT_LE_ENCRYPTION_STATE 通知 MCU 加密状态,
配对成功后返回 HCI_EVENT_NVRAM_REP, 包含配对信息。

3) LE_PAIRING_SECURE_CONNECT_JUSTWORK:

先返回 HCI_EVENT_LE_PAIRING_STATE 通知 MCU 配对状态,
再返回 HCI_EVENT_LE_ENCRYPTION_STATE 通知 MCU 加密状态,
后再返回配对成功 HCI_EVENT_NVRAM_REP, 包含配对信息。

4) LE_PAIRING_SECURE_CONNECT_NUMERIC: BLE 4.2 加密, 为数字比较方式, 手机和设备显示确认码, 用户确认是否相同。

5) LE_PAIRING_SECURE_CONNECT_PASSKEY:

先返回 HCI_EVENT_LE_TK, 包含输入 passkey 信息,
 然后返回 HCI_EVENT_LE_PAIRING_STATE 通知 MCU 配对状态,
 再返回 HCI_EVENT_LE_ENCRYPTION_STATE 通知 MCU 加密状态,
 配对成功后返回 HCI_EVENT_NVRAM_REP, 包含配对信息。

3.4.26. HCI_CMD_LE_SET_ADV_DATA (0x34, BLE_S)

HCI_CMD_LE_SET_ADV_DATA 用于设置 BLEADV DATA 。ADV Data 长度为 31。

ADV Data 可能包含 BLE 名字, HCI_CMD_SET_BLE_NAME 会自动更新 ADV Data, 所以 ADV Data 要在设置 BLE 名字之后设置。

模块收到此命令后会回复 HCI_EVENT_CMD_RES, 回复内容长度为 0x00 。

命令格式如下:

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x34
Length	Byte2	Length < 0x20
Payload	Byte3~Byte(Length-3)	Adv Data 数据

3.4.27. HCI_CMD_LE_SET_SCAN_DATA (0x35, BLE_S)

HCI_CMD_LE_SET_SCAN_DATA 用于设置 Scan Data, Scan Data 长度为 31。

Scan Data 可能包含 BLE 名字, HCI_CMD_SET_BLE_NAME 会自动更新 Scan Data, 所以 Scan Data 要在设置 BLE 名字之后设置。

模块收到此命令后会回复 HCI_EVENT_CMD_RES, 回复内容长度为 0x00。

命令格式如下:

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x35
Length	Byte2	Length < 0x20
Payload	Byte3~Byte (Length-3)	Scan Data 数据

3.4.28. HCI_CMD_LE_SEND_CONN_UPDATE_REQ (0x36, BLE_S)

HCI_CMD_LE_SEND_CONN_UPDATE_REQ 用于设置 CONNECTION PARAMETER UPDATE REQUEST 数据并发送。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x36
Length	Byte2	0x08
Payload	Byte3~Byte4	interval min: (最小单位 1.25ms)
	Byte5~Byte6	Le interval max (最小单位 1.25ms)
	Byte7~Byte8	Slave latency (最大忽略 30 个包)
	Byte9~Byte10	Timeout (最小单位 10ms)

3.4.29. HCI_CMD_LE_SET_ADV_PARM (0x37, BLE_S)

HCI_CMD_LE_SET_ADV_PARM 用于设置 ADVR 的间隔和持续的时间，操作码为 0x37。单位为 0.625ms，小端模式。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x37
Length	Byte2	0x02
Payload	Byte3~Byte4	ADV 间隔 (时间单位 0.625ms)

3.4.30. HCI_CMD_LE_START_PAIRING (0x38, BLE_S)

HCI_CMD_LE_START_PAIRING 用于开始配对，操作码为 0x38。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x38
Length	Byte2	0x00

3.4.31. HCI_CMD_SET_TX_POWER (0x42, SPP/BLE_M/S)

HCI_CMD_SET_TX_POWER 用于设置发射功率，操作码为 0x42。有五个功率档位可选。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x42
Length	Byte2	0x01
Payload	Byte4	发射功率档位: 0x00: 0dB (默认) 0x01: 3dB 0x02: 5dB 0x03: -3dB 0x04: -5dB

3.4.32. HCI_CMD_LE_CONFIRM_GKEY (0x48, BLE_S)

HCI_CMD_LE_CONFIRM_GKEY 用于 Numeric Comparison 配对方式中对密钥的比较, 收到 HCI_EVENT_GKEY 事件后返回。

模块收到此命令后会回复 HCI_EVENT_CMD_RES, 回复内容长度为 0x00。

命令格式如下:

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x48
Length	Byte2	0x01
Payload	Byte4	0x00: 密钥匹配 0x01: 密钥不匹配

3.4.33. HCI_CMD_REJECT_JUSTWORK (0x49, BLE_S)

HCI_CMD_REJECT_JUSTWORK 用于设置拒绝 Justwork 配对方式 (用于 PCI 认证), 操作码为 0x49。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x49
Length	Byte2	0x01
Payload	Byte4	0x00: 关闭拒绝 Justwork 0x01: 打开拒绝 Justwork

3.4.34. HCI_CMD_RESET_CHIP_REQ (0x51, SPP/BLE_M/S)

HCI_CMD_RESET_CHIP_REQ 用于复位芯片, 操作码为 0x51。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x51
Length	Byte2	0x00

3.4.35. HCI_CMD_LE_SET_FIXED_PASSKEY (0X61, BLE_S)

HCI_CMD_LE_SET_FIXED_PASSKEY 用于设置 Passkey, 操作码为 0x61。

例如, 设置固定 Passkey 为 123456, 十进制 123456 转换为 UINT32 的数 0x0001e240 ->小端模式 0x40 0xE2 0x01 0x00

指令应当发送 01 61 05 01 40 E2 01 00

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x61
Length	Byte2	0x05
Payload	Byte3	0x00: 随机 Passkey 0x01: 自定义 Passkey
	Byte4~Byte7	Passkey

3.4.36. HCI_CMD_DELETE_CUSTOMIZE_SERVICE (0x76, BLE_S)

HCI_CMD_DELETE_CUSTOMIZE_SERVICE 用于删除非系统服务及特征, 操作码为 0x76。

模块收到此命令后会回复 HCI_EVENT_CMD_RES, 回复内容长度为 0x00。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x76
Length	Byte2	0x00

3.4.37. HCI_CMD_ADD_SERVICE_UUID (0x77, BLE_S)

HCI_CMD_ADD_SERVICE_UUID 用于新增自定义服务, 操作码为 0x77。

模块收到此命令后会回复 HCI_EVENT_UUID_HANDLE, 回复内容长度 0x02, 回复内容为新增 Service 的 Handle。

命令格式如下:

描述	位置	取值
CMD	Byte0	0x01

Opcode	Byte1	0x77
Length	Byte2	Payload Length
Payload	Byte3	UUID LENGTH
	Byte4~Byte4+length	Service UUID(小端模式)

3.4.38. HCI_CMD_ADD_CHARACTERISTIC_UUID (0x78, BLE_S)

HCI_CMD_ADD_CHARACTERISTIC_UUID 用于新增特征，操作码为 0x78。

模块收到此命令后会回复 HCI_EVENT_UUID_HANDLE，回复内容长度 0x02，回复内容为新增 Characteristic 读写的 Handle。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x78
Length	Byte2	Payload Length
Payload	Byte3	特征值属性 0x01: Broadcast 0x02: Read 0x04: Write Without Response 0x08: Write 0x10: Notify 0x20: Indicate 0x40: Authenticated Signed Writes 0x80: Extended Properties
	Byte4	UUID LENGTH
	Byte5~Byte(5+UUID_LENGTH)	特征值 UUID (小端模式)
	Byte(5+UUID_LENGTH+1)~ Byte(5+UUID_LENGTH+2)	Read 特征时，需要 read 返回的数据长度
	Byte(5+UUID_LENGTH+3)~ Byte(5+UUID_LENGTH+3+Read_data_length)	Read 特征时，返回的数据 (大端模式)

3.4.39. HCI_CMD_BLE_CREATE_CONN (0x7B, BLE_M)

HCI_CMD_BLE_CREATE_CONN 用于建立连接，操作码为 0x7b。

模块收到此命令后会回复 HCI_EVENT_CMD_RES，数据为：02 06 02 7B 00

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x7b
Length	Byte2	0x06

Payload	Byte3~Byte8	Adv addr
---------	-------------	----------

3.4.40. HCI_TEST_CMD_CLOSE_LPM (0xFF, SPP/BLE_M/S)

HCI_TEST_CMD_CLOSE_LPM 用于关闭 LPM，操作码为 0xFF。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0xFF
Length	Byte2	0x02
Payload	Byte3	0x00: disable LPM 0x01: enable LPM
	Byte4	Bit[0:6]: GPIO 编号, 当前配置应为 0x0B Bit7=1: 输出高唤醒 Bit7=0: 输出低唤醒

3.5. EVENT 事件

3.5.1. EVENT 事件汇总

EVENT	Opcode	描述	支持协议
HCI_EVENT_SPP_CONN_REP	0x00	BT3.0 连接建立	SPP
HCI_EVENT_LE_CONN_REP	0x02	BLE 连接建立	BLE_S
HCI_EVENT_SPP_DIS_REP	0x03	BT3.0 连接断开	SPP
HCI_EVENT_LE_DIS_REP	0x05	BLE 连接断开	BLE_S
HCI_EVENT_CMD_RES	0x06	命令已完成	SPP、BLE_M/S
HCI_EVENT_SPP_DATA_REP	0x07	接收到 BT3.0 数据	SPP
HCI_EVENT_LE_DATA_REP	0x08	接收到 BLE 数据	BLE_M/S
HCI_EVENT_STANDBY_REP	0x09	模块准备好	BLE_M/S
HCI_EVENT_STATUS_RES	0x0A	状态回复	BLE_M/S
HCI_EVENT_NVRAM_REP	0x0D	上传 NVRAM 数据	BLE_M/S
HCI_EVENT_GKEY	0x0E	发送 Numeric Comparison 配对方式中产生的密钥	BLE_M/S
HCI_EVENT_INVALID_PACKET	0x0F	通知 MCU 发出的包格式错误	SPP、BLE_M/S
HCI_EVENT_GET_PASSKEY	0x10	通知 MCU 可以下发 Passkey	BLE_S
HCI_EVENT_LE_TK	0x11	BLE PASSKEY 配对方式中通知 MCU 返回密钥	BLE_S
HCI_EVENT_LE_PAIRING_STATE	0x14	通知 MCU BLE 的配对状态	BLE_S

HCI_EVENT_LE_ENCRYPTION_STATE	0x15	通知 MCU 当前加密状态	BLE_S
HCI_EVENT_LE_GKEY	0x1D	Numeric Comparison 配对方式中产生的密钥	BLE_S
HCI_EVENT_UUID_HANDLE	0x29	通知 MCU 新设置的 UUID 对应的 Handle	BLE_S
HCI_EVENT_SCAN_RES	0x2A	扫描事件上报	BLE_M
HCI_EVENT_SERVICE_RES	0x50	服务上报	BLE_M
HCI_EVENT_CHARACTER	0x51	特征上报	BLE_M

3.5.2. HCI_EVENT_SPP_CONN_REP (0x00, SPP)

HCI_EVENT_SPP_CONN_REP 表示 BT3.0 连接建立。操作码为 0x00。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x00
Length	Byte2	0x00

3.5.3. HCI_EVENT_LE_CONN_REP (0x02, BLE_S)

HCI_EVENT_LE_CONN_REP 表示 BLE 连接已经建立。操作码为 0x02。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x02
Length	Byte2	0x00

3.5.4. HCI_EVENT_SPP_DIS_REP (0x03, SPP)

HCI_EVENT_SPP_DIS_REP 表示 BT3.0 连接已经断开。操作码为 0x03。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x03
Length	Byte2	0x00

3.5.5. HCI_EVENT_LE_DIS_REP (0x05, BLE_S)

HCI_EVENT_LE_DIS_REP 表示 BLE 连接已经断开。操作码为 0x05。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x05
Length	Byte2	0x00

3.5.6. HCI_EVENT_CMD_RES (0x06, SPP/BLE_M/S)

模块完成每一条命令后都会回复事件 HCI_EVENT_CMD_RES，操作码为 0x06。

此事件的 Byte3 是命令操作码，用来指示完成了什么命令；

Byte4 是命令完成状态，用来指示命令是否成功完成；

从 Byte5 开始是长度可变的回复内容，回复内容格式参见对应的命令描述。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x06
Length	Byte2	Response Content Length + 2
Payload	Byte3	完成命令操作码
Payload	Byte4	命令完成状态： 0x00：成功 0x01：失败
	Byte5~Byte (Length + 3)	回复内容，因命令不同而有差异。

3.5.7. HCI_EVENT_SPP_DATA_REP (0x07, SPP)

HCI_EVENT_SPP_DATA_REP 模块接收到 BT3.0 数据 (SPP 协议) 后会通过此事件发送给 MCU，操作码 0x07。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x07
Length	Byte2	0x01~0xFF
Payload	Byte3~Byte (Length+3)	BT3.0 数据 (SPP 协议)

3.5.8. HCI_EVENT_LE_DATA_REP (0x08, BLE_M/S)

模块接收到 BLE 数据 (GATT 协议) 后会通过此事件发送给 MCU, 操作码 0x08。

事件格式如下:

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x08
Length	Byte2	0x01~0xFF
Payload	Byte3~Byte4	Attribute Handle
	Byte5~Byte (Length+3)	BLE 数据

3.5.9. HCI_EVENT_STANDBY_REP (0x09, BLE_M/S)

模块上电/复位初始化完成后会发送 HCI_EVENT_I_AM_READY 来通知 MCU 自己已经准备好可以开始工作。MCU 需要收到此 EVENT 后方可发送第一个 CMD。

事件格式如下 :

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x09
Length	Byte2	0x00

3.5.10. HCI_EVENT_STATUS_RES (0x0A, BLE_S)

HCI_EVENT_STATUS_RES 用于回复 HCI_CMD_STAUS_REQUEST。操作码为 0x0A。

事件格式如下:

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0A
Length	Byte2	0x01
Payload	Byte3	模块状态: bit0: 3.0 可发现 bit1: 3.0 可连接 bit2: 4.0 可发现 (广播 ADV) bit4: BT3.0 (SPP 协议) 已连接 bit5: BLE 已连接

3.5.11. HCI_EVENT_NVRAM_REP (0x0D, BLE_S)

模块需要将 NVRAM 数据保存至 MCU 时会发送 HCI_EVENT_NVRAM_REP 事件给 MCU 。操作码 0x0D。关于 NVRAM 的作用和工作原理，请参考 HCI_CMD_SET_NVRAM 。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0D
Length	Byte2	0x170
Payload	Byte3~Byte173	NVRAM 数据 (34*5)

3.5.12. HCI_EVENT_GKEY (0x0E, BLE_S)

在 Numeric Comparison 配对方式中会产生密钥，需要和配对另一方比较，MCU 比较后需要返回 HCI_EVENT_GKEY。操作码 0x0E。

例如收到 HCI_EVENT_GKEY 事件：02 0E 04 22 34 05 00

0x22 0x34 0x05 0x00 转换大端模式-> 0x00053422 -> 341026

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0E
Length	Byte2	0x04
Payload	Byte3~ Byte7	4 个字节 16 进制的密钥

3.5.13. HCI_EVENT_INVALID_PACKET (0x0F, SPP/BLE_M/S)

模块收到无法处理的指令时会发送 HCI_EVENT_UART_EXCEPTION。通常由主机发送 HCI 包格式错误引起，发出此 EVENT 后模块会主动 ASSERT，此时需将模块复位或重新上电。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0F
Length	Byte2	0x00

3.5.14. HCI_EVENT_GET_PASSKEY (0x10, BLE_S)

模块在经典蓝牙 Passkey 配对方式中会产生 Passkey，在需要输入 Passkey 时，模块会发送 HCI_EVENT_GET_PASSKEY 事件来提醒 MCU 使用 HCI_CMD_PASSKEY_ENTRY 来下发 Passkey。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x10
Length	Byte2	0x00

3.5.15. HCI_EVENT_LE_TK (0x11, BLE_S)

在 BLE PASSKEY 配对方式中，需要对 TK 值进行校验，在手机上输入对应的 TK 值进行配对。

例如收到事件 02 11 04 0F 7F 07 00，应当在手机端输入 491279 完成配对。

0x 0f 0x7f 0x07 0x00 转换大端模式-> 0x00077f0f -> 491279

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x11
Length	Byte2	0x04
Payload	Byte3~Byte6	TK 数据

3.5.16. HCI_EVENT_LE_PAIRING_STATE (0x14, BLE_S)

在蓝牙发起配对的时候，模块会向 MCU 发送事件 HCI_EVENT_LE_PAIRING_STATE。

具体格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x14
Length	Byte2	0x02
Payload	Byte3~Byte4	0x0001: BT Pairing Success 0x0101: BT Pairing Fail
		0x0080: BLE Pairing Success 0x0180: BLE Pairing Fail

3.5.17. HCI_EVENT_LE_ENCRYPTION_STATE (0x15, BLE_S)

在收到加密指令之后，模块会向 MCU 发送加密状态的事件 HCI_EVENT_LE_ENCRYPTION_STATE。

具体格式如下：

描述	位置	取值
----	----	----

EVENT	Byte0	0x02
Opcode	Byte1	0x15
Length	Byte2	0x01
Payload	Byte3	0x00: 停止加密 0x01: 开始加密

3.5.18. HCI_EVENT_LE_GKEY (0x1D, BLE_S)

在 BLE Numeric Comparison 配对方式中会产生密钥，需要和配对另一方比较，

MCU 比较后需要返回 HCI_EVENT_LE_GKEY。操作码 0x1D。

例如收到 HCI_EVENT_GKEY 事件: 02 1d 04 22 34 05 00

0x22 0x 34 0x 05 0x00 转换大端模式-> 0x00053422 -> 341026

事件格式如下:

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x1D
Length	Byte2	0x04
Payload	Byte3~Byte6	4 个字节 16 进制的密钥

3.5.19. HCI_EVENT_UUID_HANDLE (0x29, BLE_S)

模块收到设置 UUID 相关的 CMD 会回复此事件，HCI_CMD_ADD_SERVICE_UUID 和 HCI_CMD_ADD_SERVICE_UUID 命令会回复，内容为当前 UUID 对应的 Handle，其中 Notify 和 Indicate 特征的 Handle 为数据发送的 Handle，使能该 UUID 的 Handle 需要加 1。

事件格式如下:

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x29
Length	Byte2	0x02
Payload	Byte3~Byte4	Handle(小端模式)

3.5.20. HCI_EVENT_SCAN_RES (0x2A, BLE_M)

此事件为扫描事件上报。

描述	位置	取值
EVENT	Byte0	0x02

Opcode	Byte1	0x2A
Length	Byte2	0x01~0xFF
Payload	Byte3 ~Byte4+len	BLE 数据

例如:

02 2A 1D 00 1B 38 2E 44 39 4F 45 02 01 02 11 09 59 69 63 68 69 70 20 31 30 32 31 73 20 4D 6F 75

第二字节为 opcode 代表此事件是收到后上报的广播数据

第三字节为内容长度

第四字节起为蓝牙实际收到的数据

第四字节代表收到的数据类型具体参数值代表含义如下:

```
/* advertising channel PDU type */
```

```
(
```

```
0 ADV_IND
```

```
1 ADV_DIRECT_IND
```

```
2 ADV_NONCONN_IND
```

```
3 SCAN_REQ
```

```
4 SCAN_RSP
```

```
5 CONNECT_REQ
```

```
6 ADV_SCAN_IND
```

```
)
```

上述数据的第四字节为 0，代表此包数据为 不定向广播包

例如: 02 2A 0D 04 0B CC F1 3E 83 15 00 04 09 53 38 35

此包第四字节为 0x04，代表此包数据为 scan rsp。此包后续内容的数据也属于广播内容

第五字节代表后续内容的实际长度

第六字节到第十一字节是 BLE 地址 (38 2E 44 39 4F 45)

第十二字节到最后为广播内容 (02 01 02 11 09 59 69 63 68 69 70 20 31 30 32 31 73 20 4D 6F 75) 此处广播内容为默认内容

3.5.21. HCI_EVENT_SERVICE_RES (0x50, BLE_M)

该上报数据为服务上报，会上报每组数据的起始 handle 号以及结束 handle。以及服务的 uuid。用于用户通过服务的 uuid 来选择对应的发送数据 handle 来使用。

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x50
Length	Byte2	0x01~0xFF
Payload	Byte3	Len 表示每组的数据长度
	Byte4~Byte5	Service start handle

	Byte6~Byte7	Service end handle
	Byte8~Byte9+Len(byte3)- 4	Service uuid

注：该组数据可能会一次性上传多个服务。连接时可能会多次上报该事件。

3.5.22. HCI_EVENT_CHARACTER (0x51, BLE_M)

该事件用于上报从机识别到的特征。

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x51
Length	Byte2	0x01~0xFF
Payload	Byte3	Len 表示每组的数据长度，uuid 2 个字节和 16 个字节是分开发送的，因此每组数据的长度是固定的
	Byte4-Byte5	Character handle
	Byte6	特征值属性 0x01: Broadcast 0x02: Read 0x04: Write Without Response 0x08: Write 0x10: Notify 0x20: Indicate
	Byte7~Byte8	Value handle: 该 handle 用于发送数据使用的 handle。
	Byte9~Byte10+Len(byte3)-5	Character uuid
	

注：该组数据可能会一次性上传多个特征。连接时可能会多次上报该事件。

3.6. BLE 属性列表

自定义 Service:

Server	UUID	Handle
UUID_YICHIP_MAJOR_SERVICE	0x49535343-FE7D-4AE5-8FA9-9FAFD205E455	0x0C

自定义发送 Characteristic:

Characteristic	UUID	Property	Handle
UUID_CHARACTERISTIC_UPLOAD	0x49535343-1E4D-4BD9-BA61-23C647249616	Notify	0x0E

自定义接收 Characteristic:

Characteristic	UUID	Property	Handle
UUID_CHARACTERISTIC_REV1	0x49535343-8841-43F4-A8D4-ECBE34729BB3	Write Write Without Resp	0x11

4. 版本历史

版本	日期	作者	描述
V1.0	2025-3-10	Aisinochip	初始版

5. 版权声明

本文档的所有部分，其著作产权归上海航芯电子科技股份有限公司（简称航芯科技）所有，未经航芯科技授权许可，任何个人及组织不得复制、转载、仿制本文档的全部或部分组件。本文档没有任何形式的担保、立场表达或其他暗示，若有任何因本文档或其中提及的产品所有资讯所引起的直接或间接损失，航芯科技及所属员工恕不为其担保任何责任。除此以外，本文档所提到的产品规格及资讯仅供参考，内容亦会随时更新，恕不另行通知。

联系我们

公司：上海航芯电子科技股份有限公司

地址：上海市闵行区合川路 2570 号科技绿洲三期 2 号楼 702 室

邮编：200241

电话：+86-21-6125 9080

传真：+86-21-6125 9080-830

Email: service@HangChip.com

Website: www.HangChip.com