

# 蓝牙协议详解

版本：v1.0.4

Crifan Li

## 摘要

本文主要介绍了蓝牙协议背景知识，蓝牙协议栈的架构，各种profile和protocol之间的分类和关系，如何在不同平台下实现蓝牙，蓝牙在各种不同领域内的应用，进行蓝牙技术的开发时所涉及的通用的知识，以及详细解释什么是低功耗蓝牙BLE，以及BLE和标准蓝牙的区别和联系。



## 本文提供多种格式供：

在线阅读	<a href="#">HTML</a> <sup>1</sup>	<a href="#">HTMLs</a> <sup>2</sup>	<a href="#">PDF</a> <sup>3</sup>	<a href="#">CHM</a> <sup>4</sup>	<a href="#">TXT</a> <sup>5</sup>	<a href="#">RTF</a> <sup>6</sup>	<a href="#">WEBHELP</a> <sup>7</sup>
下载（7zip压缩包）	<a href="#">HTML</a> <sup>8</sup>	<a href="#">HTMLs</a> <sup>9</sup>	<a href="#">PDF</a> <sup>10</sup>	<a href="#">CHM</a> <sup>11</sup>	<a href="#">TXT</a> <sup>12</sup>	<a href="#">RTF</a> <sup>13</sup>	<a href="#">WEBHELP</a> <sup>14</sup>

HTML版本的在线地址为：

[http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/html/bluetooth\\_intro.html](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/html/bluetooth_intro.html)

有任何意见，建议，提交bug等，都欢迎去讨论组发帖讨论：

[http://www.crifan.com/bbs/categories/bluetooth\\_intro/](http://www.crifan.com/bbs/categories/bluetooth_intro/)

修订历史		
修订 1.0.4	2015-05-25	crl
<ol style="list-style-type: none"><li>1. 介绍蓝牙协议的架构</li><li>2. 蓝牙的子协议的关系</li><li>3. 添加蓝牙协议架构各种图和蓝牙协议关系整理</li><li>4. 添加蓝牙技术在不同平台和领域的实现</li><li>5. 添加蓝牙协议开发</li><li>6. 添加BLE蓝牙的详细介绍</li></ol>		

<sup>1</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/html/bluetooth\\_intro.html](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/html/bluetooth_intro.html)

<sup>2</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/htmls/index.html](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/htmls/index.html)

<sup>3</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/pdf/bluetooth\\_intro.pdf](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/pdf/bluetooth_intro.pdf)

<sup>4</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/chm/bluetooth\\_intro.chm](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/chm/bluetooth_intro.chm)

<sup>5</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/txt/bluetooth\\_intro.txt](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/txt/bluetooth_intro.txt)

<sup>6</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/rtf/bluetooth\\_intro.rtf](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/rtf/bluetooth_intro.rtf)

<sup>7</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/webhelp/index.html](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/webhelp/index.html)

<sup>8</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/html/bluetooth\\_intro.html.7z](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/html/bluetooth_intro.html.7z)

<sup>9</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/htmls/index.html.7z](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/htmls/index.html.7z)

<sup>10</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/pdf/bluetooth\\_intro.pdf.7z](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/pdf/bluetooth_intro.pdf.7z)

<sup>11</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/chm/bluetooth\\_intro.chm.7z](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/chm/bluetooth_intro.chm.7z)

<sup>12</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/txt/bluetooth\\_intro.txt.7z](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/txt/bluetooth_intro.txt.7z)

<sup>13</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/rtf/bluetooth\\_intro.rtf.7z](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/rtf/bluetooth_intro.rtf.7z)

<sup>14</sup> [http://www.crifan.com/files/doc/docbook/bluetooth\\_intro/release/webhelp/bluetooth\\_intro.webhelp.7z](http://www.crifan.com/files/doc/docbook/bluetooth_intro/release/webhelp/bluetooth_intro.webhelp.7z)

---

## 7. 添加蓝牙的现场总线领域内的应用

---

---

## 蓝牙协议详解:

Crifan Li

版本 : v1.0.4

出版日期 2015-05-25

版权 © 2015 Crifan, <http://crifan.com>

本文章遵从 : [署名-非商业性使用 2.5 中国大陆\(CC BY-NC 2.5\)](#)<sup>15</sup>

---

<sup>15</sup> [http://www.crifan.com/files/doc/docbook/soft\\_dev\\_basic/release/html/soft\\_dev\\_basic.html#cc\\_by\\_nc](http://www.crifan.com/files/doc/docbook/soft_dev_basic/release/html/soft_dev_basic.html#cc_by_nc)

---

---

# 目录

正文之前 .....	vii
1. 目的 .....	vii
2. 声明 .....	vii
1. 蓝牙协议基本知识 .....	1
1.1. 蓝牙规范协议的版本 .....	1
2. 蓝牙协议的架构 .....	4
2.1. 蓝牙的各种Profile的分类 .....	4
2.1.1. 根据重要程度来划分的蓝牙协议 .....	4
2.1.2. 根据处在某端来划分的蓝牙协议 .....	4
2.1.3. 根据作用来划分的蓝牙协议 .....	4
2.2. 蓝牙的协议栈架构 .....	6
2.3. 音频的profile .....	10
2.4. 蓝牙协议栈 vs OSI模型 vs IEEE 802 .....	11
3. 不同平台中的蓝牙技术的实现 .....	13
3.1. 蓝牙在Android中的实现 .....	13
4. 蓝牙技术的应用 .....	14
4.1. 蓝牙协议的通用关系：Host主机端和Device设备端 .....	14
4.2. 蓝牙应用之音频领域 .....	15
4.3. 蓝牙在现场总线领域内的应用 .....	17
5. 蓝牙技术的开发 .....	18
5.1. 基于BlueZ的蓝牙协议栈的开发 .....	18
6. 蓝牙协议之BLE .....	19
6.1. BLE简介 .....	19
6.2. BLE的单模和双模 .....	19
6.3. BLE蓝牙协议栈架构 .....	21
6.4. 蓝牙的超低功耗ULP的实现原理 .....	23
6.5. BLE蓝牙的应用领域 .....	25
6.6. BLE厂商和芯片 .....	27
参考书目 .....	29

---

## 插图清单

1.1. 蓝牙/UWB/ZigBee/WiFi功耗对比 .....	3
2.1. 包含了BENP的蓝牙协议架构 .....	6
2.2. 基于HCI的蓝牙协议架构 .....	6
2.3. 侧重传输协议的蓝牙协议架构 .....	7
2.4. 侧重中间件协议的蓝牙协议架构 .....	7
2.5. 侧重应用程序层的蓝牙协议架构 .....	8
2.6. 蓝牙的通用访问profile .....	8
2.7. 蓝牙协议架构之无线广播和数据报 .....	9
2.8. 基于红外的蓝牙的音频profile .....	10
2.9. 基于网络的蓝牙的音频profile .....	10
2.10. 蓝牙的音频profile的配置 .....	11
2.11. 蓝牙协议栈和OSI模型以及IEEE 802标准的对比关系 .....	12
2.12. 蓝牙协议栈和OSI模型不同层之间的关系 .....	12
4.1. 蓝牙的主机端和设备端的架构总览 .....	14
4.2. 蓝牙的主机端和设备端基于HCI通讯的软件架构 .....	15
4.3. 蓝牙音频应用：源头和目的的关系 .....	16
4.4. 蓝牙音频应用的模型 .....	16
4.5. 蓝牙音频应用的模块结构 .....	17
6.1. 蓝牙的单模和双模的通信 .....	20
6.2. 双模芯片使用其中蓝牙ULP部分与单模器件通信 .....	21
6.3. 以工厂为例来解释BLE的蓝牙协议栈架构 .....	22
6.4. BLE与标准蓝牙，WiFi的信道对比 .....	24
6.5. 蓝牙4.0中已经和将要推出的BLE的profile .....	27
6.6. BLE芯片之Nordic的nRF8001 .....	28

---

## 表格清单

1.1. 蓝牙规范协议版本 .....	1
1.2. 蓝牙BD/EDR和蓝牙BLE主要参数对比 .....	3
2.1. 蓝牙的各种协议和profile的分类 .....	4

---

# 正文之前

## 1. 目的

本文旨在讲清楚蓝牙技术是啥，系统架构如何，各种协议之间关系，以及蓝牙有哪些典型的应用。

## 2. 声明

任何问题、意见、建议等，都欢迎发邮件一起探讨：admin (at) crifan.com。

# 第 1 章 蓝牙协议基本知识

## 1.1. 蓝牙规范协议的版本

下面对于各种不同版本的蓝牙规范协议的区别，内容，进行整理如下：

表 1.1. 蓝牙规范协议版本

蓝牙协议		支持的速度	备注
版本号	发布日期		
Bluetooth v1.0和v1.0B			<ul style="list-style-type: none"><li>• 强制发送BD_ADDR</li></ul>
Bluetooth v1.1			<ul style="list-style-type: none"><li>• 对应的IEEE标准是IEEE 802.15.1-2002</li><li>• RSSI(Received Signal Strength Indicator)</li></ul>
Bluetooth v1.2		实际：721Kb/s	<ul style="list-style-type: none"><li>• 对应的IEEE标准是IEEE 802.15.1-2005</li><li>• AFH(Adaptive Frequency-Hopping spread spectrum)</li><li>• eSCO(Extended Synchronous Connections)</li><li>• HCI(Host Controller Interface)</li></ul>
Bluetooth v2.0+EDR	2004年	<ul style="list-style-type: none"><li>• 理论：3Mb/s</li><li>• 实际：2.1Mb/s</li></ul>	<ul style="list-style-type: none"><li>• EDR(<math>\pi/4</math>-DQPSK +8DPSK)</li></ul>
Bluetooth v2.1+EDR	2007-07-26	<ul style="list-style-type: none"><li>• 理论：24Mb/s -&gt; High Speed</li></ul>	<ul style="list-style-type: none"><li>• SSP(Secure Simple Pairing)</li><li>• EIR(Extended Inquiry Response)</li></ul>
Bluetooth v3.0+HS	2009-04-21		<ul style="list-style-type: none"><li>• AMP (Alternative MAC/PHY)</li><li>• -&gt;Bluetooth over 802.11 high-speed data transfer</li><li>• -&gt;Bluetooth High Speed based on Wi-Fi</li><li>• L2CAP Enhanced modes</li><li>• Unicast Connectionless Data</li><li>• Enhanced Power Control</li></ul>
Bluetooth v4.0	2010-06-30		<ul style="list-style-type: none"><li>• Bluetooth v4.0</li><li>• ==Bluetooth Smart</li><li>• =Classic Bluetooth+Bluetooth HS(High Speed)+Bluetooth BLE(Bluetooth Low Energy)</li><li>• GATT(Generic Attribute Profile)</li><li>• 带AES加密的SM(Security Manager)</li></ul>



蓝牙协议		支持的速度	备注
版本号	发布日期		
Bluetooth v4.1	2013-12-04		<ul style="list-style-type: none"> <li>• Mobile Wireless Service Coexistence Signaling</li> <li>• Train Nudging and Generalized Interlaced Scanning</li> <li>• Low Duty Cycle Directed Advertising</li> <li>• L2CAP Connection Oriented and Dedicated Channels with Credit Based Flow Control</li> <li>• Dual Mode and Topology</li> <li>• LE Link Layer Topology</li> <li>• 802.11n PAL</li> <li>• Audio Architecture Updates for Wide Band Speech</li> <li>• Fast Data Advertising Interval</li> <li>• Limited Discovery Time</li> </ul>
Bluetooth v4.2	2014-12-02		<ul style="list-style-type: none"> <li>• LE Data Packet Length Extension</li> <li>• LE Secure Connections</li> <li>• Link Layer Privacy</li> <li>• Link Layer Extended Scanner Filter Policies</li> <li>• IP connectivity for Bluetooth Smart devices will soon be available via the new Internet Protocol Support Profile (IPSP)</li> <li>• IPSP will add an IPv6 connection option for Bluetooth Smart, making it ideal for connected home and other IoT implementations</li> <li>• Bluetooth 4.2 transfers data even faster by increasing the capacity of the Bluetooth Smart packets</li> <li>• Bluetooth Smart gets smarter with industry-leading privacy settings that not only lower power consumption but also make it difficult for eavesdroppers to track a device through the Bluetooth connection without permission</li> <li>• A consumer can have higher confidence they aren't being tracked by beacons or anything else</li> </ul>

蓝牙的信号传输，物理上有多种协议实现。

详见：[Controller\\_stack - List of Bluetooth protocols - Wikipedia, the free encyclopedia](http://en.wikipedia.org/wiki/List_of_Bluetooth_protocols#Controller_stack)<sup>1</sup>

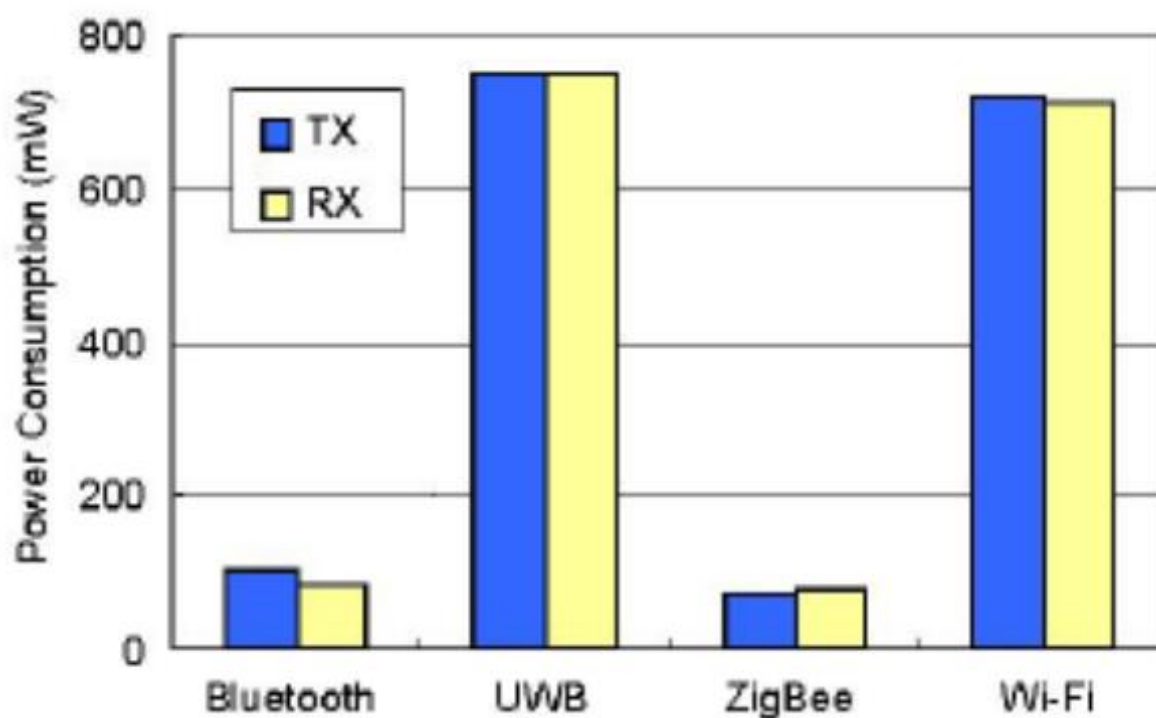
蓝牙BD/EDR和蓝牙BLE之间的主要参数的区别和对比：

**表 1.2. 蓝牙BD/EDR和蓝牙BLE主要参数对比**

对比项	蓝牙BD/EDR	蓝牙BLE
射频物理上的通道	79个频段，1MHz的通道步长	40个频段，1MHz的通道步长
发现/连接	查询/传呼	广播
微微网从设备数目	活动的7个/共255个	无限制
设备地址隐私性	无	仅私有地址寻址有效
最大数据率	1-3Mbps	1Mbps ( GFSK调制 )
加密算法	E0/SAFER+	AES-CCM
典型覆盖范围	30米	50米
最大输出功率	100mW(20dBm)	10mW(10dBm)

不同无线技术的功耗对比，包括蓝牙，UWB，ZigBee，WiFi：

**图 1.1. 蓝牙/UWB/ZigBee/WiFi功耗对比**



TODO：这里：[Android 4.2蓝牙介绍 - Innost的专栏 - 博客频道 - CSDN.NET](http://en.wikipedia.org/wiki/List_of_Bluetooth_protocols#Controller_stack)<sup>2</sup>解释的貌似不错，抽空整理过来。

<sup>1</sup> [http://en.wikipedia.org/wiki/List\\_of\\_Bluetooth\\_protocols#Controller\\_stack](http://en.wikipedia.org/wiki/List_of_Bluetooth_protocols#Controller_stack)

<sup>2</sup> <http://blog.csdn.net/innost/article/details/9187199>

# 第 2 章 蓝牙协议的架构

## 2.1. 蓝牙的各种Profile的分类

### 2.1.1. 根据重要程度来划分的蓝牙协议

蓝牙协议，也可以成为蓝牙规范，分为几大类：

- 核心协议Core Specification  
所以你常会看到，某某Profile或规范，是定义在Core Specification中的。
- 可选的协议  
比如v2.0的EDR是可选的，可以实现，也可以不实现  
  
比如v3.0的HS也是可选的

### 2.1.2. 根据处在某端来划分的蓝牙协议

蓝牙协议栈protocol stack，主要分成两类：

- Host Stack==Host主机端==操作系统端
- Controller Stack==Device设备端==controller==设备的控制器==设备的CPU==蓝牙的广播基带？+微处理器microprocessor

### 2.1.3. 根据作用来划分的蓝牙协议

蓝牙的各种协议的分类：

表 2.1. 蓝牙的各种协议和profile的分类

蓝牙profile和protocol的分类	profile缩写	profile全名	典型应用举例
强制性profile	LMP	Link Management Protocol	
	L2CAP	Logical Link Control and Adaptation Protocol	
	SDP	Service Discovery Protocol	
最常见且通用的Profile	HCI	Host Controller Interface	
	RFCOMM	Radio Frequency COMMunication	

蓝牙profile和protocol的分类	profile缩写	profile全名	典型应用举例
其他常见Profile	BNEP	Bluetooth Network Encapsulation Protocol	
	AVCTP	Audio/Video Control Transport Protocol	
	AVDTP	Audio/Video Distribution Transport Protocol	
	TCS BIN	Telephony Control Protocol – Binary	
	AT commands	attention sequence (modem prefix)	
	A2DP	Advanced Audio Distribution Profile	无绳耳机
	ATT	Attribute Profile	
	AVRCP	Audio/Video Remote Control Profile	
采纳的（别的，第三方的）协议	PPP	Point-to-Point Protocol	
	TCP	Transmission Control Protocol	
	UDP	User Datagram Protocol	
	IP	Internet Protocol	
	OBEX	Object Exchange Protocol	
	WAE	Wireless Application Environment	
	WAP	Wireless Application Protocol	
	vCard	Virtual Card	
	vCal	Virtual Calendar	



图 2.3. 侧重传输协议的蓝牙协议架构

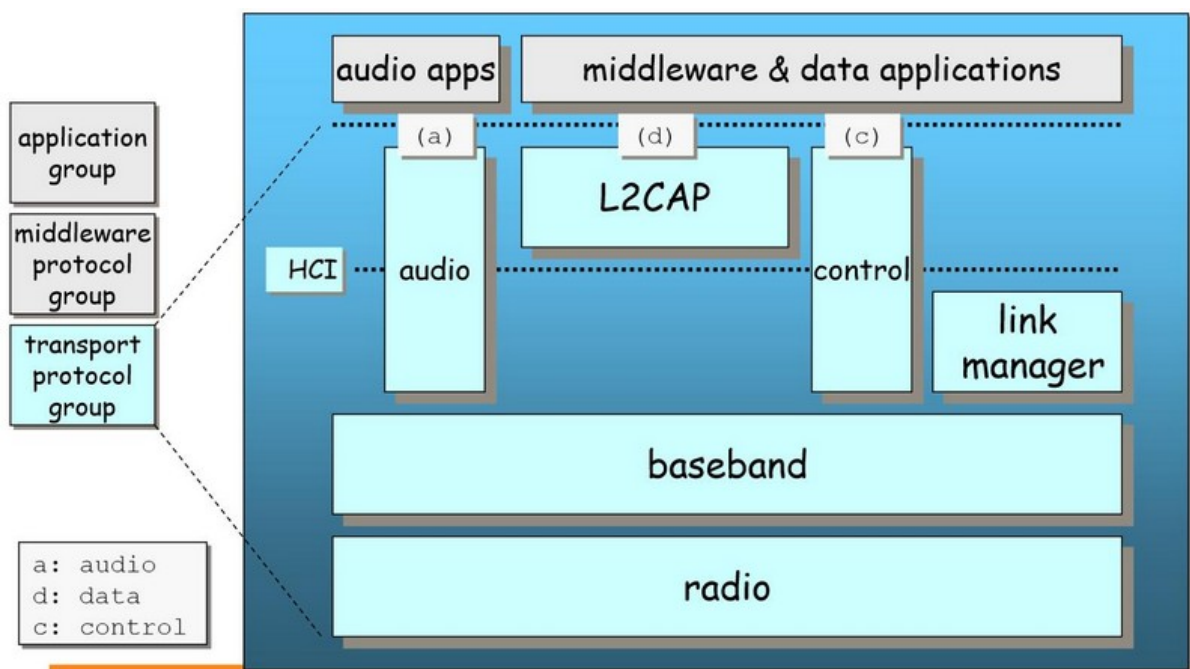


图 2.4. 侧重中间件协议的蓝牙协议架构

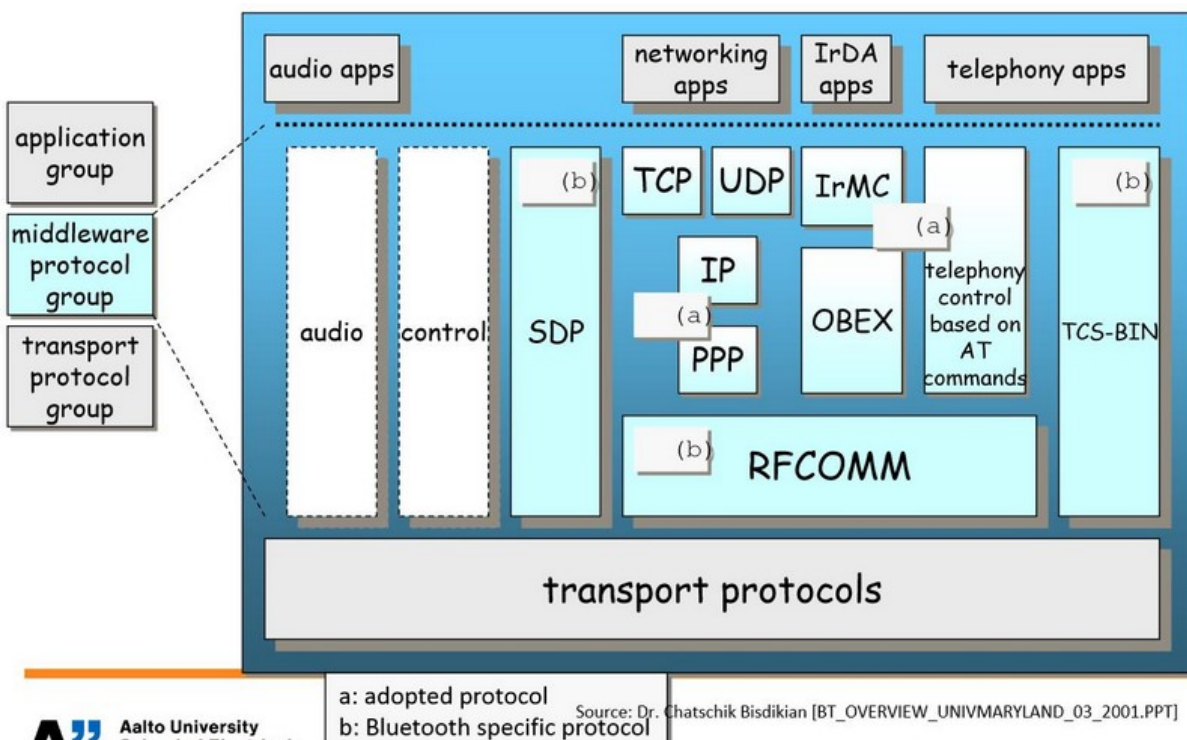
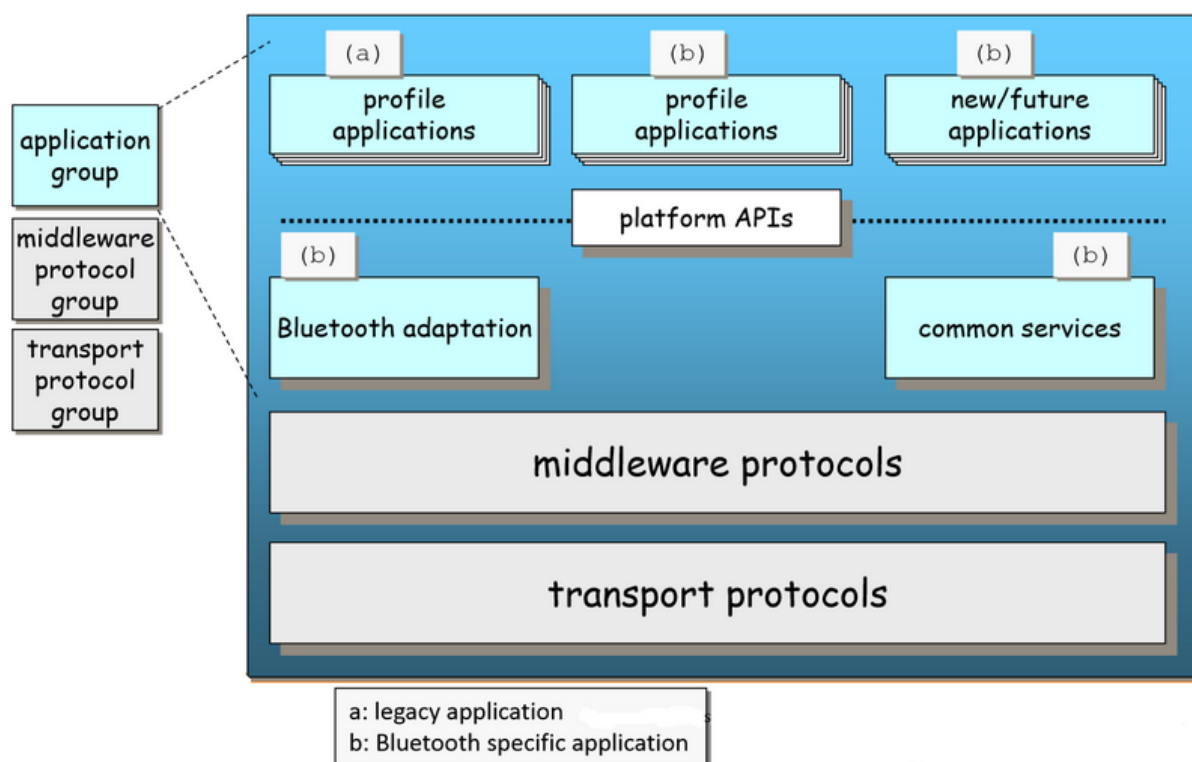




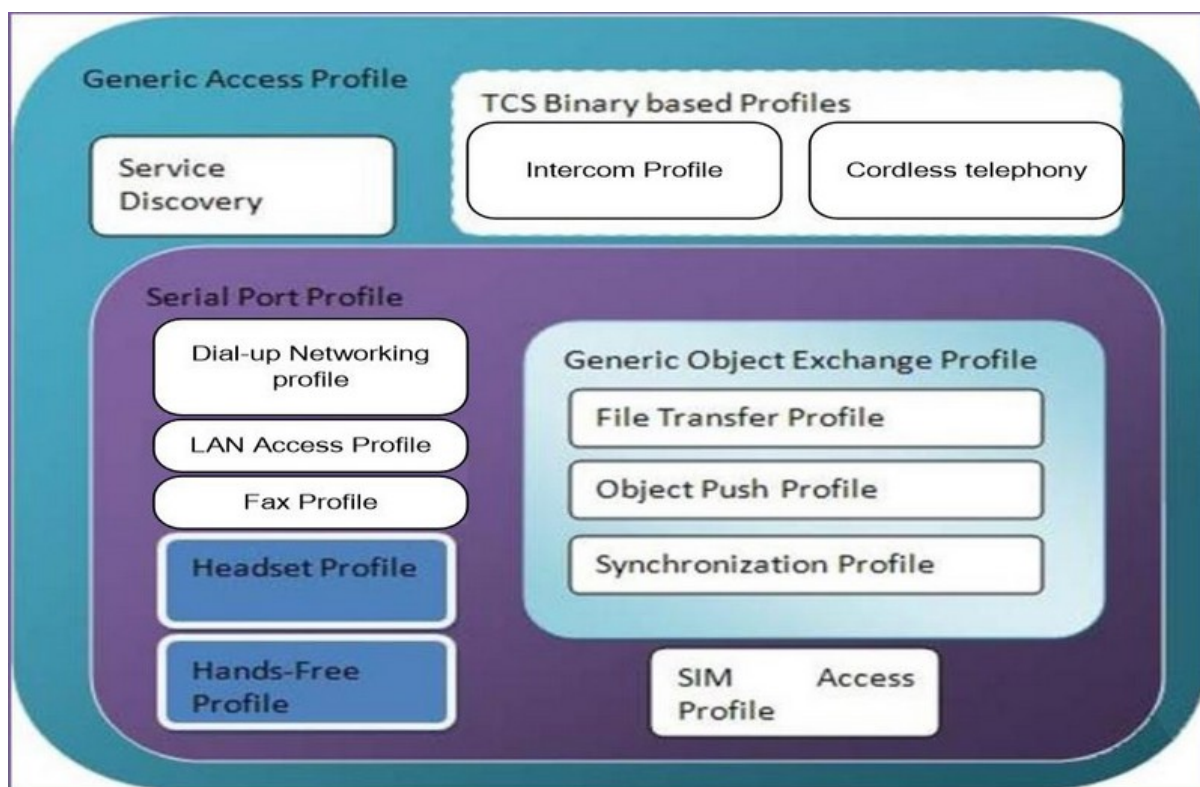
图 2.5. 侧重应用程序层的蓝牙协议架构



侧重不同profile的协议：

通用访问的profile

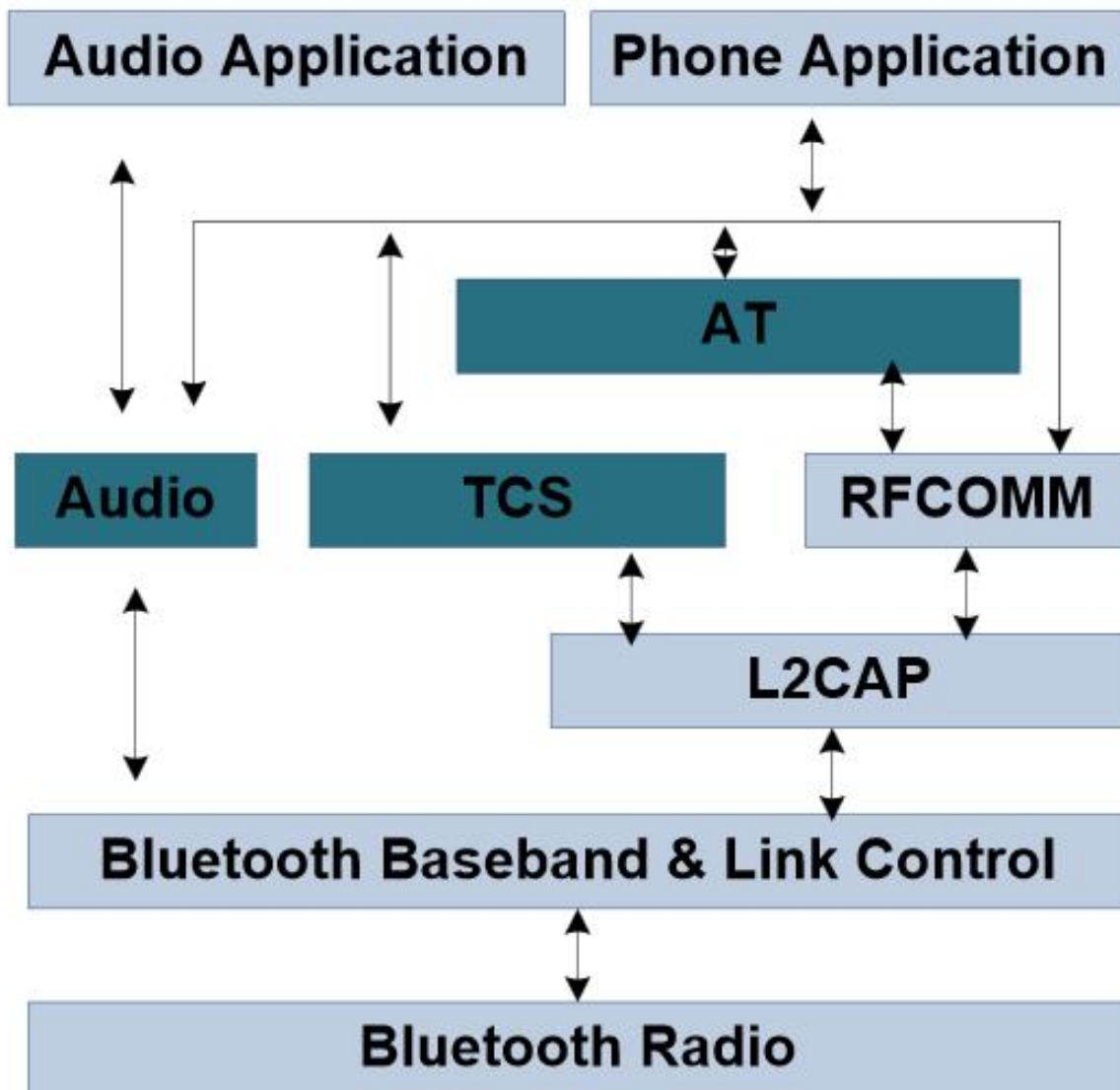
图 2.6. 蓝牙的通用访问profile



无线广播和数据报的蓝牙协议架构：

图 2.7. 蓝牙协议架构之无线广播和数据报

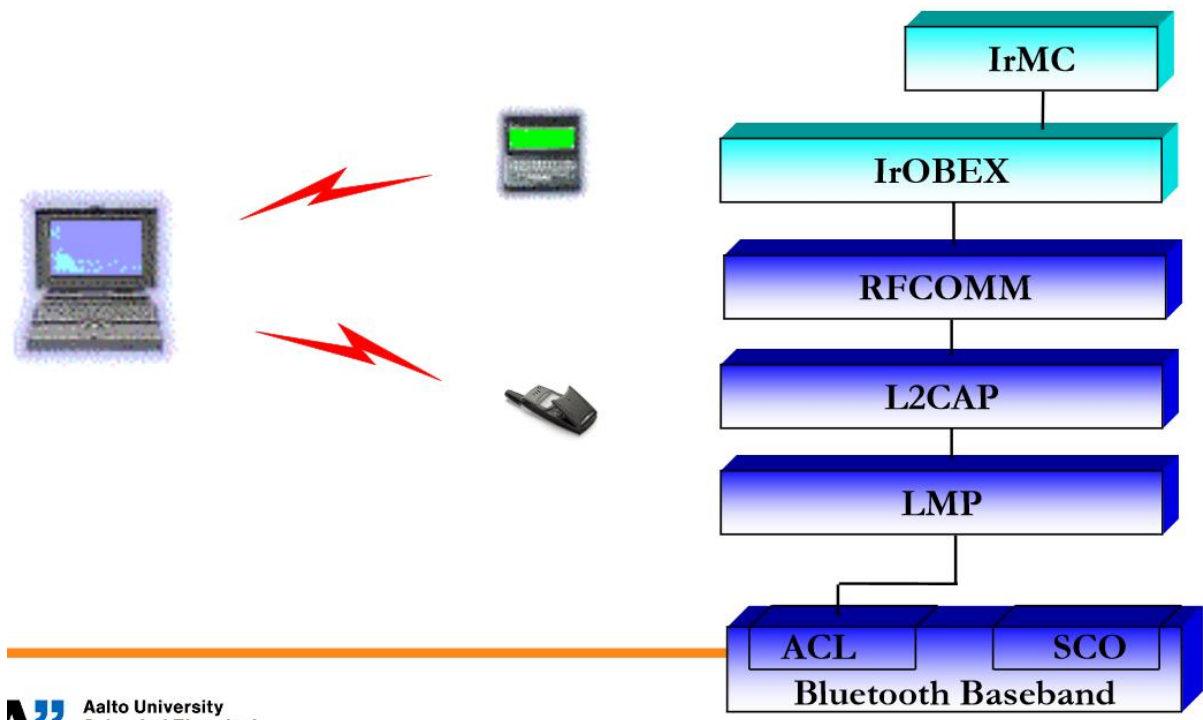
Bluetooth Radio and Telegram Protocols





## 2.3. 音频的profile

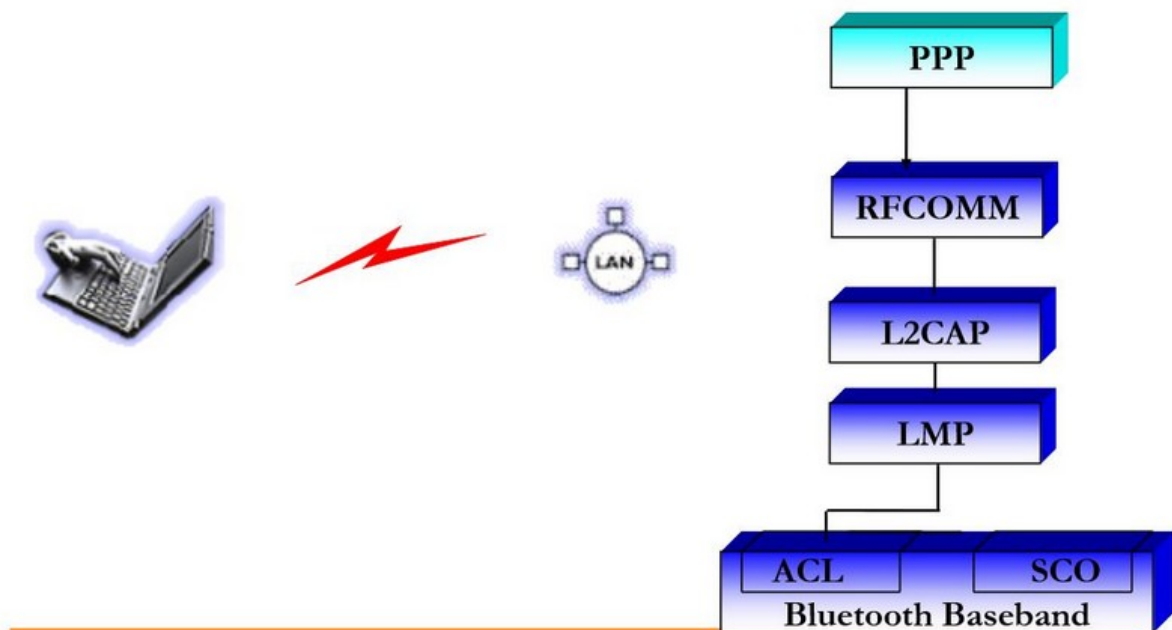
图 2.8. 基于红外的蓝牙的音频profile



Aalto University  
School of Electrical Engineering

图 2.9. 基于网络的蓝牙的音频profile

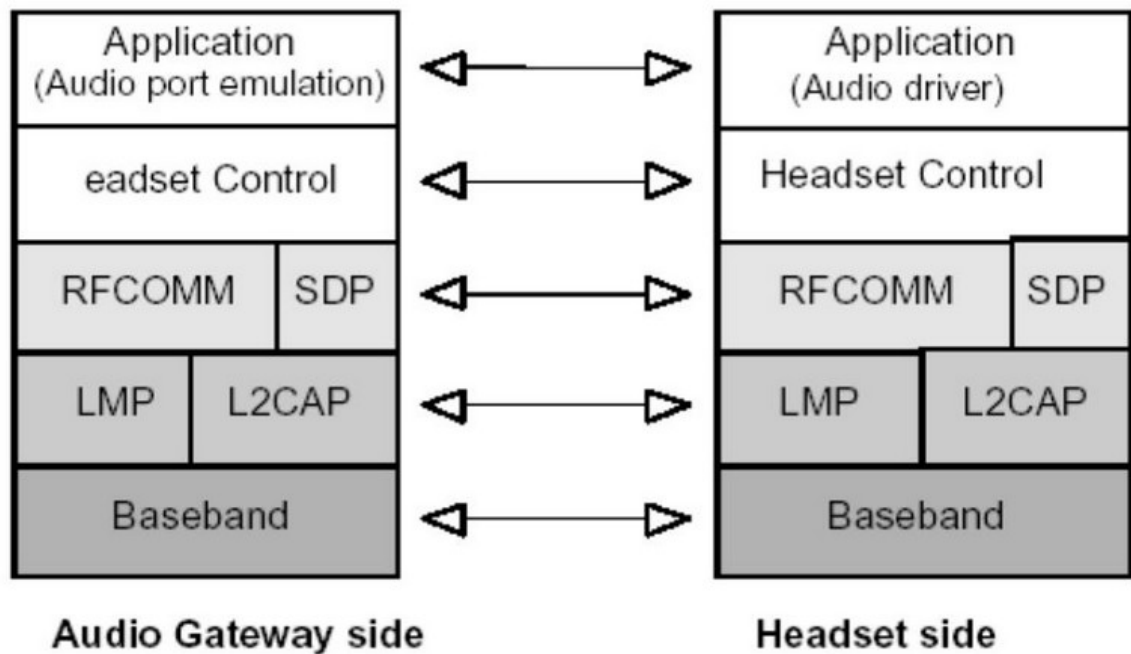
### LAN access point profile



以及对应的针对音频profile的配置：

图 2.10. 蓝牙的音频profile的配置

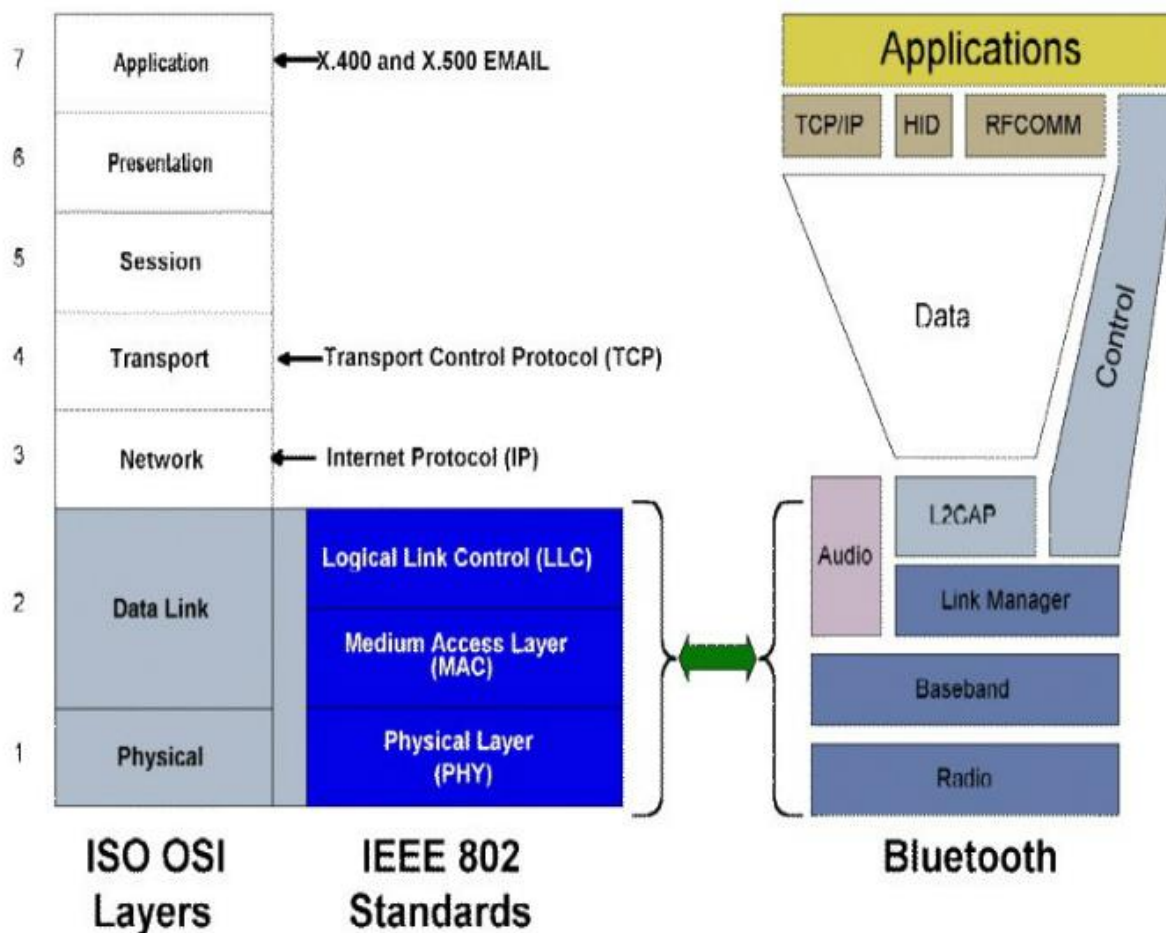
## Configuration of Headset Profile



## 2.4. 蓝牙协议栈 vs OSI模型 vs IEEE 802

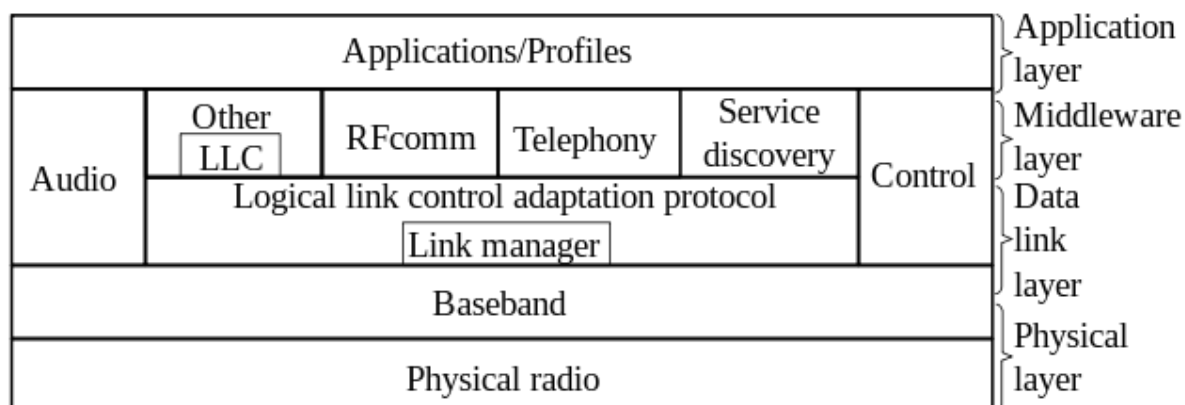
蓝牙的协议栈架构和OSI模型以及IEEE 802标准的对比关系：

图 2.11. 蓝牙协议栈和OSI模型以及IEEE 802标准的对比关系



另外也有个蓝牙协议栈和OSI不同层的对照的图，供参考：

图 2.12. 蓝牙协议栈和OSI模型不同层之间的关系



---

## 第 3 章 不同平台中的蓝牙技术的实现

### 3.1. 蓝牙在Android中的实现

Android中的蓝牙协议栈，之前是Bluez，现在改用Bluedroid

TODO：关于BlueZ和BlueDroid的对比，抽空再整理。可参考：

[在android4.2中，Google更换了android的蓝牙协议栈，从Bluez换成Bluedroid | 学步园](#)<sup>1</sup>

[Android支持蓝牙4.0版本 BLE开发 - 心有灵犀鬼才心 - 博客频道 - CSDN.NET](#)<sup>2</sup>

---

<sup>1</sup> <http://www.xuebuyuan.com/1345358.html>

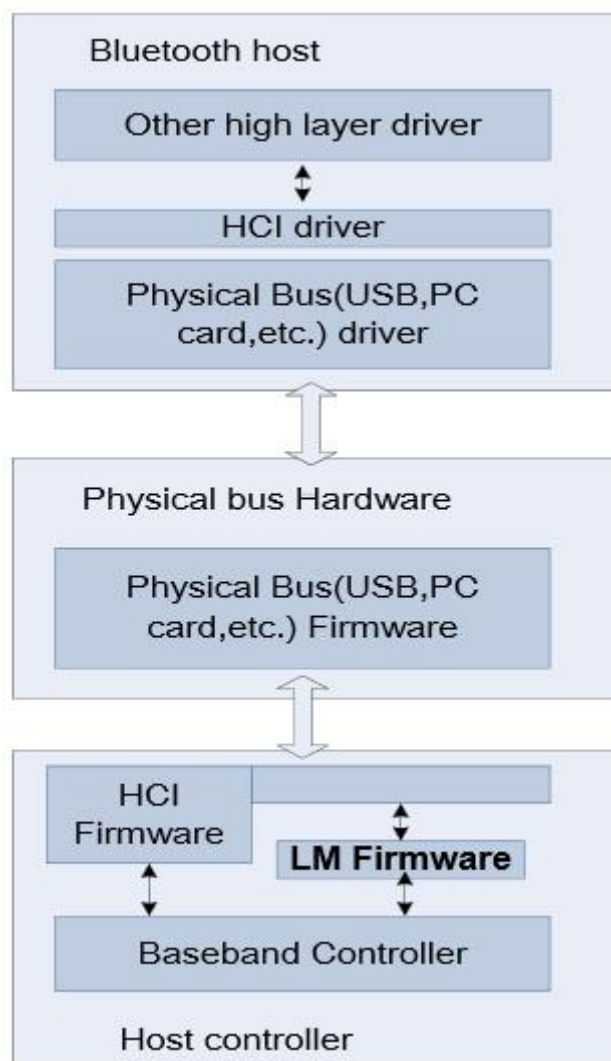
<sup>2</sup> <http://blog.csdn.net/changemyself/article/details/8454633>

## 第 4 章 蓝牙技术的应用

### 4.1. 蓝牙协议的通用关系：Host主机端和Device设备端

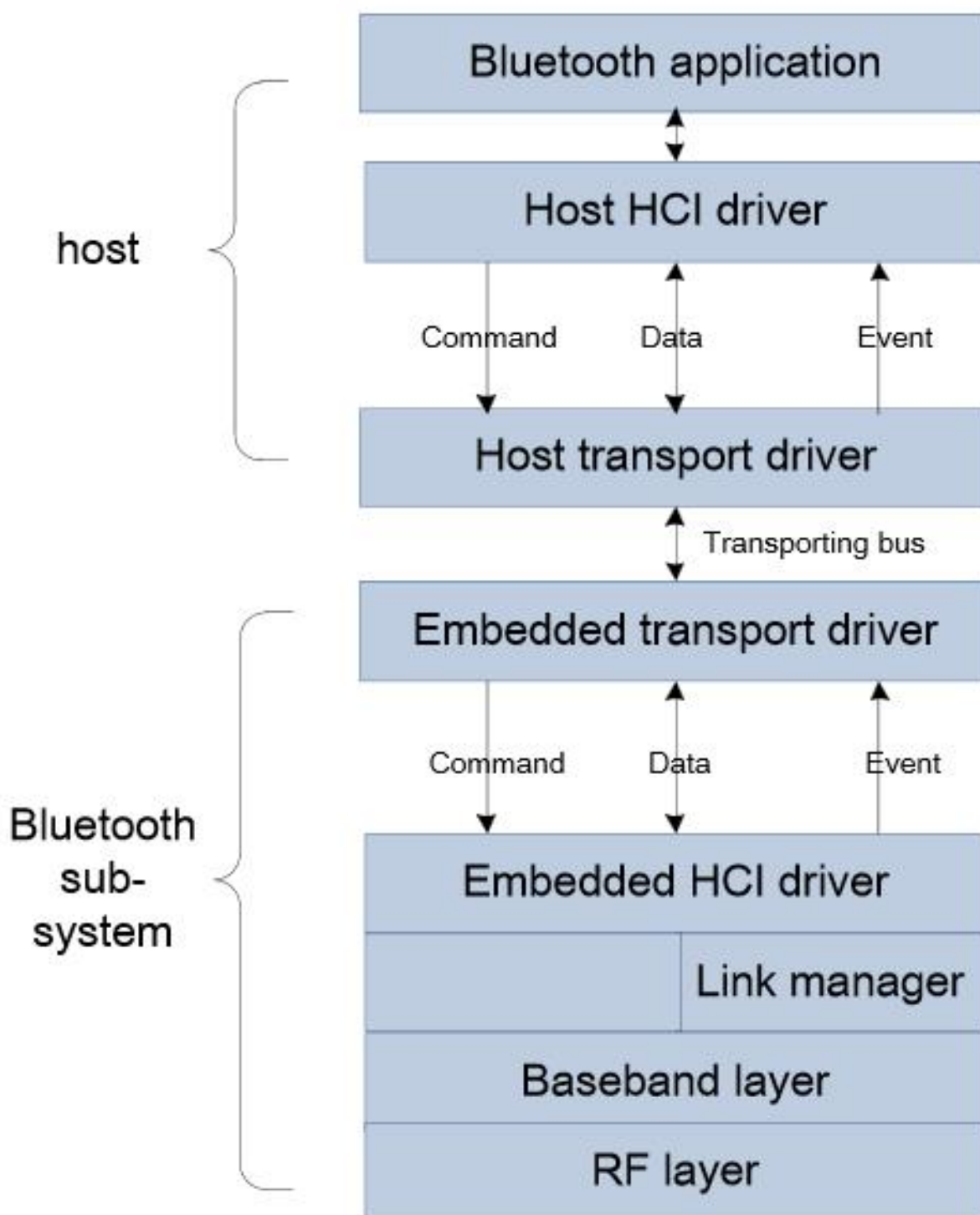
具体应用时，包括蓝牙耳机和蓝牙手机或蓝牙电脑之间的连接，都属于蓝牙的主机端和设备端之间的协作，其整体架构，都可以用下图表示：

图 4.1. 蓝牙的主机端和设备端的架构总览



以及更加详细的说明，主机端和设备端之间，都是通过HCI的接口通讯的：

图 4.2. 蓝牙的主机端和设备端基于HCI通讯的软件架构

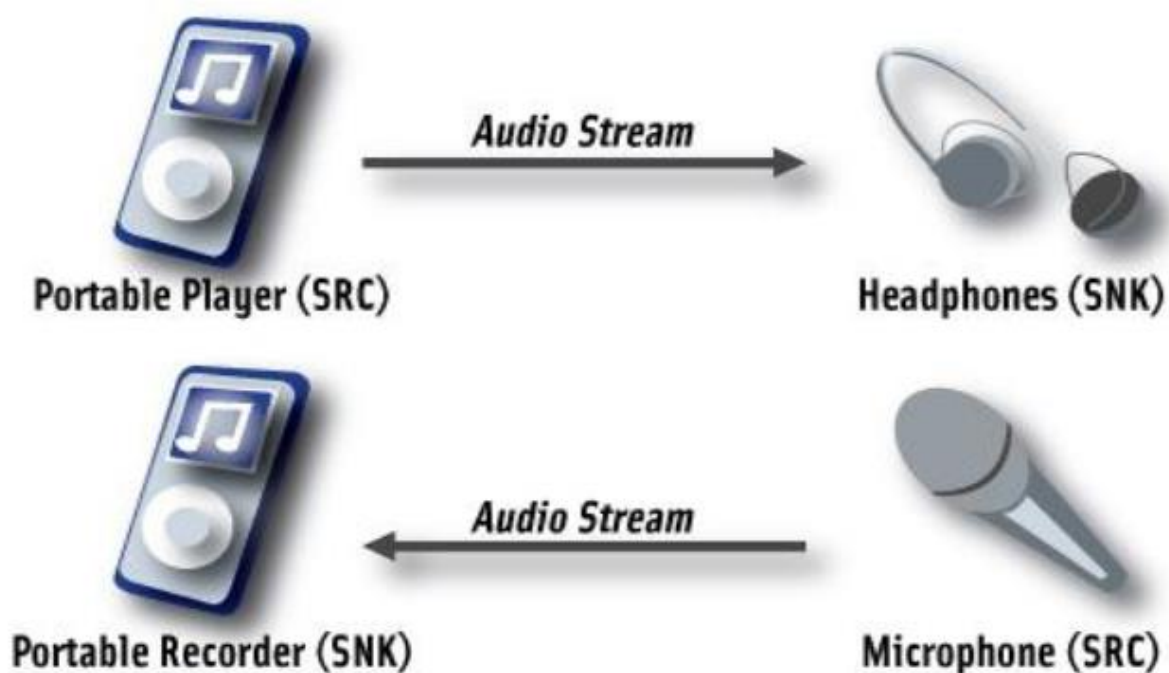


## HCI Software Architecture

### 4.2. 蓝牙应用之音频领域

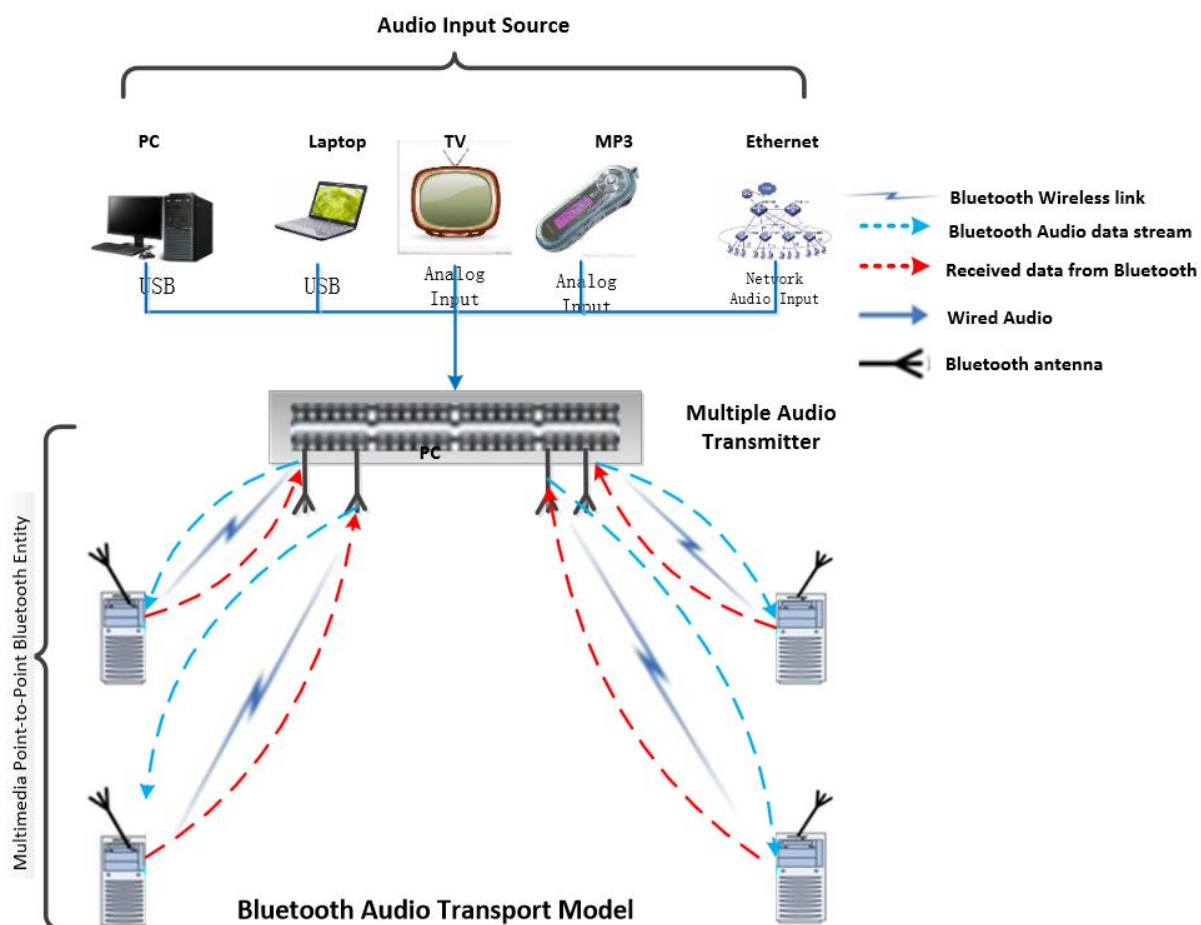
然后将蓝牙应用于音频时，官网给出的关系是：

图 4.3. 蓝牙音频应用：源头和目的的关系



对应的模型如下：

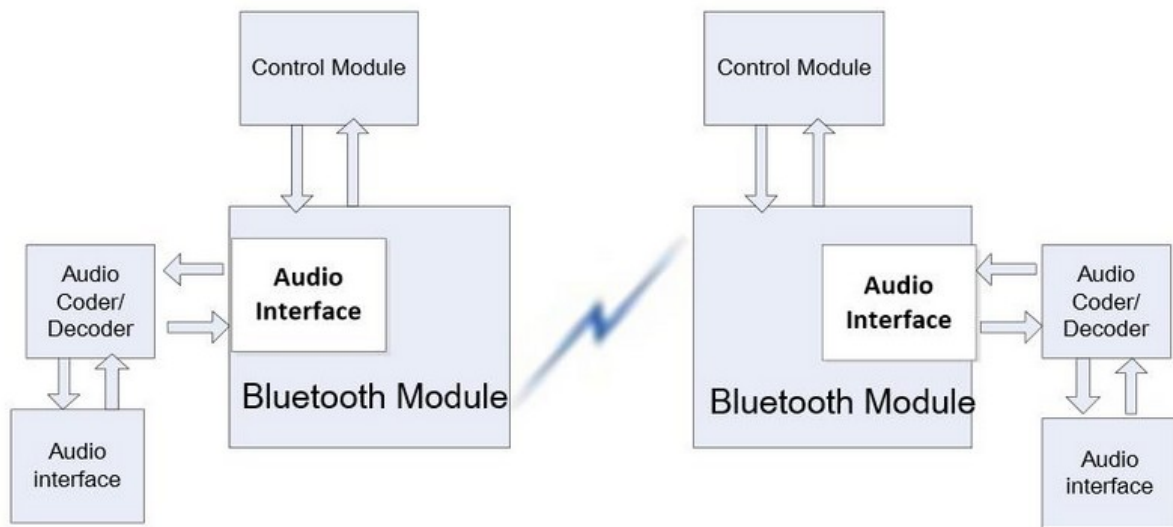
图 4.4. 蓝牙音频应用的模型





对应的模块关系是：

图 4.5. 蓝牙音频应用的模块结构



## 4.3. 蓝牙在现场总线领域内的应用

现场总线领域内的HART，新出了用蓝牙无线连接的HART猫，以及对应的Android的应用程序，可以通过蓝牙HART猫连接HART设备：

对应的Android的蓝牙app，详见：

[teknikol COMMANDER FREE - Android Apps on Google Play](https://play.google.com/store/apps/details?id=com.teknikol.commanderfree&hl=en)<sup>1</sup>

<sup>1</sup> <https://play.google.com/store/apps/details?id=com.teknikol.commanderfree&hl=en>



---

# 第 5 章 蓝牙技术的开发

## 5.1. 基于BlueZ的蓝牙协议栈的开发

基于BlueZ的蓝牙协议栈的PC端，比如常见的Ubuntu，（4.2版本之前的）旧版本的Android，则相关的测试工具有：

- hciconfig
- hciattach
- hcitool
- rfkill
- rfcomm
- sdptool
- rctest
- l2test

TODO：抽空去研究具体是如何使用的。然后把典型的使用，测试流程整理出来。可参考：

[Resources/HowTo/SamsungBTInOrigen - Linaro Wiki](https://wiki.linaro.org/Resources/HowTo/SamsungBTInOrigen) <sup>1</sup>

[linux下使用蓝牙设备 bluetooth hciconfig hcitool](http://www.360doc.com/content/12/0218/15/8157643_187595684.shtml) <sup>2</sup>

[Bluedroid与BlueZ，蓝牙测试方法的变动（基于bludroid和BlueZ的对比）](http://m.oschina.net/blog/300406) <sup>3</sup>

[Android blueZ HCI（一）：hciconfig实现及常用方法 - CLK - 博客频道 - CSDN.NET](http://blog.csdn.net/xubin341719/article/details/38640533) <sup>4</sup>

---

<sup>1</sup> <https://wiki.linaro.org/Resources/HowTo/SamsungBTInOrigen>

<sup>2</sup> [http://www.360doc.com/content/12/0218/15/8157643\\_187595684.shtml](http://www.360doc.com/content/12/0218/15/8157643_187595684.shtml)

<sup>3</sup> <http://m.oschina.net/blog/300406>

<sup>4</sup> <http://blog.csdn.net/xubin341719/article/details/38640533>

---

# 第 6 章 蓝牙协议之BLE

## 6.1. BLE简介

Bluetooth Low Energy == BLE

BLE有时候也被叫做Bluetooth Smart

BLE是标准的蓝牙（协议规范）的一个轻量级的子集

BLE是在蓝牙4.0的核心规范中引入的。

BLE，不仅是和标准的蓝牙规范是有重叠部分的，并且BLE是从骨子里就和标准规范不是一个血统的：

BLE是Nokia发起的，作为一个内部的名为Wibree的项目，后来被蓝牙组织SIG所采纳，才有了现在的BLE。

BLE之前的，临时用的名字有：Wibree，Bluetooth ULP (Ultra Low Power)

2011年下半年，改名为：

- 主机端的BLE：Bluetooth Smart Ready
- 设备（芯片，传感器）端的BLE：Bluetooth Smart

BLE，和标准蓝牙技术（比如蓝牙2.1+EDR/3.0+HS版本）一样，工作在免许可的2.4GHz ISM射频频段。

4.0以前的蓝牙，控制器和主机是分开的，而BLE中控制器和主机是在一起的。

BLE的相对于标准蓝牙的一些主要特点：

- 低成本
- 短距离
- 超低功耗(ULP)

## 6.2. BLE的单模和双模

BLE的芯片实现有两种模式：

- 单模==BLE  
只实现了BLE

部分实现了单模的蓝牙的厂商：STMicroelectronics, AMICCOM, CSR, Nordic Semiconductor, Texas Instruments

成本降低后的单模的蓝牙芯片，支持整合到高度集成和紧凑的设备，带有一个轻量级的链接层Link Layer，

支持超低功耗的空闲idle模式操作，简单的设备发现，非常节能的单点对多点数据传输，以尽可能低的功耗下的安全加密连接。

专门针对ULP操作优化了。

- 双模==Bluetooth Classic+BLE  
将Bluetooth Smart即BLE集成到已有的经典的蓝牙协议中

部分实现了双模蓝牙的厂商：Qualcomm-Atheros, CSR, Broadcom and Texas Instruments

由于双模设备要求执行标准蓝牙和蓝牙低能耗任务，因此双模芯片针对ULP操作的优化程度没有像单模芯片那么高

单模芯片可以用单节钮扣电池(如3V、220mAh的CR2032)工作很长时间(几个月甚至几年)。

标准蓝牙技术（和蓝牙低能耗双模器件）通常要求使用至少两节AAA电池（电量是钮扣电池的10至12倍，可以容忍高得多的峰值电流），

并且更多情况下最多只能工作几天或几周的时间（取决于具体应用）

注意，也有一些高度专业化的标准蓝牙设备，它们可以使用容量比AAA电池低的电池工作。

实现蓝牙协议的芯片，由于蓝牙协议的特殊性，即之前的标准的蓝牙和后期的BLE的低功耗蓝牙是不完全兼容的，因此蓝牙芯片如果想要实现对两种模式都支持的话，则需要实现蓝牙的双模。不过蓝牙双模和标准蓝牙以及蓝牙BLE，都是可以互相通信的。

用架构图表示如下：

图 6.1. 蓝牙的单模和双模的通信

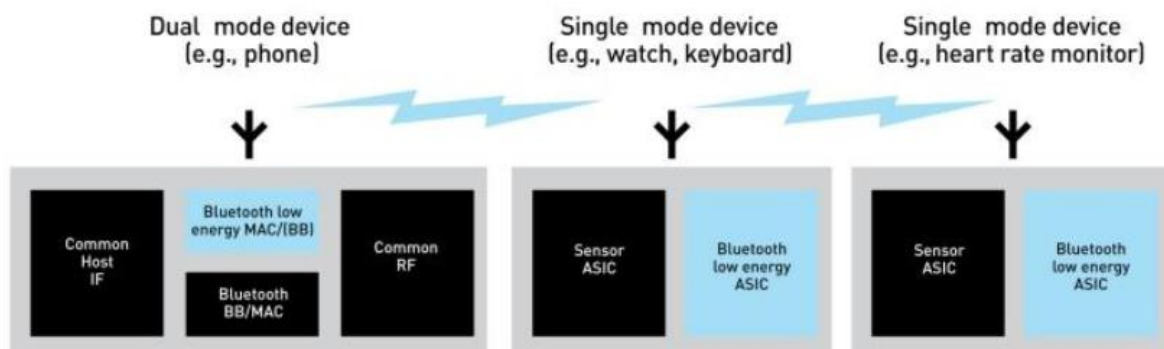
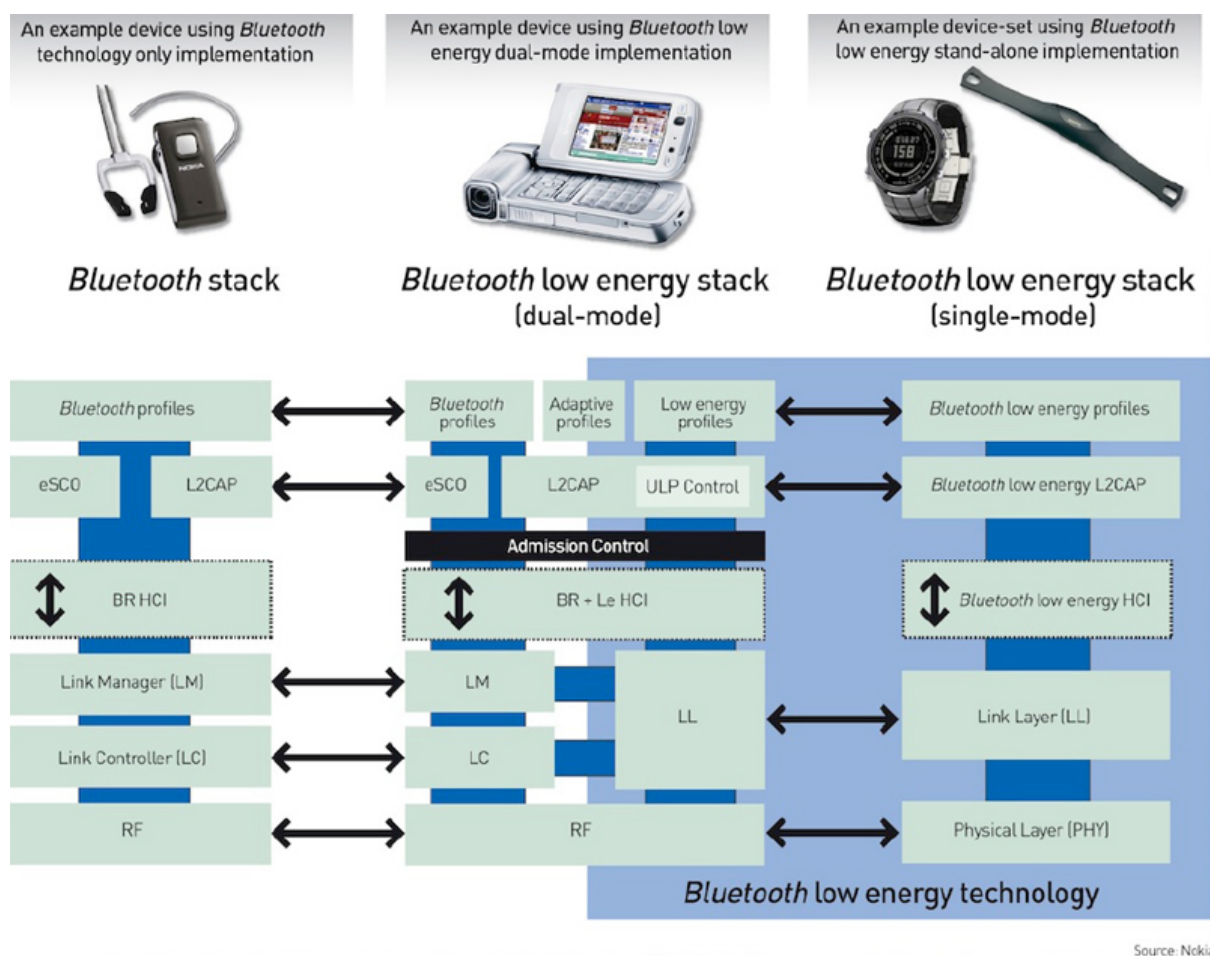


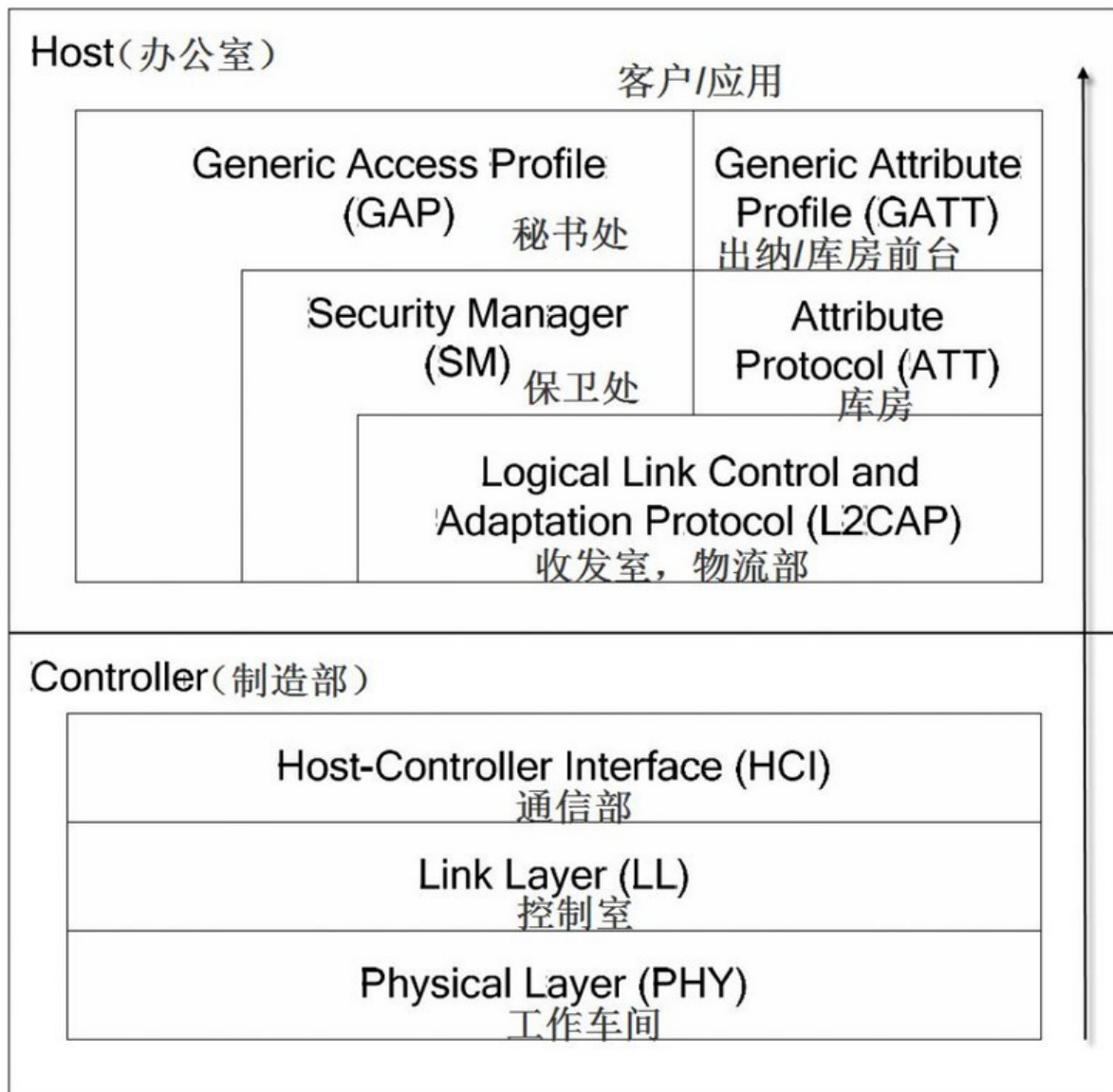
图 6.2. 双模芯片使用其中蓝牙ULP部分与单模器件通信



## 6.3. BLE蓝牙协议栈架构

BLE蓝牙协议栈的架构如下：

图 6.3. 以工厂为例来解释BLE的蓝牙协议栈架构



BLE中所有profile和应用都建构在GAP或GATT之上。

每一层的含义如下：

- PHY层==工作车间  
1Mbps自适应跳频GFSK（高斯频移键控），运行在免证的2.4GHz
- LL层==RF控制器==控制室  
控制设备处于准备（standby）、广播、监听/扫描（scan）、初始化、连接，这五种状态中一种。

五种状态切换描述为：未连接时，设备广播信息（向周围邻居讲“我来了”），另外一个设备一直监听或按需扫描（看看有没有街坊邻居家常里短可聊，打招呼“哈，你来啦”），

两个设备连接初始化（搬几把椅子到院子），设备连接上了（开聊）。

发起聊天的设备为主设备，接受聊天的设备为从设备，同一次聊天只能有一个意见领袖，即主设备和从设备不能切换。

- HCI层==接口层==通信部  
向上为主机提供软件应用程序接口（API），对外为外部硬件控制接口，可以通过串口、SPI、USB来实现设备控制
- L2CAP层==物流部  
行李打包和拆封处，提供数据封装服务
- SM层==保卫处  
提供配对和密钥分发，实现安全连接和数据交换
- ATT层==库房  
负责数据检索
- GATT层==出纳/库房前台  
出纳负责处理向上与应用打交道，而库房前台负责向下把检索任务子进程交给ATT库房去做，其关键工作是把为检索工作提供合适的profile结构，而profile由检索关键词（characteristics）组成。
- GAP层==秘书处  
对上级，提供应用程序接口  
  
对下级，管理各级职能部门，尤其是指示LL层控制室五种状态切换，指导保卫处做好机要工作

## 6.4. 蓝牙的超低功耗ULP的实现原理

相对于标准蓝牙，BLE的功耗要低很多，此处被叫做超低功耗ULP（Ultra Low Power）。

BLE采用了许多手段，去最大限度地降低功耗：

- 非常少的广播信道数  
首先要了解的是，如果无线开启的话，就是很费电的，所以BLE的设计理念就是要尽可能的降低无线开启的时间。  
  
而此理念应用到最开始的搜索，找到别的蓝牙设备，建立沟通和连接，这部分的设计，就从标准的32个信道的蓝牙，变成了3个信道的BLE。  
  
即，标准蓝牙一共有32个信道，而BLE只有3个信道。
  - > BLE搜索设备的时间大大缩短：BLE扫描其他设备只需要0.6ms~1.2ms，而标准蓝牙搜索其他设备要22.5ms。
  - > BLE定位其它无线设备所需的功耗要比标准蓝牙技术低10至20倍

值得注意的是，使用3个广告信道是某种程度上的妥协：

这是在频谱非常拥挤的部分对“开启”时间（对应于功耗）和鲁棒性的一种折衷（广告信道越少，另外一个无线设备在选用频率上广播的机会就越多，就越容易造成信号冲突）。

不过该规范的设计师对于平衡这种妥协相当有信心——比如，他们选择的广告信道不会与Wi-Fi默认信道发生冲突。

即，蓝牙低功耗技术的广告信道是经过慎重选择的，可以避免与Wi-Fi发生冲突：

**图 6.4. BLE与标准蓝牙，WiFi的信道对比**

Frequency (MHz)	Bluetooth low energy Advertising channel	Bluetooth low energy Data channel	Wi-Fi Channel
2480	39		
2478		36	
2476		35	
2474		34	
2472		33	11
2470		32	11
2468		31	11
2466		30	11
2464		29	11
2462		28	11
2460		27	11
2458		26	11
2456		25	11
2454		24	11
2452		23	11
2450		22	
2448		21	6
2446		20	6
2444		19	6
2442		18	6
2440		17	6
2438		16	6
2436		15	6
2434		14	6
2432		13	6
2430		12	6
2428		11	6
2426	38		
2424		10	
2422		9	1
2420		8	1
2418		7	1
2416		6	1
2414		5	1
2412		4	1
2410		3	1
2408		2	1
2406		1	1
2404		0	1
2402	37		1

一旦连接成功后，蓝牙低功耗技术就会切换到37个数据信道之一。



在短暂的数据传送期间，无线信号将使用标准蓝牙技术倡导的自适应跳频（AFH）技术以伪随机的方式在信道间切换（虽然标准蓝牙技术使用79个数据信道）。

要求蓝牙低功耗技术无线开启时间最短的另一个原因是它具有1Mbps的原始数据带宽——更大的带宽允许在更短的时间内发送更多的信息。

举例来说，具有250kbps带宽的另一种无线技术发送相同信息需要开启的时间要长8倍（消耗更多电池能量）

蓝牙低功耗技术“完成”一次连接(即扫描其它设备、建立链路、发送数据、认证和适当地结束)只需3ms。而标准蓝牙技术完成相同的连接周期需要数百毫秒。

- 更加“宽松的”射频参数和发送很短的数据包  
通过这两种方式限制峰值功耗：

两种技术都使用高斯频移键控(GFSK)调制，但蓝牙低功耗技术使用的调制指数是0.5，而标准蓝牙技术是0.35。0.5的指数接近高斯最小频移键控(GMSK)方案，可以降低无线设备的功耗要求(这方面的原因比较复杂，此处暂不赘述)。

更调制指数还有两个好处，即提高覆盖范围和增强健壮性。

标准蓝牙技术使用的数据包长度较长。在发送这些较长的数据包时，无线设备必须在相对较高的功耗状态保持更长的时间，从而容易使硅片发热。

这种发热将改变材料的物理特性，进而改变传送频率（中断链路），除非频繁地对无线设备进行再次校准。

再次校准将消耗更多的功率（并且要求闭环架构，使得无线设备更加复杂，从而推高设备价格）。

相反，蓝牙低功耗技术使用非常短的数据包——这能使硅片保持在低温状态。因此，蓝牙低功耗收发器不需要较耗能的再次校准和闭环架构。

- 可变连接时间间隔  
标准蓝牙技术是一种“面向连接”的无线技术，具有固定的连接时间间隔，因此是移动电话连接无线耳机等高活动连接的理想之选。

相反，蓝牙低功耗技术采用可变连接时间间隔，这个间隔根据具体应用可以设置为几毫秒到几秒不等。

因为BLE技术采用非常快速的连接方式，因此平时可以处于“非连接”状态（节省能源），

此时链路两端相互间只是知晓对方，只有在必要时才开启链路，然后在尽可能短的时间内关闭链路。

正因为如此，才使得BLE的工作模式非常适合用于从微型无线传感器（每半秒交换一次数据）或使用完全异步通信的遥控器等其它外设传送数据。

这些设备发送的数据量非常少（通常几个字节），而且发送次数也很少（例如每秒几次到每分钟一次，甚至更少）

## 6.5. BLE蓝牙的应用领域

蓝牙低功耗技术设计非常适合由于严格的功耗限制而无法使用标准蓝牙技术的应用场合。



针对于BLE，蓝牙技术联盟(Bluetooth SIG)发布了新的profile，比如：

- 个人用户接口设备  
比如手表
- 遥控器
- 距离感应告警仪  
对应的领域可能有：距离感应告警和室内定位（有时也称为室内GPS）

距离感应告警方面的应用可能有：

- 手表的距离感应告警  
比如手表将周期性地与手机进行通信，如果手机移到一定的范围之外——因而无法与用户佩戴的手表联系——它将自动锁死，同时手表发出告警。

这将防止手机意外丢失，并对任何潜在的小偷起到重要的震慑作用。

- 笔记本的距离感应告警  
距离感应告警应用还可以延伸至便携式电脑，当用户移动到一定范围之外时将便携式电脑锁定（也许当靠近的用户按下手表上的某个键时也能解锁）。
- 儿童的距离感应告警  
这种应用还能用作儿童安全设备，当儿童与父母在一定范围内时他们手上的手表能保持正常通信，当儿童跑出设定范围时发出声音告警。

蓝牙低能耗传感器的低成本和低维护量（因为电池不需要频繁更换）将鼓励在公共场所的广泛使用。

另外一种关键应用是室内定位（在没有GPS信号的地方）

室内定位方面的应用可能有：

- 大型公共建筑（如机场或火车站）  
大型公共建筑（如机场或火车站）周围的传感器不断地广播它们的位置信息

装备了蓝牙低能耗技术的手机在这个范围内通过时就可以向它的主人显示这些位置信息。

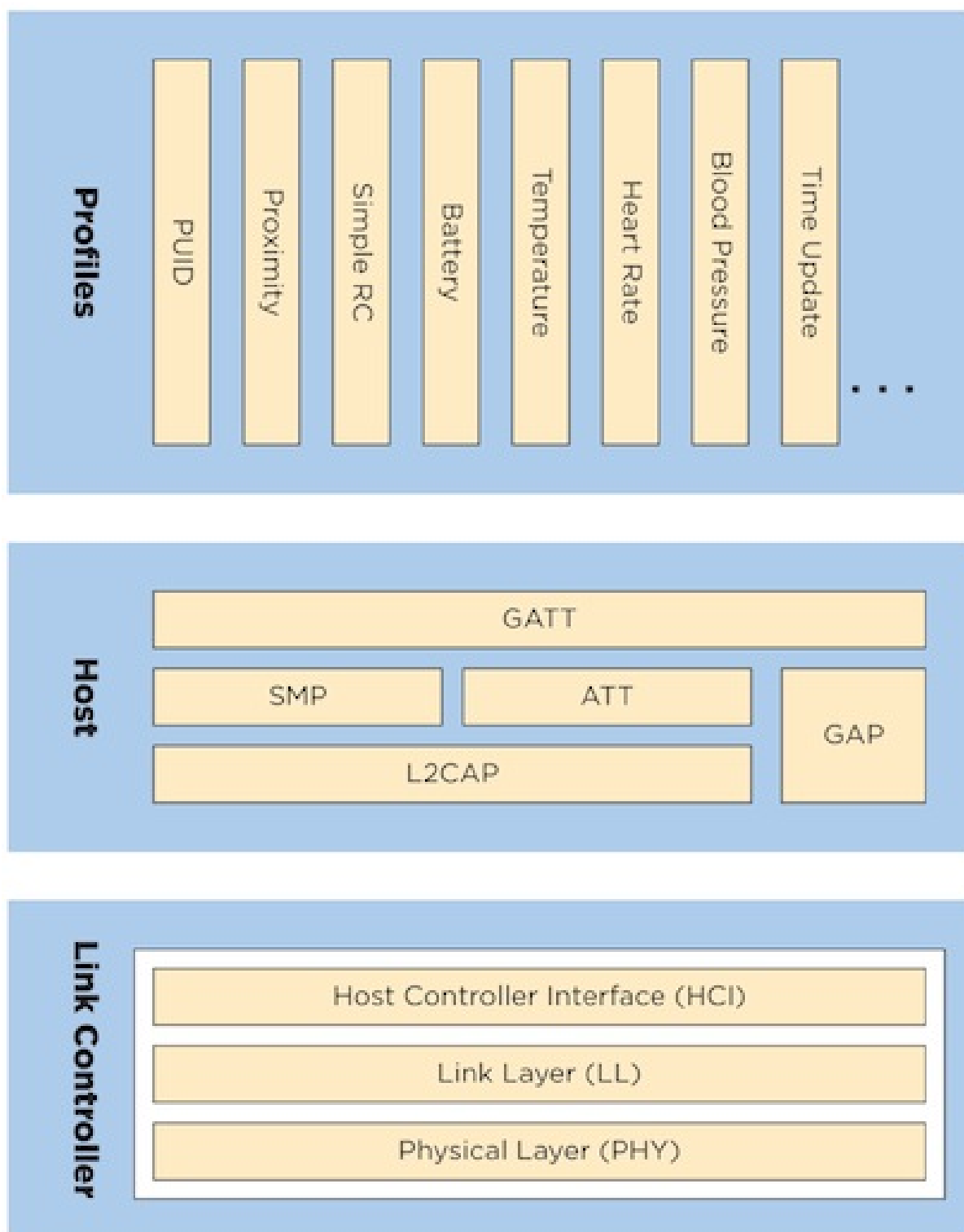
传感器还可以发送其它信息，如航班起飞时间和登机口、娱乐场所位置或附近商店的特价商品等

- 电池状态
- 心率监视器

---

其它健康和健身监视配置（如血糖仪和血压计、周期性节律仪和周期性奇异电源）将随后推出。

图 6.5. 蓝牙4.0中已经和将要推出的BLE的profile



## 6.6. BLE厂商和芯片

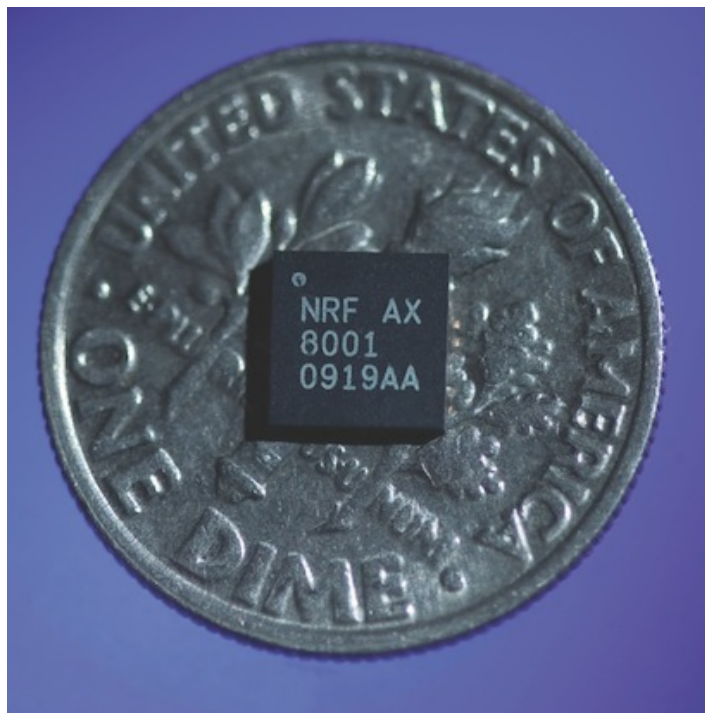
下面整理一些，一些厂家研发的BLE芯片：

- Nordic的Blue nRF8001

32引脚5x5mm QFN封装的一种单模外设解决方案

集成了完全嵌入式无线电、链路控制器和主机子系统——非常适合手表、传感器和遥控器等应用

**图 6.6. BLE芯片之Nordic的nRF8001**



---

# 参考书目

- [1] [Bluetooth Protocol Architecture](#)<sup>1</sup>
- [2] [Bluetooth - Wikipedia, the free encyclopedia](#)<sup>2</sup>
- [3] [List of Bluetooth profiles - Wikipedia, the free encyclopedia](#)<sup>3</sup>
- [4] [List of Bluetooth protocols - Wikipedia, the free encyclopedia](#)<sup>4</sup>
- [5] [6.1 Bluetooth protocol stack](#)<sup>5</sup>
- [6] [Profiles Overview | Bluetooth Development Portal](#)<sup>6</sup>
- [7] [bluetooth协议架构详解与android 蓝牙架构分析](#)<sup>7</sup>
- [8] [Introduction | Introduction to Bluetooth Low Energy | Adafruit Learning System](#)<sup>8</sup>
- [9] [蓝牙低功耗设计简介](#)<sup>9</sup>
- [10] [TI低功耗蓝牙（BLE）介绍 - 旋木的专栏 - 博客频道 - CSDN.NET](#)<sup>10</sup>
- [11] [蓝牙低功耗（BLE）技术简介 - OFweek电子工程网](#)<sup>11</sup>
- [12] [蓝牙低功耗技术内幕-RF/微波-电子工程专辑](#)<sup>12</sup>
- [13] [谈谈几个月以来开发android蓝牙4.0 BLE低功耗应用的感受 - 流风，飘然的风 - 博客园](#)<sup>13</sup>
- [14] [Bluetooth | Android Developers](#)<sup>14</sup>

---

<sup>1</sup> [http://srohit.tripod.com/bluetooth\\_sec.pdf](http://srohit.tripod.com/bluetooth_sec.pdf)

<sup>2</sup> <http://en.wikipedia.org/wiki/Bluetooth>

<sup>3</sup> [http://en.wikipedia.org/wiki/List\\_of\\_Bluetooth\\_profiles](http://en.wikipedia.org/wiki/List_of_Bluetooth_profiles)

<sup>4</sup> [http://en.wikipedia.org/wiki/List\\_of\\_Bluetooth\\_protocols](http://en.wikipedia.org/wiki/List_of_Bluetooth_protocols)

<sup>5</sup> [http://en.wikipedia.org/wiki/Bluetooth#Bluetooth\\_protocol\\_stack](http://en.wikipedia.org/wiki/Bluetooth#Bluetooth_protocol_stack)

<sup>6</sup> <https://developer.bluetooth.org/TechnologyOverview/Pages/Profiles.aspx>

<sup>7</sup> <http://course.baidu.com/view/200cac1976c66137ef061910.html>

<sup>8</sup> <https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction>

<sup>9</sup> <http://pcbdesign.hampoo.cn/TechnologyCenter/Detail/270>

<sup>10</sup> <http://blog.csdn.net/ooakk/article/details/7302425>

<sup>11</sup> <http://ee.ofweek.com/2014-01/ART-11000-2807-28772741.html>

<sup>12</sup> [http://www.eet-china.com/ART\\_8800636691\\_617687\\_TA\\_6173ca44.HTM](http://www.eet-china.com/ART_8800636691_617687_TA_6173ca44.HTM)

<sup>13</sup> [http://www.cnblogs.com/zdz8207/archive/2012/10/17/bluetooth\\_ble\\_android.html](http://www.cnblogs.com/zdz8207/archive/2012/10/17/bluetooth_ble_android.html)

<sup>14</sup> <http://developer.android.com/guide/topics/connectivity/bluetooth.html>