

网络应用热点系列

# 无线局域网

WANGLUO YINGYONG REDIAN XILIE

牛 郭 吴 李  
伟 世 志 新  
    泽 军 生  
    等 等 审  
    编 著 校

- 安全隐患
- 系统的配置和安装技术
- 面临问题及解决方案
- 相关协议
- 硬件组成
- 互连结构设计技术
- 接入技术

# 无线局域网

牛 郭 吴 李  
世 志 新  
伟 泽 军 生  
等 等 审  
编 著 校

WANGLUO YINGYONG REDIAN XILIE

人民邮电出版社

## 图书在版编目 (CIP) 数据

无线局域网/牛伟等编著. —北京: 人民邮电出版社, 2003.9  
(网络应用热点系列)

ISBN 7-115-11505-2

I. 无... II. 牛... III. 无线电通信—局部网络 IV. TN925

中国版本图书馆 CIP 数据核字 (2003) 第 065539 号

## 内 容 简 介

本书从无线局域网的基本概念和起源谈起, 详细讲述了无线局域网的互连结构、硬件组成和设计技术、协议及接入技术、系统配置安装等; 另外还介绍了无线局域网的安全隐患、面临的问题和解决途径; 最后结合案例, 介绍了无线局域网的实际应用。阅读本书后, 读者能对无线局域网这一项新兴技术有一个比较全面的了解。

本书适合于网络工程人员、技术人员, 大专院校师生, 对无线局域网络安装、配置和安全等问题感兴趣的读者阅读。

### 网络应用热点系列 无线局域网

◆ 编 著 牛 伟 郭世洋 吴志军 等  
审 校 李新生  
责任编辑 张丽华 汤 倩

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号  
邮编 100061 电子函件 315@ptpress.com.cn  
网址 <http://www.ptpress.com.cn>  
读者热线 010-67132692  
北京汉魂图文设计有限公司制作  
北京密云春雷印刷厂印刷  
新华书店总店北京发行所经销

◆ 开本: 787×1092 1/16  
印张: 18  
字数: 432 千字 2003 年 9 月第 1 版  
印数: 1-4 000 册 2003 年 9 月北京第 1 次印刷

ISBN7-115-11505-2/TP·3550

定价: 26.80 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

主 任：葛乃康

副主任：王 群 邱瑞华

主 审：郭世泽

编 委（以姓氏笔画为序）：

丁 方	王伟东	王春海	牛 伟	吴志军	李文明
李林茹	李晓天	李晓非	李新生	张静妙	何韶军
陈书旺	邱盛藩	周小平	赵树霞	胡 云	胡文颜
费瑞金	钟建业	段 榕	高双喜	高顺清	唐 烨
倪素虹	崔健悦	鲁士文	熊 华	赫晓峰	

# 丛书前言

作为现代信息基础的网络技术，其发展和应用受到了全社会的普遍关注。面对各种纷乱繁杂的网络技术，我们根据读者的实际需要，紧紧围绕“热点应用”这一主题，在对众多技术和实例进行筛选和分类汇总的基础上，组织和策划了《网络应用热点系列》图书。

本系列书从选题的策划，到每本书大纲的确定，再到具体编写和最后的审校，都本着严谨和对读者高度负责的态度，在每一个环节上都做了大量细致的工作。2002年12月，人民邮电出版社邀请了国内网络界知名专家及本系列书的所有作者参加，在北京对本系列书的读者定位、写作内容、写作方式以及写作中的各种注意事项进行了全面细致的讨论，最后从初步列出的20多个题目中精选了7个作为本系列第一批推出的图书。

这7本书是：《网络入户——最后1公里》、《上网用网任我行》、《无线局域网》、《揭开黑客的面纱》、《手机上网全接触》、《网络安全——取证与蜜罐》和《闪客必由之路》。

在本系列书的具体写作中，始终将作者的写作思路、编辑的编审要求和专家的指导紧密结合在一起，每一本书甚至是书中的每一个章节，从写作到专家审校再到编辑加工都进行了严格细致的把关。其中，许多内容都是几易其稿，力求内容的全面和表述的准确。

本系列书立足于网络基础知识和基本应用，在写作中切实考虑到读者的具体需要，在内容上力求能较为全面地反映目前网络应用的热点，并且注意基本理论、概念与实际应用的有机结合，使读者通过应用，掌握相关的概念，从而为学习其他相关的网络知识打下坚实的基础。如果说反映热点应用是本系列书的一大特点，那么内容新颖是本系列书的另一大特色。其中，像网络安全中的取证与蜜罐技术和无线局域网的组建与管理等内容，目前在国内尚属较为先进的技术，这些内容不但具有先进性和前瞻性，同时还具有较高的应用价值。另外，像最后1公里和防黑反黑技术等内容是目前非常热门的应用技术，全面掌握这些技术能使读者更符合目前社会所需人才的标准。还有，像《上网用网任我行》和《手机上网全接触》中的内容，则是目前普通用户和读者需要掌握的知识。因此在这两本书的写作中，我们也充分考虑到了这部分读者的具体特点和要求，从最简单的基础知识和基本操作入手，一点点、手把手地教会读者使用网络和通过网络进行学习的方法。

虽然编者力求这套书的完美，但是考虑到技术和用户实际需求等因素，本系列书的某些内容可能还不够完善，甚至还会存在一些不妥之处。为此，希望读者在阅读本系列书后，能够将您的意见和建议反馈给我们，以便再版时做必要的补充和修改。

编者

2003年4月

## 编者的话

随着信息技术的飞速发展，人们的工作、生活越来越离不开计算机网络。无论是信息共享、合作，还是移动用户办公，处处体现着计算机网络的價值，计算机网络已经无所不在。无线局域网是传统有线局域网的延伸和补充，是一种更加灵活的数据通信系统。无线局域网采用射频工作方式传输和接收数据，在有线局域网的基础上通过无线集线器（Hub）、无线接入节点（AP）、无线网桥和无线网卡等设备使无线通信得以实现。它减少线路连接，增强了用户机动性，而且可以通过简化相应结构实现移动局域网。

目前，有线网和无线网的各种高速网络传输标准不断形成，智能化网络专用设备和网络管理系统的普遍应用，提高了网络的性能和网络的管理能力。网络容错技术更加成熟，增强了网络抗故障能力，出现了很多成熟的网络容错设备和系统，极大地提高了现有网络带宽的利用率，网络吞吐量得到显著改善，彻底改变了无线网络的面貌。随着通信事业的高速发展，无线网络进入了一个新的天地，它具有功能强、易安装、组网灵活、即插即用、移动方便等优点，提供了不受限制的应用。网络管理人员可以迅速而容易地将它加入到现有的网络。目前，无线数据通信已逐渐成为一种重要的通信方式。

本书提供了大量无线局域网的技术实现细节，阐述了无线局域网的新理论、新技术。从无线局域网的基本概念和起源开始，详细讲述了无线局域网的互连结构、硬件组成和设计技术、协议及接入技术、系统配置安装等，重点阐述了无线局域网的安全隐患、面临的问题和解决途径，最后还通过案例，介绍了无线局域网的实际应用。

北京邮电大学信息安全中心的王鹏毅、吕慧勤和辛阳博士参与了本书的编写，董威、李基、潘剑利、杨满智、陈浙一、朱而刚、薛元星、蔡琳等进行了原始资料的搜集、整理和部分章节的编写，联合实验室的赫晓峰协助完成了审阅，在此笔者对他们表示深深地感谢。

在本书编写过程中，参考了大量相关书籍和网络文献，虽然已经在参考文献中一一列出，仍难免有遗漏之处。另外，书中难免存在不足之处，还请读者批评指正。

牛伟 郭世泽 吴志军

2003年5月

# 目 录

<b>第 1 章 无线局域网的基本概念</b> .....	1
1.1 无线局域网的起源和发展 .....	1
1.2 无线局域网的优势 .....	2
1.3 无线局域网采用的标准 .....	3
1.4 无线局域网应用 .....	9
1.4.1 无线局域网的应用介绍 .....	9
1.4.2 无线局域网应用实例 .....	11
<b>第 2 章 无线网络互连结构</b> .....	19
2.1 无线网络拓扑结构 .....	19
2.1.1 无中心的对等网络 (Ad hoc 网络) .....	19
2.1.2 有中心的结构化网络 (Infrastructure 网络) .....	21
2.2 无线局域网的连网方式 .....	22
2.2.1 回顾有线局域网的拓扑结构 .....	23
2.2.2 无线局域网的拓扑结构 .....	25
2.2.3 基于无线电的无线局域网 .....	26
2.2.4 基于红外线方式的无线局域网 .....	33
2.3 无线点对点网络 .....	35
2.3.1 无线点对点网络应用 .....	36
2.3.2 基于无线电的无线点对点网络 .....	36
2.3.3 基于激光的无线点对点网络 .....	38
<b>第 3 章 无线局域网互连部件</b> .....	41
3.1 无线路由器 .....	41
3.1.1 无线互连网络路由协议概述 .....	41
3.1.2 无线路由器的设计原理 .....	43
3.1.3 无线路由器产品实例 .....	46
3.2 无线接入点 .....	51
3.2.1 无线接入点的基本功能与原理 .....	51
3.2.2 AP 的模块设计 .....	54
3.2.3 支持移动 IP 的无线接入点详细过程 .....	55
3.2.4 基于 IEEE 802.11b 的无线接入点实现方案 .....	58



## 无线局域网

3.2.5	基于 IEEE 802.11b 的无线接入点实例	60
3.3	无线网卡	63
3.3.1	无线网卡的应用环境	63
3.3.2	基于 IEEE 802.11b 的设计方案	64
3.3.3	基于 802.11a/g 的无线网卡设计简介	69
3.3.4	无线网卡的实例	71
3.4	无线局域网天线	73
3.4.1	内置天线	73
3.4.2	外置天线	75
3.4.3	天线实例	79
3.5	无线网桥	84
3.5.1	无线网桥应用模式	84
3.5.2	无线网桥技术在无线局域网中的应用	87
3.6	无线局域网其他互连部件实例	90
3.6.1	无线局域网功率放大器	90
3.6.2	无线局域网远端供电模块	91
3.6.3	无线局域网避雷针	91
<b>第 4 章</b>	<b>无线互连技术</b>	<b>93</b>
4.1	无线通信系统接入 Internet 的方式	93
4.1.1	数字蜂窝电话接入方式	93
4.1.2	无线局域网接入方式	94
4.2	基于蜂窝的接入技术	96
4.2.1	基于第一代模拟蜂窝 AMPS 系统的 CDPD 技术	96
4.2.2	基于第二代数字蜂窝系统的 GPRS/EDGE 技术	100
4.2.3	基于 CDMA 及第三代移动通信的接入技术	106
4.3	基于无线局域网的接入技术	111
4.3.1	基于无线局域网协议 IEEE 802.11 协议族的技术	111
4.3.2	基于 HiperLAN 协议的技术	124
4.3.3	蓝牙技术 (Bluetooth)	130
4.3.4	HomeRF	135
4.3.5	IrDA	139
4.3.6	各种接入方式的优缺点及适用环境	141
<b>第 5 章</b>	<b>无线局域网组网</b>	<b>143</b>
5.1	无线局域网解决方案	143
5.1.1	无线网络拓扑配置	143
5.1.2	无线局域网典型的连接方案	144





5.1.3 室外组网方案	146
5.2 无线局域网的设计准则	148
5.2.1 选择无线局域网	148
5.2.2 无线局域网的互连结构	149
5.2.3 无线局域网设计的需求因素	149
5.2.4 选用无线网络产品的几点考虑	150
5.2.5 无线局域网的具体设计	152
5.3 无线局域网的安装	154
5.3.1 一般安装原则	154
5.3.2 室内 WLAN 考虑因素	155
5.3.3 室外 WLAN 的部署	155
5.3.4 工程常见问题及处理	160
5.4 无线局域网组网举例	161
5.4.1 网络拓扑结构设计举例	161
5.4.2 安装接入点	162
5.4.3 安装网卡	172
5.4.4 无线局域网的使用	176
<b>第 6 章 无线局域网的安全机制</b>	<b>183</b>
6.1 无线局域网的安全综述	184
6.1.1 物理层的安全	185
6.1.2 链路层的安全	186
6.1.3 网络层的安全	187
6.2 无线局域网的安全措施	188
6.2.1 无线局域网安全措施概述	189
6.2.2 如何保障无线局域网安全	190
6.2.3 无线局域网应考虑的几个基本的安全服务	195
6.3 无线局域网的安全机制 WEP	197
6.3.1 WEP 加密过程	197
6.3.2 WEP 解密过程	198
6.3.3 WEP 安全性能分析	199
6.4 无线局域网的数据加密算法 RC4	202
6.4.1 RC4 算法概述	203
6.4.2 RC4 经典加密算法 VB 版本代码	204
6.5 无线局域网安全解决方案	205
6.5.1 无线局域网威胁分析	205
6.5.2 无线网络安全解决对策	207



<b>第 7 章 无线局域网面临的问题</b> .....	213
7.1 标准问题.....	213
7.1.1 无线局域网标准概述.....	213
7.1.2 系统兼容性.....	217
7.2 射频问题.....	221
7.2.1 无线干扰的基本概念.....	221
7.2.2 无线网具体干扰形式及无线产品互联干扰.....	226
7.2.3 提高无线局域网抗干扰的先进技术.....	229
7.3 安全性问题.....	233
7.3.1 网络安全缺陷综述.....	234
7.3.2 无线局域网安全缺陷带来的问题.....	237
7.3.3 网络安全策略及其发展.....	238
7.4 无线局域网发展前景.....	245
7.4.1 无线局域网技术标准展望.....	245
7.4.2 无线局域网安全技术的发展.....	246
<b>第 8 章 无线局域网典型应用实例</b> .....	251
8.1 无线网络应用范围.....	251
8.1.1 无线网络应用分类.....	251
8.1.2 无线局域网应用介绍.....	252
8.2 无线局域网应用方案实例.....	256
8.3 无线局域网行业应用.....	259
8.3.1 无线局域网户外应用.....	259
8.3.2 无线局域网室内实用.....	263
8.4 无线局域网应用实例.....	266
8.4.1 无线局域网络在商业零售业中的应用.....	266
8.4.2 无线局域网络在零售配送业中的应用.....	270
<b>参考文献</b> .....	275

# 第 1 章 无线局域网的基本概念

无线局域网就是一种无线数据网络。它是以无线方式构建的局域网 WLAN (Wireless Local Area Network)。或者说,不用线缆将设备相连的局域网络。无线局域网常用的实现技术有:红外数据协会推出的 IrDA、家用射频工作组提出的 HomeRF、Bluetooth (蓝牙) 以及美国的 802.11 协议和欧洲的 HiperLAN2 协议等。

本章主要阐述无线局域网的基本概念、优势、各种标准协议及无线局域网的应用实例。

## 1.1 无线局域网的起源和发展

20 世纪 70 年代,人们开始了无线网的研究。在整个 80 年代,伴随着以太局域网的迅猛发展,具有不用架线、灵活性强等优点的无线网也逐渐赢得了特定市场的认可,但当时的无线网是作为有线以太网的一种补充,遵循了 IEEE 802.3 标准,使架构于 802.3 上的无线网络产品存在着许多弱点,如易受其他微波噪声干扰、性能不稳定、传输速率低、不易升级、不同厂商的产品相互不兼容等,这一切都限制了无线网的进一步应用。

1994 年, Ericsson 移动通信公司开始进行蓝牙技术的研究。1998 年 2 月, Ericsson、IBM、Nokia、Intel、Toshiba 5 家公司发起成立蓝牙特殊利益集团 BSIG (Bluetooth Special Interest Group), 目前已有 2000 多家公司成为 BSIG 的成员。开发这种新技术的目的是用无线方式在小范围内将各种移动通信设备、固定通信设备、计算机及其终端设备、智能家用电器和各种数字数据设备连接起来,组成局域网。Bluetooth 已得到 IEEE 的支持。IEEE 于 1999 年 3 月成立一个工作小组 (IEEE 802.15), 并于 1999 年秋天开始起草一项以蓝牙 1.0 版本为基础的标准,即 IEEE 802.15.1 (TG1)。

1997 年 6 月, IEEE 通过了 802.11 标准, 该标准中规定的传输速度最高仅达 2Mbit/s。此时大部分的业内人士对无线局域网仍没有兴趣, 主要是这种组件成本太高, 普及化不易。另外 2Mbit/s 的速度和有线局域网主流逐渐迈入 100Mbit/s 的 Fast Ethernet 相差太大, 昂贵的投资没有太大的价值。

1999 年秋, IEEE 802.11b 的 11Mbit/s 标准敲定, 至少和有线的上一代 Ethernet 10Mbit/s 相当, WLAN 才被视为进入市场的转机。同时 APPLE 计算机公司与 Lucent 达成协议, 将 WLAN 列为其笔记本电脑 iBook 的选用配备, 并予以部分硬件成本的补贴, 使得转接卡价格降为 99 美元, 突出显示了 iBook 的特殊价值, 随后造成市场的热卖, 并迫使 Compaq 和 Dell 等一线 Notebook 业内人士调整对采用 WLAN 技术的策略, 使用提高至 10Mbit/s 的 WLAN, 从此 WLAN 的价格大幅降低, 增加了市场的接受度。

1999 年以来, 市场开始提倡网络进入家庭, WLAN 的简单、便利和无需线缆传输的特性, 使其前景相当看好。目前市场主流 802.11b 的速率为 11Mbit/s, 电子邮件和网络浏览均没有问题, 可是在 HDTV 等数字动态影像的应用上, 速度显得不够, 必须要达到 50Mbit/s 以上。所以, 业界已开始大力推动将 WLAN 频谱从 2.4GHz 推进到 5GHz, 即美国的 802.11a 或欧洲的 HiperLAN2 标准, 但这也使 WLAN 的技术和市场发展陷入多标准的混乱局面。

802.11a 扩充了标准的物理层, 频带为 5GHz, 采用 QFSK 调制方式, 传输速率为 6~54Mbit/s。它采用正交频分复用 (OFDM) 的独特扩频技术, 可提供 25Mbit/s 的无线 ATM 接

口和 10Mbit/s 的以太网无线帧结构接口, 并支持语音、数据、图像业务。这样的速率完全能满足室内、室外的各种应用场合。但是, 采用该标准的产品目前还没有进入市场。

HiperLAN 采用面向连接的无线 ATM 技术。HiperLAN2 支持 54Mbit/s 的传输速率, 业务上支持话音等实时性要求较强的业务承载。目前, 这种技术在欧洲得到了广泛的支持, 在亚洲、美洲主要还是 IEEE 802.11 系列的产品。

2001 年 11 月 15 日, IEEE 802.11 小组通过了新的 WLAN 的标准 IEEE 802.11g。根据该标准, 在 2.4GHz 频带上可以实现最大 54Mbit/s 的数据传送, IEEE 802.11g 的推出对 WLAN 的发展起到很大的推动作用。

除了 IEEE 802.11 委员会以外, 其他一些组织在推动无线局域网市场方面也做了许多工作。例如, 1998 年 IBM、Compaq、3Com、Philips、Intel、Microsoft、HP 和 Motorola 等公司成立家用射频工作组 HRWG (Home RF Working Group), 简称为 HomeRF, 这个工作组于 1999 年颁布共享无线电接入协议 SWAP (Shared Wireless Access Protocol)。SWAP 支持家庭无线语音设备和无线数据网的共用界面。

无线局域网联盟 (WLANA) 是由无线局域网厂商建立的非营利性组织, 它主要是进行无线局域网市场和产品使用方面的培训等工作。由 3Com、Aironet、Intersil、朗讯科技、诺基亚以及 Symbol 科技公司等厂商组建的无线以太网兼容联盟 (WECA) 则主要通过在同一无线结构内对不同厂商的产品进行验证, 以实现真正意义上的多厂商产品的互操作。在未来几年内, 新的标准 802.11d、802.11e、802.11f、802.11h、802.11i、802.11j 等即将出台, 以适应新的通信形势。

## 1.2 无线局域网的优势

WLAN 利用电磁波在空中发送和接收数据, 无需线缆介质。WLAN 的数据传输速率现在已经能够达到 11Mbit/s, 传输距离可远至 20km 以上。它是对有线连网方式的一种补充和扩展, 使网络上的计算机具有可移动性, 能快速、方便地解决使用有线方式不易实现的网络连通问题。

与有线网络相比, WLAN 具有以下优点。

(1) 安装便捷 一般在网络建设中, 施工周期最长、对周边环境影响最大的是网络布线施工工程。在施工过程中, 往往需要破墙掘地、穿线架管。而 WLAN 最大的优势就是免去或减少了网络布线的工作量, 一般只要安装一个或多个接入点 (Access Point) 设备, 就可建立覆盖整个建筑或地区的局域网络。

(2) 使用灵活 在有线网络中, 网络设备的安放位置受网络信息点位置的限制。而一旦 WLAN 建成后, 在无线网的信号覆盖区域内, 任何一个位置都可以接入网络。

(3) 经济节约 由于有线网络缺少灵活性, 这就要求网络规划者尽可能地考虑未来发展的需要, 导致预设大量利用率较低的信息点。而一旦网络的发展超出了设计规划, 又要花费较多费用进行网络改造。而 WLAN 可以避免或减少以上情况的发生。

(4) 易于扩展 WLAN 有多种配置方式, 能够根据需要灵活选择。这样, WLAN 就能胜任从只有几个用户的小型局域网到上千用户的大型网络, 并且能够提供如漫游 (Roaming) 等有线网络无法提供的特性。

由于 WLAN 具有多方面的优点，其发展十分迅速。在最近几年里，WLAN 已经在医院、商店、工厂和学校等不适合网络布线的场合得到了广泛的应用。

### 1.3 无线局域网采用的标准

比较常用的无线局域网标准有 IEEE 802.11、IEEE 802.11b、IEEE 802.11a、IEEE 802.11g、Bluetooth、HomeRF、IrDA、HiperLAN2 等。

(1) IEEE 802.11 1990 年 IEEE 802 标准化委员会成立 IEEE 802.11 无线局域网 (WLAN) 标准工作组。工作组的任务是研究 1Mbit/s 和 2Mbit/s 数据速率、工作在 2.4GHz 开放频段的无线设备和网络发展的全球标准。工作组于 1997 年 6 月公布了该标准，它是第一代无线局域网标准之一。该标准定义物理层和媒体访问控制 (MAC) 规范，允许无线局域网及无线设备制造商建立互操作网络设备。

标准中，物理层定义了数据传输的信号特征和调制，定义了两个 RF 传输方法和一个红外线传输方法。RF 传输方法采用扩频调制技术，在该标准中，RF 传输标准是 FHSS 和 DSSS，工作在 2.4000~2.4835GHz 频段。直接序列扩频采用 BPSK 和 DQPSK 调制技术，支持 1Mbit/s 和 2Mbit/s 数据速率。跳频扩频采用 2~4 电平 GFSK 调制技术，支持 1Mbit/s 数据速率。红外线传输方法工作在 850~950nm 段，峰值功率为 2W，支持数据速率为 1Mbit/s 和 2Mbit/s。

媒体访问控制 (MAC) 层使用 CSMA/CA (载波监听多路访问/冲突避免) 协议。由于在 RF 传输网络中，冲突检测比较困难，所以该协议用冲突避免检测代替在 802.3 协议使用的 CSMA/CD (载波监听多路访问/冲突检测)。CSMA/CD 通过电缆中电压的变化来检测，当数据发生碰撞时，电缆中的电压就会随着发生变化；而 CSMA/CA 采用能量检测 (ED)、载波检测 (CS) 和能量载波混合检测 3 种检测信道空闲的方式。使用信道空闲评估 (CCA) 算法来决定信道是否空闲。

(2) IEEE 802.11b 为了支持更高的数据传输速率，IEEE 于 1999 年 9 月批准了 IEEE 802.11b 标准。IEEE 802.11b 标准对 IEEE 802.11 标准进行了修改和补充，其中最重要的改进就是在 IEEE 802.11 的基础上增加了两种更高的通信速率 5.5Mbit/s 和 11Mbit/s。当射频情况变差时，可将数据传输速率降低为 5.5Mbit/s、2Mbit/s 和 1Mbit/s。

IEEE 802.11b 的基本结构、特性和服务仍然由最初的 IEEE 802.11 标准定义。IEEE 802.11b 规范只影响 IEEE 802.11 标准的物理层，它增加了数据传输速率和连接性的健全。

至于安全保证，IEEE 802.11b 制定了一个有线等价保密机制 WEP (Wired Equivalent Privacy)，它工作在媒体存取控制层 (OSI MAC Layer)，提供存取控制 (Access Control) 及资料加密的机制，802.11b WEP 采用了对称性加密算法 RC4，提供 40bit 长度的加密密钥。

(3) IEEE 802.11a 802.11a 标准是已得到广泛应用的 802.11b 无线联网标准的后续标准，802.11a 的物理层速率可达 54Mbit/s，传输层可达 32Mbit/s，采用正交频分复用 (OFDM) 的扩频技术，可提供 25Mbit/s 的无线 ATM 接口和 10Mbit/s 的以太网无线帧结构接口，以及 TDD/CDMA 的空中接口；支持语音、数据、图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。目前，支持 802.11a 的芯片已经进入市场，但是其设备价格昂贵，针对点对点连接不太经济。

(4) IEEE 802.11g 由于 IEEE 802.11b 和 IEEE 802.11a 工作在不同的频段上，物理层调



制方式也不同, IEEE 802.11a 不能兼容目前的 IEEE 802.11b 的产品。同时 5GHz 的频段在许多国家还没有获得正式批准, 而且 11Mbit/s 的传输速率满足不了视频服务带宽的需求。针对上述情况, IEEE 802 小组于 2001 年 11 月 15 日通过了最新的 IEEE 802.11g 标准。IEEE 802.11g 标准方案在确保兼容现有使用 2.4GHz 频带的 IEEE 802.11b 的同时, 实现了 54Mbit/s 数据传送速度。IEEE 802.11g 中规定的调制方式有两种, 包括 IEEE 802.11a 中采用的 OFDM 与 IEEE 802.11b 中采用的 CCK。通过规定两种调制方式, 既达到了用 2.4GHz 频带实现 IEEE 802.11a 水平的数据传送速度, 也确保了与装机数量超过 1100 万台的 IEEE 802.11b 产品的兼容。同时, Ti 公司提案的可实现 22Mbit/s 数据传输速度的 PBCC-22(CCK-PBCC)调制方式与 CCK-OFDM 也可以作为选项使用。

另外, IEEE 除了制定上述的 3 个主要无线局域网协议之外, 还在不断改善这些协议。推出或即将推出以下一些新的协议。

- 802.11d, 是 802.11b 使用其他频率的版本, 以适应一些不能使用 2.4GHz 频段的国家。这些国家中的多数正在清理这个频段。

- 802.11e, 在 802.11 系列协议中增加 QoS 能力。它用 TDMA 方式取代类似 Ethernet 的 MAC 层, 为重要的数据增加额外的纠错功能。

- 802.11f, 目的是改善 802.11 协议的切换机制。使用户能够在不同的交换分区间(无线信道)或者在接入设备间漫游。这就使得无线局域网能够提供与移动通信同样的移动性。

- 802.11h, 比 802.11a 能更好地控制发送功率和选择无线信道, 与 802.11e 一起适应欧洲的更严格的标准。

- 802.11i, 改善 802.11 明显的安全缺陷。

- 802.11j, 目的是使 802.11a 和 HiperLAN2 网络能够互通。

(5) Bluetooth 1998 年 5 月, Ericsson、IBM、Intel、Nokia 和 TOSHIBA 等公司联合推出一项最新的无线网络技术, 即 Bluetooth 技术。随后这 5 家公司组建了一个特殊的兴趣组织 (SIG) 来负责此项技术的开发。后来得到包括 Motorola、Lucent、Compaq、SIEMENS、Qualcomm、3Com、TDK 等大公司在内的许多厂商的支持。1999 年 12 月 1 日, Microsoft、Lucent、3Com 和 Motorola 等 4 家公司加入到创始者行列, 使得蓝牙特殊兴趣组织由 9 家公司共同领导。1999 年 7 月蓝牙 SIG 推出了蓝牙协议 1.0 版。

蓝牙技术主要面向网络中各类数据及语音设备, 通过无线方式将它们连成一个微微网 (Piconet), 多个微微网之间也可以互连形成分布式网络 (Scatternet), 从而方便、快速地实现各类设备之间的通信。它是实现语音和数据无线传输的开放性规范, 是一种低成本、短距离的无线连接技术。

蓝牙系统中的微微网是采用蓝牙技术的设备以特定方式组成的网络。微微网的建立是由两台设备(如便携式计算机和蜂窝电话)的连接开始, 最多由 8 台设备构成。所有的蓝牙设备都是对等的, 以同样的方式工作。然而, 当一个微微网建立时, 只有一台主设备, 其他均为从设备, 而且在一个微微网存在期间将一直维持这一状况。分布式网络 (Scatternet) 是由多个独立、非同步的微微网形成的。

Bluetooth 在技术上的特点可归纳为以下几点。

- 全球可操作性。Bluetooth 使用 2.4GHz 的 ISM 频段, 该频段在全球各个国家都是有效的, 没有被任何一个组织或行业单独占有, 可自由使用。

## 第 1 章

- 10~100m 的有效无线通信距离。发射功率为 1mW (0dBm) 时有效通信距离小于或等于 10m, 这种情况适合于短距离设备, 如鼠标、键盘等; 在发射功率为 100mW (20dBm) 时有效通信距离小于或等于 100m, 这种情况适合于设备经常变动的环境, 如移动电话, 笔记本电脑等。

- 1Mbit/s 的数据传输串。
- 小尺寸、低功耗和低价格。
- 非常可靠的数据和语音传输能力。语音采用连续可变斜率调制 (CVSD) 编码方式, 其分组不重传, CVSD 方式抗衰落性强。

蓝牙技术规范包括协议 (Protocol) 和应用规范 (Profile) 两部分。协议定义了各功能元素的工作方式, 而应用规范阐述了为实现一个特定的应用模型, 各层协议间的运转协同机制。Bluetooth 的协议栈如图 1-1 所示。

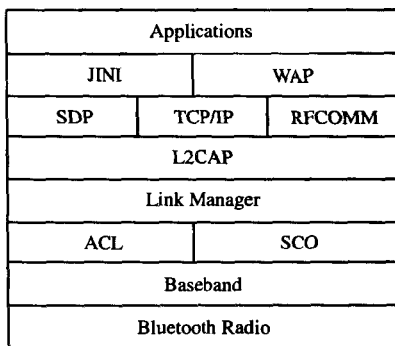


图 1-1 Bluetooth 的协议栈

协议栈中各部分功能如下。

- Bluetooth Radio (蓝牙无线电) 是蓝牙设备中负责传送和接收调制电信号的收发器。
- Baseband (基带) 即蓝牙的物理层, 负责管理物理通道和链路。
- ACL 是在物理信道上传输数据的异步无连接 (Asynchronous Connection-Less) 物理链路。
- SCO 是同步连接 (Synchronous Connection Oriented) 物理链路, 主要用于语音通信的信息传输。
- Link Manager (链路管理器) 主要处理链路建立、链路安全和链路控制等任务, 它提供认证、加密控制、功率控制等服务和 QoS 能力。
- L2CAP 即逻辑链路控制和适应层协议 (Logical Link Control and Adaptation Layer Protocol), 它位于数据链路层, 向上层协议提供复用、分段、重组和组抽象等无连接和面向连接的数据服务。
- SDP 即服务发现协议 (Service Discovery Protocol)。
- RFCOMM (串口仿真) 协议是一种简单传输协议, 可在 L2CAP 之上仿真 RS-232 (EIA/TIA-232-E) 串口电路。
- JINI 技术提供了一种简单的机制, 采用这种机制可以让设备组合起来形成即时群体, 每一种设备都向群体中的其他设备提供它们可以使用的服务。
- WAP 即无线应用协议 (Wireless Application Protocol)。



Bluetooth 的安全保证。在链路层，蓝牙系统提供了认证、加密和密钥管理等功能，每个用户都有个人标识码（UN），它会被译成 128Mbit 的链路密钥（Link Key）来进行单双向认证，一旦认证完毕，链路就会以不同长度的密码来加密（此密码以 8bit 为单位增减，最大为 128bit）。链路层安全机制提供了大量的认证方式和一个灵活的加密方式（允许协商密码长度），因为某些国家会指定最大密码长度，蓝牙系统会选取 Piconet 中的各个设备的最小和最大允许密码长度。如图 1-2 所示为蓝牙系统链路层安全机制。

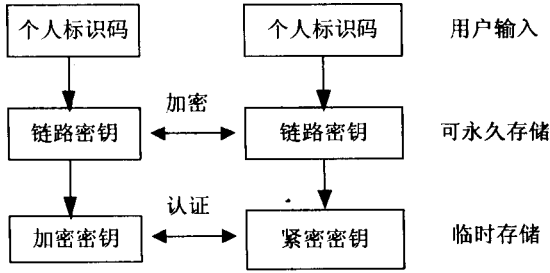


图 1-2 蓝牙系统链路层安全机制

(6) HomeRF HomeRF 技术是无绳电话技术 DECT (Digital Enhanced Cordless Telephone) 和无线局域网技术相互融合发展的产物。在 ITU 的赞助下，在 Compaq、Intel、Philips、HP、IBM 和 Microsoft 等几家大公司的参与下，HomeRF 工作小组致力于实现个人计算机与其他来自不同制造商的家用电器设备之间的数字通信，并于 1998 年制定了共享无线接入协议 (SWAP, Share Wireless Access Protocol)。无线局域网 802.11 使用 CSMA/CA 方式，适合于数据业务，而 DECT 使用 TDMA 方式，适合语音业务，SWAP 结合了 DECT 和 IEEE 802.11 的特点，使用 TDMA 加 CSMA/CA 方式，适合语音和数据业务。它也工作于 2.4GHz ISM 频段，基于该协议的网络是对等网，也就是说，网上的每一个节点都是相对独立的，不受中央节点的控制。如图 1-3 所示为 HomeRF 的 SWAP 协议模型。

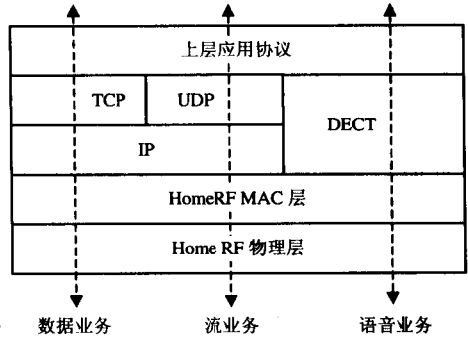


图 1-3 HomeRF 的 SWAP 协议模型

HomeRF 是针对现有无线通信标准的综合和改进：当进行数据通信时，它采用的是 IEEE 802.11 规范中的 TCP/IP 传输协议；进行语音通信时，则采用了数字化泛欧无绳电话 DECT 规范。HomeRF 的应用如下。

- 语音通信：SWAP 规范合并了 DECT 标准，该标准支持用户所期待的电话特性，在家庭和小型企业中都非常有用。使用 HomeRF 技术的无绳电话将具备传统电话的所有功能，并且



能够提供比传统无绳电话更多的便利,使电话放置的位置更加灵活。HomeRF 技术还提供了更高的语音质量和安全性,HomeRF 2.0 的话音质量可以达到 4.1MOS (Mean Opinion Score),一般的公用电话质量为 4.3MOS,移动话音的质量只有 3.4MOS,2.4GHz 的频段避免了来自远程控制设备以及监视器等装置的干扰。

提示: MOS (Mean Opinion Score) 是一种国际上流行的用来评估编码器输出音质好坏的指标。一般 4MOS 的音质称为长途音质; 3.5~4MOS 的音质称为通信质量; 3.0~3.5MOS 的音质称为专业质量; 小于 3MOS 的音质称为合成质量。

- 数据通信和流媒体业务: 为了实行对数据包的高效传输, HomeRF 采用了 IEEE 802.11 标准中的 CSMA/CA, 在一个时间点上只能有一个接入点在网络中传输数据。流业务的典型应用是视频会议、无线耳机等, HomeRF 对流媒体业务赋予高级别的优先权, 采用带有优先权的重发机制, 这样保证了实时流业务所需的带宽和较低的误码率。

- 安全保证: HomeRF 无线家庭网络的数据安全性由 Blowfish 加密算法来保证。

(7) HiperLAN2 HiperLAN2 是由 Bosch Telecom、Dell Computer、Ericsson、Nokia、Telia Mobile 和 Texas Instruments 等公司发起的, 其宗旨是推动 HiperLAN2 技术的标准化。2002 年 2 月, ETSI (European Telecom Standards Institute, 欧洲电信标准化协会) 的 BRAN (Broadband Radio Access Networks, 宽带无线接入网络) 小组公布了 HiperLAN2 标准, HiperLAN2 在 5GHz 的频段上运行, 采用 OFDM 调制方式, 物理层最高速率可达 54Mbit/s。如图 1-4 所示为 HiperLAN2 的网络结构。

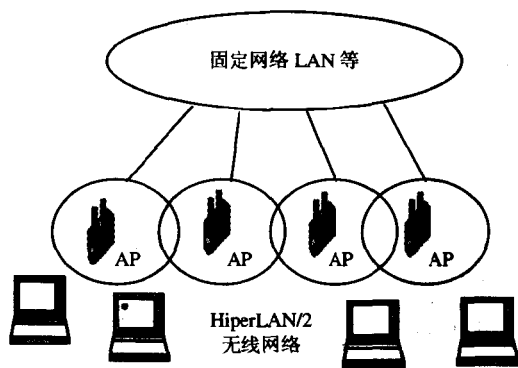


图 1-4 HiperLAN2 网络结构

HiperLAN2 技术的主要特点包括以下几方面。

- 高传输速率, HiperLAN2 物理层传输速率可以达到 54Mbit/s, 汇聚层可以达到 25Mbit/s, 物理层采用 OFDM 调制方式来传输模拟信号, OFDM 是一种在时间色散环境中非常有效的调制方式;

- 面向连接, 在 HiperLAN 网络中, 移动终端 (MT) 在与接入点 (AP) 通信之前利用 HiperLAN2 控制平面的信令功能先建立连接, 通过空中接口实现时分多址复用;

- QoS 支持 HiperLAN2 网络面向连接的特性, 使它能支持 QoS, 每一个连接可以有确定的 QoS 值, 如确定的带宽、时延、抖动、比特差错率等;

- 安全支持, HiperLAN2 网络支持安全认证和保密, 通过使用认证机制, AP 和 MT 可以