Bluetooth Pairing Protocol 蓝牙配网协议

1. 定义介绍

通讯方式:BLE
通用定义:
采集器ble_mtu 517
如果发送的数据长度大于通讯双方较小MTU值，需要分多次传送，然后在应用侧组包。
约定:
采集器蓝牙名称：DL_设备SN
例：DL_609C4E7D3C6A015
蓝牙模块需包含一组服务通道 Service UUID:00FF
Characteristic uuid :ff01
特征值支持 Write，READ,INDICATE.
数据方向：模块=>app INDICATE
数据方向：app=>模块 Write

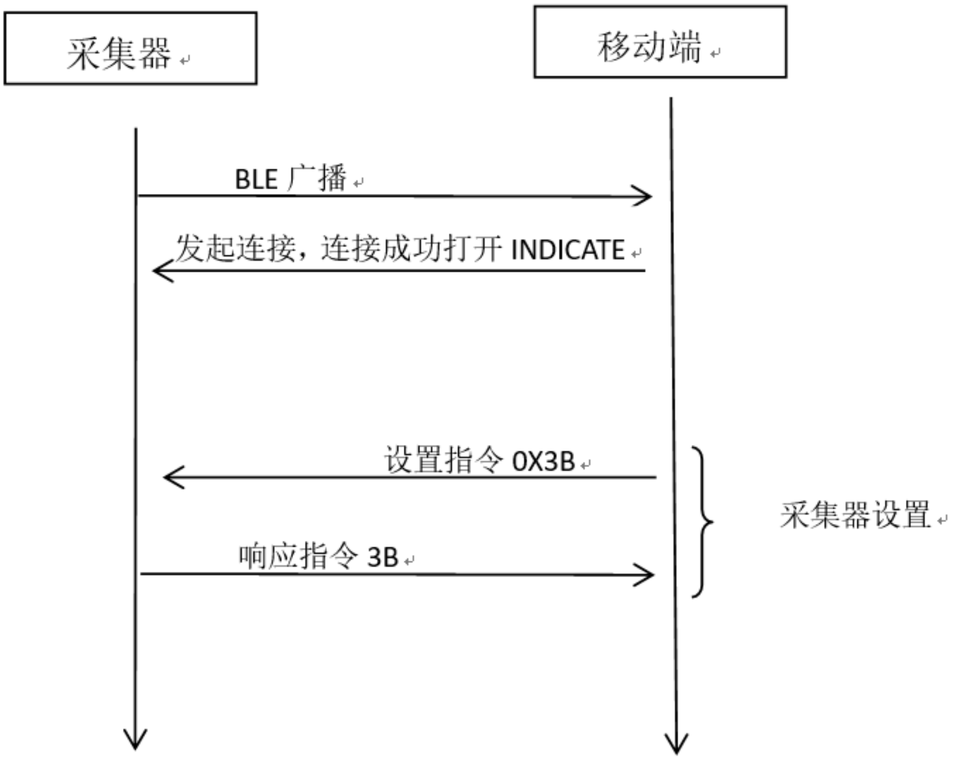
1. Introduction

Communication Method: BLE

General Definition:
Datalogger ble_mtu 517: If the length of the transmitted data exceeds the smaller MTU value between the two communication parties, it needs to be transmitted in multiple times and then grouped on the application side.

Conventions:

Bluetooth Name of the Datalogger: DL_Device SN
Example: DL_609C4E7D3C6A015The Bluetooth module must include a set of service channels:
Service UUID: 00FF
Characteristic UUID: ff01
The characteristic value supports Write, READ, and INDICATE.
Data Direction: Module => App: INDICATE; App => Module: Write



a) 数据帧头：表示上传数据包的起始位，设定为固定数据：7E7E。
b) 数据长度：表示上传数据包的长度，包括用户数据；数据长度类型Uint16
c) 功能码：表示各种功能需求和响应标志，详见各部分表
d) 时间戳：表示当前时间，单位是秒。
e) 用户数据：
f) 校验：MODBUS CRC16校验，低位在前高位在后，不含数据帧头
g) 数据帧尾：表示上传数据包的结束字符，设定为固定字符：E7E7。

a) **Data Frame Header**: Indicates the start of the uploaded data packet. Set to fixed data: 7E7E.
b) **Data Length**: Represents the length of the uploaded data packet, including user data. Data type: **Uint16**.
c) **Function Code**: Indicates various functional requirements and response flags. See respective tables for details.
d) **Timestamp**: Represents the current time in seconds.
e) **User Data**: [No specific format provided].
f) **Checksum**: **MODBUS CRC16** checksum, with low byte first and high byte second. Excludes the data frame header.
g) **Data Frame Tail**: Indicates the end of the uploaded data packet. Set to fixed character: E7E7.

2.设置采集器

命令帧:app==》采集器
功能码：0X3b

2. Setting the Datalogger

Command Frame: App ==>Datalogger

Function Code: 0x3B

数据帧头 Data Frame Header	功能码 Function Code	时间戳 Timestamp	数据长度 Data Length	用户数据 User Data	校验 Checksum	数据帧尾 Data Frame Tail
7F 7F	0x3b	4 bytes	2 bytes	N bytes	2 Bytes	F7 F7

用户数据：
user data

序号 Item	数据项 **Data Item**	数据长度 **Data Length**	数据类型 **Data Type**	备注 **Remarks**
1	设置项 Setting Item	1 1	hex hex	0x02：设置 WiFi 名密码，数据参照表 3B-2 0x02: Set WiFi name and password, dat
2	具体数据 Specific Data	N BYTE N BYTE	HEX/char HEX/char	由设置项决定 Determined by the setting item

序号 **Item**	数据项 **Data Item**	数据长度 **Data Length**	数据类型 **Data Type**	备注 **Remarks**
1	ssid长度	1 byte	HEX	
2	ssid	N bytes	char	
3	password长度	1 byte	hex	
4	password	N bytes	char	

表3B-2
Table 3B-2
应答帧：采集器==》app
Response Frame: Datalogger --> App

数据帧头 **Data Frame Header**	功能码 **Function Code**	时间戳 **Timestamp**	数据长度 **Data Length**	校验 **Checksum**	数据帧尾 **Data Frame Tail**
7F 7F	0x3b	4 bytes	0x00 0x00	2 Bytes	F7 F7

示例数据：
命令帧:app==》采集器
7F 7F 3B 11 22 33 44 00 16 02 0B 58 69 61 6F 6D 69 5F 31 34 44 43 08 31 32 33 34 35 36 37 38 D0 73 F7 F7
说明：
帧头 7F 7F
功能码：3B
时间戳：11 22 33 44
数据长度：00 16
数据项：02
Ssid长度：0B
SSID: 58 69 61 6F 6D 69 5F 31 34 44 43 (Xiaomi_14DC)
密码长度：08
密码：31 32 33 34 35 36 37 38 (12345678)

CRC:D0 73
帧尾:F7 F7
应答帧:采集器==》app
7f 7f 3b 11 22 33 44 00 00 25 d4 f7 f7

Example Data:

Command Frame: App ==> Datalogger

7F 7F 3B 11 22 33 44 00 16 02 0B 58 69 61 6F 6D 69 5F 31 34 44 43 08 31 32 33 34 35 36 37 38 D0 73 F7 F7

Explanation:

Frame Header: 7F 7F (fixed start identifier).

Function Code: 3B (configures the collector, e.g., sets Wi-Fi).

Timestamp: 11 22 33 44 (4-byte UNIX timestamp in seconds).

Data Length: 00 16 (total user data length: 22 bytes).

Setting Item: 02 (indicates Wi-Fi name and password configuration, referenced in Table 3B-2).

SSID Length: 0B (11 bytes).

SSID: 58 69 61 6F 6D 69 5F 31 34 44 43 (hex to ASCII: "Xiaomi_14DC").

Password Length: 08 (8 bytes).

Password: 31 32 33 34 35 36 37 38 (hex to ASCII: "12345678").

CRC Checksum: D0 73 (MODBUS CRC16, LSB first, excluding frame header).

Frame Tail: F7 F7 (fixed end identifier).

Response Frame: Collector ==> App

7F 7F 3B 11 22 33 44 00 00 25 D4 F7 F7

3.读取网络连接状态

命令帧:app==》采集器
功能码:0X3a

3. Read Network Connection Status

Command Frame: App ==> Datalogger
Function Code: 0X3a

数据帧头 **Data Frame Header**	功能码 **Function Code**	时间戳 **Timestamp**	数据长度 **Data Length**	用户数据 **User Data**	校验 **Checksum**	数据帧尾 **Data Frame Tail**
7F 7F	0x3a	4 bytes	00 01	1bytes	2 Bytes	F7 F7

应答帧:采集器==》app

Response Frame: Collector ==> App

数据帧头 **Data Frame Header**	功能码 **Function Code**	时间戳 **Timestamp**	数据长度 **Data Length**	用户数据 **User Data**	校验 **Checksum**	数据帧尾 **Data Frame Tail**
7F 7F	0x3a	4 bytes	2byte	Nbytes	2 Bytes	F7 F7

示例数据1获取采集器连接状态：
命令帧:app==》采集器
7F 7F 3A 11 22 33 44 00 01 04 D4 44 F7 F7
说明：
帧头 7F 7F
功能码：3A
时间戳：11 22 33 44
数据长度：00 16
用户数据：04 （固定）
CRC:D4 44
帧尾：F7 F7
应答帧：采集器==》app
7F 7F 3A 11 22 33 44 00 04 04 01 01 04 EE AB F7 F7
说明：
帧头 7F 7F
功能码：3A
时间戳：11 22 33 44
数据长度：00 04
用户数据：04 01 01 04（具体解析见表3a-1）
CRC : EE AB
帧尾：F7 F7

Example Data 1: Obtain Datalogger Connection Status

Command Frame: App ==> Collector

7F 7F 3A 11 22 33 44 00 01 04 D4 44 F7 F7

Explanation:

Frame Header: 7F 7F (fixed start identifier).

Function Code: 3A (command to read connection status).

Timestamp: 11 22 33 44 (4-byte UNIX timestamp in seconds).

Data Length: 00 01 (user data length: 1 byte).

User Data: 04 (fixed value for connection status request).

CRC Checksum: D4 44 (MODBUS CRC16, LSB first, excluding header).

Frame Tail: F7 F7 (fixed end identifier).

Response Frame: Collector ==> App

7F 7F 3A 11 22 33 44 00 04 04 01 01 04 EE AB F7 F7

Explanation:

Frame Header: 7F 7F.

Function Code: 3A (matches the command function code).

Timestamp: 11 22 33 44 (same as command frame for correlation).

Data Length: 00 04 (user data length: 4 bytes).

User Data: 04 01 01 04 (specific parsing reference Table 3A-1).

CRC Checksum: EE AB.

Frame Tail: F7 F7.

用户数据	中文定义 / **English Definition**
04 01 01 00	未接入路由 / Not connected to the router
04 01 01 01	已连接到路由器未获取到 IP/Connected to the router but no IP obtained
04 01 01 02	已连接到路由器获取到 IP/Connected to the router and IP obtained
04 01 01 03	已连接到服务器 / Connected to the server
04 01 01 04	进入透传模式 / Enter transparent transmission mode

示例数据1获取周围ssid列表：

命令帧:app==》采集器

```
7F 7F 3A 11 22 33 44 00 01 06 55 85 F7 F7
```

应答帧：采集器==》app

```
7F 7F 3A 11 22 33 44 01 2D 06 15 06 D1 79 78 31 32 33 15 C7 58 69 61 6F 6D 69 5F 38 30 44 43 2D
32 2E 34 47 2D 65 78 74 13 C7 33 36 30 E8 A1 8C E8 BD A6 E8 AE B0 E5 BD 95 E4 BB AA 0D C4
54 50 2D 4C 69 6E 6B 5F 37 44 41 30 0D C2 4D 31 2D 31 32 30 30 5F 32 2E 34 47 0B C2 46 4F 58
2D 45 53 53 2D 52 44 0F C1 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0F C0 46 4F 58 2D 45 53
53 2D 4F 46 46 49 43 45 0C BF 58 69 61 6F 6D 69 5F 31 34 44 43 0B BF 45 53 50 5F 44 33 36 38 31
39 0B BF 46 4F 58 2D 45 53 53 2D 52 44 0F BF 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0B BE
46 4F 58 2D 45 53 53 2D 52 44 0B BD 46 4F 58 2D 45 53 53 2D 52 44 0F BC 46 4F 58 2D 45 53 53
2D 4F 46 46 49 43 45 0B BB 46 4F 58 2D 45 53 53 2D 52 44 10 B9 46 4F 58 2D 45 53 53 2D 46 61
63 74 6F 72 79 0B B5 46 4F 58 2D 45 53 53 2D 52 44 0B B3 46 4F 58 2D 45 53 53 2D 52 44 0F B3
46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0F B2 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 C5
39 F7 F7
```

说明：

帧头:7F 7F

功能码:3A

时间戳:11 22 33 44

数据长度: 01 2D

数据项(查询ssid列表固定):06

ssid数量：15

(第一条ssid信息长度)：06

(第一条ssid信息)：D1 79 78 31 32 33　(信号强势 -47ssid名称:yx123)

(第二条ssid信息长度)：15

```
(第二条ssid信息)：C7 58 69 61 6F 6D 69 5F 38 30 44 43 2D 32 2E 34 47 2D 65 78 74
13 C7 33 36 30 E8 A1 8C E8 BD A6 E8 AE B0 E5 BD 95 E4 BB AA 0D C4 54 50 2D 4C 69 6E 6B 5F
37 44 41 30 0D C2 4D 31 2D 31 32 30 30 5F 32 2E 34 47 0B C2 46 4F 58 2D 45 53 53 2D 52 44 0F
C1 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0F C0 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45
0C BF 58 69 61 6F 6D 69 5F 31 34 44 43 0B BF 45 53 50 5F 44 33 36 38 31 39 0B BF 46 4F 58 2D
45 53 53 2D 52 44 0F BF 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0B BE 46 4F 58 2D 45 53 53
2D 52 44 0B BD 46 4F 58 2D 45 53 53 2D 52 44 0F BC 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45
0B BB 46 4F 58 2D 45 53 53 2D 52 44 10 B9 46 4F 58 2D 45 53 53 2D 46 61 63 74 6F 72 79 0B B5
46 4F 58 2D 45 53 53 2D 52 44 0B B3 46 4F 58 2D 45 53 53 2D 52 44 0F B3 46 4F 58 2D 45 53 53
2D 4F 46 46 49 43 45 0F B2 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45
```

CRC:C5 39

帧尾：F7 F7

Nbytes SSID信息组成：

1byte 信号强度	(N-1)bytes ssid名称
Int8	ASCII码

Example Data 1: Obtain Surrounding SSID List

Command Frame: App ==> Collector

7F 7F 3A 11 22 33 44 00 01 06 55 85 F7 F7

Response Frame: Collector ==> App

7F 7F 3A 11 22 33 44 01 2D 06 15 06 D1 79 78 31 32 33 15 C7 58 69 61 6F 6D 69 5F 38 30 44 43 2D 32 2E 34 47 2D 65 78 74 13 C7 33 36 30 E8 A1 8C E8 BD A6 E8 AE B0 E5 BD 95 E4 BB AA 0D C4 54 50 2D 4C 69 6E 6B 5F 37 44 41 30 0D C2 4D 31 2D 31 32 30 00 5F 32 2E 34 47 0B C2 46 4F 58 2D 45 53 53 2D 52 44 0F C1 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0F C0 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0C BF 58 69 61 6F 6D 69 5F 31 34 44 43 0B BF 45 53 50 5F 44 33 36 38 31 39 0B BF 46 4F 58 2D 45 53 53 2D 52 44 0F BF 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0B BE 46 4F 58 2D 45 53 53 2D 52 44 0B BD 46 4F 58 2D 45 53 53 2D 52 44 0F BC 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0B BB 46 4F 58 2D 45 53 53 2D 52 44 10 B9 46 4F 58 2D 45 53 53 2D 46 61 63 74 6F 72 79 0B B5 46 4F 58 2D 45 53 53 2D 52 44 0B B3 46 4F 58 2D 45 53 53 2D 52 44 0F B3 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0F B2 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 C5 39 F7 F7

Explanation:

Frame Header: 7F 7F (fixed start identifier).

Function Code: 3A (command to query SSID list).

Timestamp: 11 22 33 44 (4-byte UNIX timestamp in seconds).

Data Length: 01 2D (total user data length: 45 bytes).

Data Item (fixed for SSID list query): 06.

Number of SSIDs: 15 (indicated by the first data byte after the fixed item).
(First SSID information length): 06
(First SSID information): D1 79 78 31 32 33 (Signal strength: -47, SSID name: yx123)
(Second SSID information length): 15
(Second SSID information)：C7 58 69 61 6F 6D 69 5F 38 30 44 43 2D 32 2E 34 47 2D 65 78 74 13 C7 33 36 30 E8 A1 8C E8 BD A6 E8 AE B0 E5 BD 95 E4 BB AA 0D C4 54 50 2D 4C 69 6E 6B 5F 37 44 41 30 0D C2 4D 31 2D 31 32 30 30 5F 32 2E 34 47 0B C2 46 4F 58 2D 45 53 53 2D 52 44 0F C1 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0F C0 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0C BF 58 69 61 6F 6D 69 5F 31 34 44 43 0B BF 45 53 50 5F 44 33 36 38 31 39 0B BF 46 4F 58 2D 45 53 53 2D 52 44 0F BF 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0B BE 46 4F 58 2D 45 53 53 2D 52 44 0B BD 46 4F 58 2D 45 53 53 2D 52 44 0F BC 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0B BB 46 4F 58 2D 45 53 53 2D 52 44 10 B9 46 4F 58 2D 45 53 53 2D 46 61 63 74 6F 72 79 0B B5 46 4F 58 2D 45 53 53 2D 52 44 0B B3 46 4F 58 2D 45 53 53 2D 52 44 0F B3 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45 0F B2 46 4F 58 2D 45 53 53 2D 4F 46 46 49 43 45
CRC:C5 39
Frame Tail：F7 F7
Nbytes SSID information composition：

1 字节 / 1 byte	**(N-1) 字节 /(N-1) bytes**
信号强度 Signal Strength (Int8)	SSID 名称 SSID Name (ASCII characters)

4. 常见问题

§ 问：什么是正确的步骤？
答：配网只需要关注上面一条指令即可，其他数据可忽略
§ 问：什么是 "时间戳"？对我们来说，似乎与 Unix 时间戳无关（太短了）。
答：没有“时间戳”可以用随机u32（非零）代替
§ 问：我们需要如何解释有效载荷？我们假设 FuncCode 2A 与连接设置有某种关系。
答：除配网指令应答外收到的数据可忽略
§ 尾页：在我们的转储中，我们收到了 E7E7，但根据文档，应该是 F7F7。
答：配网只需要关注上面一条指令即可，其他数据可忽略
§ 问：什么才是正确的？
答：配网只需要关注上面一条指令即可，其他数据可忽略

§ 我们还不能计算出正确的校验和。
§ 问：我们需要把哪些数据放进去？(从头开始，FuncCode，时间戳，DataLen，用户数据？）
答：不包含数据帧头，从功能码到用户数据
§ 问：我们到底需要使用什么算法？你们有参考的实现方法吗，比如用 C 语言？
答：CRC-16:MODBUS
§ 问：在文档中，你们说 "低位在前，高位在后" -> 这里是指字节吗？如果不是，请详细解释：)
答：是字节
§ 收到指示 15 秒后，设备会终止 BLE 连接。
答：是的，是为防止被不使用的设备长时间占用连接，15秒内收到可解析数据（如配网指令，查询指令）就不会断开。
§ 我们假设需要完成握手。
§ 问：如何完成？
答：配网不需要握手，连接成功发送配网指令即可，其他数据请忽略

WIFI 设置：

o 问：我们如何才能读出设备是否已成功连接，或者如果未成功连接，错误出在哪里？(通过 Blueetoth LE）
答：可以，参考状态读取状态指令
o 问：支持哪些 Wifi 安全模式（WPA、WPA2、WPA3、WEP）？固件会自动正确选择它们吗？
答：出于安全考虑，不支持WEP,
- 问：我们无法通过 "Fox Cloud 2.0 "应用程序连接电池。这样可以吗？
答：电池数据通过逆变器上传。

4. Common Questions

- **Question**: What is correct process?

Answer: For network configuration, just focus on the above - mentioned instruction. Other data can be ignored.

- **Question**: What is a "timestamp"? For us, it seems to have nothing to do with the Unix timestamp (it's too short).

Answer: If there is no "timestamp", a random u32 (non - zero) can be used instead.

- **Question**: How do we interpret the payload? We assume that FuncCode 2A has some relationship with the connection settings.

Answer: Ignore the data received except for the response to the network configuration instruction.

- **Question (from the last page)**: In our dump, we received E7E7, but according to the document, it should be F7F7.

Answer: For network configuration, just focus on the above - mentioned instruction. Other data can be ignored.

- **Question**: What is correct after all?

Answer: For network configuration, just focus on the above - mentioned instruction. Other data can be ignored.

- **Question**: We haven't been able to calculate the correct checksum yet. What data do we need to put in? (From the beginning, FuncCode, timestamp, DataLen, user data?)

Answer: Exclude the data frame header, and include data from the function code to the user data.

- **Question**: What algorithm do we actually need to use? Do you have a reference implementation, for example, in C language?

Answer: CRC - 16: MODBUS.

- **Question**: In the document, it says "lower byte first, higher byte second". Does this refer to bytes? If not, please explain in detail.

Answer: Yes, it refers to bytes.

- **Question**: The device will terminate the BLE connection 15 seconds after receiving the indication. Why?

Answer: Yes, this is to prevent the connection from being occupied by unused devices for a long time. If parsable data (such as network configuration instructions, query instructions) is received within 15 seconds, the connection will not be disconnected.

- **Question**: We assume that handshake is required. How to complete it?

Answer: Handshake is not required for network configuration. Just send the network configuration instruction after the connection is successful. Please ignore other data.

WiFi Settings

- **Question**: How can we tell if the device has been successfully connected, or if not, where the error is? (Through Bluetooth LE)

Answer: Yes, refer to the status - reading instruction.

- **Question**: Which Wi - Fi security modes are supported (WPA, WPA2, WPA3, WEP)? Will the firmware automatically select the correct one?

Answer: For security reasons, WEP is not supported.

- **Question**: We can't connect to the battery through the "Fox Cloud 2.0" application. Is this okay?

Answer: battery is recognized via the inverter.