

BLUEZ

简介

duyh@haierubic.com

2017/05/19

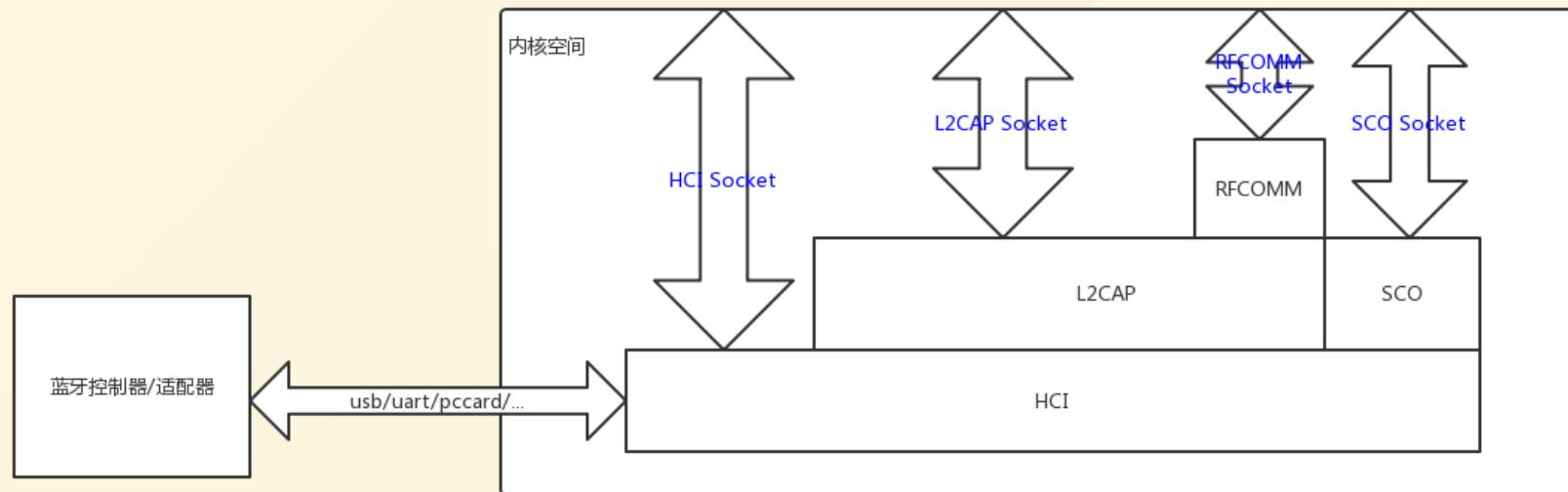
BLUEZ

BlueZ是Linux官方蓝牙协议栈,基于GPL发布的开源项目，最新版本5.45，协议栈分为内核态和用户态两部分<http://www.bluez.org/>

- 内核态—主要是一些核心协议的实现和一些设备驱动，对用户态提供socket接口
- 用户态—主要是一个daemon进程实现蓝牙设备和profile的管理，还有一些命令行工具，使用socket接口同内核交互

内核部分从Linux2.4.6开始便进入Linux内核进行维护

内核部分



```
int fd = socket(PF_BLUETOOTH, SOCK_RAW, BTPROTO_HCI);
int fd = socket(AF_BLUETOOTH, SOCK_SEQPACKET, BTPROTO_L2CAP);
int fd = socket(AF_BLUETOOTH, SOCK_STREAM, BTPROTO_RFCOMM);
```

HCI—主机控制接口

HCI接口通过发送和接收分组报文来完成蓝牙适配器的管理，配置，和数据通信，是bluez最底层的软件操作接口

- 命令分组 - 向蓝牙适配器发送控制命令
- 事件分组 - 蓝牙适配器通知上来的事件
- 数据分组 - 适配器间交互的数据包

命令分组

- 链路控制命令-扫描，连接，PIN请求等
- 链路策略命令-模式，服务质量，角色管理等
- 主机控制器与基带命令-读写设备名，扫描时间参数等
- 信息命令-读取蓝牙版本，HCI缓冲容量等
- 状态命令-读取连接句柄的状态等
- 测试命令-回环模式下读写测试等

事件分组

- 通用事件-包括命令完成包和命令状态包
- 出错事件-如产生丢失和数据缓冲区溢出
- 测试事件-测试模式下发出的事件

数据分组

- ACL-异步无连接分组
- SCO-同步有连接分组

L2CAP—逻辑链路控制与适配协议

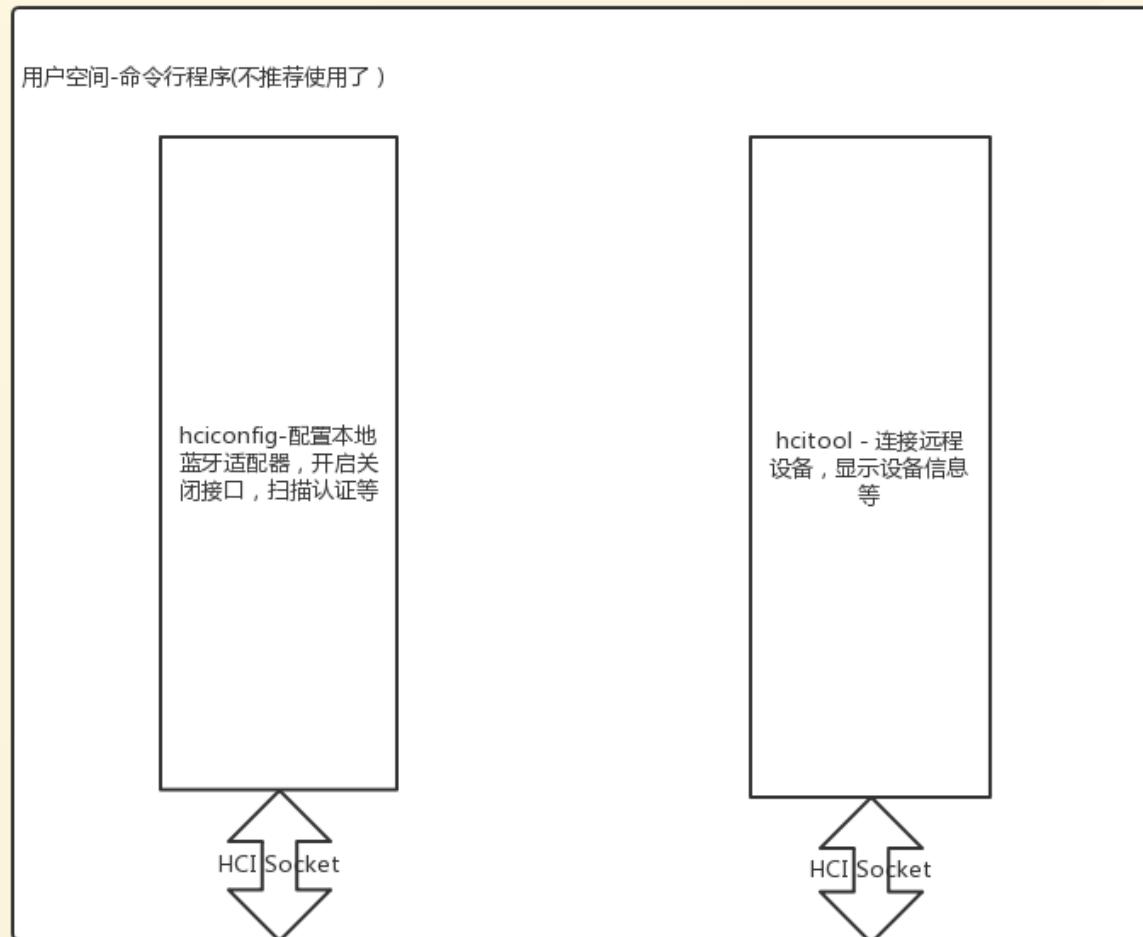
- 协议复用-底层传输协议没有提供对高层协议的复用机制,L2CAP层可以区分其上的SDP、RFCOMM、TCS等
- 分段重组-L2CAP层帮助实现基带的短PDU和高层的长PDU相互传输，L2CAP本身不完成任何PDU的分段重组，具体的分段重组有低层和高层来完成
- 服务质量信息的交换-蓝牙建立连接的过程中，L2CAP允许交互蓝牙所期望的服务质量，建立完成后，通过监视资源的使用情况，来保证服务质量
- 组抽象-L2CAP忽略地址组概念，他只关心数据

SCO & RFCOMM

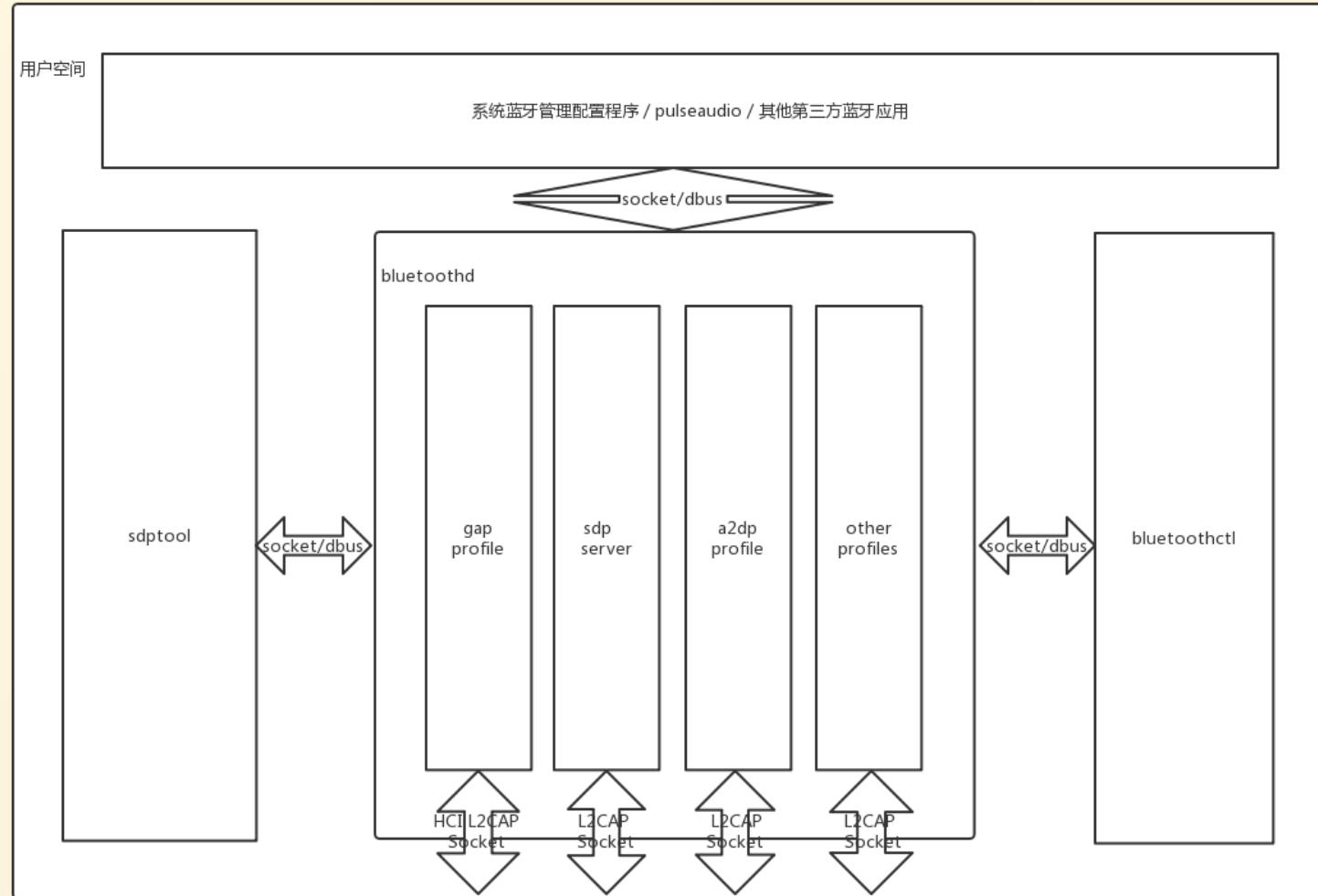
- **SCO**-语音通话接口，向用户态提供socket接口，下层使用HCI SCO数据分组
- **RFCOMM**-模拟串口接口，向用户态提供socket接口，下层使用L2CAP层接口

基本上90%的蓝牙profile应用都是使用hci/l2cap接口完成，所以其他的接口或者协议可以暂时忽略

命令行工具



用户空间daemon进程



设备发现配对演示

SDP服务发现演示

A2DP音频播放演示

BLE简介

ATT

GATT

GATT读写演示

完