

IEEE 802.11

金 纯 陈林星 杨吉云 编著
缪 丹 审校

无线局域网



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
[Http://www.phei.com.cn](http://www.phei.com.cn)

IEEE 802.11 无线局域网

金纯 陈林星 杨吉云 编著

缪丹 审校

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书专门介绍当前在无线局域网技术领域内的热点技术——IEEE 802.11 无线局域网。主要内容包括：IEEE 802.11 无线局域网的基本概念；媒介访问控制（MAC）层的服务定义与规范、帧结构、功能、管理实体；鉴权与加密；物理层的服务定义；高速直接序列扩频物理层技术规范；跳频扩频物理层技术规范；IEEE 802.11 无线局域网的应用等。

本书内容新颖，概念清楚，层次明晰，可帮助读者尽快了解和掌握 IEEE 802.11 无线局域网技术及其应用知识。

本书可供从事 IEEE 802.11 无线局域网的技术人员及有关院校师生阅读。对于正在或者想要应用和设计无线媒介访问控制机制-虚拟载波访问机制（即 RTS/CTS 分组相互交换机制）的工程技术人员或相关人员，本书也可以提供很好的参考和借鉴作用。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

图书在版编目（CIP）数据

IEEE 802.11 无线局域网/金纯编著. —北京：电子工业出版社，2004.1

ISBN 7-5053-9426-6

I. I… II. 金… 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 111750 号

责任编辑：张来盛 宋 梅

印 刷：北京天竺颖华印刷厂

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

经 销：各地新华书店

开 本：787×1092 1/16 印张：20 字数：510 千字

印 次：2004 年 1 月第 1 次印刷

印 数：4000 册 定价：29.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。
联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前 言

无线局域网(WLAN)是采用无线传输媒介的计算机局域网。其特点是成本低,灵活性、移动性强,吞吐量高(IEEE 802.11b 传输速率最高达 11Mb/s, IEEE 802.11a 传输速率最高达 54Mb/s),通信可靠(因为具有扩频抗干扰能力)。

从网络层次结构来看,IEEE 802.11 无线局域网包括物理层和 MAC 层两个层次的内容,而 MAC 层以上的层次并未涉及。IEEE 802.11 无线局域网的 MAC 层对所有类型的 IEEE 802.11 无线局域网物理层均适用。IEEE 802.11 无线局域网的 MAC 层协议结合了 CSMA/CA 物理载波侦听多址访问与碰撞退避机制以及基于控制分组 RTS, CTS 握手对话的虚拟载波侦听多址访问与碰撞退避机制,前者是面向发送方的,后者是面向接收方的。因此,IEEE 802.11 无线局域网的 MAC 层协议是同时从发送方和接收方来解决无线媒介上分组传输碰撞问题的。迄今为止,学术界仍然认为 IEEE 802.11 无线局域网的 MAC 层协议解决了无线网络通信中令人头痛的“隐含终端”问题。IEEE 802.11 无线局域网的 MAC 层协议是一个性能优良的无线媒介访问控制协议。

IEEE 802.11 无线局域网的物理层目前包括五个方面的内容:一是基于直接序列扩频(DSSS)技术的物理层,工作在 2.4 GHz 频段;二是基于高速直接序列扩频(HR/DSSS)技术的物理层,工作在 2.4 GHz 频段;三是基于跳频扩频(FHSS)技术的物理层,工作在 2.4GHz 频段;四是基于频分正交复接(OFDM)技术的物理层(本书未包括),工作在 5.8 GHz 频段;五是基于红外线传输技术的物理层(本书未包括),工作在 2.4 GHz 频段。

无线局域网(WLAN)既能够作为一个独立的移动通信网来使用,也可以与有线网络共同使用,还可以作为有线网络的备份或替代网络,尤其适用于不适合布线的地方。无线局域网的应用场合非场广泛,比如:城市建筑群间通信,学校校园网络,工矿企业厂区自动化控制与管理网络,银行和金融证券城区网络,城市交通信息网络,矿山、水利、油田等区域网络,港口、码头、江河湖坝区网络,野外勘测、实验等流动网络,军事、公安流动网络等。由此可见,无线局域网具有潜在的巨大商机,而且正在不断显现出来。

本书是专门描述 IEEE 802.11 无线局域网的,其目的是为 IEEE 802.11 无线局域网设计者、无线网络研究和开发人员、网络规划人员、网络管理人员,以及 IEEE 802.11 无线局域网(WLAN)用户等理解和掌握 IEEE 802.11 无线局域网技术提供一些帮助。本书的编写安排如下:

第 1 章概述,简单介绍了无线局域网的特点、应用以及有关标准。

第 2 章基本概念,描述了 IEEE 802.11 无线局域网的特点、体系结构、服务以及各种服务之间的关系、网络参考模型等。

第 3 章 MAC 层服务,阐述 IEEE 802.11 无线局域网 MAC 层提供的服务及其服务原语。

第 4 章帧格式,详细描述 IEEE 802.11 无线局域网 MAC 层的帧格式。

第 5 章鉴权与加密,对 IEEE 802.11 无线局域网的鉴权和 WEP 加密算法等作了论述。

第 6 章 MAC 层功能介绍,内容主要有 MAC 体系结构、分布式协调功能(DCF)和集中协调功能(PCF)的功能机理、协议数据单元(PDU)的分段传输及其分段重组、多速率支持和各种分组传输中的帧交换顺序等。

第 7 章层管理,介绍 IEEE 802.11 无线局域网的管理模型和通用管理原语,详细说明了

媒介访问控制子层管理实体服务访问点（MLME SAP）接口和物理层管理实体服务访问点（PLME SAP）接口中各条原语的功能、语义、产生的时间，以及接收后的效果。

第 8 章 MAC 层管理实体，涉及的内容有同步、功率管理、关联和重新关联和管理信息数据库（MIB）定义等。

第 9 章物理层（PHY）服务技术规范，说明了 IEEE 802.11 物理层的功能和服务及其范围，详细阐述了 PHY 和 MAC 子层之间的交互和物理层服务访问点（PHY-SAP）中的各条原语。

第 10 章高速直接序列扩频物理层技术规范，包括高速物理层的物理层收敛协议（PLCP）子层、物理层管理实体（PLME）和物理媒介依赖（PMD）等方面的内容。

第 11 章 2.4 GHz 频带的直接序列扩频（DSSS）物理层（PHY）技术规范，包括直接序列扩频（DSSS）物理层的物理层收敛协议（PLCP）子层、物理层管理实体（PLME）和物理媒介依赖（PMD）等方面的内容。

第 12 章跳频扩频物理层技术规范，包括跳频扩频（FHSS）物理层的特性、特定服务参数、物理层收敛协议（PLCP）子层、物理层管理实体服务访问点（PLME SAP）层管理、物理媒介依赖（PMD）子层、1.0 Mb/s 的物理媒介依赖（PMD）子层、2.0 Mb/s 的物理媒介依赖（PMD）子层和物理层管理信息数据库（MIB）等内容。

附录 A 为专业术语的解释，附录 B 为英文缩写词、英文全名及中文对照。

IEEE 802.11 是一个内容繁多的体系，既涉及了无线直接序列扩频（DSSS）传输技术、高速直接序列扩频（HR/DSSS）传输技术、跳频扩频（FHSS）传输技术、OFDM 无线传输技术（本书未包括这部分内容），还容纳了翔实的媒介访问控制（MAC）协议。这么多的内容，如果要在本书和 IEEE 802.11 英文标准之间进行对照阅读的话，还是有点不快捷，为此将本书的章节编排和 IEEE 802.11 英文标准的条款编排对照如下表所示。

本书的章号	IEEE 802.11 英文标准条款号	对应章的名称
2	5	基本概念
3	6	MAC 层服务
4	7	帧格式
5	8	鉴权与加密
6	9	MAC 层功能介绍
7	10	层管理
8	11	MAC 层管理实体
9	12	物理层（PHY）服务技术规范
10	18	高速直接序列扩频物理层技术规范
11	15	2.4GHz 频带的直接序列扩频（DSSS）物理层（PHY）技术规范
12	14	跳频扩频物理层技术规范
附录 A	3	专业术语定义
附录 B	4	缩写词

为了便于理解和对照，作者在写作本书时，将一个术语的中文名称和英文缩写并排列在一起，两者的并排顺序有时是中文名称在前而英文缩写紧随其后，有时是英文缩写在前而中

文名称紧随其后，这样随意编排是为了防止排版时不至于把一个连接着的英文缩写分在两行中，给阅读视觉带来不方便。比如，“媒介访问控制服务数据单元”和英文缩写“MSDU”指的是同一个概念，作者在本书中把这两个书写格式并排写在一起，有时写成“媒介访问控制服务数据单元（MSDU）”，有时写成“MSDU（媒介访问控制服务数据单元）”。

本书是在金纯的策划和主持下、由四位作者共同完成的。重庆金美通信有限责任公司的高级工程师陈林星编写第 11、12 章及附录 A 和附录 B，并负责全书的最后校对和统稿。其余部分分别由金纯、重庆大学计算机系杨吉云和重庆大学孙睿博士共同完成。邮电学院缪丹对全书进行了审校。另外，我们衷心感谢重庆大学计算机系教授许光辰、重庆蓝牙无线技术研究所秦利君、重庆大学硕士研究生田新建为本书的先期编写工作作出的贡献。

由于作者知识有限，本书难免有缺陷甚至错误，敬请作者指出和谅解。

编著者

2003 年 11 月

目 录

第 1 章 概述	(1)
1.1 无线局域网 (WLAN) 的特点	(1)
1.1.1 传输方式	(1)
1.1.2 无线组网特点	(2)
1.1.3 安全性等同于有线	(2)
1.2 WLAN 的应用	(3)
1.3 无线局域网 (WLAN) 的标准	(4)
1.3.1 802.11 家族	(4)
1.3.2 蓝牙	(6)
1.3.3 家庭网络 HomeRF	(7)
1.3.4 IrDA	(7)
第 2 章 基本概念	(8)
2.1 无线局域网的特点	(8)
2.1.1 目的地址不等于目的物理位置	(8)
2.1.2 传输媒介对设计的影响	(8)
2.1.3 处理移动站点 (STA) 的影响	(8)
2.1.4 与 IEEE 802 其他协议层的交互作用	(9)
2.2 IEEE 802.11b 体系结构的组成部分	(9)
2.2.1 将独立的基本服务集 (BSS) 作为一个 ad hoc 网络	(10)
2.2.2 分发系统概念	(10)
2.2.3 扩展服务集 (ESS) 和独立基本服务集 (IBSS) 的区别	(11)
2.2.4 区域概念	(12)
2.2.5 与有线局域网的综合	(13)
2.3 逻辑服务接口	(14)
2.3.1 站点服务 (SS)	(14)
2.3.2 分发系统服务 (DSS)	(15)
2.3.3 多维逻辑地址空间	(15)
2.4 服务概述	(16)
2.4.1 信息在分发系统中的分发	(16)
2.4.2 支持分发服务的服务	(17)
2.4.3 访问和机密性控制服务	(18)
2.5 各个服务间的关系	(20)
2.5.1 1 类帧	(21)
2.5.2 2 类帧	(22)
2.5.3 3 类帧	(22)
2.6 支持服务的帧内容	(23)

11/5/05

2.6.1 数据	(23)
2.6.2 关联	(23)
2.6.3 重新关联	(24)
2.6.4 取消关联	(24)
2.6.5 加密	(25)
2.6.6 鉴权	(25)
2.6.7 取消鉴权	(26)
2.7 参考模型	(26)
第3章 MAC 层服务	(27)
3.1 MAC 层服务概述	(27)
3.1.1 异步数据服务	(27)
3.1.2 安全服务	(27)
3.1.3 媒介访问控制服务数据单元 (MSDU) 排序	(27)
3.2 详细的服务规范	(28)
3.2.1 MAC 数据服务	(28)
第4章 帧格式	(32)
4.1 MAC 帧格式	(32)
4.1.1 描述约定	(32)
4.1.2 通用帧格式	(33)
4.1.3 域	(33)
4.2 帧格式类型	(40)
4.2.1 控制帧	(40)
4.2.2 数据帧	(44)
4.2.3 管理帧	(47)
4.3 管理帧帧实体的组成部分	(52)
4.3.1 固定域	(52)
4.3.2 信息单元	(57)
第5章 鉴权与加密	(63)
5.1 鉴权服务	(63)
5.1.1 开放系统鉴权	(63)
5.1.2 共享密钥鉴权	(64)
5.2 WEP 算法	(66)
5.2.1 介绍	(66)
5.2.2 WEP 算法的特性	(67)
5.2.3 WEP 加密原理	(67)
5.2.4 WEP 算法的技术规范	(69)
5.2.5 WEP 帧实体扩展	(69)
5.3 与安全性相关的管理信息数据库 (MIB) 属性	(70)

第 6 章 MAC 层功能介绍	(72)
6.1 MAC 体系结构	(72)
6.1.1 载波侦听多址访问 / 碰撞回避 (CSMA/CA) 机制	(72)
6.1.2 分布式协调功能 (DCF)	(73)
6.1.3 集中协调功能 (PCF)	(73)
6.1.4 分布式协调功能 (DCF) 和集中协调功能 (PCF) 的共存	(74)
6.1.5 分段 / 分段重组概述	(74)
6.1.6 MAC 层数据服务	(75)
6.2 分布式协调功能 (DCF)	(75)
6.2.1 载波侦听机制	(76)
6.2.2 MAC 级应答	(76)
6.2.3 帧间间隔 (IFS)	(76)
6.2.4 随机退避时间	(78)
6.2.5 分布式协调功能 (DCF) 访问规程	(79)
6.2.6 媒介访问控制协议数据单元 (MPDU) 的定向传送规程	(85)
6.2.7 广播和多目标传输媒介访问控制协议数据单元 (MPDU) 传送规程	(85)
6.2.8 ACK (应答) 规程	(86)
6.2.9 拷贝帧的检测和恢复	(87)
6.2.10 分布式协调功能 (DCF) 的定时关系	(87)
6.3 集中协调功能 (PCF)	(88)
6.3.1 无竞争期间 (CFP) 结构和定时	(89)
6.3.2 集中协调功能 (PCF) 访问规程	(91)
6.3.3 集中协调功能 (PCF) 传输规程	(92)
6.3.4 无竞争轮询列表	(95)
6.4 分段	(96)
6.5 分段重组	(97)
6.6 多速率支持	(98)
6.7 帧交换顺序	(98)
6.8 媒介访问控制服务数据单元 (MSDU) 发送限制	(100)
第 7 章 层管理	(101)
7.1 管理模型概述	(101)
7.2 通用管理原语	(101)
7.3 媒介访问控制子层管理实体服务访问点 (MLME SAP) 接口	(102)
7.3.1 功率管理	(103)
7.3.2 扫描	(104)
7.3.3 同步	(107)
7.3.4 鉴权	(109)
7.3.5 取消鉴权	(111)
7.3.6 关联	(114)

7.3.7 重新关联	(116)
7.3.8 去关联	(118)
7.3.9 复位	(120)
7.3.10 构建(构建一个新的 BSS)	(121)
7.4 物理层管理实体服务访问点 (PLME SAP) 接口	(124)
7.4.1 物理层管理实体复位请求原语 (PLME-RESET.request)	(124)
7.4.2 物理层管理实体特性请求 (PLME-CHARACTERISTICS.request)	(124)
7.4.3 物理层管理实体特性证实原语 (PLME-CHARACTERISTICS.confirm)	(125)
7.4.4 物理层管理实体直接序列扩频测试模式请求原语 (PLME-DSSSTESTMODE.request)	(127)
7.4.5 物理层管理实体直接序列扩频测试输出请求原语 (PLME-DSSSTESTOUTPUT.request)	(128)
第 8 章 MAC 层管理实体	(130)
8.1 同步	(130)
8.1.1 基本途径	(130)
8.1.2 同步维护	(130)
8.1.3 捕获同步, 扫描	(132)
8.1.4 调整站点 (STA) 的定时器	(135)
8.1.5 跳频物理层 (FH PHY) 的定时同步	(135)
8.2 功率管理	(136)
8.2.1 基础网络中的功率管理	(136)
8.2.2 独立基本服务集 (IBSS) 中的功率管理	(141)
8.3 关联和重新关联	(144)
8.3.1 站点 (STA) 关联规程	(145)
8.3.2 访问点 (AP) 关联规程	(145)
8.3.3 站点 (STA) 重新关联规程	(145)
8.3.4 访问点 (AP) 重新关联规程	(145)
8.4 管理信息数据库 (MIB) 定义	(146)
8.4.1 站点 (STA) 管理属性	(146)
8.4.2 MAC 属性	(147)
第 9 章 物理层 (PHY) 服务技术规范	(150)
9.1 范围	(150)
9.2 物理层 (PHY) 功能	(150)
9.3 物理层 (PHY) 服务技术规范详述	(150)
9.3.1 应用范围和领域	(150)
9.3.2 服务概述	(150)
9.3.3 MAC 和 PHY 的交互概述	(151)
9.3.4 基本服务和选项	(151)
9.3.5 物理层服务访问点 (PHY-SAP) 服务详细描述	(152)
第 10 章 高速直接序列扩频物理层技术规范	(159)

10.1 概述	(159)
10.1.1 范围	(159)
10.1.2 高速物理层功能实体	(160)
10.1.3 服务说明	(160)
10.2 高速物理层收敛协议 (PLCP) 子层	(161)
10.2.1 概述	(161)
10.2.2 物理层收敛协议数据单元 (PPDU) 的格式	(161)
10.2.3 PLCP PPDU 各个域的定义	(163)
10.2.4 物理层收敛协议 (PLCP/High Rate PHY) 数据扰码器和解扰器	(169)
10.2.5 物理层收敛协议 (PLCP) 的发送规程	(169)
10.2.6 物理层收敛协议 (PLCP) 的接收规程	(172)
10.3 高速物理层管理实体 (PLME)	(175)
10.3.1 PLME_SAP 子层管理原语	(175)
10.3.2 高速 PHY MIB	(176)
10.3.3 直接序列扩频物理层 (PHY) 的特性	(176)
10.3.4 高速发送时间 (TXTIME) 的计算	(177)
10.3.5 矢量描述	(177)
10.4 高速物理媒介依赖 (PMD) 子层	(178)
10.4.1 应用的范围和场合	(178)
10.4.2 服务概述	(178)
10.4.3 交互概述	(178)
10.4.4 基本服务和选项	(178)
10.4.5 物理媒介依赖服务访问点 (PMD_SAP) 服务详细规范	(179)
10.4.6 物理媒介依赖 (PMD) 的通用工作规范	(188)
10.4.7 物理媒介依赖 (PMD) 发送技术规范	(198)
10.4.8 物理媒介依赖 (PMD) 接收机技术规范	(202)
第 11 章 2.4 GHz 频带的直接序列扩频 (DSSS) 物理层 (PHY) 技术规范	(204)
11.1 概述	(204)
11.1.1 范围	(204)
11.1.2 直接序列扩频 (DSSS) 物理层 (PHY) 的功能	(204)
11.1.3 服务规范方法与符号	(205)
11.2 直接序列扩频 (DSSS) 物理层收敛协议 (PLCP) 子层	(205)
11.2.1 概述	(205)
11.2.2 物理层收敛协议 (PLCP) 帧格式	(205)
11.2.3 物理层收敛协议 (PLCP) 组成域的定义	(206)
11.2.4 物理层收敛协议 (PLCP) / 直接序列扩频 (DSSS) 物理层 (PHY) 数 据扰码器和解扰器	(207)
11.2.5 物理层收敛协议 (PLCP) 的数据调制和调制速率的改变	(209)
11.2.6 物理层收敛协议 (PLCP) 发送规程	(209)

11.2.7 物理层收敛协议 (PLCP) 接收规程	(211)
11.3 直接序列扩频 (DSSS) 物理层管理实体 (PLME)	(213)
11.3.1 物理层管理实体服务访问点 (PLME_SAP) 子层的管理原语	(213)
11.3.2 直接序列扩频物理层 (DSSS PHY) 管理信息数据库	(214)
11.3.3 直接序列物理层 (DS PHY) 的特性	(214)
11.4 直接序列扩频 (DSSS) 物理媒介依赖子层	(215)
11.4.1 应用的范围和领域	(215)
11.4.2 服务概述	(216)
11.4.3 交互作用概述	(216)
11.4.4 基本服务和选项	(216)
11.4.5 物理媒介依赖服务访问点 (PMD_DAP) 的详细服务技术规范	(218)
11.4.6 物理媒介依赖 (PMD) 的通用操作技术规范	(227)
11.4.7 物理媒介依赖发送技术规范	(229)
11.4.8 物理媒介依赖 (PMD) 接收机技术规范	(233)
第 12 章 跳频扩频物理层技术规范	(235)
12.1 概述	(235)
12.1.1 跳频扩频 (FHSS) 物理层概述	(235)
12.1.2 跳频扩频 (FHSS) 物理层的功能	(235)
12.1.3 服务规范方法和符号	(236)
12.2 跳频扩频 (FHSS) 物理层 (PHY) 特定的服务参数清单	(236)
12.2.1 概述	(236)
12.2.2 发送矢量 (TXVECTOR) 的参数	(236)
12.2.3 接收矢量 (RXVECTOR) 的参数	(237)
12.3 跳频扩频 (FHSS) 物理层收敛协议 (PLCP) 子层	(237)
12.3.1 概述	(237)
12.3.2 物理层收敛协议 (PLCP) 帧格式	(238)
12.3.3 物理层收敛协议 (PLCP) 状态机	(241)
12.4 物理层管理实体 (PLME) 服务访问点 (SAP) 层管理	(252)
12.4.1 概述	(252)
12.4.2 跳频 (FH) 物理层 (PHY) 特定的 MAC 子层管理实体 (MLME) 规程	(252)
12.4.3 跳频 (FH) 物理层 (PHY) 管理实体状态机	(252)
12.5 跳频扩频 (FHSS) 物理媒介依赖 (PMD) 子层服务	(254)
12.5.1 应用范围和场合	(254)
12.5.2 服务概述	(254)
12.5.3 交互作用概述	(255)
12.5.4 基本服务与选项	(255)
12.5.5 物理媒介依赖服务访问点 (PMD_SAP) 详细的服务技术规范	(256)
12.6 跳频扩频 (FHSS PMD) 子层, 1.0Mb/s	(261)
12.6.1 1.0 Mb/s PMD 的通用操作技术规范	(261)

12.6.2	常规规则要求	(262)
12.6.3	工作频率范围	(262)
12.6.4	工作信道数量	(262)
12.6.5	工作信道的中心频率	(263)
12.6.6	占用信道带宽	(265)
12.6.7	最小跳频速率	(265)
12.6.8	跳频序列	(265)
12.6.9	多余辐射	(279)
12.6.10	调制	(279)
12.6.11	信道数据速率	(280)
12.6.12	信道切换 / 设置时间	(280)
12.6.13	从接收转换到发送的转换时间	(280)
12.6.14	物理媒介依赖 (PMD) 的发送技术规范	(280)
12.6.15	物理媒介依赖 (PMD) 的接收技术规范	(282)
12.6.16	工作温度范围	(283)
12.7	跳频扩频 (FHSS) 物理媒介依赖 (PMD) 子层, 2.0Mb/s	(284)
12.7.1	概述	(284)
12.7.2	四进制 GFSK 调制	(284)
12.7.3	信道数据速率	(285)
12.8	跳频扩频 (FHSS) 物理层管理信息数据库 (MIB)	(286)
12.9	跳频 (FH) 物理层 (PHY) 的特性	(293)
附录 A	专业术语定义	(295)
附录 B	缩写词	(301)

第 1 章 概 述

局域网（LAN）是处于同一建筑、同一单位或方圆几千米区域内的专用网络。局域网常用于连接公司办公室或工厂里的个人计算机和工作站，以便共享资源（如打印机）和交换信息。局域网采用的传输媒介多为有线电视或者光纤，这种局域网称为有线局域网。有线局域网应用非常广泛，而且传输速率高，构建成本低，但有一些固有的缺点：铺设电缆或检查电缆是否断线工作相当耗时。再者，由于企业及应用环境不断更新与发展，原有企业网络可能会需要重新布局，重新安装网络线路，虽然电缆本身并不贵，可是请技术人员来配线的成本很高，尤其是旧的大楼，工程费用就更高了。更关键的是有线局域网中的设备的使用位置是固定的，不允许在使用中移动设备。这些缺点导致在很多场合下使用有线局域网非常不方便。

而采用无线传输媒介的计算机局域网——无线局域网（WLAN）是相当方便的数据传输系统，是取代双绞铜线所构成的局域网络，WLAN 的简单存取结构使得用户能够实现“信息随身化，便利走天下”的理想境界。

1.1 无线局域网（WLAN）的特点

1.1.1 传输方式

WLAN 的传输方式包括 WLAN 采用的传输媒介、选择的频段及调制方式。目前 WLAN 采用的传输媒介主要有两种，即微波与红外线。采用微波作为传输媒介的 WLAN 技术根据调制方式不同，又可分为扩频方式与窄带调制方式。

1. 扩频方式

在扩频方式中，数据基带信号的频谱被扩展至几倍至几十倍之后再被搬移至射频前端发射出去。这一做法虽然牺牲了频带带宽，却提高了通信系统的抗干扰能力和安全性。由于单位频带内的功率降低，对其他电子设备的干扰相对减小。采用扩频方式的 WLAN 一般选择所谓的 ISM 频段，这里的 ISM 分别取自 Industrial（工业的）、Scientific（科研的）及 Medical（医疗的）的第一个字母。许多工业、科研和医疗设备都使用该频段。欧、美、日等国家的无线管理机构分别设置了各自的 ISM 频段。例如，美国的 ISM 频段由 902 MHz~928 MHz，2.4 GHz~2.484 GHz 和 5.725 GHz~5.850 GHz 三个频段组成。如果发送功率及带外辐射满足美国联邦通信委员会（FCC）的要求，则无须向 FCC 提出专门的申请即可使用这些 ISM 频段。

2. 窄带调制方式

在窄带调制方式中，数据基带信号的频谱不做任何扩展即被直接搬移到射频前端发射出去。与扩频方式相比，窄带调制方式占用频带少，频带利用率高。采用窄带调制方式的 WLAN

一般选用专用频段，需要经过国家无线电管理部门的许可方可使用。当然，也可选用 ISM 频段，这样可免去向无线电管理委员会申请。但带来的问题是，当临近的仪器设备或通信设备也在使用这一频段时，会严重影响通信质量，通信的可靠性无法得到保证。

3. 红外线方式

基于红外线的传输技术最近几年有了很大发展。目前广泛使用的家电遥控器几乎都是采用红外线传输技术。作为 WLAN 的传输方式，红外线方式的最大优点是这种传输方式不受无线电干扰，且红外线的使用不受国家无线管理委员会的限制。然而，红外线对非透明物体的透过性极差，这导致传输距离受限制。

1.1.2 无线组网特点

1. 通信可靠

抗干扰能力强，具有理想的接收灵敏度，全向天线能够提供强大的、可靠的无线传输。

2. 成本低

使用 WLAN 可以避免安装线缆的高成本费用、租用线路的月租费用以及当设备需要移动而增加的相关费用。

3. 灵活性

由于没有线缆的限制，用户可以随心所欲地增加工作站或重新配置工作站。

4. 移动性

WLAN 设置允许用户在任何时间、任何地点访问网络数据，不需要指定明确的访问地点，因此用户可以在网络中漫游。

5. 高吞吐量

WLAN 可以实现 54Mb/s 的数据传输速率，这个数字高于 T1 和 E1 线路的速率；WLAN 的安装工作非常简捷，不需要施工许可证，不需要布线或开挖沟槽。

1.1.3 安全性等同于有线

在无线通信领域，安全性是人们一直关注的一个问题，WLAN 通过使用额外的安全机制使其安全性等同于有线系统的安全性。这些安全机制包括：DSSS 扩频技术，FHSS 扩频技术，在单个工作站一级实现访问控制，使用网络标识和一种基于 RC4 加密技术的可选加密机制等。

1.2 WLAN 的应用

WLAN 的应用范围非常广泛，主要分为室内和室外两种应用。室内应用包括大型办公室、车间、智能仓库、临时办公室和会议室和证券市场等；室外应用包括城市建筑群间通信、学校校园网络、工矿企业厂区自动化控制与管理网络、银行金融证券城域网、矿山、水利、油田、港口、码头、江河湖坝、野外勘测实验、军事移动网和公安移动网等。

1. 有线网络的备份

对于某些关键应用，如金融、证券、税务、军事以及公安等，计算机网络系统的可靠性是至关重要的，这对于增强竞争力、提高服务质量或增强战斗力等具有举足轻重的作用。

因此，怎样保障计算机网络的可靠性是一个非常重要的课题。利用计算机无线网络作为有线网络的备份，可以大幅度提高网络系统的可靠性。当有线网络出现故障时，系统可自动切换到无线网络，应用可照常进行。

2. 移动通信

无线网络相对于有线网络具有很大的灵活性和机动性。无线网络的站点可以按照需要在一定的区域内移动（漫游），从而实现移动通信。

移动通信可用于实现流动银行、流动税收和移动备份等系统。

3. 有线网络的替代

在组建城域网或广域网时，无线网络相对于有线网络具有很高的性能价格比，可作为 DDN，FR 和 X.25 等的替代网络。

利用无线网络技术组建城域网或广域网可避免昂贵的线路租用费。无线网络的速率比一般的租用线路高得多，但价格相对较便宜，由于网络设备属于自己，便于维护和管理，避免了不必要的麻烦。

4. 不适合布线的地方

在难于布线的室外环境下，WLAN 可充分发挥其高速率、组网灵活之优点。尤其在公共通信网不发达的状态下，WLAN 可作为区域网（覆盖范围几十千米）使用。下面列出几种应用情况：

- ① 城市建筑群间通信；
- ② 学校校园网络；
- ③ 工矿企业厂区自动化控制与管理网络；
- ④ 银行、金融证券城区网络；
- ⑤ 城市交通信息网络；
- ⑥ 矿山、水利、油田等区域网络；
- ⑦ 港口、码头、江河湖坝区网络；
- ⑧ 野外勘测、实验等流动网络；

⑨ 军事、公安流动网络等。

1.3 无线局域网（WLAN）的标准

最早的 WLAN 产品运行在 900MHz 的频段上，速度大约只有 1Mb/s~2Mb/s。1992 年，工作在 2.4GHz 频段上的 WLAN 产品问世，之后的大多数 WLAN 产品也都在此频段上运行。目前的 WLAN 产品所采用的技术标准主要包括：IEEE 802.11、IEEE 802.11b、IEEE 802.11a、IEEE 802.11g、HomeRF、IrDA 和蓝牙。

1.3.1 802.11 家族

1. IEEE 802.11

1997 年 6 月，IEEE 推出了第 1 代 WLAN 标准——IEEE802.11（1997 版），随后在 1999 年推出了新的 IEEE802.11（1999 版）。该标准定义了物理层和媒介访问控制子层（MAC）的技术规范，允许 WLAN 及无线设备制造商在一定范围内建立互操作网络设备。任何 LAN 应用、网络操作系统或协议（包括 TCP/IP 和 Novell NetWare）在遵守 IEEE 802.11 标准的无线 LAN 上运行时，就像它们运行在以太网上一样容易。

IEEE 802.11 在物理层定义了数据传输的信号特征和调制方法，定义了两种无线电射频（RF）传输方式和一种红外线传输方式。其中 RF 传输标准包括直接序列扩频技术（Direct Sequence Spread Spectrum, DSSS）和跳频扩频技术（Frequency Hopping Spread Spectrum, FHSS）。DSSS 采用一个长度为 11 比特的 Barker 序列来对以无线方式发送的数据进行编码。每个 Barker 序列表示一个二进制数据位（1 或 0），并被转换成可以通过无线方式发送的波形信号。这些波形信号如果使用二进制相移键控（BPSK）调制技术，可以以 1Mb/s 的速率进行发射；如果使用正交相移键控（QPSK）调制技术，发射速率可以达到 2Mb/s。FHSS 利用 GFSK 二进制或四进制调制方式可以达到 2Mb/s 的工作速率。

由于在无线网络中碰撞检测较困难，IEEE 802.11 规定媒介访问控制（MAC）子层采用碰撞回避（CA）协议，而不是碰撞检测（CD）协议。为了尽量减少数据的传输碰撞和重试发送，防止各站点无序争用信道，WLAN 中采用了与以太网 CSMA/CD 相类似的 CSMA/CA（载波侦听多址访问 / 碰撞回避）协议。CSMA/CA 通信方式将时间域的划分与帧格式紧密联系起来，保证某一时刻只有一个站点发送，实现了网络系统的集中控制。因传输媒介不同，CSMA/CD 与 CSMA/CA 的检测方式也不同。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三种检测信道空闲的方式。

2. IEEE 802.11b

由于现行的以太网技术可以实现 10Mb/s，100Mb/s 乃至 1000Mb/s 等不同速率以太网之间的兼容，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