普通高等教育规划教材

蓝牙技术基础

喻宗泉　主编

机械工业出版社
CHINA MACHINE PRESS

普通高等教育规划教材

蓝牙技术基础

主　编　喻宗泉
参　编　张有生　喻晗

机械工业出版社

蓝牙技术是近年来产生与发展、用于近距离无线通信的一门新技术。本书从蓝牙技术的基础知识出发，重点介绍一系列相关技术。全书共分7章，内容包括：蓝牙技术基础知识；蓝牙运行信道上的电波传播技术；蓝牙发射和接收技术；蓝牙分组和数据传输技术；蓝牙信息安全技术；蓝牙核心协议；蓝牙开发与测试技术。

本书内容先进、结构新颖、层次清晰、条理分明。在编排上充分考虑到便于教学和自学，文字叙述通俗易懂，尽量避免繁琐的数学推导，注意了在基础内容和较深内容之间的有机衔接，避免跨度太大而使读者难于接受。

本书可作为各类高等院校“蓝牙技术”课程教学用书，也可供信息类、通信类、计算机类专业技术人员、管理人员及自学者学习与参考。

图书在版编目（CIP）数据

蓝牙技术基础/喻宗泉主编 .—北京：机械工业出版社，2006.1
普通高等教育规划教材
ISBN 7-111-18040-2

Ⅰ.蓝… Ⅱ.喻… Ⅲ.短距离-无线电通信：数字通信-通信技术-高等学校-教材 Ⅳ.TN929.5

中国版本图书馆CIP数据核字（2005）第146013号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
策划编辑：刘丽敏
责任编辑：刘丽敏 版式设计：冉晓华 责任校对：魏俊云
封面设计：张 静 责任印制：洪汉军
北京京丰印刷厂印刷
2006年1月第1版·第1次印刷
787mm×1092mm 1/16·11.75印张·284千字
定价：18.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68326294
封面无防伪标均为盗版

前　言

1994年，蓝牙的名称问世，10余年来，蓝牙技术的快速发展不仅仅填补了近距离无线通信的空白，更重要的是极大地推动、扩大并完善了无线通信的应用范围。从一开始人们期待它能取代家用电器之间互连的线缆，发展到今天进入蓝牙微微网中的各种数据与语音能以极为便利的方式完成交换，蓝牙技术越来越受到人们的关注。

用无线连接代替有线连接，有时候看起来很简单：用一个无线电信号发送器和一个接收器就可以了，事实上并非如此，蓝牙技术是一门综合技术，涉及到信息的产生、信息的传递、信息的处理，因此，蓝牙技术是高频电子技术、电磁波传播技术、计算机技术、计算机网络技术、无线通信技术等多种学科交叉形成的一门新型通信技术。随着蓝牙的普及，家用电器、通信产品、网络产品、计算机及其操作系统、日常生活消费品（如汽车）等这些昔日彼此不相干的物品，都会因为引进蓝牙技术变得紧密相连，并且有了一个共同的名称：蓝牙产品。

蓝牙技术由核心技术和规范协议两部分组成。其中蓝牙核心技术由三个部分组成：蓝牙信号的发送和接收，以分组形式的数据传输和信息安全，蓝牙产品的开发和测试。蓝牙规范协议就是蓝牙信号在无线信道传输时应当遵守的游戏规则。

蓝牙技术走进课堂已是大势所趋，本书正是顺应这一潮流而编写，全书以循序渐进的笔法对蓝牙两大组成部分进行了通俗的叙述。全书共分7章。第1章介绍蓝牙基础知识，包括蓝牙的含义及名称由来、蓝牙协议栈的层次结构。第2章介绍蓝牙运行信道上的电波传播技术，分析了无线信道上的传播特征，直射、反射和散射的规律及噪声干扰。第3章介绍蓝牙无线电波发射和接收的技术特征，发射频率的选择及蓝牙设备寻址。第4章分析蓝牙分组传输过程中数据的处理方法和传输控制过程。第5章蓝牙信息安全技术，介绍保障蓝牙信息安全所需的措施。第6章介绍各个核心协议的基本规则及接口。第7章是开发测试技术，叙述了如何开发一个蓝牙产品，如何向SIG提出认证和测试。

为了便于组织教学和自学，本书在章节编排上合理、新颖，层次结构鲜明，既有利于课堂教学，又便于学生自学。每一小节后面有复习思考题，能及时巩固本节所学内容。为了使基础内容和较深内容之间顺利过渡，在陈述上作了有机衔接，避免跨度过大造成阅读困难，对难于理解的内容用足够的篇幅讲解清楚。每一章开头有提示，结尾有小结，后面有习题与思考题，便于读者了解全章全貌。

本书由喻宗泉主编，张有生、喻晗参编。第4~6章由喻宗泉编写，第2、3章由张有生编写，第1、7章由喻晗编写。书稿的录入和图稿绘制工作由丁霄霞完成。全书由喻宗泉统稿。

由于编者水平有限，加之时间仓促，各章节虽经反复推敲，数易其稿，但错误及不妥之处依旧难免，敬请读者批评指正。

征询读者意见E-mail地址：喻宗泉 wjd3g@163．com

编　者

目　录

第 1 章　蓝牙技术基础知识

开发蓝牙技术的目的是将近距离的信息产品实现无线连接，使它们之间安全地完成信息的传递和交换，如同无线通信网络把世界各地的移动通信设备连接起来一样。本章从 3 个方面概括描述这一新技术的基础知识，便于读者了解什么是蓝牙、蓝牙的主要内容以及蓝牙技术的若干特征。

1.1　蓝牙技术简介

1.1.1　什么是蓝牙技术

蓝牙技术不是凭空产生的，而是信息产业发展到了一定阶段必然出现的产物。随着人们生产生活质量的日益提高，在我们周围出现了越来越多的电子产品。例如计算机、电信设备、网络、家用电器、家用汽车的自动控制部分等。这些电子产品在刚开始问世的时候，它们完全是各自独立设计、独立生产、独立存在、独立地为人类服务。随着生产的发展和生活的需要，这些彼此独立的产品开始要求建立联系、实现信息的交换。把它们连成一个整体的方法只能是有线连接和无线连接两种。多年来人们使用电缆线进行有线连接，例如一台计算机就是由主机、键盘、显示器等通过总线连接而成的（总线是传递信息的公共通道）。当接入计算机的电子产品越来越多时，例如再接入扬声器、扫描仪、打印机、摄像头等，连接用的电缆信号线就越多。如果要让计算机和另一些电子产品交换数据，例如移动通信设备、数码相机、数字电视机等，使用的电缆线必然更多、更乱。能否使用“无线通信”的方式代替总线的“有线连接”呢？答复是肯定的。“无线连接”的最大优点就是斩断了每个电子产品的通信电缆线尾巴；最大问题是通信无线电信号不能像电缆线那样由发送源直达接收目的地，而是会向四周散射，接收不可靠性和泄密不安全性大为增加。

蓝牙技术是一种近距离地保证可靠接收和信息安全的无线通信技术。

长期以来，现代通信技术致力于远距离的宽带通信网和全球漫游式的无线通信，企图把全世界的每一个角落都纳入到有线或无线的网络之中，但是近距离的数字通信却一直被忽略，直到 20 世纪末，才提到议事日程。蓝牙技术所要解决的问题是在 10m 范围内实现各种电子产品信息的无线传输，消除它们之间纵横交错的连接电缆，它必须实现如下一些技术要求：

1）完好的替代功能：蓝牙所用的无线通道必须要像有线电缆一样准确无误地发送或接收数据，而无线通道上信息的传播环境比有线通道受到的干扰多得多、传送环境复杂得多。

2）信息安全功能：电波在空间传播时会出现散射现象，于是无线信道传送的保密程度将远低于有线信道，蓝牙信息的安全问题不能忽视。

3）承载能力：同时连接多个设备，要有足够的传输速率，支持不同类型（如声音和数据）的信息的发送或接收。

4）超低功率：设备可用电池供电。

5）致密性高：蓝牙芯片内部结构复杂但体积小。

6）全球通用：使用户能在世界各地方便使用。

蓝牙网络功能：蓝牙技术把计算机、家电、通信等领域中的电子产品使用无线方式连接，自然而然形成一个以使用者个人为中心的网络，称为个人区域网 PAN。这个网络的性质有两条，就是可移动性和自动接入性。所谓“可移动性”是指能随时随地联网或下网，进、入网的终端不受限制。所谓“自动接入”是指蓝牙设备所具备的入网方式不受接入点或服务器的制约，在 10m 空间范围内和接入数量有规定的情况下，自动建立与其他蓝牙设备之间的联系。联系过程是自动完成的，不需要人们的干预。

蓝牙技术的实现有赖于硬件电路和软件程序的双重支撑。硬件电路是一种 $1cm^3$ 的嵌入式微功率芯片，如此小的体积、功率便于它嵌入到普通电子产品中；控制软件的职责是搜索并联系起其他也嵌入有蓝牙芯片的电子产品，联系过程是一场信息交换的过程。信息交换通过发送、接收无线电波实现，发送功率越大，传播的距离就越远。但它们并不成正比，通常 100mW 的发射功率可传输 100m。而 1mW 的发射功率应传输 10m 左右，不能按比例减到只有 1m。

为了实用方便起见，对蓝牙芯片的基本要求有：

1）在 10m 范围内实现一点对多点的通信，一个蓝牙芯片最多可同时与 7 个相同芯片实现无线通信。

2）蓝牙数据传输速率有效值应达到每条信道 721Kbit/s，是普通电话线的 13 倍左右，最高 1Mbit/s。

3）使用频段 2.4～2.4835GHz，这一频段属工业和医疗的自由频段，无需申请无线电波使用许可证，方便在全世界推广使用。

4）要求成本低廉，价格与所取代的电缆线基本持平，例如批量生产的蓝牙芯片产品，成本尽量控制在 5 美元左右。

近期蓝牙的主要目标是取代各种电缆连接，通过统一标准的无线链路网将数字设备连成一个密不可分的整体，方便灵活、低成本、低功耗，像移动通信那样传输语音，像互联网那样传输信息。蓝牙的主要长远目标是占领家用和商用的近距离数据传输市场。

1.1.2 蓝牙名称的由来

1. 蓝牙技术的命名

1994 年，瑞典爱立信公司移动通信部在一项课题研究中，确定使用无线电射频技术实现移动电话与周围器件之间的低成本、低功耗的无线互联，并将互联的技术规范命令为蓝牙（Bluetooth）。

将这种近距离的无线通信技术规范称之为“蓝牙”，反映了技术规范研制人的思维方式和思维活动。目前对这一名称来源的解释有多种，一种说法是和狼的牙齿有关系，狼牙虽然参差不齐，错落有致，但这颗颗都能穿透猎物的牙齿却能紧密地啮合，在月夜里反射出闪闪的蓝光。各种原理用途不相同的家用电器或其他一些工具中，每一件都能给人们生活带来方便，使用蓝牙规范却能让它们成为一个整体。

还有一种说法是 Bluetooth 来源于公元 10 世纪一位丹麦国王的名字，这位国王名叫

Harald Gormsson，他在担任国王之前曾是一个海盗首领，传说因他厚爱吃蓝莓致使牙齿染成了蓝色，于是落下了 Blatand 的外号，而 Blatand 译成英文就是 Bluetooth。Harald 国王生于公元 908 年，一千多年后在瑞典还有人记起他的蓝牙齿，那是因为他曾为民众做了许多好事。他穿梭于各种派别之间进行协调、沟通，不是依靠武力，而是通过协商与谈判，将种族冲突不断、海盗猖獗、酋长分割的丹麦和挪威统一起来。建立起横跨斯卡格拉克海峡两岸的 Danes 王朝，使国民生活好起来，并从此信奉耶稣基督。今天，在瑞典 Lund 城爱立信研发中心的大门口，一块于 1999 年树立的蓝牙纪念碑上，依旧刻着耶稣的圣像，只不过耶稣一手拿着掌上计算机，一手拿着移动电话，象征着蓝牙技术将计算机领域、通信领域、家电产品联系在一起。

在蓝牙技术飞速发展的几年时间里，人们已经不再过多关心它的名字是来自于狼的牙齿，还是来自于国王的牙齿，而是热衷于它的技术规范给信息产业带来的新变化。

“Bluetooth”传入中国后，在大陆将其直译为“蓝牙”；在台湾省被译为“蓝芽”，寓意着蓝色的无线通信新技术正处于萌芽状态。

2. 蓝牙名称的认同和蓝牙 SIG 组织

爱立信公司提出“蓝牙技术规范草案”，是在开展一项重大课题的研究之后，这项课题就是研究把各种各样的通信设备通过移动电话接入蜂窝式移动通信网。爱立信公司的研究从一开始就引起了一些大公司的注意。1998 年 2 月，由世界上最有名的 5 个 IT 产业公司（爱立信、Intel、IBM、东芝、诺基亚）发起组建“蓝牙特殊利益小组”（Special Interest Group，SIG），小组的任务是制订蓝牙技术标准、如何测试蓝牙产品、协调各国蓝牙技术的使用频段。SIG 于 1998 年 5 月正式成立，1999 年 12 月，又有 4 家公司（3Com、微软、摩托罗拉和朗讯）加入 SIG。这样一来，上述 9 个公司成为 SIG 的创始成员和领导成员，通常把这 9 个公司称为 SIG 的倡议者，后来加入的其他成员被称为 SIG 的响应者。

微软加入 SIG 有着深层次的考虑。1999 年 11 月，比尔·盖茨专程拜访了拉斯维加斯的一个仅有 11 名员工的小公司，这家公司已研制成功装配有蓝牙技术的一种胸卡。考察后，微软于 1999 年 12 月宣布全面支持蓝牙并参加 SIG。在这些大公司的影响下，2000 年 4 月，参加 SIG 的公司已达到 1790 家，2001 年 6 月激增到 2491 家。在各种通信或网络方面的国际组织中，SIG 的成员无疑是最多的。从行业来看范围也是最广的，其中有名的成员有：

通信行业：爱立信、诺基亚、西门子、AT&T、摩托罗拉、日立、英国电讯、阿尔卡特等。

IC 生产行业：Intel、Philips、松下、三星、AMD、TI 等。

计算机硬件行业：IBM、NEC、惠普、康柏、宏碁、戴尔等。

计算机软件行业：微软等。

汽车行业：宝马、沃尔沃、福特、Delco 等。

家用电器及外围 I/O 设备等行业：东芝、卡西欧、爱普生、LG、夏普、索尼、TDK、松下、三菱重工、三洋等。

网络产品行业：3Com、朗讯等。

SIG 有如此的吸引力，是因为蓝牙名称已被普遍认可，发展蓝牙技术已是大势所趋，并且参加 SIG 的成员享有一系列的优惠条件。SIG 已经拥有两千多个成员，称其为“小组”似乎不太合适，因此，中文译名近来将其译为“蓝牙特殊利益集团”。

SIG 规定，加入 SIG 的条件是愿意签署《蓝牙 SIG 成员协议》而不收取任何费用，该协议规定了 SIG 成员的权利和义务。SIG 成员必须尽到的义务是：

1）将自己开发的蓝牙相关技术无偿地贡献给小组其他成员。

2）研制开发的蓝牙产品必须符号蓝牙协议规范。

3）产品要想使用蓝牙标识，必须事先通过蓝牙认证。

SIG 成员享有的权利是：

1）免费使用蓝牙协议及相应的所有专利。

2）可以使用蓝牙商标。

3）在通过蓝牙认证后，可以使用蓝牙标识。

4）在蓝牙协议向社会公开之前，可以优先获得该项协议。

5）在正式蓝牙协议公布前，可先期得到该项协议。

蓝牙 SIG 组织的职责是：

1）制订《蓝牙 SIG 成员协议》，吸引新的成员。

2）制订、修改和完善蓝牙协议。

对小组成员生产的蓝牙产品完成认证，考核该项产品是否符合蓝牙协议。认证的具体内容是看其是否满足蓝牙无线链接、蓝牙有关协议、应用规范、信息安全等方面的要求；看其是否满足销售国无线电管理的要求。

SIG 是一个适应市场需求的、开放的国际标准化组织，是由生产厂家自己发起的、以自身利益为出发点的组织，它不是一个由各国政府决定的机构。只要是 SIG 成员，都有权无偿使用新技术，无偿使用蓝牙专利而不交任何费用。小组成员都可以无偿使用蓝牙规范指导生产，并且一旦通过认证就可以畅通无阻地进入市场，而对希望加入 SIG 的公司不分大小、不分行业、不受歧视。SIG 组织的迅速扩充正是由于它的开放性所决定的。

在 SIG 之前，已经有过一些因技术开放而成功、因技术保守而失败的例子。风靡全球的 IBM-PC 计算机正是因为其硬、软件的公开，已经牢牢占据计算机市场的主导地位，有的品牌计算机因技术资料开放程度不够致使所占市场分额甚少，甚至还有曾经辉煌过的品牌最后不得不破产。又如互联网的迅速普及与发展，与开放的网络管理和通信协议密不可分。SIG 顺应了这一历史潮流，它联合起不同的产业、部门从事技术开发和实际应用，从而获得了普遍认可，赢得广泛支持，使参与其中的每一个成员都有事可作，有利可图。如此多的精英汇聚在 SIG 中，从古至今极为罕见。

SIG 是一个非营利的科研、生产、营销厂商组织，它的主要职责是制订蓝牙技术规范和推广蓝牙技术。9 个倡议者的分工是制订规范并开发市场项目，其他响应者只需签署《蓝牙 SIG 成员协议》，保证自己的产品符合蓝牙技术规范。SIG 由 7 个委员会组成，它们是管制委员会、法律委员会、测试和互操作委员会、管理业务委员会、结构检查委员会、市场开发委员会和认证委员会，各委员会有不同的分工。管制委员会的任务是协调与各国的关系、制订有关安全管制、航空管制等相关政策；法律委员会的任务是负责蓝牙知识产权等法律问题；测试和互操作委员会的主要工作是承担蓝牙技术应用中的测试和互操作；管理业务委员会负责 SIG 的日常业务；结构检查委员会检查各 SIG 成员开发的蓝牙产品是否符合蓝牙协议；市场开发委员会主要负责开发蓝牙市场；认证委员会负责 SIG 成员提出的蓝牙产品认证要求。

SIG 在成员之间交换信息使用 3 种文档：一种是协议，用于规范从无线层到应用层的具

体要求；一种是剖面，用于规范应用层中各协议的使用；一种是测试，反映协议和剖面的测试过程。蓝牙 SIG 每年召开 3 次蓝牙年会（UnPlugFests），年会是 SIG 为其成员利益举行的会议，主要讨论产品互操作性测试方面的问题，为各种蓝牙产品提供测试机会。

1.1.3　蓝牙技术特征

1999 年 7 月，蓝牙 SIG 推出蓝牙规范 1.0 版本，版本中提出了蓝牙技术的主要技术指标和系统参数，见表 1-1。系统参数主要以满足美国联邦通信委员会 FCC 的要求为基准制订的，如果用到其他一些国家，还需适当作一些修改。该表所列各项技术特征是对蓝牙系统的最低要求，少数个别指标没有作特别规定。从实际执行情况看，蓝牙产品的指标大多已经超过这些标准。

表 1-1　蓝牙技术的主要技术指标和系统参数

技 术 指 标	参 数 说 明
工作频段	ISM 频段，2.402 ~ 2.480GHz
工作方式	全双工，时分双工
业务类型	支持电路交换和分组交换业务
最大数据传输速率	1Mbit/s
非同步信道速率	非对称连接 721/57.6Kbit/s，对称连接 433.9Kbit/s
同步信道速率	64Kbit/s
发射功率	美国 FCC 要求 < 0dBm(1mW)，其他国家可扩展为 20dBm(100mW)
跳频频道数	79 个，每个频道带宽 1MHz
频道带宽	1MHz ± 140kHz(电平 1)，± 175kHz(电平 0)，按 - 20dB 定义
跳频速率	1600 次/s
工作模式	等待(Park)/保持(Hold)/呼吸(Sniff)
数据连接方式	面向连接的同步链路 SCO，面向无连接的异步链路 ACO
纠错方式	1/3FEC，2/3FEC，ARQ
鉴权方式	质询-响应
信道加密	采用 0 位、40 位、60 位密钥
调制技术	二进制 GFSK（$BT = 0.5, 0.28 < h < 0.35$）
语音编码技术	PCM，CVSD
接收机灵敏度	- 70dBm@ 0.1%位误差率
最大传输距离	10m

复习思考题

1. 蓝牙技术诞生于哪一年？
2. 对蓝牙芯片的基本要求是什么？

1.2 蓝牙技术协议

所谓“协议”是游戏双方为使游戏顺利进行而共同认可且遵守的一种规则，离开了游戏规则，游戏将无法进行。蓝牙协议就是使用蓝牙技术的各方共同约定的技术规范。主要蓝牙协议的集合，构成了蓝牙协议栈。在蓝牙协议栈内，各种协议并不是杂乱无章地堆放在一起，而是有层次地按序排列，形成了蓝牙独有的协议体系结构。

1.2.1 蓝牙技术协议的体系结构

蓝牙协议体系由 3 层组成，分别是底层、中间层和应用层，如图 1-1 所示。底层有一些硬件模块：射频 RF、基带层 BB 和链路管理层 LM。中间层由软件模块构成，包括逻辑链路控制和适配协议 L2CAP、服务发现协议 SDP、串口仿真协议 RFCOMM 和电话通信协议 TCS。应用层位于最高端，对应各种应用模型的剖面，目前定义了 13 种剖面。

1. 底层

底层又称底层硬件模块，其中射频 RF（Radio and Antenna）的功能是完成数据位流的过滤和传输。由数据位形成的数据位流在一位一位地通过 RF 时，要求 RF 满足 ISM 频段传输 2.4GHz 微波的一系列要求。2.4GHz 的 ISM 频段是工业、科学和医疗频段，使用时无需授权。在蓝牙技术的工作频段内，要求蓝牙设备提供 720Kbit/s 的数据交换速率。射频 RF 的功率定义有 100mW、2.5mW 和 1mW3 种，不同的功率有不同的传输距离指标，例如蓝牙设备功率为 1mW（0dBm）时，发射半径约为 10m，发送时采用跳频技术消除干扰、减少衰落；采用功率控制技术控制发射功率。

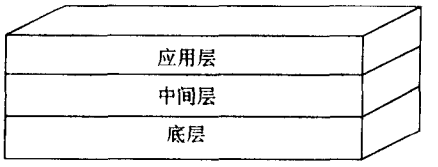

图 1-1 蓝牙协议体系

基带层 BB（Base Band）的功能是实现蓝牙数据传输或信息帧的传输。传输业务分为电路交换和分组交换两种不同类型。

链路管理协议（Link Manager Protocol，LMP）用于规定如何建立和拆除连接，以及链路的控制和安全。蓝牙技术定义了两种不同的链路类型：面向连接的同步链路 SCO 和面向无连接的异步链路 ACL，每种链路容许 16 种不同的分组，其中有 4 组是控制分组。同步链路 SCO 的发送特征有两个：一个是链路建立之前，必须先建立异步链路 ACL 传送控制信息；另一个是链路一旦建立，主从节点无需查询便可直接发送 SCO 数据组，发送时间是在保留的时隙内，这就要求 SCO 数据包结构对称，同时包括 1 个、2 个或 3 个时隙。SCO 数据包既可以用于传送语音，又可以用于传送数据，只不过限于重发被损坏的数据。ACL 数据包无论是发送还是接收，都应当有奇数个时隙，便于整个帧的时隙成为偶数。

ACL 链路的带宽由蓝牙网的主节点控制，蓝牙网是一种微微网（Piconet）。最多限于 256 个蓝牙设备连接而成，处于工作状态的只有 1 个主节点和 7 个从节点，网上其他多余节点均处于空闲状态。从节点在发送数据前，必须接受查询，只有被主节点选中才允许发送，每个从节点占用的带宽也由主节点决定。主节点的另一功能是决定了微微网中连接的对称性。

由多个相互重叠的微微网组成的网络称为散射网（Scatternet），散射网中的各微微网之

间允许重叠、允许交叉、允许共享从设备。网络中的底层硬件模块构成了蓝牙技术的核心内容，是任何一个蓝牙设备必须具备的部分。在使用这些硬件模块时，为方便起见，蓝牙技术规定了连接时的节能状态、纠错方式、系统的移动性和安全性。

连接时的节能状态有 3 种，分别是等待（Park）、保持（Hold）和呼吸（Sniff）状态，目的是为了保证较低功率场合中蓝牙设备也能实现连接。所谓“等待状态”是指节点被赋予 Park 地址（又称 PMA 地点），按一定的时间间隔监听主节点的声音。主节点能够发出的声音信号有 3 种：一是询问该节点是否愿意成为活动节点；二是询问其他正在“等待”的节点是否愿意成为活动节点；三是广播消息。所谓“保持状态”是指节点保持停止传送数据，只有在激活后才重新开始传送数据。所谓“呼吸状态”是指从节点时睡时醒，从微微网收听信息的速率明显降低。从节能效果看，Park 最好，Hold 其次，Sniff 最低。

蓝牙技术采用了 3 种纠错方式，分别是 1/3 前向纠错 FEC、2/3 前向纠错 FEC 以及自动重发 ARQ。不同的链路有不同的链路管理，SCO 链路选用 1/3 前向纠错；ACL 选用 2/3 前向纠错；在无编号发送中选用自动重发方式，这时接收端要么向发送端发送一个确认正确收到数据的信息，要么发送一个没有收到的错误消息，如果是后者，发送端将自动重发。对比起“自动重发”，“前向纠错”能减少重发的可能，特别适合于信道中噪声较大的场合。选用哪种纠错方法可以在软件中定义。

蓝牙安全问题是由于蓝牙技术的移动性和开放性引来的，尽管蓝牙跳频技术本身有一定的安全系数，但链路层和应用层的安全管理依旧十分重要。链路层中的安全措施是为每一个用户提供一个个人标识码 PIN，蓝牙系统将其翻译成 128 位的链路密钥（Link Key）并进行单双向认证，蓝牙安全机制提供了大量的认证方案。认证完毕后，链路使用不同长度的密码将其加密，加密方案机动灵活到允许协商密码的长度，不同的国家规定有不同的密码长度，例如美国的密码长度为 128 位，西班牙的密码长度仅为 48 位。如果美国和西班牙的蓝牙设备互相通信，链路自行选择长度 48 位来加密。蓝牙系统有能力为连入微微网中各蓝牙设备选择较小的最大容许加密长度。

2. 中间层

中间层又称中间协议层软件模块，其中的逻辑链路控制和适配协议（Logical Link Control and Adaptation Protocol，L2CAP）具有拆装数据、控制服务质量和协议复用等功能，为中间层其他协议提供实施基础，是蓝牙协议栈的核心之一。L2CAP 向上层提供面向连接或无连接的数据服务，允许上层协议和应用层发送或接收多达 64KB 的数据分组，并且能完成分组的分割或提取、重新组装等。

服务发现协议（Service Discovery Protocol，SDP）的作用是为上层应用层给出一种机制，该机制能发现网络中的可用协议，并解释这些可用协议的特征。蓝牙环境和普通网络环境下的服务发现存在较大的差别：蓝牙环境中由于移动 RF 环境变化显著，因此业务参数均在不断地变化；普通网络环境下的服务发现却没有如此明显。SDP 突出了蓝牙环境，使得只要使用基于客户/服务器机制，就能按照蓝牙服务类型和属性定义发现服务的方式。

电话通信协议（Telephone Control Protocol，TCS）用作提供蓝牙设备间语音和数据的呼叫控制指令，它是一个面向 bit（位）、基于 ITU-T 控制规范的协议，对语音的支持是蓝牙技术与 WLAN 的重要区别。

串口仿真协议 RFCOMM 用于射频通信，它能依据 ETSI0710 串口仿真协议，在 L2CAP 上

仿真 RS-232 九针串口电缆接口，蓝牙设备能在无线传输中通过 RFCOMM 实现对 TCP/IP、PPP、WAP 等高层协议的支持；通过支持 AT 命令集实现移动通信设备、传真机和调制解调器之间的无线连接。

3. 应用层

蓝牙应用层由 SIG 定义了一些基本应用模型，每一种应用模型都对应一个“剖面”，规范了相应模型的功能和使用协议。不同厂家在生产时只要遵照相同的“剖面”，彼此产品之间就能互通。常见的一些应用模型有文件传输、数据同步、局域网接入、拨号网络、头戴式耳机、对讲机、无绳电话等。

文件传输是指蓝牙设备之间传送各种数据信息文件，包括 Excel 文件、PowerPoint 文件、声音文件、图像文件、Word 文档等，传送时整个文件夹、目录或流媒体格式都允许，用户既可以浏览其他蓝牙设备上的文件夹，也可以新建或删除文件夹。传输文件的设备显然要求是蓝牙设备，如计算机、智能电话或 PDA，不论哪一种设备，从传输角度看，可以归结成客户/服务器。客户能从服务器下载，也能向服务器发送文件。服务器是一种使用 OBEX 文件夹列表格式的远端蓝牙设备，要求其支持目标交换服务、支持文件夹浏览功能，还要求其允许客户修改、创建文件夹或文件。

数据同步在两个通信设备进行通信时必不可少，只有同步，才能让信息正确无误地传送，也能保证用户在任何时候、选择任何蓝牙设备，都能正确获得信息。与其他的数据同步信息比较，蓝牙设备数据同步还有一个鲜明特征，就是接收设备既可以处于通电工作状态，也可以处于休眠状态，甚至还可以处于未开机状态。例如移动电话接到一条消息，就可以把该消息发送至笔记本电脑，而笔记本电脑甚至允许在包中没有开机。显然，数据同步能够使不同蓝牙设备的“个人信息管理”（Personal Information Management，PIM）成为现实。需要传送的数据信息通常包括电话本、消息、日历、备忘录等，传送的协议或格式由收发双方共同确认，例如当移动通信设备靠近笔记本电脑时，允许其自动与笔记本电脑同步。数据同步模型需要 IrMC 客户和 IrMC 服务器的支撑，在 IrMC 客户端有一个同步机，功能是向 IrMC 服务器上传或下载 PIM 数据，提供接收同步初始化命令，此外也可以暂时充作服务器使用；IrMC 服务器提供目标交换服务，如果提供同步初始化信息，也暂时充当客户使用。常见的 IrMC 客户有个人计算机或笔记本电脑，IrMC 服务器有移动电话。

局域网接入模型允许多个数据终端采取无线接入方式从同一个接入点进入局域网，一旦连接成功，数据终端便能享受局域网提供的一切服务，两个不同类型的蓝牙设备便能直接对话。蓝牙设备要想访问局域网，需遵从蓝牙标准 V1.0 中定义的 PPP 协议，在连接时也要采用相同的 PPP 结构。PPP 是由 IETF 制定的能够解决接入网络时授权、加密、数据压缩等操作的协议。“局域网接入”离不开接入点 LAP 和数据终端。LAP 起 PPP 服务器的作用，提供的接入服务包括家庭网络、USB、Cable Modem 、Firewire、以太网以及光纤令牌网等。数据终端起 PPP 客户的作用，它与一个 LAP 建立起 PPP 连接，构成局域网接入，接入后，数据终端就能享受 LAP 提供的服务。笔记本电脑、PDA、个人计算机是常见的数据终端。

拨号网络是一种不同于上述模型的服务器，在这种模型中，通常使用蓝牙移动电话、蓝牙 Modem 构成“互联网网桥”，例如个人计算机访问拨号网络时就可以利用移动电话作为无线 Modem 使用，或者用个人计算机接收数据。在这种应用中，移动终端设备或 Modem 就是接入到公共网络的网关，个人计算机或笔记本电脑就成为终端，享受网关提供的服务。在网

关提供服务和终端享受服务之前，必须进行初始化，包括 PIN 码转换、链路密钥 Link Key 创建、实施完“服务发现”等，在发出呼叫或接收呼叫前建立起物理链路。网关和数据终端间通过虚拟串口实现通信。

头戴式耳机在蓝牙技术中作移动通信终端和个人计算机的语音输入、输出接口用，它能够让用户摆脱通话电缆的约束。为了不用手动就能让用户摘机、挂机，头戴式耳机必须能发送 AT 命令且能接收相应的编码信号。

对讲机是一种具有同时发送和接收功能的蓝牙设备，为了使两个蓝牙设备近距离建立直接语音通路，使直接对讲成为可能，链路必须首先建立并使用基于电话的信令，语音调试方式可选用 PCM 调试或 CVSD 调试。

无绳电话意味着室内近距离无线通信成为现实，内置蓝牙芯片的无绳电话通过基站接入 PSTN 进行语音传输，从而有效地降低了通话成本。无绳电话模型依旧定义有网关和终端，网关是外部网络的终点，收纳所有进入网络的通信信息，它能起到外部网络呼叫、建立请求中心的任务，进入或来自外部网络的呼叫都由网关处理。有的网关能同时支持多个活动终端，有的网关只能支持一个活动终端。从蓝牙设备种类看，能成为网关的只能是卫星基站、GSM 基站、H .323 基站、PSTN 或 ISDN 家庭基站；作终端的只能是无绳电话、双模蜂窝电话或个人计算机等。

蓝牙应用层为蓝牙产品开发、生产商提供了一些不同的模型，随着蓝牙技术的发展，新的蓝牙应用方式还会不断地出现。应用层面的开发也给人们的生活带来日久深远的影响。不久的将来，一系列实际应用将会进入人们的生活之中。例如，当你乘坐公交车的时候，你的手机将会自动为你付费；当你付费消费时，刷卡可能会被淘汰；当你还在为公务繁忙的时候，可能会自动接收到亲人平安回家的信息；你还可以用手机或无绳电话开启汽车车门，或是驱动自动驾驶装置将车从车库里开到家门口，恭迎你的光临。

1.2.2　蓝牙核心协议

蓝牙协议按其实施的功能可以划分成 4 类：

1）蓝牙核心协议：有基带 BB、链接管理 LMP、链接控制和适配 L2CAP、服务发现 SDP 协议。

2）蓝牙电缆替代协议：有串口仿真 RFCOMM 协议。

3）蓝牙电话控制协议：有电话通信 TCS 协议、AT 命令集。

4）蓝牙选用协议：有 PPP、UDD/TCP/IP、WAP、OBEX、WAE、VCard、VCal、IrMC 等。

在以上 4 类协议中，最主要最基本的是蓝牙核心协议，蓝牙设备基本上都需要核心协议（此外，还需要无线规范），其他协议按蓝牙设备的需要而选定。

基带协议 Base Band 是为微微网内各蓝牙单元用射频构成物理链接而设立的。蓝牙射频系统是一个跳频系统，它的任一个分组应在指定的频率和时隙内发送，并且可以通过查询使每一个蓝牙单元发现发送范围内的单元及它们的地址时钟，也还可以通过呼叫确定实际连接的单元。基带数据分组有面向连接和无连接两种方式，并在同一射频范围内实现多路数据传送。

链路管理协议 LMP 用于链路的设置与控制，它能够建立或清除蓝牙单元之间的连接、功率控制、认证和加密。

链路控制和适配协议 L2CAP 和 LMP 都位于 ISO/OSI 七层协议的第二层链路层，它们的

工作是并行的，致使基带数据业务可以越过 LMP 直接通过 L2CAP 把数据传送到高层。L2CAP 允许高层按 64KB 长度分组或传送。虽然基带协议提供有面向连接和无连接两种物理连接方式，但 L2CAP 只支持无连接这一种。

服务发现协议 SDP 的功能是：用户只有通过它才能获得设备信息、服务信息和服务特征，蓝牙单元之间有不同的 SDP 连接，才能适应各种不同用户的需求。

1.2.3 蓝牙协议栈

蓝牙协议体系中的底层、中间层、应用层三层叠放形成了蓝牙协议栈，如图 1-2 所示。图中给出了常用部分协议。

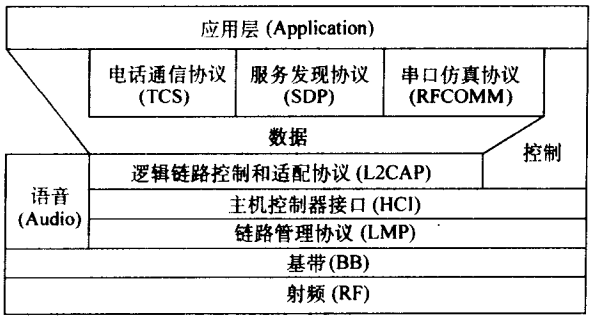

图 1-2 蓝牙协议栈

底层硬件模块的上面是中间协议层，两层之间的接口使用主机控制器接口 HCI（Host Controller Interface），HCI 的功能是解释并传递两层之间的消息和数据。由于底层是硬件层，中间协议层是软件层，HCI 成为硬、软件之间必不可少的接口，软件通过 HCI 调用底层 LMP/BB 和 RF 等硬件。HCI 以下的功能由蓝牙设备实施；HCI 以上的功能由软件运行在主机上实现。HCI 对于上、下两层数据的传输都是透明的。

进入 21 世纪后，蓝牙 SIG 在蓝牙规范 1.0 版本基础上又陆续推出了新的版本。版本规范了蓝牙协议栈使用分层结构实现数据流的过滤与传输。各协议按其用途可以分为专用协议和非专用协议，前者如 L2CAP 和 LMP，后者如对象交换协议 OBEX 和用户数据报协议 UDP。在众多的蓝牙协议中，使用协议栈有利于理清各协议之间彼此的关系，让高层协议尽可能发挥它们自身的功用。考虑到高层协议都应当以物理层和数据链接层作为基础，蓝牙技术使用开放性的规范版本能让 SIG 各成员自由自在地选用专用协议或者习惯性地使用非专用协议。

复习思考题

1. 蓝牙协议体系采用分层结构有什么好处?
2. 蓝牙协议按功能划分成几类?

1.3 蓝牙技术应用

蓝牙技术是一门实用技术，从它诞生的那一刻起，无不和它的应用联系在一起。蓝牙技术规范具有直接左右蓝牙产品的鲜明特征。

1.3.1 蓝牙产品

内置蓝牙芯片且遵守蓝牙技术协议的产品称为蓝牙产品。能够满足这一条件的产品非常多，涉及的领域也相当广泛，但是最早进入市场的蓝牙产品却是在蓝牙规范 1.0 版本问世两

年以后，其间的研制、开发、认证都需要时间，需要一个认识并完善的过程。2001 年 8 月 9 日，在 2001 年 2 月由 SIG 新推出蓝牙规范 1.1 版本后 6 个月左右，瑞典爱立信公司在中国的台湾推出世界上第一台内置蓝牙芯片的手机，型号 T39m/mc，该手机具有 3 种蓝牙功能：

1）在办公室或家庭内，使用蓝牙耳机可在 10m 范围内接听无线电话。

2）10m 范围内无限连通笔记本电脑让其上网。

3）两名 T39mc 用户能通过手机交换名片、对打游戏。

近几年来，蓝牙产品通过 SIG 认证的已超过 400 种，这些产品大体有两种类型，一类是在已有的家用电器产品上增加蓝牙功能，如手机、耳机、笔记本电脑、掌上计算机、照相机、摄像机、接入设备等。另一类是以蓝牙功能为主的新产品，如无线移动硬盘、无线电子钱包、蓝牙笔、蓝牙手表、蓝牙电子衣、蓝牙音乐衣、蓝牙虚拟键盘、蓝牙收音机、蓝牙点菜宝、蓝牙电子书、蓝牙股票机、蓝牙标签等。

1. 蓝牙手机

在一切使用蓝牙技术的产品中，蓝牙手机对蓝牙技术的推广使用无疑具有极其重要的作用。蓝牙手机的发展经历三个阶段：第一阶段以爱立信公司的 T36 型手机为代表；第二阶段以爱立信公司的 T39 型手机为代表；第三阶段的代表是众多移动电话商所研制和生产的功能各异的手机。

T36 手机是爱立信公司于 2000 年在新加坡举行的亚太通信技术展览会上推出的世界上第一台外挂蓝牙模块手机，能够无线连接其他蓝牙设备，与该公司其他蓝牙设备一起使用。例如想拨打电话或电话铃响表示有电话时，可以按动蓝牙耳机上的一个键通过 T36 发出呼叫或接听声音；此外，还可以使用语音命令浏览菜单系统，在手机存储器中存储语音备忘录。T36 支持全世界 120 多个国家使用的 GSM 频率（含 900MHz、1800MHz、1900MHz）以及高速电路交换数据（HSCSD）业务。其通话时间和待机时间分别是 455min 和 200h。该机有 T36m 和 T36mc 两个子型号，其中 T36mc 还带有 1 个简单易学的中文界面，便于发送、接收中文短信业务（SMS），可在机内电话簿上存储中文信息。

T39 手机的突出优点是第一款将蓝牙芯片集成在内部的手机，从而结束了在此以前移动电话需要外挂蓝牙插件才能具备蓝牙功能的历史。在使用时，T39 手机也需要配合蓝牙耳机使用，手机可以放在衣兜或挎包里，只用耳机完成接听或通话，耳机和手机之间无线连通。T39 手机能无线连接的蓝牙设备多至 7 个，包括掌上计算机、笔记本电脑和其他蓝牙设备。除打电话外，还可以与其他 T39 用户交换电子名片、电话簿、日程表、响铃音乐、网球游戏、无线对打等。它的一些主要功能有：

1）无线接入功能：支持 GSM 3 种频率，900MHz、1800MHz、1900MHz。使用距离为 10m 范围内自由通话。

2）漫游功能：一机在手，漫游世界 120 多个国家。

3）传输功能：支持通用分组无线业务 GPRS，传输速率 115Kbit/s，比一般 GSM 上网速度快 4 倍以上。GPRS 的突出优点是能让用户持续占线，但只在传输数据时收费。

4）浏览功能：由于该手机内置 WAP1.2.1 版浏览器，使得解码 WAP 的密码、认证用户与服务器成为可能。

5）高速交换功能：传送速率比 GSM 的快 3 倍，可达 28.8Kbit/s，支持 HSCSD（高速电路交换数据）技术。