LG BT Introduction （based on Android Q（10））

V1.0

2022/08/26

修订历史（Revision History）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 日期 | 版本 | 修改 | 作者 | Reviewer |
| **2022/08/26** | Version 1.0 | 初稿（基于Android 10） | Tianyu Ao |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[修订历史（Revision History） 2](#_Toc112658165)

[表格目录 4](#_Toc112658166)

[图表目录 5](#_Toc112658167)

[词汇表 6](#_Toc112658168)

[1 LG BT Structure 7](#_Toc112658169)

[1.1 代码结构 7](#_Toc112658170)

[1.2 log及其获取方法 8](#_Toc112658171)

[1.3 LG BT函数调用流程 8](#_Toc112658172)

[1.4 LG BT学习指导 10](#_Toc112658173)

表格目录

**未找到图形项目表。**

图表目录

[图 1‑1 LG代码结构 7](#_Toc112533592)

[图 1‑2 Log获取方法 8](#_Toc112533593)

[图 1‑3 LG BT函数调用流程 9](#_Toc112533594)

词汇表

|  |  |
| --- | --- |
| 缩写 | 含义 |
| BT | Bluetooth |
| BLE | Bluetooth Low Energy |
| HCI | Host Controller Interface |

# LG BT Structure

## 代码结构

BT通常分为Host模块与Controller模块。在LG BT结构中，sil->BT-USB为Host部分，Kernel-USB->Firmware为Controller部分，空中交互数据为air data。

在LG代码中，sil层主要印度团队负责。Controller及firmware为台湾团队负责。LG kernel相关问题为LG平台负责。Stack->BT-USB为苏州负责。具体代码结构如下图所示。



图 1‑1 LG代码结构

在LG代码中，bt/btif为sil层提供bt接口，供上层调用BT协议栈，执行BT功能。在BT协议栈中，代码调用流程通常为btif->bta->btm->btu或btif->bta->l2cap->bte，之后通过btu或bte命令将数据发送至HCI层。在HCI中，通过socket将数据在发送至libbt-vendor进一步处理。在libbt-vendor中，通过write函数将数据写入BT芯片，写入过程会调用BT-USB、kernel-USB驱动。之后通过controller与firmware，发送BT数据包。

## log及其获取方法

在LG平台中，有些log使用conf文件配置，有些log默认生成，有些log可使用luna command生成，有些log使用log抓取工具获得，具体log获取方法如下图。



图 1‑2 Log获取方法

## LG BT函数调用流程

Bluetooth首先调用bt/btif/bluetooth.cc/init()、bt/btif/bluetooth.cc/enable()函数对整个Bluetooth初始化。例如，HCI中会调用bt/hci/hci\_layer\_rtkbt.cc/hci\_initialize()，libbt-vendor中会调用bt\_vendor\_rtk.c/init()、bt\_vendor\_rtk.c/op()。从btif开始，通常的函数调用流程可总结为图1-3。

蓝牙数据包发送流程（→）：

在btif中，BR/EDR设备一般通过服务发现协议（Service Discovery Protocol，SDP）查找对端设备服务，以了解对端设备是否支持某些Profile。BLE设备一般通过属性协议（Attribute Protocol，ATT）、通用属性协议（Generic Attribute Protocol，GATT）查找对端设备属性，以了解对端设备是否支持某些BLE属性。此外，BR/EDR设备inquiry、page，BLE设备advertiser、scan等操作，btif也提供了相应的接口。



图 1‑3 LG BT函数调用流程

在bta中，通过profile或某些蓝牙操作的状态机，执行具体的蓝牙动作。执行动作后，蓝牙数据通常会向L2CAP层传输，并通过安全管理协议（Security Manager Protocol，SMP）保证数据安全。蓝牙command通常会向BTM层传输。

在L2CAP与BTM层中，通过调用BTE层bte\_main\_hci\_send()函数将数据发送至HCI层。通过调用BTU层btu\_hcif\_send\_cmd()、btu\_gap\_ex\_hcif\_send\_cmd()、btu\_hcif\_send\_cmd\_with\_cb()等函数将不同类型command发送至HCI层。

在HCI中，主要通过图1-3中相应函数将数据或command发送至libbt-vendor。在libbt-vendor中，通常使用userial\_recv\_socket\_thread()、userial\_coex\_thread()等线程函数，将数据或command发送至BT芯片，发送过程中会调用rtk\_btdev.c的部分函数。此外，有些command会直接调用rtk\_send\_command()函数，在libbt-vendor中直接发送command至BT芯片。

在BT芯片中的数据或command经过controller与firmware，向空中发送需要被发送数据包或执行command后需要被发送的包。

蓝牙数据包接收过程（→）：

当发送端设备发出BT空中包后，接收端BT设备接收该空中包。之后，该空中包经过firmware与controller解析，将相应数据发送至libbt-vendor，并调用userial\_recv\_uart\_thread()线程函数，将数据进一步发送至HCI层。（有些数据包不是BT空中包，而是直接从firmware返回的包）

在HCI层中，利用hci\_rx()函数接收libbt-vendor中的数据。之后根据数据类型，调用hci\_event\_received()、acl\_event\_received()、sco\_data\_received()等函数。数据分类后，若数据类型为event，则进一步调用filter\_incoming\_event()函数对event数据进一步分类，之后通过对应callback函数将数据传递至需要该数据的模块。若是其他类型，则直径调用对应callback函数，将数据传递至需要该数据的模块。

## LG BT学习指导

前置知识（可以看到对应知识的代码再去了解）：

1. c、c++语言基础。
2. 了解线程相关概念及c、c++线程实现方法和常用函数。
3. 了解c、c++中socket使用方法。
4. 了解Linux中select、poll、epoll、ioctl、open、read、write、文件描述符（fd）等使用方法。
5. 了解c、c++函数指针、智能指针等概念，通过函数指针寻找相应的回调（callback）函数。

BT功能可以从StartAdvertising开始学习（command相对简单）。

理论部分：

可以先看core sepc vol6 part:D 3.1、3.2、3.3的LE广播过程，然后结合core sepc vol4 part:E找到对应的HCI命令和参数，同时可以参照btsnoop(HCI) log，里面有具体参数。之后可继续学习core sepc vol6 part:B 2.3，学习一下广播包类型。

代码部分：

从bt/btif/src/btif\_ble\_advertiser.cc/StartAdvertising开始，结合stack log看，stack log里有函数的调用流程。BT的log通常在/var/log里。

大致了解StartAdvertising代码调用流程后，可以自己总结一下函数调用流程图。可先总结btif->HCI过程，HCI->libbt-vendor->controller过程较为复杂，可之后慢慢了解。

学习StartAdvertising之后，可继续按以下步骤进行学习：

1. 结合core spec及代码学习le scan
2. 结合core spec及代码学习BR/EDR inquiry、page（bond）。
3. 结合core spec、profile sepc及代码学习各种profile功能，并理解sdp、gatt、l2cap等功能。