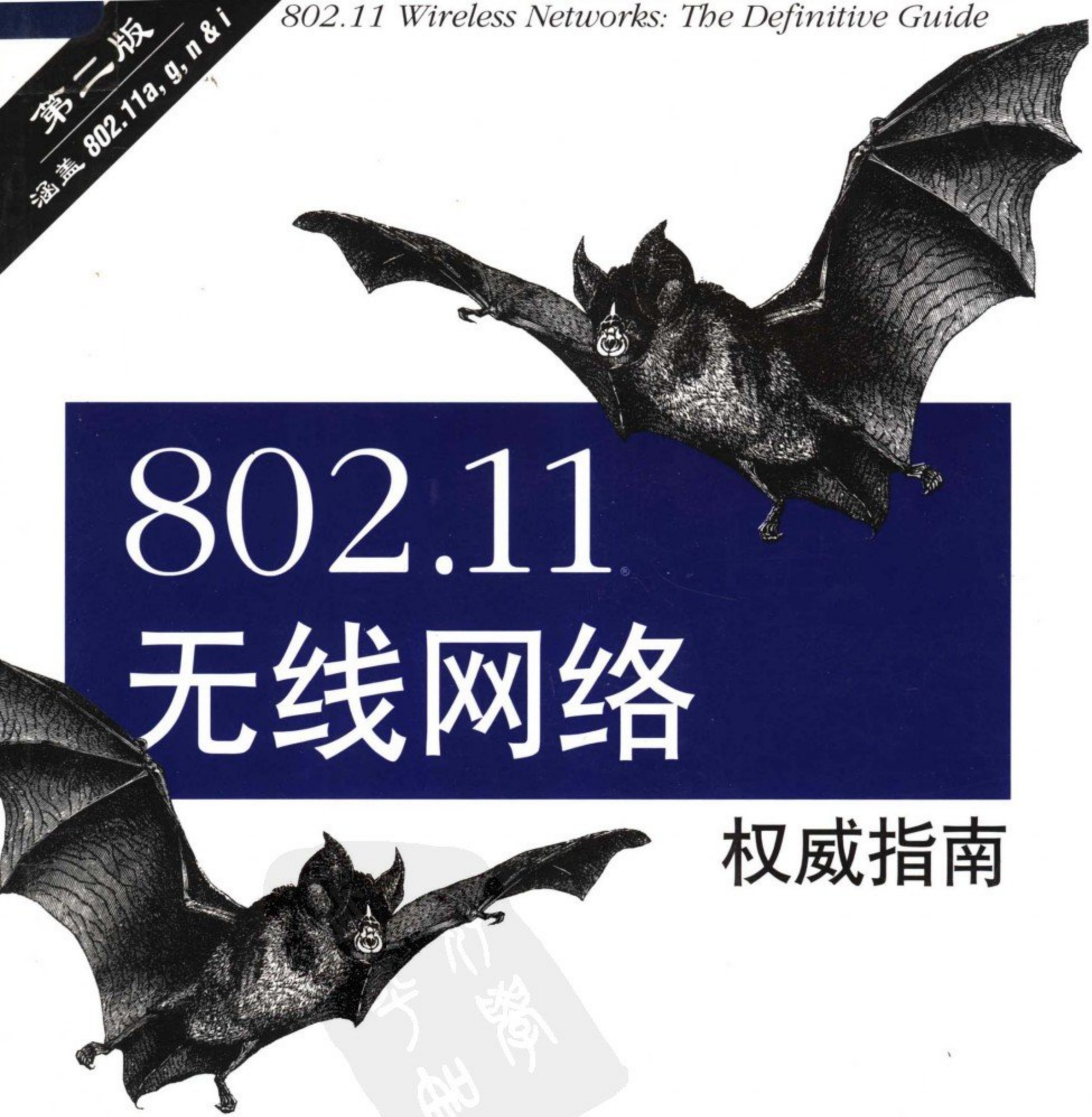
802.11 Wireless Networks: The Definitive Guide

第二版

涵盖 802.11a, g, n & i



802.11 无线网络

权威指南

O'REILLY®
東南大學出版社

Matthew S. Gast 著
O'Reilly Taiwan 公司 编译

O'REILLY®

802.11无线网络权威指南

使用无线网络是一种获得解放的、自由的经历。但是在这种经历的背后存在着一个复杂的协议，并且当数据不只限于在物理线路上传输时甚至会产生一些更为复杂的问题。怎样构造网络才能让移动用户活动自如？怎样扩展无线网络才能让它在任何需要的地方都可用？无线网络会产生哪些安全问题？怎样把无线网络调整到最佳性能？怎样提供足够的容量来支持最初预期的用户？怎样处理因更多的用户接入网络所带来的各种问题？

《802.11无线网络权威指南》第二版讨论了上述所有问题及其他相关问题。本书主要是为部署或维护无线网络的严谨的系统管理员或网络管理员编写的。书中广泛讨论了无线网络的安全问题，包括使用WEP标准的安全问题，并讨论了动态WEP和802.1X、802.11i安全标准。由于对于任何严谨的网络管理员来说网络监控都是一项必需的工作，因此本书有专门的章节阐述如何使用Ethereal及其他工具进行网络分析和故障排除。

《802.11无线网络权威指南》同时还介绍了无线网络的最新发展。除了802.11b和11a标准之外，本书同时涵盖802.11g，并前瞻了正在成为标准的802.11n协议。这个新的版本扩展了网络规划及架构的讨论，并特别关注了访问点之间的移动性、频谱管理和功率控制。本书是目前唯一的讲述了如何衡量无线网络性能及如何调整网络到最佳性能的工具书。

最后，《802.11无线网络权威指南》展示了怎样配置无线网卡和Linux、Windows与MAC OS X系统，以及怎样处理访问点。很少有一本书能够把你需要掌握的理论和完成工作所需要的实际经验与建议有机地结合在一起。《802.11无线网络权威指南》就是这样的一本好书。如果你负责管理无线网络，你就需要这本书。

Matthew S. Gast 是无线网络规划和部署方面的权威作者。

Visit O'Reilly on the Web at
www.oreilly.com

O'Reilly Media, Inc. 授权东南大学出版社出版

ISBN 978-7-5641-1006-2
9 787564 110062 >
定价：79.00元

此简体中文版仅限于在中华人民共和国境内(但不允许在中国香港、澳门特别行政区和中国台湾地区)销售发行
This Authorized Edition for sale only in the territory of People's Republic of China (excluding Hong Kong, Macao and Taiwan)

TN92-62/2

2007

第二版

802.11®无线网络权威指南

Matthew S. Gast 著

O'Reilly Taiwan 公司 编译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc. 授权东南大学出版社出版

南京・东南大学出版社

图书在版编目（CIP）数据

802.11® 无线网络权威指南：第2版 /（美）加斯特（Gast, M. S.）著；O'Reilly Taiwan 公司编译．－南京：东南大学出版社，2007.12

书名原文：802.11® Wireless Networks: The Definitive Guide, second edition

ISBN 978-7-5641-1006-2

I. 8… II. ①加… ②O… III. 无线电通信－通信网－指南 IV. TN92-62

中国版本图书馆 CIP 数据核字（2007）第 187616 号

江苏省版权局著作权合同登记

图字：10-2006-214 号

©2005 by O'Reilly Media, Inc.

Simplified Chinese Edition, jointly published by O'Reilly Media, Inc. and Southeast University Press, 2007. Authorized translation of the English edition, 2005 O'Reilly Media, Inc., the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 O'Reilly Media, Inc. 出版 2005。

简体中文版由东南大学出版社出版 2007。英文原版的翻译得到 O'Reilly Media, Inc. 的授权。此简体中文版的出版和销售得到出版权和销售权的所有者 —— O'Reilly Media, Inc. 的许可。

版权所有，未得书面许可，本书的任何部分和全部不得以任何形式重制。

802.11® 无线网络权威指南（第二版）

出版发行：东南大学出版社
地　　址：南京四牌楼 2 号　　邮编：210096
出 版 人：江　汉
网　　址：http://press.seu.edu.cn
电子邮件：press@seu.edu.cn
经　　销：全国各地新华书店
印　　刷：扬中市印刷有限公司
开　　本：787 毫米 × 980 毫米　16 开本
印　　张：38.75 印张
字　　数：650 千字
版　　次：2007 年 12 月第 1 版
印　　次：2007 年 12 月第 1 次印刷
书　　号：ISBN 978-7-5641-1006-2/TP · 163
印　　数：0001-4000 册
定　　价：79.00 元（册）

本社图书若有印装质量问题，请直接与读者服务部联系。电话（传真）：025-83792328

O'Reilly Media, Inc. 介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc.授权东南大学出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc.是世界上在Unix、X、Internet和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的《The Whole Internet User's Guide & Catalog》（被纽约公共图书馆评为二十世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc.一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc.是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc.具有深厚的计算机专业背景，这使得O'Reilly Media, Inc.形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc.所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc.还有许多固定的作者群体——他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc.依靠他们及时地推出图书。因为O'Reilly Media, Inc.紧密地与计算机业界联系着，所以O'Reilly Media, Inc.知道市场上真正需要什么图书。

作者简介

Matthew S. Gast 曾协助各种组织了解无线网络技术，建设具有扩充性的、基于标准的安全无线局域网络。过去这几年，他自愿在 Interop Labs 担任工程师与讲师，他在那里与许多顶尖的工程师共事，学到了各种先进的网络安全协议并在研讨会中传达给其他与会者。Matthew 参加过的研讨会不计其数，范围横跨各大陆，他在研讨会上所连接过的无线网络比他在撰写本书第二版时所连接过的还多。他在加入目前所任职的无线局域网络系统公司之前，曾在数家网络安全公司工作过几年。

Matthew 目前的专业领域（professional interests）是身份识别管理（identity management）与身份认证协议（authentication protocol）、联盟式网络（federated network）以及动态授权（dynamic authorization）。空闲的时候，Matthew 喜欢在他漫游式的生活形态中充分利用数字电视并偶尔为新创公司提供建议。

封面介绍

《802.11 无线网络权威指南》第二版的封面动物是蹄鼻蝠（horseshoe bat，学名为 *Rhinolophus hipposideros*）。这种数量稀少、濒临绝种的蝙蝠在欧洲蹄鼻蝠中体型最小，重量通常只有 4～10 克，展翼长度可达 19～25 公分。由于鼻子附近的皮肤呈叶状马蹄形因而得名。此鼻叶（nose-leaf）有助于修正与引导其鼻孔发射出的超声波（一种称为“回声定位”的感觉方式），借此辨识周围的环境、侦测障碍物、彼此沟通以及寻找食物。蝙蝠的回声定位系统相当精确，可以侦测蚊子（gnat）大小的昆虫以及细如发丝的物体。

小蹄鼻蝠（lesser horseshoe bat）的栖息地散见各处，分布于不列颠群岛至阿拉伯半岛与中亚以及摩洛哥至苏丹地区。小蹄鼻蝠原本是穴居型蝙蝠，不过夏日繁殖季节也有可能群聚于旧农舍的屋檐。有时候，它们会筑巢于灌木与空心木林。繁殖集群（maternity colonies）通常会聚集 30 ～ 70 只蝙蝠，不过有人曾经发现由 200 只母蝙蝠聚集而成的繁殖集群。小蹄鼻蝠有时会聚在一起冬眠，时间由十月至翌年四月底或五月初。它们冬天的巢穴通常位于地底下，如洞穴或隧道。小蹄鼻蝠利用脚趾悬挂并以两翼包覆身体。虽然通常倒吊于开放且无遮蔽的地点，不过它们很少成群地挤在一块。

目录

序 1

前 言 3

第一章 无线网络导论 13

为何需要无线？ 13

无线网络的特色 17

各式各样的网络 20

第二章 802.11 网络概论 23

IEEE 802 网络技术族谱 24

802.11 相关术语及其设计 25

802.11 网络的运作方式 33

移动性的支持 39

第三章 802.11 MAC 基础 43

MAC 所面临的挑战 44

MAC 访问模式与时机 47

利用DCF进行基于竞争的访问 52
帧的分段与重组 55
帧格式 57
802.11对上层协议的封装 65
基于竞争的数据服务 66
帧的处理与桥接 74

第四章 802.11成帧细节 78
数据帧 78
控制帧 87
管理帧 93
帧传送、关联与身份验证状态 123

第五章 有线等效加密 127
WEP的密码学背景 128
WEP的加密操作 130
关于WEP的种种问题 136
动态WEP 140

第六章 802.11x用户身份验证 142
可扩展身份验证协议（EAP） 143
EAP认证方式（EAP Method） 149
802.1X：网络连接端口的认证 154
802.1X与无线局域网 158

第七章 802.11：RSN、TKIP与CCMP 162
临时密钥完整性协议（TKIP） 162
计数器模式及密码块链消息认证码协议（CCMP） 173
强健安全网络（RSN）的运作方式 176

第八章 管理操作 182

管理结构 182
扫描 183
身份验证 188
预先身份验证 192
关联操作 196
节省电力 200
定时器的同步 208
频谱的管理 211

第九章 PCF 无竞争服务 224

以 PCF 提供无竞争访问 224
PCF 帧的封装细节 228
电源管理与 PCF 233

第十章 物理层概述 235

物理层结构 235
无线链路 235
RF 传播与 802.11 242
802.11 的 RF 工程 247

第十一章 跳频物理层 251

跳频传输 251
高斯频移键控（GFSK） 256
FH PLCP 259
FH PMD 261
FH PHY 的特性 262

第十二章 直接序列物理层：DSSS 与 HR/DSSS (802.11b) 263

直接序列传输 263
差分相移键控（DPSK） 270
"原本的" 直接序列物理层 273
补码键控（CCK） 277
高速直接序列物理层（HR/DSSS PHY） 278

第十三章 802.11a 与 802.11j: 5-GHz OFDM PHY ... 286

正交频分复用（OFDM） 287
802.11a 所采用的 OFDM 293
OFDM PLCP 301
OFDM PMD 304
OFDM PHY 的特性 308

第十四章 802.11g：增强速率物理层 309

802.11g 的组件 309
ERP 的物理层会聚过程（PLCP） 314
ERP 的物理媒介相关（PMD） 319

第十五章 802.11n 前瞻：MRMO-OFDM 322

共同功能 323
WWiSE 325
TGnSync 336
比较与结论 350

第十六章 802.11 硬件 353

802.11 接口的一般结构 353
实现上的差异 358
解读规格表 360

第十七章 802.11 与 Windows 362
Windows XP 362
Windows 200 377
Windows 计算机验证 378

第十八章 802.11 与 Macintosh 382
AirPort Extreme 网卡 382
在 AirPort 上使用 802.1X 389

第十九章 802.11 与 Linux 396
Linux 所支持的 PCMCIA 396
Linux 无线扩展功能与工具 405
Agere (Lucent) Orinoco 411
采用 Atheros 芯片组的网卡与 MADwifi 413
在 Linux 中使用 xsupplicant 416

第二十章 使用 802.11 接入点 423
接入点的基本功能 424
以 Ethernet 供电（PoE） 429
选购接入点 432
Cisco 1200 接入点 434
Apple AirPort 接入点 440

第二十一章 无线网络逻辑架构 445
评估逻辑架构 445
网络拓扑范例 458
逻辑架构的选择 477

第二十二章 安全性架构 480
安全性的定义与分析 481

身份验证与访问控制 485
以加密确保私密性 494
安全协议的选择 501
私设接入点 511

第二十三章 网络规划与项目管理 517
项目规划与需求 518
网络需求 519
物理层的选择与设计 530
接入点摆放位置规划 534
使用天线调整覆盖范围 541

第二十四章 802.11 网络分析 548
网络分析工具 548
Ethereal 550
802.11 网络分析项目清单 561
其他工具 565

第二十五章 802.11 性能与调整 568
802.11 性能评估 568
改善性能 571
802.11 可调参数 573

第二十六章 结论与展望 580
标准化工作 580
无线网络的当前趋势 582
结语 591

名词解释 593

序

早在碰面之前，Matthew Gast就已经是我的心灵导师。当我发现Apple果真推出传闻已久的基于802.11b的AirPort基站，便于2000年10月开始报道无线数据网络。

我曾经热衷于所谓的红外线无线网络，也曾浪费许多时间研究一些“有趣”却走入死胡同的网络技术。我原本以为802.11b不过是另一种玩具，很高兴我是错的！

一路这样摸索过来，让我遇见了第一版的《802.11无线网络权威指南》。这玩意真能和宣传的一样吗？我对ISO参考模型、TCP/IP与Ethernet帧还算颇有了解，不过仍然无法将Ethernet的共享竞争（shared contention）与这种容许众声喧哗的媒介放在一块。

通过文字与图表，Matthew教我一些原本我并不了解的东西。过去5年，我在《纽约时报》(New York Times)、《西雅图时报》(The Seattle Times)、*PC World*以及自己所开设的Wi-Fi Networking News（*http://www.wifinetnews.com*）网站上发表过许多文章。为了以浅显易懂的方式向一般大众解释何谓Wi-Fi，当我深入探究技术细节时这些文字图表都是我一再回顾的东西。

一开始，我从《802.11无线网络权威指南》学习相关缩略术语(acronym)。通过Matthew的这本书，我后来终于超越了只知WDS代表Wireless Distribution System的程度，真正了解接入点之间如何通过允许四方协商封包传输的802.11内置机制来彼此交换数据。

斗转星移，802.11家族逐渐成熟而多样化，如今本书的第一版已经稍嫌过时。不过令人惊讶的是，这些所谓的“创新”仍然根植于20世纪90年代初期至中期的技术发展。相较于2005年的“咖哩肉汤”，本书第一版的缩略术语（alphabet soup）只能用清淡来形容（译注1）。

译注1：*alphabet soup*原本是指康宝公司推出的一种浓汤，里面有英文字母状的面团，后来引申为缩略术语（acronym）。

为了弥补本书第一版与无线网络发展现况之间的差距，Matthew持续在O'Reilly的Wireless DevCenter发表文章，每一篇我都迫不及待地仔细拜读。在一场Wi-Fi Planet所举办的会议上，有人把Matthew介绍给我认识。我们可说是一见如故：如果记得没错的话，当时我追着他请教802.1X的相关细节，而他只想谈谈我的书，了解我在做些什么。（之前我写过两本通俗的Wi-Fi方面的书，不过无法与Matthew这本优秀的技术书相提并论。）

从那时起，我就坐拥少有的特权，得以分享Matthew的真知灼见。Matthew从不轻易论断，而是倾向于深入研究。与生俱来的好奇心驱使他不断深掘，直到获得技术上与逻辑上一致的答案。

以发展过程错综复杂且充满政治角力的802.1X标准为例。（若非Matthew，我还不知道X应该大写，因为802.1X是独立而非附属于其他规格的标准。虽然大伙遵循的是IEEE所立下的规矩，不过连IEEE本身都犯了这个错误。）

802.1X本身并不复杂，它采用一种通用的消息传递方式来进行身份验证，称为可扩展身份验证协议（Extensible Authentication Protocol，简称EAP）。不过对于如何确保EAP本身的安全性，则十足反映出Microsoft与Cisco之间的竞争。为了控制这项老的协议，两家公司角力的结果反而让EAP无法达到更高的安全性。

Matthew跳脱这些沾染宗教色彩的论战，在O'Reilly Network发表了一篇文章，列举出各种可行的方法、所遭遇的困难以及互用性议题。这些精华都收录在本书当中，而且增加了不少篇幅。本书出版之前，我想读者很难在其他地方找到更完整、更具说服力的解释；你很难在他处找到比这些内容更清晰、更容易理解且不受市场政治左右的文章。

有时候，Matthew会将本书迟迟未能改版归咎于自己加入了一家生产无线网络交换器的新创公司。不过我倒认为，读者反而因此受惠于这些焚膏继晷、得之不易的知识。

以往，Matthew与802.11之间的关系就像是熟悉自家一草一木的工匠。马桶坏了，他就动手换个阀;客厅需要新的电源插座，他就研究看看如何进行，然后接条线过来。

但是Matthew的新工作让他从周末的家居战士变身为万能师傅。打掉内墙、重砌、铺管与架线不仅难不倒他，Matthew还会偶尔抱怨一下当地的建筑法规。

很荣幸能够认识Matthew，更荣幸的是能够介绍这本书给各位，让各位都能够一探过去几年来我和其他人一直共享的秘密花园。

——Glenn Fleishman

西雅图，华盛顿

2005年2月

前言

人们可以行动自如，而网络则不然。

相比较于其他说法，这句话更足以解释无线局域网络（wireless LAN）在硬件方面的爆炸性成长。不过短短几年，无线局域网络已经从昂贵、新奇的事物，成长为当前的主流技术。

无线网络让用户摆脱网络连接端口的束缚，不再受制于网络的物理位置。不过要摆脱具体的网络限制，需要不少的协议工程。为了给用户提供不受空间限制的服务，网络必须掌握更多用户所在位置的信息。

写作本书的很多时间是花在飞机上、机场里以及火车上。要将演变中的网络技术浓缩为一本书，大部分的研究工作都离不开因特网。要不是能够随时随地访问网络，本书或许得耽搁更久方能问世。

无线网络的优势使它们快速成长为数十亿美元的设备市场。如今wireless LAN在整个网络环节中已占有一席之地，学习如何掌握wireless LAN自然成为人们必须面对的课题。

解放的普罗米修斯：Wireless LAN的种种可能性

相较于固定（或有线）网络，无线网络具备下列优点：

移动性

用户有四处游走的需要，不过数据通常集中存储。能够让用户在移动间访问数据可大幅提高生产力。构建网络是为了给用户提供有价值的服务。过去，网络设计人员所关注的焦点在于网络连接端口，因为每个连接端口通常对应到一位用户。不过无线网络并没有物理连接端口，因此用户身份便成为网络设计的中心。

部署容易，构建快速

对传统的有线局域网络（wired LAN）而言，要在某些场所布线相当困难。建筑物老旧通常是问题所在:要在一栋设计蓝图已经不知去向的旧式石材建筑中穿墙布线，的确不是件容易的事。此外，有些地区碍于法令限制，要在列为古迹的建筑物中架设局域网络更是难上加难。就算装置地点位于新建的设施中，除了所费不赀，布线也十分耗时。

灵活性

既然无需网线，也就没有重新布线的问题。利用无线网络，用户可以迅速构建小型、临时性的组网络以供会议之用，随意游走于各间办公室也变得易如反掌。相形之下，无线网络的扩展十分容易，因为网络媒介无处不在。用户再也不必到处拉线、接线甚至是绕线。灵活性是“hot spot”（热点）市场，包括旅馆、机场、车站（甚至是列车本身）、图书馆以及咖啡馆在内的最大卖点。

成本

有时候，采用无线技术可以节省不少成本。举例而言，可以利用802.1®设备在两栋建筑物之间搭设一道无线网桥（wireless bridge）。设置无线网桥需要支付一些初期购置成本，包括户外设备、无线接入点（access point）以及无线网卡（wireless interface）。扣除初期的固定资本支出，基于802.11的视距（line-of-sight）网络每月所需要支付的运营成本可说是微乎其微。长期而言，这种点对点(point-to-point)的无线链路远比电话公司所提供的专线便宜得多。

虽然有上述种种好处，但在1997年802.11标准制定之前，用户只能屈就于个别厂商所提供的解决方案，承担其所附带的风险。直到802.11开始席卷市场，传输速度随即由2Mbps跳升为11Mbps甚至是54Mbps。无线适配卡以及天线的标准化，使得构建无线网络不再遥不可及。许多服务供应商（service provider）趁势推出相关服务，一些主要城市的志愿团体也开始利用802.11构建公用无线网络（public wireless network）。

802.11已经成为一种普遍公认的连接方式。只要有一组接入点，就可以为访客提供连接服务，不必再通过Ethernet开放公用连接端口。802.11成为标准的这几年来，“热点”(hot spot）一词的含义已经从带点异国情调的固定场所，转变为能够在行进间提供连接的技术。以802.11搭配卫星上行链路，就算移动速度很快，一样可以访问因特网。有些铁路通勤系统已经开始提供移动式热点。即便巡航速度（cruising speed）高达每小时550英里，波音公司的Connexion也可以在飞机上提供类似服务。

致读者

本书主要针对需要进一步学习wireless LAN的操作（operation）、部署（deployment）以及监控（monitoring）等种种技术方面的读者：

- 打算将802.11设备整合到现有网络或是构建基于802.11的网络的架构人员(network architect)。
- 负责构建与维护802.11网络的网络管理人员(network administrator)。
- 关心由802.11设备的部署可能衍生的安全问题以及致力于解决这些问题的安全专业人员(security professional)。

本书假设读者具备某种程度的计算机网络相关背景知识。读者应该对IEEE 802网络(特别是Ethernet)、OSI参考模型、TCP/IP以及其他相关网络通信协议有基本的了解。对大多数网管人员而言，无线局域网络并非全新领域，不过还是有若干新的概念，特别是在无线电传输方面。

付梓书(Book in Black and White)序曲，第2号作品

有些技术变动得十分快速，想要为之著书立说并不容易。困难之处部分是因为无法十分确定应该涵盖哪些内容。本书改版的这几年间，安全性占据整个发展的主轴，因此更新这方面的信息就成为本次改版的重点。本书有两个主要目的：除了教授读者802.11标准本身，也提供构建802.11 wireless LAN实践上的建议。这两个目的本身互不冲突，因此各位可以按图索骥，挑选自己感兴趣的章节。为了协助读者决定阅读顺序以及对章节部署有整体的概念，兹将各章内容摘要于下：

第一章 无线网络导论

论述了无线网络与传统有线网络之间的差异以及采用无线媒介时必须面临的种种问题，例如网络界限模糊以及媒介不可靠等问题。wireless LAN或许具体展现了Christian Huitema所说的“Internet没有中心，只有不断扩展的边际”。当wireless LAN技术逐渐普及，整个边际也就更加模糊了。

第二章 802.11 网络概论

描述了802.11 Wireless LAN的整体架构。802.11有点类似于Ethernet，不过加入了一些新的网络组件以及一堆新的缩略术语。读者可在本章看到使用802.11网络时会接触到的网络组件。大致而言，这些组件包括工作站(station，配备无线网卡的移动设备、接入点(access point，位于工作站与分布式系统之间的桥接器)以及分布式系统本身(distribution system，即有线骨干网络)。工作站在逻辑上被划归为基本服务集(Basic Service Set，简称BSS)。如果没有接入点参与其中，该网络即是较为松散、由工作站彼此自治(ad-hoc confederation)的独立基本服务集(independent BSS，简称IBSS)。接入点允许个别的BSS彼此串联为逻辑上相连的组，这种结构称为扩展服务集(Extended Service Set，简称ESS)。

第三章 802.11MAC 基础

深入探讨了 802.11 标准的媒体访问控制（Media Access Control，简称 MAC）层协议。和所有 IEEE 802 网络一样，802.11 将 MAC 层功能与物理媒介访问功能加以隔离。802.11 包含了许多不同的物理层，不过使用相同的 MAC。网络媒介的访问方式主要还是通过竞争（contention），不过其所采用的是冲突避免（collision avoidance，即 CSMS/CA）而非冲突检测（collision detection，即 CSMA/CD）。本章同时探讨了 802.11 帧（frame）的数据封装方式（data encapsulation），让网络管理人员得以了解传输数据时所使用的帧格式。

第四章 802.11 成帧细节

以第三章为基础，详细说明了不同类型的帧及其使用场合。本章比较偏向参考之用，而不是作为实际的阅读材料。本章详细描述了三种主要帧：数据帧（data frame）负责搬运数据，控制帧（control frame）扮演监督（supervisory）的角色，管理帧（management frame）负责协助 802.11 MAC 完成其他扩展操作。信标（Beacon）除了用来宣布 802.11 网络的存在并协助整个关联过程（association process）外，对工作站进行身份验证时也派得上用场。

第五章 有线等效加密（WEP）

描述了有线等效加密（Wired Equivalent Privacy，简称 WEP）协议。虽然有瑕疵，WEP 仍是无线局域网络安全领域的许多后续工作的基础。本章探讨了何谓 WEP、WEP 如何运作以及为何不能依赖 WEP 提供有用的隐私与安全。

第六章 802.1X 用户身份验证

描述了 802.1X 身份验证架构。搭配可扩展身份验证协议（Extensible Authentication Protocol），802.1X 为无线局域网络提供了坚固的身份验证解决方案，同时改善了加密方面的功能。

第七章 802.11i：RSN、TKIP 与 CCMP

描述了 802.11i 无线局域网络安全标准。为了解决 WEP 的基本瑕疵，802.11i 设计了两种新式的链路层加密协议及产生与传递密钥的机制。

第八章 管理操作

主要探讨 802.11 网络的管理操作。加入任何网络之前，工作站必须通过扫描，寻找由接入点或 IBSS 创建者主动发布的网络。传送任何数据之前，工作站与接入点之间必须处于连接状态。本章同时探讨了 MAC 内置的电源管理功能，它可让以电池供电的工作站进入休眠模式并且定时醒来接收为其暂存的数据。

第九章 PCF 无竞争服务

主要探讨点协调功能（point coordination function，简称 PCF）。PCF 在实现上并不常见，因此本章可略过不读。PCF 是以无竞争（contention-free）方式访问无线

媒介的基础。在无竞争访问中，无线媒介由中央控制，访问时必须持有令牌(token)，此令牌通常由接入点提供。

第十章 物理层概述

探讨了802.11模型中物理层（physical layer，简称PHY）的一般架构。PHY本身可进一步区分为两个子层（sublayer）。物理层会聚过程（Physical Layer Convergence Procedure，简称PLCP）子层除了加入前导码（preamble）以形成完整帧外，同时还加入了本身的标头；而物理媒体相关（Physical Medium Dependent，简称PMD）子层则会为帧加入调制（modulation）的细节。较常见的PHY是以射频（radio frequency，简称RF）作为无线媒介，因此本章将以RF系统与技术的简短讨论作为结尾。

第十一章 FH PHY

描述的是最早期的802.11物理层。市面上已经很难买到FH PHY相关产品，不过早期大多数设备均采用此物理层。历年来一直参与802.11技术发展的机构或许还有熟悉此物理层的需要。

第十二章 DS PHY：DSSS与HR/DSSS（802.11b）

主要探讨以直接序列扩频技术为基础的两种物理层。802.11原始标准所规范的物理层提供1Mbps与2Mbps两种速率。不过，直到802.11b加入5.5Mbps与11Mbps这两种传输速率，整个技术才算真正起飞。本章将一并描述这两种密切相关的物理层。

第十三章 802.11a与802.11j：5-GHz OFDM PHY

探讨了802.11a标准所定义的5-GHz物理层，传输速度可达54Mbps。此物理层所使用的调制技术称为正交频分复用（orthogonal frequency division multiplexing，简称OFDM）。此物理层需要稍加修改后方能在日本使用，亦即后来的802.11j标准。

第十四章 802.11g：增强速率物理层

主要探讨一种使用OFDM技术但与802.11b共享2.4 GHz频带的物理层。802.11g大幅压缩了802.11b的生存空间，也是新式笔记本计算机常见的内置联网方式。此物理层与802.11a物理层几乎完全相同，差别在于802.11g可以向下兼容于使用相同频带的旧设备。

第十五章 802.11n前瞻：MIMO-OFDM

描述了目前仍在开发中的物理层。为了提供更高速率，802.11n所使用的物理层是以多进多出（multiple-input/multiple-output，简称MIMO）为基础。本书即将付印之际，这两份标准建议书尚在委员会中争斗。两者在本章均有探讨。

第十六章 802.11 硬件

开始从理论性议题过渡到标准的实现议题。802.11算是比较宽松的标准，留给实现相当大的空间。不同的网卡可能具有不同的性能，协议的实现上也可能有所差异。这些差异主要来自于硬件的建构方式。

第十七章 802.11 与 Windows

描述了 Windows 驱动程序的基本安装流程以及安全方面的配置设定。

第十八章 802.11 与 Macintosh

描述了如何在MacOS X上使用AirPort网卡连接至802.11网络。焦点放在Mac OS X 10.3，因为这是包含 802.1X 支持的第一个软件版本。

第十九章 802.11 与 Linux

描述了如何让Linux系统支持802.11网络。交代了如何让操作系统支持PC Card之后，本章接着会说明如何使用无线扩展功能（wireless extension）的API。于此将探讨两种常见的驱动程序，一种支持旧式的Orinoco 802.11b网卡，另一种则支持使用 Atheros 芯片组的新式网卡，称为MADwifi。最后，本章将说明如何使用xsupplicant进行802.1X安全配置设定。

第二十章 使用 802.11 接入点

探讨了802.11基础（infrastructure）网络所使用的设备。商用接入点产品的功能各不相同。本章描述了接入点上常见的功能，提供采购建议以及两个实际的设定范例。

第二十一章 无线网络逻辑架构

这是本书论述层次的第三次转变，从 802.11 个别设备的实现过渡到如何构建较大规模的 802.11 网络。构建网络时有几种不同的做法可供选择，这些做法各有其优缺点。除了列举常见的网络拓扑类型，本章还会提供选择上的建议。

第二十二章安全架构

应该接着上一章阅读。安全架构的主要挑战在于如何以开放性媒介提供网络访问，同时又能兼顾网络安全。安全性的选择与架构上的选择互相影响。本章提出了设计网络时必须面临的几项重要抉择：打算使用何种身份验证方式？如何与现有的用户数据库整合？如何加密以确保数据安全？如何处理未经授权的接入点部署问题？

第二十三章 网络规划与项目管理

这是针对网管人员的最后一章。设计大规模的无线网络之所以困难，是因为要求访问的用户数量太多。如何确保网络具备足够带宽以满足来自四面八方的用户需求，免不了需要事先规划。接入点的位置选择绝大部分取决于无线电波环境。传统而言，这是构建网络时最耗时的工作。

第二十四章 802.11 网络分析

主要教导网络管理人员如何得知 wireless LAN 发生了什么事。不论在有线还是无线网络中，网络分析软件都具有相当重要的价值。本章探讨了如何使用网络分析软件以及各种症状的含义。其次，也描述了如何编译 Ethereal 分析软件以及如何着手进行一般问题的障碍排除。

第二十五章 802.11 性能调整

主要探讨网管人员如何提升吞吐量。一开始，本章会描述如何计算有效载荷数据（payload data）的整体吞吐量以及提升性能的一般做法。有时候，调整一些常见的 802.11 参数或许会有所帮助。

第二十六章 结论与展望

用来总结 802.11 工作小组目前正在进行的标准化工作。综述这些进行中的工作之后，至少我可以预见与希望未来本书改版时可以不必大费周章。

与第一版的主要差异

2002 年至 2005 年这 3 年间无线局域网络历经相当大的变动。标准本身持续演进，提供更高的安全性与互用性。依据“更快、更好、更便宜”的典型技术发展形态，大多数802.11接口的数据传输率已经从 802.11b 的 2 Mbps 或 11 Mbps 跃升为 802.11a 与 802.11g 的 54 Mbps。即便在大规模网络的应用上仍有其限制，速度更快与向下兼容已经证明是802.11g在商业上制胜的配方。即将标准化的802.11n意在进一步提升速度。用户莫不迫切期待物理层技术的进一步发展，由准标准（pre-standard）产品相当受欢迎即可印证。本书增加了两个全新的章节，分别探讨802.11g 与 802.11n。在 802.11h 的频谱管理发展过程中，欧洲采用 802.11a 纯属偶然事件，因此管理章节必须大幅改写。

本书第一版于 2002 年发行时，802.11 的安全性经常受到质疑。WEP 显然有所不足，不过当时并没有更好的替代方案。大多数网管人员比较习惯应付内置（而非外挂）的远程访问系统。802.11i的发展大幅简化了网络的安全防护工作。如今，安全性的考虑已经内置于规范说明书中，不像以往那样需要假以外求。安全性的改良散见全书，从说明新协议如何运作的全新章节到如何将之运用于客户端，甚至是构建网络时如何选择不同的选项。比起 3 年前，筛选适当的安全性选项如今变得更为复杂，因此有必要从初版的一节扩增为独立的一章。

3 年前，接入点大多十分昂贵，而且数量一多，接入点的表现就不如人意。进行网络部署时，通常得试着突破当时既有设备的种种限制。3 年后，接入点的功能更强、选择更多，部署时也更具灵活性。如今已经有多种选项可供选择，不再需要屈就“一体适用”（one size fits all）的部署模型。安全性协议已有长足的改善，如今探讨部署技术时已经可以

着眼于它能够为组织贡献什么，而不必再担心或聚焦于如何防止失控的情况发生。因此，原本有关网络部署的篇幅扩增为3章，分别探讨部署过程的各个主要部分。

排版约定

斜体字（*Italic*）：

- 路径名称、文件名称、类名以及目录
- 新定义的术语
- Internet 地址，例如域名与 URL

黑体字（**Bold**）：

- GUI 组件

等宽字（`Constant Width`）：

- 屏幕上应该逐字键入的命令行及其选项
- 所有列出的程序代码

等宽斜体字（*`Constant Width Italic`*）：

- 指出可以由你自己的程序中的实际值替换的项目的占位符

等宽黑体字（**`Constant Width Bold`**）：

- 程序代码范例中由用户键入的文字

建议与问题

O'Reilly公司是世界性的计算机信息出版公司。我们永远乐意听到读者对出版品的意见，包括如何让本书可以更好的建议、指正本书的错误或是读者建议本书往后改版时应该再加进来的其他主题。以下是本公司的联络资料：

美国：

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

中国：

100080 北京市海淀区知春路 49 号希格玛公寓 B 座 809 室
奥莱理软件（北京）有限公司

本书的网页上列出了勘误表、示例和任何额外的信息。可登录以下网址查询：

http://www.oreilly.com/catalog/802dot112/（原版书）
http://www.oreilly.com.cn/book.php?bn=978-7-5641-1006-2（中文版）

在一个快速发展的领域中，一些短小的文章总是能架起最新实践的情况和印刷成书之间的桥梁。读者可以访问我的博客和文章：

http://www.oreillynet.com/pub/au/692/

如果想要发表关于本书的评论和技术问题，请发邮件至：

bookquestions@oreilly.com
info@mail.oreilly.com.cn

关于图书、会议、资源中心和 O'Reilly 网络的更多信息，请查看我们的站点：

http://www.oreilly.com
http://www.oreilly.com.cn

致谢

尽管乐于相信各位阅读本书是因为它的娱乐价值，但我还不至于如此天真。相比较于枯燥的技术规范书，技术类书籍的价值在于能够正确地呈现细节，并且用比较容易理解的方式加以表达。每一本技术类书籍背后都有一个审稿团队负责检阅初稿并协助改善。我的审阅小组找出了一堆错误，使本书更加完善。Tropos Networks 的 Malik Audeh 博士堪称我的无线电良知（找不到更好的字眼可以形容）。我并非无线电方面的专家，我所拥有的无线电知识都是因为对 802.11 感兴趣而学习得来的。802.11 问世之前，Malik 就已经通晓无线电技术，而我一直有幸可以分享他的见识。Texas A&M 的 Gerry Greager 在FCC法规与无照设备的管理方面提供了不少意见。由于无线局域网络近年来不断颠覆这些法规，因此这些意见益发显现其价值。Glenn Fleishman 答应为本书写序时，我压根想不到他竟然会耗费那么多心力，从更为宏观的脉络来了解802.11。他所建议的一些细节是参考过去几年他在自己的 Wi-Fi Networking News 网站上所发表的一些文章。同样身为作家，Gleen 指出几个地方可以提供更好的范例，让我的论点更加清楚。最后要感谢 Open1X 项目的 Terry Simons，他在 Linux 上的 802.11 以及几乎所有主要操作系统上的 802.1X supplicant 花费了不少工夫。Terry 同时也是 Utah 大学无线身份验证系统的架构师。从本书中论及安全规范以及使用申请者（supplicant）与构建身份验证系统（authentication system）的实践部分都可以感受到他的专长。

至于协助我赶上当前802.11的发展潮流以及与我分享他们所知的其他人士，我同样深表感谢。2002年起，我有幸能够参与Interop Lab无线安全性与802.1X的相关会议。与课堂相比，现实世界总是太过混乱。每年我从这些自愿参与的活动中所学习到的远比参加特定的课程来得更多。通过Interop Labs，我认识了xsupplicant项目的首席开发者Chris Hessing。Chris总是慷慨地倾囊相授，为我解释密钥如何在802.11中传递，这可没有想象中简单！我的同事Sudheer Matta总是不吝对我说明标准界发生了什么新鲜事以及MAC小组的工作记录细节。

感谢O'Reilly所提供的各式各样的协助。2001年，当我开始写作本书的第一版时，Ellie Volckhausen所设计的封面就挂在我的座位前面以及我所拥有的大部分电子设备上面。（在我的手机上看起来一样很棒！）Jessamyn Read将我成堆的速描转为可供陈列的插图，而且是在相当紧凑的期限内完成的。我不知道产品编辑Colleen Gorman花了多少时间才完成本书，希望她的家人和她的猫咪Phineas能够原谅我。如同以往，我得感谢编辑Mike Loukides所展现的智慧。Mike让整个项目保持了以往我们合作时所习惯的方式，而他所具备的业余无线电背景也在我写到天线与RF传输的相关章节时特别有帮助（还有很多很多必须感谢他的，例如有关Aricebo电波望远镜的注释）！

写作和生命中的其他事情没有两样，精华都在细节里。要保持正确，通常意味着重写、重写再重写。进学院之前，我并没有任何大型写作项目的经验，直到修了一门Brad Bateman教授所开设的美国金融体系（U.S. Financial System）课程。虽然我的确学到货币在经济系统的流通以及联邦储备系统（Federal Reserve）用以形成策略的工具，但回顾既往，我觉得最有价值的还是掌握到如何撰写结构严谨的长篇论文。除了写作，Bateman教授十分强调重写过程，在写作本书时，我不时用到这个技巧。不过，我并不只是将Bateman教授当作杰出的写作导师，或者仅止于在复杂的经济问题上为学生解惑的经济学者。Bateman教授不会受限于自己的学术专长。准备写作本书的第二版时，我参加了他的一场演讲，主题和我的母校的社会史有关。在令人神往的一个小时中，他追溯了母校的历史及其与较广泛的社会运动之间的关系，这解释了我的母校何以拥有目前的文化。如此深入的剖析远超过我当学生时所能理解的程度。并非所有教授都会考虑如何让学生为进入研究而先做准备，也不是所有教授都会将他们的教诲局限于课堂中。在他的影响之下，我学到如何成为一个更好的作家、经济学家以及公民。

写作一本书时，感谢其他人有形的贡献总是比较容易。然而在每个作家背后，都有一些默默付出的亲人与朋友。如同以往，我的妻子Ali以无比的幽默感纵容我的写作习惯，特别是为本书所牺牲的无数周末。一些朋友以各种形式的鼓励与协助支持本书的写作，为此，我必须感谢Annie、Aramazd、Brian、Dameon、Kevin以及Nick（依字母顺序排列）。

—— Matthew Gast

加州，旧金山

2005年2月

第一章

无线网络导论

在过去的5年中，整个世界逐渐走向移动化。因此，连接世界的传统方式已经无法应付新的生活方式所带来的挑战。如果非得通过实体电缆才能够连接到网络，用户的活动范围势必大幅缩小。无线网络便无此限制，用户可以享有较宽广的活动空间。因此，无线技术正逐渐侵占传统的“固定式”（fixed）或“有线式”（wired）网络所占有的领域。这种改变对每天开车的人来说分外明显，因为边开车边使用移动电话的驾驶行为，已经让他们随时都得面对攸关生死的挑战。

语音通信的无线化造就了一个全新的产业。为电话注入移动性，已经对于语音通信事业造成了深刻的影响。因为如此一来，人与人之间就可以直接联系，不必受限于设备（connected to people,not devices）。在计算机网络领域，我们面临着同样深刻的巨变。无线电话之所以如此受到欢迎，是因为人们可以丝毫不受地点的影响而相互沟通。针对计算机网络而发展出的种种新技术，让Internet连接得以提供相同的无线功能。到目前为止，802.11算是最成功的无线网络技术。

在本书的第一版中，我曾经提到802.11将是引领移动数据网络的顶尖趋势。当时，802.11正与第三代移动技术竞逐主流地位（mindshare）。毋庸置疑的是，如今看来802.11算是略胜一筹。

为何需要无线？

然而，如果我们现在就一头栽进特定技术的细节中，未免有些言之过早。不论其所使用的协议如何设计，不论其所传送的数据属于何种类型，各种无线网络之间其实具备许多共同的优点。

无线网络最明显的优点在于提供给人们移动性（mobility）。无线网络的用户可以连接至

现有网络，而后随意漫游。通过发射塔（cell tower），用户可以一边开车，一边利用手机通话。起初手机十分昂贵，价格因素使得手机用户局限在销售经理（需要高度的移动性）以及重要的决策阶层（需要随时能够联络上）。移动电话已经被证实是一项十分有用的服务，如今手机在美国已相当普及，至于欧洲就更不在话下了（注 1）。

同样地，无线数据网络（wireless data network）让软件开发人员从此不必再受Ethernet缆线的束缚，他们可以在图书馆、会议室、停车场甚至对街的咖啡馆工作。只要用户不走出基站（base station）的覆盖范围，即可使用网络资源。垂手可及的无线网络设备能够轻易覆盖整个公司，只要花些工夫，用点特殊设备，就可以让802.11网络的覆盖范围扩展至想要的地区，距离甚至可以长达数英里（1 英里 =1609 米）。

无线网络通常具备相当大的灵活性，换个说法就是部署快速。无线网络可以通过基站让用户连接到现有的网络。在802.11网络中，基站又称为接入点（access point）。然而不论有用户多少，无线网络基础建设在本质上并没有什么差异。要在某个地区提供无线网络服务，必须先将基站与天线摆放到位。一旦完成基础建设之后，要在无线网络中加入新用户就只不过是授权（authorization）之劳。虽然基础建设完工之后仍需经过配置设定的步骤才能够辨认用户身份以及提供服务，不过单就授权本身而言，并不需要新增额外的设备。要在无线网络中新增一位用户，只需设定基础设备的配置，不必拉线、打洞与配置网络插座（注 2）。

灵活性对服务供应商（service provider）而言十分重要。“hot spot”（热点）连接市场是802.11设备厂商的必争之地。班机或列车误点时，在机场与车站等候的商务人士或许会有上网的需求，咖啡馆以及其他公众聚集的社交场合亦然。有些咖啡馆已经开始提供Internet访问服务，通过无线网络访问Internet不过是现有服务的自然延伸。虽然Ethernet的插座一样能够提供访问服务，但是通过有线网络的做法也并非全然没有问题。主要是布线既贵且费时，有时甚至需要重新装潢。此外，辨别哪条线路出现问题时通常是艺术的成分大于科学。如果使用无线网络，不但可以省下装潢的工夫，也不用费神分析（或瞎猜）损坏在何处。只要基础设施的有线网络可以连上 Internet，那么不论使用人数有

注 1：虽然我在美国的大部分同事、朋友以及家人都有手机，但相形之下只能算是小儿科。在欧洲，几乎每个人都有手机。写作本书时，我在芬兰所遇到的一位出租车司机曾骄傲地对我说，他们一家四口就拥有六部手机！

注 2：此处并未考虑规模的复杂性。如果新用户的数量超出现有系统的负荷，当然必须进行系统的升级。系统扩充既贵且费时，特别是如果还需要法规核准时。不过，我的基本论点依然成立：在无线网络中新增一位用户通常会变成系统配置的设定（涉及比特的移动或改变），在固定式网络中新增一位用户就得考虑实际架线的问题（涉及原子的移动），而移动比特远比移动原子容易得多。

多少，无线网络都可以满足每个人的需求。虽然无线局域网络的带宽有限，但实际上WAN（广域网络）的带宽成本才是小型 hot spot 网络的瓶颈所在。

灵活性对老旧建筑而言特别重要，因为可以避免大兴土木。一旦建筑物被列为古迹，改建就更加困难。除了满足业主需求，改建工程还必须满足古迹维护单位的限制条件，以免破坏历史文物。无线网络在类似环境中可以快速部署，因为有线网络的安装通常只占其中一小部分。

另一方面，灵活性造就了基层小区网络（grassroots community networks）的发展。随着802.11设备价格的快速滑落，各式各样的志愿团体开始设置开放给公众使用的无线共享网络。小区无线网络也打破了DSL的限制，让以往不敢有如此奢望的小区也能够以高速访问 Internet。在传统有线网络难以企及的化外之地，小区无线网络特别成功。

802.11 早期使用概况

虽然呈现爆炸性增长，不过 802.11 并非全面均衡发展。有些市场增长较快，因为无线网络对这些市场而言特别有价值。通常，越重视移动性与灵活性的市场，对无线局域网络的兴趣就越大。

负责物流的后勤组织（如 UPS、FedEx 或者航空公司）或许是率先采用 802.11 的用户。在 802.11 之前，包裹追踪使用专属的无线局域网络。标准化使得产品价格下滑，也使得网络设备供货商彼此间的竞争激烈，因此以标准化产品取代专属产品，可说是简单不过的决定。

医疗产业也是无线网络的早期用户，因为医疗器械通常需要较大的灵活性。病患需要在医院中移来移去，而照料病患的医疗专业人员算是经济体系中最机动的一群工作者。技术先进的医疗组织早就采用无线局域网络传递病历，让医生更方便地取得病历的相关信息，有助于医疗质量的改善。计算机化的病历可以跨部门传送，人们无需再费神去解读某些传奇大夫鬼画符似的笔迹。在纷扰嘈杂的急诊室，能否快速取得图像数据有时会成为救命的关键。有些医院已经采用个人计算机，通过无线局域网络，让具有特殊配备的“急救车”（crash cart）可以实时访问 X 光片，这样医师就可以实时诊断，不必等到 X 光片显像完成。

有些教育机构对于无线局域网络十分狂热。10年前，为了吸引学生，各家学院无不吹嘘自家校园的网络如何如何。能够提供越多的高速上网的场所，就能够更吸引学生。如今，教育界的要闻是各学院已经开始在整个校园布建无线局域网络。学生通常是移动网络的重要用户，并可以受惠于课堂间或者是“第二个家”（homes away from home，如图书馆、工作室、实验室，视主修而定）中随处可用的网络。

和所有网络一样，无线网络同样是通过网络媒介传送数据。无线网络所使用的媒介属于某种形式的电磁辐射（注3）。为了满足移动网络的使用需求，此媒介必须能够覆盖较广的区域，好让用户能够在其所覆盖的范围内移动。早期的无线网络通常使用红外线(infrared light)。不过红外线本身有其限制，容易受到墙壁、隔间以及其他办公设备阻隔。无线电波可以穿透大部分办公设备，提供了较广的服务范围。因此，市面上绝大多数的802.11产品均采用无线电波作为物理层。

无线电频谱：关键资源

无线设备被限定在某个特定频带（frequency band）上操作。每个频带都有相应的带宽(bandwidth)，即该频带可供使用的频率空间总和。带宽是评断链路（link）数据传输能力的基准。种种数学、信息以及信号处理理论均可证明，较大的带宽可以传输更多的信息。举例而言，模拟移动电话信道需使用20 kHz的带宽，而电视信号比较复杂，因此需要用到6 MHz的带宽。

无线电频谱（radio spectrum）的使用受到主管当局严格控制，主要是通过核发许可证的方式。在美国，主管机关是联邦通信委员会（Federal Communications Commission，简称FCC）。美洲有些国家直接采用FCC法规。欧洲的主管机关是CEPT旗下的欧洲无线电通信局（European Radiocommunications Office，简称ERO）。至于其他地区，则由国际电信联盟（International Telecomunications Union，简称ITU）把关。为了防止重复使用无线电波，通常以频带（band）来配置频率（frequency）。所谓频带，其实就是分配给特定应用的频率范围。美国地区常用的频带列于表1-1（注4）。

表1-1：美国地区常用频带

频带	频率范围
UHF, ISM	902~928 MHz
S-频带	2~4 GHz
S-频带，ISM	2.4~2.5 GHz

注3：某些无线网络应用采用的是激光，激光束焦点十分集中，特别适合用在端点固定不动的应用场合。在“固定式无线”应用的场合中，以激光取代其他访问技术（例如电话专线）十分常见。

注4：完整的频谱分配表可自美国国家通信和信息管理局（National Telecommunications and Information Administration）下载，网址在*http://www.ntia.doc.gov/osmhome/allochrt.pdf*。

表1-1：美国地区常用频带（续）

频带	频率范围
C-频带	4~8 GHz
C-频带，卫星下行链路	3.7~4.2 GHz
C-频带，雷达（气象）	5.25~5.925 GHz
C-频带，ISM	5.725~5.875 GHz
C-频带，卫星上行链路	5.925~6.425 GHz
X-频带	8~12 GHz
X-频带，雷达（警用/气象）	8.5~10.55 GHz
Ku-频带	12~18 GHz
Ku-频带，雷达（警用）	13.4~14 GHz
	15.7~17.7 GHz

ISM频带

表1-1中，有三个标示为ISM的频带。所谓ISM，即工业（industrial）、科学（scientific）与医疗（medical）。大致而言，ISM频带是保留给工业、科学或者医疗设备使用的。微波炉是大家最熟悉的ISM设备，使用的是2.4~GHz ISM频带，因为该频段内的电磁辐射特别利有于加热含水物质。

之所以特别提到ISM，是因为只要设备符合功率限制，不需要申请许可证（license-free）即可使用这些频段。802.11和许多其他设备均使用ISM频带。常见的无绳电话（cordless phone）同样使用ISM频带。802.11b与802.11g设备使用2.4 GHz ISM频带，而802.11a设备则使用5 GHz频带。

较常见的802.11b/g设备使用ISM的S-频带。只要设备所使用的功率不高，ISM频带一般不需经过授权使用。毕竟，使用微波炉还得申请许可证并没有太大的意义。同样地，无线网络的架设与使用也无需申请许可证。

无线网络的特色

无线网络对固定式网络而言是绝佳的互补，而非取而代之的技术。就像移动电话与固定电话，无线局域网络给用户提供移动性，和固定式网络形成互补。数据的访问还是得通过服务器与数据中心的设备，不过服务器位于何处并不重要。由于服务器通常无需移动，因此可以使用固定电缆彼此相连。另一方面，无线网络在设计上必须能够涵盖较大的范

围以服务快速移动的用户。通常802.11接入点的涵盖范围不大，因此无法服务位于快速移动交通工具上的用户。

没有实体界限

传统网络安全的重点在于防护网络设备的实体安全。网络数据通常是流动于铜质电缆或光纤等事先规划好的路径上，至于网络的基础建设，则是通过坚固的实体访问控制来加以保护。设备通常被安全地锁在配线柜（wiring closet）中，用户也不会有重新设定的机会。安全性基本上来自于物理层的防护（当然有其限度）。虽然还是有可能被窃听或转接，但通过实体的访问控制，要想鬼鬼祟祟地访问网络就比较困难。

相较于一般网络，无线网络所使用的媒介更为开放。从定义上来说，无线网络所使用的媒介不像实体电缆那样有明确定义的路径，而只是经过特殊编码与调制过的无线电波链路。既然这些原本就是众所皆知的开放标准，任何对无线电技术有所了解的人均可随意发送和接受信号。只要手上拥有正确的网卡（network interface），拦劫数据本来就是轻而易举，何况这些网卡可以在任何消费性电子卖场以不到50美元购得。仔细在网络上找找，说不定花不到一半的价钱就可买到。

此外，无线电波通常会偏离原来的目的地。无线网络媒介没有明显的实体界限，何况发送端和接收端还可以使用高增益天线来延长传输距离。构建无线网络时，各位必须仔细思考如何防范未经授权的使用（unauthorized use）、流量注入（traffic injection）以及流量分析（traffic analysis）。随着无线通信协议的成熟，验证无线用户的身份与适当加密数据的工具目前已经随处可得。

动态物理媒介

有线网络一经设立，就开始变得无趣。意思是说，它是可预测的。一旦将网线拉至适当的位置，它们就日复一日做同样的事，不会有所改变。只要网络是根据规范说明书所记载的工程规则设计的，运作上就不会有什么问题。提升有线网络的容量也不是什么难事，只要将配线柜中的交换器升级即可。

相对地，无线局域网络所使用的物理媒介就比较动态。无线电波遇到物体会反射，可以穿墙，而且通常有点难以预料。无线电波可能遭遇到传播上的问题（比如多重路径干扰与死角）并因此而断线。既然所使用的媒介不可靠，无线网络就必须仔细验证所接收到的帧以防止帧漏失。802.11以肯定确认（positive acknowledgment）来应对，牺牲一些流量以确保帧的传送。

无线电链路存在着有线网络所没有的种种限制。由于无线电频谱属于相对稀少的资源，因此必须谨慎管理。要使无线电网络的速度更快有两种方式：分配更多频谱或提升链路

的编码能力，使它在单位时间内可以装载更多数据。额外分配频谱比较罕见，特别是对无照网络而言。802.11 网络将工作站的无线信道的带宽维持在 30 MHz 不变，它是以大幅改良编码的方式来提升速度。较快的编码方式可以提升速度，不过也有潜在的缺点。编码方式越快，接收器就必须分辨越细微的信号差异，因此就需要越高的信噪比(signal-to-noise ratio)。数据速率越高，工作站就越要尽可能靠近接入点。表 1-2 显示了 802.11 各种物理层标准及其速度。

表 1-2：802.11 各种物理层（PHY）标准的比较

IEEE 标准	速度	频带	附注
802.11	1 Mbps 2 Mbps	2.4 GHz	首份 PHY 标准（1997）。同时支持跳频与直接序列调制技术
802.11a	最大可到 54 Mbps	5 GHz	第二份 PHY 标准（1999），产品迟至 2000 年末才推出
802.11b	5.5 Mbps 11 Mbps	2.4 GHz	第三份 PHY 标准，不过是第二波主流产品。这是本书第一版付印时最常见的 802.11 设备，也是本书第二版完成后设备数量最多的老产品
802.11g	最大可到 54 Mbps	2.4 GHz	第四份 PHY 标准（2003）。它在 2.4 GHz 频带上采用 802.11a 的编码技术，以期达到更高的速度。它向下兼容于现有的 802.11b 网络，也是 2005 年膝上型计算机上最常见的技术

无线电本质上属于一种广播媒介。一个工作站在进行传送时，所有其他工作站只能聆听。接入点的角色有点像是以往的共享式Ethernet集线器，每个接入点的传输能力固定且必须由所有连接用户共享。要增加网络的容量，网管人员必须添加接入点，同时缩小现有接入点的覆盖范围。

安全性

许多无线网络以无线电波为媒介，这种媒介本质上就是开放且易遭拦劫的。如何适当地保护无线网络传输向来就是通信协议设计者主要考虑的。802.11本身并未纳入安全性协议。为适应无线媒介本身的不可靠性以及提供移动性，需要使用一些协议以提供帧传输确认、省电以及行动性功能。安全性的优先级相当低，早期的规范说明书所提出的协议也被证明并不适用。

无线网络必须进行身份验证，以防未经授权的用户访问。经过认证的连接操作也必须予以加密，以防止数据遭人拦截或遭未经授权用户灌注数据。本书第一版问世后，用来提供强势加密和认证的技术已经浮现，它们是本书（第二版）改版的主要组成部分。

各式各样的网络

无线网络是个热门产业。有些无线技术主要针对数据传输。蓝牙（Bluetooth）是用于在接口设备之间构建微型网络（small network）的标准，即某种形式的无线电缆（wireless wire）。业界人士大多十分熟悉有关蓝牙的种种宣传（hype），虽然在实际产品问世前蓝牙似乎就已经“阵亡”。在第一版中，我曾提到很少见到有人使用蓝牙产品，不过近来蓝牙已经相当普遍了（我现在经常使用蓝牙耳机）。

第2.5代（2.5G）与第三代（3G）移动电话网络也是大家所熟悉的无线技术。它们承诺可以在每个蜂窝中（cell）提供兆位（megabit）的数据传输率，以及提供获得DSL与cable modem客户高度评价的随时连接（always on）服务。经过3G设备厂商这几年的宣传与推动，3G商用服务终于开始进行。2.5G服务，像GPRS，EDGE以及1xRTT，如今已经相当普遍，采用UMTS或EV-DO的第三代网络也即将问世。（为了通勤时能够在火车上上网，我最近才申请无限的GPRS服务。）有些文章引用这些技术的峰值，以为它们可以达到每秒数百千位甚至兆位，其实这些带宽必须由蜂窝的所有用户共享。实际的下行速度大概相当于调制解调器拨号，无法与802.11的hot spot相提并论。

本书的主题是802.11网络。802.11有不少称谓，根据谈论它的人不同，会有不同的名字。有人称802.11为无线以太网（*wireless Ethernet*），强调其与传统有线以太网（802.3）之间的血缘关系。本书第一版问世之后，突然爆红的一种称谓是*Wi-Fi*。Wi-Fi是Wi-Fi联盟所推广的互用性认证计划。至于Wi-Fi联盟，乃是由802.11设备厂商所组成的主要商业组织。Wi-Fi联盟的前身称为无线以太网兼容性联盟（Wireless Ethernet Compatibility Alliance，简称WECA），负责检测会员的产品是否与802.11标准兼容（注5）。执行兼容性测试的尚有其他组织，例如New Hampshire大学的互用性实验室（InterOperability Lab，简称IOL）最近就推出了一个无线测试联盟。

标准的好处

有许多标准团体参与了802.11相关标准的制定过程，因为802.11跨越了许多网络中原来明显的界限。大部分的任务还是落在IEEE身上，不过实际对无线局域网标准做出重要贡献的有以下几个主要单位。

首先是电气和电子工程师协会（IEEE）。除了专业社团活动，IEEE也制定电子设备的标准，包括各种不同的通信技术。IEEE制定标准时是以项目进行的，每个项目均以编号代表。到目前为止，最著名的IEEE项目就是负责开发局域网标准的802项目。每个项目

注5：关于Wi-Fi联盟及其认证方案的细节详见*http://www.wi-fi.org/*。

还会另外划分为许多工作组（working group），负责解决某个特定方面问题的标准。工作组同样会被赋予一个编号，位于项目编号的点号之后。举例而言，使用最广泛的IEEE LAN技术 Ethernet 就是由第3个工作组802.3负责标准化的。Wireless LAN 则是由第11个工作组负责，因此称为802.11。

每个工作组又会另外细分出许多任务组（task group），来修订标准的特定方面或另外添加到功能性的通用领域，它们以英文字母表示（有些英文字母不容易区别，例如小写的“l”，则不予使用）。在无线网络领域，第一个广为人知的是任务组B（TGb），负责制定802.11b规范说明书。表1-3列出了一些比较基本的802.11标准。

注意： 值得注意的是，标准所使用的英文字母的大小写也有不同的意义。小写英文字母代表非独立的标准，它无法脱离母标准而独自存在；至于大写字母则代表完全独立的规范。

802.11b在802.11中增加新的条款，但无法独自存在，因此使用小写的“b”表示。相对地，像是802.11Q与802.1X等标准，本身就是独立完整的规范说明书，因此使用大写的英文字母表示。

每隔一段时间，这些非独立的任务组所做的增补就会被汇整到主要的母规范说明书里。802.11的首度改版发布于1997年。针对文字所做的一些细微修改发布为802.11-1999，过去很长的一段时间都是以它为依据。最近的一次修订为802.11-2003。

表1-3：各种802.11标准

IEEE 标准	附注
802.11	首份物理层标准（1997）。制定MAC以及原本速度较慢的跳频与直接序列调制技术
802.11a	第二份物理层标准（1999）。产品迟至2000年底才推出
802.11b	第三份物理层标准（1999），不过是第二波主流产品。本书第一版撰写时最常见的802.11设备
TGc	负责更正802.11a编码范例的任务组。既然只是更正标准，因此并没有所谓的802.11c
802.11d	扩展跳频物理层的功能，使之能在不同的管制区域（regulatory domains）中使用
TGe（未来的802.11e）	为MAC制定服务质量（quality-of-service，简称QoS）扩展功能的任务组。在标准完成之前，将会先制定出称为Wi-Fi多媒体（Wi-Fi Multi-Media，简称WMM）的过渡性版本
802.11F	改善接入点间漫游功能的接入点内部协议(Inter-access point protocol)

表1-3：各种802.11标准（续）

IEEE标准	附注
802.11g	最近才标准化（2003），用于使用ISM频带的物理层
802.11h	使802.11a符合欧洲无线电发射管制的标准。其他管制者也以此机制作为不同用途
802.11i	改善链路层的安全性
802.11j	修改802.11a，使之符合日本无线电波管制的标准
TGk（未来的802.11k）	改善客户端与网络间的通信，使无线电波稀有资源的管理与运用更有效率
TGm	负责将802.11a、802.11b、802.11d以及TGc所做的变动整合至802.11主规范说明书的任务组中。可将“m”想成maintenance（维护）
TGn（未来的802.11n）	为了制定高速传输（high-throughput）标准所成立的任务组。它的设计目标是超越100 Mbps的吞吐量。未来的标准将称为802.11n
TGp（未来的802.11p）	负责让802.11适用于汽车环境的任务组。一开始的用途可能是作为电子收费的标准协议
TGr（未来的802.11r）	加强漫游（roaming）的性能
TGs（未来的802.11s）	负责让802.11适用于网状网络技术（mesh networking technology）的任务组
TGT（未来的802.11T）	负责为802.11设计测试与测量标准的任务组。因为这是一份独立的标准，因此以大写字母表示
Tgu（未来的802.11u）	负责让802.11与其他不同网络技术互通的任务组

当无线网络的认证显然已经出现基本破绽时，IEEE采用了一些最初开发自IETF的身份验证标准。Wireless LAN的身份验证相当依赖由IETF所制定的协议。

Wi-Fi联盟是由贸易协会、测试机构以及标准制定机构所组成的。它主要扮演贸易协会的角色，服务它的会员，不过它也以Wi-Fi认证而广为人知。接受Wi-Fi认证的产品会与一些大厂的产品测试互用性，通过测试的产品即有权使用Wi-Fi标记。

Wi-Fi联盟在标准化方面所做的努力主要是为了支持IEEE。当无线网络的安全开始受到质疑时，Wi-Fi联盟出面制定了一项过渡的安全规范，称为Wi-Fi保护访问（Wi-Fi Protected Access，简称WPA）。WPA基本上是IEEE安全任务组的阶段性工作成果。它比较像是一种营销性而非技术性的标准，毕竟技术面是由IEEE所主导开发的。不过，在安全的无线局域网解决方案的开发过程中，它扮演了一种推手的角色。

第二章

802.11 网络概论

凡事若能综观形势（lay of the land），通常有助于进一步探究细节。研究网络相关议题时，导论性的基本介绍通常在所难免，因为所使用的缩略术语（acronyms）可能不在少数。不幸的是，802.11所使用的缩略术语数量创下历来新高，因此披树见林的介绍也就更加重要了。要深入了解802.11，各位必须习惯这些晦涩的专有名词以及一系列由三个字母所组成的缩略术语。本章是连贯整本书的粘合剂。阅读本章，不仅能初步认识802.11与一些重要的概念，也可以了解通信协议背后的设计原理以及它们如何提供类似Ethernet的使用经验。之后，各位大可根据自身的兴趣与需要，深入探究低层协议的细节或者直接跳至实际网络部署的相关章节。

本导览之所以重要，部分是因为在此所介绍的缩略术语散见全书各处。就802.11而言，本章还肩负其他更重要的任务。802.11与Ethernet十分类似，熟悉Ethernet的来龙去脉虽然有助于理解802.11，不过要了解802.11如何将传统Ethernet技术应用到无线领域，还需要具备一些其他的背景知识。为了弥补有线网络与802.11无线网络媒介间的差距，必须另外加入一些管理功能。802.11的核心本质上属于一种善意的谎言（a white lie），这关系到媒介访问控制（media access control，简称MAC）的真实含义。每张无线网络接口卡均会被赋予一个48位的MAC地址，看起来与Ethernet网络接口卡没有两样。事实上，指派给802.11网卡的MAC地址来自同一个地址池（address pool），因此就算与有线Ethernet工作站部署在同一网络，也必然具备独一无二的地址。

对外部的网络设备而言，这些MAC地址看起来是固定的，与其他IEEE 802网络没有什么差别。如同Ethernet地址，802.11的MAC地址一样会出现在ARP列表中，使用相同的厂商名称前缀（vendor prefix），两者根本无从区分。熟知内情的802.11网络设备（接入点与其他802.11设备）知道的更多。802.11与Ethernet设备之间存在许多差异，最明

显的莫过于802.11设备具备移动性，它们可以轻易在不同网络区段间自由移动。802.11设备对此了然于胸，因此能够根据移动式工作站的当前位置传送帧（frame）。

IEEE 802 网络技术族谱

IEEE 802家族是由一系列局域网（local area network，简称LAN）技术规范所组成的，802.11是其中的成员之一。从图2-1可看出802家族成员间的关系以及它们在OSI模型中的角色定位。

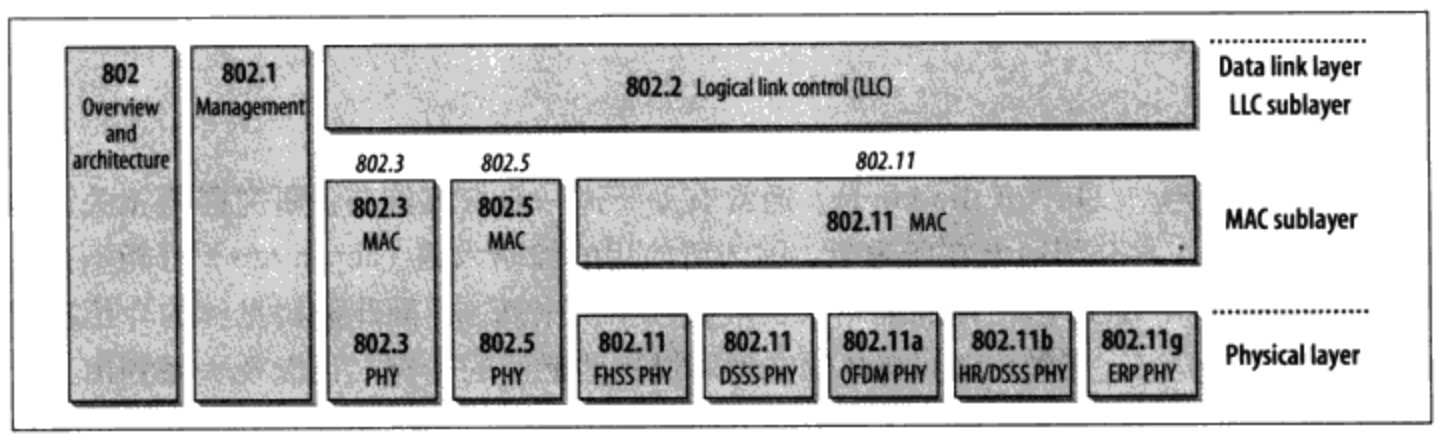


图2-1：IEEE 802家族及其与OSI模型的关系

IEEE 802规范的重心放在OSI模型最下面的两层，因为它们同时涵盖了物理（physical，简称PHY）与数据链路（data link）组件。只要是802网络，就必然会同时具备MAC与PHY两种组件。MAC是一组用以决定如何访问媒介与传送数据的规则，至于传送与接收的细节则交由PHY负责。

802系列中的个别规范是由点号后的一位数定义的。例如，802.3是载波监听多路访问/冲突检测(Carrier Sense Multiple Access network with Collision Detection，简称CSMA/CD）规范，与（通常误称的）Ethernet有关，802.5则是Token Ring规范。此外，802协议堆栈还包括其他成员。802.2所规范的链路层（link layer）称为逻辑链路控制层(Logical Link Control，简称LLC)，可供所有底层局域网技术使用。802网络的管理功能规范于802.1中。而802.1的范围涵盖桥接（802.1D）以及虚拟局域网（802.1Q）。

说穿了，802.11只不过是另一种可以利用802.2/LLC封装（encapsulation）的链路层。802.11基本规范涵盖了802.11MAC以及两种物理层（physical layer）：一种是跳频扩频(frequency-hopping spread-spectrum，简称FHSS）物理层，另一种是直接序列扩频(direct-sequence spread-spectrum，简称DSSS）物理层。后来改版时，802.11陆续加入了其他不同的物理层。802.11b规范了高速直接序列扩频（HR/DSSS）物理层。基于802.11b的产品在1999年问世，是第一款于大众市场销售的物理层。802.11a所规范的

物理层主要是以正交频分复用（orthogonal frequency division multiplexing，简称OFDM）技术为基础。基于802.11a的产品在本书第一版完成之际已经开始发布。802.11g是目前最新开发的物理层，它采用OFDM以便提升连接速度，但同时也能够向下兼容于802.11b。不过，向下兼容是需要付出代价的。如果802.11b与802.11g的用户同时访问同一个接入点，将需要用到额外的协议，因此会拖累802.11g用户的连接速度。

“802.11只不过是802.2的另一种链路层”这种说法，其实抹杀了本书其他部分所交代的细节。然而，这些细节正是802.11之所以动人之处。802.11允许在移动时访问网络，为此，802.11在MAC中加入了许多额外的功能。因此，相较于IEEE 802 MAC规范，802.11 MAC有若巴洛克风格一般繁杂。

以无线电波（radio wave）为物理层还需要比较复杂的PHY。802.11将PHY进一步划分为两个一般组件：一个是物理层会聚过程（Physical Layer Convergence Procedure，简称PLCP），负责将MAC帧映射到传输媒介；另一个是物理媒体相关（Physical Medium Dependent，简称PMD），负责传送这些帧。PLCP横跨MAC与物理层，如图2-2所示。在802.11网络中，PLCP将帧传至空中之前，会在其中加入一些字段。

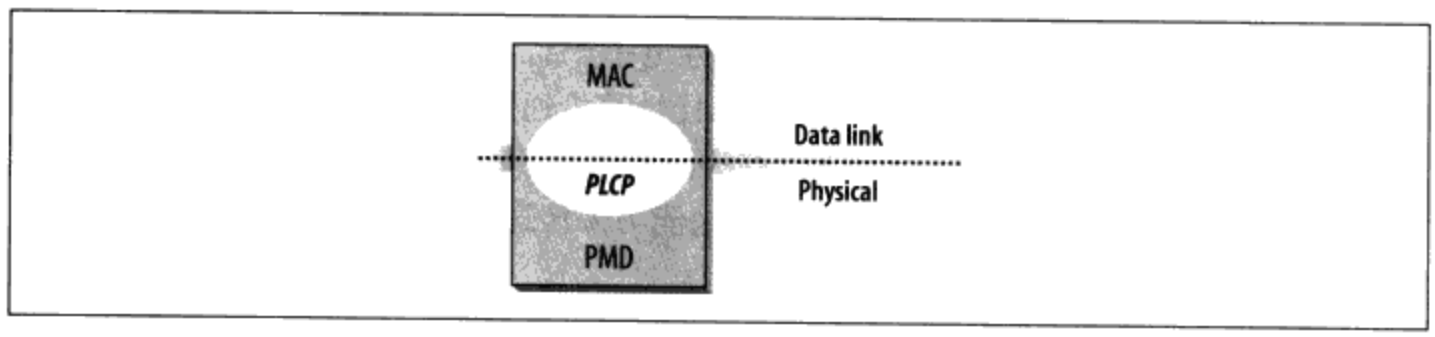


图2-2：PHY组件

凡这种种，不免让人有“知也无涯，何为止境”之问。不过知道得越多，必然更游刃有余，任何技术都是。虽然802.11协议中可供调校之处（knobs and dials）颇多，但为了降低复杂度，实际产品大多刻意加以隐藏。只有在网络拥堵时，例如流量异常或用户过多，这些功能的用处才会被突显出来。时至今日，网络在上述两方面已经几乎濒临极限。各位或许想要跳过与协议有关的章节，直接了解如何规划与构建802.11网络，对此我不能苛责。读完本章之后，各位可以直接跳至第十七至二十三章，等到需要（或想要）进一步了解这些协议的内部运作时再回过头来阅读这些章节也成。

802.11 相关术语及其设计

802.11网络包含四种主要物理组件，如图2-3所示。

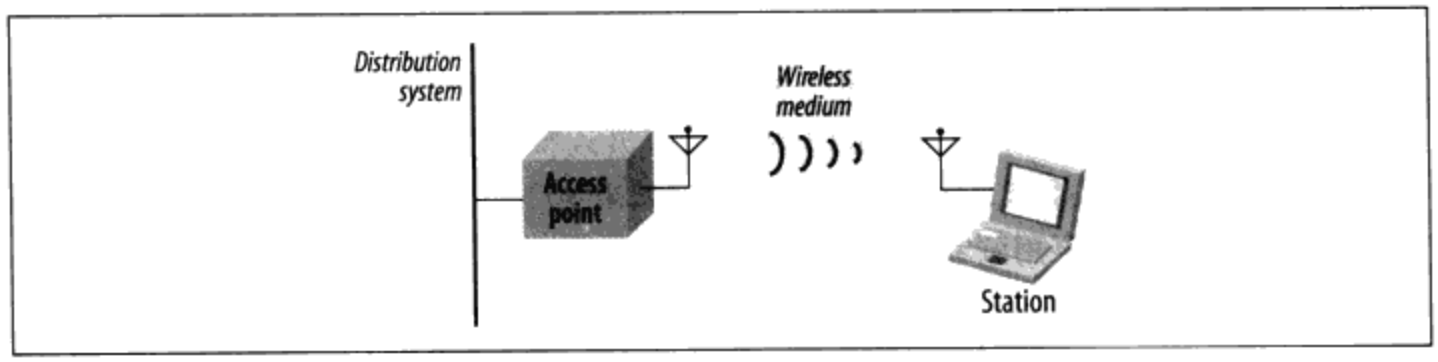


图2-3：802.11 LAN的组件

这些组件包括：

工作站（Station）

构建网络的目的是为了在工作站间传送数据。所谓的工作站（station），是指配备无线网络接口的计算设备。通常，工作站是以电池供电的膝上型（laptop）或手持式（handheld）计算机。然而，工作站不见得就是便携式（portable）计算设备。有时候，使用无线网络的目的是为了省去拉线的麻烦，桌上型（desktop）计算机一样可以使用无线局域网。较宽广的开放空间也可以受惠于无线网络，例如生产线可以使用无线局域网来相互连接。在消费性电子产品方面，802.11也快速成为一种连接标准。Apple的AirPort Express可以让计算机通过802.11与音响连接。TiVo数字录像机也可以连接到无线网络。有些消费性电子产品厂商已经加入802.11工作组，显然是为了借助802.11的高速传输能力来传送多媒体数据。

接入点（Access Point）

802.11网络所使用的帧必须经过转换，方能被传递至其他不同类型的网络。具备无线至有线（wireless-to-wired）的桥接功能的设备称为接入点（access point，简称AP），接入点的功能不仅于此，但桥接（bridging）最为重要。起初，厂商倾向于将接入点的所有功能置于单一设备中，不过一些较新的产品则是将802.11协议分割为两部分："精简型"接入点（thin AP）与接入点控制器（AP controller）。

无线媒介（Wireless medium）

802.11标准以无线媒介（wireless medium）在工作站之间传递帧。其所定义的物理层不只是一种，这种架构允许多种物理层同时支持802.11MAC。802.11最初标准化了两种射频（radio frequency，简称RF）物理层以及一种红外线（infrared）物理层，然而事后证明RF物理层较受欢迎。此外，一些其他的射频物理层也已经标准化了。

分布式系统（Distribution system）

当几个接入点串联以覆盖较大区域时，彼此之间必须相互通信以掌握移动式工作站的行踪。分布式系统（distribution system）属于802.11的逻辑组件，负责将帧

(frame) 转送至目的地。802.11并未规范分布式系统的技术细节。大多数商用产品是以桥接引擎 (bridging engine) 和分布式系统媒介 (distribution system medium) 共同组成分布式系统。分布式系统是接入点间转发帧的骨干网络，因此通常就称为骨干网络 (*backbone network*)。所有在商业上获得成功的产品几乎都是以Ethernet为骨干网络。

网络类型

基本服务集 (*basic service set*，简称BSS) 是802.11网络的基本组件 (building block)，由一组相互通信的工作站所构成。工作站之间的通信在某个模糊地带进行着，称为基本服务区域 (*basic service area*)，此区域受限于所使用的无线媒介的传播特性 (注 1)。只要位于基本服务区域，工作站就可以跟同一个BSS的其他成员通信。BSS分为两种，如图 2-4 所示。

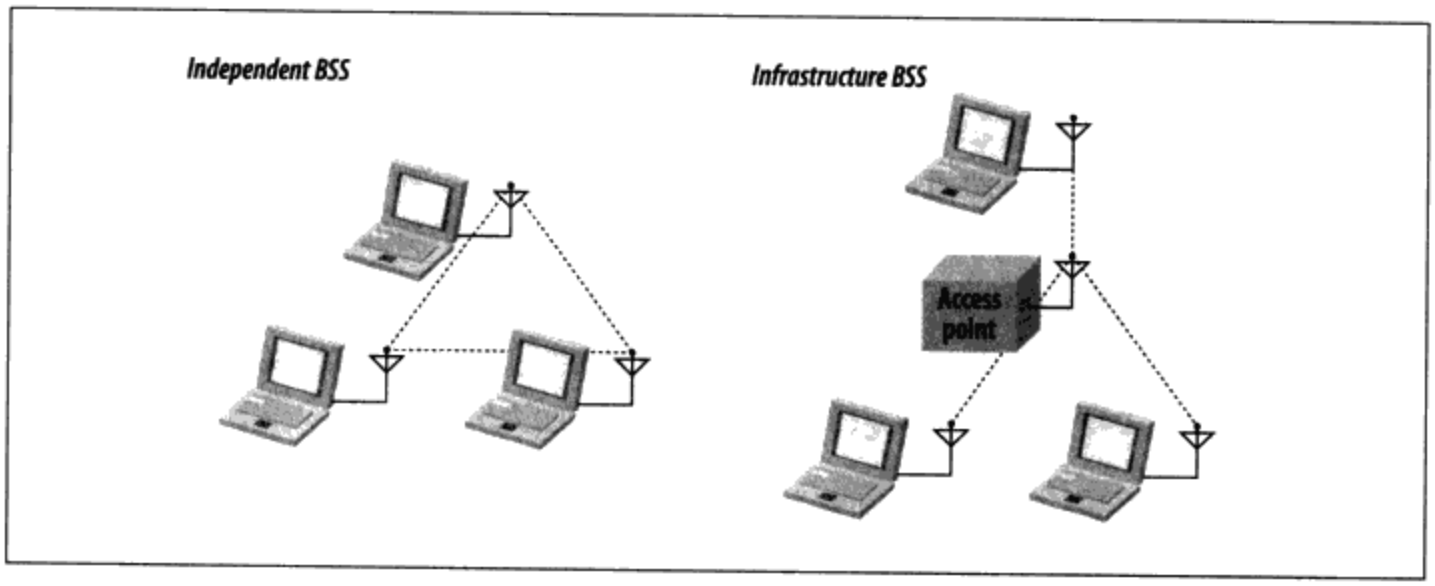


图2-4：独立型与基础结构型网络的基本服务集

独立型网络

图 2-4 的左边为独立基本服务集 (independent BSS，简称IBSS)。在IBSS中，工作站相互之间可以直接通信，但两者间的距离必须在可以直接通信的范围内。最低限度的802.11网络是由两个工作站所组成的IBSS。通常，IBSS是由少数几个工作站为了特定目的而组成的暂时性网络。一种常见的情况是在会议室中支持个别会议之用。会议一开

注 1：任何无线媒介都是在三维空间中传播。从这个观点来看，服务区域 (service area) 或许应该称为服务空间 (service volume)。不过，“区域” (area) 这个词已广为使用与接受。

始，与会人员相互会形成一个IBSS以便传递数据；当会议结束，IBSS随即瓦解（注2）。正因为持续时间不长、规模甚小且目的特殊，IBSS 有时被称为特设BSS（*ad hoc BSS*）或特设网络（*ad hoc network*）（译注1）。

基础结构型网络

图2-4中右侧为基础结构型基本服务集（为了避免混淆，不可将*infrastructure BSS*简称为IBSS）。判断是否为基础结构型网络，只要查看是否有接入点参与其中即可。接入点负责基础结构型网络所有的通信，包括同一服务区域中所有移动节点之间的通信。位于基础结构型基本服务集中的移动式工作站如有必要跟其他移动式工作站通信，必须经过两个步骤。首先，由初始对话的工作站将帧传递给接入点。其次，由接入点将此帧转送至目的地。既然所有通信都必须通过接入点，基础结构型网络所对应的基本服务区域就相当于接入点的传送范围。虽然这种做法比直接传送耗费较多的资源，不过它有两个主要的优点：

- 基础结构型基本服务集被界定在接入点的传输范围内。所有移动式工作站都必须位于接入点的传输范围之内，不过移动式工作站之间的距离则无限制。允许移动式工作站彼此直接通信虽然可以省下一些带宽，不过代价是相对提高了物理层的复杂度，因为每个工作站都必须维持与服务区域中其他工作站的邻接关系。
- 接入点在基础结构型网络里的作用是协助工作站节省电力。接入点可以记住有哪些工作站处于省电状态并且为之暂存帧。以电池供电的工作站可以关闭无线收发器，只有在传输或接收来自接入点的暂存帧时才会加以开启。

在基础结构型网络里，工作站必须先与接入点建立关联（associate），才能取得网络服务。所谓关联，是指移动式工作站加入某个802.11网络的过程。逻辑上，这相当于在Ethernet插上网线。整个过程并不对称，因为开启连接过程的必然是移动式工作站，接入点只是基于关联请求的内容，判定是否准许该工作站访问网络。对移动式工作站而言，关联必须独一无二：每个移动式工作站同一时间内只能与一个接入点连接（注3）。802.11标准并未限制接入点可服务的移动式工作站的数量。当然，实现上还是必须加以限制。不过，实际上无线网络的吞吐量相对较低，很少需要予以限制。

注2： IBSS在LAN方面也有类似的用法。

译注1： “ad hoc”系拉丁文，原意是“特别的”、“针对特殊情况的”，由于ad hoc网络的点对点（peer-to-peer）性质，亦称为点对点网络。

注3： 有位审稿者提到，在VLAN发展之前，传统Ethernet网络也有类似的限制。他问这种限制还会持续多久。我并未参与标准化的工作，因此无法直接回答这个问题。不过，我同意这是个值得注意的问题。

扩展服务区域

BSS的服务范围可以涵盖整个小型办公室或家庭，不过无法服务较广的区域。802.11允许我们将几个BSS串联为扩展服务集（*extended service set*，简称ESS），借此扩展无线网络的覆盖区域。所谓ESS，就是利用骨干网络将几个BSS串联在一起。所有位于同一个ESS的接入点将会使用相同的服务组标识符（*service set identifier*，简称SSID），通常就是用户所谓的网络“名称”。

802.11并未规定非得使用何种骨干技术，只要求骨干必须提供一组特定的服务功能。图2-5所示的ESS是四个BSS的联合（只要所有接入点均隶属同一个ESS）。实际部署时，BSS之间的重叠程度可能较图2-5更高。在实际生活中，总是希望扩展服务区域是连续的，不可能要求用户从BSS1走到BSS2时还要绕道BSS3。

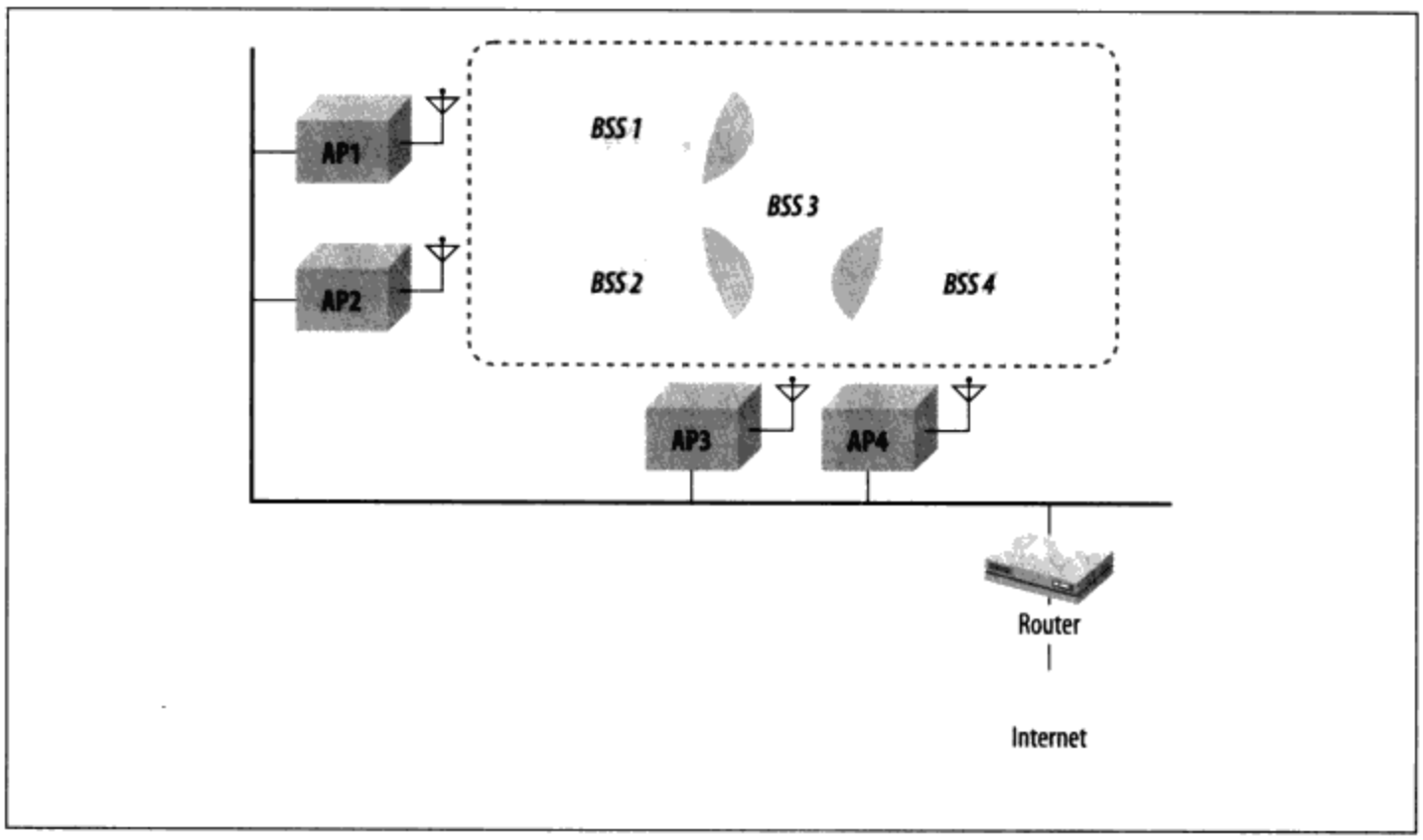


图 2-5：扩展服务集

隶属同一个ESS的工作站可以相互通信，即使这些工作站位于不同的基本服务区域或是在这些基本服务区域中移动。为了让ESS里的工作站能够相互通信，无线媒介必须能够在第二层（链路层）进行连接。由于接入点扮演着桥接器的角色，因此ESS里的工作站若要相互通信，则骨干网络也必须能够在第二层进行连接。第一代接入点必须通过集线器（hub）或者虚拟局域网（virtual LAN）才能与第二层直接连接，不过，较新型的产品当中通常已经内置了某种隧道（tunneling）技术，可以模拟出第二层的连接环境。

注意： 802.11 为ESS提供了链路层漫游（link-layer mobility）的功能，不过骨干网络必须是单一链路层网域。这项重要的限制通常是部署无线局域网时的主要考虑因素，也是厂商间区分产品的主要方式。

早期的接入点必须通过同一集线器或虚拟局域网访问骨干网络，不过较新型的产品可以直接与骨干连接。有些新产品可以通过 802.1Q 标记（tag）同时支持多组 VLAN，而且可以根据身份验证信息来动态建立虚拟局域网。

扩展服务区域是802.11 网络所支持的最高级抽象概念。ESS 所属的接入点会相互合作，让外界能够使用单一 MAC 地址与ESS 里的其他工作站通信，不论其置身何处。在图2-5中，路由器可使用单一MAC地址传递帧给移动式工作站，由该工作站所关联的接入点负责传送帧。路由器无需在意移动式工作站位于何处，而是靠接入点传送帧。

多组 BSS 所构成的环境：虚拟 AP

早期的802.11 芯片只能够创建单一BSS（基本服务集）。而单一 AP（接入点）只能为用户提供一个“无线网络”，而且该网络上所有用户的权限如果并非完全相同，但也相去不远。在早期用户寥寥可数的环境里，单一逻辑网络可能就已足够。不过当无线网络逐渐普及，单一网络开始不够用了。

举例而言，各机构会有固定的访客，其中许多人手上就有802.11 设备，而且需要（或者强烈想要）与因特网连接。这些访客并非可信的用户。通常为了满足这些访客的上网需求，将会在相同的实体设施上另辟两个扩展服务集。目前的802.11芯片组已经可以使用相同的物理层来创建多组网络。以当前的芯片组而言，每个接入点的硬件设备可以创建两组 BSS，其中一组可供客户访问，称之为 *guest*；另外一组则供内部使用，称之为 *internal*。在此 AP 当中，各 SSID 被分别关联至不同的VLAN。guest 网络会被连接至不知名或为不可信用户所准备的 VLAN，而且被置于防火墙外。

于无线电领域内，无线设备将会发现两组不同的网络，然后依其所需连接至合适的网络（当然，要访问内部网络必须经过身份验证，以防止未经授权人士使用）。连接至 *guest* 网络的用户会被引导至访客所使用的VLAN，而连接至 *internal* 网络的用户则必须经过身份验证，然后被引导至内部网络。

上述虚构的例子说明了虚拟接入点的发展情况。每个 BSS 就像一个自给自足的 AP，拥有自己的 ESSID、MAC 地址、身份验证配置以及加密设定。虚拟接入点也可以用来创建具有不同安全等级（security level）的并行网络（parallel network），对此，第二十二章将会有深入的讨论。目前，802.11 芯片组最多可以创建 32 组甚至 64 组 BSS，对各种情况而言应该都已经够用了。

强健安全网络（Robust Security Network）

早期无线局域网内置的安全机制已被证明是不堪一击。2004 年 6 月成为标准的 802.11i 规范了一组经改良的安全机制，目的是提供强健且安全的网络关联。一旦使用 802.11i 所定义的、经改良的身份验证与机密性协议，就可称之为强健安全网络关联（*robust security network associations*，简称 RSNA）。产品可以通过硬件、软件或软硬件兼具的方式支持802.11i，这取决于该设备所使用的架构。不支持此协议的硬件被归类为*pre-RSN*。有些pre-RSN设备可以通过升级的方式来支持 802.11i，不过大多数较旧的设备是无法升级的。

再论分布式系统

既然读者已经了解如何构建扩展服务集，我打算回过头来重新查看分布式系统这个概念。802.11是以能给无线工作站提供哪些服务来描述分布式系统。虽然本章稍后即将深入探讨这些服务，不过现在仍值得我们从较高层次的来查看其运作方式。分布式系统可借由串联接入点来提供移动性（mobility）。当帧被传送至分布式系统后，随即会被送至正确的接入点，而后由接入点转送至目的地。

分布式系统必须负责追踪工作站实际的位置以及帧的传送。若要传送帧给某个移动式工作站，分布式系统必须负责将之传递给服务该移动式工作站的接入点。以图 2-5 的路由器为例，该路由器仅会以某移动式工作站的MAC为目的地地址。如图2-5所示，ESS的分布式系统必须负责将帧传递给正确的接入点。显然，有部分传递机制属于Ethernet所构成的骨干网络，不过该骨干网络并不代表整个分布式系统，因为它无法在多个接入点间作出选择。以 802.11 的语言来讲，Ethernet 所构成的骨干网络是个分布式系统媒介，并非分布式系统的全部。

要找出分布式系统的其他成分，我们必须查看接入点本身。目前市面上的大部分接入点都是扮演桥接器的角色。这些接入点至少具备一个无线网络接口以及一个Ethernet网络接口。Ethernet网络接口可用来连接现有的网络，而无线网络接口则成为该网络的扩展。这两种网络媒介之间的帧转送是由桥接引擎加以控制。

接入点、骨干网络以及分布式系统之间的关系如图 2-6 所示。接入点具备两种不同的接口，分别连接至同一个桥接引擎。图中的箭头代表往返桥接引擎的可能路径。帧将会通过桥接器被送至无线网络，任何由桥接器的无线端口所送出的帧都会传给所有已关联的工作站。每个已关联的工作站均可传递帧至接入点。最后，桥接器的骨干端口可以直接与骨干网络交互。在图 2-6 中，分布式系统是由桥接引擎及有线骨干网络所组成的。

在基础结构型网络里，移动式工作站所送出的每个帧都必须用到分布式系统。这并不难

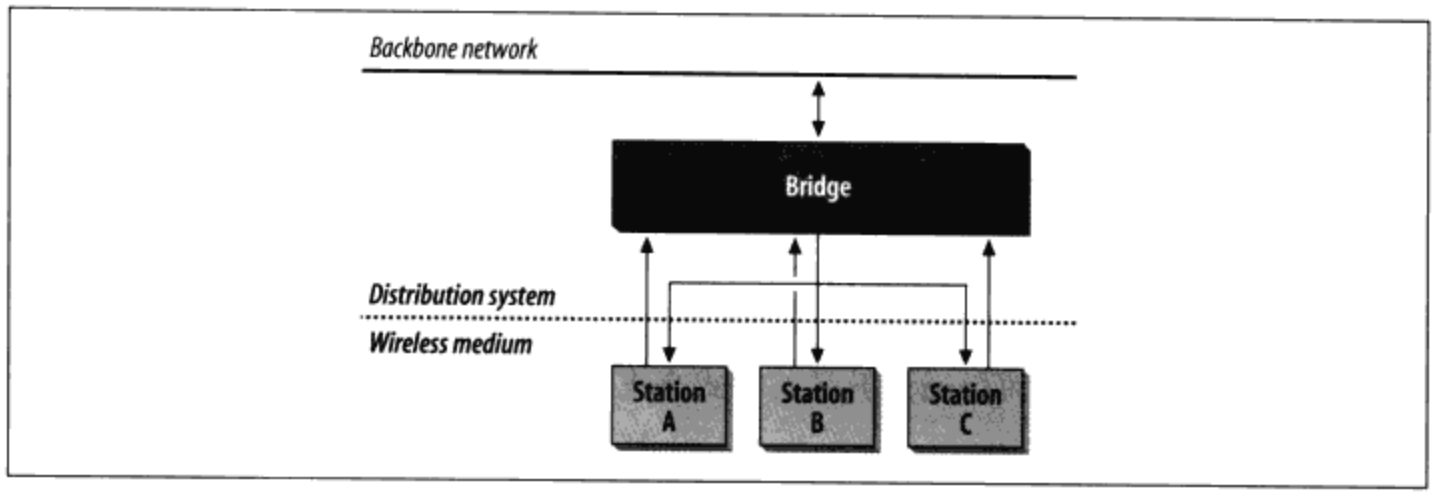


图 2-6：在普通 802.11 接入点实现中常见的分布式系统

理解，毕竟每个工作站都必须连接至分布式系统。无线工作站在基础结构型网络里必须依赖分布式系统才能相互通信，因为它们无法直接连接。工作站 A 要传送帧给工作站 B 的唯一方式是通过接入点里桥接引擎的转发（relay）。不过桥接器本身属于分布式系统的组件。虽然分布式系统所使用的是哪些组件似乎纯粹是技术上的考虑，但实际上 802.11 MAC 里某些功能与分布式系统有十分密切的关系。

接入点间的通信是分布式系统的一部分

分布式系统包含了管理关联的方式。一个无线工作站在同一时间内只能与一个接入点关联。如果某工作站已经与某接入点关联，位于同一个ESS的其他接入点必须能够得知此工作站。如图 2-5 所示，AP4 必须得知所有与 AP1 关联的工作站。如果一个与 AP4 关联的无线工作站送出帧给一个与 AP1 关联的工作站，那么 AP4 的桥接引擎必须通过 Ethernet 所构成的骨干网络将此帧送给 AP1，如此 AP1 才能够将之传递至最终目的地。要实现整个分布式系统，接入点必须通知其他工作站所关联的接入点。当然，市面上有许多接入点会在骨干媒介中采用接入点内部协议（inter-access point protocol，简称 IAPP）。有些厂商自行开发专属协议，以便在接入点间传递关联数据。目前所制定的 IAPP 标准称为 802.11F，不过还没听说有哪些产品已经实际采用它。

无线桥接器与分布式系统

到目前为止，我都假设分布式统媒介就是现有的固定式网络。虽然情况通常是如此，但 802.11 规范明确提到过，无线媒介本身也可以作为分布式系统。这种无线分布式系统（*wireless distribution system*，简称 WDS）的配置通常称为“无线桥接器”（wireless bridge）配置，因为它允许网络工程师在链路层连接两个局域网。无线桥接器可用来快速连接不同的实体网段，十分适合接入供应商（access provider）使用。市面上大部分的 802.11 接入点均支持无线桥接功能，不过有些较旧的机型可能必须更新固件。

网络界限

由于无线媒介的性质，802.11 网络的界限（boundary）可以说是相当模糊。事实上，某种程度的模糊是必要的。和移动电话网络一样，允许基本服务区域相互重叠，不仅可让工作站与基本服务区域之间的转换的成功机率提高，也可以提供最高层次的网络覆盖。图 2-7 右边的基本服务区域相互重叠得十分明显。这意味着，当工作站从 BSS2 移动至 BSS4 时不会失去信号；这同时也意味着，就算 AP3（或者 AP4）失灵，也不致于使整个网络瘫痪。另一方面，如果 AP2 出现故障，则整个网络就会被分割为两个彼此隔开的区域，位于 BSS1 的工作站只要离开 BSS1 所涵盖的范围而进入 BSS3 或 BSS4，就会失去与 BSS1 的连接。如何填补这些“覆盖盲区”（coverage holes）以避免网络瘫痪乃是网络设计阶段必须注意的事项。有些新产品提供动态电波调整功能，可以在实际运作时自动填补接入点间的覆盖盲区。

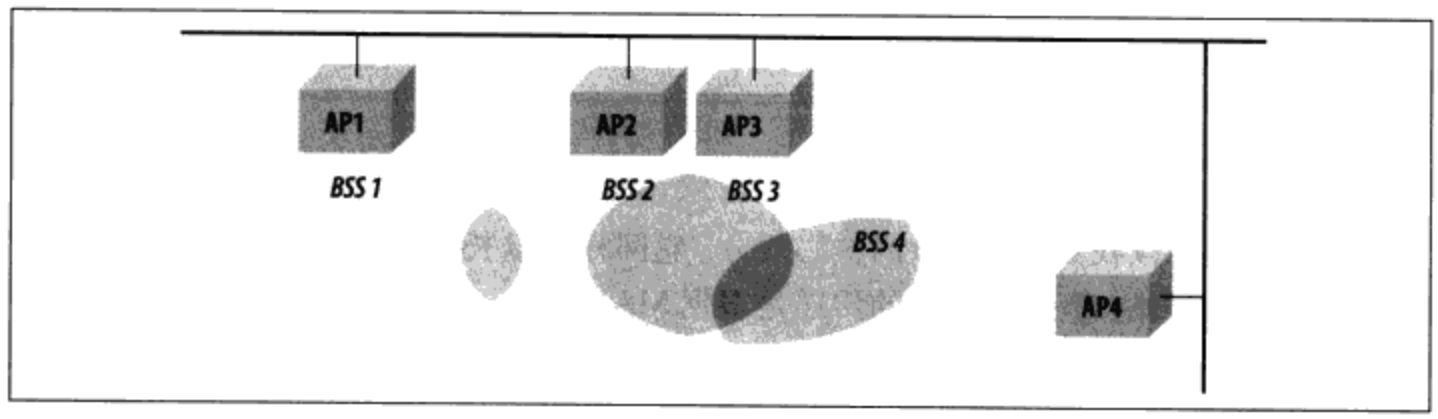


图 2-7：ESS 中相互重叠的 BSS

不同类型的802.11网络亦可相互重叠。在接入点所涵盖的基本服务区域中也可以另辟独立型 BSS。图 2-8 显示了这两者在空间上的重叠。一个接入点位于图 2-8 的上方，其基本服务区域以阴影表示。两个工作站以基础结构模式运作，通过接入点相互通信。三个工作站设定为独立型BSS，彼此间可以直接通信。虽然这五个工作站被指派至两个不同的BSS，但它们所使用的还是相同的无线媒介。工作站只有通过 802.11 MAC 所规范的规则才能够访问媒介。这些规则在设计上就已考虑到如何能够让多个802.11网络并存于相同的空间中。这两个BSS必须共享单一无线信道的带宽，因此共存的BSS之间必然会有性能上的抵消。

802.11 网络的运作方式

802.11在设计之初就是作为较上层协议的另一个链路层。熟悉Ethernet的网管人员应该马上就可适应 802.11。802.11 网络与 Ethernet 的渊源之深，有时它甚至被称为“无线 Ethernet”。

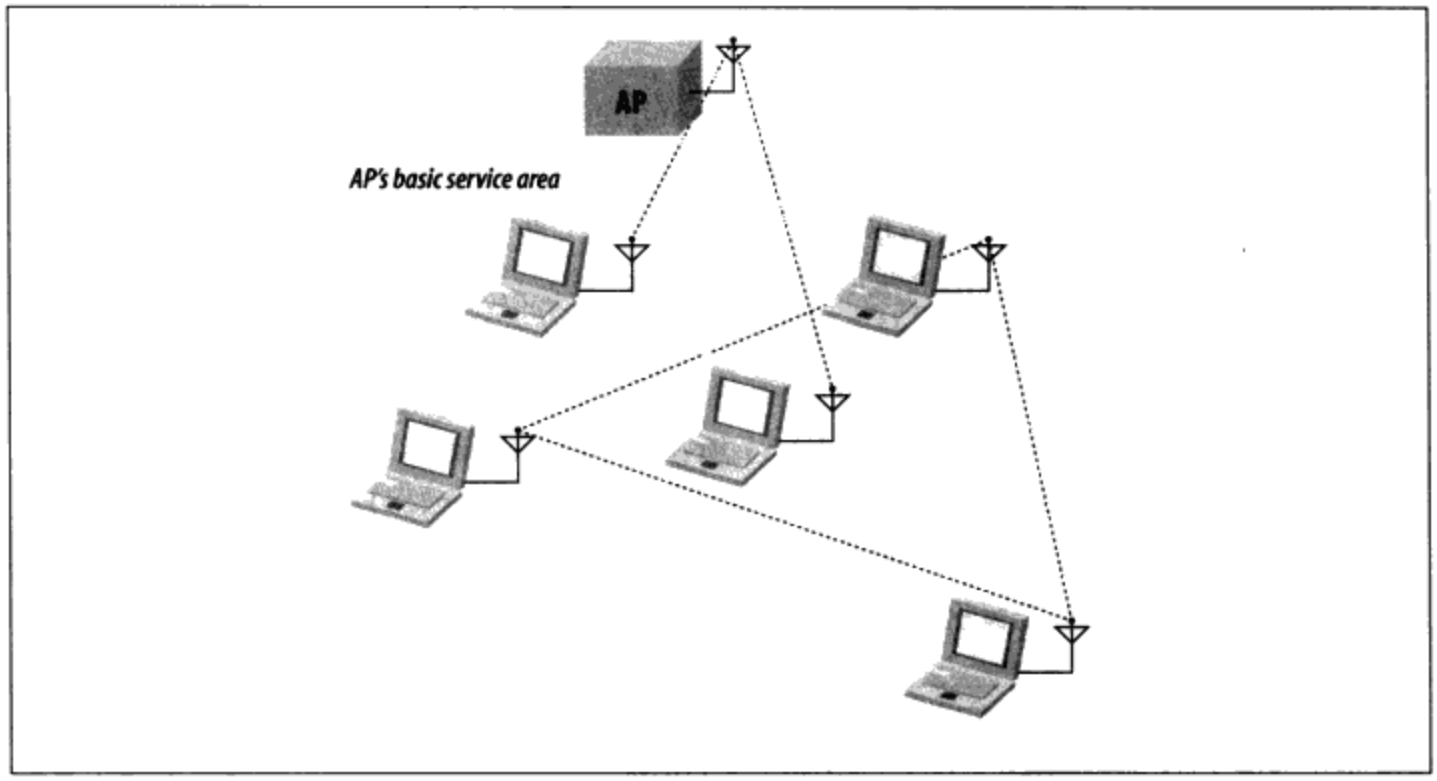


图2-8：不同类型的无线网络相互重叠

802.11里同样可以找到Ethernet的核心成分。它同样是以长度为48位的IEEE 802 MAC地址来区别工作站。概念上，帧的传递是根据MAC地址。虽然802.11为了克服无线信道可靠性不够的缺点（注4）而纳入了某些机制以确保基本的可靠性，但帧传递实际上是不可靠的。

从用户的观点来看，802.11跟Ethernet没有两样。不过，网管人员必须对802.11有更进一步的了解。既要提供MAC层次的移动性，又要依循之前的802标准所规划的路径，所以必须加入一些额外的服务与较复杂的帧格式。

网络服务

定义网络技术的方式之一就是看它能够提供哪些服务，而不论设备制造商如何实现这些服务。802.11总共可以提供9种服务，其中3种用来传送数据，其余6种均属管理操作，目的是让网络能够追踪移动节点及传递帧。

以下内容说明这9种服务并摘录于表2-1中：

注4：我所谓的“不够”（poor）只是相对的说法。不过无线传输的可靠性的确不能和有线网络的可靠性相提并论。

分布式（Distribution）

只要基础结构型网络里的移动式工作站传送任何数据就会使用这项服务。一旦接入点接收到帧，就会使用分布式服务将帧送至目的地。任何使用接入点的通信都会通过分布式服务传播，包括关联至同一个接入点的两个移动式工作站的相互通信。

整合（Integration）

整合服务是由分布式系统提供，它让分布式系统得以连接至非 IEEE 802.11 网络。整合功能将因所使用的分布式系统而异，因此除了必须提供的服务，802.11 并未加以规范。

关联（Association）

之所以能够将帧传递给移动式工作站，是因为移动式工作站会向接入点登记或与接入点产生关联。产生关联之后，分布式系统即可根据这些登记信息判断哪个移动式工作站该使用哪个接入点。未关联的工作站不算“在网络上”，就像拔掉 Ethernet 网线的工作站。802.11 虽规范了使用这些关联数据的分布式系统必须提供哪些功能，但对于如何实现这些功能并未强制规定。如果使用强健安全网络协议（robust security network protocol），那么关联之后才能进行身份验证。在身份验证完成之前，接入点会丢弃来自工作站的所有数据。

重新关联（Reassociation）

当移动式工作站在同一个扩展服务区域里的基本服务区域之间移动时，它必须随时评估信号的强度并在必要时切换所关联的接入点。重新关联是由移动式工作站所开启，当信号强度显示最好切换关联对象时便会如此做。接入点不可能直接开启重新关联服务。（有些 AP 会刻意将工作站剔除，强迫它们进行重新关联过程。未来，随着更优秀网管标准的发展，重新关联会更密切依赖底层的基础建设。）

一旦完成重新关联，分布式系统会更新工作站的位置记录，以反映出可通过哪个接入点连上工作站。和关联服务一样，在强健安全网络中，除非已经成功完成身份验证，否则来自工作站的数据均会被丢弃。

取消关联（Disassociation）

要结束现有关联，工作站可以利用取消关联服务。当工作站启动取消关联服务时，存储于分布式系统的关联数据随即会被移除。一旦取消关联，工作站即不再附接在网络上。在工作站的关机过程中，取消关联是个礼貌性的动作。不过 MAC 在设计时已经考虑到工作站未正式取消关联的情况。

身份验证（Authentication）

实体安全防护在有线局域网安全解决方案中是不可或缺的一部分。网络和连接点（attachment point）受到限制，通常只有位于外围访问控制设备（perimeter access control device）之后的办公区才能加以访问。网络设备可以通过加锁的配线柜（locked wiring closet）加以保护，而办公室与隔间的网络插座只在必要时才连接

至网络。无线网络无法提供相同层次的实体保护，因此必须依赖额外的身份验证例程，以保证访问网络的用户已获得授权。身份验证是关联的必要前提，唯有经过身份验证的用户才允许使用网络。

工作站与无线网络连接的过程中可能经过多次身份验证。关联之前，工作站会先以本身的MAC地址来跟接入点进行基本的身份验证。此时的身份验证通常称为802.11身份验证，有别于后续所进行的牢靠而经过加密的用户身份验证。

解除身份验证（Deauthentication）

解除认证用来终结一段身份验证关系。因为获准使用网络之前必须经过身份验证，解除身份验证的副作用就是终止当前的关联。在强健安全网络中，解除身份验证也会清除密钥信息。

机密性（Confidentiality）

在有线局域网中，坚固的实体控制可以防止对于数据的绝大部分攻击。攻击者必须能够实际访问网络媒介，才有可能窥视往来的内容。在有线网络中，网线与其他计算资源一样也要受到实体保护。在设计上，实际访问无线网络相对而言较为容易，只要使用正确的天线与调制方式就能办到。

802.11初次改版时，机密性（confidentiality）服务原本称为私密性（privacy）服务，而且是由目前已经毫无可信度的有线等效加密（Wired Equivalent Privacy，简称WEP）协议所提供的。除了新的加密机制，802.11i另外提供了两种WEP无法解决的关键服务来加强机密性服务，即基于用户的身份验证（user-based authentication）以及密钥管理服务。

MSDU传递

一个网络如果无法传递数据给接收端，大概也没有什么用。工作站所提供的MSDU（MAC Service Data Unit）传递服务负责将数据传送给实际的接收端。

传输功率控制（Transmit Power Control，简称TPC）

TPC是在802.11h中定义的新服务。欧洲标准要求操作于5 GHz频带的工作站必须能够控制电波的传输功率，避免干扰其他同样使用5 GHz频带的用户。传输功率控制也有助于避免干扰其他无线局域网。传输距离是传输功率的函数：工作站的传输功率越高，传输距离就越远，也就越容易干扰邻近的网络。如果可以将传输功率调到“刚刚好”（just right），就可以避免干扰到邻近的工作站。

动态频率选择（Dynamic Frequency Selection，简称DFS）

某些雷达系统的操作在5 GHz范围内。因此，有些管理者强制要求无线局域网必须能够检测雷达系统以及选择未被雷达系统所使用的频率。有些管理者甚至要求无线局域网必须能够均衡使用（uniform use）5 GHz频带，因此网络必须具备重映射信道（remap channel）的能力。

表2-1：网络服务

服务	此服务属于工作站还是分布式系统？	说明
分布式	分布式系统	传递帧时，可使用此服务来决定目的地位于基础结构网络上的地址
整合	分布式系统	用来将帧传递至无线网络以外的 IEEE 802 LAN
关联	分布式系统	用来建立 AP（作为网关使用）与特定移动式工作站间的关联
重新关联	分布式系统	用来变更 AP（作为网关使用）与特定移动式工作站间的关联
取消关联	分布式系统	用来从网络移除无线工作站
身份验证	工作站	建立关联之前用来进行身份验证（利用 MAC 地址）
解除身份验证	工作站	用来终结一段身份验证关系，其副作用是终止当前关联
机密性	工作站	用来防止窃听
MSDU 传送	工作站	用来传递数据至接收端
传输功率控制（TPC）	工作站 / 频谱管理	降低工作站传输功率以减少干扰
动态频率选择（DFS）	工作站 / 频谱管理	避免在 5 GHz 频带干扰雷达操作

工作站服务

每个与 802.11 兼容的工作站都必须提供工作站服务，任何宣称符合 802.11 规范的产品也都必须具备这项功能。移动式工作站与接入点的无线接口都会提供工作站服务。工作站提供帧传递（frame delivery）服务让消息得以传递，为了支持此项任务，工作站还必须以身份验证服务来建立关联。工作站或许也希望利用机密性功能，在消息传递至容易遭受侵害的无线链路时加以保护。

分布式系统服务

分布式系统服务负责将接入点连接至分布式系统。接入点的主要任务是通过对无线端提供关联与集成服务，将有线网络所提供的服务扩展至无线网络。分布式系统另外一项重要的任务是管理移动式工作站的关联。为了维护关联数据以及工作站的位置信息，分布式系统还提供了关联、重新关联以及取消关联等服务。

机密性与访问控制

机密性与访问控制服务彼此密不可分。除了传输数据的保密性（secrecy），机密性服务也提供帧内容的完整性（integrity）。保密性与完整性均依赖共享式加密密钥（shared cryptographic keying），因此机密性服务必然依赖其他服务来提供身份验证与密钥管理。

身份验证与密钥管理（Authentication and key management，简称AKM）

如果无法防范未经授权的用户，密码学上的完整性就没有什么价值可言。机密性服务依赖身份验证与密钥管理的配套使用来确定用户的身份并建立加密密钥。身份验证也可以通过其他外部协议，比如802.1X，或者预共享密钥（pre-shared key）来完成。

加密算法（Cryptographic algorithm）

帧可以通过传统的WEP算法获得保护，使用40或104位长的密钥、TKIP（临时密钥完整性协议）或者CCMP（CBC-MAC计数模式协议）。我们将于第五章与第七章详细探讨这些算法。

来源真实性（Origin authenticity）

TKIP与CCMP让接收端得以验证传送端的MAC地址以避免伪装攻击（spoofing attack）。来源真实性只能保护单播数据（unicast data）。

重放检测（Replay detection）

TKIP与CCMP会使用序号计数器（sequence counter）来验证所接收的帧以防范重放攻击（replay attack）。“太旧”的帧就会被丢弃。

其他外部协议与系统

机密性服务极其依赖其他外部协议。密钥管理由802.1X提供，而802.1X则会搭配EAP来传递身份验证数据。802.11并未限制使用何种协议，不过最普遍的做法是以EAP提供身份验证并以RADIUS接入认证服务器。

频谱管理服务

频谱管理服务是工作站服务的一部分。这项服务让无线网络得以响应环境并动态更变电波的设定值。为了符合电波管理的要求，802.1h定义了两种服务。

第一种服务称为传输功率控制（TPC），用来动态调整工作站的传输功率。接入点可以利用TPC操作来告知工作站最大容许功率，如果工作站所使用的功率不符合电波管理的要求，也可以拒绝连接。工作站可以利用TPC调整功率，使传输距离“刚刚好”可以连上接入点。数字移动电话系统（digital cellular system）也有类似功能，被设计来延长手

机电池的使用时间（注5）。较低的传输功率也有助于延长电池的使用时间，但是效果取决于手机能够降低多少传输功率。

第二种服务称为动态频率选择（DFS），主要是为了在欧洲地区避免干扰5 GHz频带的雷达系统。虽然原本是为了符合欧洲管理者的需求，不过背后所依循的原则还是跟其他管理者的需求没有两样。DFS是美国于2004年决定在5 GHz频带开放更多频谱的关键（注6）。接入点可借助DFS所提供的功能，让某个信道静默（quiet the channel）后不受干扰地搜索雷达。不过，DFS最重要的功能在于可以为接入点重新分配信道。切换信道之前，工作站均会接到通知。

移动性的支持

移动性是采用802.11网络的主要动机所在。在工作站移动时传送数据，就好比在移动时用手机通话。

802.11所提供的移动性存在于链路层的基本服务区域之间。它并无法理解链路层以上究竟发生什么事。在设计规划802.11时，网络工程师必须特别小心，好让无线层的无间隙转换（seamless transition）在工作站IP地址可被保留的网络协议层也得到支持。就802.11而言，接入点之间可能出现三种转换：

不转换

如果工作站并未离开当前接入点的服务范围，就无需转换。此状态之所以发生，可能是因为工作站并未移动，或是仍在当前接入点的基本服务区域中移动（注7）。（当然，这种说法可能会引起争论，不过规范就是如此定义的。）

BSS转换

工作站持续监控来自所有接入点的信号强度与信号质量。在扩展服务区域中，802.11提供了MAC层次的移动性。附接至分布式系统的工作站可以将所送出的帧

注5: 功率控制也有助于简化接入点所使用的电子电路，因为如此一来，所有待接收信号大概都相去不远。

注6: 此决策决定于2003年11月并发表于FCC 03-287。决策内容详见 *http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-287A1.pdf*。虽然频谱已经分配了，但撰写本书时，测试程序仍在开发阶段。所以，此频带尚无已通过FCC认证的设备。

注7: 虽然从我的解释听来似乎可以轻易区别出“静止”与“局部移动”的状态，其实不然。RF传播所涉及的物理特性使得难以预测某个工作站是否正在移动，因为信号强度可能会因为屋内摆设的位置不同而有所差异，其中当然还包括随意走动的人们。

寻址到某个移动式工作站的MAC地址，并让接入点充当该移动式工作站的最终跳跃点(final hop)。分布式系统上的工作站无需知道某个移动式工作站的确切位置，只要该移动式工作站位于同样的扩展服务区域内即可。

图2-9展示了BSS转换的过程。本图中有三个接入点被赋予相同的ESS。一开始，以*t=1*表示配备802.11无线网卡的膝上型计算机位于AP1的基本服务区域并与AP1关联。当该膝上型计算机离开AP1的基本服务区域并于*t=2*进入AP2的范围时，就发生所谓的BSS转换。该移动式工作站会使用重新关联服务与AP2关联，而AP2则会开始送出帧给该移动式工作站。

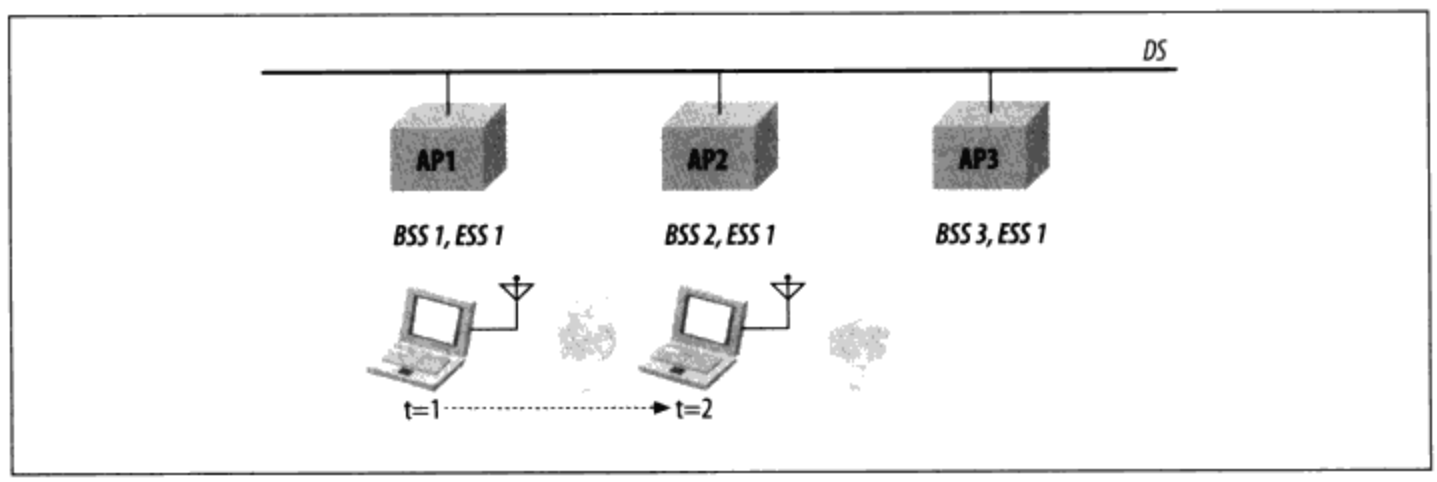


图2-9：BSS转换

BSS转换需要接入点的相互合作。在上述情况下，AP2必须通知AP1该移动式工作站现在已经与AP2关联。802.11并未规范BSS转换过程中接入点之间如何通信的细节。

值得注意的是，即使这两个接入点隶属于同一个扩展集，它们之间却可能是由一部路由器所连接的，即受限于第三层协议。在这种情况下，仅使用802.11协议并无法保证可以达到无间隙漫游。

ESS转换

所谓ESS转换，是指从某个ESS移动至另一个ESS。802.11并未支持此类转换，不过允许工作站在离开第一个ESS的范围之后与第二个ESS里的接入点关联。可以确定的是，较上层的连接必然会因此而中断。比较正确的说法是，802.11所支持的ESS转换仅能够让工作站比较容易与新的扩展服务区域中的接入点关联。要能够维持较高层次的连接，必须得到协议簇的支持。以TCP/IP为例，要支持无间隙的ESS转换，必须使用Mobile IP。

图2-10展示了ESS的转换过程。图2-10中，四个基本服务区域组成了两个扩展服务区域。目前尚未支持从左边的ESS无间隙地转换至右边的ESS。之所以支持ESS

转换，是因为移动式工作站会立即与第二个ESS里的接入点关联。只要离开第一个ESS的范围，任何作用中的网络连接都会随之断线。

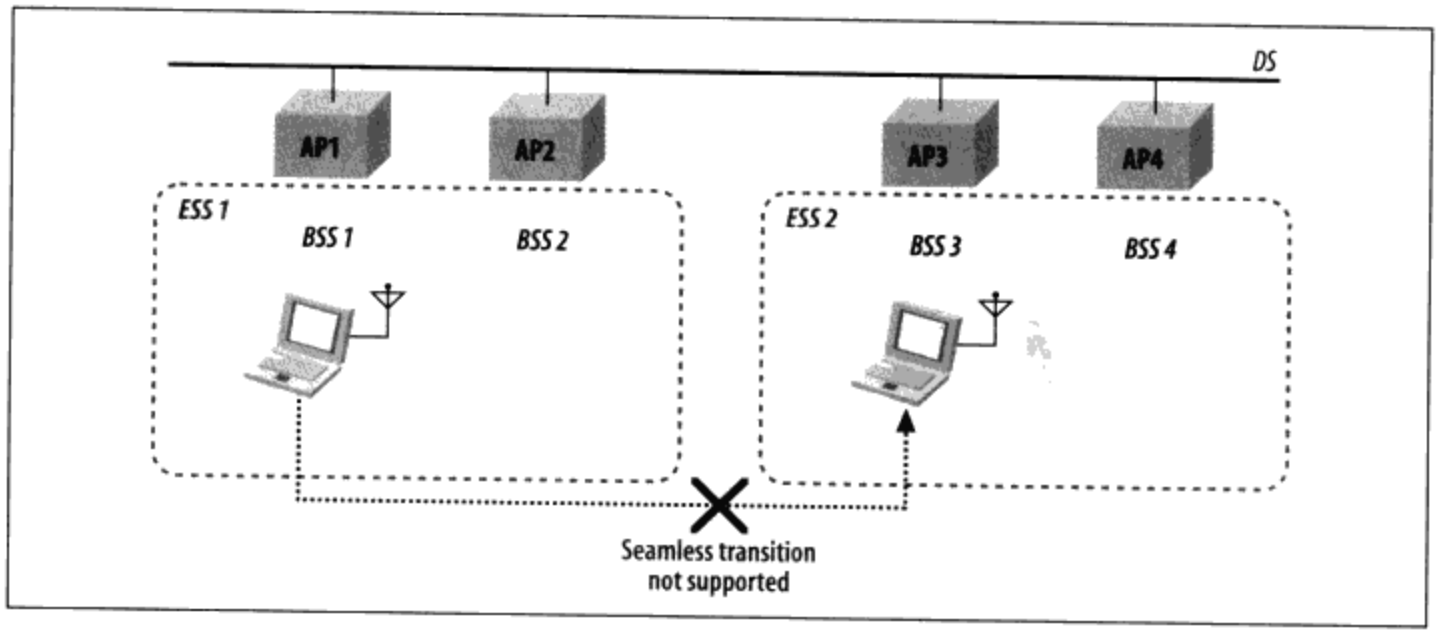


图 2-10：ESS 转换

移动性网络设计

在设计上，绝大多数的网络皆采用一组接入点访问一组资源。同一网络组织所控制的所有接入点均会被赋予相同的 SSID，使用无线网络时，工作站就以此 SSID 进行连接。

工作站四处移动时，除了持续监视网络连接状态，也会在不同接入点间进行切换。802.11可以确保工作站移至不同接入点时维持关联，只要这些关联隶属于同一个SSID，但是网络设计人员在构建网络时必须将移动性纳入考虑。较小的网络通常是由单一的 VLAN、单一的子网所构成，这时就不必担心移动性的问题。跨网段的较大网络则必须使用额外技术才能够支持移动性。有些产品仅使用单一的VLAN核心，不论工作站置身何处均关联至相同的VLAN。较新的产品甚至会根据身份验证数据为工作站动态指派 VLAN。因此不论置身何处，只要用户一连接到网络，就会被引导至相同的VLAN。这类交换式网络只会要求无线局域网设备必须正确标注帧。有些产品支持 Mobile IP 标准或者使用自创的 VPN 技术。这些移动性策略的取舍将于第二十一章深入探讨。

事实上，ESS转换相当罕见，通常只发生在用户离开某个网域并进入到另一个网域时（例如，某个 hot spot 的公司网络）。此时，两个网络可能使用不同的 IP 地址，两者之间也不存在足以在不中断网络层连接的情况下无间隙地转移工作站的信任关系。

专属的移动性系统

为了提供移动性，有些厂商会设计各自专属的协议与流程，特别是那些专门设计产品来

构建大规模网络的设备厂商。在我着手修订本书时，802.11尚存的一个大问题是：必须以同一个IP子网来提供漫游。如此一来，无线局域网的部署除了必须在架构上进行实际的规划，在骨干网络之上也免不了要有所调整。有些厂商为了尽快填补这些空隙，让工作站能够在各种类型的网络之间来去自如以及可以在接入点之间快速漫游，早已着手开发各自的专属协议。这些解决方案的基本概念将会在本书后半段与部署相关的章节中加以探讨。

第三章

802.11 MAC 基础

本章开始深入探讨802.11标准。第二章从宏观的角度概述了802.11，同时还论及标准本身所具备的一些基本属性。过了这个分水岭，本书将分为理论与实务两个部分。往后接连几章的内容大多与802.11规范及其所采用的相关标准有关。然而，不是非得俱细靡遗地了解相关协议才能够构建有线或无线网络。不过，有些时候还是需要对底层的运作机制有比较深入的了解。

- 虽然802.11已广泛且迅速地为人们所接受，但是安全议题还是持续占据新闻头条。人们无疑会征求网络管理人员对安全议题所持有的见解，特别是在与无线局域网相关的提案中。要了解以及参与这些讨论，请阅读第五章和第六章。使用静态密钥的WEP机制已全然遭到破解，使用802.1X与动态WEP密钥的方案显然较为坚固。如果辅以第七章所探讨的802.11i相关协议，那就更加牢靠了。
- 无线网络的故障排除与有线网络类似，不过更加复杂。封包监听软件（packet sniffer）向来是故障排除的得力助手。不过，各位必须了解各种封包的含义，方能正确诠释网络的行为，完全发挥封包监听软件的功效。
- 调整无线网络离不开规范说明书所列举的种种参数以及底层无线电技术的种种行为。要理解网络的种种行为以及可以优化到什么程度，需要对这些参数有所认识并知道无线电波在你的使用环境中如何传播。
- 有些设备驱动程序会开放一些可供调整的低端设定（low-level knobs and dials）。大部分的驱动程序都会为这些参数提供调整过的默认值，少数驱动程序则允许用户自由设定。由于手上拥有源代码，因此开放源码软件的用户也可以随意试验。
- 无线局域网技术的发展十分快速，随时都会加入新的协议特色。深入了解这些基本协议，有助于了解这些新功能的运作方式以及它们对现有网络而言有何种意义。

和生命中的其他事物一样，了解越多，就越好掌握。Ethernet 通常不会带来什么麻烦（trouble-free），不过认真的网管人员心知肚明，一旦遇上问题，没有什么比得上对于网络如何运作的充分了解与知识。在本书第一版问世时，802.11 网络有点免费奉送（free ride）的味道。因为 802.11 够酷，就算一时断线，用户通常也不以为然。过去，无线联网并非一种权利（right），而是一种特权（privilege）。另一方面，无线网络与用户的数量相对而言并不多，因此极少遭遇到负载问题。服务半打用户的Ethernet大概不成问题，但是一旦在网络中加入了几台高用量的服务器、几百个用户以及相互关联的桥接器与路由器，问题就会开始浮现。无线网络亦然。几个接入点服务半打用户也不成问题，但当用户数成倍增长而且有几个无线网络彼此重叠时，每个无线网络各自拥有一组接入点，负载问题必然随之浮现。

这就是为什么该阅读本章的理由。接下来让我们仔细瞧瞧。802.11规范的关键在于MAC（媒介访问控制层）。MAC 位于各式物理层之上，控制数据的传输。它负责核心成帧操作（core framing operation）以及与有线骨干网络之间的交互。不同的物理层可能提供不同的传输速度，不过物理层之间必须彼此互用（interoperate）。

802.11 并未大幅偏离之前的 IEEE 802 标准。802.11 成功地将 Ethernet 类型的网络应用到无线链路之上。和Ethernet一样，802.11采用载波监听多路访问（carrier sense multiple access，简称 CSMA）机制来控制对传输媒介的访问。不过，冲突（collisions）会浪费宝贵的传输资源，因此802.11转而使用冲突避免（CSMA/CA）机制，而非使用Ethernet所实行的冲突检测（CSMA/CD）机制。和 Ethernet 一样，802.11 采用的是不具中枢控制功能的分布式访问机制，因此每个 802.11 工作站访问媒介的方式都一样。802.11 与 Ethernet 之间的主要差异在于所使用的底层媒介不同。

本章首先会描述当初设计MAC时必须克服的难题，以便洞悉MAC设计人员的动机，随后说明这些媒介的访问规则以及基本的帧结构。如果各位只想了解802.11网络上的基本帧序列，可以直接跳至本章结尾。要进一步了解 MAC，可以参阅 802.11 标准第 9 款（Clause 9）所列的正式规范。详细的 MAC 状态图（state diagram）列于附录三中。

MAC 所面临的挑战

无线网络环境与传统有线网络环境的差异性为网络协议设计人员带来了种种挑战。本节将讨论 802.11 设计人员所面临的一些难题。

射频链路品质

在有线的Ethernet中，假设对方必然会收到所传送的帧是合理的。无线链路（radio link）

则不然，特别是使用无需授权的ISM频带时。即使窄带（narrowband）传输将会受到噪声与干扰的影响，未经许可的设备（unlicensed device）也必须假设干扰的存在并且提供克服干扰的方法。为了克服微波炉以及其他射频(RF)来源所导致的辐射问题，802.11设计人员曾经考虑过几种解决方案。除了噪声问题，多径衰落（multipath fading）所造成的布线死区（dead spot）（译注 1）也可能导致帧无法传送。

和其他链路层协议不同，802.11采用肯定确认（positive acknowledgment）机制。所有传送出去的帧都必须得到响应，如图3-1所示。只要有任何一个环节失败，该帧即被视为已经漏失。

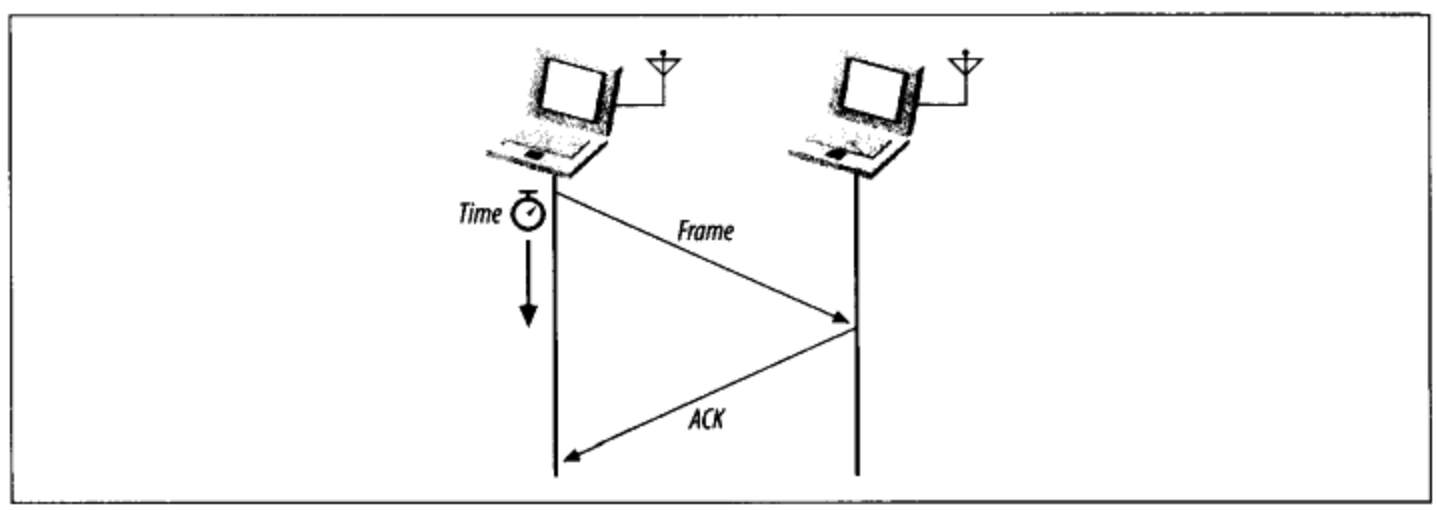


图 3-1：数据传输的肯定确认

图3-1所列的步骤称为原子操作（atomic operation），意指不可分割的单一事务单元（single transactional unit）。虽然整个事务过程包含好几个步骤，但还是会被视为单一的不可分割的操作。原子操作可说是“非成即败”（all or nothing）。若没有完成所有步骤，则整个操作就被视为失败。数据帧的传送者必须收到响应，否则该帧即被视为已经漏失。从传送者的角度而言，究竟是一开始的数据帧还是响应消息在传输过程中漏失并不重要。因为不论如何，数据帧还是得予以重传。

将帧传送视为基本操作会让事情变得比较复杂，因为如此一来，整个事务就分为两个步骤，分别由两个不同的工作站所控制。在事务过程中，这两个工作站必须彼此合作，依

译注 1：在无线链路中，射频信号可能来自发送端（直线信号），也可能来自物体（例如建筑物、车辆）的反射（反射信号），这会对接收端形成多重传输路径。接收端所收到的实际信号为直线信号与反射信号的总和。若直线信号与反射信号刚好振幅相同且相位相反，则接收端所收到的信号总和会形成所谓的收信死区。这种由多重路径所造成的信号衰减称为多径衰落（multipath fading）。因为这是物理学家Rayleigh最早提出的现象，所以又称为Rayleigh Fading。

次取得网络媒介的控制权以便进行传输操作。802.11允许工作站在基本操作期间锁定媒介，避免基本操作被其他试图竞争传输媒介的工作站打断。

无线链路的质量也会影响网络操作的速度。信号质量较佳，就可以用较高的速度来传送数据。信号质量通常随着距离的拉长而有所减损，即802.11工作站的数据传输速度取决于它和接入点之间的相对位置。工作站必须具备某种机制，可以判断何时该变更数据传递速率以适应环境的改变。此外，网络中所有工作站必须能够以不同的速度进行数据的传输。支持多种速率的规则，将于本章稍后探讨。

隐藏节点的问题

在Ethernet网络中，工作站是通过接收传输信号来行使CSMA/CD的载波监听功能。物理的媒介线路中包含了信号，而且会传输至各网络节点。无线网络的界限比较模糊，有时候并不是每个节点都可以跟其他节点直接通信，如图3-2所示。

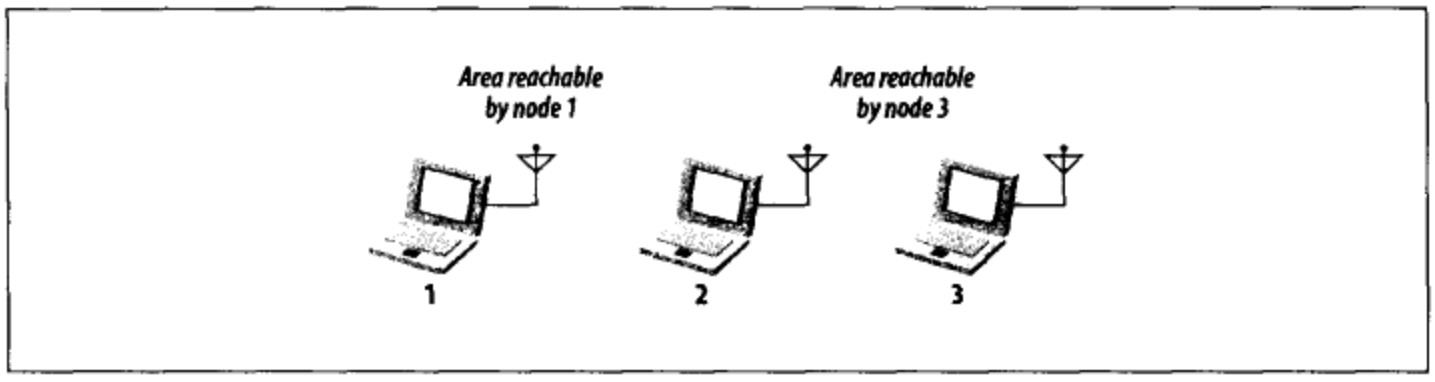


图3-2：节点1与节点3互为隐藏节点

如图3-2所示，节点2可以直接跟节点1及节点3通信，不过某些因素导致节点1与节点3无法直接通信（这与障碍物的关系并不大，节点1与节点3之间可能只是因为距离过远，无法收到对方的无线电波）。从节点1的角度来看，节点3属于隐藏节点（hidden node）。如果使用简单的传输祈求（transmit-and-pray）协议，节点1与节点3有可能在同一时间传送数据，这会造成节点2无从响应任何数据。此外，节点1与节点3无从得知发生错误，因为只有节点2才知道有冲突发生。

在无线网络中，由隐藏节点所导致的冲突问题相当难以监测，因为无线收发器（wireless transceiver）通常只有半双工（*half-duplex*）工作模式，即无法同时收发数据。为了防止冲突发生，802.11允许工作站使用Request to Send（请求发送，简称RTS）及Clear to Send（清除发送，简称CTS）信号来清空传送区域。由于RTS与CTS帧均会延长帧交易过程，因此RTS帧、CTS帧、数据帧以及最后的响应帧均被视为相同原子操作的一部分。图3-3说明了整个过程。

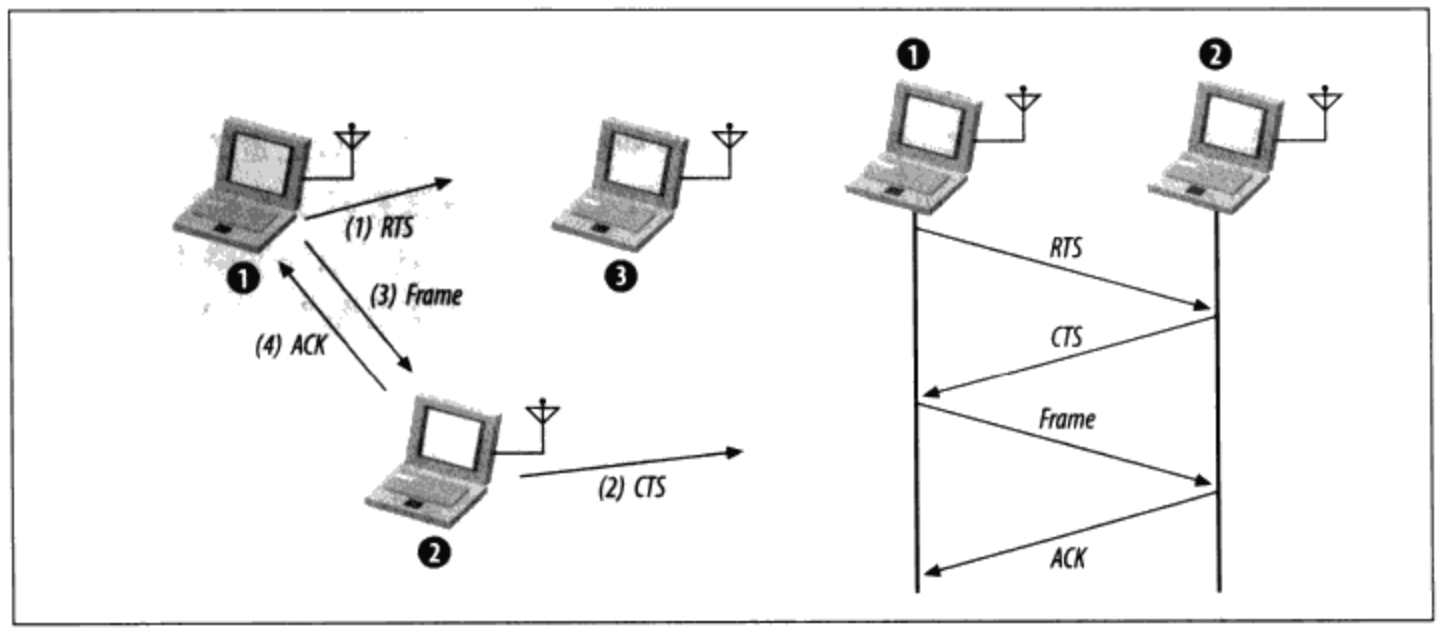


图 3-3：以 RTS/CTS 进行清空

如图 3-3 所示，节点 1 有个帧待传，因此送出一个 RTS 帧以启动整个过程。RTS 帧本身带有两个目的：预约无线链路的使用权与要求接收到这一帧的其他工作站保持沉默。一旦收到 RTS 帧，接收端会以 CTS 帧应答。和 RTS 帧一样，CTS 帧也会令附近的工作站保持沉默。等到 RTS/CTS 完成交换过程，节点 1 即可传送之前待传的帧，而无需担心来自其他隐藏节点的干扰。

整个 RTS/CTS 传输过程会用到好几个帧，实际开始传送数据之前的退避（backoff）也会消耗一定的带宽。因此，它通常只用在高用量的环境下以及传输竞争比较显著的场合。对低用量的环境而言，通常无此必要。

随着 802.11 逐渐成熟，隐藏节点已经不再是问题。在小型、静止的只有几个工作站共享一个接入点的网络里，很少会有同时进行传输的情况，何况还有不少闲置带宽可供重传之用。在比较大型的网络环境里，由于覆盖范围内有相当密集的接入点，工作站很有可能坐落在好几个接入点的共同覆盖范围内。（事实上，有些工作站的传输距离对大多数网络而言可能太远，这一点将留待有关网络规划的章节中再进行探讨。）

如果 802.11 网卡的驱动程序支持，用户可通过调整 RTS 阈值（threshold）来控制 RTS/CTS 交换过程。只要帧大于此阈值，RTS/CTS 交换过程就会进行；小于此阈值则会直接传送帧。

MAC 访问模式与时机

无线媒介的访问是由协调功能（coordination function）控制。Ethernet 之类的 CSMA/CA 访问是由分布式协调功能（*distributed coordination function*，简称 DCF）控制。如

果需要用到无竞争服务（contention-free service），则可通过构建于DCF之上的点协调功能（*point coordination function*，简称PCF）来控制。在各取所需（free-for-all）的DCF与精确控制的PCF之间，网络也可以介于两种极端之间采取中庸之道的混合协调功能（*hybrid coordination function*，简称HCF）。无竞争服务只于基础结构型网络（infrastructure network）中提供，不过只要工作站支持HCF，就可以在网络中提供服务质量（quality of service，简称QoS）功能。协调功能的细节请见图3-4以及下列说明：

DCF（分布式协调功能）

DCF是标准CSMA/CA访问机制的基础。和Ethernet一样，在传送数据之前，它会先检查无线链路是否处于清空状态。为了避免冲突的发生，当某个传送者占据信道时，工作站会随机为每个帧选定一段退避（backoff）时间。在某些情况之下，DCF可利用CTS/RTS清空技术进一步减少发生冲突的可能性。

PCF（点协调功能）

点协调功能提供的是无竞争服务。称为点协调者（point coordinator）的特殊工作站可以确保不必通过竞争即可使用媒介。点协调者位于接入点，因此只有基础结构型网络才会使用PCF。为了赋予比标准竞争式服务还高的优先级，PCF允许工作站经过一段较短的时间间隔后即可传送帧。PCF在实现上并不常见，第九章对此有详细的说明。

HCF（混合协调功能）

有些应用需要比尽力传递（best-effort delivery）更高一级的服务质量，却又不需要用到PCF那么严格的时机控制。HCF允许工作站维护多组服务队列，针对需要更高服务质量的应用提供更多的无线媒介访问机会。HCF尚未完全标准化，不过终将成为802.11e标准的一部分。

将服务质量纳入802.11 MAC当中是项艰巨的任务。由于涉及到成帧（framing）、队列管理（queue management）以及信号产生（signaling）等种种复杂层面，撰写本书时，标准委员会还在为服务质量规范说明书争论不休，因此相关议题将留待未来改版时再予以探讨。

载波监听功能与网络分配矢量

载波监听（carrier sensing）主要用来判断媒介是否处于可用状态。802.11具备两种载波监听功能：物理载波监听（physical carrier-sensing）与虚拟载波监听（virtual carrier-sensing）。只要其中有一个监听功能显示媒介处于忙碌状态，MAC就会将此状况汇报给较高层的协议。

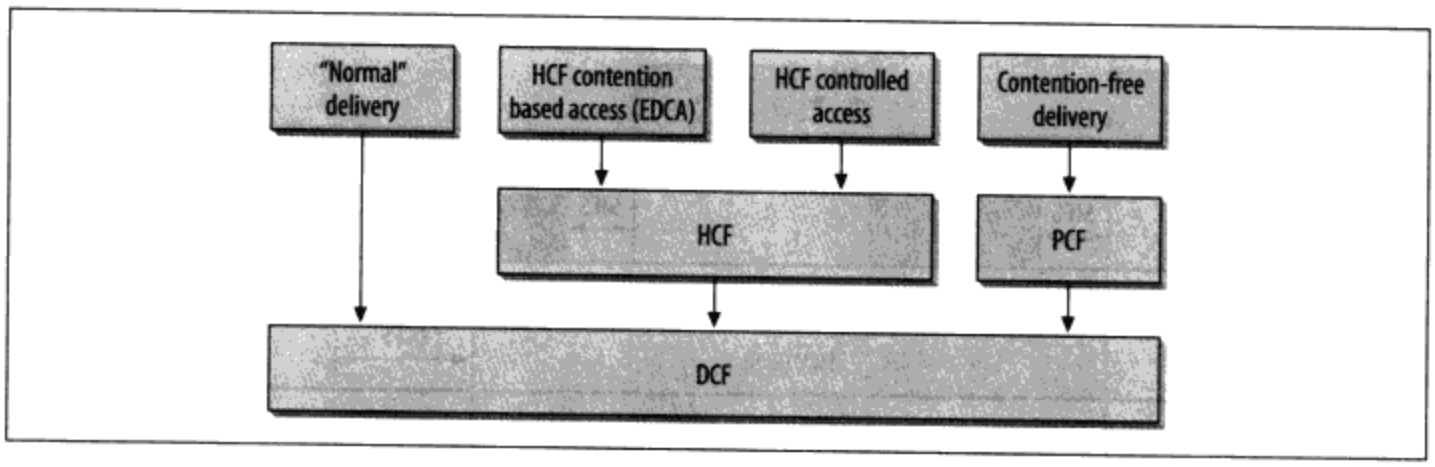


图 3-4：MAC 协调功能

物理载波监听功能是由物理层所提供，取决于所使用的媒介与调制方式。要为基于射频的媒介打造物理载波监听硬件相当不易（更确切的说法是十分昂贵），原因是除非采用昂贵的电子零件，否则收发器无法同时进行收发的动作。此外，由于隐藏节点随处可见，物理载波监听并无法提供所有必要的信息。

虚拟载波监听是由网络分配矢量（Network Allocation Vector，简称NAV）所提供。802.11 的帧通常会包含一个 Duration 字段，用来预订一段媒介使用时间。NAV 本身其实就是一个定时器（timer），用来指定预计要占用媒介多少时间，以微秒（microsecond）为单位。工作站会将NAV 设定为预计使用媒介的时间，这包括完成整个操作必须用到的所有帧。其他工作站会将NAV的值倒数至零。只要NAV的值不为零，就代表媒介处于忙碌状态，此即虚拟载波监听功能。当 NAV 为零时，虚拟载波监听功能会显示媒介处于闲置状态。

利用 NAV 可保证工作站的原子操作（atomic operation）不被中断。例如，图 3-3 所示的 RTS/CTS 过程即属一种基本操作。图 3-5 说明了 NAV 如何保障整个过程不受干扰。（这是本书中的图解所使用的标准格式，用以说明多个工作站之间的互动，每个工作站各自有相应的定时器。）工作站对媒介的访问操作可用加上阴影的条状图（shaded bar）来表示，每个条状图（bar）均会标上帧类型。没有任何操作之处会标上帧间间隔（interframe spacing）。在此图底部，NAV线（line）上的条状图代表NAV定时器。NAV 是由 RTS 与 CTS 帧上的标头来载送的，此处之所以特别画出一条 NAV线，是为了要显示NAV 与空中实际传输情况的关系。只要在 NAV 线上出现 NAV 条状图，工作站就必须延迟访问媒介，因为虚拟载波监听机制将会指出媒介正处于忙碌状态。

为了确保整个过程不被中断，节点 1 会在其 RTS 帧中设定 NAV，以防止传送 RTS 时其他工作站对媒介进行访问。所有收到 RTS 帧的工作站均会延迟访问媒介，直到 NAV 消失。

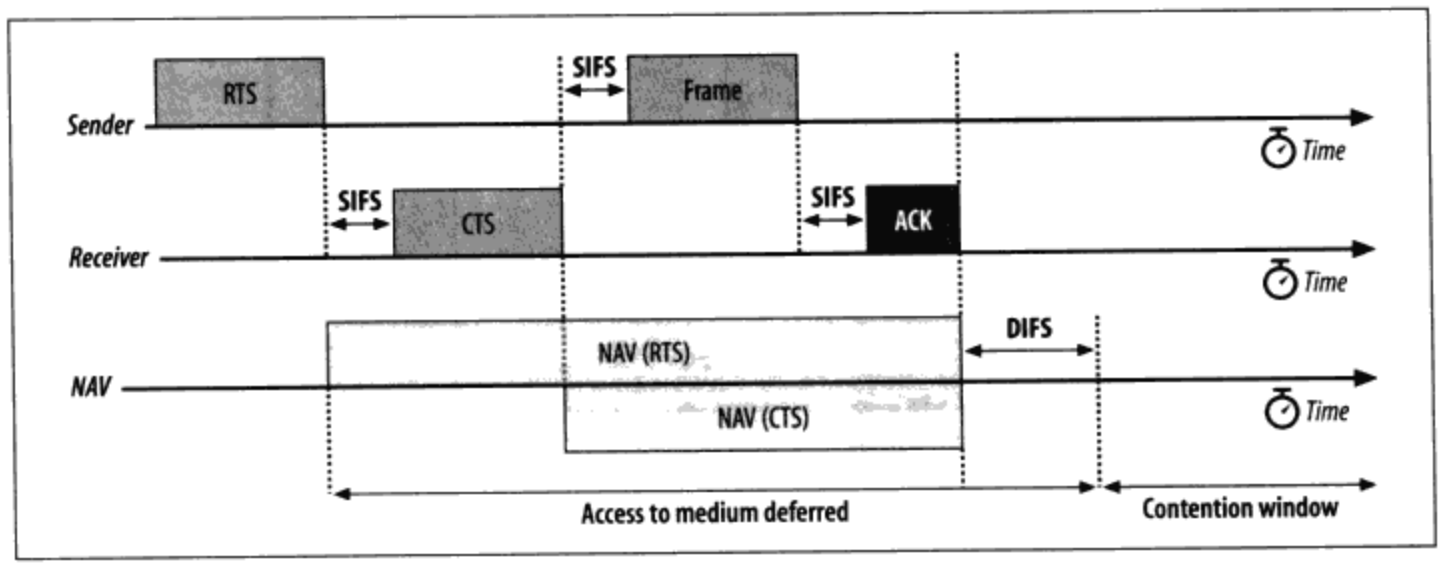


图 3-5：利用 NAV 进行虚拟载波监听

然而，不见得网络上的每一个工作站均会收到这些 RTS 帧。因此，接收端会以 CTS 帧加以响应，其中也包含 NAV，不过为时较短。此 NAV 可防止其他工作站在传输过程中访问媒介，直到传输过程结束。一旦完成整个过程，经过一段分布式帧间间隔（distributed interframe space，简称DIFS）之后，任何工作站均可对媒介进行访问，此时便进入竞争窗口（contention window），如图 3-5 右边所示。

在有多个网络交界的拥堵地区，RTS/CTS交换过程也可以派上用场。位于相同物理信道的工作站均会收到NAV，因而会适当地延迟对媒介的访问，就算这些工作站分别配置于不同的网络之上。

帧间间隔

和传统Ethernet一样，帧间间隔（interframe spacing）在协调媒介的访问上扮演着重要的角色。802.11 会用到四种不同的帧间间隔，其中三种用来决定媒介的访问，它们之间的关系如图 3-6 所示。

现在我们已经知道，因为802.11 MAC 内置了避免冲突的功能，所以工作站会延迟媒介的访问，直到媒介再度闲置。不同的帧间间隔会为不同类型的传输产生不同的优先次序。其后的决策逻辑十分简单：当媒介闲置下来时，高优先级的数据所等待的时间较短。因此，如有任何高优先级的数据待传，在优先级较低的帧试图访问媒介之前，优先级较高的数据早就将媒介占为己用了。为了维持不同数据传输率（data rate）的互用性，帧间间隔的时间值都是固定的，与传输率无关。（这只是使用相同无线资源的不同物理层所导致的问题之一，因为不同的物理层会使用不同的调制技术。）不过，不同的物理层可以指定不同的帧间间隔时间。

短帧间间隔（Short interframe space，简称 SIFS）

SIFS 用于高优先级的传输场合，例如 RTS/CTS 以及肯定确认帧。经过一段 SIFS（时间），即可进行高优先级的传输。一旦高优先级传输开始，媒介即处于忙碌状态，因此相较于必须等待较长时间才能传输的帧，SIFS 消失后即可进行传输的帧的优先级较高。

PCF 帧间间隔（PCF interframe space，简称 PIFS）

PIFS 主要被 PCF 使用在无竞争操作中，有时被误称为优先级帧间间隔（priority interframe space）。在无竞争时期，有数据待传的工作站可以等待 PIFS 后再加以传送，其优先级高于任何竞争式传输。

DCF 帧间间隔（DCF interframe space，简称 DIFS）

DIFS 是竞争式服务中最短的媒介闲置时间。如果媒介闲置时间长于 DIFS，则工作站可以立即对媒介进行访问。

扩展帧间间隔（Extended interframe space，简称 EIFS）

图 3-6 并没有标明 EIFS，因为 EIFS 并非固定的时间间隔。只有在帧传输出现错误时才会用到 EIFS。

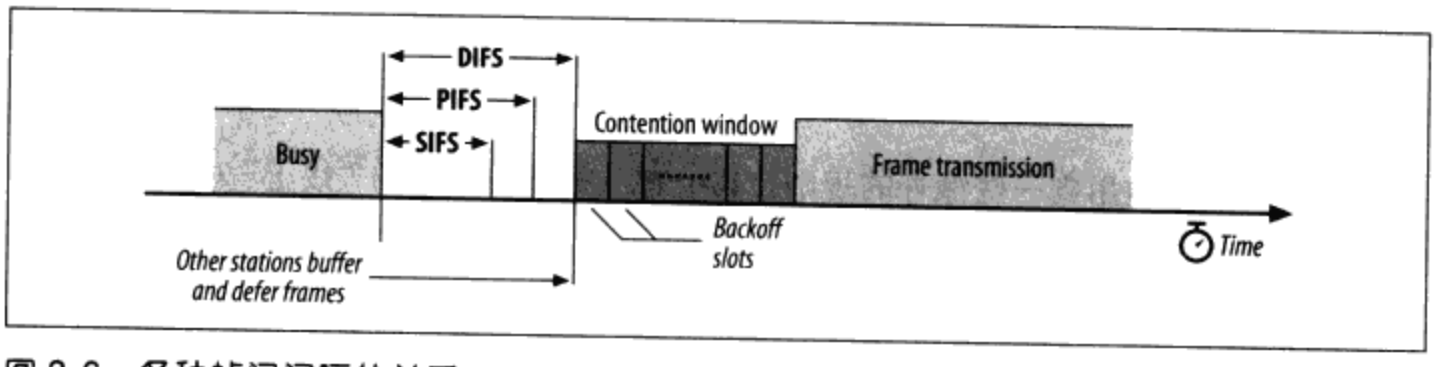


图 3-6：各种帧间间隔的关系

帧间间隔与优先级

一开始，原子操作和一般传送并无不同：在可以开始传送之前，原子操作同样必须等候一段帧间间隔（通常是 DIFS）。不过，其后的步骤即开始使用 SIFS，而非 DIFS。由于 SIFS 短于其他帧间间隔，一项原子操作的第二个（以及之后的）步骤会在其他类型的帧被传送之前将媒介占为己用。利用 SIFS 与 NAV，工作站可以视需要掌控媒介一段时间。

如图 3-5 所示，SIFS 被应用在不同单位的原子操作之间。当传送端取得媒介访问权时，接收端会在 SIFS 之后响应 CTS。任何试图在 RTS 结束之后访问媒介的工作站至少必须等候一段 DIFS。若在 DIFS 进行时 SIFS 已先行结束，则会开始传送 CTS。

利用 DCF 进行基于竞争的访问

大部分的传输操作均会采用 DCF（分布式协调功能），它提供了类似 Ethernet 的基于竞争的服务。DCF 允许多个独立的工作站彼此交互，无需通过中心控制节点，因此可以运用于 IBSS 网络或基础结构型网络。

试图传送任何数据之前，工作站必须查看媒介是否处于闲置状态。若它处于忙碌状态，工作站必须延迟访问并利用指数退避（exponential backoff）算法来避免发生冲突。

我们可从 802.11 MAC 的规则中归纳出一组经常使用的基本规则，其他额外规则的应用则视情况而定。在所有使用 DCF 的传输中将会运用到两项基本规则：

1. 如果媒介闲置时间长于 DIFS，便可立即进行传输。载波监听同时可以物理与虚拟（NAV）两种方式进行。
   a. 如果之前的帧接收无误，则媒介必须至少空出一段 DIFS。
   b. 如果之前的传输出现错误，则媒介必须至少空出一段 EIFS。
2. 如果媒介处于忙碌状态，则工作站必须等候至信道再度闲置，802.11 称之为访问延迟（*access deferral*）。一旦访问延迟，工作站会等候媒介闲置一段 DIFS，同时准备指数退避过程（exponential backoff procedure）。

在特定情况下会运用到一些额外的规则。其中有一些规则取决于“线上”（on the wire）的特殊情况且与之前传送的结果有关。

1. 错误恢复（error recovery）是发送端的责任。发送端预期每个帧均应收到确认，如果没有收到确认则必须负责发送帧，直到成功为止。
   a. 唯有收到肯定确认（positive acknowledgment）才表示发送成功。原子交换操作必须全部完成才算成功。如果某个预期的确认迟迟未到，发送端即会认定其已丢失，必须重新发送。
   b. 所有单播（unicast）数据必须被确认，广播数据则不予确认。（因此，即使无线链路本质上属于广播媒介，相较于广播数据，单播数据基本上还是具备较高的服务质量。）
   c. 只要发送失败，重试计数器（retry counter）就会累加，然后重新发送。发送失败有可能是因为访问媒介失败，也可能是因为得不到确认。不论如何，重传时会等待一段较长时间（详见下一节）。
2. 多帧序列可以在传送过程的每个步骤中更新 NAV。当所收到的媒介预订时间比当

前的NAV还长时，工作站即会更新NAV。设定NAV的方式是以个别的帧为基准，对此下一章会有更详细的说明。

3. 以下的帧类型可在SIFS之后传输，因此优先级较高：确认(acknowledgment)、RTS/CTS交换过程中的CTS以及片段序列(fragment sequence)中的帧片段(fragment)。
   a. 一旦发送出第一个帧，工作站就会取得信道的控制权。后续帧及其确认均可使用SIFS 进行传送，以锁定信道不被其他工作站占用。
   b. 传送操作中，后续帧会将 NAV 更新成该媒介预计使用的时间。
4. 如果较高层的包（higher-level packet）的大小超过所设定的阈值（threshold），则必须使用扩展帧序列（extended frame sequence）。
   a. 包的大小超过 RTS 阈值，必须使用 RTS/CTS 交换过程。
   b. 长度超过分段（fragmentation）阈值，必须加以分段。

DCF 与错误恢复

错误检测与更正（error detection and correction）是由开始原子帧交换过程的工作站来担任。一旦检测到错误，该工作站必须负责重新发送。错误检测必须由发送端负责。有时候，发送端可根据肯定确认来推论帧是否已经丢失。只要帧被重新发送，重试计数器（retry counter）就会累加。

每个帧或帧片段会分别对应到一个重试计数器。工作站本身有两个重试计数器：短帧重试计数器（short retry counter）与长帧重试计数器（long retry counter）。长度小于RTS阈值的帧被视为短帧；长度超过该阈值的帧则为长帧。根据帧的长度，可分别对应到长或短帧重试计数器。帧重试计数由零起算，只要帧传送失败即累加。

短帧重试计数器会在下列情况发生时清零：

- 之前传送的 RTS 得到 CTS 响应
- 之前传送的未分段帧得到 MAC 层的响应
- 收到广播（broadcast）或组播（multicast）的帧

长帧重试计数器会在下列情况发生时清零：

- 之前传送的帧大于 RTS 阈值并且得到 MAC 层的响应
- 收到广播或组播的帧

除了相应的重试计数器，MAC 会赋予每个帧片段一个最长的“生存时间”(lifetime)。

传送出第一个帧片段之后，生存时间计时器（lifetime counter）随即启动。一旦超过生存时间，该帧便会被丢弃，因此不会重试其余的帧片段。当然，上层协议也可能检测到数据丢失而予以重传。不过，当上层协议（如TCP）重传数据时，实际上传给802.11 MAC的仍是新的帧，所有重试计数器也会被清零。

使用重试计数器

和大部分其他的网络协议一样，802.11是通过重传机制来提供可靠性（reliability）。数据传送是通过原子步骤（atomic sequence），而且整个过程必须完成才算传送成功。当工作站传送帧时，必须得到接收端的确认，否则传送便被视为失败。若传送失败，则与该帧（或帧片段）相应的重试计数器便会累加。如果达到重传限制，该帧随即被丢弃并将此状况告知上层协议。

之所以要有短帧与长帧，其中一个原因是为了让网络管理人员利用不同长度的帧来调整网络的稳定性。长帧需要较多的缓存空间，所以两种不同重传限制的一个潜在应用即是放宽长帧的重传限制，以减少所需的缓存空间。

DCF的退避算法

当帧传送完成且经过一段DIFS，工作站便会试图传送之前拥堵的数据。DIFS之后紧接的一段时间称为竞争窗口（*contention window*）或退避窗口（*backoff window*）。此窗口（window）可进一步分割为时隙（slot）。时隙长度因媒介而异，速度较高的物理层会使用较短的时隙。工作站会随机挑选某个时隙，等候该时隙到来以便访问媒介。所有时隙的选择机会均等。当多个工作站试图同时传送数据时，挑到第一个时隙（即取得最小随机编号）的工作站可以优先传送。根据802.11标准，所有这些时隙编号不应有差异。唯一值得注意的例外请见本章稍后有关Spectralink语音优先级的相关说明。

如同Ethernet，每当传送失败时，退避时间（backoff time）便会从一个范围中被挑选出来。图3-7以DSSS（直接序列扩频）物理层为例，显示当传送次数增加，竞争窗口（contention window）随之增长的情况。不同物理层会使用不同大小的退避时间，不过原则是相同的。竞争窗口的大小通常是2的指数倍数减1（例如31、63、127、255）。每当重试计数器累增，竞争窗口即移至下一个2的指数倍数。竞争窗口的大小受到物理层的限制。例如，DS物理层限制竞争窗口最多为1023个传送时隙。

当竞争窗口到达最大极限时就会维持该数字，直到它被重新设定。允许使用较长的竞争窗口，可以在多个工作站试图同时访问媒介时保持MAC算法的稳定，即使负载极大。当帧传送成功，竞争窗口即被重设为最小值；如果到达重试计数器的上限，则该帧随即被丢弃。

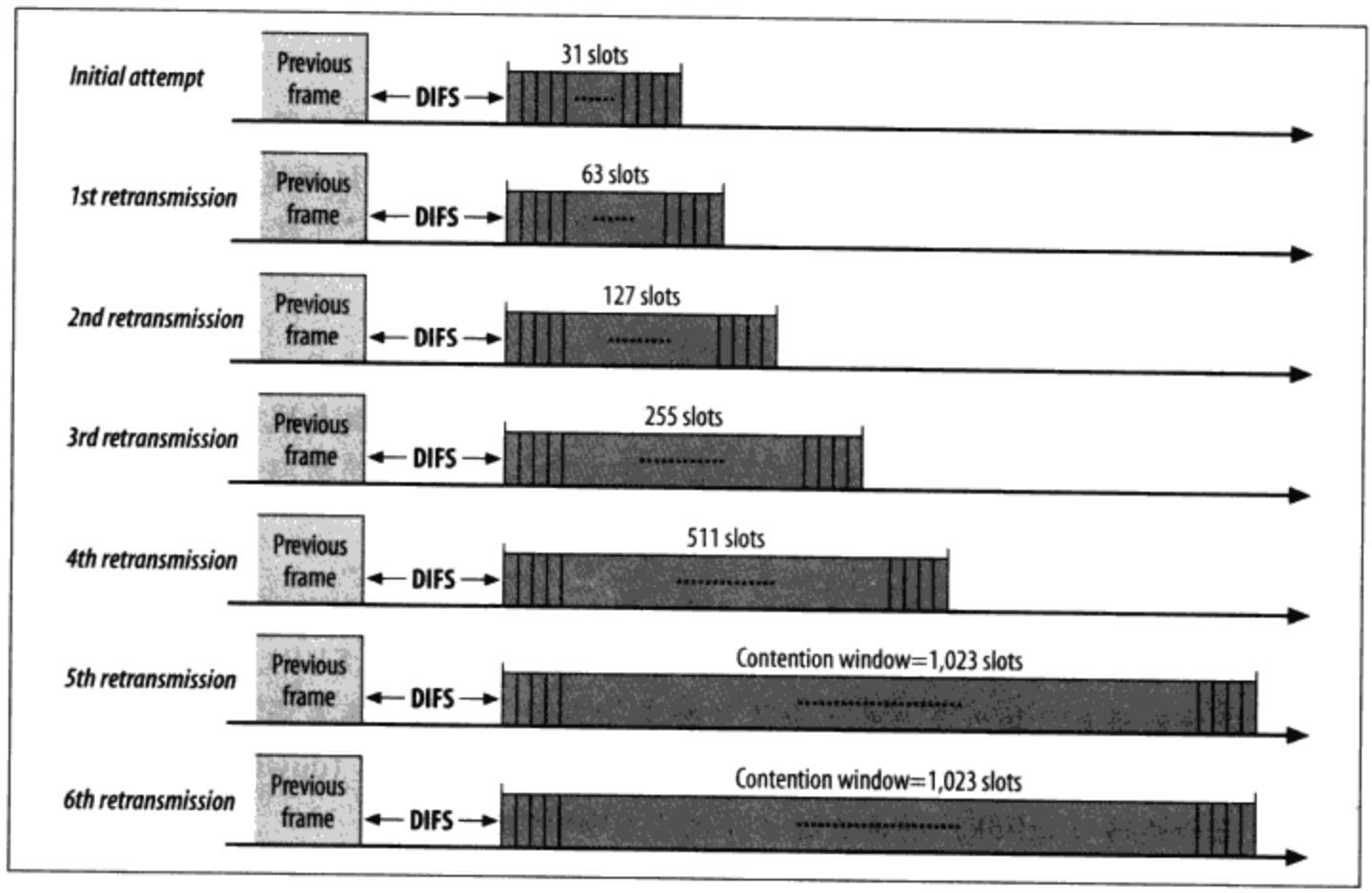


图 3-7：DSSS（直接序列扩频）的竞争窗口

帧的分段与重组

来自较上层的封包以及某些较大型的管理帧可能必须经过分段，无线信道才有办法加以传送。当干扰存在时，分段封包也有助于提升可靠性。利用帧的分段，无线局域网工作站可让干扰只影响较小的帧片段，而非较大的帧。通过降低可能被干扰的数据量，帧分段可以提高整体的有效吞吐量。干扰可能来自不同的来源。虽然并非全部，但还是有些微波炉会对2.4 GHz网络造成干扰。在交流电振幅斜升（ramp-up）到斜降（ramp-down）这段期间，磁控管会产生电磁辐射，因此有一半时间会受到微波的干扰（注1）。有些新型的无绳电话（cordless phone）也会造成干扰（注2）。至于户外的网络，可能造成干扰的因素就更多了。

注1：在美国，家电产品使用60Hz交流电，因此在每16毫秒的周期中，微波炉所造成的干扰有8毫秒。其他国家使用50Hz交电流，因此在每20毫秒的周期中大约有10毫秒会受到干扰。

Spectralink 语音优先级

要在无线网络上支持语音必须面临的挑战之一，就是语音对于网络服务质量的敏感度远高于数据方面的应用。假设某图形文件有1500个字节的数据延迟了1/10秒，用户通常不会有所感觉。不过，如果通电话时迟延了1/10秒，那就令人无法忍受了。

要在IP网络上提供高质量的服务已经相当困难，换成无线局域网，那更是难上加难。设计无线局域网语音网络时，工程师遇到的主要问题是无线局域网对所有数据均一视同仁。假设有一个短语音帧和一个长数据帧，此时无线局域网并不会特别偏爱任一个帧。

Spectralink是一家手持802.11电话制造商，该公司制定了一组特殊的扩展协议，称为Spectralink语音优先级（Spectralink Voice Priority，简称SVP），让网络更适合用来传输语音。接入点与手机中均包含SVP组件，让语音享有高于数据的优先级，同时在接入点中管理语音通话。不论是从接入点下行链路（downlink）还是自手机上行链路（uplink）的语音通话，均由SVP协助管理。

要支持SVP，接入点必须以零退避（zero backoff）机制传递语音帧。选取退避时隙的时候，支持SVP的接入点并未依循802.11标准，而是直接选择编号为零的时隙。竞争无线媒介的时候，取得零退避时隙的语音帧将具备实质的优先级，因为数据帧所取得的时隙编号必定大于零。严格来讲，采用零退避机制的工作站已经不再兼容于802.11，因为它以固定的方式强迫取得特定的退避时隙。（不过，为了维持高负载时的网络稳定性，重传的语音帧必须依循退避规则。）

通过零退避机制，支持SVP的接入点可以确保语音帧能够优先访问媒介。同时，这类接入点也必须追踪语音帧并提供优先的队列处理。SVP要求语音帧必须被置于传送队列的最前面。接入点可以用不同的方式提供传送队列，重要的是其所提供的功能必须将语音帧移至传送队列的最前面。有些接入点可能只有一个传送队列，此时语音帧会被置于队列最前面。有些接入点会使用多个传送队列，其中将会有一个队列专门用来传送高优先级的语音帧。

利用帧的分段，无线局域网工作站可让干扰只影响较小的帧片段，而非较大的帧。通过降低可能被干扰的数据量，帧分段可以提高整体的有效吞吐量。当上层封包的大小超过

注2： 如果你打算在同一地点使用无绳电话（cordless phone）与无线局域网络（wireless LAN），建议可以在eBay上面买部900 MHz的无绳电话。

网络管理人员所设定的分段阈值（fragmentation threshold）时，就会进行帧的分段。每个帧片段（fragment）都有相同的帧序号（frame sequence number）以及一个递增的帧片段编号（fragment number）以便于重组。帧控制信息（frame control information）用来指示是否还有其他帧片段待收。构成整个帧的所有帧片段通常会在所谓的片段突发期（*fragmentation burst*）传送，如图 3-8 所示。其中包含了一个 RTS/CTS 交换过程，因为片段与RTS/CTS 阈值通常会被设定为相同的数值。此图同时显示了如何以NAV 与SIFS 的组合来控制媒介的访问。

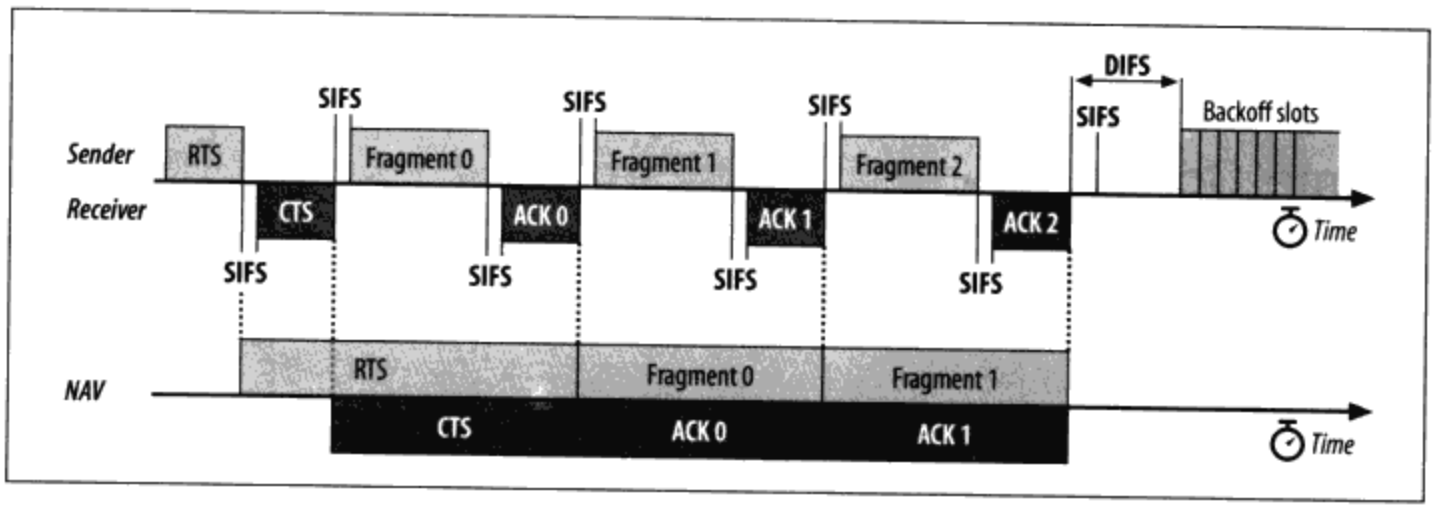


图 3-8：片段突发期（fragmentation burst）

帧片段与其确认之间以 SIFS 区隔，因此工作站在片段突发期（fragmentation burst）会一直持有信道的掌控权。NAV可确保其他工作站在此片段突发期间不使用该信道。正如任何的RTS/CTS 交换，RTS 与CTS 会将NAV 设定成从预定时间到第一个帧片段结束。其后的帧片段会彼此串联。每个帧片段都会设定NAV，继续掌握媒介的使用权，直到下一个帧的确认结束。图 3-8 中，Fragment 0 设定了 NAV 并继续掌控媒介直到 ACK 1，而Fragment 1 也设定了NAV 并继续掌控媒介直到 ACK 2，依此类推。当最后一个帧片段及其确认送出时，NAV 即会被设定为0，代表媒介即将在片段突发期完成之后释放。

帧格式

为迎接无线数据链路所带来的挑战，MAC被迫采用了许多特殊的功能，其中包括使用四个地址字段。并非每个帧都会用到所有的地址字段，这些地址字段的值也会因为MAC帧类型的不同而有所差异。不同类型的帧使用何种地址字段的细节会在第四章加以说明。图 3-9 展示了一般的 802.11 MAC 帧。本节所有图示均依循 IEEE 802.11 的格式。字段的传送顺序由左至右，最高有效位（most significant bit）将会最后出现。

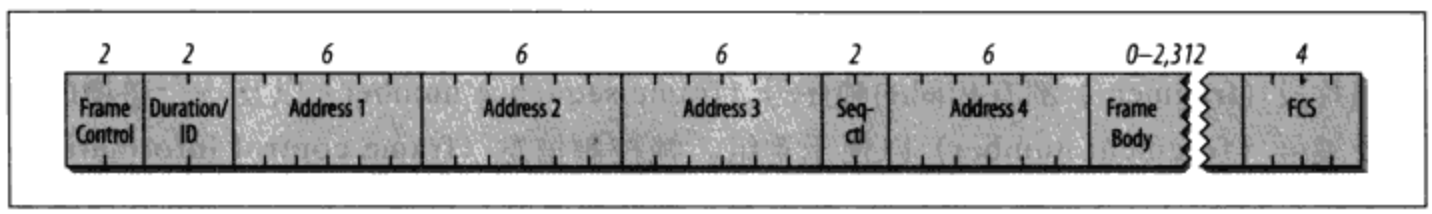


图3-9：一般的802.11 MAC帧

802.11 MAC帧并未包含Ethernet帧的某些典型功能，其中最显著的是type/length字段以及preamble（前导码）。preamble属于物理层，而封装细节（如type与length）则出现在802.11帧所携带的标头（header）中。

Frame Control字段

所有帧的开头均是长为两个字节的Frame Control（帧控制）字段，如图3-10所示。Frame Control字段包括以下子字段：

Protocol 字段

Protocol（协议版本）字段由两位构成，用以显示该帧所使用的MAC版本。目前，802.11 MAC只有一个版本，它的协议编号为0。如果IEEE将来推出不同于原始规范的MAC版本，才会出现其他的版本编号。到目前为止，802.11改版尚不需用到新的协议编号。

Type 与 Subtype 字段

Type（类型）与Subtype（子类型）字段用来指定使用的帧类型。为了因应噪声与提升可靠性，802.11 MAC内置了一些管理功能。有些功能之前已经提过，如RTS/CTS操作与确认（acknowledgment）。表3-1显示了Type与Subtype字段跟帧类型的对应关系。

如表3-1所示，最高有效位会最先出现，恰好与图3-10相反。因此，Type子字段是frame control字段的第三位之后的第二个位（b3 b2），而Subtype子字段则是第七位之后的第六、第五以及第四位（b7 b6 b5 b4）。

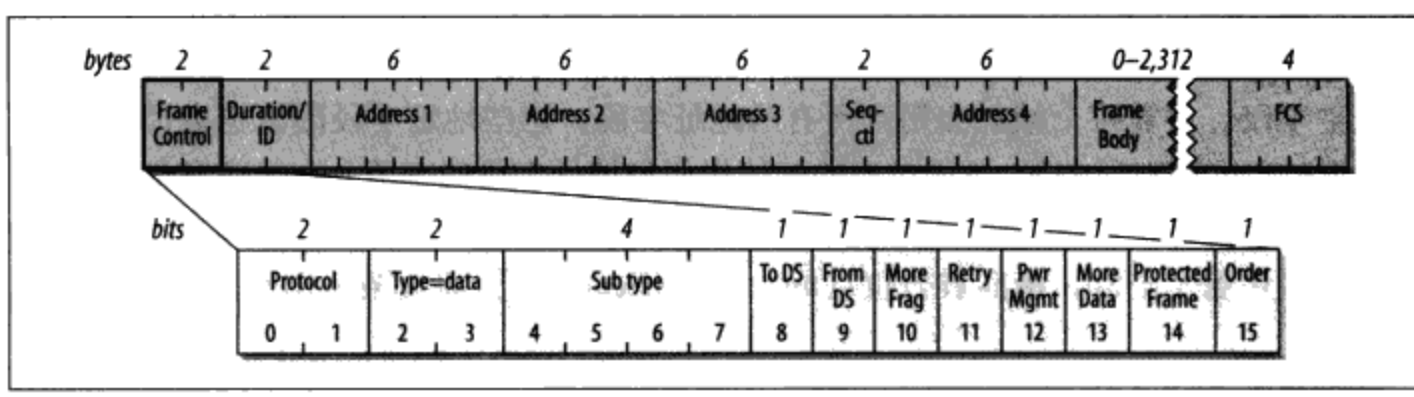


图3-10：Frame Control字段

表3-1：Type 与Subtype 字段的值与名称

Subtype 的值	Subtype 的名称
Management frame（管理帧：Type=00）[a]	
0000	Association request（关联请求）
0001	Association response（关联响应）
0010	Reassociation request（重新关联请求）
0011	Reassociation response（重新关联响应）
0100	Probe request（探测请求）
0101	Probe response（探测响应）
1000	Beacon（信标）
1001	ATIM（通知传输指示消息）
1010	Disassociation（取消关联）
1011	Authentication（身份验证）
1100	Deauthentication（解除身份验证）
Control frame（控制帧：Type=01）[b]	
1010	Power Save (PS)-Poll（省电－轮询）
1011	RTS（请求发送）
1100	CTS（清除发送）
1101	ACK（确认）
1110	CF-End（无竞争周期结束）
1111	CF-End（无竞争周期结束）+CF-ACK（无竞争周期确认）
Data frame（数据帧：Type=10）[c]	
0000	Data（数据）
0001	Data+ CF-ACK
0010	Data+ CF-Poll
0011	Data+ CF-ACK+CF-Poll
0100	Null data（无数据：未传送数据）
0101	CF-ACK（未传送数据）
0110	CF-Poll（未传送数据）
0111	Data+ CF-ACK + CF-Poll
1000	QoS Data[c]
1001	QoS Data + CF-ACK[c]

表3-1：Type与Subtype字段的值与名称（续）

Subtype 的值	Subtype 的名称
1010	QoS Data + CF-Poll[c]
1011	QoS Data + CF-ACK + CF-Poll[c]
1100	QoS Null（未传送数据）[c]
1101	QoS CF-ACK（未传送数据）[c]
1110	QoS CF-Poll（未传送数据）[c]
1111	QoS CF-ACK+CF-Poll（未传送数据）[c]
（帧类型11尚未使用）	

a: 管理帧的Subtype值0110~0111与1101~1111目前并未使用。

b: 控制帧的Subtype值0000~1001目前并未使用。

c: 由802.11e任务小组提议，但尚未标准化。注意这些帧均以1开头，因此有人称第一个位为QoS位。

To DS与From DS位

这两个位用来指示帧的目的地是否为分布式系统（distribution system）。在基础结构型网络里，每个帧都会设定其中一个DS位。你可以根据表3-2来解读这两个位。第四章将会说明地址字段的解读取决于这两个位的设定。

表3-2：To DS与From DS位所代表的意义

	To DS=0	To DS=1
From DS=0	所有管理与控制帧。IBSS里的数据帧（非基础结构型数据帧）	基础结构型网络里无线工作站所传送的数据帧
From DS=1	基础结构型网络里无线工作站所收到的数据帧	无线桥接器上的数据帧

More fragments位

此位的功能类似IP的“more fragments”位。若较上层的封包经过MAC分段处理，除了最后一个片段，其他片段均会将此位设定为1。大型的数据帧以及某些管理帧可能需要加以分段，除此之外的其他帧则会将此位设定为0。实际上，大多数数据帧均会以最大的Ethernet大小进行传送，不过帧分段并不常用。

Retry位

有时候可能需要重传帧。任何重传的帧会将此位设定为1以协助接收端剔除重复的帧。

Power management 位

802.11 网络适配器通常以 PC Card 的形式出现，主要用于以电池供电的膝上型或手持式计算机。为了延长电池的使用时间，通常可以关闭网络接口以节省电力。此位用来指出发送端在完成当前的原子帧交换之后是否进入省电（power-save）模式。1 代表工作站即将进入省电模式，而0则代表工作站会一直保持在清醒状态。接入点必须行使一系列重要的管理功能，所以不允许进入省电模式，因此接入点所传送的帧中此位必然为0。

More data 位

为了服务处于省电模式中的工作站，接入点会将这些从分布式系统接收来的帧加以缓存。接入点如果设定此位，即代表至少有一个帧待传给休眠中的工作站。

Protected Frame 位

相对于固定式网络，无线传送本质上就比较容易被拦截。如果帧受到链路层安全协议的保护，则此位会被设定为1，而且该帧会略有不同。之前，Protected Frame 位被称为 WEP 位。

Order 位

帧与帧片段可依次传送，不过发送端与接收端的MAC 必须付出额外的代价。一旦进行严格依次（strict ordering）传送，则此位会被设定为 1。

Duration/ID 字段

Duration/ID 字段紧跟在 Frame Control 字段之后。此字段有许多功用，有三种可能的形式，如图 3-11 所示。

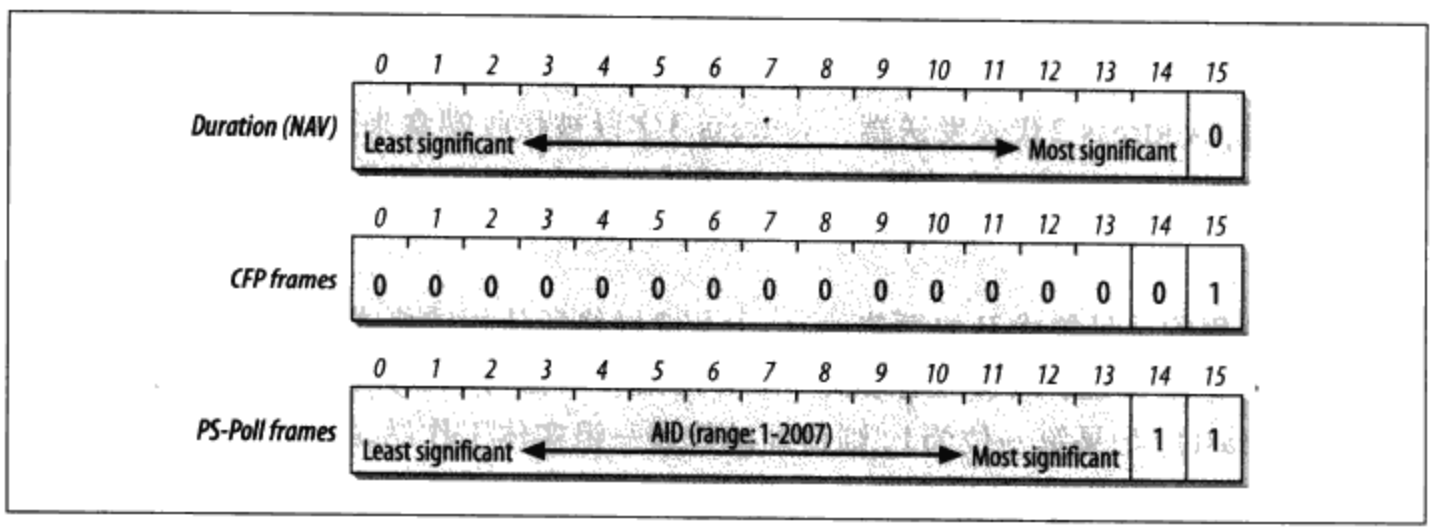


图 3-11：Duration/ID 字段

Duration：设定 NAV

当第15个位被设定为0时，Duration/ID字段就会被用来设定NAV。此数值代表当前所进行的传送预计使用媒介多少微秒。工作站必须监视所收到的任何帧头并据此更新NAV。任何超出预计使用媒介时间的数值均会更新NAV，同时阻止其他工作站访问媒介。

无竞争周期所传送的帧

在无竞争周期（contention-free period，简称CFP），第14位为0，而第15位为1，其他所有位均为0，因此Duration/ID字段的值为32768。这个数值被解读为NAV。它让没有收到Beacon（信标）帧（注3）的任何工作站都得以公告无竞争周期，以便将NAV更新为适当的数值，从而避免干扰到无竞争传送。

PS-Poll 帧

在PS-Poll（省电－轮询）帧中，第14位与第15位会被同时设定为1。移动式工作站可以关闭天线以达到省电目的。休眠中的工作站必须定期醒来。为确保不遗漏任何帧，从休眠状态醒来的工作站必须送出一个PS-Poll帧，以便从接入点取得之前缓存的任何帧。此外，苏醒的工作站会在PS-Poll帧中加入关联标识符（association ID，简称AID），以显示其所隶属的BSS。AID包含在PS-Poll帧中，其值介于1~2007，而介于2008~16383的值目前并未使用。

Address 字段

一个802.11帧最多可以包含4个地址（Address）字段。这些地址字段均经过编号，因为随着帧类型的不同，这些字段的作用也有所差异（详见第四章）。基本上，Address 1代表接收端、Address 2代表发送端、Address 3字段被接收端拿来过滤地址。举例而言，在基础结构型网络里，第三个地址字段会被接收端用来判断该帧是否属于其所关联的网络（注4）。

802.11所使用的寻址模式乃依循其他IEEE 802网络所使用的格式，包括Ethernet。地址本身的长度有48位。如果传送给实际媒介的第一个位为0，则该地址代表单一工作站（单播，unicast）。如果第一位为1，则该地址代表一组实体工作站，称为组播（multicast）

注3： Beacon帧是管理帧的子类型（subtype），因此首字母以大写表示。

注4： 802.11规定工作站应该忽略那些不属于相同BSSID的帧，不过大多数产品并未正确实现BSSID的过滤功能，还是会将接收到的所有帧传给上层协议。

地址。如果所有位均为1，该帧即属广播（broadcast），因此会传送给所有连接至无线媒介的工作站。

这些长为48位的地址有各种不同的用途：

目的地地址

和Ethernet一样，目的地地址（destination address）是长为48位的IEEE MAC标识符，代表最后的接收端，即负责将帧交付上层协议处理的工作站。

来源地址

这是长为48位的IEEE MAC标识符，代表传送的来源。每个帧只能来自单一工作站，因此Individual/Group位必然为0，代表来源地址（source address）为单一工作站。

接收端地址

这是长为48位的IEEE MAC标识符，代表负责处理该帧的无线工作站。如果是无线工作站，接收端地址（receiver address）即为目的地地址（destination address）。如果帧的目的地是与接入点相连的Ethernet节点，接收端即为接入点的无线接口，而目的地地址可能是接至Ethernet的一部路由器。

发送端地址

这是长为48位的IEEE MAC标识符，代表将帧传送至无线媒介的无线接口。发送端地址（transmitter address）通常只用于无线桥接。

基本服务集标识符（BSSID）

要在同一区域划分不同的无线局域网络，可以为工作站指定所要使用的BSS（基本服务集）。在基础结构型（infrastructure）网络里，BSSID（基本服务集标识符）即是接入点无线接口所使用的MAC地址。而独立型（ad hoc）网络则会产生一个随机的BSSID并将Universal/Local位设定为1，以防止与其他官方指定的MAC地址产生冲突。

要使用多少地址字段取决于帧类型。大部分的数据帧会用到3个字段：来源、目的地以及BSSID。数据帧中，地址字段的编号与排列方式取决于帧的传送路径。大部分的传送只会用到3个地址，这解释了为什么在帧格式中4个地址字段只有其中3个字段是相邻的。

顺序控制（Sequence Control）字段

此字段的长度为16位，用来重组帧片段以及丢弃重复帧。它是由4位的片段编号（fragment number）字段以及12位的顺序编号（sequence number）字段组成，如图3-12所示。控制帧未使用顺序编号，因此并无Sequence Control字段。

当上层帧交付给MAC传送时，会被赋予一个顺序编号。此字段的作用相当于已传帧的计数器取4096的模数（modulo）。此计数器从0起算，MAC每处理一个上层封包它就会累加1。如果上层封包被分段处理，则所有帧片段都会具有相同的顺序编号。如果是重传帧，则顺序编号不会有任何改变。

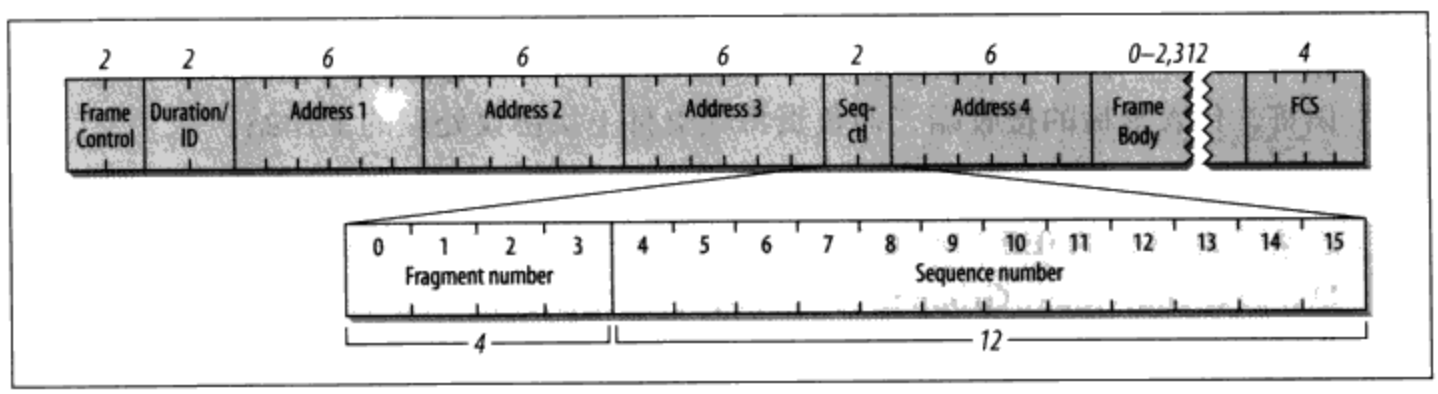


图3-12：Sequence Control字段

帧片段之间的差异在于片段编号。第一个片段的编号为0，其后每个片段的编号依序累加1。重传的片段编号会保持原始的顺序编号以协助重组。

具备QoS扩展功能的工作站对Sequence Control字段的解读稍有不同，因为这类工作站必须同时维护多组传送队列。

帧主体

帧主体（frame body）也称为数据字段（Data field），负责在工作站之间传递上层有效载荷（payload）。在最初制定的规范中，802.11帧最多可以传送2304个字节的有效载荷（实现时必须能够容纳更多数据，以便将安全性与QoS相关标头纳入其中）。802.2 LLC标头具有8个字节，最多可以传送2296个字节的网络协议有效载荷。防止分段必须在协议层加以处理。在IP网络中，Path MTU Discovery（路径最大传输单元找寻，RFC 1191）可阻止大于1500个字节的帧的传送。

802.11与其他链路层技术不同之处表现在两个显著的方面。首先，在802.11帧中并无任何上层协议的标记（tag）可供区别。上层协议是以额外标头的type字段加以标记，同时以之作为802.11有效载荷的开始。其次，802.11通常不会将帧填补至最小长度。802.11所使用的帧并不大，随着芯片与电子技术的发展，目前已经没有填补的必要。

帧校验序列（FCS）

和Ethernet一样，802.11帧也是以帧校验序列（frame check sequence，简称FCS）结束。FCS通常被视为循环冗余校验（cyclic redundancy check，简称CRC）码，因为底

层的数学运算相同。FCS让工作站能够检查所收到的帧的完整性。FCS的计算范围涵盖MAC标头里所有字段以及帧主体。虽然802.3与802.11计算FCS的方法相同，不过802.11所使用的MAC标头与802.3不同，因此接入点必须重新计算FCS。

当帧送至无线接口时会先计算FCS，然后再经RF或IR链路传送出去。接收端随后会为收到的帧计算FCS，然后与记录在帧中的FCS进行比较。如果两者相符，则该帧极有可能在传送过程中未受损。

在Ethernet上，如果帧的FCS有误则随即予以丢弃，否则就传递给上层协议处理。在802.11网络上，通过完整性校验的帧还需要接收端送出确认。例如，接收正确数据的帧必须得到肯定确认，否则就必须重传。对于未能通过FCS校验的帧，802.11并未提供否定确认机制，在重传之前，工作站必须等候确认逾时。

802.11对上层协议的封装

和所有其他的802链路层（link layer）一样，802.11可以传送各种不同的网络层协议（network-layer protocol）。和Ethernet不同的是，802.11是以802.2的逻辑链路控制（logical-link control，简称LLC）封装来携带上层协议。图3-13显示了如何以802.2 LLC封装来携带IP封包。如图3-13所示，802.1h与RFC 1042所使用的MAC标头长度为12个字节，其内容为Ethernet上的来源MAC地址与目的MAC地址，或者是前面所提到的长802.11 MAC标头。

传送时，用来封装LLC数据的方式有两种，一种是RFC 1042所描述的方式，另外一种则是802.1H所规范的方式。两种标准各自有其别名，RFC 1042有时候被称为*IETF*封装，而802.1H有时候则被称为隧道封装（tunnel encapsulation）。

这两种方式十分相似，如图3-13所示。此图最上方为Ethernet帧，它具有MAC标头（由来源与目的MAC地址组成）、类型代码（type code）、嵌套封包（embedded packet）以及帧检查（frame check）等字段。在IP领域里，Type code不是代表IP本身的0x0800（十进制的2048），就是代表地址解析协议（Address Resolution Protocol，简称ARP）的0x0806（十进制的2054）。

RFC 1042与802.1H均衍生自802.2的子网访问协议（sub-network access protocol，简称SNAP）。MAC地址会被复制到封装帧（encapsulation frame）的开头，然后插入SNAP标头。SNAP标头以目的地服务接入点（*destination service access point*，简称DSAP）与源服务接入点（*source service access* point，简称SSAP）开始。在地址之后，SNAP包含了一个控制（Control）字段。和高层数据链路协议（high-level data link control，简称HDLC）及其衍生协议一样，此控制字段会被设定为0x03，代表未编号信息

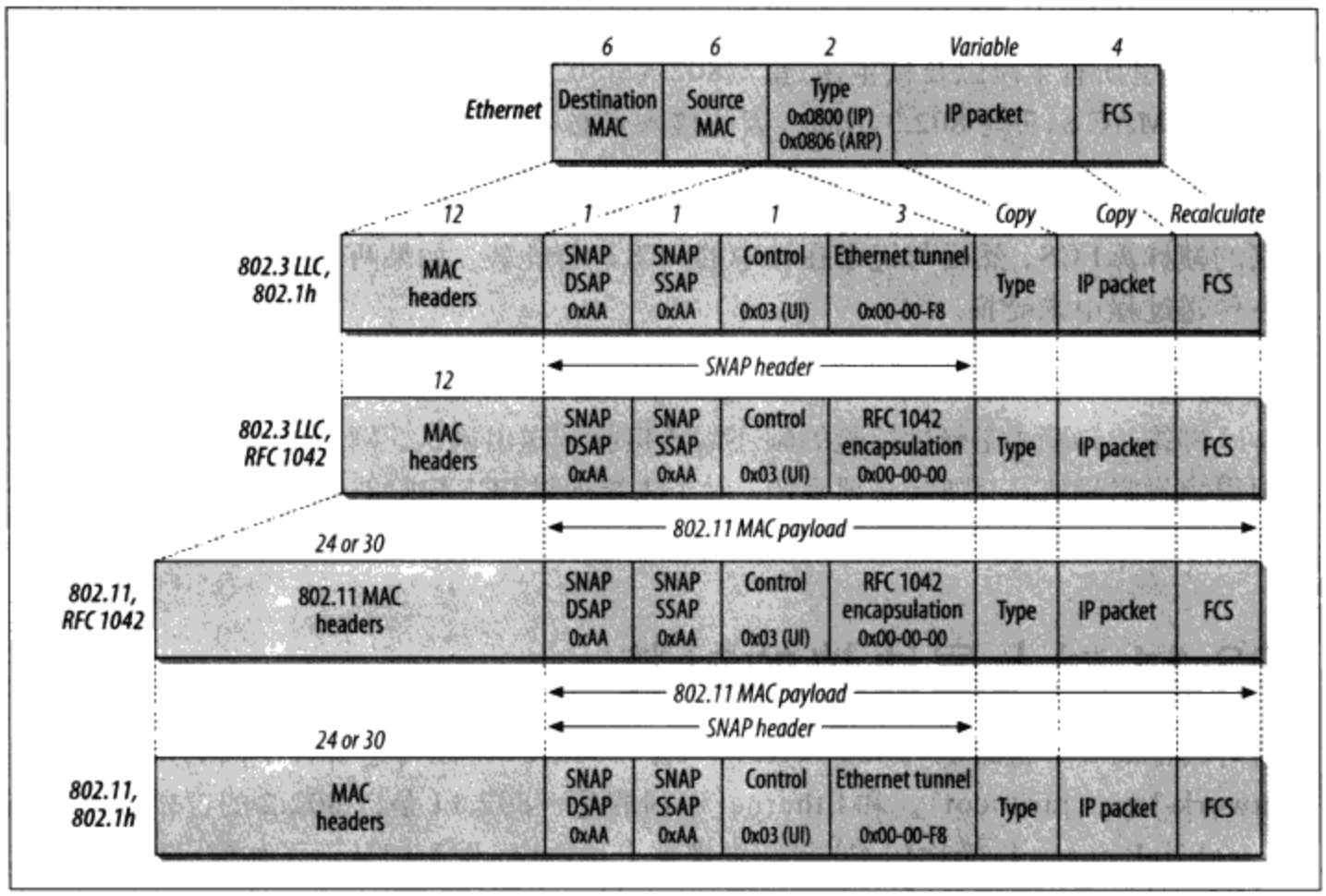


图3-13：802.11里的IP封装

(unnumbered information，简称UI)，是映射到IP datagram所谓的尽力传递(best-effort delivery）的范畴。SNAP所置入的最后一个字段是组织唯一标识符（organizationally unique identifier，简称OUI)。起初，IEEE希望用一个字节的服务接入点来涵盖网络协议编号，不过后来证明这种想法过于乐观。因此，SNAP只得从原本的Ethernet帧复制一份类型代码(type code)。802.1H与RFC 1042之间的唯一差异在于其所使用的OUI。

有些产品可以让用户在两种封装标准之间进行切换，虽然这种功能并不常见。以Microsoft操作系统而言，AppleTalk与IPX协议栈默认使用802.1H，其他协议则使用RFC 1042。目前大部分接入点均依循Microsoft的做法，不再提供封装方式的切换选项。事实上，由于Microsoft所实行的封装方式得到广泛的支持，因此Wi-Fi联盟的认证测试项目也将之包含在内。

基于竞争的数据服务

为了提高可靠性，802.11纳入了许多额外的功能。这些功能导致某些规则的混乱，因而无法判断何时该允许使用何种类型的帧。这些额外的功能也让网络管理人员更难预测哪

些帧会往来于所查看的网络中。本节的目的在于厘清802.11局域网中负责运送数据的原子交换过程（atomic exchange）。（大部分的管理帧只会声明给该区域中相关的对象，信息的传递纯粹是单向的。）

本节所陈述的是原子交换过程，也就是说数据的交换过程必须被视为单一整体。举例而言，单播（unicast）数据必须得到确认以确保数据传送无误。虽然整个数据的交换过程包含两个帧，但数据交换本身只是单一操作。只要有一方失误，整个操作就必须重新来过。802.11 定义了两组截然不同的原子交换过程。其一为 DCF，用于基于竞争的服务（contention-based service），详见本章。第二种交换方式为 PCF，用于无竞争服务（contention-free service）。无竞争服务所使用的帧交换方式不仅错综复杂，而且难以理解。鉴于商业化产品很少实现无竞争服务，其交换过程不再赘述。

DCF 使用的帧交换方式在 802.11 MAC 中占有决定性的地位。根据 DCF 的规定，所有的产品都必须提供尽力传递的功能。为了实现基于竞争的MAC，处于作用状态的工作站必须处理每个帧的MAC标头。整个帧交换过程从某个工作站在DIFS之后取得闲置媒介的使用权时开始。

广播与组播数据或管理帧

广播与组播帧的交换过程最为简单，因为这些帧无需响应。这两种帧也可以视为组帧（group frame），因为其接收对象不限于单一工作站。成帧（framing）与寻址（addressing）在 802.11 中较为复杂，适用此规则的帧的类型如下所示：

- 广播数据帧会在 Address1 字段中填入广播地址
- 组播数据帧会在 Address1 字段中填入组播地址
- 广播管理帧会在Address1字段中填入广播地址（Beacon、Probe Request以及IBSS ATIM 帧）

组播帧无法分段，也无需得到确认。整个原子交换过程只牵涉到一个帧，根据基于竞争的访问控制（contention-based access control）规则加以传送。传送结束后，所有工作站必须等待一段DIFS，然后在竞争窗口（contention window）倒数随机产生的延迟时间。

因为帧的交换过程只牵涉到一个帧，所以将NAV（网络分配矢量）设定为0。既然此后已无其他帧，也就不必使用虚拟载波监听来锁定媒介以防止其他工作站的访问。传送该帧之后，所有工作站均会等候一段 DIFS，然后通过竞争窗口（contention window）开始为任何被延迟的帧进行倒数。整个交换过程详见图 3-14。

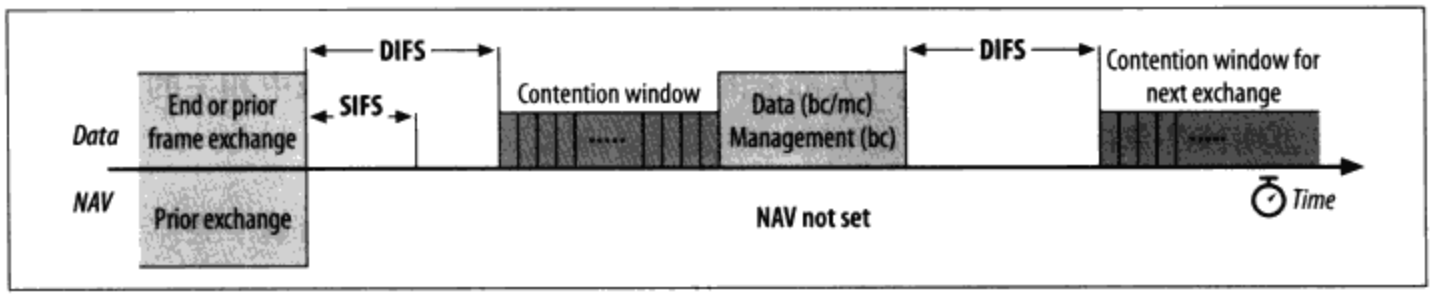


图 3-14：广播 / 组播数据以及广播管理的基本帧交换过程

因环境而异，组播帧可能会遇到劣质的服务质量，因为这些帧没有得到任何确认。所以有些工作站可能会遗漏广播或组播流量，不过 MAC 并未内置任何机制可用来重传广播或组播帧。

单播帧

在 802.11 标准中，针对个别工作站所传送的帧称为直接数据（direct data）。本书使用较通俗的词，称之为单播（*unicast*）。单播帧必须得到确认以确保可靠性，也意味着可借助各种机制来改善传送效率。本节所描述的交换过程适用于任何单播帧，因此也适用于管理帧与数据帧。实际上，这些操作通常只用于数据帧。

基本的肯定确认（最后一个片段）

两个工作站之间的传送可靠性建立在简单的肯定确认上。单播数据帧必须得到肯定确认，否则该帧即会被认定为已经遗失。单一帧及其确认是最基本的例子，如图 3-15 所示。

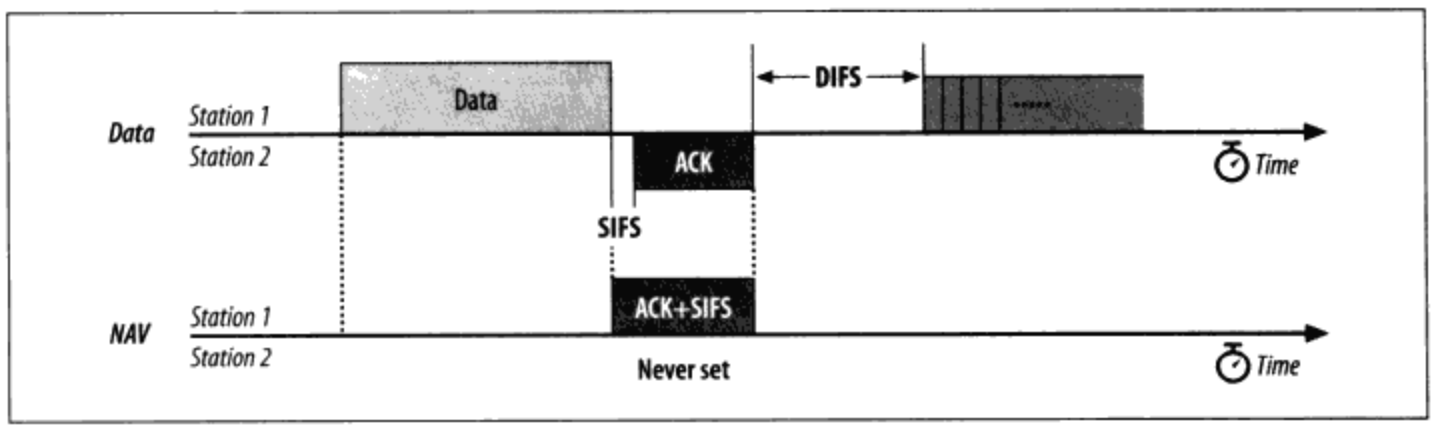


图 3-15：数据的基本肯定确认

此帧会利用 NAV 为其本身、其确认及发生于其间的 SIFS 预订媒介使用权。设定较长的 NAV 是为了替整个交换过程锁定虚拟载波，以保证接收端可以传送确认。因为此交换过程是以 ACK 结束，所以没有必要再锁定虚拟载波，因此该 ACK 中的 NAV 会被设定为 0。

帧分段

包括 IP 在内，一些较上层的网络协议或多或少都会用到帧分段（fragmentation）。在网络层（network-layer）进行分段的缺点是接收端必须重组；如果帧在传送过程中遗失，整个封包就必须重传。在链路层（link layer）使用分段机制可以提升速度，即以较小的 MTU 在跳跃点（hop）间传送数据（注 5）。此外，802.11 可以利用帧分段来避免干扰。无线电波干扰通常会以瞬间且高能量的突波形式出现，而且经常与 AC 电源线同步。将帧加以分段可保护大部分帧不会被损坏。基本分段机制如图 3-16 所示。

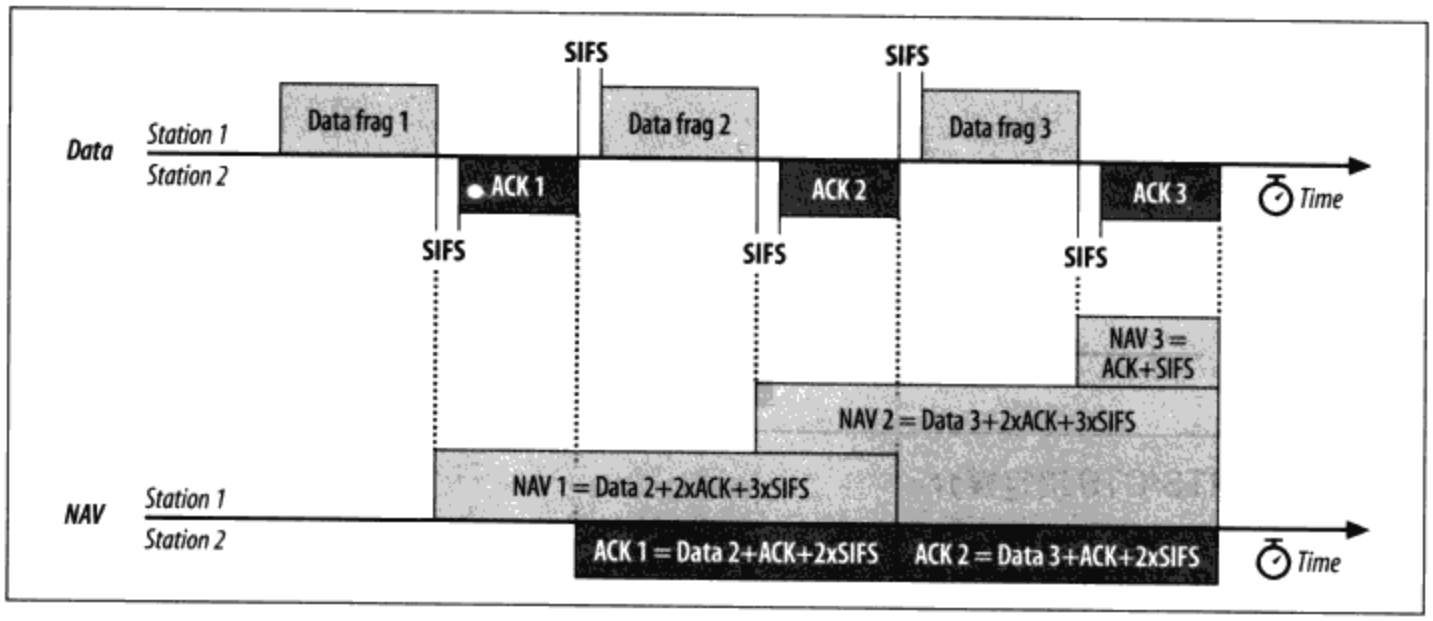


图 3-16：帧分段

最后两个帧的交换和之前的过程没有两样，NAV的设定也完全相同。不过，倒数第二个帧之前的所有帧均会使用NAV为下一个帧锁定媒介。第一个数据帧会将NAV的时间设定至足以涵盖 ACK1、下一个帧片段及其确认（ACK2）。为了表示是帧片段，MAC 会将帧头的控制字段的 More Fragments 位设定为 1。最后一个确认（ACK3）除外，其余确认都会继续为下一个数据片段及其确认延长锁定媒介的时间。后续的数据帧会继续延长NAV以涵盖后续的确认，直到最后一个数据帧才会将More Fragments 位设定为0，而最后一个确认（ACK3）则会将NAV 设定为0。帧片段的数量并无限制，不过帧的总长度必须短于 PHY 对交换过程所做的限制。

帧分段是由MAC的分段阈值（fragmentation threshold）参数控制。大部分的网卡驱动程序都允许用户设定此参数。任何超过分段阈值的帧都会被分段，分段方式因具体实现而异。调高分段阈值意味着帧的传送负担较小，不过帧遗失与损坏的成本较高，因为将会有较多的数据必须丢弃与重传。调低分段阈值意味着传送负担较重，不过在面临较恶劣的环境时，这种做法可以提供较好的稳定性。

注 5：　多链路点对点协议（Multi-link PPP；RFC 1990）所采用的方式。

RTS/CTS

为保证媒介使用权以及数据传送不被中断，工作站可使用RTS/CTS的交换方式。图3-17说明了整个过程。RTS/CTS交换的做法和帧分段没有什么两样，只是RTS帧并未携带任何数据。RTS中的NAV可让CTS完成操作，而CTS则可用来为数据帧保留媒介使用权。

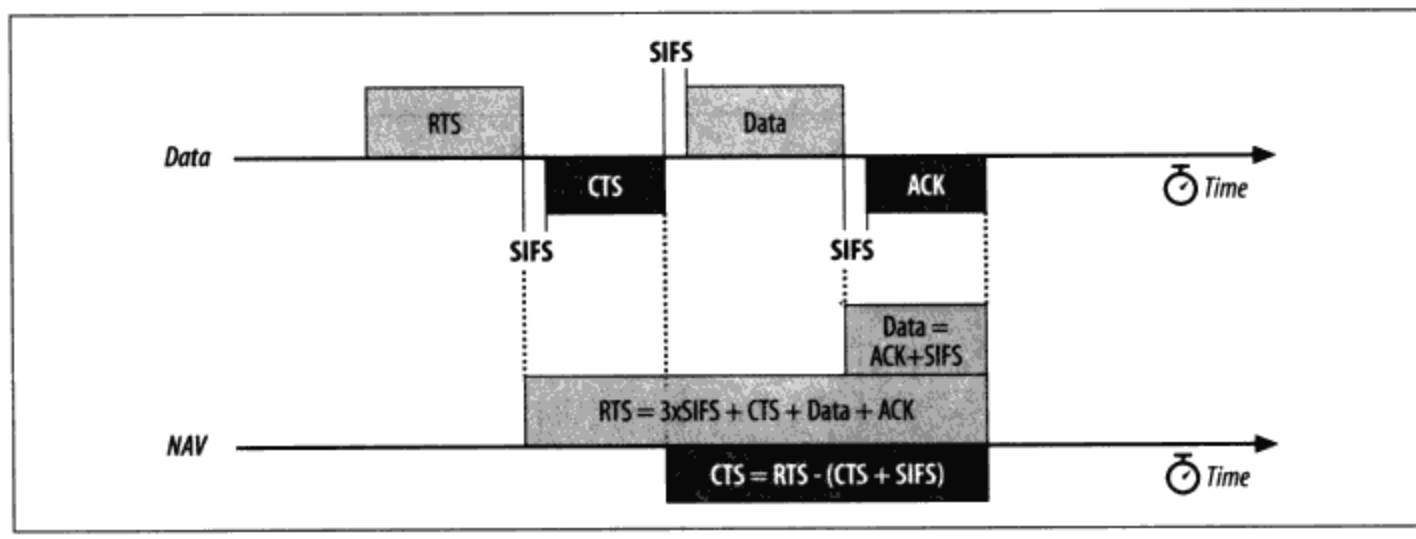


图3-17：以RTS/CTS锁定媒介

RTS/CTS可用在所有的帧交换、非帧交换或介于两者之间。和帧分段一样，RTS/CTS是由驱动程序中的阈值来控制的。超过该阈值的帧由RTS/CTS先行清空媒介，而较小的帧则被直接传送。

RTS/CTS与帧分段

实际上，RTS/CTS交换通常与帧分段并行（图3-18）。虽然经过分段，帧片段还是有一定的长度，因此可受惠于RTS/CTS过程所确保的媒介独家使用权，免于隐藏节点的竞争。有些厂商将帧分段阈值与RTS/CTS阈值的默认值设成一样。

省电程序（Powersaving Sequence）

在RF系统中，放大器是最耗电的组件，它负责将送出的信号放大并将收到的信号放大至可处理的水平。802.11工作站可以关闭无线电波收发器并且定期进入休眠状态，以维持最长的电池使用时间。在休眠期间，接入点会为每个处于休眠状态的工作站缓存单播帧。若有缓存帧，接入点会由后续的Beacon帧告知工作站。从省电状态苏醒的工作站可以使用PS-Poll帧取得这些缓存帧。

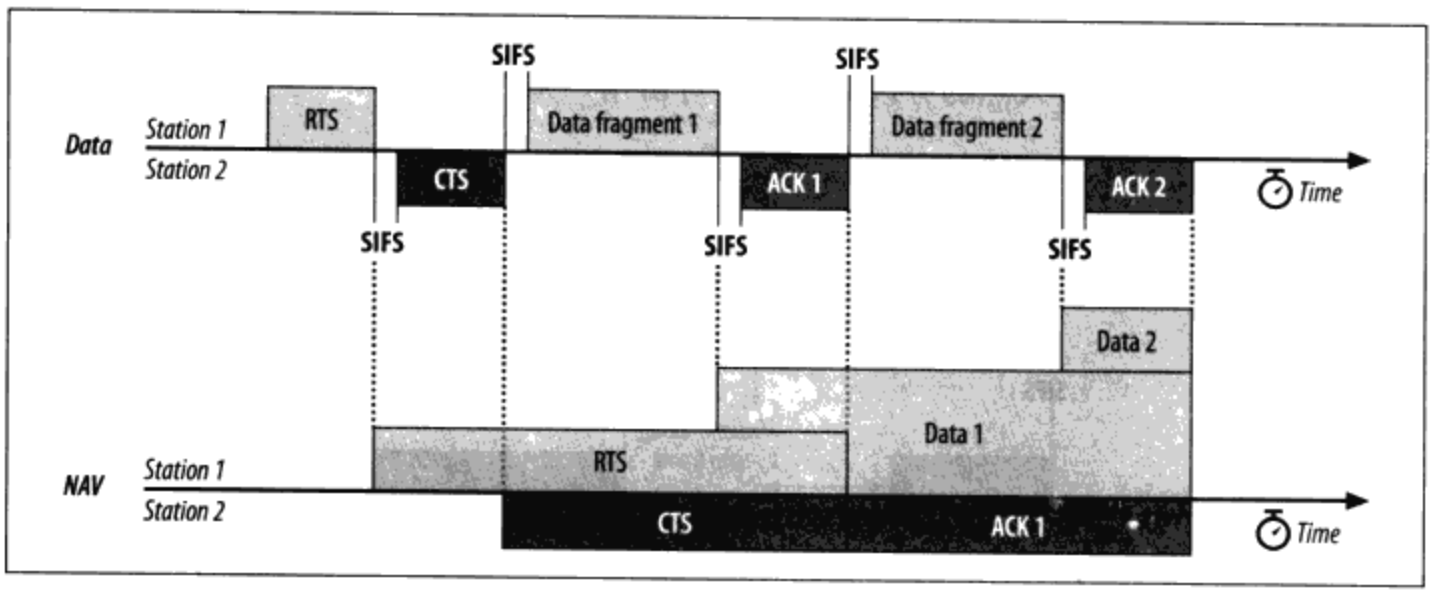


图 3-18：RTS/CTS 与帧分段

接收到 PS-Poll 帧的接入点可以立即采取响应，也可以等到环境许可、比较空闲时再予以响应。有时候，采用哪种 PS-Poll 响应由接入点所采用的芯片组的厂商决定。有些芯片组厂商同时支持两种模式，有些则只支持一种。802.11 只要求支持一种方式即可，因此两种做法均符合标准要求。

立即响应

接入点可以对 PS-Poll（省电－轮询）帧立即作出响应。经过一段 SIFS（短帧间间隔），接入点即可传送帧。如图 3-19 所示，PS-Poll 帧隐含了 NAV。PS-Poll 帧的 Duration/ID 字段中包含了 Association ID（关联标识符），因此接入点可以判断哪些帧是为该工作站所缓存的。不过，MAC 规范说明书要求所有收到 PS-Poll 的工作站都必须更新 NAV，将 NAV 的值设定为一个 SIFS（短帧间间隔）加上一个 ACK。虽然此 NAV 对数据帧而言过短，但接入点会取得媒介使用权，而所有工作站都会为了这个数据帧而延迟访问媒介。当数据帧传送结束时，NAV 随即更新以反映该数据帧头中的数值。

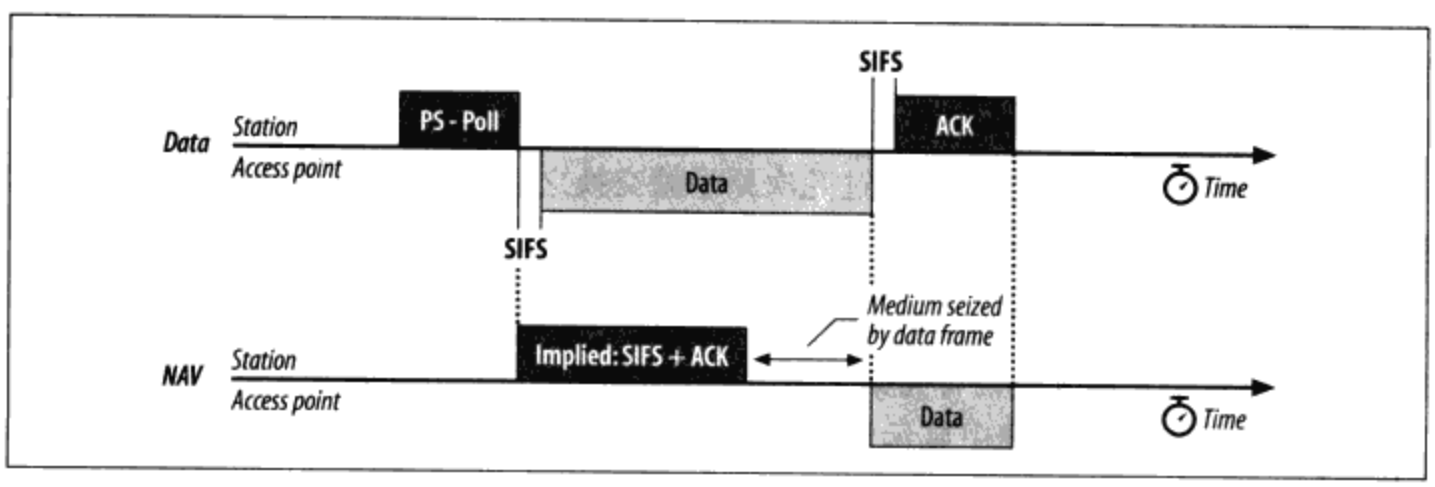


图 3-19：立即的 PS-Poll 响应

如果缓存的帧过大，则必须进行分段。图3-20说明了帧分段情况下的PS-Poll立即响应。和其他工作站一样，接入点的分段阈值通常可由用户来设定。

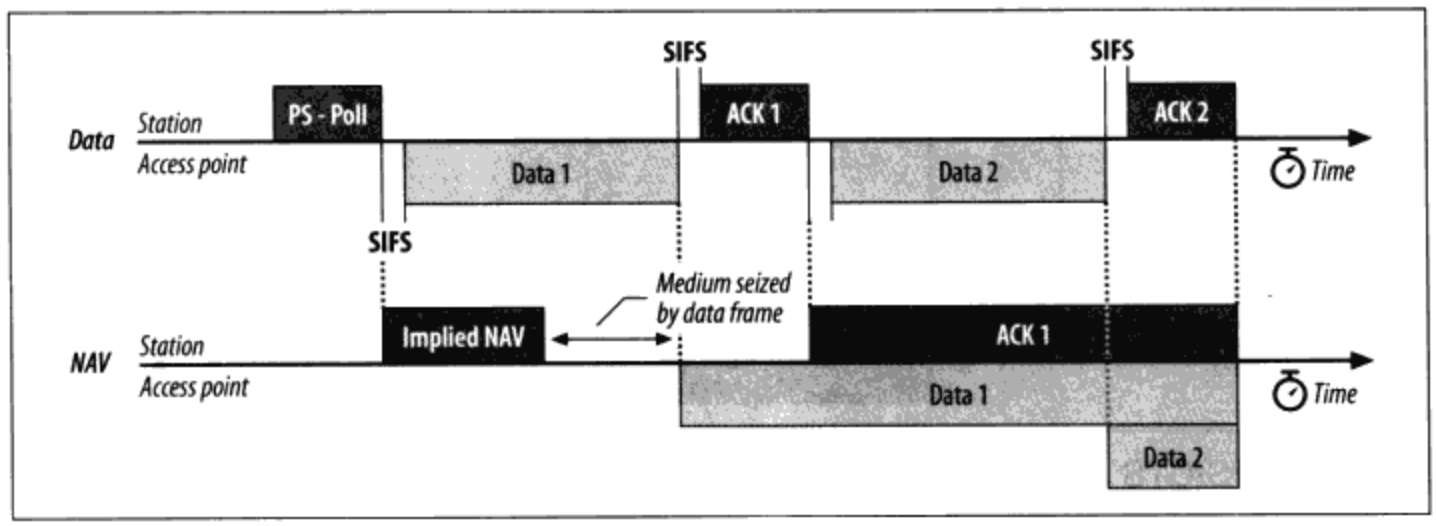


图3-20：帧分段情况下的PS-Poll立即响应

延迟响应

除了立即响应，接入点可以先回复一个简单响应。这种做法称为延迟响应（deferred response），因为接入点虽然响应了访问缓存帧的请求，但并未立即采取实际的发送行动。使用延迟响应的优点之一在于接入点方面的软件较易实现，因为确认信息可以通过芯片组固件立即传送，至于数据则可以先予以缓存，然后依正常流程传送。

通过PS-Poll请求帧的工作站必须保持清醒，直到该帧传送完成。不过，在基于竞争的服务期间，接入点可以在任何时间点传送帧。此时工作站不能返回省电模式，除非接收到一个Beacon帧，其中对应至该工作站的TIM（traffic indication map，传输指示映射）位已被清除。

图3-21说明了整个过程。此图中，工作站刚从省电模式转变为活跃模式（active mode），同时注意到接入点已经为它缓存了帧。于是工作站会发出PS-Poll给接入点，要求接收这些缓存帧。不过，接入点可能会选择延迟响应，因此只响应了一个ACK。到目前为止，接入点已经确认了工作站的缓存帧的请求，并且承诺即将在某个时间点加以传送。工作站必须在活跃模式下等候，也许经过几次原子帧交换之后，接入点就会送出工作站所要的数据。虽然在图3-21中并未显示，不过缓存帧还是有可能被分段的。

收到数据帧之后，工作站还必须停留在清醒状态，直到下一个Beacon帧被传送出来。Beacon帧只是用来提醒是否有为某个工作站缓存的帧，没有办法告知实际的帧数量。一旦工作站收到的Beacon帧中显示已无缓存帧，便可断定已经完成缓存帧的接收，然后返回省电模式。

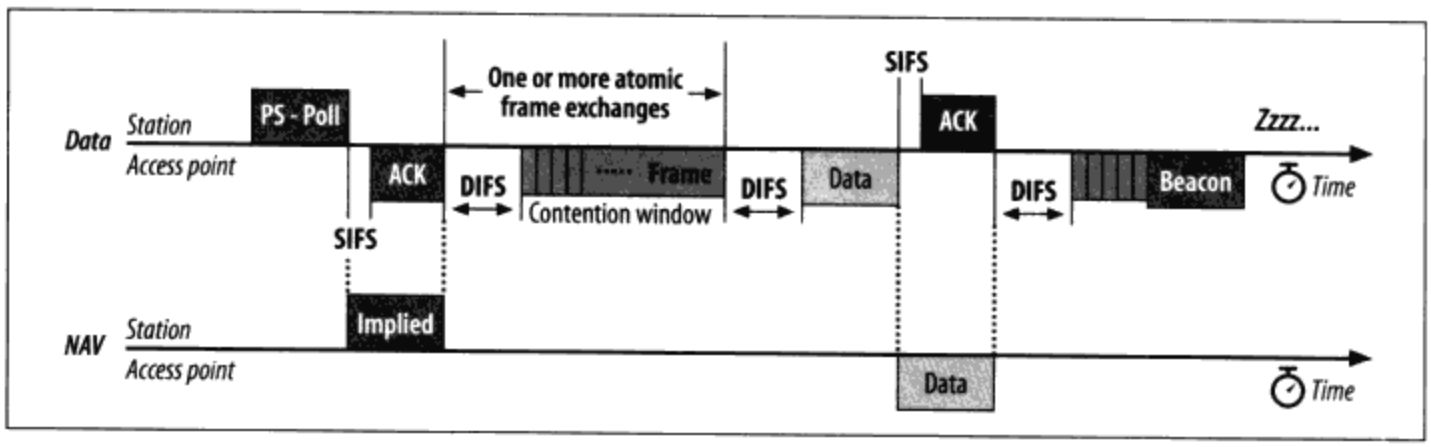


图 3-21：PS-Poll 延迟响应的范例

多种速率支持

能够以不同速度操作的网络技术必须具备一种机制，可以协商出一种收发端彼此均可接受的数据传送速率。速度协商对工作站而言尤其方便。工作站可以经常变换速度，以适应无线电波环境的快速变动。当工作站间的距离改变时，速度也会随之变动。工作站必须能够适应随时变动的环境，必要时更改传送速率。和一些其他协议功能一样，802.11 标准并未规范该如何选择传送速率。标准只是提出一般原则，在实现上厂商中享有相当大的自由。其中，有些通则适用于所有工作站：

1. 每个工作站均持有一份操作速率（operational rate）列表，其中记录工作站与所连接BSS 均支持的所有速率。（所谓BSS，通常相当于一个接入点，不过较新的产品可以让用户根据虚拟接入点自定义操作速率。）高于操作速率集的传送速率是不允许用来传送帧的。

2. 每个 BSS 必须负责维护一组基本速率，即打算加入此 BSS 的工作站所必须支持的速率列表。任何传送至组接收地址的帧必须以基本速率传送，以确保所有工作站均可正确解读。

3. 用来开始帧交换的控制帧，如 RTS 与 CTS，必须以基本速率集中的一种速率来进行传送。此规则可以确保必须以 CTS 响应 RTS 帧的工作站能够以相同速率操作。

   — 控制帧可以用于向下兼容（backward-compatiblity）模式，又称为防护（protection）模式，参见第十四章。防护模式是为了避免新旧工作站之间相互干扰，因为较旧的工作站或许只支持较慢的电波调制，新式工作站却可以使用较快的调制方式。如果所在地区的有些工作站不支持较新的调制方式，则必须以较旧的调制方式传送防护帧（protection frame）。

4. 发送给特定工作站的帧会在 Address 1 字段记载单播目的地地址。单播帧（unicast frame）可以使用目的端支持的任一速率传送。至于数据速率的选择方式，802.11 标准并未加以规范。

— 无竞争周期所使用的帧可以带有多重目的，参见第九章。如果帧中包含ACK，则它就是用来回应之前的帧发送者而不是帧接收者。发送端必须确保该帧是以接收端及目的端工作站均支持的速率传送的。

5. ACK或CTS之类的确认帧必须以基本速率集所包含的速率传送，但不能快于这次传送所使用的初始帧。响应帧必须使用与初始帧相同的调制方式（DSSS、CCK或OFDM）（注6）。

选速与降速

市面上所有802.11接口均支持某种降速机制，可以适应不同网络环境调降所使用的数据率。速率选择（rate selection）主要决定一张网卡该在何时提高速率以提高链路品质。802.11标准并未规范工作站如何决定降速（或升速），因此速率选择如何实现就留给芯片组厂商自行决定。几乎所有芯片组均有自己的一套选速机制，因此大多数802.11接口的操作方式均有所不同。速率选择是可编程的，一般是由驱动接口的程序代码控制。速率选择机制可以通过驱动程序或者固件升级。

最常被用来判断何时应该变速的算法，其实是通过一些不是那么严谨的信号质量测量。信号质量可以直接就信噪比（signal-to-noise ratio）加以测量，或者间接观察有多少帧需要重传。直接测量信噪比可以针对最近一个帧的瞬间信号质量，或者就最近一段时间所接收到的一定数量的帧取平均数。有些芯片组会直接测量信噪比，不过随后会将之转换为相应的“信号质量”（signal quality）。当信号质量变差，芯片就会以降速来应变（注7）。

至于间接量测，则是监测瞬间或平均遗失多少帧，然后予以适度补偿。采用间接测量的算法简单来讲就是：如果帧已经遗失且帧重试计数器已经用尽，那就降速至下一档，然后重试一遍。反复进行以上步骤直到帧送出，或者一直尝试到以最低速率都无法成功传送为止。采用间接信号质量测量的芯片组或许会稍微修改上述算法，以避免耗费过多时间在物理层所支持的所有速率间逐次降速。尤其是近来的芯片组均支持不少的速率，在较低速率上反复重试将会相当费时。

帧的处理与桥接

无线接入点的核心其实就是桥接器，负责在无线与有线媒介之间转换帧。虽然802.11并未限制非得使用何种有线媒介技术，但放弃Ethernet不用的接入点还真没见过。大多数

注6：这点并未被严格遵守。有家芯片组厂商固定以24 Mbps传送ACK帧，因为24 Mbps通常是必要数据率（mandatory data rate）中速度最快的。

注7：信号质量测量通常是工作站在接入点间移动时作为是否漫游的决策依据。不过，并没有标准规范如何（甚至是否）将信号质量当成漫游算法的输入项。

接入点在设计上就是扮演802.11与Ethernet之间的桥梁，因此了解帧在两种媒介之间的传送方式就相当重要了。如图 3-22 所示。

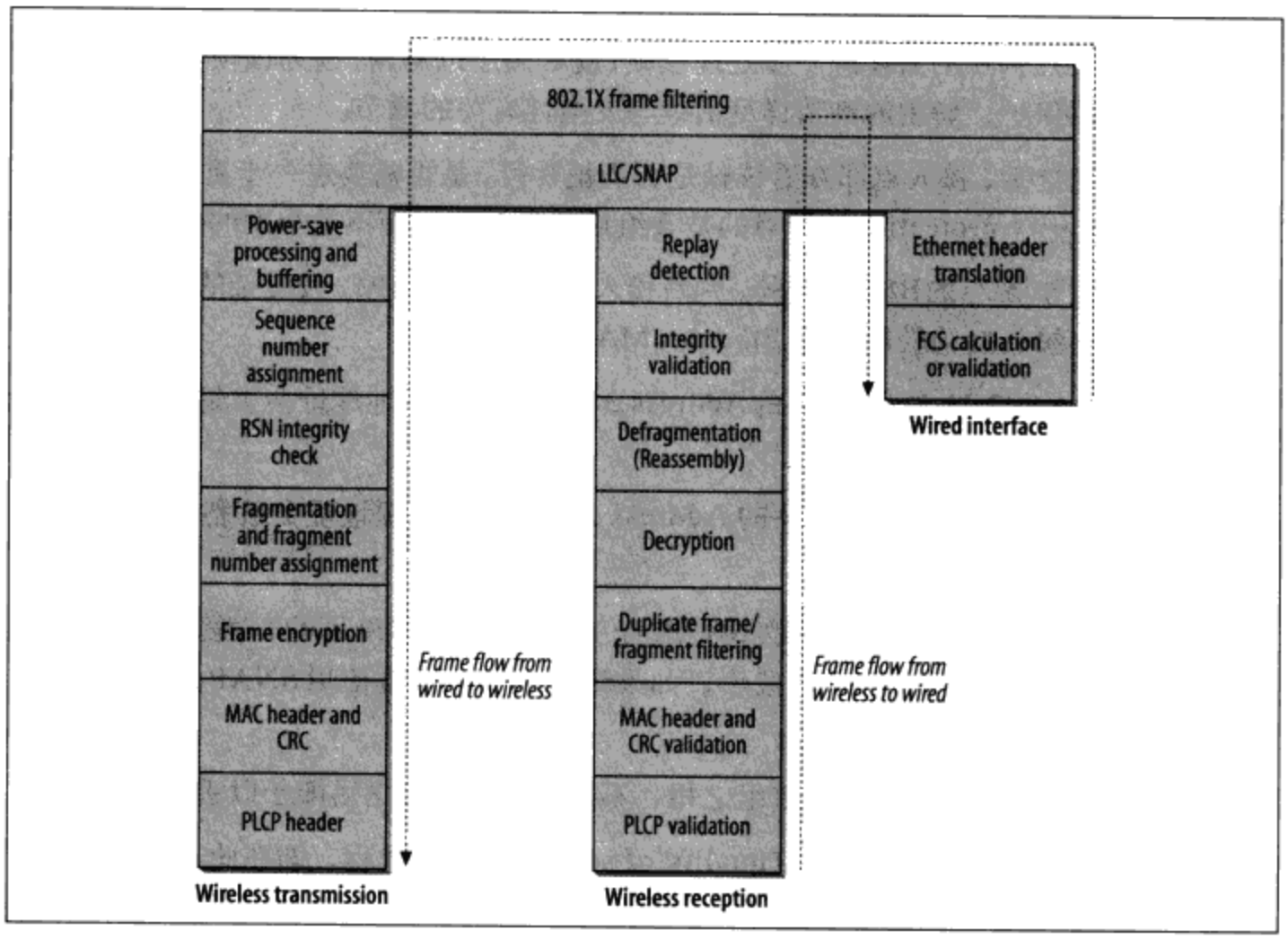


图 3-22：在无线与有线媒介之间转换帧

无线媒介至有线媒介（802.11 至 Ethernet）

当接入点的无线接口接收到准备传送至有线网络的帧时，接入点必须在两种媒介之间桥接帧（bridge the frame）。不正式地说，以下是接入点必须进行的一系列操作：

1. 当接入点接收到一个帧时，首先会检测该帧基本的完整性。接下来，接入点会针对所使用的物理层，查看本章之前讨论过的物理层标头，然后验证 802.11 帧上的帧校验码（FCS）。
2. 验证帧接收无误后，接入点就会继续查看是否应该进一步处理该帧。
   a. 传送至接入点的帧会将接入点的MAC地址（即BSSID）作为802.11 MAC标头的Address 1字段。不匹配该接入点的BSSID的帧应予以丢弃（有些产品并未实现此步骤）。

b. 802.11 MAC接着检测且移除重复的帧。产生重复帧的原因很多，不过最常见的情况是802.11确认在传送过程中遗失或损坏。为了简化上层协议的操作，因此由802.11 MAC负责剔除重复的帧。

3. 一旦接入点判断出需要进一步处理该帧，就必须予以解密，因为该帧受到链路层安全算法的保护。解密的细节详见后续与安全性有关的章节。

4. 成功解密之后，接入点即查看该帧是否为帧片段，是否需要进一步重组。完整性保护（integrity protection）针对的是重组后的完整帧，而不是个别的帧片段。

5. 如果经过步骤2a的BSSID校验，判断接入点必须桥接该帧，较复杂的802.11 MAC标头就会被转换为较简单的Ethernet MAC标头。

   a. 记录在802.11 MAC标头的Address 3字段里的目的地地址会被复制到Ethernet的目的地地址。

   b. 记录在802.11 MAC标头的Address 2字段里的来源地址会被复制到Ethernet的来源地址。

   c. 在802.11 Data字段里的SNAP标头将（Type字段里的）类型代码复制到Ethernet帧里的Type字段中。如果该Ethernet帧也使用SNAP，就复制整个SNAP标头。

   d. 顺序信息主要供帧片段重组之用，不过当帧被桥接之后即予以丢弃。

   e. 如果有标准的服务质量（quality of service）处理过程，即在此进行无线接口与有线接口的QoS映射。不过到目前为止，用来表示服务质量的形式，通常就是在有线帧中使用802.1p优先级位或者其他的控制形式。

6. 重新计算FCS（帧校验码）。Ethernet与802.11使用相同的算法来计算FCS，不过802.11帧多出一些字段，同时受FCS保护。

7. 将产生的新帧交付给Ethernet接口传送。

有线媒介至无线媒介（Ethernet至802.11）

将帧从接入点有线端桥接至无线媒介的过程刚好相反：

1. 验证Ethernet FCS后，接入点首先会查看是否需要进一步处理所接收到的帧，即查看该帧的目的地址是否属于当前与接入点关联的工作站。

2. 将SNAP标头附加于Ethernet帧的数据之前。上层封包以SNAP标头进行封装，而其Type字段从Ethernet帧里的类型代码复制而来。如果该Ethernet帧也使用SNAP，则复制整个SNAP标头。

3. 对帧的传送进行调度。802.11 包含复杂的省电操作，将帧置于传送队列（transmit queue）之前，接入点可能会将帧缓存于缓冲区。省电操作将于第八章详述。
4. 一旦帧被置于队列待传，就会被赋予一个顺序编号。如有必要，所产生的数据可以用完整性校验值加以保护。如果帧需要分段，则会根据事先设定好的分段阈值进行分段。分段帧时，Sequence Control 字段中的片段编号也会被赋值。
5. 如果帧需要保护，则对帧（或每个帧片段）的主体加密。
6. 802.11 MAC 标头根据 Ethernet MAC 标头产生。
   a. 将 Ethernet 的目的地地址复制到 802.11 MAC 标头的 Address 1 字段。
   b. 将 BSSID 置于 Address 2 字段以作为无线媒介上帧的发送者。
   c. 将帧的来源地址复制到 MAC 标头的 Address 3 字段中。
   d. 将其他字段填入802.11 MAC标头。也就是把预计传送时间填入Duration字段，并把适当的标记填入 Frame Control 字段。
7. 重新计算 FCS（帧校验码）。Ethernet 与 802.11 使用相同的算法来计算 FCS，不过 802.11 帧多出一些字段，同时受 FCS 保护。
8. 将产生的新帧交付给 802.11 接口传送。

服务质量扩展功能

服务质量扩展功能（quality of service extension）会影响帧的传送顺序，但并不会改变帧通过802.11 MAC的基本路径。802.11e服务质量扩展功能并非只用单一传送队列，而是在上述有线至无线桥接过程中的第 4、5、7 步中采用多组传送队列。这些步骤会根据优先次序（priority order）进行帧处理，而优先次序取决于帧的内容以及配置设定中预先指定的优先级分级规则。

第四章

802.11 成帧细节

第三章主要说明帧(frame)的基本结构及其组成字段，不过并未深入探究各种不同类型帧的细节。Ethernet的成帧（framing）十分简单，只要为帧加上前导码（preamble）、寻址信息以及在结尾加上校验码即可。相对而言，802.11的成帧就比较复杂，因为无线媒介必须将有线网络所没有的帧类型以及各式管理功能纳入考虑。

802.11帧主要有三种类型。数据帧（data frame）好比802.11中的驮马，负责在工作站之间搬运数据，它可能会因为所处的网络环境不同而有所差异。控制帧（control frame）通常与数据帧搭配使用，负责区域的清空（area clearing）、信道的取得（channel acquisition）以及载波监听的维护（carrier-sensing maintenance），并于收到数据时予以肯定确认（positive acknowledgment of received data），借此提高工作站之间数据传送的可靠性。管理帧（management frame）负责监督，主要用来加入或退出无线网络以及处理接入点之间关联的转移事宜。

本章只供参考之用。每个作者的生命有限，不可能只是为了将这些细节讲述得入木三分而投注所有精力。各位不妨完全略过本章，等到需要深入探究帧结构时再回头来看。成帧细节通常不在网络管理人员必懂的范围之内，只有一些少数例外。同时，本章使用了大量的缩写名词，不懂之处请参考书后的名词术语。

数据帧

数据帧（data frame）会将上层协议的数据置于帧主体中（frame body）中加以传递。图4-1显示了数据帧的基本结构。会用到哪些字段取决于该数据帧所属的类型。

不同类型的数据帧可根据功能加以分类，其中的一种方式将数据帧分为用于基于竞争的服务的（contention-based service）及用于无竞争服务（contention-free service）的两

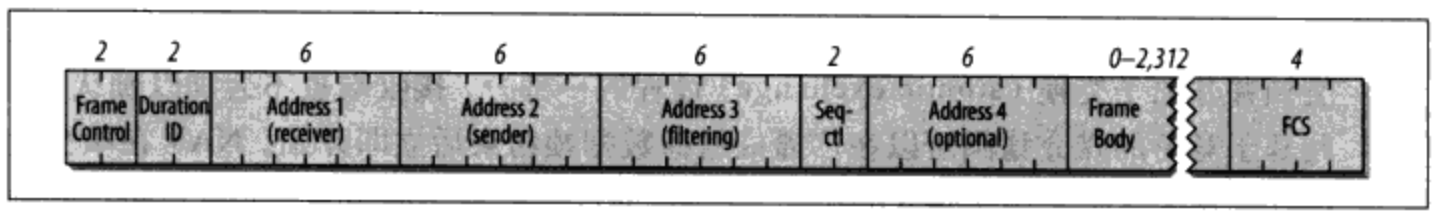


图 4-1：一般的数据帧

种数据帧。只能在无竞争周期（contention-free period）出现的帧，就不可能在IBSS（独立基本服务集）中使用。另一种区分方式，则是对携带数据与提供管理功能的帧加以区别。表 4-1 显示了数据帧的分类方式。无竞争服务所使用的帧在第九章会有更详细的讨论。

表4-1：数据帧的各种分类方式

帧类型	基于竞争的服务	无竞争服务	携带数据	未携带数据
Data	✓		✓	
Data+CF-ACK		✓	✓	
Data+CF-Poll		AP only	✓	
Data+CF-ACK+CF-Poll		AP only	✓	
Null	✓	✓		✓
CF-ACK		✓		✓
CF-Poll		AP only		✓
CF-ACK+CF-Poll		AP only		✓

Frame Control（帧控制）

Frame Control（帧控制）字段各个位的用法在第三章说明过。每个帧控制位都可能影响到 MAC 标头中其他字段的解读方式。最值得注意的是那些地址字段，它们的意义将因 ToDS 及 FromDS 位的值的不同而不同。

Duration（持续时间）

Duration（持续时间）字段用来记载网络分配矢量（Network Allocation Vector，简称 NAV）的值。访问媒介的时间限制由 NAV 指定。数据帧的 Duration 字段的设定必须依循四项规范：

1. 无竞争周期所传递的任何帧必须将Duration字段设定为32768。此规范适用于无竞争周期所传递的任何数据帧。

2. 目的地为广播或组播地址的帧（Address 1 字段设定了组位）的持续时间为0。此类帧并非原子交换（atomic exchange）过程的一部分，接收端也不会加以确认，因此基于竞争的媒介访问可以在广播或组播数据帧结束后立即开始。NAV 在帧交换过程中用来保护对传送媒介的访问。既然广播或组播帧之后不会有来自链路层的确认，因此没有必要为后续帧锁定媒介使用权。

3. 如果 Frame Control 字段中的 More Fragments（更多片段）位为 0，表示该帧已无其余片段。最后的帧片段只需为本身的确认预订媒介使用权，之后就可以恢复基于竞争的访问了。Duration字段会被设定为传送一个短帧间间隔及片段响应所需要的时间。整个过程如图 4-2 所示。倒数第二个片段的Duration字段会为最后一个片段锁定媒介使用权。

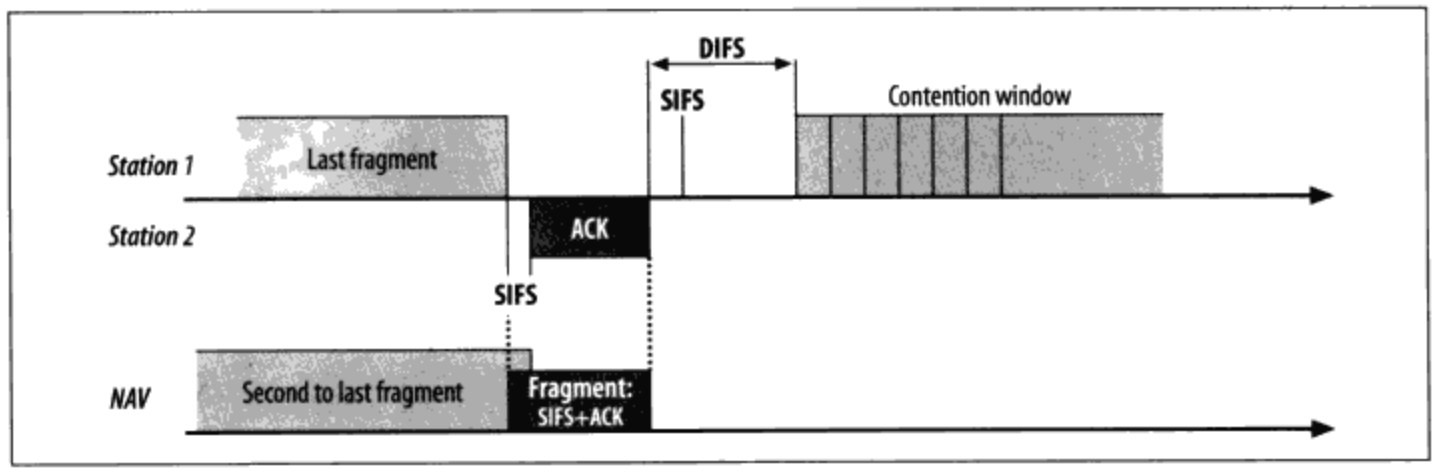


图 4-2：最终片段 Duration 设定

4. 如果Frame Control字段的More Fragments位被设定为1，则表示其后还有帧片段。因此，Duration 字段便会被设定为传送 2 个确认加上 3 个短帧间间隔及下一个帧片段所需要的时间。为非最终片段设定 NAV 的方式本质上与 RTS 相同，所以也称为虚拟 RTS。

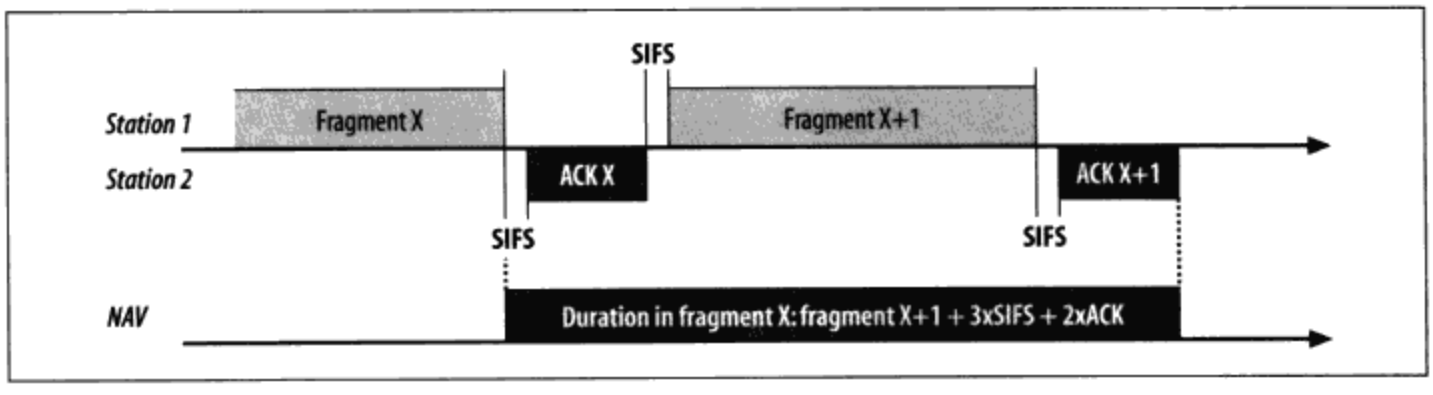


图 4-3：非最终片段的 Duration 设定

寻址与 DS 位

地址字段的编号与功能取决于设定了哪个DS（分布式系统）位，因此所使用的网络类型会间接影响到地址字段的用法。表4-2列出了地址字段在数据帧中的各种用法。只有无线桥接器（wireless bridge）才会使用第四个地址字段，因此比较少见。

表4-2：地址字段在数据帧中的用法

功能	ToDS	FromDS	Address 1（接收端）	Address 2（发送端）	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	未使用
To AP（基础结构型）	1	0	BSSID	SA	DA	未使用
From AP（基础结构型）	0	1	DA	BSSID	SA	未使用
WDS（桥接器）	1	1	RA	TA	DA	SA

Address 1 字段代表帧接收端的地址。在某些情况下，接收端（receiver）即为目的地（destination），但不总是这样。目的地是指负责处理帧中网络层封包的工作站；而接收端则是负责将无线电波解码为802.11帧的工作站。如果Address 1字段被设为广播或组播地址，则必须同时检查BSSID（基本服务集标识符）。工作站只会响应来自同一个基本服务集的广播或组播，至于来自其他不同BSS的则加以忽略（注1）。Address 2字段是发送端的地址，用来发送确认信息。发送端（transmitter）不见得就是来源地（sender）。来源地是指产生帧中网络层协议封包的工作站；而发送端则是负责将帧传送至无线链路。Address 3 字段则是供接入点与分布式系统过滤之用，不过该字段的用法取决于所使用的网络类型。

由于IBSS（独立基本服务集）并未使用接入点，因此不会涉及分布式系统。发送端即为帧的来源，而接收端即为帧的目的地。每个帧都会记载BSSID（基本服务集标识符），因此工作站可以检查广播与组播信息。只有隶属同一个BSS的工作站才会处理该广播或组播信息。在IBSS中，BSSID是由随机数产生器随机产生的。

802.11对来源地与发送端以及目的地与接收端有明确的区别。将帧送至无线媒介的发送端不见得就是帧的产生者。目的地地址与接收端地址同样有此区别。接收端可能只是中间目的地，而帧只有到达目的地，才会由上层的协议加以处理。

注1：并非所有网卡均能正确无误地完成过滤BSSID的动作。很多产品并不会先行验证BSSID是否无误，而是将所有广播信息直接传递给上层协议。

BSSID

每个BSS都会被赋予一个BSSID，它是一个长度为48位的二进制标识符，用来识别不同的BSS。BSSID的主要优点是它可作为过滤之用。虽然不同的802.11网络彼此之间可能重叠，但即使如此也不应该让相互重叠的网络收到彼此的链路层广播。

在infrastructure BSS（基础结构型基本服务集）中，BSSID就是创建该BSS的接入点上无线接口的MAC地址。而IBSS（独立基本服务集）则必须创建BSSID，才能产生网络。为了让所创建的地址尽量不重复，BSSID有46位是随机产生的。其所产生的BSSID会将Universal/Local位设定为1，代表这是一个本地地址，至于Individual/Group位则会设定为0。两个不同的IBSS如果要产生相同的BSSID，那么它们所产生的46位随机数必须完全相同。

有一个BSSID会被保留不用，就是所有位均设定为1的BSSID，又称为广播型BSSID。使用广播型BSSID的帧可以不被MAC中任何的BSSID filter所过滤。BSSID的广播只有在移动式工作站送出probe request（探查请求）以试图找出有哪些网络可以加入时才会被用到。probe帧要能够探测现有的网络，就不能被BSSID filter过滤掉。probe帧是唯一允许使用广播型BSSID的帧。

图4-4展示了一个简单的网络，其中有某个无线客户端通过802.11网络连接至服务器。客户端将帧传送给服务器时，地址字段的用法如表4-2的第二行所示。

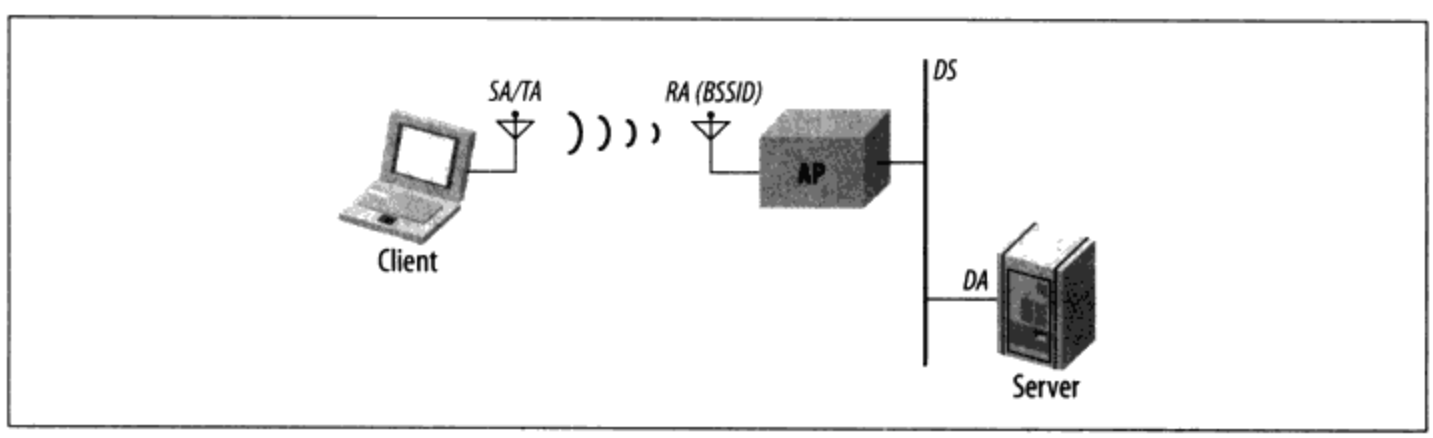


图4-4：将帧传送至服务器时地址字段的用法

如果帧的目的地位于分布式系统（distribution system，简称DS），则客户端既是来源地也是发送端。至于无线帧的接收端则是接入点，不过该接入点只是个中间目的地。当帧送达接入点时，该帧会经分布式系统转送给服务器。因此，分布式是接收端，而服务器

才是最后的目的地。在基础结构型网络里，接入点会以其无线接口的地址创建相应的BSS，这就是为什么接收端地址（Address 1）会被设定为BSSID的原因。

当服务器响应客户端时，帧会通过接入点被传送给客户端，如图4-5所示。这种情况相当于表4-2的第三行。

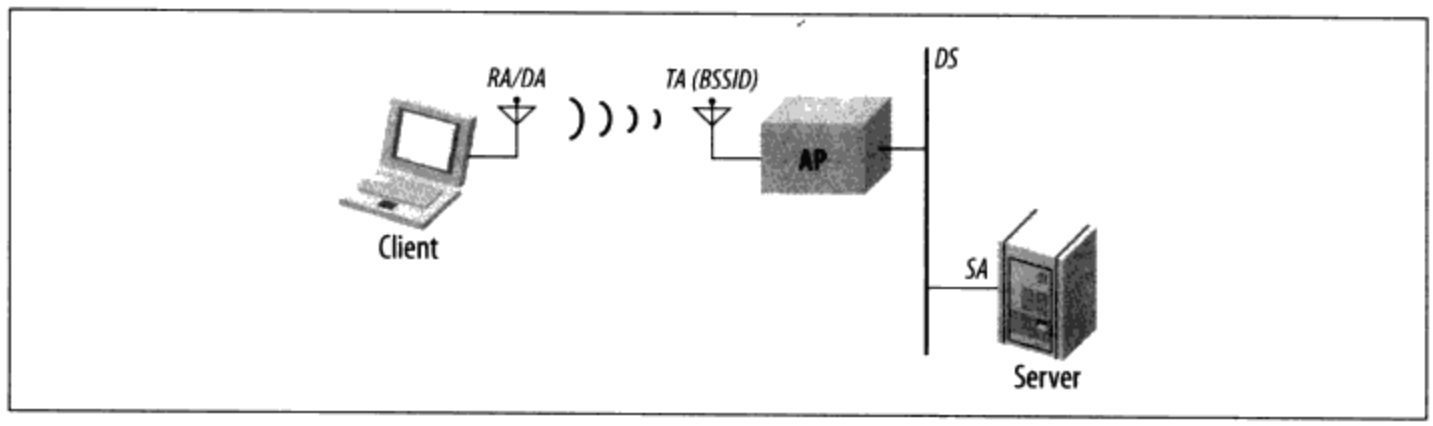


图4-5：帧来自分布式系统时地址字段的用法

由于帧产生自服务器，所以服务器的MAC地址即为该帧的源地址（source address，简称SA）。当帧通过接入点转送出去时，接入点将会以自己的无线接口作为发送端地址（transmitter address，简称TA）。如同前一个例子，接入点的接口地址就是BSSID。帧最后会被送至客户端，此时客户端既是目的地（destination）也是接收端（receiver）。

表4-2的第四行展示了地址字段在无线分布式系统（wireless distribution system，简称WDS）中的用法。无线分布式系统有时也称为无线桥接器（wireless bridge）。如图4-6所示，两条有线网络通过扮演无线桥接器角色的基站彼此相连。从客户端送至服务器的帧会经过802.11 WDS。该无线帧的源地址与目的地地址依然对应到客户端与服务器的地址。不过，这些帧还是会区分无线媒介上帧的发送端与接收端。对于由客户端送至服务器的帧而言，发送端就是客户端这边的接入点，而接收端就是服务器这边的接入点。将来源地与传送端分开的好处是，当服务器这边的接入点送出必要的802.11响应给对方的接入点时，不会干扰到有线链路层。

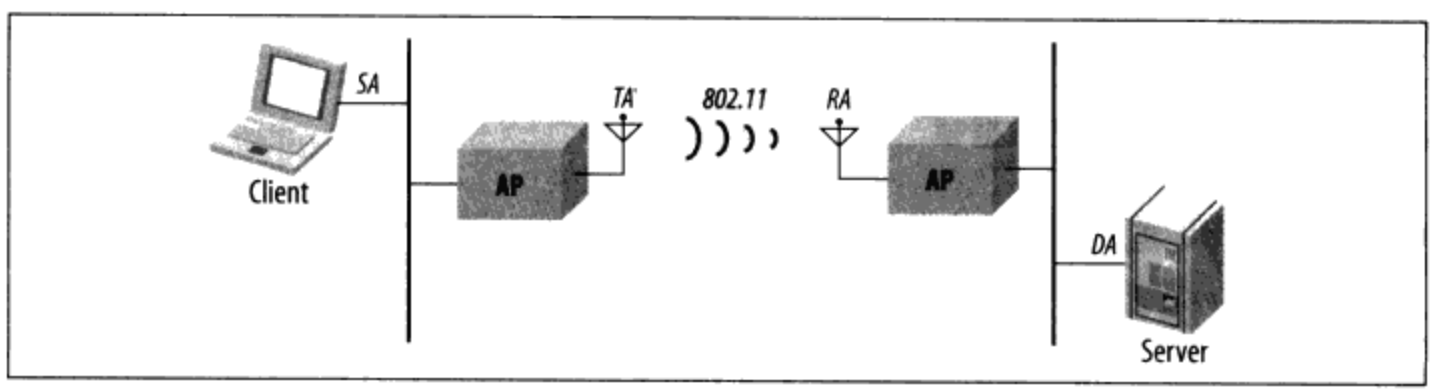


图4-6：无线分布式系统

数据帧的类型主题

802.11具有数种不同类型的数据帧。要使用何种帧，取决于服务是属于基于竞争的还是无竞争的。基于效率上的考虑，无竞争帧中可以纳入其他功能。只要改变帧的子类型(subtype)，无竞争周期中的数据帧可用来确认其他帧，如此便可省去帧间间隔以及一一确认所带来的负担。以下是常见的数据帧类型：

Data（数据）

子类型为Data的帧只有在基于竞争的访问周期才会被传送。这类简单的帧只有一个目的，即在工作站间传送帧主体。

Null（空）

Null帧（注2）看起来有点奇怪。它是由MAC标头与FCS标尾所组成。在传统的Ethernet中，Null帧无非就是额外的负担。在802.11网络中，移动式工作站会利用Null帧来通知接入点改变省电状态。当工作站进入休眠状态时，接入点必须开始为之缓存帧。如果该移动式工作站没有数据要经分布式系统传送，也可以使用Null帧，同时将Frame Control（帧控制）字段的Power Management（电源管理）位设定为1。接入点不可能进入省电模式，因此不会传送Null帧。Null帧的用法如图4-7所示。

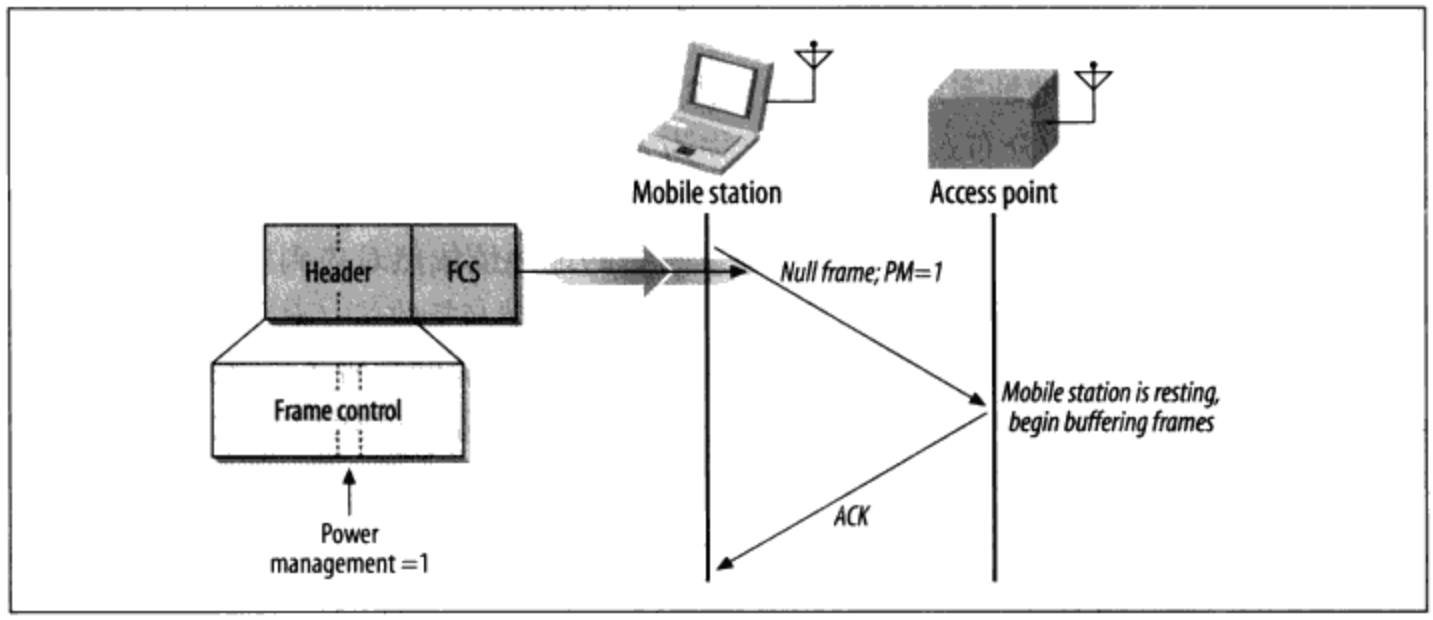


图4-7：子类型为Null的数据帧

此外尚有一些在无竞争周期使用的帧类型。不过，无竞争服务在实现上并不常见，相关

注2: 为了强调“Null”是规范说明书所指定的帧类型，而不是一般的英文单词，“Null”的首字母将会以大写来表示。

帧（Data+CF-ACK、Data+CF-Poll、Data+CF-ACK+CF-Poll、CF-ACK、CF-Poll 以及 CF-ACK+CF-Poll）的探讨详见第九章。

数据帧的封装

数据帧的形式取决于网络的类型。帧究竟属于何种类型，完全取决于subtype（子类型）字段，而与其他字段是否出现在帧中无关。

IBSS 帧

在 IBSS 中使用的 address 字段有三种，如图 4-8 所示。第一个地址代表 receiver（接收端），同时也是 IBSS 网络中的 destination（目的地）地址。第二个地址是 source（来源地）地址。在这些地址之后，伴随而来的是 IBSS 的 BSSID。当无线 MAC 收到一个帧时，首先会去检查 BSSID，只有 BSSID 与工作站的相同的帧才会交由上层协议处理。

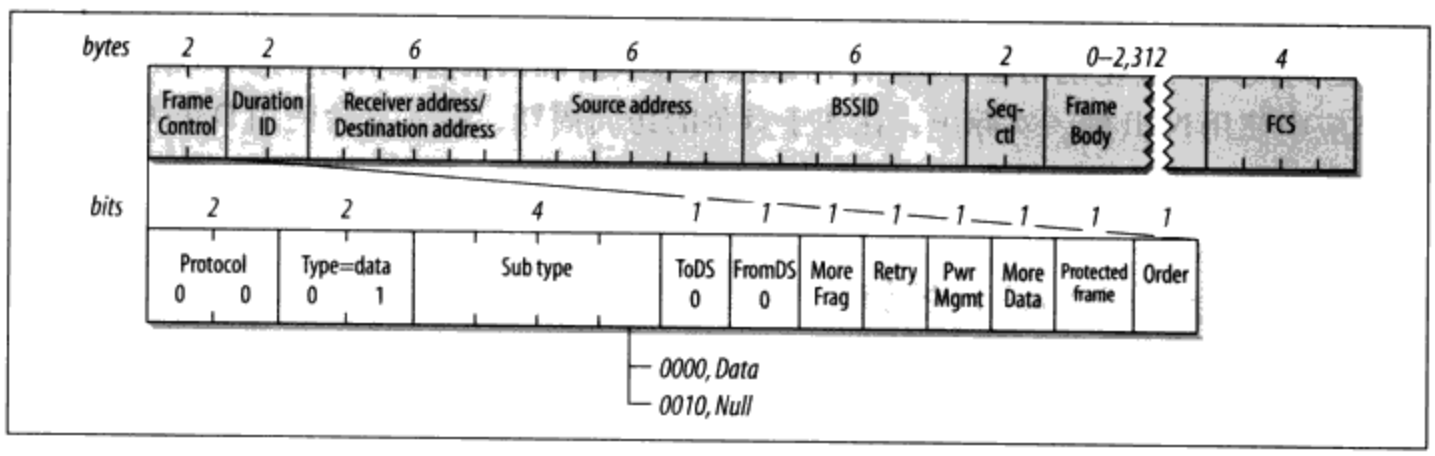


图 4-8：IBSS 数据帧

IBSS 数据帧的子类型不是 data 就是 Null，后者只是用来告知目前的电源管理状态。

传送来自接入点（From AP）的帧

图 4-9 显示了从接入点传送给移动式工作站的帧格式。和所有数据帧一样，第一个地址字段代表无线网络中接收该帧的 receiver（接收端），即该帧的目的地。第二个地址字段存放了 transmitter（发送端）的地址。在 infrastructure（基础结构型）网络中，transmitter（发送端）地址即为接入点（AP）上无线接口的地址，同时也是 BSSID。最后，该帧会记载帧的来源 MAC 地址。区分 source（来源地）与 transmitter（发送端）之所以必要，是因为 802.11 MAC 会将确认送给帧的 transmitter（即接入点），而较上层的协议会将回复送给帧的 source（来源地）。

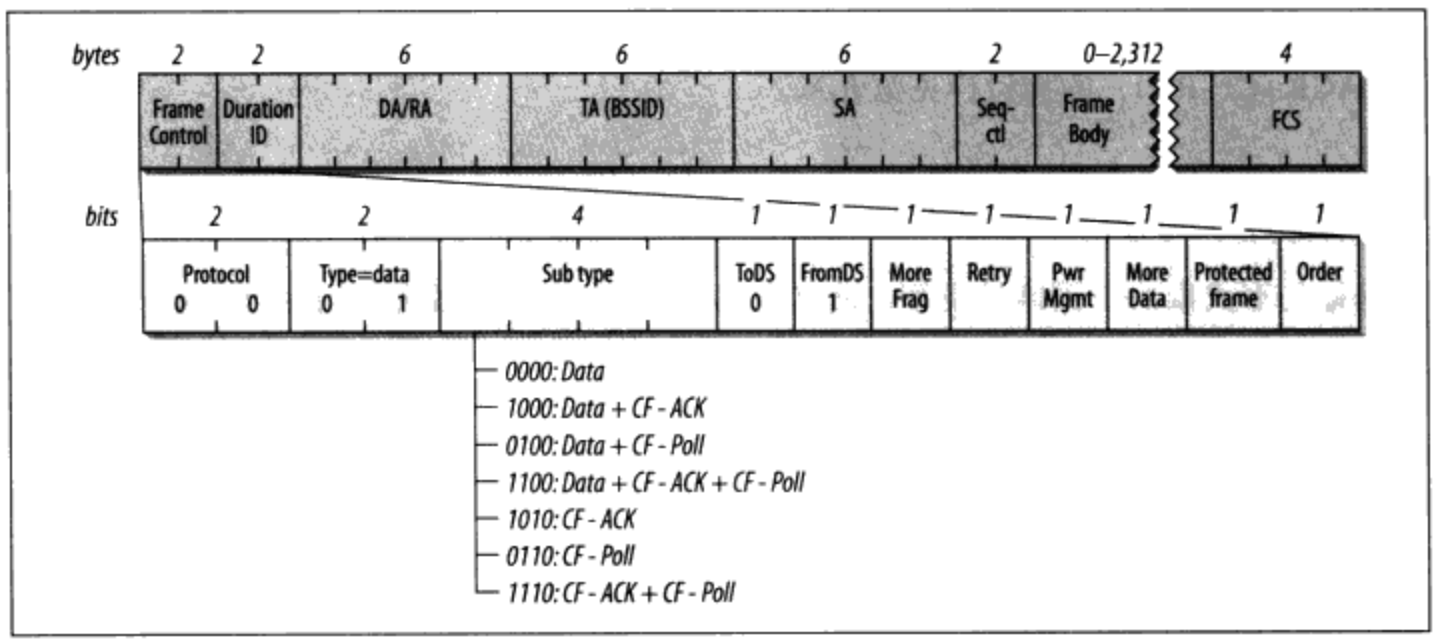


图 4-9：来自接入点的数据帧

在 802.11 的规范说明书中并未明文禁止接入点传送 Null 帧，不过这么做并没有任何意义。因为接入点禁止使用省电例程，所以接入点只会确认来自工作站的 Null 帧，而不会在响应中使用 Null 帧。实际上，在基于竞争的访问周期，接入点会使用 Data 帧，而在无竞争周期，则是使用包含 CF-Poll 功能的帧。

传送至接入点（To AP）的帧

图 4-10 显示了在 infrastructure（基础结构型）网络里，移动式工作站传送给所连接的接入点的帧格式。接收端地址（RA）为 BSSID。在基础结构型网络里，BSSID 即为接入点的 MAC 地址。送至接入点的帧，其来源地 / 发送端地址（SA/TA）是无线工作站的网络接口。接入点并未进行地址过滤的动作，而是使用第三个地址（DA）将数据转送至位于分布式系统的适当位置。

传送至分布式系统（DS）的帧的 ToDS 位会被设定为 1，而 FromDS 位会被设定为 0。在基础结构型网络中，移动式工作站不能扮演点协调者（point coordinator）的角色，因此不能传送含有 CF-Poll（无竞争 – 轮询）功能的帧。

WDS 中的帧

当接入点被部署成无线桥接器（或者 WDS）时会用到 4 个地址字段，如图 4-11 所示。和其他数据帧一样，WDS 帧会使用第一个地址（RA）代表 receiver（接收端），第二个地址（TA）代表 transmitter（发送端）。MAC 层会使用这两个地址送出确认并控制流量，例如 RTS、CTS 以及 ACK 帧。另外两个地址字段（SA 与 DA）则是用来记载帧的

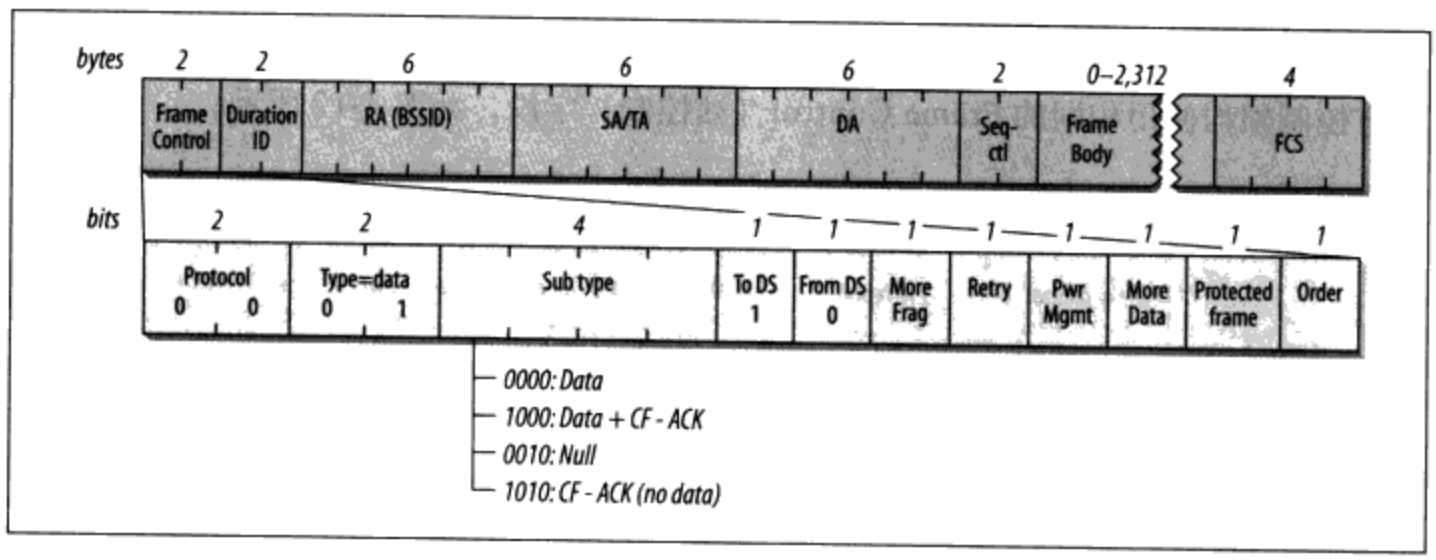


图 4-10：传送至接入点的数据帧

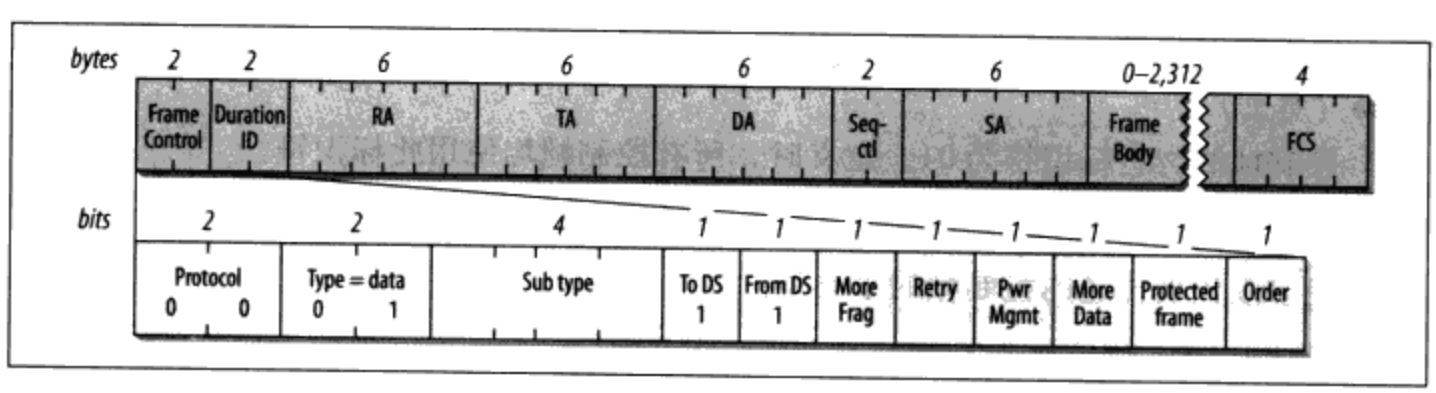


图 4-11：WDS 帧

source（来源地）以及 destination（目的地）地址，并且将之与无线链路（wireless link）所使用的地址区分开来。

在无线桥接链路中，通常不会存在移动式工作站，也不会使用无竞争周期。接入点禁止进入省电模式，因此 Power Management（电源管理）位必然被设定为 0。

经过加密的帧

受到链路层安全协议保护的帧并不算新的帧类型。当帧经过加密处理后，Frame Control（帧控制）字段的 Protected Frame 位会被设定为 1，至于 Frame Body（帧主体）字段则是以第五章或第七章所描述的加密标头开始，这取决于所使用的是何种协议。

控制帧

控制帧主要用于协助数据帧的传递。它们可用来管理无线媒介的访问（但非媒介本身）以及提供 MAC 层的可靠性。

一般的帧控制字段

所有控制帧均使用相同的 Frame Control（帧控制）字段，如图 4-12 所示。

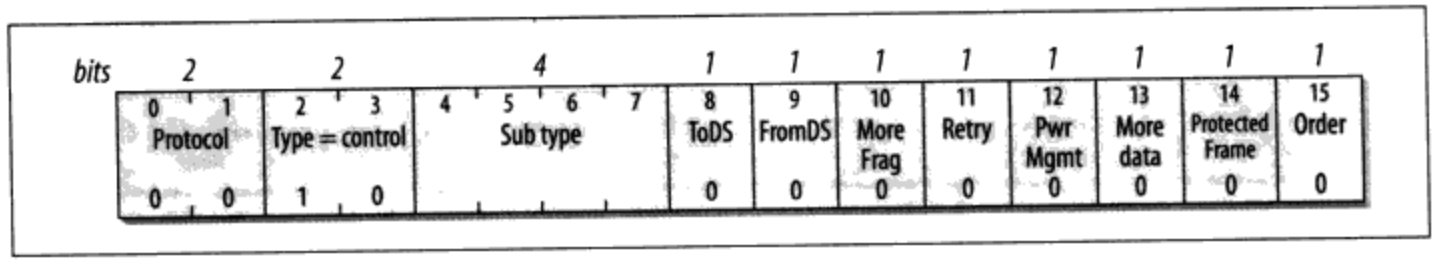


图 4-12：控制帧中的 Frame Control 字段

Protocol（协议版本）

在图 4-12 中，协议版本的值为 0，因为这是目前绝无仅有的版本。未来可能会出现其他新的版本。

Type（类型）

控制帧的类型标识符为 01。定义时，所有控制帧均使用此标识符。

Subtype（子类型）

此字段代表传送的控制帧的子类型。

ToDS 与 FromDS 位

控制帧负责仲裁无线媒介的访问，因此只能够由无线工作站产生。分布式系统（DS）并不会收发控制帧，因此这两个位必然为 0。

More Fragments（更多片段）位

控制帧不可能被分段，因此这个位必然为 0。

Retry（重试）位

控制帧不像管理帧或数据帧那样，必须在队列中等候重新发送，因此这个位必然为 0。

Power Management（电源管理）位

此位用来指示完成当前的帧交换过程后，传送端的电源管理状态。

More Data（更多数据）位

此位只用于管理帧及数据帧中，在控制帧中此位必然为 0。

Protected Frame（受保护帧）位

控制帧不会经过加密，因此对控制帧而言，此位必然为 0。

Order（次序）位

控制帧是原子帧交换程序（atomic frame exchange operation）的组成要件，因此必须依序传送，所以这个位必然为 0。

RTS（请求发送）

RTS 帧可用来取得媒介的控制权，以便传送“大型”帧。至于多大可称为“大型”，则是由网卡驱动程序中的 RTS threshold（阈值）来定义。媒介访问权只能保留给单播（unicast）帧使用，而广播（broadcast）与组播（multicast）帧只是被简单地传送。RTS 帧的格式如图 4-13 所示。就和所有控制帧一样，RTS 帧只包含帧头。帧主体中并未包含任何数据，帧头之后即为 FCS（帧校验码）。

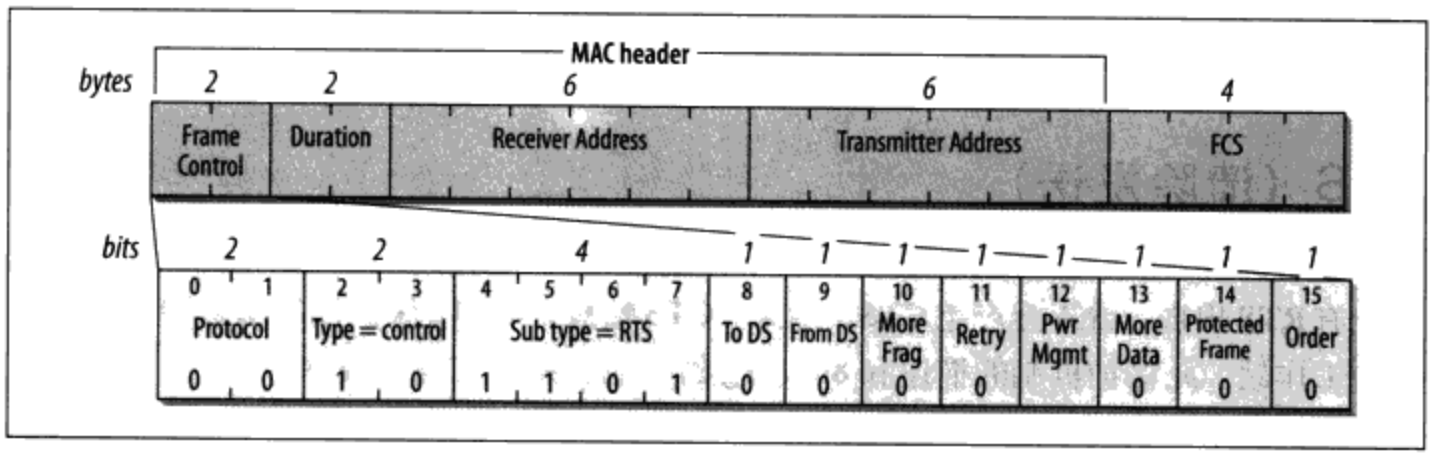


图 4-13：RTS 帧

RTS 的 MAC 标头由 4 个字段构成：

Frame Control（帧控制）

Frame Control 字段并没有任何特殊之处。帧的 subtype（子类型）字段被设定为 1011，代表 RTS 帧。除此之外，它与其他的控制帧有相同的字段。（在 802.11 规范说明书中，最重要的位是最后一个位，因此在 subtype 字段中，第 7 个位代表最重要的位。）

Duration（持续时间）

RTS 帧会试图预约媒介使用权，供帧交换过程使用，因此 RTS 帧传送者必须计算 RTS 帧结束后还需要多少时间用于帧交换。图 4-14 说明了整个交换过程，总共需要 3 个 SIFS 周期、1 个 CTS 持续时间、最后的 ACK 加上传送第一个帧或帧片段所需要的时间。（片段突发期会使用后续的帧片段来更新Duration字段。）传送所需要的微秒数经过计算后会置于Duration字段中。假使计算的结果不是整数，则会被修改为下一个整数微秒数。

Address 1 字段：Receiver Address（接收端地址）

接收大型帧的工作站地址。

Address 2 字段：Transmitter Address（发送端地址）

RTS 帧的发送端地址。

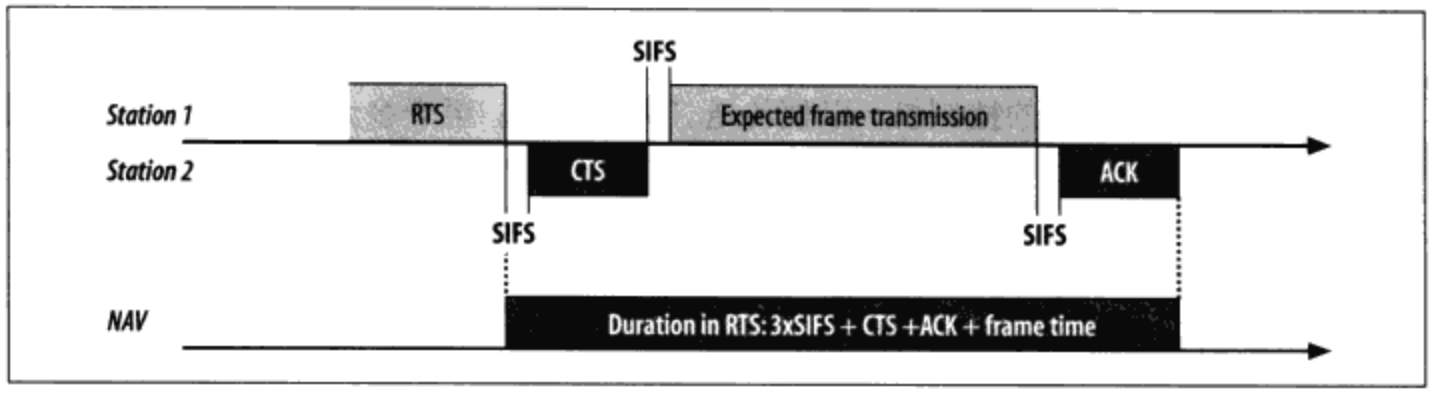


图 4-14：RTS 帧中的 Duration 字段

CTS（清除发送）

CTS 帧有两种目的，其格式如图 4-15 所示。起初，CTS 帧仅用于回复 RTS 帧，如果之前没有RTS 出现，就不会产生CTS。后来，CTS 帧被 802.11g 保护机制用来避免干扰较旧的工作站。此保护机制的描述和 802.11g 的其他资料详见第十四章。

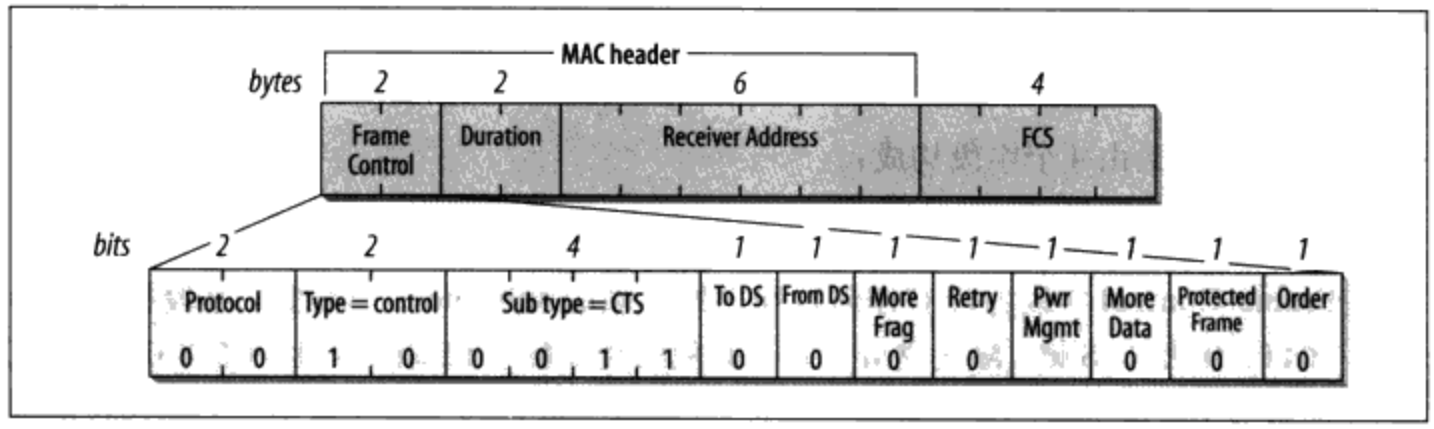


图 4-15：CTS 帧

CTS 帧的 MAC 标头由 3 个字段构成：

Frame Control（帧控制）

帧的 subtype（子类型）字段被设定为 1100，代表 CTS 帧。

Duration（持续时间）

用来响应 RTS 时，CTS 帧的发送端会以 RTS 帧的 duration 值作为持续时间的计算基准。RTS 帧会为整个 RTS-CTS-frame-ACK 交换过程预留媒介使用时间。不过当 CTS 帧被传送出去后，只剩下其他未传帧或帧片段及其确认待传。CTS 帧发送端会将 RTS 帧的 duration 值减去传送 CTS 帧及其后的短帧间间隔所需要的时间，然后将计算结果置于 CTS 的 Duration 字段中。图 4-16 显示了 CTS duration 与 RTS duration 的关系。用于保护交换（protection exchanges）时，CTS 帧所依循的规则将留待和保护机制一起讨论。

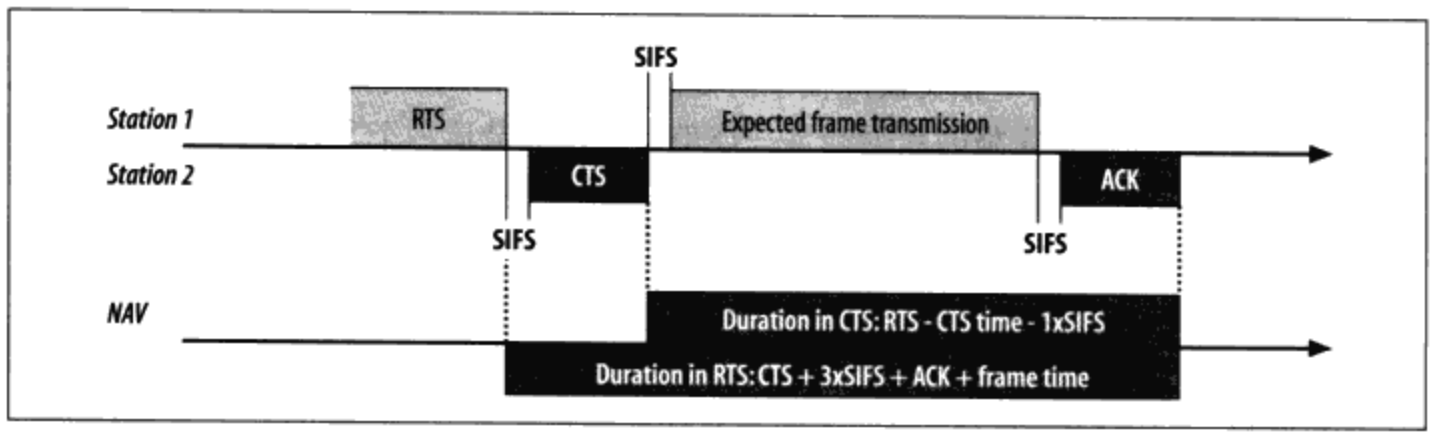


图 4-16：CTS 持续时间

Address 1 字段：Receiver Address（接收端地址）

CTS 帧的接收端即为之前 RTS 帧的发送端，因此 MAC 会将 RTS 帧的发送端地址复制到 CTS 帧的接收端地址。802.11g 保护操作所使用的 CTS 帧会被传送给发出 RTS 的工作站，而且只用来设定 NAV。

ACK（确认）

ACK 帧（图 4-17）就是 MAC 以及任何数据的传送（包括一般传送、RTS/CTS 交换之前的帧、帧片段）所需要的肯定确认（positive acknowledgment）。服务质量扩展功能放宽了对于数据帧的单一确认的要求。要评估响应机制对净吞吐量（net throughput）所造成的影响，详见第二十五章。

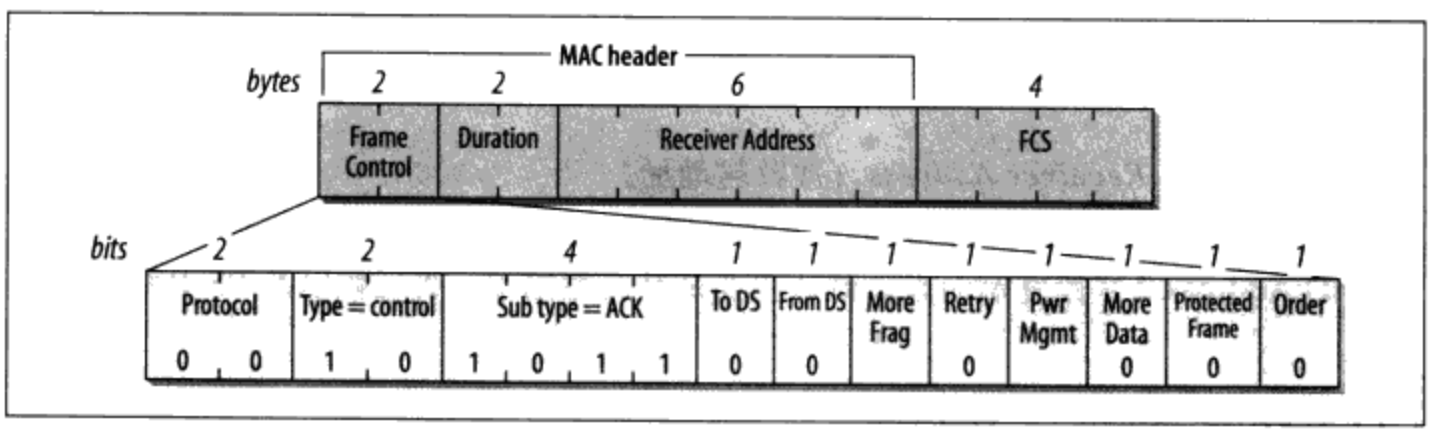


图 4-17：ACK 帧

ACK 帧的 MAC 标头由 3 个字段构成：

Frame Control（帧控制）

帧的 subtype（子类型）字段被设定为 1101，代表 ACK 帧。

Duration（持续时间）

根据ACK信号在整个帧交换过程中所处的位置，duration（持续时间）的值可以有两种设定方式。在完整的数据帧及一连串帧片段的最后一个片段中，duration会被设定为0。数据发送端会将Frame Control（帧控制）字段中的More Fragments（更多片段）位设定为0，表示数据传送已经结束。如果More Fragments 位为0，表示整个传送已经完成，没有必要再延长对无线信道的控制权，因此会将duration设定为0。

如果More Fragments位为1，表示尚有帧片段在传送中。此时Duration字段的用法和CTS帧中的Duration字段相同。传送ACK以及其短帧间间隔所需要的时间，将从最近的帧片段所记载的duration（持续时间）中减去。如果不是最后一个ACK帧，duration的计算方式就类似CTS duration的计算方式。事实上，802.11的规范说明书将ACK帧中的duration设定称为虚拟CTS。

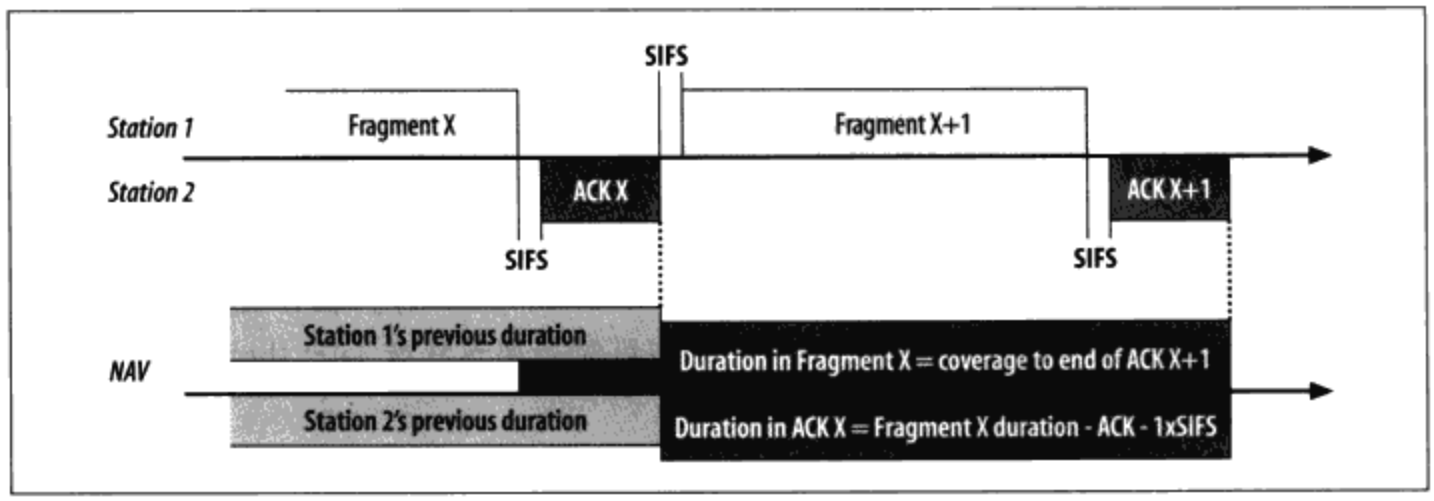


图4-18：非最终ACK帧的Duration字段

Address 1 字段：Receiver Address（接收端地址）

接收端地址是由所要确认的发送端帧复制而来。就技术而言，它是从所要确认的帧的Address 2字段复制而来。确认主要是针对数据帧、管理帧以及PS-Poll帧。

PS-Poll（省电－轮询）

当一个移动式工作站从省电模式中苏醒后，便会传送一个PS-Poll帧给接入点以取得任何缓存帧。PS-Poll帧的格式如图4-19所示。省电模式的运作方式的进一步细节详见第八章。

PS-Poll帧的MAC标头由4个字段构成：

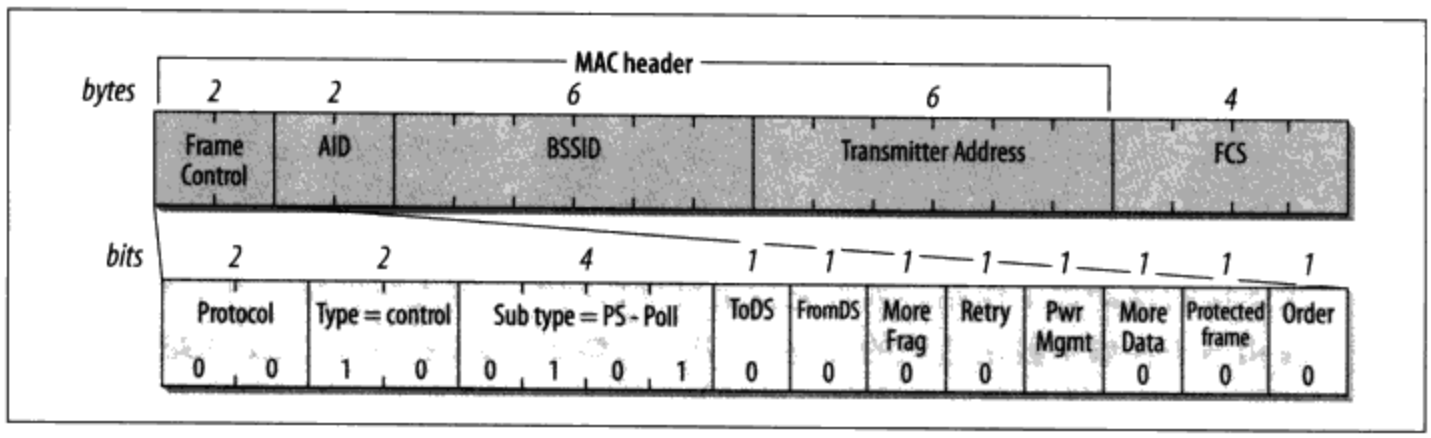


图 4-19：PS-Poll 帧

Frame Control（帧控制）

帧的 subtype（子类型）字段被设定为 1010，代表 PS-Poll 帧。

AID（关联标识符）

PS-Poll 帧会以 MAC 标头的第三位与第四位来代表关联标识符（association ID）。关联标识符是接入点指定的一个数值，用来识别关联。将此标识符放入帧中，可让接入点找出为其（移动式工作站）缓存的帧。

Address 1 字段：BSSID

此字段包含发送端当前所在 BSS 的 BSSID，此 BSS 由当前所关联的接入点创建。

Address 2 字段：Transmitter Address（传送端地址）

此为 PS-Poll 帧发送端的 MAC 地址。

在 PS-Poll 帧中并未包含 duration 信息，因此无法更新 NAV。不过，所有收到 PS-Poll 帧的工作站都会以短帧间间隔加上传送 ACK 信号所需要的时间来更新 NAV。这一自动调整机制使得接入点在传送 ACK 信号时，不容易与移动式工作站发生冲突。

关联标识符（AID）

在 PS-Poll 帧中，Duration/ID 字段是关联标识符，而非虚拟载波监听功能所使用的数值。当移动式工作站与接入点关联时，接入点会从 1~2007 这个范围内指派一个值来作为关联标识符（AID）。AID 的各种用法散见于全书。

管理帧

在 802.11 规范说明书中，管理所占据的篇幅最多。各式各样的管理帧只为了给有线网络提供相当简单的服务。对有线网络而言，识别一部工作站并非难事，毕竟控制中心与工

作站之间必须通过布线方能建立连接。有时候，配线柜(wiring closet)的插线面板(patch panel)可加速网络的构建，不过重点还是在于建立新的连接时可通过个人检查进行身份验证。

无线网络必须建立一些管理机制才能提供类似的功能。802.11将整个过程分解为三个步骤。寻求连接的移动式工作站必须首先找出可供访问的兼容无线网络。在有线网络中，这个步骤相当于在墙上找出适当的插座。其次，网络系统必须对移动式工作站进行身份验证，才能决定是否让工作站与网络系统连接。在有线网络方面，身份验证是由网络系统本身提供。如果必须通过网线才能够取得信号，那么能够使用网线至少也算得上是一种认证。最后，移动式工作站必须与接入点建立关联，这样才能访问有线骨干网络，这相当于将网线插到有线网络系统。

管理帧的结构

802.11管理帧的基本结构如图4-20所示。所有管理帧的MAC标头都一样，与帧的子类型无关。管理帧会使用信息元素（带有数字标签的数据块）来与其他系统交换信息。

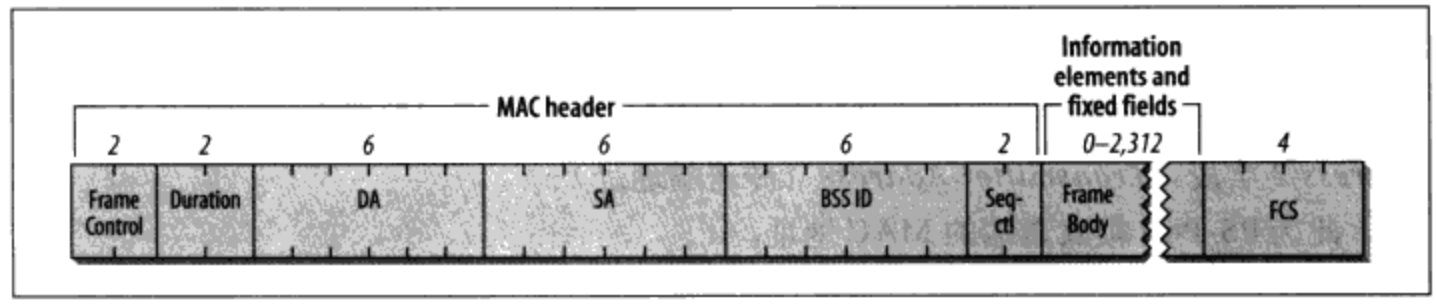


图4-20：管理帧的基本结构

地址字段

和其他帧一样，第一个地址字段是给帧的目的地地址使用的。有些管理帧主要用来维护单一BSS的特性。为了限制广播或组播管理帧所造成的副作用，收到管理帧之后，工作站必须加以查验，虽然不是所有实现均会执行这个BSSID过滤流程。只有在广播或组播帧来自工作站当前所关联的BSSID时，它们才会被送至MAC管理层。唯一的例外是Beacon帧，毕竟它是用来宣布802.11网络的存在。

BSSID是以大家熟悉的方式来指定的。接入点会以本身无线网络接口的MAC地址作为BSSID。移动式工作站会采用当前关联的接入点的BSSID。位于IBSS的工作站则会使用BSS创建之初随机产生的BSSID。唯一的例外是：寻找特定网络的工作站可以在发出的帧中指定该特定网络的BSSID，或者使用broadcast（广播型）BSSID来搜索所有邻近的网络。

计算持续时间

管理帧使用 Duration（持续时间）字段的方式和其他帧没有不同：

1. 无竞争周期内所传送的任何帧均会将持续时间设为 32768。
2. 基于竞争的访问周期内利用DCF所传送的帧会通过Duration字段防止别人访问媒介，以确保原子帧交换（atomic frame exchanges）得以完成。
   a. 如果是广播或组播帧（目的地地址为组地址），则持续时间会设定为0。广播与组播帧无需得到确认，因此 NAV 无需防止别人访问媒介。
   b. 如果不是最终片段，则持续时间会设为3个SIFS加上下一个片段及其确认所需要的微秒数。
   c. 最终帧片段的持续时间会设定为一个响应加上一个 SIFS 所需要的时间。

帧主体

管理帧十分灵活。帧主体（frame body）中的大部分数据如果使用长度固定的字段，就称为固定字段（*fixed field*）；如果字段长度不定，就称为信息元素（*information element*）。所谓信息元素，是指长度不定的数据块（data blob）。每个数据块均会标注类型编号与大小，各种信息元素的数据字段都有特定的解释方式。新版的802.11规范说明书允许定义新的信息元素，根据旧版规范说明书所实现的产品可忽略这些新元素。实现时，硬件一般采取向下兼容（backward-compatible）原则，因此较旧的产品通常无法加入根据新标准所建立的网络。还好，新功能通常可以停用，以便向下兼容。

除了探讨这些作为基本组件的固定字段与信息元素，本节还会说明这些基本组件如何构成管理帧。802.11 强制规定了这些信息元素的排列次序，不过并非所有元素均有必要。本书将以特定的顺序说明这些基本组件，谈到各个子类型时，也会特别标明哪些元素比较少见，哪些元素彼此互不兼容。

长度固定的管理帧组件

在管理帧中，可能出现的长度固定的字段有 10 种。长度固定的字段一般简称为字段（*field*），以便与长度不定的信息元素有所区别。字段本身并无标头可与帧主体的其他部分进行区别。因为长度与次序固定，所以不需要以字段标头来界定。

Authentication Algorithm Number 字段

Authentication Algorithm Number（身份验证算法编号）字段占用了2个字节，如图4-21所示。此字段代表关联发生之前，802.11层（802.11-level）的最初认证过程所使用的认

证类型（确认过程在第八章会有更详尽的探讨）。此字段容许的值范围列于表4-3中。目前只定义了两种值，其他值保留给未来版本使用。

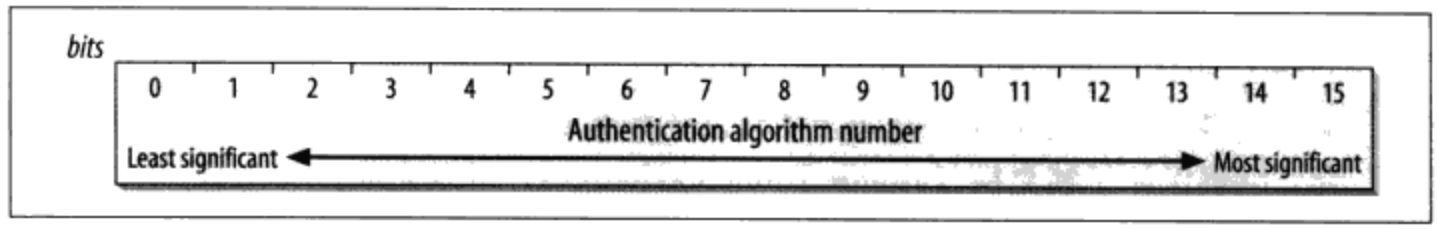


图4-21：Authentication Algorithm Number字段

表4-3：Authentication Algorithm Number字段的容许值

值	意义
0	开放系统身份验证（Open System authentication）
1	共享密钥身份验证（Shared Key authentication）
2~65535	保留

Authentication Transaction Sequence Number字段

身份验证过程分为好几个步骤，其中包含从接入点所发出的质询（challenge）以及试图关联的移动式工作站所做出的响应。如图4-22所示，Authentication Transaction Sequence Number（身份验证处理序列号）字段是由2个字节所构成，用以追踪身份验证的进度。此字段值介于1到65535之间，其值不可为0。此字段的用法将于第八章讨论。

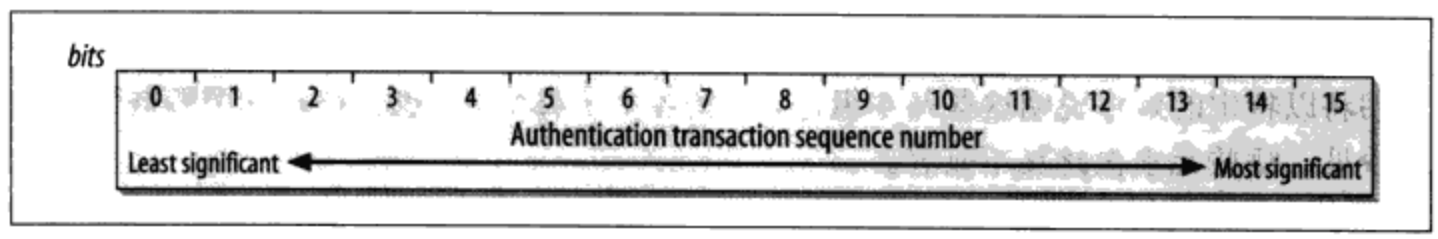


图4-22：Authentication Transaction Sequence Number字段

Beacon interval字段

每隔一段时间就会发出的Beacon（信标）信号用来宣布802.11网络的存在。Beacon帧中除了包含BSS参数的信息，也包含接入点缓存帧的信息，因此移动式工作站必须仔细聆听Beacons信号。Beacon interval（信标间隔）字段的长度为16位，用来设定Beacon信号之间相隔多少时间单位。时间单位通常缩写为TU，代表1024微秒（microsecond），

相当于1毫秒（millisecond）。有些文档中会以千－微秒（kilo-microseconds）（注3）来表示时间单位。Beacon interval 字段通常会被设定为100个时间单位，相当于每100毫秒或0.1秒传送一次 Beacon 信号。

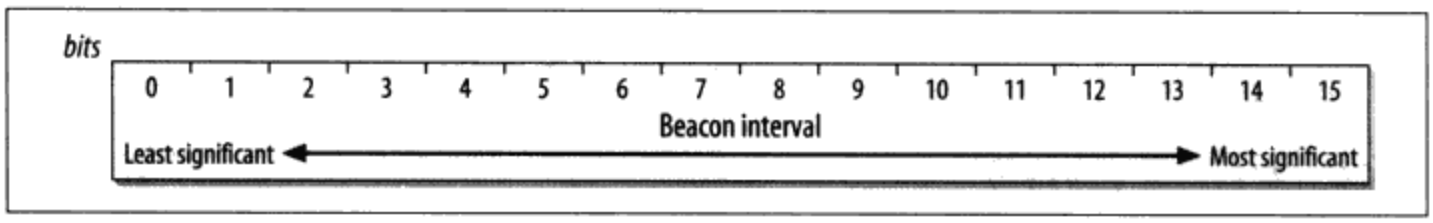


图 4-23：Beacon Interval 字段

Capability Information 字段

图 4-24 所示的是长度为16位的Capability Information（性能信息）字段，传送Beacon信号的时候，它被用来通告网络具备何种性能。Capability Information字段也可以使用在Probe Request与Probe Response帧中。在本字段中，每个位各自代表一个标记(flag)，对应到网络所具备的某种特殊功能。工作站会使用这些通告数据来判断自己是否支持该BSS 所有的功能。未实现性能通告中所有功能的工作站就无法加入该 BSS。

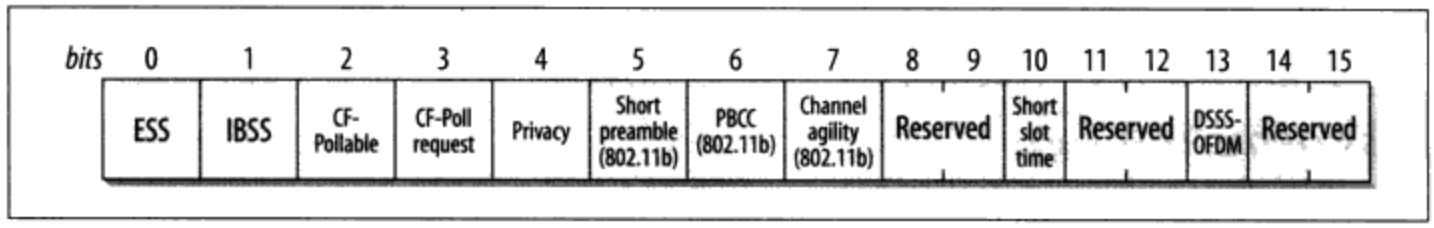


图 4-24：Capability Information 字段

ESS/IBSS（扩展服务集/独立基本服务集）

这两个位彼此互斥(mutually exclusive)。接入点会将ESS字段设定为1，而将IBSS字段设定为0，表示接入点属于infrastructure（基础结构型）网络的一部分。IBSS中的工作站则会将ESS 字段设定为0，而将IBSS 字段设定为1。

Privacy（保密性）

将Privacy 位设定为1，代表需要使用WEP以维持机密性。在infrastructure 网络中，发送端为接入点。在IBSS里，Beacon信号必须由IBSS中的某个工作站负责。

注3：千－微秒（kilo-microsecond）是相当奇怪的组合，因为它以2的乘方来计算kilo，而以较为常见的1/1000来表示 micro。想必国际度量衡局(International Bureau of Weights and Measures)可能会对这种用法提出抗议。

Short Preamble（短前导码）

802.11b 规范新增此字段是为了支持高速直接序列扩频物理层（high-rate DSSS PHY）。将之设定为 1，代表此网络目前使用短前导码（short preamble），对此第十章会有进一步的说明。0代表不使用此选项，并且在该BSS中禁止使用短前导码。802.11g 规定使用短前导码，因此在依据 802.11g 标准所构建的网络中，此字段必然被设定为 1。

PBCC（封包二进制回旋码）

802.11b 规范新增此字段是为了支持高速直接序列扩频物理层（high-rate DSSS PHY）。将之设定为 1，代表此网络目前使用第十二章所描述的封包二进制回旋码（packet binary convolution coding）调制机制，或是第十四章所描述的 802.11g PBCC调制机制。0代表不使用此选项并且在该BSS中禁止使用封包二进制回旋码。

Channel Agility（机动信道转换）

此字段加入 802.11b 规范是为了支持高速直接序列扩频物理层（high-rate DSSS PHY）。将之设定为1，代表此网络使用机动信道转换（Channel Agility）选项，对此第十二章会有进一步的说明。0代表不使用此选项并且在该BSS中禁止使用机动信道转换。

Short Slot Time（802.11g）

此位若设定为 1，代表使用 802.11 所支持的较短的时隙，这将于第十四章讨论。

DSSS-OFDM（802.11g）

此位若设定为 1，代表使用 802.11g 的 DSSS-OFDM 帧构造（frame construction）选项。

Contention-free polling（无竞争－轮询）位

工作站与接入点使用这两个位（CF-Pollable 与 CF-Poll Request）当作标签。这些标签的意义如表 4-4 所示。

表4-4：Capability Information（性能信息）字段中polling位所代表的意义

CF-Pollable 工作站的用法	CF-Poll Request	意义
0	0	工作站不支持轮询（polling）
0	1	工作站支持轮询，但并未要求置于轮询表（polling list）中
1	0	工作站支持轮询且要求将之置于轮询表中
1	1	工作站虽然支持，但要求不要对其轮询（结果是该工作站会被视为不支持无竞争操作）

表4-4：Capability Information（性能信息）字段中polling位所代表的意义（续）

CF-Pollable	CF-Poll Request	意义
接入点的用法		
0	0	接入点并未支持（实现）点协调功能（point coordination function）
0	1	接入点使用PCF来传递，但并不支持轮询
1	0	接入点使用PCF来传递与轮询
1	1	保留；尚未使用

Current AP Address 字段

移动式工作站可以使用图4-25所示的Current AP Address（当前接入点的地址）字段来表明当前关联的接入点的MAC地址。这个字段的用途是便于关联（association）与重新关联（reassociation）的进行。工作站会借此传送上一次所关联的接入点的地址。当工作站打算与不同的接入点建立关联时，此字段可用来转换关联以及取回所有缓存的帧。

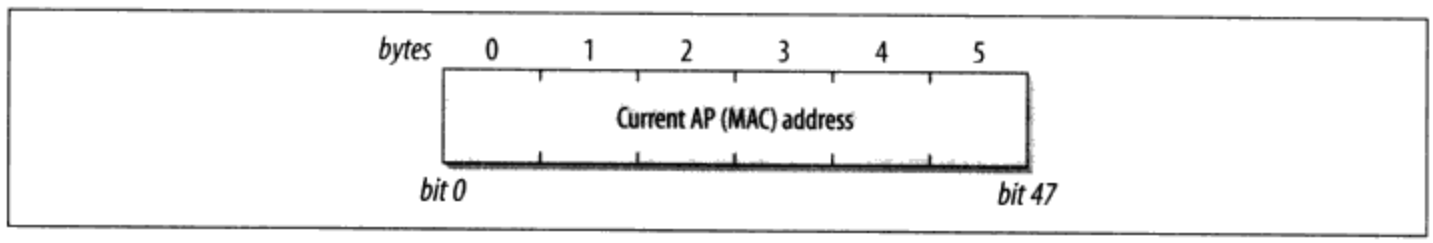


图4-25：Current AP Address 字段

Listen interval 字段

为了节省电池的电能，工作站可以暂时关闭802.11网络接口的天线。当工作站处于休眠状态时，接入点必须为之缓存帧。休眠中的工作站会定期醒来聆听往来消息，以判断是否有帧缓存于接入点。当工作站与接入点关联时，会将Listen Interval（聆听间隔）记录下来。所谓Listen Interval，其实就是以Beacon interval（信标间隔）为单位所计算出的休眠时间。图4-26所示的Listen Interval允许移动式工作站指出接入点必须为它缓存帧多长时间。聆听间隔越久，接入点就必须使用越多的内存来缓存帧。接入点可以借此项功能估计所需资源，以决定是否拒绝资源密集（resource-intensive）的关联。第八章会进一步描述Listen Interval。

Association ID 字段

图4-27所示的是长度为16位的Association ID（关联标识符）字段。当工作站与接入

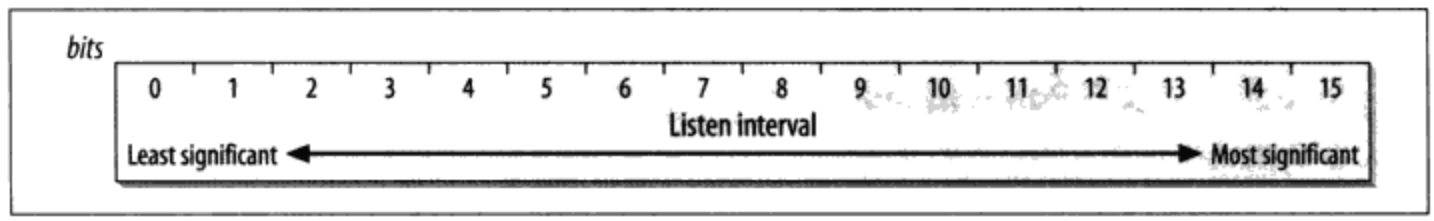


图 4-26：Listen Interval 字段

点关联时，就会被赋予一个关联标识符来协助控制与管理。虽然关联标识符的可用位数为 14，不过只有 1~2007 可以使用。为了与 MAC 标头的 Duration/ID 字段兼容，最重要的两个位均被设定为 1。

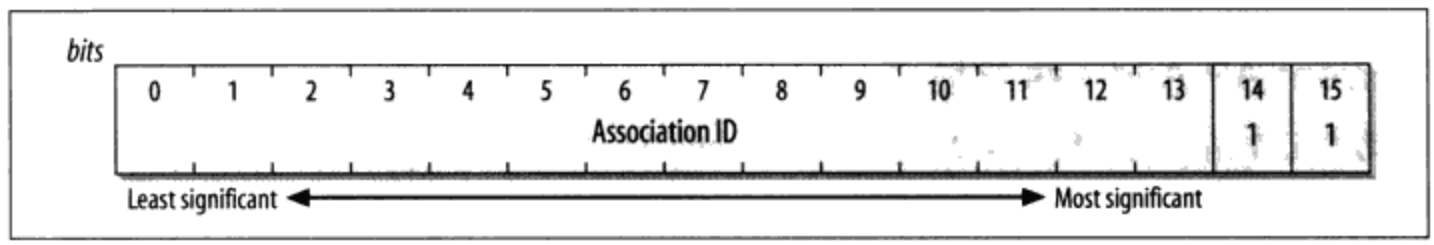


图4-27：Association ID字段

Timestamp 字段

图 4-28 所显示的Timestamp（时间戳）字段可用来同步 BSS 中的工作站。BSS 的主计时器会定期传送目前已作用的微秒数。当计数器到达最大值时便会从头开始计数。（对一个长度为64 位、可计数超过 580000 年的计数器而言，很难遇到从头开始计数的一天。）

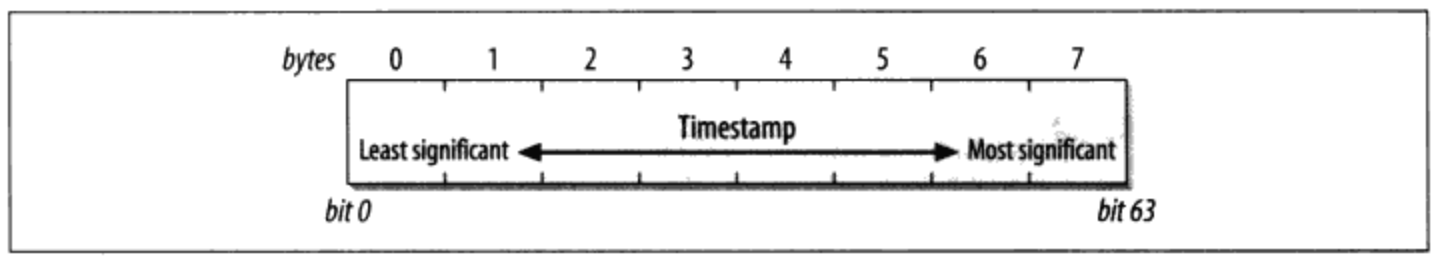


图 4-28：Timestamp 字段

Reason Code 字段

当对方不适合加入网络时，工作站会送出Disassociation（取消关联）或Deauthentication（解除身份验证）帧作为响应。这些帧中包含一个长度为 16 位的 Reason Code（原因代码）字段，表示对方的做法有误，如图 4-29 所示。表 4-5 列出了产生原因代码的理由。要完全了解原因代码的用法，必须对各种帧以及 802.11 工作站的状态有所了解。关于这一点，本节已有讨论。

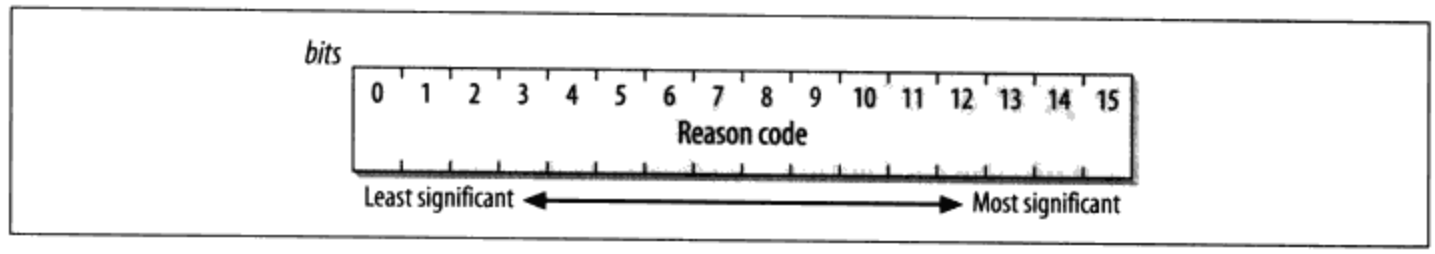


图 4-29：Reason Code 字段

表4-5：原因代码

代码	意义
0	保留；未使用
1	未指定
2	之前的身份验证无效
3	工作站已经离开基本服务区域或扩展服务区域，目前已经解除身份验证
4	闲置计时器（inactivity timer）超时且工作站已经取消关联
5	接入点资源不足，因而取消关联
6	从尚未认证的工作站收到的帧类型或子类型不正确
7	从尚未关联的工作站收到的帧类型或子类型不正确
8	工作站已经离开基本服务区域或扩展服务区域，目前已经取消关联
9	在身份验证完成之前要求关联或重新关联
10(802.11h)	无法接受 Power Capability 信息元素的设定值，因而取消关联
11(802.11h)	无法接受 Supported Channels 信息元素的设定值，因而取消关联
12	保留
13(802.11i)	信息元素不正确（802.11i 加入的原因代码，因此应该是 802.11i 的信息元素）
14(802.11i)	消息完整性校验失败
15(802.11i)	4 次密钥握手（4-way keying handshake）超时
16(802.11i)	组密钥握手（Group key handshake）超时
17(802.11i)	4 次握手信息元素的安全参数与初始参数集不符
18(802.11i)	成组密码（group cipher）不正确
19(802.11i)	成对密码（pairwise cipher）不正确
20(802.11i)	身份验证与密钥管理协议不正确
21(802.11i)	未支持的强健安全网络信息元素（RSN IE）版本
22(802.11i)	RSN IE 的性能（capability）项不正确
23(802.11i)	802.1X 身份验证失败

表4-5：原因代码（续）

代码	意义
24(802.11i)	所设定的使用策略（policy）拒绝所提议的密码组
25-65,535	保留；未使用

Status Code 字段

状态码用来表示某项操作成功或失败。Status Code（状态码）字段如图 4-30 所示。如果某项操作成功，该字段的值就会被设定为0，否则被设为非零值。表4-6列出了标准的状态码。

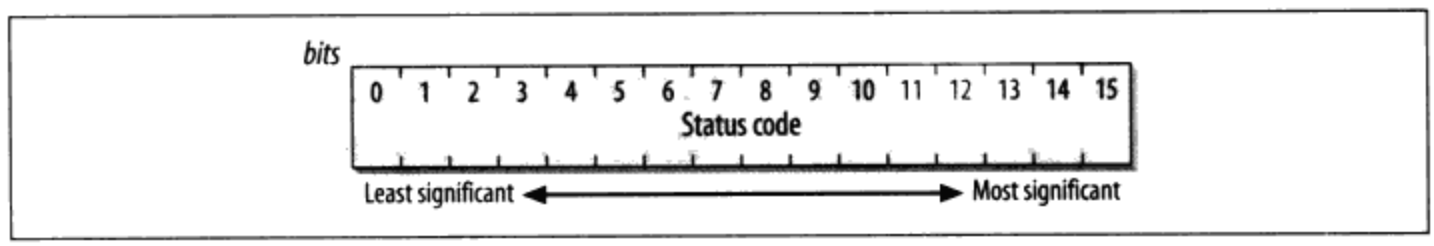


图 4-30：Status Code 字段

表4-6：状态码

代码	意义
0	操作成功
1	未指定失败原因
2~9	保留；未使用
10	所要求的性能范围过广无法支持
11	拒绝重新关联；之前的关联无法识别与转移
12	拒绝关联，原因是不在 802.11 标准所指定的范围内
13	不支持所使用的身份验证算法
14	超乎预期的身份验证序号
15	身份验证被拒绝；响应信息有误
16	身份验证被拒绝；下一个帧并未出现在预定的窗口内
17	关联被拒绝；接入点资源有限
18	关联被拒绝；工作站并未支持 BSS 要求的所有数据传送速率
19(802.11b)	关联被拒绝；工作站并未支持 Short Preamble 功能
20(802.11b)	关联被拒绝；工作站并未支持 PBCC 调制功能

表4-6：状态码（续）

代码	意义
21(802.11b)	关联被拒绝；工作站并未支持 Channel Agility 功能
22(802.11h)	关联被拒绝；需要 Spectrum Management 功能
23(802.11h)	关联被拒绝；不接受 Power Capability 值
24(802.11h)	关联被拒绝；不接受 Supported Channels
25(802.11g)	关联被拒绝；工作站并未支持 Short Slot Time 功能
26(802.11g)	关联被拒绝；工作站并未支持 DSSS-OFDM 功能
27~39	保留
40(802.11i)	信息元素不正确
41(802.11i)	成组（广播/组播）密码不正确
42(802.11i)	成对（单播）密码不正确
43(802.11i)	身份验证与密钥管理协议（AKMP）不正确
44(802.11i)	未支持的强健安全网络信息元素（RSN IE）版本
45(802.11i)	不支持此 RSN IE 性能（capability）
46(802.11i)	密码组被使用策略拒绝
47-65,535	保留给未来的标准使用

管理帧的信息元素

信息元素（information element）是管理帧的可变长组件。信息元素通常包含一个 Element ID（元素标识符）字段、一个 Length（长度）字段以及一个长度不定的字段，如图 4-31 所示。Element ID 编号的标准值如表 4-7 所示。

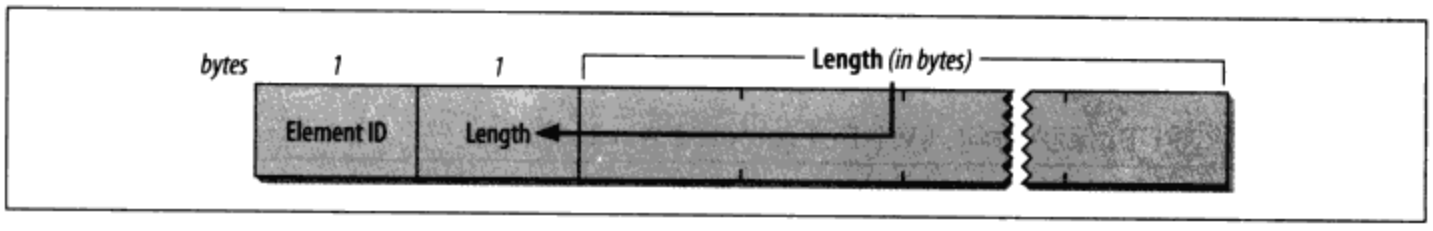


图 4-31：一般管理帧的信息元素

表4-7：信息元素

Element ID	名称
0	服务集标识符（SSID）
1	所支持的速率（Supported Rates）

表4-7：信息元素（续）

Element ID	名称
2	跳频参数集（FH Parameter Set）
3	直接序列参数集（DS Parameter Set）
4	无竞争参数集（CF Parameter Set）
5	传输指示映射（TIM）
6	IBSS 参数集
7-15	保留；未使用
16	质询文本（challenge text）
17~31	保留[a]（在802.11共享密钥身份验证停用之前，保留给质询文本作为未来扩充用）
32(802.11h)	功率限制（Power Constraint）
33(802.11h)	功率性能（Power Capability）
34(802.11h)	发送功率控制请求（Transmit Power Control (TPC) Request）
35(802.11h)	发送功率控制报告（TPC Report）
36(802.11h)	所支持的信道（Supported Channels）
37(802.11h)	信道切换声明（Channel Switch Announcement）
38(802.11h)	测量请求（Measurement Request）
39(802.11h)	测量报告（Measurement Report）
40(802.11h)	静默（Quiet）
41(802.11h)	IBSS 动态选频（IBSS DFS）
42(802.11g)	ERP 信息（ERP information）
43~49	保留
48(802.11i)	强健安全网络（Robust Security Network）
50(802.11g)	扩展支持速率（Extended Supported Rates）
32~255	保留；未使用
221[b]	Wi-Fi 保护访问（Wi-Fi Protected Access）

a: 由于不再建议使用 802.11 共享密钥身份验证，因此未来应该不会用到这些字段。

b: 此为 WPA 使用的信息元素，并不属于 802.11 官方版本的内容。不过这项功能在实现时十分常见，因此将它列在此表中。

Service Set Identity（SSID）信息元素

网络管理人员通常比较喜欢跟文字、数字或名称打交道，而不是48位的MAC地址。广义的 802.11 网络不是扩展服务集（extended service set），就是独立基本服务集

(independent BSS)。如图 4-32 所示的 SSID 允许网管人员为服务集（service set）指定标识符。试图加入网络的工作站可以扫描当前区域的所有网络，然后以特定的 SSID 加入。共同组成扩展服务区域（extended service area）的所有基本服务区域（basic service area）都会使用相同的 SSID。

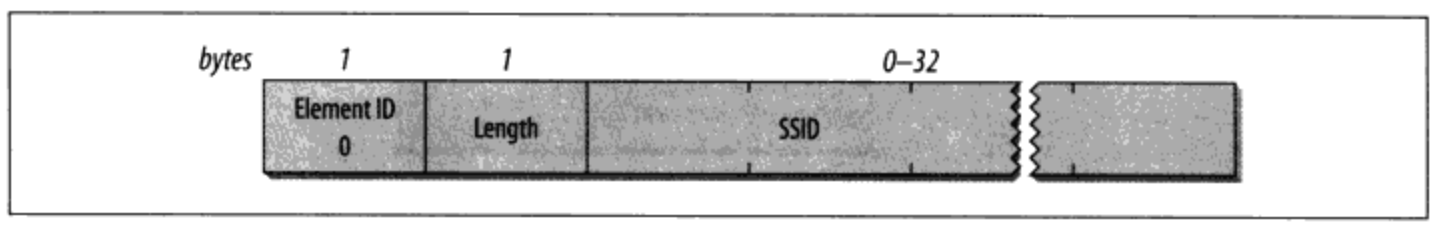


图 4-32：SSID（服务集标识符）信息元素

有些文档将 SSID 视为网络名称，因为网管人员通常以字符串来指定 SSID。其实，SSID 不过是由字节所形成的字符串，用来标示所属网络的BSSID。有些产品要求此字符串必须是以 null（即 0）结尾的 ASCII 字符串，虽然标准对此并无特别规范。

SSID 的长度介于 0 至 32 个字节之间。如果完全不加指定，这种特例就称为 *broadcast SSID*。broadcast SSID 只用于 Probe Request 帧，工作站可以借此找出该区域中所有的 802.11 网络。

Supported Rates 信息元素

无线局域网支持数种标准速率。802.11 网络可以使用 Supported Rates（所支持的速率）信息元素来指定其所支持的速率。当移动式工作站试图加入网络时，会先查看该网络所使用的数据速率。有些速率是强制性的，每个工作站都必须支持，有些则是选择性的。

Supported Rates 信息元素如图 4-33 所示。它是由一串字节构成。每个字节会使用 7 个低位来代表数据速率（data rate）；最高位则是用来表示该数据速率是否为强制性的。如果是强制性速率，则最高位为1；非强制性速率则为0。此信息元素最多可包括8种速率。随着各种数据速率的增加，目前已将 Extended Supported Rates（扩展支持速率）元素标准化，以便处理 8 种以上的速率。

在802.11 规范说明书最初的版本中，是以7个位来对数据速率进行编码，而数据速率为 500 kbps 的倍数。新的技术，特别是 ETSI 的 HIPERLAN，必须以不同的方式来解读。当这 7 个位用来编码数据速率时，每种编码均为500 kbps的倍数，那么可编码的最高数据速率为63.5 Mbps。无线网络的改进与发展，使得这个速率在不久的将来即可实现。因此，IEEE 在802.11b 中改用简单的标记来代表所支持的速率。先前已经标准化的速率则根据500 kbps的倍数予以标记，不过未来的标准可能会有所变动。目前使用的标准值如表 4-8 所示。

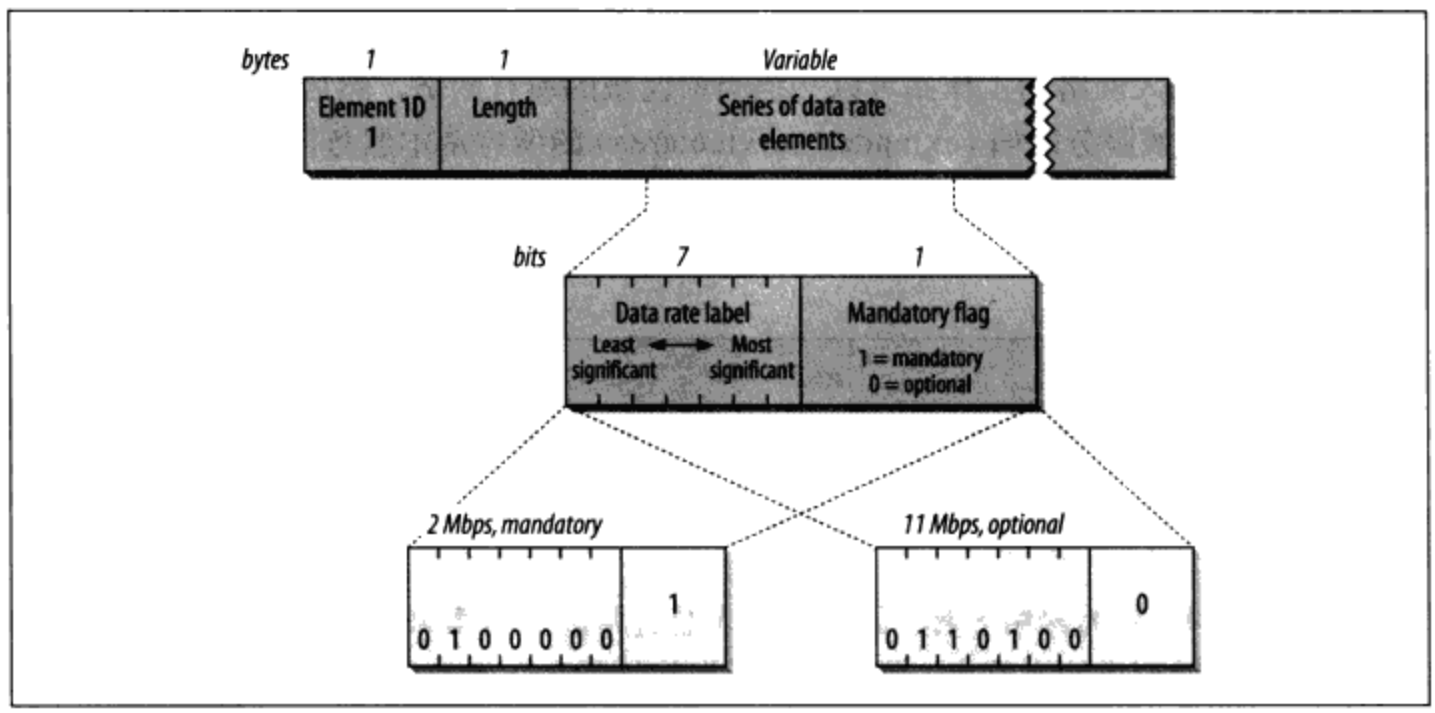


图4-33：Supported Rates（所支持的速率）信息元素

表4-8：数据速率标签

二进制数值	相应的速率（Mbps）
2	1
4	2
11(802.11b)	5.5
12(802.11g)	6
18(802.11g)	9
22(802.11b)	11
24(802.11g)	12
36(802.11g)	18
44(802.11g)	22（802.11g PBCC 可选项）
48(802.11g)	24
66(802.11g)	33（802.11g PBCC 可选项）
72(802.11g)	36
96(802.11g)	48
108(802.11g)	54

图4-33显示了如何同时编码两种数据速率。除了支持强制性的2-Mbps服务，也支持选择性的11-Mbps服务。

FH Parameter Set 信息元素

FH Parameter Set（跳频参数集）信息元素如图 4-34 所示，其中包含了加入 802.11 跳频（frequency-hopping）网络所需要的参数。

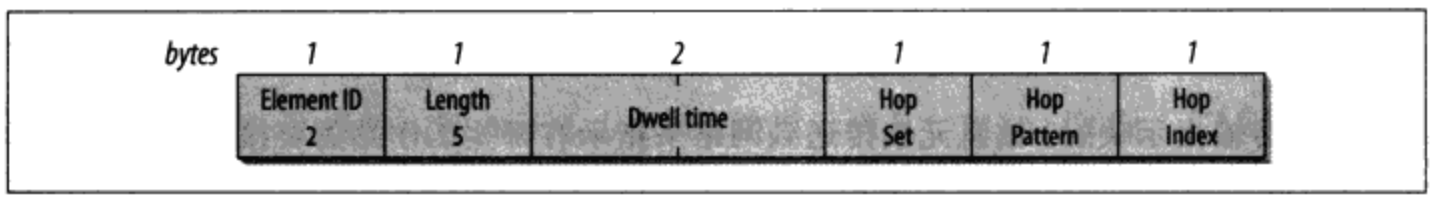


图 4-34：FH Parameter Set（跳频参数集）信息元素

在 FH Parameter Set 中有 4 个特别针对 802.11 跳频式网络的字段。对此第十二章会有更深入的描述。

Dwell Time（驻留时间）

802.11 FH网络会在信道与信道之间跳跃。停留在每个信道上的时间称为*dwell time*（驻留时间）。驻留时间是以时间单位（time unit，简称 TU）来表示。

Hop Set（跳频组合）

802.11 跳频物理层定义了若干跳频模式（hopping pattern）。此字段的长度为 1 个字节，代表使用的跳频模式组合。

Hop Pattern（跳频模式）

工作站从跳频集中挑出一种跳频模式。此字段的长度为 1 个字节，代表所使用的跳频模式。

Hop Index（跳频索引）

每种跳频模式均包含一组跳频序列。此字段的长度为 1 个字节，代表当前位于跳频序列的哪一点上。

DS Parameter Set 信息元素

802.11 直接序列（Direct-sequence）网络只有一个参数：网络所使用的信道数。高速直接序列（high-rate direct sequence）网络使用相同的信道，因此可以使用相同的参数集。信道数以 1 个字节进行编码，如图 4-35 所示。

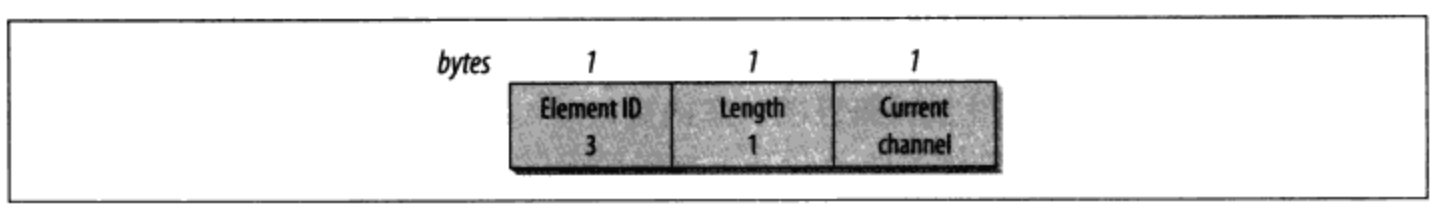


图 4-35：DS Parameter Set（直接序列参数集）信息元素

Traffic Indication Map（TIM）信息元素

接入点会为处于休睡状态的工作站缓存帧。每隔一段时间，接入点就会尝试传送这些缓存帧给休眠中的工作站。这样安排的理由是，启动发送器比启动接收器所耗费的电力要多。802.11的设计者预见到未来将会有以电池供电的移动式工作站定期传送缓存帧给工作站的决定，这主要是为了延长设备的电池使用时间。

将TIM（传输指示映射）信息元素传送到网络来指示有哪些工作站需要接收待传数据只是此操作的一部分。

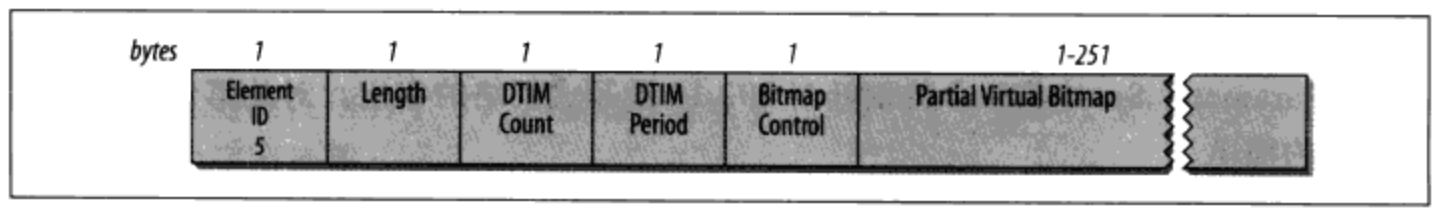


图4-36：Traffic Indication Map（传输指示映射）信息元素

TIM的内容是虚拟位映射（*virtual bitmap*），这是由2008个位组成的逻辑结构。每个位分别绑定到一个关联标识符（Association ID）。当某个关联标识符有数据缓存时，相应的位就会设成1；否则会设成0。

DTIM Count（DTIM 计数）

此字段的长度为1个字节，代表下一个DTIM（Delivery Traffic Indication Map，延迟传输指示映射）帧前即将传送的Beacon帧数。DTIM帧用来表示所缓存的广播与组播帧即将被传送。并非所有Beacon帧都为DTIM帧。

DTIM Period（DTIM 周期）

此字段的长度为1个字节，代表两个DTIM帧之间的Beacon间隔数。值0目前保留未用。DTIM会由此周期倒数至0。

Bitmap Control（位映射控制）与Partial Virtual Bitmap（部分虚拟位映射）

Bitmap Control（位映射控制）字段可进一步划分为2个子字段。位0用来表示关联标识符0的待传状态，主要是保留给组播（multicast）使用。其他7个位则是保留给Bitmap Offset（位映射偏移）子字段使用。

为了节省带宽，可以通过Bitmap Offset子字段，只传送一部分“虚拟位映射”。Bitmap Offset是与虚拟位映射的开头处相关联。利用Bitmap Offset子字段及Length字段，802.11工作站可以推断虚拟位映射有哪些部分包括在内。

CF Parameter Set 信息元素

CF Parameter Set（无竞争参数集）信息元素出现在支持无竞争（contention-free）操作的接入点所传送的 Beacon 帧中。无竞争服务并非必要，因此留待第九章讨论。

IBSS Parameter Set 信息元素

IBSS 目前只有一个参数，即 ATIM（通知传输指示消息）窗口，如图 4-37 所示。此字段只用于IBSS Beacon 帧，用来表示IBSS 中 ATIM 帧之间相隔的时间单位（TU）数量。

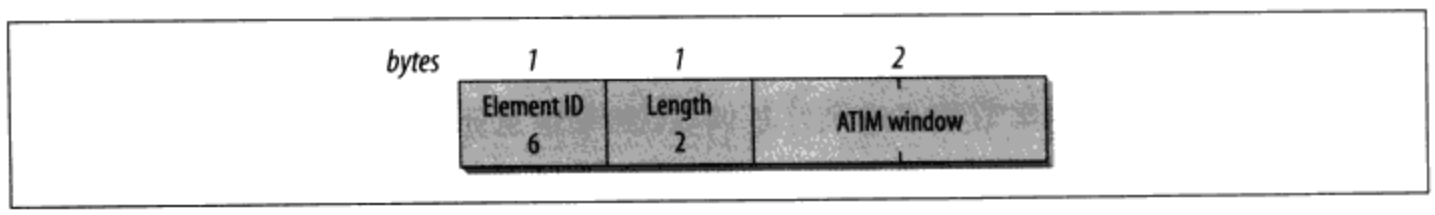


图 4-37：IBSS 参数集信息元素

Country 信息元素

802.11规范说明书原本是针对主要的工业化国家现有的管理规定所设计的。为了避免每新增一个国家就得重新修订规范，因此在规范说明书中加入新的规定，让网络能够提供管理规范给新加入的工作站。此机制的核心就是 Country 信息元素，如图 4-38 所示。

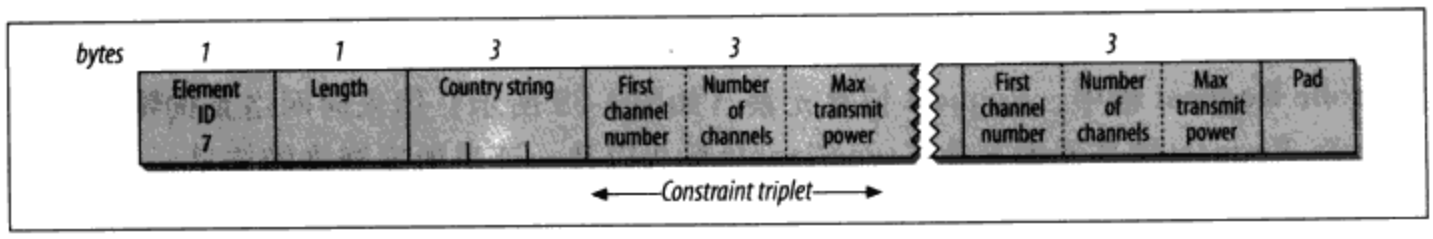


图 4-38：Country 信息元素

在type/length信息元素标头之后的是国家标识符（country identifier），之后是一系列由 3 个字节构成的用于限制的描述符（three-byte descriptor）。每组限制描述均注明特定频段，它们彼此不会重复，因为每个特定频率只会有一个最大允许功率。

Country String（国家字符串，3 个字节）

由 3 个字符所构成的ASCII字符串，代表工作站的使用国家。前两个字符即ISO国家代码（例如US代表美国）。有些国家对于室内与室外有不同的管理规定，第三个字符即是用来区别这个的。如果室内室外的管理规定相同，第三个字符则为空白。如果只想指定室内或室外的管理规定，可以分别将第三个字符设为“I”或“O”。

First Channel Number（第一信道编号，1 个字节）

第一信道编号是符合功率限制的最低信道。每种PHY所指定的信道编号将于适当的章节探讨。

Number of Channels（信道数，1 个字节）

符合功率限制的频段大小是由信道数来指定的。信道大小随PHY的不同而有所不同。

Maximum Transmit Power（最大传送功率，1 个字节）

最大传送功率，以dBm为单位。

Pad（补零码，1 个字节；可有可无）

信息元素所使用的字节数必须刚好是偶数。如果信息元素的长度恰为奇数，就必须用一个字节补零。

Hopping Pattern Parameter（跳频模式参数）与 Hopping Pattern Table（跳频模式表）信息元素

第十一章所描述的802.11跳频规范是根据设计当时的管理规定所制定的。这两个元素可以用来制定新的跳频样式，以便符合其他国家的管理规定。如此一来，若要采用不同的跳频物理层，就不需要进一步修订规范说明书了。

Request 信息元素

在Probe Request帧中，Request信息元素（如图4-39所示）用来向网络查询特定的信息元素。Request信息元素本身有type/length标头以及一连串所要查询的信息元素编号。

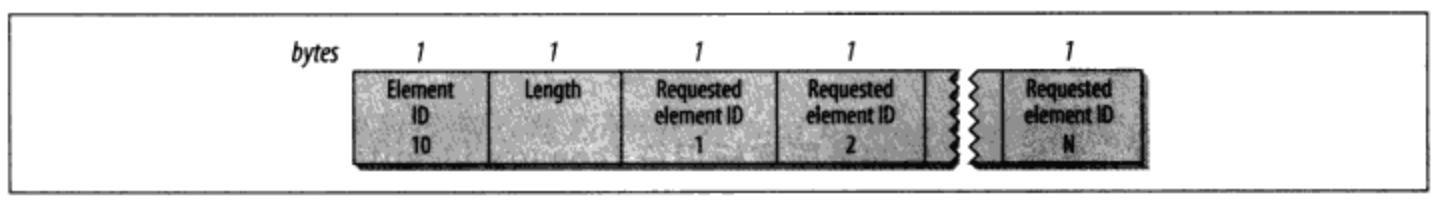


图4-39：Request信息元素

Challenge Text 信息元素

802.11所定义的共享密钥（shared-key）身份验证系统会要求移动式工作站必须成功解码一个加密过的质询。这个质询使用Challenge Text（质询文本）信息元素进行传送，如图4-40所示。

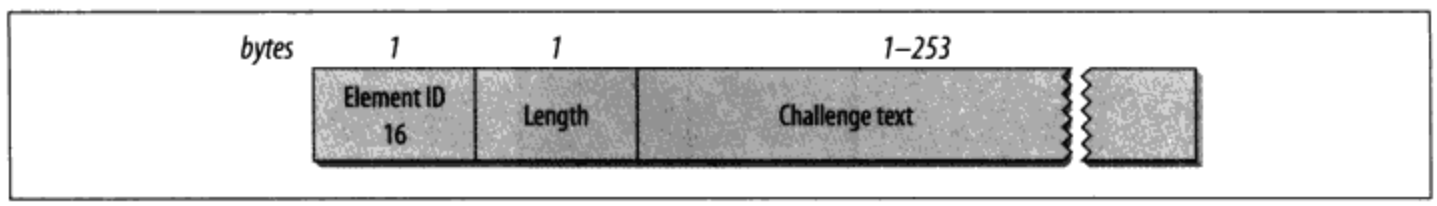


图 4-40：Challenge Text（质询文本）信息元素

Power Constraint 信息元素

Power Constraint（功率限制）信息元素允许网络向工作站描述其所允许的最大传送功率。除了规定上的最大值，另外还有实际使用时的最大值。此信息元素只有 1 个字段，长度为 1 个字节，其中记录的整数值是规定上的最大值减去实际使用时的最大值，以 dBm 为单位。例如，假设规定上允许的最大功率为 10 dBm，但是此信息元素值为 2，那么此工作站就会将本身的最大传送功率设为 8 dBm（如图 4-41 所示）。

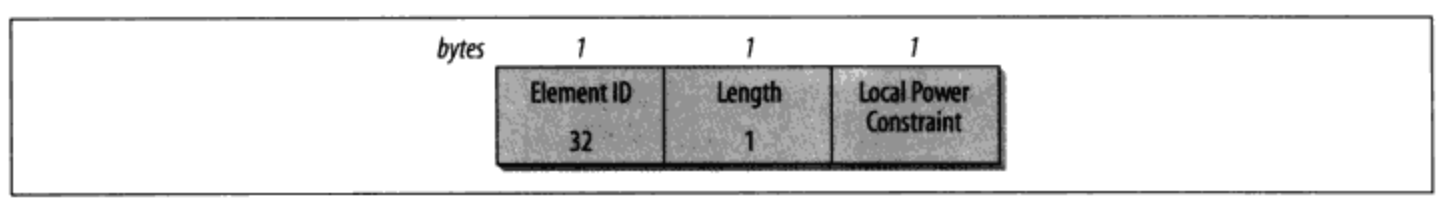


图 4-41：Power Constraint（功率限制）信息元素

Power Capability 信息元素

802.11 工作站通常以电池供电，在无线电波的性能上无法与接入点相提并论。还有部分原因是，移动式工作站通常不需要像接入点那样以高功率进行传送。Power Capability（功率性能）信息元素让工作站能够报告本身最低与最高的传送功率，以dBm为单位（如图 4-42 所示）。

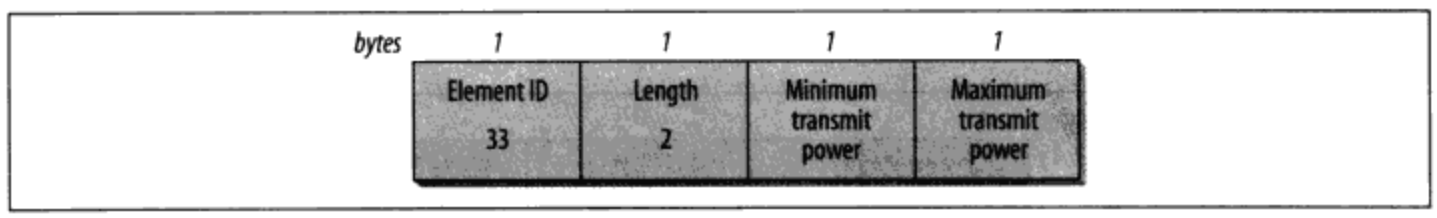


图 4-42：Power Capability（功率性能）信息元素

TPC Request 信息元素

Transmit Power Control（传送功率控制，简称 TPC）Request 信息元素用来请求无线链路管理信息。此信息元素并无其他关联的数据，因此长度字段必然为0（如图4-43所示）。

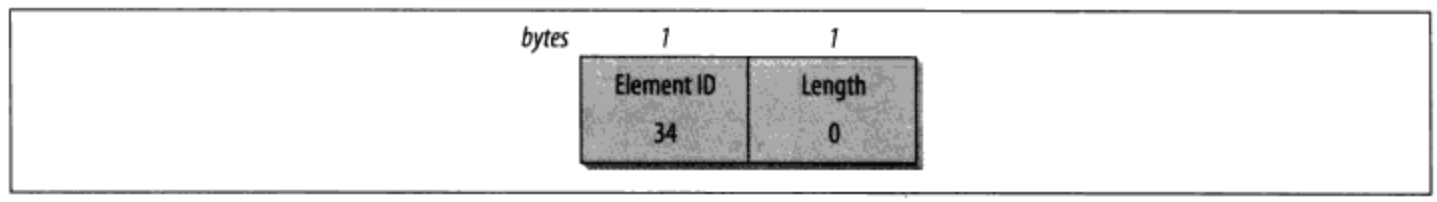


图4-43：TPC Request信息元素

TPC Report信息元素

知道整个链路的衰减情况可以帮助工作站了解该如何调整传送功率。TPC Report信息元素散见于各种管理帧中，由两个长度各为1个字节的字段构成（如图4-44所示）。第一个字段代表传送功率，即包含此信息元素的帧的传送功率，以dBm为单位。第二个字段代表链路界限（link margin），即工作站所提出的安全界限值，同样以dBm为单位。工作站将会根据这两个值来调整本身的传送功率，就像第八章所说的那样。

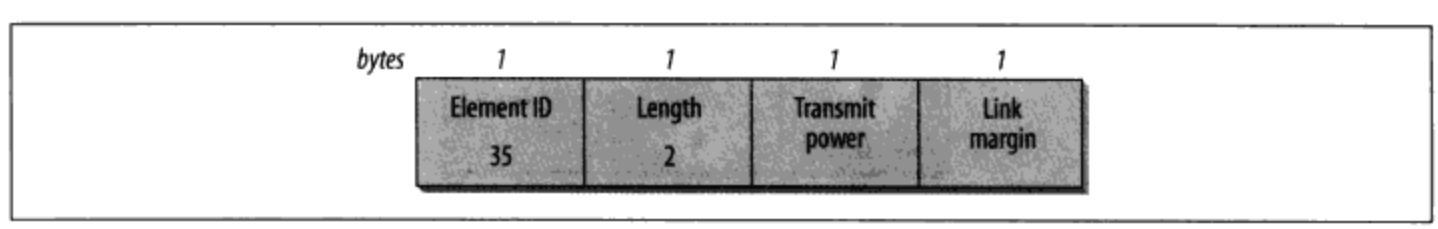


图4-44：TPC Report信息元素

Supported Channel信息元素

Supported Channel（所支持的信道）信息元素与Country信息元素相似，用来记载所支持的子频段。在标头之后的是一系列子频段的描述符（sub-band descriptor）。每组子频段描述符由第一信道编号，即所支持的子频段中的最低信道，以及子频段的信道数组成（如图4-45所示）。举例来说，如果设备只支持信道40至52，那么第一信道编号即为40，信道数则为12。

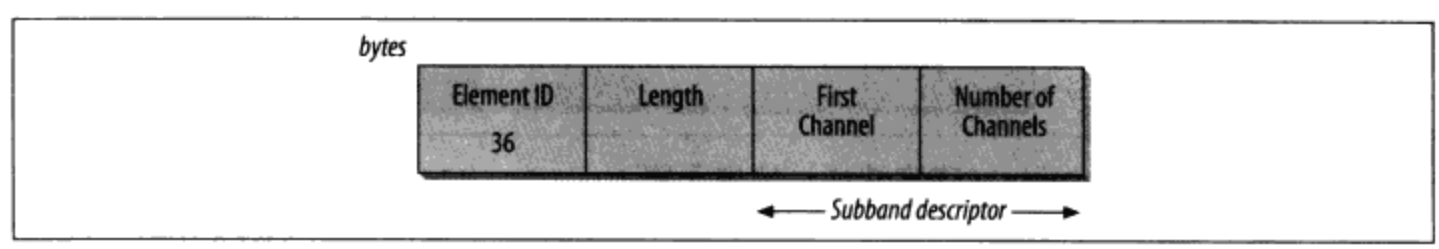


图4-45：Supported Channel（所支持的信道）信息元素

Channel Switch Announcement信息元素

802.11h为网络加入了动态切换信道的能力。为了警告网络中的工作站即将变换信道，可

以在管理帧中加入如图 4-46 所示的 Channel Switch Announcement（信道切换声明）信息元素。

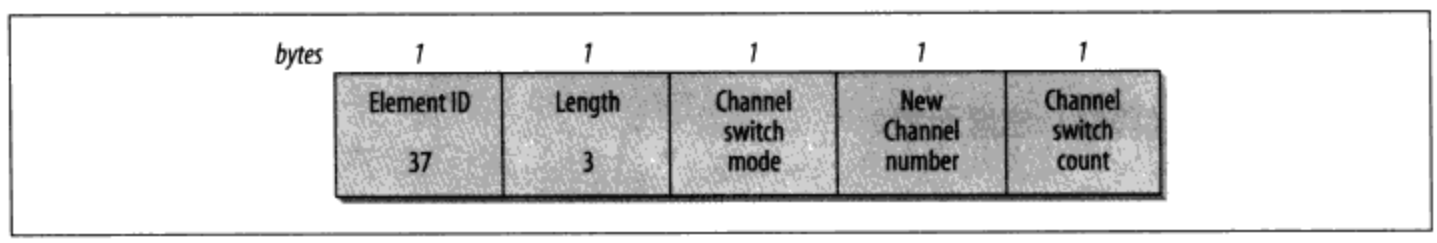


图 4-46：Channel Switch Announcement（通道切换声明）信息元素

Channel Switch Mode（信道切换模式）

当操作信道改变时，通信会突然中断。如果此字段设定为 1，已关联的工作站就会停止传送帧，直到信道切换完成；如果设定为 0，则帧的传送就不受限制。

New Channel Number（新信道编号）

切换后的新信道编号。目前此字段的值尚不需要超过 255。

Channel Switch Count（信道切换计时）

信道切换可以被预先安排时间。此字段记载了再过多少 Beacon 帧间间隔后进行信道切换。信道切换会在传送 Beacon 帧之前进行。非零值代表等待多少个 Beacon 间隔；0 代表信道切换可以立刻进行，无需多作警告。

Measurement Request（测量请求）与 Measurement Report（测量报告）信息元素

对于信道与功率设定的监控而言，定期进行信道测量十分重要。为了让工作站能够提出测量请求与接收量测报告，因此定义了这两种信息元素。测量报告属于 802.11h 的关键组件，将于第八章的“频谱管理”一节中详细探讨。

Quiet 信息元素

开发动态选频的理由之一，是为了避免与特定的军用雷达技术彼此干扰。要找出是否有雷达或其他干扰源存在，接入点可以使用 Quite（静默）信息元素来暂时关闭该信道，以改善测量的质量，如图 4-47 所示。

在标头之后有 4 个字段：

Quiet Count（静默计时）

静默期可以被预先安排。此字段记载了再过多少 Beacon 间隔后开始进入静默期。它的运作方式类似于 Channel Switch Count 字段。

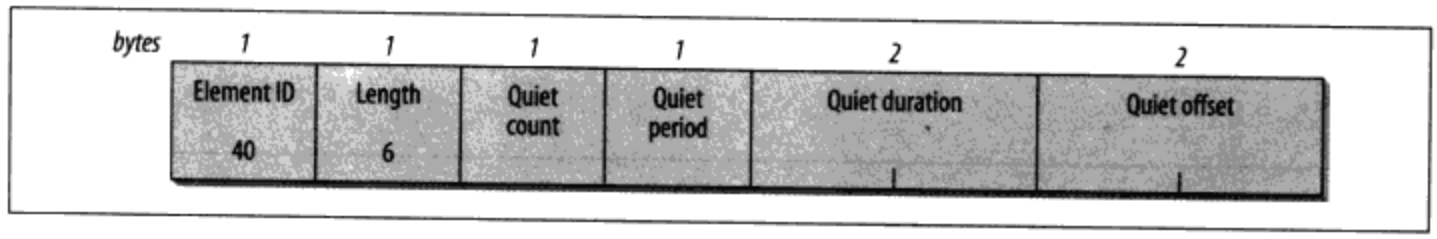


图4-47：Quiet（静默）信息元素

Quiet Period（静默期）

静默期也可以被定期地预先安排。如果此字段值为0，代表没有预先安排的静默期；非零值则代表每段禁声期之间相距多少 Beacon 间隔。

Quiet Duration（静默持续时间）

静默期不一定要持续一整个Beacon间隔（时间）。此字段用来指定静默期打算持续多少个单位时间。

Quiet Offset（静默偏移时间）

静默期不一定要始于某个Beacon间隔。此字段用来指定Beacon间隔开始后经过多少个单位时间后开始进入下一个静默期。这个值必须小于 Beacon 间隔（时间）。

IBSS DFS 信息元素

在基础结构型（infrastructure）网络里，接入点负责动态选频（dynamic frequency selection，简称 DFS）。至于独立型（independent）网络，则必须有指定由谁进行动态选频的算法。在 IBSS 中负责动态选频的工作站可以在管理帧中传递 IBSS DFS 信息元素，如图 4-48 所示。

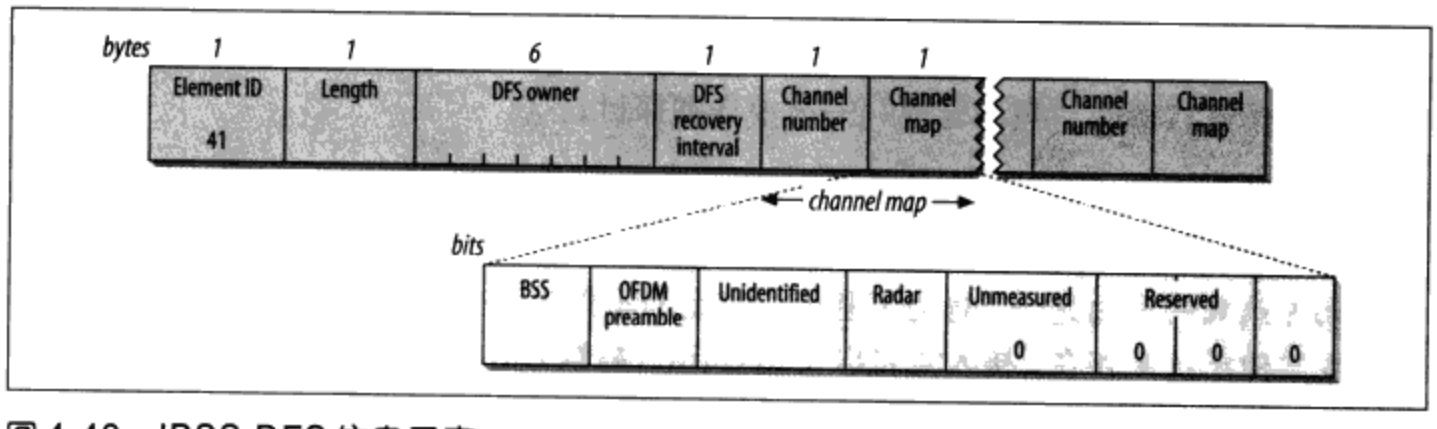


图4-48：IBSS DFS信息元素

紧跟在标头之后的是负责维护DFS信息的工作站的MAC地址以及测量间隔。之后就是一系列的信道映射表（channel map），用来报告在每个信道上都探测到什么。信道映射表由一个信道编号以及一个映射字节构成，其中包含下列字段：

BSS（1 位）

如果在测量期间探测到来自其他网络的帧，则此位会被设定。

OFDM Preamble（1 位）

如果探测到 802.11a 的短训练序列（short training sequence），但其余的帧并未追随其后，则此位会被设定。HIPERLAN/2 网络采用的是一样的前导码，但显然是使用不同的帧结构。

Unidentified Signal（1 位）

当接收到的信号功率颇高，但无法分辨此信号究竟是来自另一个 802.11 网络（因此要设定 BSS 位）、另一个 OFDM 网络（因此要设定 OFDM Preamble 位）还是一个雷达信号（因此要设定 Radar 位），则此位就会被设定。标准中并未明确规范功率必须高到何种程度才可以设定此位。

Radar（1 位）

如果在测量期间探测到雷达信号，则此位会被设定。必须探测哪些雷达系统由管理当局定义，而非 802.11 任务组。

Unmeasured（1 位）

如果未曾测量该信道，则此位会被设定。如果未曾测量，当然也就探测不到任何东西，因此上述 4 位均会被设定为 0。

ERP 信息

802.11g 定义了增强速率物理层（extended rate PHY，简称 ERP）。为了向下兼容，另外定义了 ERP 信息元素，如图 4-49 所示。在最初的定义里，它相当于一个字节中的 3 个位标记（flag）。

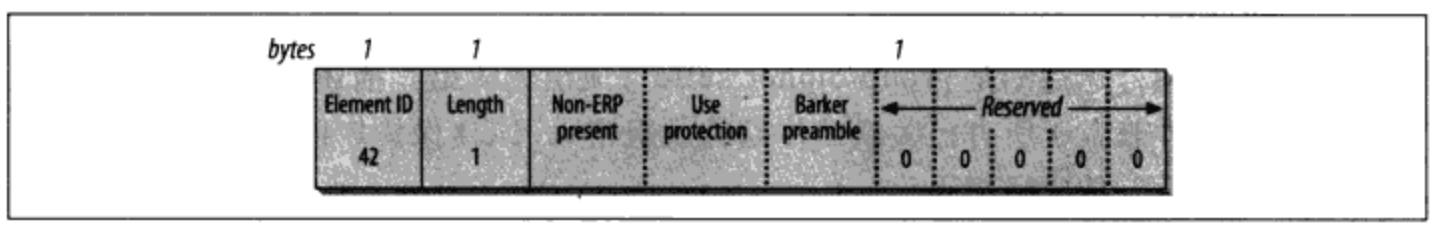


图 4-49：ERP 信息元素

Non-ERP present（无 ERP 信息）

当比较老旧、非 802.11g 的工作站与网络关联时，就会设定此位。如果探测到相邻网络无法使用 802.11g，也会设定此位。

Use Protection（使用保护机制）

当网络中出现无法以802.11g的数据速率运作的工作站，此防护位就会被设定为1。这样一来就可以向下兼容于比较旧的工作站，如第十四章所述。

Barker Preamble Mode（Barker 前导码模式）

如果关联到网络的工作站没有能力使用第十二章所描述的短前导码模式，则此位就会被设定。

Robust Security Network（RSN）信息元素

既然 802.11i 大幅改善了安全性，因此有必要开发一种方式，让工作站之间能够彼此交换安全性信息。用来实现此目标的主要工具即是Robust Security Network（强健安全网络，简称RSN）信息元素，如图 4-50 所示。其中包含几种可变的成分，在某些情况下，就算不计标头，RSN 信息元素也有可能超出信息元素长度的 255 个字节的限制。

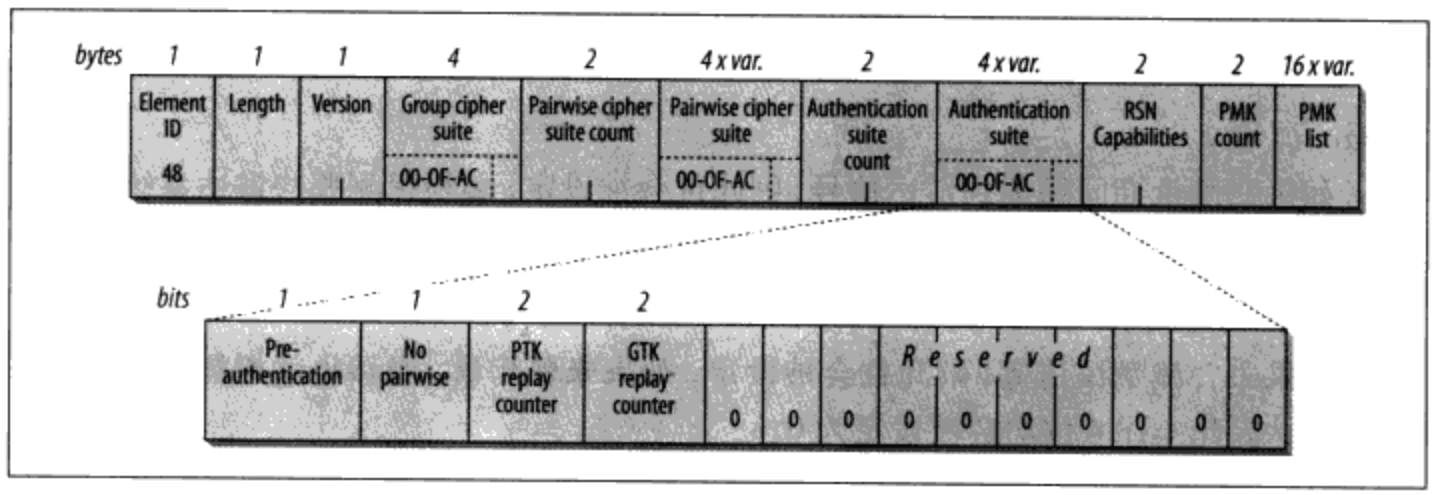


图 4-50：Robust Security Network（强健安全网络）信息元素

Version（版本）

Version 属于必要字段。802.11i 定义了版本 1，0 保留未用，版本 2 及以上则尚未定义。

Group cipher suite（成组密码组）

紧跟版本编号之后的是 group cipher suite（成组密码组）描述符。接入点必须从中选择一种兼容于所有已关联工作站的成组密码，以便保护广播与组播帧。同时间只允许选择一种成组密码。

密码组选择器（cipher suite selector）的长度为 4 个字节，由厂商的OUI以及代表密码的编号组成。标准化的密码组如表 4-9 所示（未出现在该表的值代表保留未用）。802.11i 所使用的 OUI 为 00-0F-AC，为 802.11 工作组所拥有。

表4-9：密码组

OUI	组类型	定义
00-0F-AC(802.11)	0	使用成组密码组（只对成对密码有效）
00-0F-AC	1	WEP-40

表4-9：密码组（续）

OUI	组类型	定义
00-0F-AC	2	TKIP
00-0F-AC	3	保留
00-0F-AC	4	CCMP
00-0F-AC	5	WEP-104

Pairwise Cipher Suite (count + list)（成对密码组（计数 + 列表））

除了成组密码组，必然要有一些用来保护单播（unicast）帧的成对密码组。它是由2个字节的计数以及一系列其所支持的密码描述符所组成。密码组选择器（cipher suite selector）可以设定为0，代表只支持分组密码组。除了信息元素的大小之外，支持多少成对密码并无限制。

Authentication and Key Management (AKM) suite (count + list)（身份验证与密钥管理组（计数 + 列表））

和成对密码组选择器（pairwise cipher suite selector）一样，目前也存在好几种身份验证类型。它是由计数以及一系列4个字节的标识符所构成。和密码组一样，由4个字节所构成的标识符包含了一个OUI以及一组类型编号。标准的身份验证类型如表4-10所示。

表4-10：身份验证与密钥管理组合

OUI	组合类型	身份验证	密钥管理
00-0F-AC	1	802.1X 或 PMK 缓存	密钥衍生自预共享密钥（pre-shared key），如第七章所述
00-0F-AC	2	预共享密钥	密钥衍生自预共享密钥，如第七章所述
Vendor OUI	Any	厂商自定义	厂商自定义

RSN Capabilities（RSN 性能）

此字段的长度为2个字节，由4个标记（flag）构成，用来描述发送端的能力。其后的位保留未用，必须设定为0。

Pre-authentication（预先身份验证）

接入点可以设定此位，代表它可以和网络中其他接入点进行预先身份验证，以便安全地移转连接事宜；否则，此位会被设定为0。预先身份验证将于第八章探讨。

No Pairwise（无成对密钥）

如果工作站除了较牢靠的单播密钥（unicast key）外也支持手动设定的WEP密钥作为广播数据之用，则此位就会被设定。虽然工作站支持，但除非绝对必要，否则不会使用这种配制设定。

Pairwise Replay Counter（成对重放计数器）与Group Replay Counter（组重放计数器）

在逐渐浮出台面的服务质量扩展功能中，每个优先级可以拥有好几个不同的重放计数器。这些位用来描述工作站所支持的重放计数器的数量。

PMK list (count + list)(PMK 列表（计数 + 列表）)

如果由接入点缓存成对主密钥（pairwise master key），就可以在接入点之间进行快速换手。工作站可以在进行关联时给接入点提供一串主钥，这样就可以免除费时的身份验证过程。PMK 缓存在第八章中有更为详细的讨论。

Extended Supported Rates 信息元素

Extended Supported Rates 信息元素的作用和图 4-33 的 Supported Rates 元素没有什么不同，不过它允许信息元素的内容超过 255 个字节。

Wi-Fi Protected Access (Wi-FI 保护访问，简称 WPA)

Wi-FI保护访问是从802.11i中抽出部分功能并稍做修改，目的是为了尽快将TKIP推出到市场上。它相当于图4-50的Robust Security Network信息元素，不过做了以下变动：

- 元素标识符（element ID）为 221，而非 48。
- WPA 特有的 00:50:F2:01 标记（tag）被插入在版本字段之前。
- 使用微软的 OUI（00:50:F2）而非 802.11 工作组的 OUI。
- 此信息元素只支持一种密码组（cipher suite）以及一种身份验证组合（authentication suite）。不过，有些 WAP 实现并未遵照此项限制。
- 使用 TKIP（而非 CCMP）作为默认的密码。
- WPA 不支持预先身份验证，因此 preauthentication capabilities 位必然设定为 0。

管理帧的类型

管理帧的主体所包含的固定字段与信息元素是用来运送信息的。管理帧有好几种，分别负责链路层的各种维护功能。

Beacon（信标）帧

Beacon帧是相当重要的网络维护任务，主要用来声明某个网络的存在。定期传送的信标可让移动式工作站得知该网络的存在，从而调整加入该网络所必需的参数。在基础结构型网络里，接入点必须负责传送 Beacon 帧。Beacon 帧所及范围即为基本服务区域。在基础结构型网络里，所有通信都必须通过接入点，因此工作站不能距离太远，否则便无法接收到信标。

图 4-51 依次显示了 Beacon 帧所使用的各个字段。信标不一定会用到所有字段。选择性的字段只有在用到时才会出现。只有在使用跳频（frequency hopping，简称 FH）或直接序列（direct-sequence，简称 DS）物理层技术时，才会用到 FH 与 DS 参数集。任何时候只能使用一种物理层，因此 FH 与 DS 参数集是彼此互斥的。

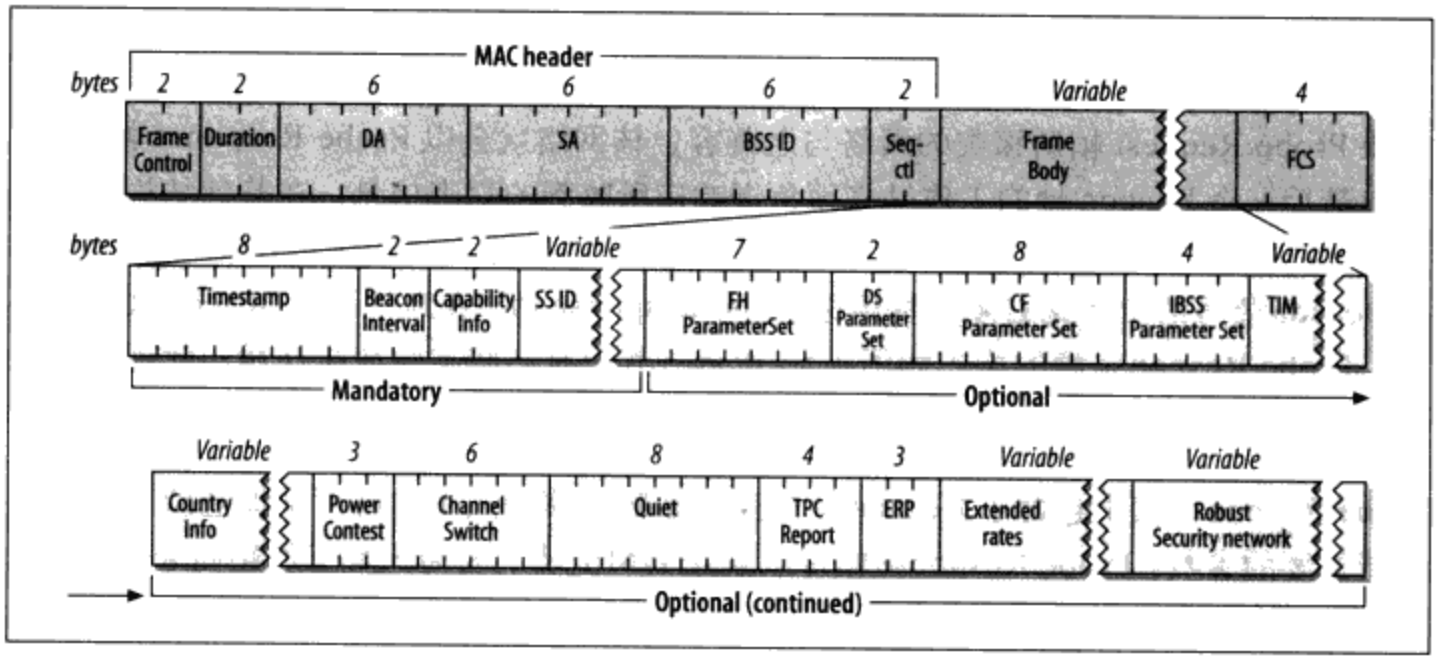


图 4-51：Beacon（信标）帧

CF 参数集只用于支持 PCF 的接入点所产生的帧中，至于是否支持 PCF 并非强制性的。TIM 只用于接入点所产生的 Beacon 帧中，因为只有接入点才会缓存帧。如果有特定国家的跳频扩展元素，则必然随附在 Country 信息元素之后。不过，跳频网络如今已不常见，为求简单，我省略了跳频扩展元素。同样地，若是出现 IBSS DFS 元素，则其必然位于 Quiet 与 TPC Report 元素之间。

Probe Request 帧

移动式工作站将会利用 Probe Request（探查请求）帧来扫描所在区域内目前有哪些 802.11 网络。Probe Request 帧的格式如图 4-52 所示，所有字段均为必要的的。

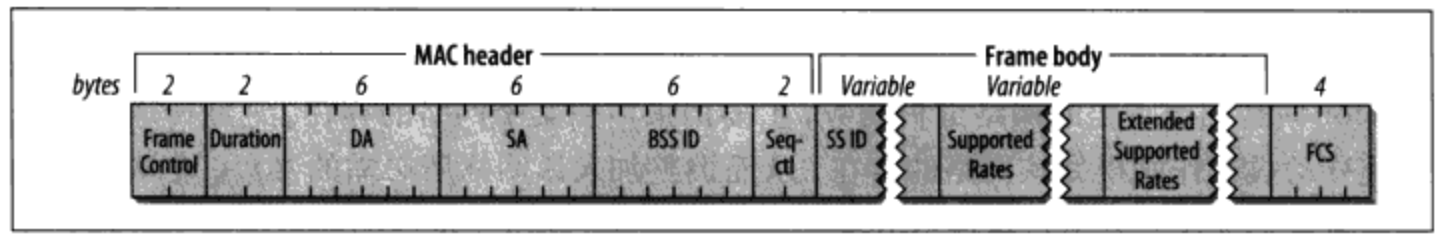


图4-52：Probe Request（探查请求）帧

Probe Request帧包含两个字段：SSID以及Supported Rates（移动式工作站所支持的速率）。收到Probe Request帧的工作站会据此判断对方能否加入网络。为了相处愉快，移动式工作站必须支持网络所要求的所有数据速率并以SSID表明所要加入的网络。SSID可被设定为特定网络的SSID或任何兼容网络的SSID。允许网卡加入任何网络的驱动程序将会在Probe Requests中使用broadcast SSID（广播形式的服务集标识符）。

Probe Response 帧

如果Probe Request帧所探查的网络与之兼容，该网络就会以Probe Response帧响应。送出最后一个Beacon帧的工作站必须负责响应所收到的探查信息。在基础结构型网络里，负责响应的工作站即为接入点。在IBSS当中，工作站会轮流传送Beacon信号。传送Beacon信号的工作站必须负责传送Probe Response帧，直到下一个Beacon被发送出来。Probe Response帧的格式如图4-53所示。其中有某些字段彼此互斥，此规则同样适用于Probe Response帧以及Beacon帧。

Probe Response帧中包含了Beacon帧的所有参数，移动式工作站可根据它调整加入网络所需要的参数。Probe Response帧可以剔除TIM元素，因为此时工作站尚未关联，因此不必知道哪些关联在接入点中有缓存帧。

IBSS的通知传输指示消息（ATIM）帧

IBSS中没有接入点，因此无法仰赖接入点来缓存帧。IBSS中的工作站如果为处于休眠状态的接收者缓存帧，就会在传递期间送出一个ATIM（announcement traffic indication message）帧来通知对方有信息待传，如图4-54所示。

Disassociation 帧与 Deauthentication 帧

Disassociation（取消关联）帧用来终结一段关联关系，而Deauthentication（解除身份验证）帧则用来终结一段认证关系。两者均包含一个固定字段，即Reason Code（原因代码），如图4-55所示。当然，Frame Control字段彼此不同，因为不同类型的管理帧拥有不同的子类型。802.11改版并不需要改变此格式，但几次修订时均加入了新的原因代码。

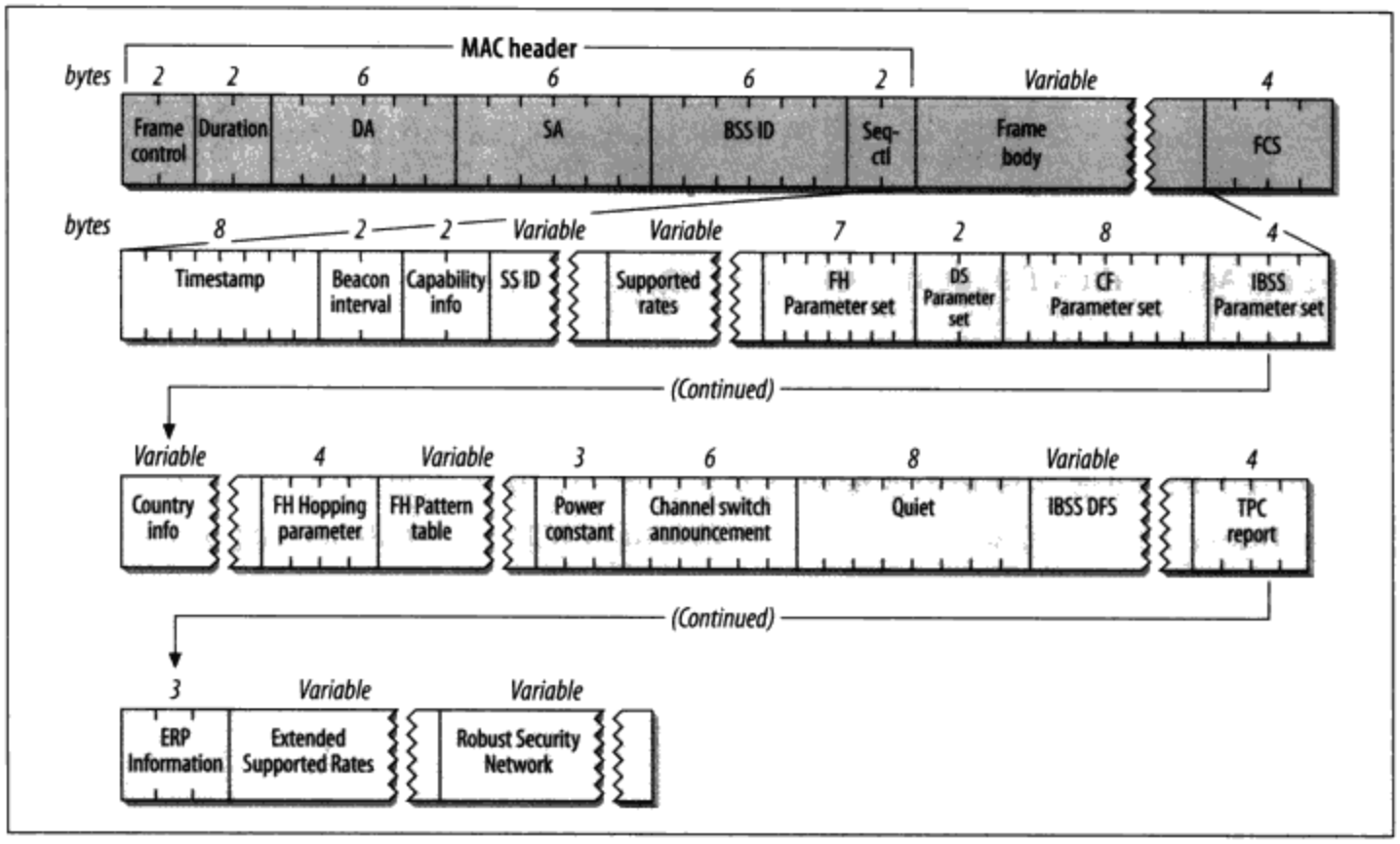


图 4-53：Prob Response（探查响应）帧

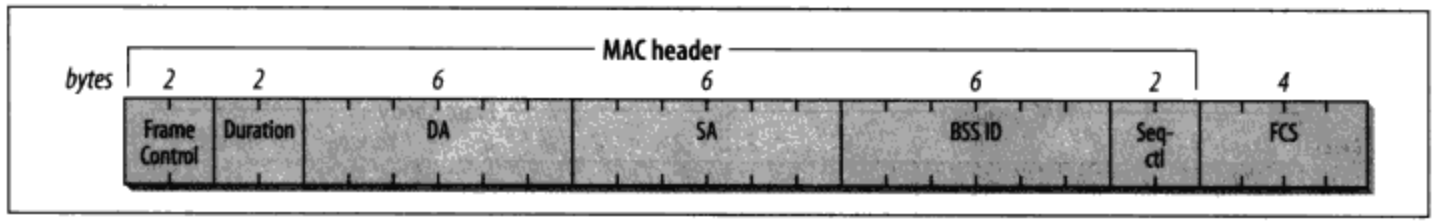


图 4-54：ATIM 帧

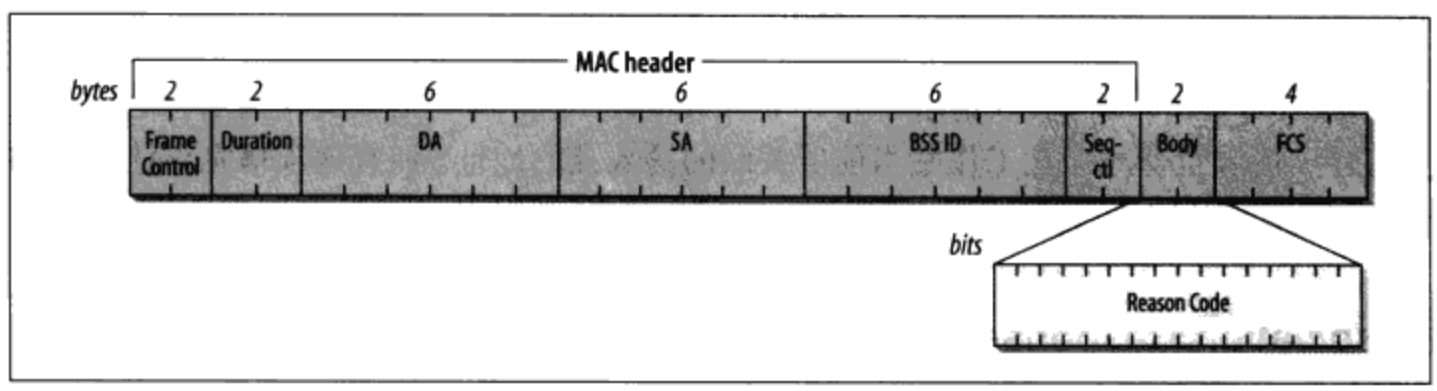


图 4-55：Disassociation（取消关联）帧与 Deauthentication（解除身份验证）帧

Association Request 帧

一旦移动式工作站找到兼容网络并且通过身份验证，便会发送 Association Request（关联请求）帧以试图加入网络。Association Request 帧的格式如图 4-56 所示。

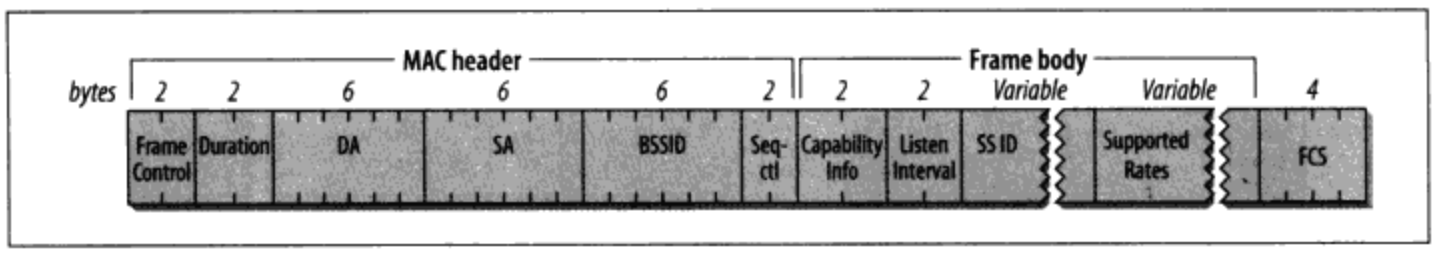


图 4-56：Association Request（关联请求）帧

Capability Information（性能信息）字段用来指出移动式工作站所要加入的网络类型。在接受关联请求之前，接入点会验证 Capability Information、SSID 以及（Extended）Supported Rated 等字段是否匹配网络参数。此外，接入点也会记录工作站所使用的 Listen Interval（聆听间隔，即移动式工作站每隔多久聆听一次 Beacon 帧以监视 TIM 信息）。支持频谱管理的工作站有 power（功率）与 channel（信道）性能信息元素，支持安全访问的工作站则有 RSN 信息元素。

Reassociation Request 帧

位于相同扩展服务区域，但在不同基本服务区域之间游走的移动式工作站若要再次使用分布式系统，必须与网络重新关联。如果工作站暂时离开接入点所涵盖的范围，之后要重新加入的时候也必须重新关联，如图 4-57 所示。

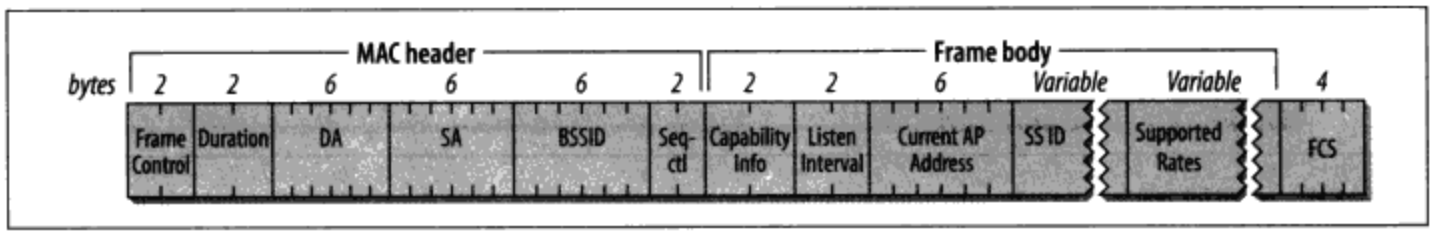


图 4-57：Reassociation Request（重新关联请求）帧

Association Request（关联请求）与 Reassociation Request（重新关联请求）之间的差别在于，后者包含移动式工作站当前所关联的接入点的地址。拥有这项信息可让新旧接入点彼此联系以及转移接入点数据。转移项目包括先前连接的基站所缓存的帧。

Association Response 帧与 Reassociation Response 帧

当移动式工作站试图连接接入点时，接入点会回复一个 Association Response（关联响应）或 Reassociation Response（重新关联响应）帧，如图 4-58 所示。两者之间的差别是 Frame Control 字段所记载的 subtype 字段。所有字段均属必要。在响应的过程中，接入点会指定一个 Association ID（关联标识符），至于指定的方式则因实现而异。

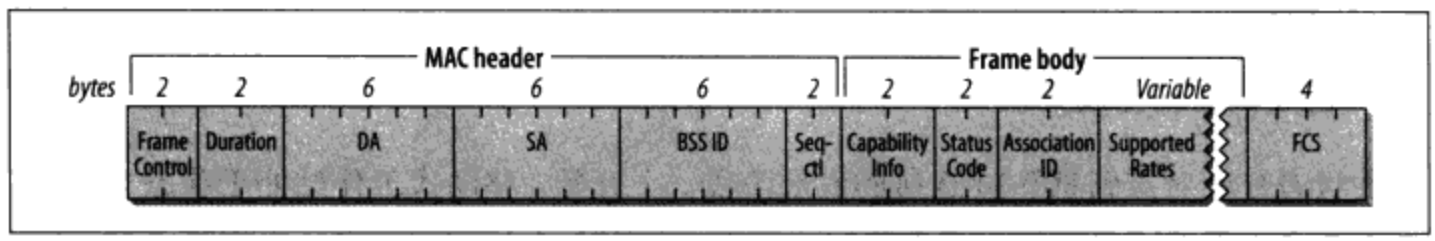


图 4-58：(Re) Association Response（(重新）关联响应）帧

Authentication 帧

在802.11网络发展初期，工作站使用共享密钥以及如图4-59所示的Authentication帧进行身份验证。到了802.11i，共享密钥身份验证虽然仍保留在标准中，但却无法与新的安全机制兼容。如果工作站使用共享密钥进行身份验证，将不允许使用较为牢靠的安全性协议，如第八章所述。

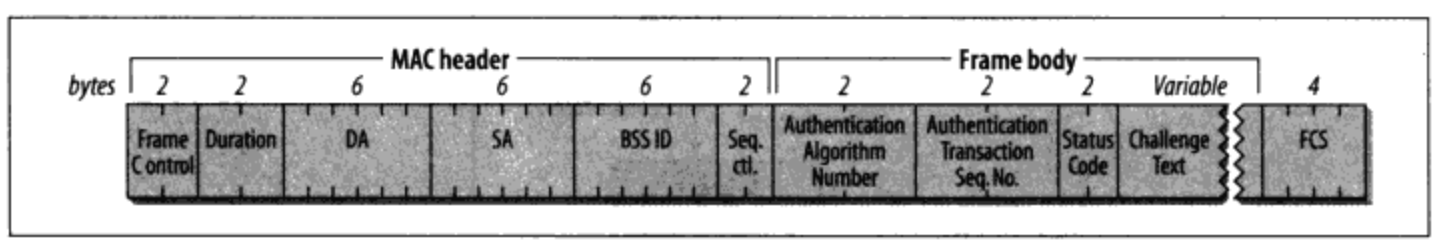


图 4-59：Authentication（身份验证）帧

不同的身份验证算法可以同时存在。Authentication Algorithm Number（身份验证算法编号）字段用于选择算法。整个认证过程可能包含好几个步骤（与所使用的算法有关），因此认证的过程中每个帧都有其序号。Status Code 与 Challenge Text 的用法因算法而异，相关细节将于第八章讨论。

Action 帧

802.11h 加入了对 Action 帧的支持，用来触发测量动作。这些帧将于第八章的“频谱管理”一节详加描述。

帧传送、关联与身份验证状态

所能传送的帧类型依关联状态与身份验证状态的不同而有所不同。工作站可能已经过认证或未经认证，也可能已经关联或尚未关联。这两个变量的组合有三种可能状态，结果构成了 802.11 的网络发展层次：

1. 初始状态：未经认证且尚未关联

2. 已经认证但尚未关联
3. 已经认证且已经关联

每种状态分别对应到802.11连接的发展阶段。一开始，移动式工作站处于状态1，只有进入状态3才可以通过分布式系统传送数据。(IBSS不包含接入点，也无需进行关联，因此只会停留在状态2。) 802.11帧传送的整体状态图如图4-60所示。

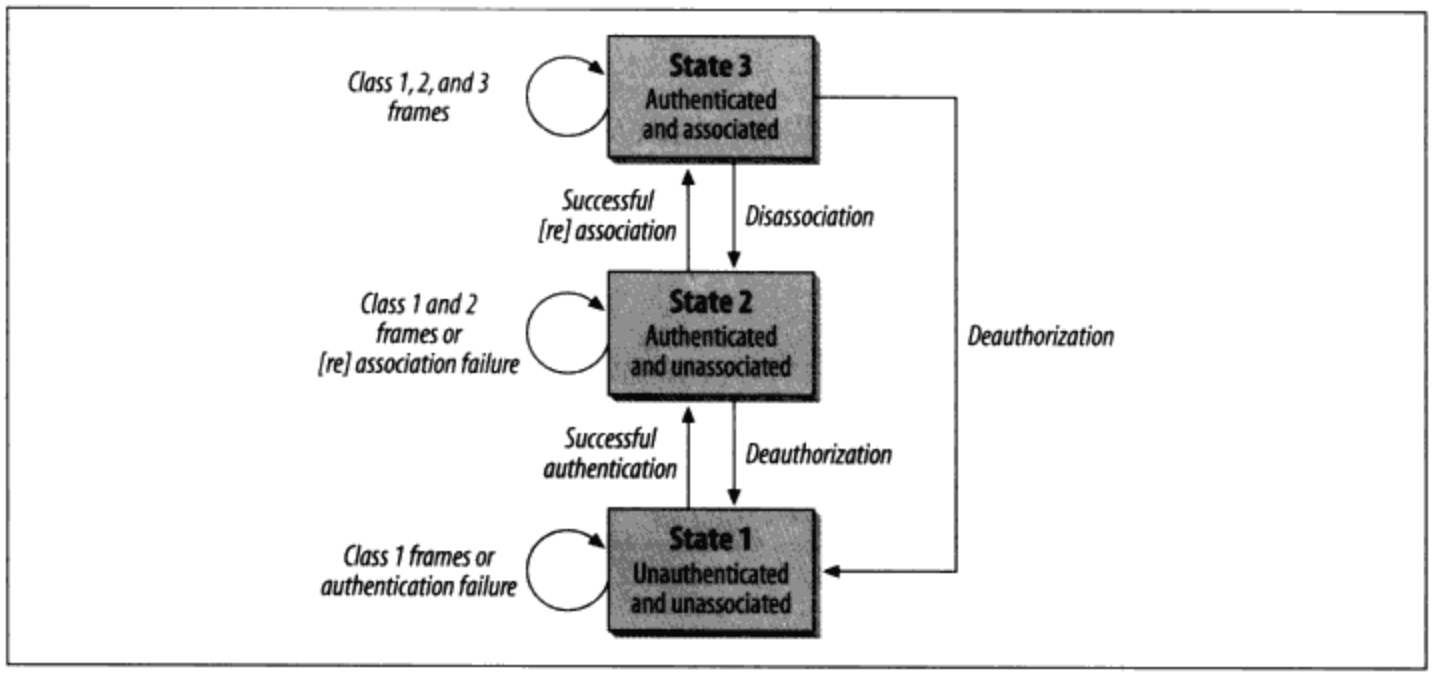


图4-60：802.11整体状态图

帧等级

帧可以被划分为3种等级。在状态1可以传递第1级帧；在状态2可以传送第1级与第2级帧；在状态3则可以传递第1、2与3级帧。

第1级帧

第1级帧可以在任何状态中传递，它让802.11的工作站能够进行基本操作。在IBSS中，控制帧主要用来依循CSMA/CA规则以及传送帧。工作站也会使用第1级帧来寻找基础结构型网络并与之进行身份验证。表4-11列出了属于第1级的各种帧。

表4-11：第1级帧

控制帧	管理帧	数据帧
Request to Send(RTS)	Probe Request	ToDS与FromDS位都设为0的任何帧
Clear to Send(CTS)	Probe Response	
Acknowledgment(ACK)	Beacon	

表4-11：第1级帧（续）

控制帧	管理帧	数据帧
CF-End	Authentication	
CF-End+CF-ACK	Deauthentication	
	通知传输指示消息（ATIM）	

第2级帧

工作站只有在经过身份验证之后才能够传送第2级帧，而且第2级帧只能使用于状态2与状态3。第2级帧主要用来管理关联。关联或重新关联成功后，工作站就会进入状态3；如果关联失败，则工作站依然处于状态2。当工作站收到未经认证的工作站所传来的第2级帧时，就会响应一个Deauthentication（解除身份验证）帧，将对方推回状态1（注4）。表4-12列出了所有的第2级帧。

表4-12：第2级帧

控制帧	管理帧	数据帧
无	Association Request/Response	无
	Reassociation Request/Response	
	Disassociation	

第3级帧

第3级帧的使用时机是在工作站认证成功并与接入点关联之后。一旦工作站进入状态3，就可以使用分布式系统服务，也可以和接入点范围以外的对象进行通信。在状态3，工作站还可以利用PS-Poll帧享受接入点所提供的省电服务。表4-13列出了不同类型的第3级帧。

表4-13：第3级帧

控制帧	管理帧	数据帧
PS-Poll	Deauthentication	任何帧，包含ToDS或FromDS位都设为1的所有帧

注4：只有在帧未经过滤时才会有此拒绝的动作。帧过滤可以避免来自不同BSS的帧引发拒绝的动作。

如果收到的帧来自一个已经验证但尚未关联的工作站，接入点就会响应一个Disassociation（取消关联）帧，迫使工作站回到状态2。如果发出帧的工作站尚未经过验证，则接入点会响应一个Deauthentication（解除身份验证）帧，迫使工作站回到状态1。

第五章

有线等效加密

不曾为之震撼的人，
哪里懂得量子理论。
——Niels Bohr

在无线网络领域中，“广播”（broadcast）一词具有崭新的含义。无线网络使用开放性媒介，如果传输链路未采取适当的加密保护，使用时的风险就会大幅增加。既然是开放性的网络媒介，那么只要拥有适当的设备，任何人均可窥视未经保护的数据。以无线局域网而言，所谓“适当的设备”是指能够接收和解读802.11的接口，而这种设备并不算昂贵。如果需要更高档的设备，可以考虑使用具有高增益的外接天线。既然天线已经相当便宜，各位最好假设有意攻击的黑客早就人手一支了。

防止数据被拦劫属于加密协议的范畴。当帧经过空气时，必须加以保护才能免遭毒手。保护有好几种形式，不过最常被引用的两种非正式目的，就是维护网络数据的保密性以及确保数据未被改动。起初，有线等效加密（WEP）标准被视为无线安全的解决方案。不过在802.11问世的前4年，研究人员发现WEP并不安全。

倘若WEP真是如此差劲，为何还要为它浪费时间呢？因为有些时候，某些特殊设备只支持WEP。况且WEP的设计相当容易实现，虽然它不如后续出现的加密协议复杂，但也不要求有多么强大的计算能力。一些老的设备，特别是手持应用方面的设备，也许缺乏足够的处理能力而无法运行得更为顺畅，因此WEP已经算是最佳选择。此外，较新的技术，如TKIP，仍旧会用到WEP的帧处理操作，因此了解WEP也就十分重要了。

WEP 的密码学背景

探讨 WEP 的设计之前，有必要先了解一些基本的密码学概念。我并非密码学专家，本书也不适合深究密码学，对此本章只能轻描淡写（注 1）。

WEP 用以保护数据的 RC4 密码（cipher）属于对称性（密钥）流密码（stream cipher）。RC4 具备所有流密码的共同特性。一般而言，流密码会用到称为密钥流（keystream）的位流。密钥流随后会与信息结合，产生密文（ciphertext）。为了还原原始信息，接收端会以相同的密钥流处理密文。RC4 会利用异或（exclusive OR，简称 XOR）运算结合密钥流与密文。图 5-1 说明了整个过程。

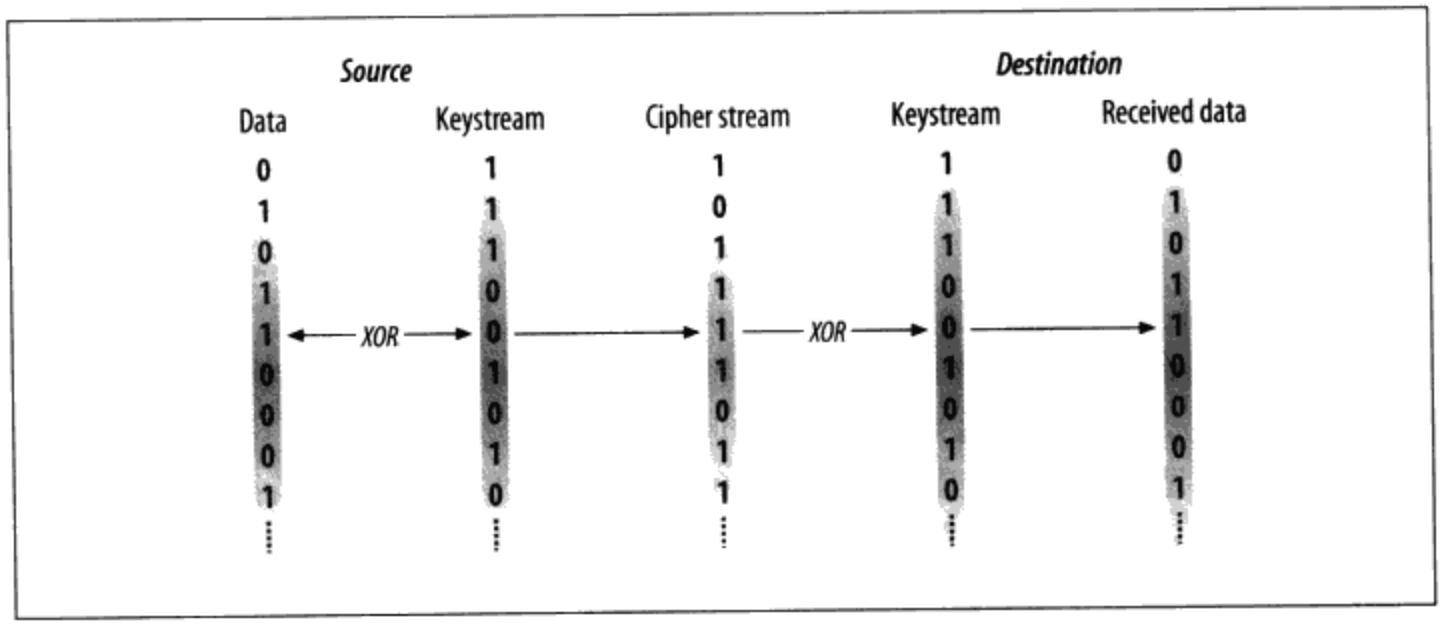


图 5-1：流密码的一般运作流程

流密码的运作方式通常是会先选用一把较短的密钥，然后将之展开为与信息等长的伪随机数密钥流。此过程如图 5-2 所示。伪随机数生成器（pseudorandom number generator，简称 PRNG）是一组用来将密钥展开为密钥流（keystream）的规则。为了还原数据，双方必须拥有相同的秘钥（secret key），并且使用相同的算法将密钥展开为伪随机数序列（pseudorandom sequence）。

既然流密码的安全性完全取决于密钥流的随机程度，因此密钥如何展开为密钥流（key-to-keystream expansion）在设计上就极为重要。当 802.11 工作组决定采用它时，RC4 看似十分安全。不过当 RC4 被选为 WEP 的加密引擎后，其所带动的一连串相关研究发现 RC4 密码锁本身隐含了极大的瑕疵，我们将于稍后提及。

注 1：对相关加密算法细节感兴趣的读者，可以参考 Bruce Schneier 所著的《Applied Cryptography》（Wiley,1996）。

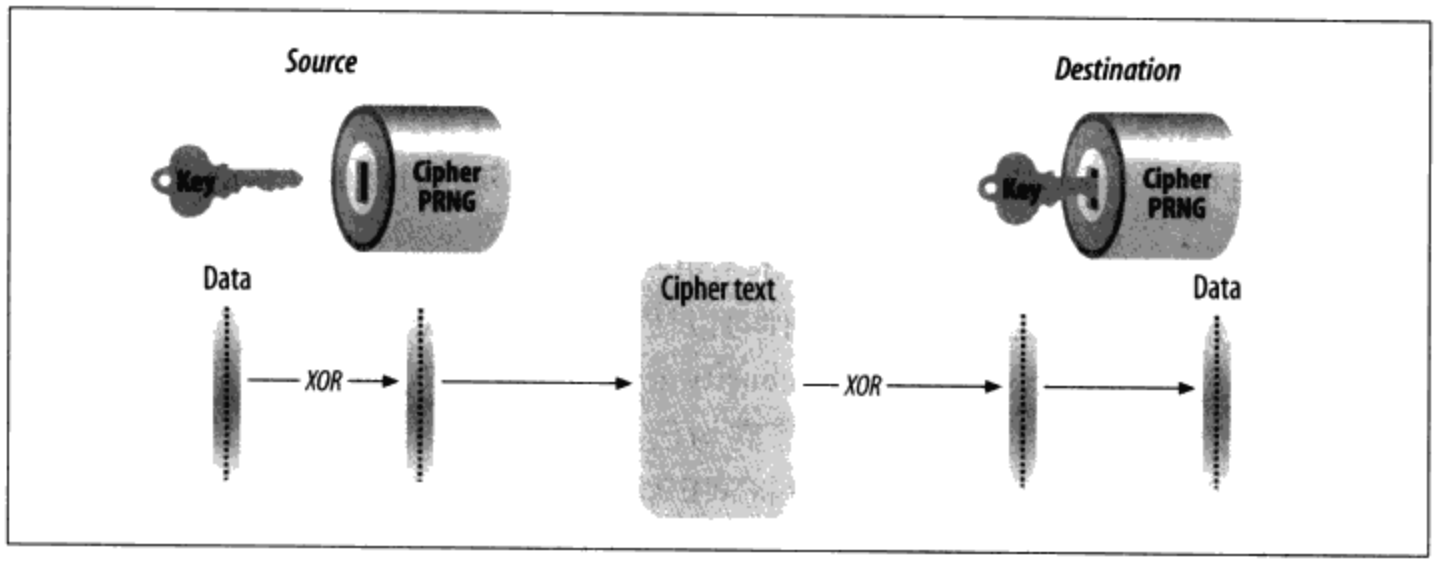


图 5-2：密钥流密码的运作流程

流密码的安全性

一个完全随机的密钥流通常称为一次性密码本（*one-time pad*），它是经过数学证明的目前已知的唯一可以防范任何攻击的加密方式。一次性密码本很少被使用，因为除了密钥流必须完全随机并与受保护的数据等长，而且还不得重复使用。

可能遭受攻击的对象不只是底层所使用的密码。加密系统中的任何弱点都可能让攻击者乘虚而入。在以VENONA（薇诺娜）为代号的著名任务中，西方国家之所以能够破解前苏联的信息，是因为对方重复使用一次性密码本进行加密（注2）。想要重复使用一次性密码本的冲动不难理解。就算只是保护一丁点数据，也要用到大量的加密素材，何况这些密码本还得安全地送达接收者手上。光是这一点，实际上就是莫大的挑战。每个数据位都必须用到相应的一次性密码本位。54 Mbps的网络可以传送大约25 Mbps的用户数据。就算网络操作只用掉10%的带宽，以一天8小时的数据传输而言，总计也要传送9 gigabytes左右的数据。要将好几个gigabytes的密钥素材传给每个接入点根本就不切实际。

流密码锁是安全与实际考虑下的折中产物。一次性密码本所具备的完全随机性（以及绝对安全性）虽然吸引人，但考虑到实际的困难以及产生与传递解密文件的成本，若非要求绝对安全的信息，实际上它并不值得采用。流密码使用密钥流的随机程度虽然较低，但已足以应付绝大多数的应用。

注2：　各位可以在美国国家安全局（United Stats National Security Agency）的网站上（*http://www.nsa.gov/docs/venona*）取得该计划的一些公开数据。

密码政治学

密码学的讨论如果未能交代围绕其应用的种种法律与管理上的考虑，就不能称得上完整。WEP的应用有三项主要议题，虽然这些议题的效应将会随着时间的推移而递减。

WEP需要通过RC4密码来加密帧。编写本书第一版时，WEP只是一种可有可无的选项，并未内置到所有产品中。经过授权的软件可以使用RC4程序代码，不过开放源码项目对此则有所顾虑，因为可能会侵犯RSA Security公司的知识产权。本书第一版问世后这项顾虑才逐渐消失。所有主要的芯片组厂商均已获得RC4加密的授权并且将它集成进802.11芯片组。设备驱动程序只需负责将WEP密钥交付硬件处理即可。让网卡硬件处理加密事宜，意味着软件无需顾虑是否会侵犯到RSA的知识产权。

起初，WEP在设计上之所以采用短密钥，是为了符合美国对加密产品的出口管制。一开始，标准要求采用40位的短密钥，不过现在几乎所有市面上的产品都至少支持104位的密钥。短期而言，长密钥似乎是标准的重要扩展功能，不过其所能够提供的额外安全性已经被证明是纯属虚幻。

最后，有些政府严格管制任何加密系统的使用，包括WEP在内。除了美国的出口管制，有些国家还有进口管制，限制加密设备的进口。其他政府也有权提出一些额外的加密限制。中国政府自行开发了一种替代方案，称为无线局域网鉴别和保密基础结构（WLAN Authentication and Privacy Infrastructure，简称WAPI）的安全系统，并将之列为中国无线局域网设备的可选项。

WEP的加密操作

通信安全有三个主要目的。当数据经过网络时，数据安全协议必须能够协助网管人员实现这些目的。机密性（confidentiality）是为了防止数据不受未授权的第三者拦截；完整性（integrity）则确保数据没有被修改；而真实性（authentication）是所有安全策略的基础，因为数据的可信度部分取决于数据源的可靠性。用户必须确认数据来自期望的数据源。系统必须利用认证来适当保护数据。授权（authorization）与访问控制（access control）两者均奠基于真实性之上。在允许访问任何数据之前，系统必须确认用户的身份（真实性）以及是否允许该用户访问数据（授权）。

为了实现上述目的，WEP本身提供了一些机制，虽然这些机制在遭受严重攻击时可能失效。帧主体加密机制（frame body encryption）主要用来提供机密性（confidentiality）。完整性校验序列（integrity check sequence）用来在传送过程中保护数据，让接收者能够验证所收到的数据在传送过程中未被更改过。实际上，WEP在这些领域中还有欠缺，它需要用到一些额外的补强措施，这些将留待下两章探讨。

WEP 的数据处理

机密性与完整性的操作同时进行，如图 5-3 所示。加密之前，帧会通过完整性校验算法，产生一个称为完整性校验值（integrity check value，简称 ICV）的散列值（hash）。ICV 可确保帧在传送过程中未被改变。帧本身与 ICV 两者均经过加密，因此 ICV 不会被攻击者任意宰割。

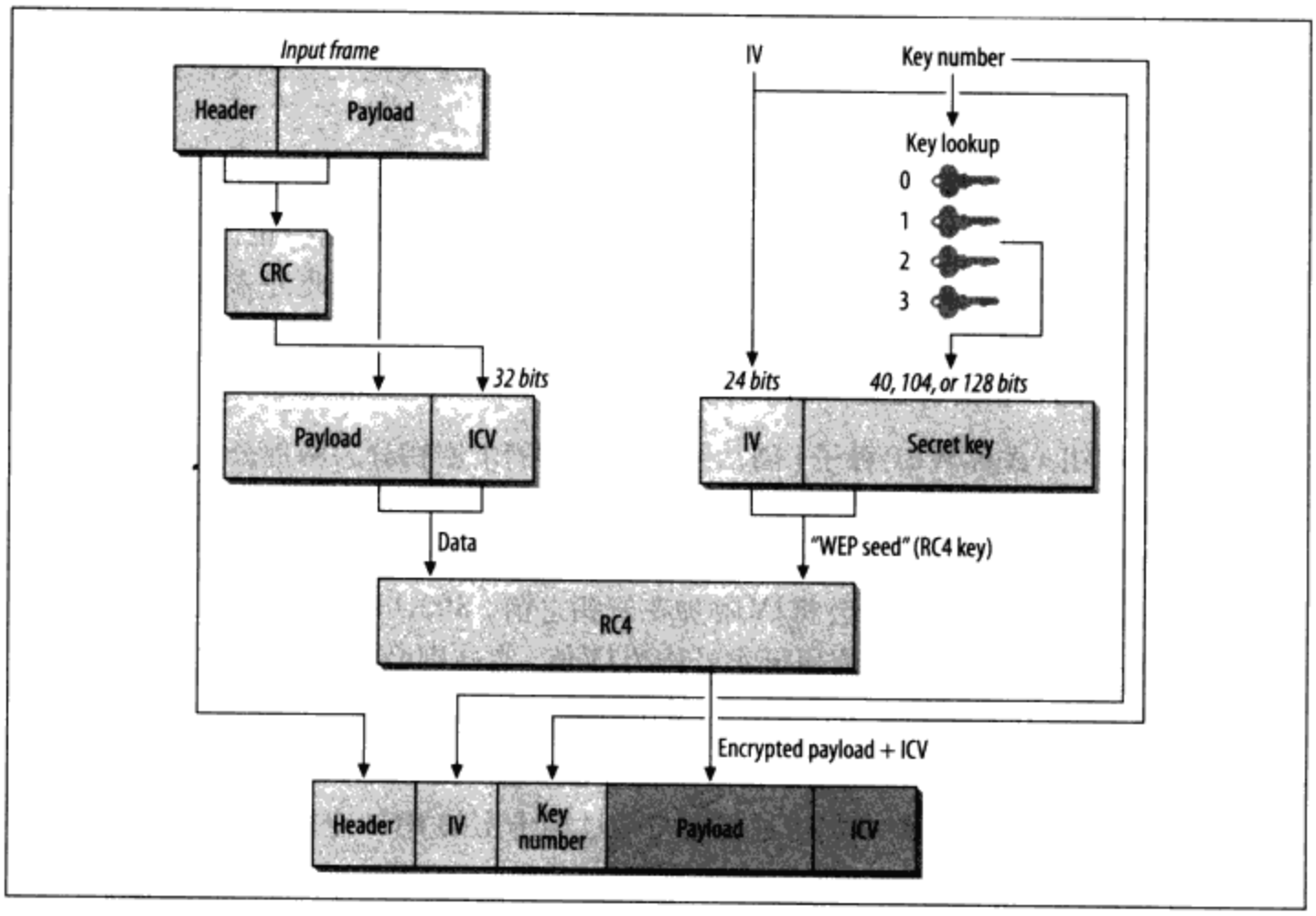


图 5-3：WEP 的动作方式

WEP 需要以下三个输入项：

- 需要保护的有效载荷（payload），这些数据来自上层协议堆栈（protocol stack）。
- 秘钥（secret key），用来加密帧。依实现方式的不同，可以用密钥位字符串（string of key bits）或者密钥编号（key number）来指定密钥。WEP 允许同时存储 4 种密钥。
- 初始向量（initialization vector，简称 IV），和秘钥（secret key）一起在传送帧时使用。

经过处理后，WEP 会产生一个单一输出项：

- 加密过的帧，可以通过不安全的网络加以传送，其中包含足够的信息使对方能够解密。

WEP的数据传送

驱动程序以及接口硬件负责处理数据，然后送出加密过的封包，顺序如下：

1. 802.11帧被放在队列中等待传送。帧由标头和有效载荷（payload）组成。WEP只保护802.11 MAC的有效载荷，至于802.11帧头以及其他底层协议标头则丝毫没有改变。
2. 根据802.11 MAC帧的有效载荷计算出完整性校验值。由于此校验值是针对帧的有效载荷来计算的，因此计算所涵盖的范围始于SNAP标头的第一位，直到帧主体的最后一个数据位。此时，802.11帧校验值尚未计算出来，因此并未包含在ICV的计算当中。WEP所使用的ICV属于循环冗余校验（Cyclic Redundancy Check，简称CRC）码，稍后有更进一步的说明。
3. 帧加密密钥（或称WEP种子）随后组装完成。WEP密钥分为两部分：秘钥（secret key）以及初始向量（IV）。如果使用同一个密钥，流密码会产生相同密钥流，因此另以初始向量为每个帧产生不同的流密码。为了避免出现使用相同密钥流进行加密的情况，传送帧的工作站会将IV附加在密钥之前。802.11并未限制选取IV时非得使用何种算法；有些产品使用流水号作为IV值，有些则会使用伪随机散列算法。如何选择IV具有重要的安全含义，选得不好就可能危及密钥。
4. 帧加密密钥被当成RC4密钥，用以加密来自步骤1的802.11 MAC有效载荷以及来自步骤2的ICV。整个加密过程通常通过网卡上的RC4专用电路来协助完成。
5. 将有效载荷加密之后，工作站就会开始组装待传的帧。802.11标头本身维持不变，802.11 MAC标头与加密过的有效载荷之间则插入了WEP标头。除了IV，WEP标头中还包含密钥编号。WEP最多允许定义4个密钥，因此发送端必须分辨目前使用的是哪一个密钥。一旦附加上最后的标头，就可以针对整个MAC帧，即从标头算起，直到（加密过的）ICV结束，计算出802.11帧校验（FCS）码。

解密过程刚好相反。与任何无线网络的传送过程相同，首先是验证FCS，确保所接收到的帧未在传送过程中损毁。解读帧受保护的部分时，接收端会使用密钥，加上IV，然后产生密钥流。得到解密过的数据后，接下来则是验证ICV。如果ICV验证无误，就根据SNAP标头所记载的内容，将封包数据交给适当的上层协议。

WEP密钥的长度

理论上，WEP可以搭配任意长度的密钥，因为RC4并未要求非得使用特定长度的密钥。

不过，大多数产品均支持一种或两种长度的密钥。唯一出现在标准中的密钥长度是64位的WEP种子（seed），其中40位是两个工作站进行传送时所共享的密码。不同厂商会以各种不同的名称来称呼标准的WEP模式：standard WEP、802.11-compliant WEP、40-bit WEP、40+24-bit WEP，甚至是64-bit WEP。我个人认为最后一种说法纯粹是误导，这是以共享密钥（shared key）而非以共享秘钥（shared secret）的长度来蒙骗消费者。不过，这似乎已经成为业界的某种标准了。

另外一种比较常见的做法就是采用较长的密钥，通常是使用128-bit的WEP种子，其中有104位密而不宣。有些文档称之为WEP-104，虽然宣传时通常称之为128-bit WEP。虽然比较少见，但使用长度为128位的密钥并非不曾听闻，结果WEP种子的长度就变成了152位。容易令人混淆的是，这种少见的做法通常也称为128-bit WEP，因为密钥长度的不同，使得它与WEP-104彼此不兼容。有家厂商甚至提供256位的密钥，虽然这种做法能否提升安全性着实令人怀疑。

在设计完善的密码系统中，使用较长的密钥可以获得较高的安全性。每增加一位，就会让可能产生的密钥数量加倍。因此，理论上要破解系统的时间也随之加倍。然而，WEP并非设计完善的密码系统，况且在密钥中多加几位并不能带来多少好处。已经被揭露的最佳攻击手法可以在短短几秒钟内破解WEP取得密钥，不论密钥的长度是多少。

WEP密钥的类型

WEP可以使用两种不同类型的密钥。映射密钥（mapped key）用来保护流动于特定来源与接收端之间的数据。映射密钥有时也称为单播密钥（unicast key）或工作站密钥（station key），因为它们适合用来保护单播数据。在基础结构型（infrastructure）网络里，数据是在工作站与接入点之间流动的。802.11帧中同时包含了接收端与目的地地址。单播数据可以有许多不同的目的地地址，不过流动于基础结构型网络里的单播帧均会以接入点的MAC地址作为接收端地址。所有来自或传至工作站的单播帧均可以使用单一映射密钥进行加密。如果两个802.11工作站之间并不存在映射关系，就必须改用默认密钥（default key），有时也称为广播密钥（broadcast key）。默认密钥天生就适合用于广播与组播帧，因为组地址代表多个工作站，因此无法支持映射密钥关系。

手动（静态）与自动（动态）的WEP

802.11并未规范WEP必须使用特定的密钥分配机制。对WEP而言，反正密钥就是会神奇出现。早期的WEP实现必须手动分配密钥。网管人员必须负责将一个默认密钥分配到网络中的所有工作站，这个过程通常是手动完成的。密钥的更新也是通过手动方式。实际上，大部分的网络都会被部署成长时间使用同一个密钥，因为更新密钥对网管而言其实是莫大的负担。因此，不具密钥分配机制的WEP通常称为手动WEP或静态WEP。

手动密钥是个很糟的概念。要管理整个网络中这么多接入点的密钥分配是相当困难的事。密钥是用来保护数据的，如果组织中有知道密钥的人离职，就应该予以更换。理论上，设计完善的加密系统在使用密钥时，会尽可能将它们局限在某些特定的目的上以防止密钥被破解。静态的 WEP 在每个工作站所传送的各个帧中均使用同一个密钥，一旦密钥被破解，后果将不堪设想。

如果没有明确的理由，就不该采用静态WEP。除了聊胜于无，静态WEP其实乏善可陈。它可以有效地制止散弹式的攻击（casual attack），但无法防御集中火力型的侵略(determined assault)。许多低功率设备，例如 802.11 电话、手持条形码扫描器甚至是PDA，无法提供优于WEP的解决方案。除非这些设备被完全被汰，否则在这种情况下，静态 WEP 仍旧是保护链路层安全的唯一选择。

比较好的解决方案是动态WEP。在动态WEP中，每个工作站会使用两个密钥，而不是所有工作站共享一个密钥。其中一个密钥是经过映射的密钥，为工作站与接入点所共享，用来保护单播帧。另外一个密钥是默认密钥，为同一服务集中所有工作站所共享，用来保护广播与组播帧。工作站所使用的加密密钥是通过密钥加密密钥(key encryption key)来分配，至于用来衍生密钥加密密钥的认证协议，则留待下一章探讨。

动态WEP具有许多静态WEP所不能及的显著优势。从最抽象的层面而言，每个密钥都有范围（scope）上的限制。由于减小密钥的使用次数，使其不再使用得如此频繁，相对就可以减小密钥被破解的机会。有心人士当然可以集中火力攻击这些密钥，不过可供搜集的个别密钥数据一旦变少，攻击就变得更加费时。同等重要的是，动态密钥正如其名，本身会随着时间而改变。接入点可以每隔一段时间就更换密钥，如此一来，攻击者就不得不放弃已经搜集到的数据，只能另起炉灶，重新对其他密钥发动攻击。只要更新密钥的时间间隔足够短，就可以大幅减少密钥遭受到的攻击。动态 WEP 的解决方案将于本章稍后探讨。

WEP 密钥的编号与存储

WEP 密钥有其相对应的编号，802.11 工作站最多可以指定 4 个密钥。起初，WEP 密钥编号是为了协助更换网络密钥。指定好新的密钥后，工作站可以逐步切换，而不必让所有工作站同时切换。举例而言，假设组织原本使用编号为 0 的密钥，如要更换，可以指定使用编号为 1 的密钥。如此一来，工作站至少有一段缓冲时间来逐渐改用编号为 1 的密钥，而不是在同一时间内全面更新。等到过渡期结束，对编号为0的密钥就予以停用。

在动态 WEP 解决方案里，密钥编号扮演着不太一样的角色。每个工作站均会从接入点处接收到两个密钥：一个映射密钥，通常存储为 0 号密钥；一个默认密钥，通常存储为

1 号密钥。工作站以 0 号密钥保护单播数据，以 1 号密钥保护广播数据。当帧被放在队列中待传时，驱动程序将会以 0 号密钥加密单播帧，以 1 号密钥加密广播帧。

802.11 刚问世时，有些网卡并不支持 WEP 或只能借助主机的 CPU 进行 RC4 加密运算，因此性能大打折扣。以硬件实现 RC4 其实相当容易，1999 年以后，几乎所有市面上的无线局域网接口均已内置了 RC4 硬件加密的功能，以免软件加密拖垮整体性能（包含大多数较晚推出的 802.11b 网卡）。有些较旧的网卡还通过固件限制只能使用长度为 40 位而非 104 位的密钥，如 Orinoco 所推出的银卡（Silver Card）与金卡（Gold Card）。后续发布的固件已经不再限制可使用的密钥长度。

为了让帧的加密更有效率，许多 802.11 芯片组内含一种称为密钥缓存（*key cache*）的数据结构。密钥缓取由目的地地址、密钥识别编号、密钥本身各个位的对应关系组成。大多数工作站的网卡的芯片组都有 4 个密钥槽。静态 WEP 使用其中一个密钥槽，动态 WEP 使用两个。当帧放在队列中待传时，首先会在密钥缓存中查询目的地地址，所查到的密钥就用来加密帧。动态密钥在功能上和静态 WEP 一样，不过密钥缓存的内容可能会被密钥管理软件所取代。

适用于网卡与适用于接入点的芯片组的不同之处在于后者有较大的密钥缓存，通常可以容纳 256 个或更多的密钥项目。就算每个工作站需要用到两个密钥（一个映射密钥与一个默认密钥），这样的数据结构就可以处理 100 个以上的工作站的密钥。既然大多数的无线链路技术所消耗的带宽有限，这样的数据结构应该就绰绰有余。不过，有些早期支持动态生成密钥的接入点并无法维护过大的密钥数据结构，必须让好几个工作站共享密钥。为了节约成本，有些厂商甚至在接入点里使用网卡的芯片组。如此一来，这些接入点就只有 4 个密钥槽，所有与该接入点连接的工作站就得共享同一个单播密钥。

WEP 的帧格式

一旦使用 WEP 进行加密，帧主体就会增加 8 个字节。其中 4 个字节作为帧主体的 IV 标头，另外 4 个字节则作为 ICV 标尾。如图 5-4 所示。

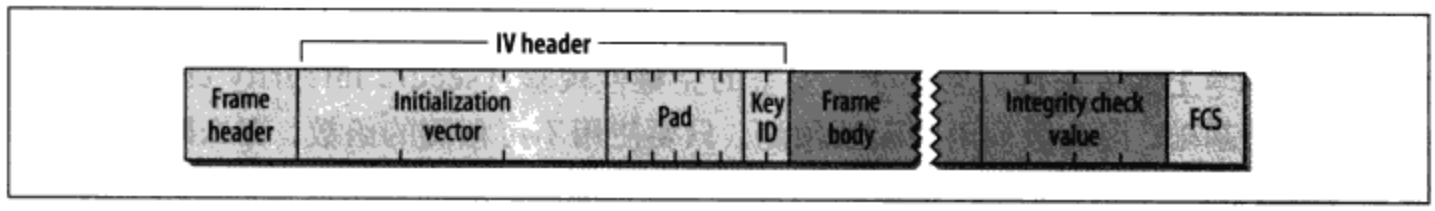


图 5-4：WEP 帧的扩展

IV 标头使用 3 个字节来容纳长度为 24 位的 IV，而第四个字节则包含填充位（padding bit）以及密钥标识符（key ID）。使用默认密钥时，KEY ID 子字段可用来识别加密帧

的默认密钥。如果选择使用密钥映射关系（key mapping relationship），则Key ID子字段的值为0。最后一个字节中有6个填充位必须为0。数据帧的32位循环冗余校验（CRC）码提供了完整性检查，附加于帧主体之后，同时被RC4保护。帧校验序列（frame check sequence，简称FCS）则是用来保护加密过的数据。

关于WEP的种种问题

密码学者在WEP中发现了许多瑕疵。WEP的设计者规定采用RC4，而RC4向来被公认为是一种坚固的密码（strong cryptographic cipher）。然而，攻击者并非只能对加密算法采取正面攻击，整个密码系统中的任何弱点都可以是侧翼包抄的对象。摧毁WEP的方式来自各种不同角度。比较值得注意的一个案例是，某家厂商所生产的无线接入点无意间暴露了WEP密钥，攻击者可以通过SNMP加以取得。不过，大部分的新闻舆论均将矛头指向实现，即设计上的瑕疵，要改正此缺陷可就困难多了。

RC4在密码学上的物性

重复使用密钥流（keystream）是所有流密码（stream ciper）系统的主要弱点。以同样的RC4密钥流加密帧时，对两个加密过的封包（encrypted packet）做XOR运算，和对两个明文封包（plaintext packet）做XOR运算的结果是相同的。只要对帧主体（frame body）的结构分析两个相邻的流（stream），攻击者即可得知明文帧的内容。为了避免重复使用密钥流，WEP利用IV对不同的封包以不同的RC4密钥进行加密。不过，IV属于封包标头的一部分，而且本身并未加密，因此窃听者仍能够从相同的RC4密钥所加密的封包中找出线索。

实现问题的推波助澜，更进一步削弱了系统的安全性。802.11认识到，使用相同的IV为大量帧进行加密并不安全，必须加以避免。所以802.11标准允许每个帧各自使用不同的IV，但并未强制要求。

WEP包含了完整性检查，不过其所使用的算法为循环冗余校验（cyclic redundancy check，简称为CRC）。个别位如果被修改，大多数都可通过CRC检测得知，然而它并不具备密码学上的安全性。密码学上安全的完整性校验（secure integrity check）是以散列函数为基础，因为散列函数无法预测。只要使用不可预测的函数，那么即使攻击者仅改变帧中的一个位，完整性校验码也会以不可预测的方式而有所改变。如此一来，就算攻击者想利用相同的完整性校验码找出被更改的帧，其机会不仅微乎其微，而且也不可能实时完成。从密码学的角度来看，CRC码并不安全。CRC是相当直接的数学运算，而且要预测改变一个位将如何影响CRC的计算结果其实是十分容易的。（这个特性通常

会被压缩过的数据文件拿来修复文件！如果只有一些位受损，有时候就可以从CRC值发现并加以更正。）

WEP系统设计上的瑕疵

直到加州伯克利大学的因特网安全、应用、认证与加密（Internet Security, Applications, Authentication and Cryptography，简称ISAAC）小组针对WEP标准所做的初步分析报告出炉后（注3），WEP设计上的瑕疵才凸显出来。研究人员在WEP当中所发现的问题没有一个是和RC4的破解有关。以下是已知问题的总结，有些问题之前已经提过：

1. 手动管理密钥是问题的症结之一。撇开分配相同密码给所有使用成员的庞大工程不说，安全上的顾虑就足以让人恶梦连连。新的密钥必须在某个特定时刻分配给所有系统，而只要有任何使用WEP的成员离开公司，那么基于安全上的考虑，实际的做法必然倾向于重新分配密钥。广为人知的秘密通常不算是秘密。只要取得WEP密钥就能够进行被动式嗅探攻击（passive sniffing attack），而密钥通常不会经常更改。一旦取得WEP密钥，嗅探攻击就变得十分容易，特别是在802.11分析软件中加入解密功能之后。
2. 标准的静态WEP只提供长度为40位的密钥。长久以来安全专家一直质疑长度为40位的密钥的适合性，有些专家建议至少以长度为128位的密钥来保护重要数据（注4）。自从WEP的瑕疵被披露以来，业界标准所提供的密钥长度最多只达到104位。
3. 一旦重复使用密钥流（keystream），流密码（stream cipher）就容易被识破。WEP采用IV的方式让攻击者得以在密钥流的重复使用中找出蛛丝马迹。更糟的是，拙劣的实现如果没有采用随机IV，就会使问题更加严重。Berkeley小组发现，市面上居然有一张网卡可以将IV由0开始算起，而后每个帧的IV值逐步递增。此外，可供运用的IV值（IV空间）并不大（小于1700万），因此在忙碌的网络上必然会产生重复的情况。
4. 如果不常更换密钥，攻击者就可以采集伯克利小组所说的解密字典（decryption dictionarie），即积累以相同密钥流加密的大量帧。一旦采用相同IV的帧累积到一定程度，那么就算秘钥没被发现，也可以从未加密的帧中推断出更多的数据。不过系统与网络管理人员通常十分忙碌，偶尔更换一次秘钥根本就是常规的。

注3：各位可以在以下网址取得这份报告：*http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*。接下来的第3至第6个问题是由这份报告汇整而来。

注4：公平而论，WEP原本的设计就是将出口问题纳入考虑，目的是为了符合美国当时对加密系统的出口管制。使用较长的密钥必然会损及美制802.11产品的商业可行性。

5. WEP使用CRC进行完整性检查。虽然完整性校验值本身经过RC4密钥流加密，但是CRC并没有密码学上的安全性。完整性检查如果不够完善，就无法防范有心人士在神不知鬼不觉的情况下更改帧（注5）。
6. 接入点（access point）具有解读帧的特权。就概念而言，攻击者可以诱骗接入点重新发送经WEP加密的帧，针对此特殊功能发动攻势。接入点所收到的帧将会在解密后被重新传送到攻击者的工作站。如果攻击者使用WEP，那么接入点还会以攻击者的密钥加密帧，反而为其助攻。

针对WEP的密钥恢复攻击

2001年8月，Scott Fluhrer、Itsik Mantin以及Adi Shamir联合发表了一篇名为《Weaknesses in the Key Scheduling Algorithm of RC4》（RC4的密钥调度算法中的弱点）的论文。在该篇论文末尾，三位作者描述了理论上如何攻击WEP。攻击的重点在于RC4将密钥展开为密钥流的方式（此过程称为密钥调度算法）所露出的破绽。

Fluhrer-Mantin-Shamir攻击（或简称为FMS攻击）假设：已加密的有效载荷（encrypted payload）的第一个字节是可还原的。对一些加密系统而言，这是相当大胆的假设。不过，由于802.11采用WEP来保护帧，而802.11帧本身却是以SNAP标头为首。因此，第一个字节的明文（cleartext）值恰为众所皆知的0xAA（SNAP标头的第一个字节）。既然知道第一个字节的明文，若与第一个已加密的字节进行XOR运算，便可轻易推断出密钥流的第一个字节。

该篇论文将攻击的焦点锁定在以(B+3):FF:N为格式的弱密钥（weak key）上。每个弱IV（weak IV）用来攻击该RC4密钥的某个特殊字节。密钥字节由0算起。因此，对应到密钥的第零个字节的弱IV格式即为3:FF:N，第二个字节必然是0xFF。此外，虽然必须知道该密钥的第三个字节，但其值未定。

标准的WEP密钥内含40个秘密位，或可以视为编号由0至4的5个字节。在以标准WEP作为防护的网络中，弱IV的第一个字节必然不会超出由3（B=0）到7（B=4）的范围，而第二个字节的值必定为255。虽然必须特别注记第三个字节，不过其值未定。在静态WEP网络中，存在5 × 1 × 256=1280个弱IV。这篇论文出版之后，陆陆续续又发现了许多不同的弱IV，使得弱IV的总数攀升至9 000个左右，相当于IV总数的5%。这些

注5：802.11规定帧遗失时必须重传，因此攻击者得以重送经过调包的帧，利用瞒天过海的手法让接收端误认其为合法的而加以接受。

新发现的弱点主要取决于IV字节之间的关系。有兴趣的读者可以参考WEP破解工具的源代码（注6）。

每个弱IV所泄露的信息和密钥的某个特定字节有关。通过应用概率论，Fluhrer、Mantin以及Shamir预测：要确定一个密钥字节大概需要解析60个案例。最糟糕的是，一旦破解的字节越多，攻击的速度就会越快。破解第一个密钥字节有助于破解第二个，依此类推。积小胜为大胜，总体而言，攻击是以线性时间进行。将密钥长度加倍，攻克的时间也只是以等比的方式增加。

既然理论如此诱人，对实际系统发动攻击不过是时间早晚的问题。2001年8月初，Adam Stubblefield、John Ioannidis以及Avi Rubin应用FMS理论，对一套试验性质的实际网络进行攻击，结果相当令人震惊（注7）。在他们的测试中，确定一个密钥的字节通常需要解析60个案例，而完全破解密钥也大概只需要解析256个案例。从订购无线网卡到找出完整的密钥，实际攻克的时间不超过一个星期。编写攻击程序只需要几个小时。破解密钥大概需要五六百万个封包，这对不算忙碌的网络而言也不过是个小数目。

不过，和公开的破解程序代码比起来，破解报告可以说是微不足道。Fluhrer/Mantin/Shamir提出的攻击方式在实现上并不困难，棘手之处在于如何找出RC4的弱点。2001年8月底，一套可以恢复WEP密钥的开放源码程序AirSnort问世，随后也陆续出现了许多类似工具。

防范密钥恢复攻击

较长的密钥对防范密钥恢复攻击并无帮助。还原密钥所需要的时间可以分为搜集攻击所需的足够帧的搜集时间，以及运行程序得出密钥所需的计算时间。计算时间花不到几秒钟，搜集时间才是主导攻击的因素。较长的密钥需要稍微多一点的计算时间，但搜集时间仍然维持不变。当密钥长度增加时，就可以捕获更多弱IV。

有些厂商采用了一种防范机制，即避免使用弱IV。大多数厂商已经修改自家产品，在使用IV之前先行比对，若是属于弱IV则以非弱IV替换。遗憾的是，缩小IV空间的结果将导致IV重复使用的情况更容易发生。

网管人员可以使用比较牢靠的协议，比如第七章将探讨的802.11i，来应对密钥恢复攻击。对某些组织而言，这是一种解决方案。不过，新的协议不见得像动态WEP一样与现有设备兼容。为了减少使用WEP，如果更新密钥（re-key）对网络造成的负担尚在可接受范围内，大多数网管人员都会将此时间间隔设定为5至15分钟。

注6：　举例而言，各位可以参考Airsnort的源代码，比如*crack.c*中的*classify()*函数。

注7：　整个事件在AT&T实验室的技术报告TD-4ZCPZZ中有更完整的描述。

动态 WEP

随着注意力开始转向安全性，业界随即着手开发能够显著改善安全性的无线局域网技术。第一步是通过动态密钥更新以弥补 WEP 的不足。动态 WEP 使用的是一组不同的密钥，而不是让网络中所有工作站共享一个静态密钥来加密所有帧。实际的做法是，网络上所有工作站使用一个密钥来加密广播帧，但个别工作站使用自己的映射密钥来加密单播帧（注 8）。

分层式安全协议

写作本书第一版时，WEP 被视为一种不安全的安全系统。古老而又需要手动分配的、使用静态密钥的WEP基本上已遭破解。当大家逐渐了解WEP所能提供的防护相对有限且不足以保护大多数网络环境之际，有个任务组就此成立，负责加强 MAC 的安全性。该工作组的工作成果最后在 2004 年 6 月成为 802.11i 标准。

在研究证实 WEP 存在瑕疵与开发出较安全的技术以便支持之前，网管人员只能转而采用已经证明的位于较上层的安全协议，比如 IPSec（第三层）、SSL（第四层）以及 SSH（第七层）。既然静态 WEP 只能提供最低限度的安全性，较上层技术在加密上所提供的额外防护便有其价值所在。

随着较牢靠链路层技术的发展，分层式安全协议不再像以前那样是仙丹妙药（magic bullet）。要使用 IPSec，必须先安装、设定客户端软件。采用 SSL 的 VPN 在设定上比较简单，不过在非网页应用上则有其缺点。SSH 较为人所熟知，而且可以任意产生 TCP 传输隧道（TCP tunnel），不过通常需要大幅修改用户流程。（当各位阅读本书时，可能已经习惯使用 SSH；不过，或许各位并不希望让用户陷于苦海。）

随着本章与下两章所探讨的链路层安全技术的发展，现在我们终于能够在链路层打造安全的网络环境。一种日渐普及、用来构建安全无线网络的做法是，首先考虑这些新技术的能耐，然后再决定需要在上层协议中加入何种额外防护。如何在这些取舍间找出平衡点是本书与部署相关章节的主要议题。

注 8：只要有适当的密钥分配协议，甚至可以让好几个不同的组共享相同的设施。工作站使用自己的映射密钥来传递单播帧，也可以形成几个彼此独立的广播组，各组使用自己的默认密钥来传递组帧。

WEP 并未制定出一套密钥管理框架。密钥的生成与分配是通过一组 802.11 未曾明文规定的系统。最早也是最简单的密钥管理框架就是通过手动的方式来实现。网管人员必须指定一串位以作为密钥，然后将之分配给位于相同802.11服务集的所有工作站。要设定密钥，网管人员必须亲自搞定需要设定的机器。

动态 WEP 使用经过改良的密钥管理框架。它使用较坚固的加密协议来产生密钥，同时通过加密以便在不安全的网络上分配密钥，不再凡事依赖网管人员手动完成。WEP密钥的产生通常会运用到下一章所探讨的加密认证协议。

动态WEP处理帧时和静态WEP采取的方式相同。唯一的差别在于前者使用经过改良的机制，每隔一段时间就会产生并分配新的密钥。动态 WEP 所采用的自动密钥管理机制相比较于静态 WEP 而言，能够提供更好的安全性，因为它动态地缩短了每把密钥的使用时间。更新密钥后仍可使用原本的帧初始向量，因为两者对应到不同的WEP种子。如此一来，通过Fluhrer/Mantin/Shamir所进行的密钥恢复攻击就必须在同一个密钥的使用期间完成。动态WEP 并不完美，不过比起静态WEP 已有显著的改善。几乎所有网卡与驱动程序都已支持动态 WEP。

第六章

802.11x 用户身份验证

你叫什么名字?

你在寻找什么?

你最喜欢的颜色是?

——守桥者（*Bridgekeeper*）

巨蟒与圣杯（*Monty Python and the Holy Grail*）

过去的几年，安全一直是无线局域网相关报道的主轴。一些民意调查显示，网络管理人员认为安全乃是无线局域网能否广为接受的最大障碍。许多安全问题其实可以追溯到WEP设计上的瑕疵。

静态WEP企图同时解决好几个问题。它既打算提供身份验证（authentication）以限定拥有特定密钥方能进行网络访问，也想要提供机密性（confidentiality）以在数据经过无线链路时予以加密。最后分析发现，它在这两方面的表现都不是特别好。身份验证与机密性都是无线局域网的重要议题，也是本书第一版问世后许多技术发展的重心。

本章主要探讨身份验证，它是802.1X在链路层所提供的机制（注1）。本书第一版问世以来，802.1X已经成熟许多，并且逐渐成为无线局域网上身份验证协议的首选（注2）。

注1：802.1X中的X以大写表示。在IEEE的命名原则里，小写字母（比如“802.11a”和“802.11b”）保留给修订现有标准的附加规范使用，大写字母则用于独立的规范。既然802.1X本身是个完整独立的协议规范，因此以大写字母来表示。

注2：我个人用来判断一项规范是否成熟的标准，就是有没有开放源码实现。开放源码软件通常扮演相当有价值的角色，除了使专属实现产品不敢任意妄为（keeping proprietary implementations honest）以外，也为用户提供低成本的事实校验。在802.1X世界里，xsupplicant和wpa_supplicant项目就属此类。

静态WEP只是对拥有加密密钥的机器进行身份验证。802.1X则允许网管人员对用户而非机器进行身份验证，同时可以确保用户连接至合法、经过授权而非窃取个人数据的冒牌网络。

识别用户（而非机器）的身份可以让网络架构更有效率。如此一来，就没有必要以功能来区分用户或者对物理位置上的物理连接端口实施安全管理；相反地，用户身份与访问权限均可整合进网络的交换结构中并且一路伴随用户。无线局域网通常会首先强制采用身份识别策略。公司通常是使用一段时间后发现无线网络的好处，然后希望将它整合进有线网络。不论用户置身何处或者使用何种方式连上网络，身份识别策略均可如影随形。

802.1X的复杂之处在于它本身只是一个框架。它是IEEE采用IETF的可扩展身份验证协议（Extensible Authentication Protocol，简称EAP）制定而成。EAP属于一种框架协议，最初规范于RFC 2284，后来经RFC 3748更新。EAP本身并未规范如何识别用户，但允许协议设计人员打造自己的EAP认证方式（*EAP method*），即用来进行交换操作的子协议。EAP认证方式可以有不同目的，因此通常根据特殊情况的需求采用不同的方式识别用户的身份。不过在详细探讨不同认证方式之前，必须先了解EAP的运作方式。

可扩展身份验证协议（EAP）

802.1X的基础是EAP。由于近年来无线网络的发展，原本的EAP标准已经不敷使用，更新后的版本请见RFC3748。当PPP在20世纪90年代初期问世时，有两种协议可用来识别用户的身份，两者都会用到PPP协议编号。身份验证不可能“一体适用”（one size fits all），而且它在当时算是相当活跃的研究领域。IETF并未摒弃可能就此无用的PPP协议编号，而是制定了EAP标准。EAP是一种简单的封装方式，可以运行于任何的链路层，不过它在PPP链路上并未广泛使用。EAP的基本架构如图6-1所示，在设计上是为了能够运行于任何的链路层以及使用各种身份验证方式。

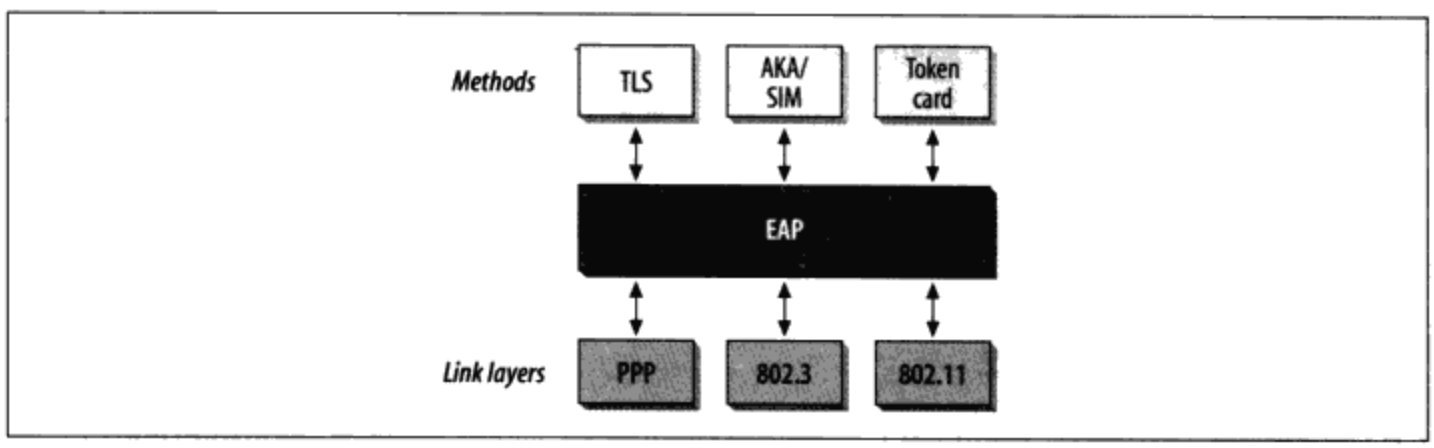


图6-1：EAP的架构

EAP 的封包格式

EAP的封包格式如图 6-2 所示。在 PPP 链路上使用时，EAP是由 PPP 帧所承载，协议编号为 0xC227。EAP 并不是非得运行在 PPP 之上，图 6-2 的封包可以通过任何一种帧来承载。EAP 封包包含下列字段：

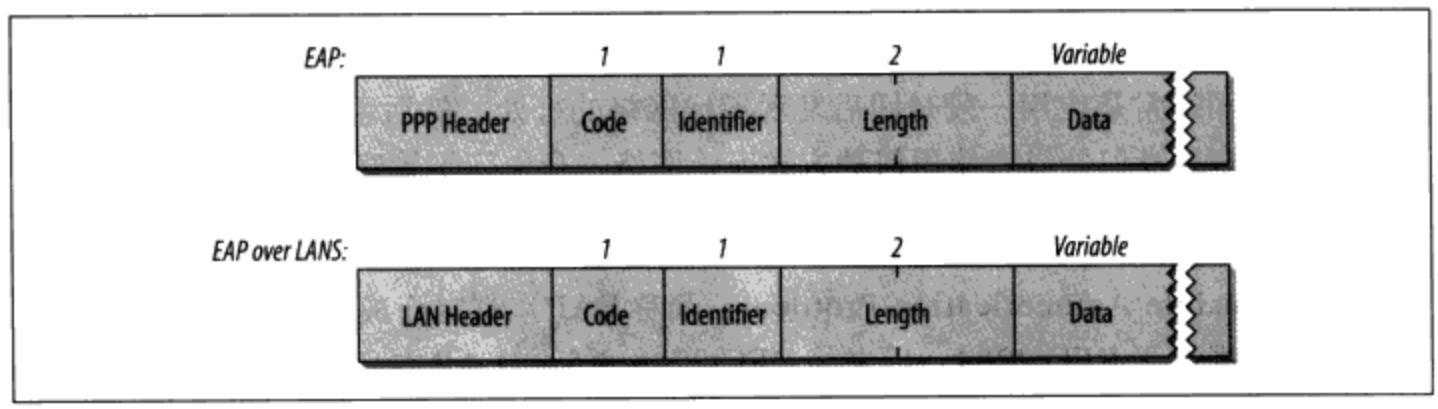


图 6-2：EAP 的封包格式

Code（类型代码）

封包的第一个字段是 Code（类型代码），其长度为 1 个字节，代表 EAP 封包的类型。封包的 Data（数据）字段必须通过此字段来解析。

Identifier（标识符）

Identifier（标识符）字段的长度为 1 个字节。其内容为 1 个无符号整数，用来匹配请求与响应。重传时会使用相同的 identifier number（标识符编号），新的传送则使用新的 identifier number。

Length（长度）

Length（长度）字段本身占有 2 个字节。它记载了整个封包的总字节数，包括Code、Identifier、Length 以及 Data 这 4 个字段。在某些链路层协议中，有时可能必须补零（padding）。EAP 会假设所有超过 Length 字段所记载的长度的数据都是链路层额外添加的，因此可以忽略不计。

Data（数据）

最后一个是 Data（数据）字段，其长度不定，取决于封包的类型，Data 字段也可能不占用任何字节。Data 字段如何解析完全取决于 Code 字段的值。

EAP 的请求与响应

EAP的交换操作由请求（request）与响应（response）构成。认证者（authenticator）会送出请求给想要进行访问的系统，并根据所得到的响应决定是否允许对方进行访问。如

果认证者已经送出请求，客户端系统只能送出响应封包，不容许发送多余的封包来请求身份验证。请求与响应封包的格式如图 6-3 所示。

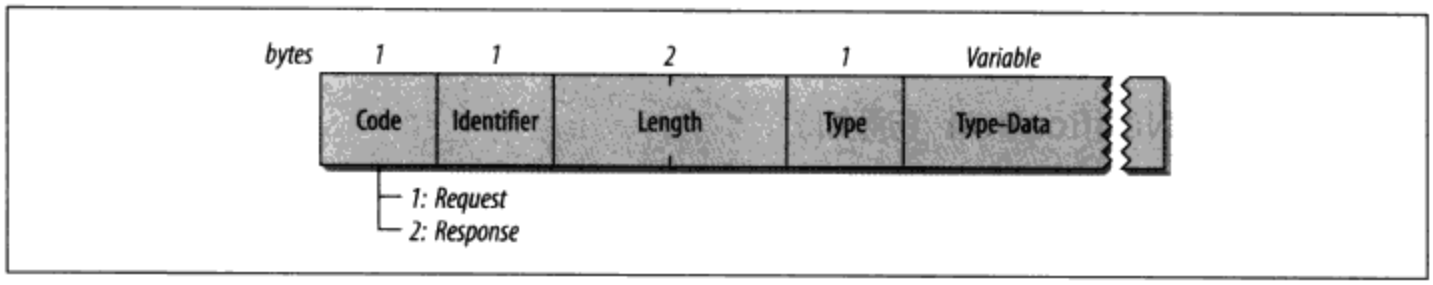


图 6-3：EPA 的请求与响应封包的格式

Code 字段的值为 1 代表请求，2 代表响应。Identifier 与 Length 字段的用法，如上一节的基本格式所述。Data 字段用来携带请求与响应所使用的数据。每个 Data 字段会携带一种数据，可再细分为 type identifier code（类型标识符）以及 associated data（关联数据）：

Type（类型）

Type（类型）字段的长度为 1 个字节，代表请求或响应类型。每个封包只能使用一种类型。唯一的例外是，响应的 Type 字段与其对应的请求一致。即当无法接受某个请求时，对方可以送出一个 NAK 来提议使用不同的类型。大于或等于 4 的 Type 字段值代表身份验证方式。

Type-Data（类型－数据）

Type-Data（类型－数据）字段长度不定，必须根据每种类型的规则加以诠释。

类型代码 1：Identity（身份）

认证者通常会以 Identity（身份）类型作为最初的请求，这一般以 *EAP-Request/Identity* 来表示或者简写为*Request/Identity*，表示认证者试图建立某种用户名称以便进行身份验证。通常 EAP Identity 即为用户身份，或许附带一些路由信息。有些技术的运作方式是送出对应于机器的 EAP Indentity。在一开始的 Request/Identity 封包中，如果有任何信息出现在 Type-Data 字段中，它就会被用来提示用户，虽然这比较不常见。如果 Type-Data 字段存在并且包含提示字符串，则此字符串长度可以从 EAP 封包的长度推论得知，不必另外使用界定符（delimiter）。

有些 EAP 实现可以提示用户（指人）输入必要的信息以判断其身份，虽然这并非必要。为了使用起来更方便，大多数 EAP 实现也允许静态设定身份。一旦知道用户名称，EAP 客户端程序就会响应一个 *Response/Identity* 封包。Response/Identity 封包的 Type-Data 字段包含了用户名称。它可以是“纯粹”的用户名称，例如*mgast*，或者是附带 Internet 风格的域名（*mgast@domain.com*），或者是 Windows 风格的域名（*DOMAIN\mgast*）。

有些EAP实现可能会在送出认证质询（authentication challenge）信息之前试图找出用户的身份。如果用户不存在，整个认证过程就算失败，不会再做进一步的处理。大部分的实现会再次送出身份请求以防用户打字错误。

类型代码2：Notification（通知）

认证者可以使用Notification（通知）类型传送消息给用户。用户的系统随后可将*Request/Notification*中的消息显示给用户看。Notification消息是由认证系统提供消息给用户，例如密码即将过期或者账号被锁定的原因。Notification消息在802.1X中并不常用。Notification请求的回复中必须有送出的响应。不过，*Request/Notification*属于简单的确认（acknowledgment），而Type-Data字段的长度为0。

类型代码3：NAK（否定确认）

nullac knowledgment（否定确认，简称NAK）主要用来建议使用新的身份验证方式。认证者会在送出的质询（challenge）消息中指定身份验证所使用的类型代码（type code）。身份验证类型的代码为4及以上的数字。如果用户的系统不支持质询所使用的身份验证类型，可以回复NAK。NAK的Type-Data字段包含其所建议使用的认证类型。大多数802.1X实现并不会主动协商，如果客户端尝试使用不支持的类型，则只会记录一个错误消息。

EAP身份验证方式

除了流量控制与协商消息，EAP也会为身份验证的方式指定类型代码。EAP会把证明用户身份的操作授权给一个称为*EAP method*（一组验证用户身份的规则）的附属协议。

使用EAP method的优点是，EAP从此可以不用去管验证用户的细节。如果需求改变，这是无线网络普及之后常有的情况，就可以开发新的EAP method来满足这个需求。表6-1列出了一些EAP method以及它们的类型代码。无线局域网常用的EAP method将于本章稍后详细说明。

表6-1：802.1X身份验证常用的EAP认证方式（EAP method）

类型代码	身份验证协议	说明
4	MD5 Challenge	EAP中类似CHAP的认证方式
6	GTC	原本打算与RSA SecurID之类的令牌卡（token card）一起使用
13	EAP-TLS	以数字证书（digital certificate）相互认证

表6-1：802.1X身份验证常用的EAP认证方式（EAP method）（续）

类型代码	身份验证协议	说明
21	TTLS	隧道式TLS；以TLS加密保护较弱的身份验证方式
25	PEAP	防护型EAP；以TLS加密保护较弱的EAP认证方式
18	EAP-SIM	以移动电话的用户识别模块（Subscriber Identity Module，简称SIM）卡进行身份验证
29	MS-CHAP-V2	Microsoft的经加密的密码（password）身份验证；兼容于Windows域

EAP认证的成功与失败

在EAP交换结束之后，用户不是认证成功，就是认证失败。一旦认证者判断出整个交换过程已经完成，就会发出一个EAP-Success（代码3）或EAP-Failure（代码4）帧，以结束整个EAP交换过程。实现时，在送出认证失败信息之前，允许用户送出多个请求信息，好让用户有机会获得正确的认证数据。

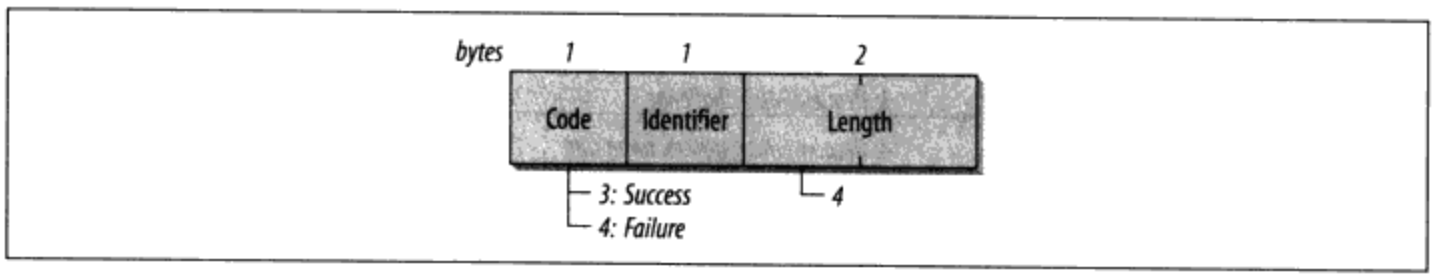


图6-4：EAP认证成功与失败的帧

无论是成功还是失败，帧都不会再经过任何形式的验证。在拨号的世界里，电话网络提供了某种程度的安全性，可以确保发送者必然位于线路的另外一端。在无线局域网络中，若要解决未能进一步验证Success与Failure帧的情况，可能需要额外的设计。

EAP交换范例

EAP交换范例如图6-5所示。这并不是无线网络中“实际”可见的交换过程，因为其中用到了一些未曾广泛部署的协议。举这个例子只是为了让读者对EAP协议的运作方式有基本的概念。EAP交换过程是一系列的步骤，从认证请求开始，以成功或失败信息结束。附带说明，在EAP认证方式交换过程中，由认证者所发送的封包是以*Request/Method*表示，如果是客户端所答复的响应则以*Response/Method*表示。

1. 认证者（authenticator）发出一个Request/Identity（请求/身份证明）封包以识别

用户身份。Request/Identity 封包有两个目的，除了启动交换过程外，也用来告诉客户端在身份验证完成之前网络将会丢弃任何传输数据。

2. 客户端要求用户输入标识符，随后将所搜集到的用户标识符以 Response/Identify（响应 / 身份证明）消息送出。

3. 一旦认出该用户，认证者随即会送出认证质询。在图6-5的第三个步骤中，认证者以一个 Request/MD-5 Challenge（请求 /MD-5 质询）封包送出 MD-5 Challenge（MD-5 质询）给用户。

4. 客户端在设定上是以 token card（令牌卡）进行身份验证，因此它会送出一个 Response/NAK（响应 / 否定确认）消息，提议以 Generic Token Card（一般令牌卡）作为认证机制。

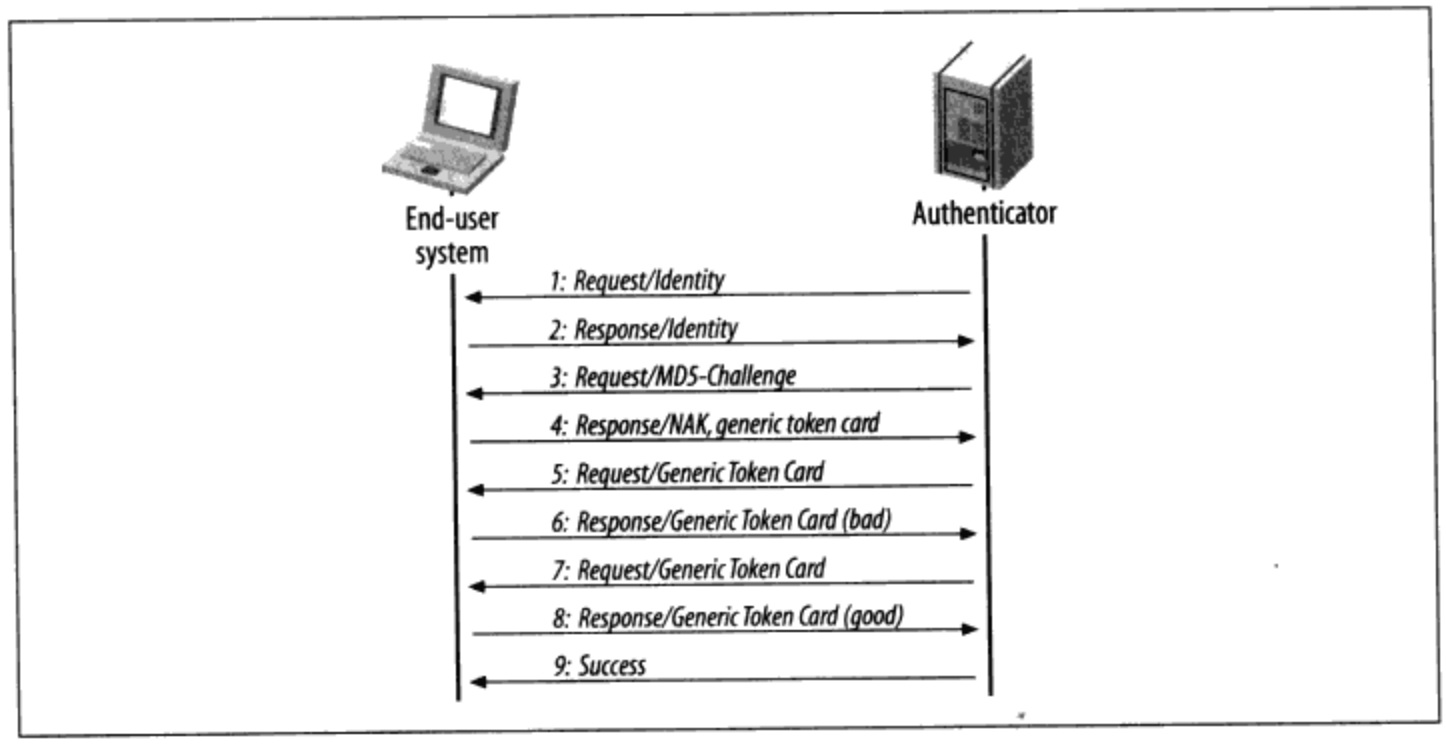


图 6-5：简单的 EAP 交换过程

5. 认证者会送出一个 Request/Generic Token Card（请求 / 一般令牌卡）的质询，要求取得卡号（numerical sequence on the card）。

6. 用户输入卡号，通过 Response/Generic Token Card（响应 / 一般令牌卡）送回。

7. 用户的响应并不正确，因此认证失败。不过，这个认证者在 EAP 的实现中允许多次认证，因此会送出第二个 Request/Generic Token Card（请求 / 一般令牌卡）的质询。

8. 用户再度响应，依然通过 Response/Generic Token Card（响应 / 一般令牌卡）传递。

9. 此次的响应正确，因此认证者发出一个 Success（成功）消息。

EAP 认证方式（EAP Method）

可扩展性（EAP 当中的“E”）既是 EAP 最大的优点也是最大的缺点。可扩展性让协议能够在有新的需求浮现时开发新的功能。正因为本身的可扩展性，EAP 已经从保留 PPP 协议编号的方式转变为无线局域网安全防护的基础。不过，要正确部署 EAP 可能不容易，因为要选择正确的协议选项之前必须先厘清一大堆问题。EAP 之所以具有灵活性，关键在于它本身只是一个框架。当新的需求浮现时就可以设计出新的认证方式，就算要用于无线局域网也不成问题。

无线局域网安全防护协议这个议题十分广泛，本章试图一点一滴（bit-by-bit）勾勒出协议运作机制的细节。很多复杂的细节只会以文字来描述，不会用详细的封包格式图来说明。

加密的方式

EAP method 的选择通常取决于后端所使用的身份验证系统。早期的 EAP method 主要将焦点放在如何提供与认证服务器之间的传输信道上。针对无线网络所设计的新型认证方式除了可以跟认证服务器进行能信，也符合无线局域网特有的三项要求：

为用户的数据提供坚固的加密（cryptographic）防护

在定义上，无线局域网应该被视为一种开放媒介。若要确保安全，任何通过无线网络传送的数据都必须加以保护。大多数针对无线局域网所设计的 EAP method 均采用 TLS 来提供私密数据的加密防护。

相互认证

早期无线局域网协议的设计将身份验证视为接入点对用户提出的要求。随着接入点价格的滑落，如今攻击者已经能够部署“欺骗”（rogue）接入点，用来窃取用户的私密数据。依常理判断，除了用户的身份验证，客户端设备还必须验证它们所连接的网络是否正确无误。

派生密钥

使用手动定义的密钥的 WEP 机制只能为无线链路上的帧提供很少的保护。较坚固的安全防护协议必须使用由熵池（entropy pool）派生而成的动态密钥。提供坚固的加密防护的副作用是，此类协议还会产生一份共享的加密流，可用来传递密钥给链路层安全防护协议。

LEAP

Cisco专属的Lightweight EAP（轻量级EAP，简称LEAP）（注3）是最早广泛使用的无线网络身份验证方式。相对于通过手动方式设定密钥的WEP，LEAP可以说是往前迈进了一大步，虽然它还有很多地方有待改进。基本上，LEAP进行了两次MS-CHAP version 1交换。第一次由用户对网络进行验证，第二次由网络对用户进行身份验证。动态密钥派生自MS-CHAP交换。

一些最糟糕的安全问题都是由MS-CHAP version 1所引起的。MS-CHAP version 1有一些安全上的问题，容易导致字典式攻击（dictionary attack）。攻击LEAP弱点的程序代码目前已经广泛流传。

LEAP算是一种过渡性的解决方案，虽然相较于手动设定密钥的WEP而言，它在安全上有显著的优点，不过使用过时的MS-CHAP作为核心反而缩短了它的使用寿命。等到其他协议陆续问世后，LEAP就没有存在的必要了。目前，Cisco建议使用PEAP或者EAP-FAST作为替代方案。

类型代码13：EAP-TLS

Transport Layer Security（传输层安全，简称TLS）协议原本就是设计来用于易被窃听的链路层上。TLS的前身是确保安全网络事务的协议Secure Socket Layer（安全套接层，简称SSL）。从许多方面来看，无线局域网的用例（use case）与因特网类似。数据必须在完全不可信赖且攻击者林立的网络环境中进行传送。TLS的目的就是在不可信赖的网络环境中建立一条可信赖的通信管道（channel）。

TLS通过证书交换来进行相互认证。用户必须将数字证书送交认证服务器以进行验证，但是认证服务器也必须提供本身的证书。通过可信赖的证书发行机构验证服务器证书的真伪，客户端就可以确定所连接的网络经过了证书发行机构授权。

EAP-TLS是第一个符合无线网络三项要求的身份验证方式。证书提供了牢靠的用户对网络以及网络对用户的双向认证。相互认证可以防范所谓的“欺骗”（rogue）接入点，让客户端能够判断接入点是否由正确的部门而非为了窃取密码的有心人士所设立。TLS还会建立一组主秘钥（master secret），用来派生出链路层安全防护协议所需要的密钥。

EAP-TLS虽然安全，不过并未被广泛使用。无线网络中任何潜在的用户都必须配备本身的数字证书。产生与分配证书以及遵循验证步骤都是莫大的挑战。已经采用公钥基础结

注3： 有些标准以“EAP-CiscoWireless”来称呼LEAP。

构（public key infrastructure，简称 PKI）的机构如果要使用 EAP-TLS 的话相当容易；而有些机构并不想构建 PKI，因而另外选用其他方式。

类型代码 21：EAP-TTLS 与类型代码 25：EAP-PEAP

实际上，需要使用 PKI 是无线局域网中推行坚固的身份验证时的主要障碍。PKI 不论在技术还是流程上都是一项艰巨的任务。大多数的组织宁可利用现有的身份验证系统，例如 Windows domain 或 Active Directory，LDAP directory 或者 Kerberos realm。重复使用现成的账号比起重新创建一套类似的身份验证系统来得简单。有两种 EAP method 能够搭配所谓的“旧式身份验证方式”一起使用，分别是隧道式 TLS（Tunneled TLS，简称 TTLS）与受保护的 EAP（Protected EAP，简称 PEAP）。

TTLS 与 PEAP 的运作方式相似。首先，协议会使用类似于 EAP-TLS 的方式建立起一个 TLS 隧道。进行下一个步骤之前，会先使用认证服务器的数字证书来验证此网络是否可信赖。第二个步骤是使用 TLS 隧道为旧式的身份验证协议加密，然后以它验证用户身份。有时候第一个步骤也称为“外层”（outer）身份验证，因为它是用来保护第二个或者“内层”（inner）身份验证的隧道。

证书还是免不了，但只有外层身份验证需要用到。TTLS 与 PEAP 将证书数目从千百张缩减为屈指可数，只有认证服务器需要使用证书。这就是为什么 TTLS 与 PEAP 远比 EAP-TLS 受欢迎。一般机构可以自行设立小型的证书管理中心，不必依赖外部证书机构所签发的昂贵证书。

TTLS 与 PEAP 之间些微的差异在于内层身份验证的处理方式。TTLS 使用加密信道来交换 attribute-value pair（属性 - 值对，简称 AVP），PEAP 则是在加密信道内进行第二次 EAP 交换。采用 AVP 使得 TTLS 较具灵活性，因为 AVP 可用来执行 EAP method 未提供的身份验证方式。

使用 TTLS 与 PEAP 的些许好处是，内层与外层身份验证可以使用不同的用户名称。这两种协议在进行外层身份验证时可以匿名进行，只有在加密信道中才会显示用户的真实身份，如此一来就不会在未经加密的帧中暴露用户名称。不过并非所有客户端软件均可隐藏用户的身份。

非加密式 EAP 认证方式

若无坚固的加密防护，有些 EAP method 并不适合直接用于无线网络。不过，它们可以作为 PEAP 或 TTLS 的内层身份验证方式。

类型代码4：MD-5 Challenge（MD-5质询）

MD-5 Challenge（MD-5质询）相当于RFC 1994所规范的CHAP协议。身份验证请求中包含了给客户端的质询。客户端只要能够成功响应质询，就可以证明它的确握有共享密钥。所有的EAP实现必须支持MD-5 Challenge。不过，它在无线网络领域并未得到广泛使用，因为它无法在无线网络上提供动态密钥。

类型代码6：Generic Token Card（一般令牌卡）

RSA公司的SecurID以及Secure Computing公司的Safeword，这一类的token card（令牌卡）在某些机构里特别受欢迎，因为它们（以“随机”的方式）提供类似一次性密码的安全性，但是没有一次性密码（one-time password，简称OTP）的种种麻烦。在请求消息中包含了身份验证所需要的Generic Token Card信息。请求消息的Type-Data字段的长度必须大于零。在响应消息里，Type-Data字段用来携带从token card复制的信息。在请求与响应封包里，EAP封包的Length字段则是用来计算Type-Data请求消息的长度。

EAP-GTC与EAP标准同样规范于RFC 2284。它允许通过网络交换明文身份验证证书。除了搭配令牌卡使用，EAP-GTC通常会被当成以“用户名称+密码”进行身份验证的EAP认证方式。如果数据库中现有的用户账号有只能进行比较但无法读取的单向加密密码（one-way encrypted password），EAP-GTC将能提供用来验证用户身份的EAP认证方式。当然，如果想要以EAP-GTC来传输可重复使用的密码，那么你必须使用隧道（tunnel）加以保护。

类型代码29：EAP-MSCHAP-V2

Microsoft CHAP version 2（简称MS-CHAP-V2）最早出现在Windows 2000操作系统中，规范于RFC 2759。它被设计用来解决MS-CHAP的缺陷，除了移除旧式客户端进行密码（password）编码时的弱点，还提供相互认证以及改善密钥生成与更换的机制。

MS-CHAP-V2广泛使用于Microsoft工作站，通常作为内层身份验证方式并搭配PEAP一起使用。MS-CHAP-V2是Windows网域最常见的内层身份验证方式。作为EAP认证方式使用时，EAP-MSCHAP-V2可以搭配TTLS或者PEAP一起使用。

类型代码18：EAP-SIM与类型代码23：EAP-AKA

还有两种值得注意的EAP认证方式：EAP-SIM与EAP-AKA，它们已经通过标准制定流程，主要是通过移动电话数据库进行身份验证。EAP-SIM为GSM电话网络上的SIM卡数据库提供了一个接口。EAP-AKA则是基于第三代移动电话网络上所使用的身份验证系统，称为Authentication and Key Agreement（认证与密钥协商，简称AKA）。

EAP-SIM 与 EAP-AKA 对于想要以移动电话账号整合计费功能的电信公司而言特别有用。他们可以使用现成的智能型芯片以及用户账号来验证用户的身份，用户不必另外指定新的密码即可访问数据网络。

其他的内层身份验证方式

TTLS 并不是只能搭配 EAP method 作为内层的身份验证方式。因此，有些较旧的身份验证方式也可以搭配 TTLS 一起使用。有些网络存放用户数据库的方式无法搭配 EAP method 一起使用，因为没有任何的 EAP method 能够提供可用的接口。

密码认证协议（Password Authentication Protocol，简称 PAP）

PAP 规范于 RFC 1334，原本是设计来和 PPP 一起使用。PAP 以未经加密的方式在网络上传递用户名称与密码。PAP 不能直接使用于无线网络，只能作为 TTLS 里的内层认证方式以确保不泄露密码。

PAP 可以和任何类型的身份验证系统一起使用。网络登录可通过网络操作系统加以验证。令牌卡（token card）服务器可用来验证明文令牌码（cleartext token code）。PAP 也可用于只能进行比较但无法读取的单向加密密码（one-way encrypted password）。单向加密密码用于 Unix 的 */etc/passwd* 密码文件以及大多数的 LDAP 目录中。Kerbero 系统也是以单向加密来存放密码的。

质询握手认证协议（Challenge Handshake Authentication Protocol，简称 CHAP）

和 PAP 一样，CHAP 原本也是设计来和 PPP 一起使用的，规范于 RFC 1994。使用 CHAP 进行认证时，认证服务器首先会发出质询信息给客户端，而客户端只要能够成功响应质询信息，就可以证明它的确握有共享密钥。

CHAP 原本是设计来避免以明文方式传递密码之类的秘密。CHAP 的缺点是连接双方都必须知道明文密码。在服务器方面，此密码要不是以明文方式存放，就是尽管经过加密但有办法加以解密，这样服务器软件才能将之还原为明文。

无线环境通常不会使用 CHAP，除非现有的用户数据库十分庞大，而且所使用的就是 CHAP。

MS-CHAP, version 1

MS-CHAP 是由 Microsoft 设计的用来提供类似 CHAP 的功能，但是针对 Windows 操作系统提供加强型的功能。它是 Microsoft 的专属协议，不过规范于 RFC 2433。和 CHAP

不同，MS-CHAP 并不需要以明文方式将共享秘钥存放于连接双方。MS-CHAP 将会使用 MD4 散列来存放用户密码，而不是采用明文密码来作为共享的秘钥。

在使用Microsoft认证数据库的环境中，MS-CHAP比较有用。不过以安全的观点来看，MS-CHAP 存在某些特殊的问题，除非必须支持相当旧的 Microsoft 操作系统，例如 Windows 95/98，否则最好不要使用。MS-CHAP 并不是 EAP method，只有 TTLS 才支持它。

限制 EAP 认证方式

有些EAP method比较坚固。为了安全起见，有些设备厂商会在认证者当中限制可以使用的 EAP method。EAP-MD5 通常被列在 EAP 类型限制列表中，因为它比其他采用 TLS 的认证方式要脆弱得多。

其实限制EAP认证方式并没有必要，实际使用时反而可能会妨碍良好的安全性。有些限制条件只允许采用 TLS 的隧道认证方式（类型 13、21 与 25）。如果之后出现新的 EAP 认证方式，有些具备这项功能的实现产品会默认禁用。允许调整限制条件或许是可行的解决方案，不过目前并未听说有这类实现产品出现。

从安全的观点来看，限制 EAP 认证方式实际上并没有太大的价值。认证服务器可以强迫使用坚固的认证方式，拒绝那些使用脆弱认证方式的请求。无论如何，没有密钥素材就无法连接至网络。如果认证过程中无法产生需要的密钥，有些接入点就会将认证过程视为无效，并且将客户端踢出网络，要求对方重新进行认证。进行 EAP-MD5 认证时，如果未能产生密钥，当接入点解除客户端的关联时，就必须重新开始。

部分是因为这些问题，EAP 规范中并不允许限制 EAP 认证方式。RFC 3748 的 2.3 节强制要求认证者必须将所有 EAP 认证方式转送给认证服务器处理。

802.1X：网络连接端口的认证

局域网在20世纪90年代被广为使用，其连接端口也如雨后春笋般四处涌现。某些类型的组织，例如大学，被要求开放的呼声所困扰。网络资源必须开放给用户群，不过群体本身并不固定。学生和其他网络用户不同，他们经常游走于不同的计算机之间，而且没有固定的网络地址；他们会毕业、迁移、注册入学、离开校园、工作或因为其他改变而需要更改使用权限。虽然网络访问权限必须足以容纳整个变动不定的社群，不过学校的经费通常有限，因此如何防止未经授权的外来者访问网络就变得十分重要。

简而言之，就是要使用网络，必须经过登录。然而不只是学校受惠于此，经过认证才能访问网络资源，对 Internet 服务供应商而言早已司空见惯，企业之所以会被这种做法所吸引，主要是因为如此一来，雇用计划可以很灵活。

在链路层（link layer）采用认证机制并不是什么新鲜事。网络连接端口的认证在拨号访问服务器上已经使用了多年。大部分的机构早已采用各种机制作为用户认证之用，例如 RADIUS 服务器与 LDAP 目录服务。以 PPP over Ethernet（简称 PPPoE）的用户认证为Ethernet访问进行把关的做法并不难理解，不过如此一来会增加系统的负荷与复杂度。因此，IEEE 采用 PPP 认证协议并开发了基于局域网络的版本。最后出炉的标准称为 802.1X，“基于端口的网络访问控制”（Port-Based Network Access Control）。

802.1X 的架构及相关术语

802.1X 为认证会话过程定义了三个组件，如图 6-6 a)所示。申请者（*supplicant*）是寻求访问网络资源的用户机器。网络访问由认证者（*authenticator*）控制，它扮演着传统拨号网络中访问服务器的角色。申请者与认证者在规范说明书中称为端口认证实体（Port Authentication Entity，简称 PAE）。认证者只负责链路层的认证交换过程，并不维护任何用户信息。任何认证请求均会被转送至认证服务器（例如RADIUS）进行实际的处理。

支持 802.1X 的设备上，各个连接端口若非处于授权状态（即可以使用该连接端口），就是处于未授权状态（即无法使用该连接端口）。不过即使处于未授权状态，如果网络管理人员允许的话，规范说明书中还是允许使用 DHCP 以及其他初始化信息。

整个认证交换过程在逻辑上是通过申请者与认证服务器来完成的，认证者只是扮演中介的角色。图6-6 b)所示为逻辑上的协议结构。申请者与认证者之间（即前端）使用由802.X 所定义的 EAPover LAN（简称 EAPOL）协议，在后端则是通过 RADIUS 封包来传递 EAP。有些文献称之为“EAP over RADIUS”。就算连接端口尚未得到授权，也尚未取得 IP 地址，申请者还是能够持续与 RADIUS 服务器进行 EAP 交换。

图6-6可以有两种不同的解读方式。在企业中，申请者是位于企业网络周边的一部主机，而 RADIUS 服务器则位于企业核心。本图同时显示了一家以 802.1 X 认证用户身份的 ISP，图左为 ISP 的访问范围，而图右则是 ISP 的骨干网络。

RADIUS 的好处是支持多种用户数据库。除了本地的数据库，RADIUS 服务器也可以作为通往 LDAP directory、Unix NIS 或 PAM、Kerboros realms、Microsoft Windows 用户账号，甚至是其他RADIUS 服务器的网关。RADIUS 相当有灵活性，甚至可以用统一格式整合截然不同的用户数据库。使用 RADIUS 在 Windows domain 或者 Active Directory 上提供认证时会有一些限制，这将于第二十二章加以探讨。

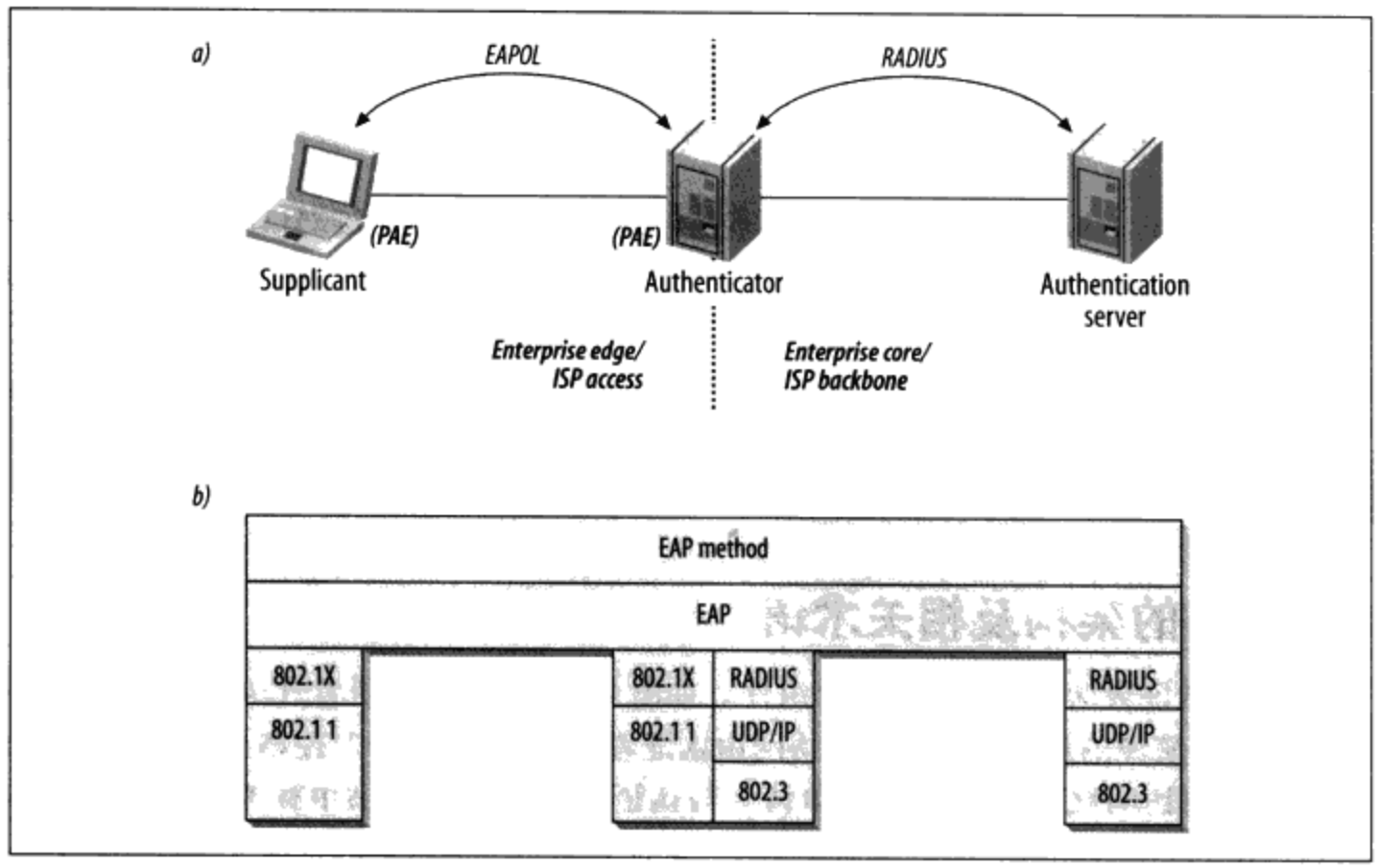


图 6-6：802.1x 的架构

802.1X只是一个框架，并非一套完整的规范。实际的认证机制其实是通过认证服务器来完成的。802.1X所提供的机制主要是用来发出质询信息以及确认或拒绝访问，实际上并不负责判断对方是否有权访问。改变认证的方式不需要大幅更动用户的设备或整个网络的基础设施。认证服务器可以重新设定配置以便“外挂”其他新的认证服务，而不必更换用户所使用的驱动程序或交换器的固件。

802.1X 的帧过滤

802.1X 利用允许任何数据通过之前必须先经过认证，来防范网络被未经授权的用户访问。处于未授权状态的连接端口通常限定只能传送认证帧，其他数据都会被丢弃。802.1X标准对如何完成整个过程有正式的探讨。不过以本书而言，只要说明未授权的连接端口会丢弃所有非EAPOL帧就够了。一旦工作站成功验证，就可以将数据帧送至适当的网络。

EAPOL 的封装格式

EAPOL的基本帧格式如图 6-7所示。目前有许多网络分析软件均可分析EAPOL的封装格式，包括 Ethereal。此帧的组成字段如下：

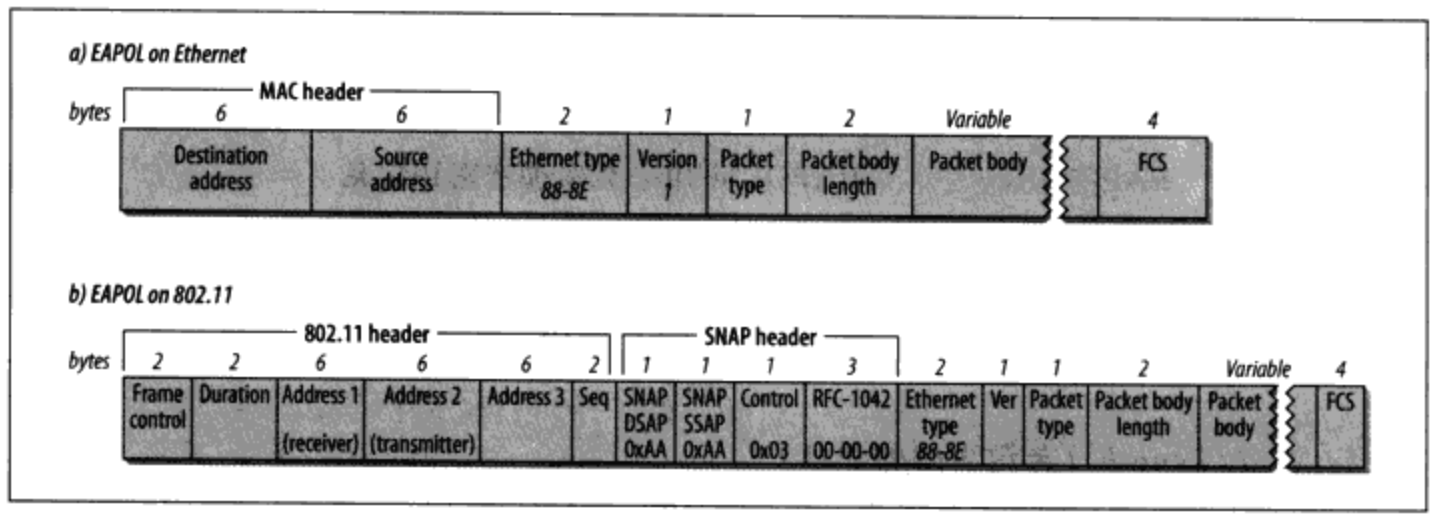


图 6-7：EAPOL 的帧格式

MAC 标头

图 6-7 所示为有线 Ethernet 以及 802.11 的封装格式。虽然 802.1X 帧的有效载荷（payload）相同，但是两者所使用的 MAC 标头并不一致。

Ethernet Type（以太网络类型）

和其他的 Ethernet 帧一样，Ethernet Type 字段包含了长度为 2 个字节的 type code（类型代码），EAPOL 的类型代码为 88-8e。

Version（版本）

第 1 版标准化于 2001 年版的 802.1X，第 2 版规范于 802.1X-2004。本章所描述的是 2001 年版，因为实现时比较常见。

Packet Type（封包类型）

EAPOL 是 EAP 的扩展。除了上一节所描述的 EAP 消息，EAPOL 还加入一些额外的消息，让 EAP 能够适用于基于连接端口的 LAN 环境。表 6-2 列出了所有封包类型及其说明。

表6-2：EAPOL消息的类型

封包类型	名称	说明
0000 0000	EAP-Packet	包含了一个经过封装的 EAP 帧。大部分的帧均属 EAP-Packet 帧
0000 0001	EAPOL-Start	申请者可以主动送出 EAPOL-Start 帧，不必等候来自认证者的质询信息。认证者会送出一个 EAP-Request/Identity 帧作为响应
0000 0010	EAPOL-Logoff	当某个系统不再需要使用网络时，便可发出一个 EAPOL-Logoff 帧，让连接端口重新回到未授权状态

表6-2：EAPOL消息的类型（续）

封包类型	名称	说明
0000 0011	EAPOL-Key	EAPOL 可用来交换加密密钥信息
0000 0100	EAPOL-Encap-sulated-ASF-Alert	警告标准讨论（Alerting Standards Forum，简称ASF）定义了一种方式，可让警告信息（例如SNMP trap）通过此类型的帧传送给未经授权的连接端口

Packet Body Length（封包主体的长度）

此字段本身的长度为2个字节，用来计算Packet Body（封包主体）字段的长度。如果没有封包内容，则此字段的值为0。

Packet Body（封包主体）

此字段的长度不定。EAPOL-Start与EAPOL-Logoff消息除外，此字段会出现于所有的EAPOL帧中。EAP-Packet帧所封装的是一个EAP封包，EAPOL-Key帧所封装的是一个密钥，而EAPOL-Encapsulated-ASF-Alert帧所封装的则是一段警告信息。

寻址

在类似Ethernet的共享媒介中，申请者是将EAPOL消息送至01:80:C2:00:00:03这个组地址。在802.11网络上并不存在类似的地址，而且只有在关联过程允许申请者（移动式工作站）以及认证者（接入点）交换MAC地址之后，才能进行EAPOL。在802.11这样的环境里，EAPOL会要求使用工作站的地址。

802.1X与无线局域网

802.1X为任何局域网，包括无线局域网，提供了一个用户认证的框架。就本书的目的而言，无线网络中802.1X中的“连接端口”，相当于无线设备与接入点之间的关联(association)。当链路层开始起作用时，Association Request与Association Response帧交换成功的信息会告知802.1X状态引擎（state engine）。一旦关联成功，工作站就可以开始进行802.1X帧交换过程，尝试取得授权。802.1X认证交换与密钥分配完成后，用户就会收到接口已经启用的信息。

802.11网络中的802.1X交换范例

EAPOL交换与EAP交换看起来几乎一样，主要的差别在于申请者可以发出EAPOL-Start帧触发EAP交换，也可以在网络使用完毕后发出EAPOL-Logoff消息解除连接端口的授

权。本节的范例假设后端以RADIUS为认证服务器，因此范例中会显示认证者将来自前端的EAP信息转换为后端的RADIUS信息。RADIUS封包中的EAP认证规范于RFC 2869。

范例中还显示出认证者是使用EAPOL-Key帧来分配密钥信息给链路层安全防护协议。图6-8所示的是在802.11网络上进行EAPOL交换的范例。此图所示范的是认证成功的例子，步骤如下：

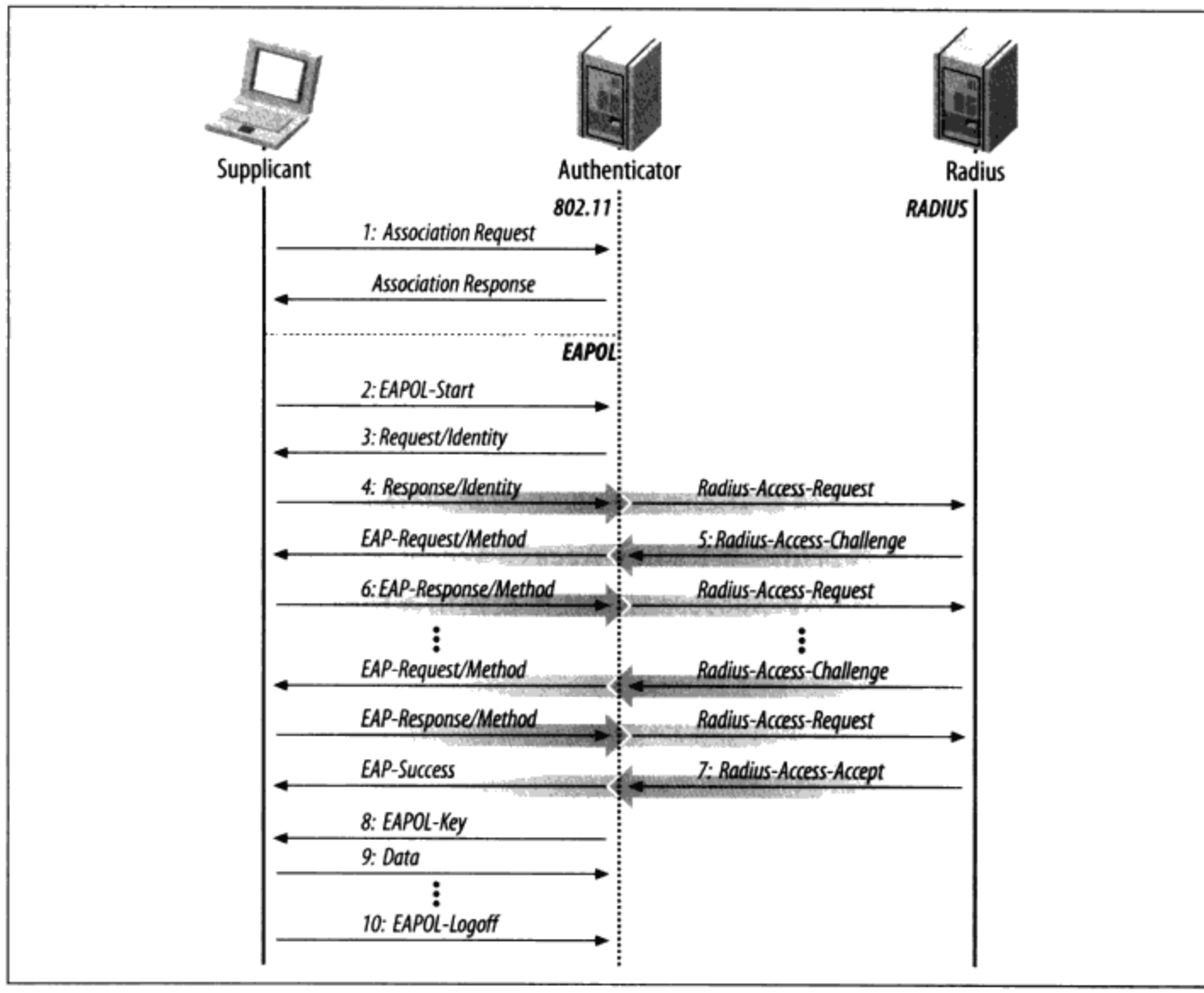


图6-8：802.11网络上典型的802.1x交换

1. 申请者关联至802.11网络。关联只用到两个帧，这种简单的交换过程几乎都会成功。
2. 申请者发出一个EAPOL-Start消息，开始进行802.1X交换过程。这个步骤并非必要，并非所有申请者都会送出EAPOL-Start消息，因此可能没有这个步骤。

3. “正常的”EAP交换过程开始。认证者（接入点）发出一个EAP-Request/Identity帧。如果接入点只为已经认证成功的关联转送帧，在发送Request/Identity帧之前可能就没有EAPOL-Start。主动发出的Request/Identity帧用来指示申请者必须进行802.1X认证。
4. 申请者以EAP-Response/Identity帧进行回复，此帧随后被转换为Radius-Access-Request封包送给RADIUS服务器。
5. RADIUS服务器判断需要使用那个类型的认证，并且在送出的EAP-Request信息中指定认证方式的类型。EAP-Request被封装于Radius-Access-Challenge封包中送给接入点。接入点收到封包后即将EAP-Request传递给申请者。EAP-Request信息通常会被表示为*EAP-Request/Method*，其中的“Method”代表所使用的EAP认证方式。如果目前使用的是PEAP，则返回的封包将以EAP-Request/PEAP来表示。
6. 申请者从用户方面取得响应，然后返回EAP-Response。认证者会将此响应转换为送给RADIUS的Radius-Access-Request封包，针对质询信息所作的响应则存放于数据字段中。

   — 步骤5与步骤6不断重复进行，直到认证完成为止。如果使用的是需要交换证书的EAP认证方式，免不了要多次重复这些步骤。有些EAP交换可能需要在客户端与RADIUS服务器之间反复进行10到20次。

7. 既然RADIUS服务器送出一个Radius-Access-Accept封包允许对方访问网络，因此认证者会发出一个EAP-Success帧并且授权使用连接端口。访问权限也可以由RADIUS服务器所返回的参数来决定。
8. 收到Access-Accept封包后，接入点会立即使用EAPOL-Key消息将密钥分配给申请者。密钥的分配将于下一章讨论。
9. 一旦申请者安装好密钥，就可以开始传送数据帧来访问网络。DHCP配置设定通常会在此刻进行。
10. 当申请者不再需要访问网络，就会送出一个EAPOL-Logoff消息，使连接端口恢复成未授权状态。

类似图6-8的交换过程可以在任何时间点进行。用户并不需要发出EAPOL-Start消息来启动EAPOL交换过程。任何时刻，申请者都可以开始进行EAPOL交换过程，发出EAP-Request/Identity帧来更新认证数据。需要重新进行认证通常是因为会话超时，此时就必须更新密钥。

动态产生密钥

EAPOL-Key 帧让接入点能够传送密钥给客户端，反之亦然。密钥交换帧只有在认证成功之后才会传送，这样可以避免密钥信息外泄。EAPOL-Key 帧也可以用来定期动态更新密钥。WEP的诸多弱点均因为长时间使用相同的密钥而产生。如果很难为网络上的所有工作站更新密钥，长期使用相同的密钥就在所难免。许多专家建议定期更换 WEP 密钥，不过一直没有实际的机制存在，直到 802.1X 问世之后这个问题才得到解决。

第七章

802.11：RSN、TKIP与CCMP

802.1X所提供的认证与密钥管理框架解决了WEP在设计上的两项主要瑕疵。其他尚待解决的缺陷主要是WEP的加密机制缺乏机密性。修正链路层加密协议的工作由802.11工作组（working group）的任务组（Task Group）I负责。几经延迟，这项任务终于在2004年6月完成，认可后正式成为标准。

802.11i采用双轨并行的做法以解决链路层加密协议的弱点问题。802.11i组成自两种新的链路层加密协议。第一种称为Temporal Key Integrity Protocol（临时密钥完整性协议，简称TKIP），被设计来尽可能强化pre-802.11i硬件的安全性。另外一种则是重新打造的加密协议，称为Counter Mode with CBC-MAC Protocol（计数器模式及密码块链消息认证码协议，简称CCMP），被设计来提供最高等级的安全性。

临时密钥完整性协议（TKIP）

第一种广为使用的新式链路层加密协议是临时密钥完整性协议（TKIP）（注1）。开发TKIP的主要动机是为了升级旧式基于WEP硬件的安全性。通常，具备WEP功能的芯片组都支持RC4加密机制。既然加密的重责大任由硬件负责，那么只要通过软件或固件，就可以达到升级的目的。TKIP保留了WEP的基本结构与操作方式，因为它原本就是一个设计来升级基于WEP的解决方案的软件。

注1：　制定标准的过程中，TKIP原本称为“WEP2”。当WEP最后被证明存在瑕疵时，此协议就被更名为“TKIP”，以便与WEP有所区别。

TKIP 与 WEP 的差异

为了克服 WEP 易遭受攻击的弱点，TKIP 整合了许多新协议的功能。尽管保留了 WEP 的基本架构与操作方式，不过TKIP为WEP最易遭受攻击的弱点另外绑上了“安全带”：

密钥层次结构与自动密钥管理

不同于WEP直接使用单一主密钥（master key）的做法，TKIP使用到了多个主密钥。最后用来加密帧的密钥是从这些主密钥派生而来。另外，TKIP 也提供密钥管理操作，使得主密钥的更新可以在安全的情况下进行。

每帧生成密钥（per-frame keying）

虽然TKIP保留WEP所使用的RC4帧加密机制，不过为了防范针对弱WEP密钥的攻击，它会为每个帧（从主密钥）派生出特有的RC4 密钥。为每个帧准备独特密钥的过程称为密钥混合（key mixing）。

序列号计数器（sequence counter）

为每个帧编序列号即可识别出次序错乱的帧，如此便能防范所谓的重放攻击（replay attack），亦即攻击者先拦截有效封包，等候一段时间再予以重传的攻击。

新的消息完整性校验（message integrity check，简称MIC）

TKIP以一种比较牢靠的称为*Michael*的完整性校验散列算法，取代WEP所使用的线性散列算法。Michael较为牢靠，探测伪造帧也更加容易。此外，源地址受到完整性校验的保护，就可以探测出宣称来自特定来源的伪造帧。

消息完整性校验失败的对策

设计时，TKIP是为了实现于现有的硬件，因此不免有所限制。Michael可能遭受主动式攻击而被攻陷，因此TKIP 包含了一些对策（countermeasure）以控制主动式攻击可能造成的损害。

此外，TKIP也经常与基于802.1X的密钥管理协议并用，如此一来，就可以借由身份验证事务来产生 TKIP 主密钥。

TKIP 初始向量的使用与密钥混合

WEP的主要破绽在于WEP的随机数种子（seed）是由初始向量（initialization vector，简称IV）以及 WEP 密钥所构成。既然随机数种子是由 IV 与密钥串联而成，IV 本身就泄露了大部分的密钥结构。如此一来，攻击者就可以观察IV的重复使用情况，进一步挖掘出用以加密帧的相同密钥流。以24-bit的IV而言，大约可以容纳1600万（16 million）个帧。在比较繁忙的网络上，这个数目并不算多。更糟的是，此IV空间受限于当时所使用的密钥。如果使用静态WEP，则IV空间是由网络上所有工作站所共享。何况，IV本

身构成密钥的前24位早已是众所皆知，难免会被第五章所提到的Fluher/Mantin/Shamir攻击法所破解。

为了防范针对初始向量的攻击，TKIP将IV的长度从24位倍增为48位。如此一来，初始向量空间即由1600万（16 million）增加为281万亿（281 trillion），可以有效防止IV空间在密钥的使用期限内耗尽。

TKIP同时以密钥混合（key mixing）的方式来防范针对WEP的攻击。通过密钥混合，用来加密个别帧的RC4密钥就会各自不同。在TKIP中，各个帧均会被特有的RC4密钥加密。换句话说，密钥混合进一步扩展了初始向量空间，稍后对此会有更为详细的探讨。一旦密钥混合过程将传送者的MAC地址纳入计算，就算两个工作站使用相同的初始向量，也可以衍生出不同的RC4密钥来加密帧。此外，密钥混合也有助于防范著名的Fluhrer/Mantin/Shamir攻击。此类攻击要能奏效，就必须搜集一些带有相同秘密位的“弱密钥”。只要各个帧使用不同密钥，TKIP就能够防止攻击者搜集足够的数据而针对这些密钥发动攻击。

TKIP序列号计数器与重放攻击保护

除了空间变大之外，TKIP初始向量本身也扮演着序列号计数器（sequence counter）的角色。每次安装新的主密钥，初始向量/序列号计数器就会被重设为1。每传一个帧，序列号计数器就会随之累加1。

为了防范重放攻击（replay attack），TKIP会保留来自各工作站的最近序列号。一旦成功接收到某个帧，就会以它与最近接收到的帧序列号进行比对。如果大于前值就予以接受，否则就予以拒绝。

服务质量（quality of service）扩展功能由任务组E负责开发。目前802.11e草案中有一项块确认（block acknowledgment）协议功能，它以单一帧确认多次传送。2005年1月所出版的802.11e草案中规定，检测重放攻击之前，必须先完成因块确认所导致的重新排序操作。

802.11单播帧（unicast frame）必须被确认。如果原始帧或其确认已经遗失，则该帧必须重传。在接收端可能重复接收到相同的序列号。序列号重复有可能只是因为连接出错，不一定就是有人正在进行主动式攻击。

Michael完整性校验与对策

WEP的完整性校验（integrity check）属于线性散列值，完全不适合加密应用。TKIP在设计上所面临的主要挑战之一，就是在强化完整性校验的同时还必须维持合理的性能。

设计 TKIP 时，大多数 802.11 芯片组所使用的处理器性能都不够强，数学运算不够快，无法及时进行完整性校验。实现时，Michael完全是采用swap、shift之类的接位(bitwise)运算方式，甚至是通过丢弃特定位的方式。因此，即使在大多数802.11接口上所使用的微处理器上运行，也不会对性能造成影响。（本章稍后将会详述 Michael。）

从 Micheal的设计中大致上可以看出它无法提供多少安全性。虽然远比循环冗余校验码好，不过它还是无法抵挡持续执着的攻击。TKIP 整合了一些对策，以关闭网络与更新密钥来侦测及应对主动攻击。

既然 Michael 需要准备对策，也就意味着底层所使用的密码学基础存在弱点。设计时，Michael 被迫与市面上目前采用RC4的大多数硬件兼容。虽然存在上述种种限制，其实 Michael 的设计相当精致，也已经将功能发挥得淋漓尽致，不过它仍然是建造在浮沙上的高塔。Michael 是否够安全就留待时间说明，就算明年就出现针对它的攻击，我也不会感到惊讶。不过，TKIP 在协议设计上的改良，有助于将恶意攻击的负面效果限制在某种范围内。我认为Michael 可能会屈服于拒绝服务（denial-of-service）攻击，但不至于导致大规模的网络瘫痪。

TKIP 的数据处理与操作

和 WEP 一样，TKIP 也支持加密与完整性保护过程，如图 7-1 所示。从图中可以清楚看出，TKIP 可以说是围绕着 WEP 而设计的一套安全功能。

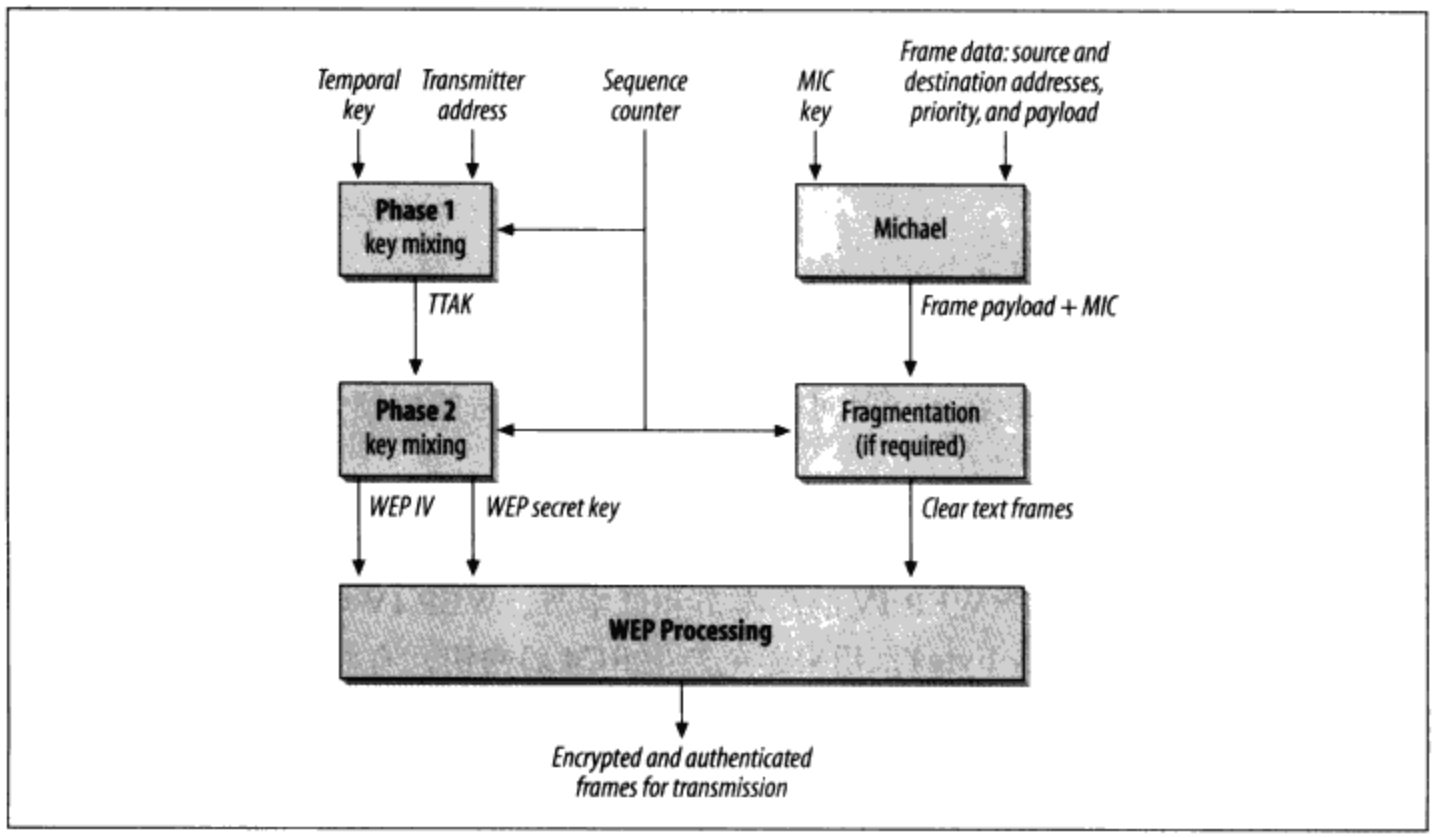


图 7-1：TKIP 的帧处理 —— 加密

TKIP会以下列项目作为输入项：

- 帧。
- 用来加密帧的临时密钥（*temporal key*）。
- Michael用来保护帧内容的MIC密钥。TKIP会派生出一对密钥，使得工作站至接入点的MIC密钥不同于接入点至工作站的MIC密钥。TKIP与WEP的不同之处在于MIC使用了密钥。
- 发送端地址也会被当成TKIP的输入项，因为必须用它来进行来源身份验证。发送端地址可以由帧提供，不必来自上层软件。
- 由驱动程序或固件所维护的序列号计数器（sequence counter）。

TKIP的密钥混合过程与密钥的构造

TKIP会为所传送的每个帧构造一把独特的密钥。此密钥派生自初始向量/序列号计数器、帧的发送端地址（未必是帧来源）以及临时密钥。密钥混合（key mixing）可以确保各个帧所使用的密钥彼此间存在显著的差异，以及防范任何假设WEP密钥的秘密成分维持不变的攻击。将发送端地址纳入密钥混合的计算，这样不同的工作站就算使用相同的初始向量，也会派生出不同的RC4密钥。

密钥混合功能的设计受限于802.11控制器的处理能力，如图7-2所示。TKIP将混合密钥的计算过程分为两阶段。第一阶段以发送端地址、序列号的前32位及128位的临时密钥作为输入项，输出项则是一个长度为80位的值。虽然有点复杂，不过所有计算都是由一些“简单”的运算（如addition、shift与XOR）所组成，以便减轻计算的负担。只要序列号的前32位为常数，第一阶段所计算出来的值也必然为常数，因此只要每65535个帧计算一次即可。

密钥混合的第二阶段必须对每个帧进行计算。第二阶段以第一阶段所计算的结果、临时密钥与序列号的最后16位为输入项。在这些输入项中，有所变动的只有序列号。它的变动方式经过明确定义，因此在实现时可以根据下一组序列号的值预先计算待传帧所需的数值。

密钥混合过程第二阶段的输出值是128位的RC4密钥，可以作为WEP的随机数种子。最后16位则是用来产生一个WEP IV的高字节和低字节。WEP IV中间的字节是一个值固定的虚设字节（dummy byte），用来避免产生RC4弱密钥。有些802.11接口可通过硬件的协助将RC4密钥作为输入项以产生密钥流，然后运用得到的密钥流来加密帧。密钥混合过程的第二阶段的输出项可以直接传给那些配备此类支持硬件的802.11接口。

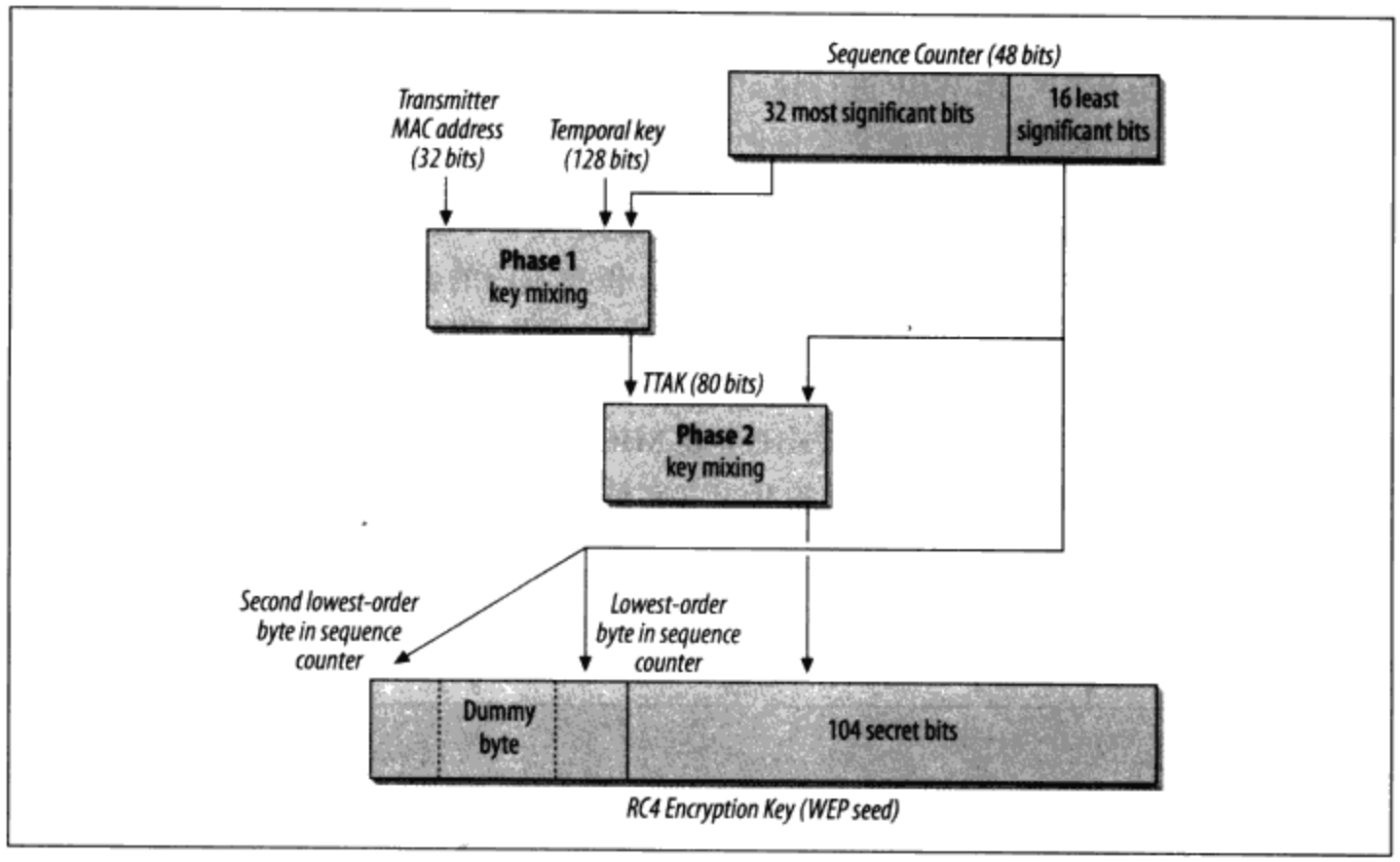


图 7-2：TKIP 密钥混合

TKIP 的数据传送

帧产生后，接着发送给 TKIP 以传送，过程如下：

1. 将 802.11 帧放在队列中等待传送（queued for transmission）。其中包含帧头以及有效载荷（payload）。和 WEP 一样，TKIP 只保护 802.11 MAC 的有效载荷，至于 802.11 帧头以及下层协议的标头则原封不动。
2. 计算消息完整性校验值（Message Integrity Check，简称 MIC）。和 WEP 不同的是，TKIP 的 MIC 属于较完善的加密散列。它以秘钥（secret key）作为验证过程的一部分，而且不只是保护 802.11 帧有效载荷。除了帧数据，MIC 还纳入了来源与目的地地址，以及未来 802.11e 标准将会用到的优先级位（priority bit）。
3. 赋予每个帧片段一个序列号。与 WEP 初始向量不同，TKIP 的序列号计数器会随每个帧片段累加。如果帧无需分段，那么只要编一个序列号即可，如果帧被分割为数个片段，计数器则会依片段数量累加。
4. 每个帧均会以其独有的 WEP 密钥进行加密。通过密钥混合过程，TKIP 为每个帧产生 WEP 密钥。每个帧所拥有的密钥（per-frame key）将会传给 WEP 以作为 IV 与秘钥之用。对每个帧而言，这两者均会随之变动。

5. 帧本身加上步骤2所得到的Michael消息完整性校验值以及步骤4所得到的RC4密钥一并传给WEP，由WEP进行帧封装操作，如第五章所述。值得注意的是，这意味着，受到TKIP保护的帧将会同时包含WEP的成分。

TKIP帧有类似于WEP的封装过程。图7-3所示的是受到TKIP保护的帧封装格式。IV/KeyID（初始向量/密钥标识符）保留自WEP，但有不同的含义。最前面的3个字节记载了部分的TKIP序列号以及目前使用的密钥编号。虽然TKIP支持多组密钥，但实际上只有KeyID 0会被分配使用。至于Extended IV（扩展初始向量，简称EIV）字段，则是用来记载其余的序列号。接下来TKIP会将MIC（消息完整性校验）码附加于有效载荷数据之后。而WEP会加入其自身的ICV（完整性校验值），以尽量维持WEP格式不变。

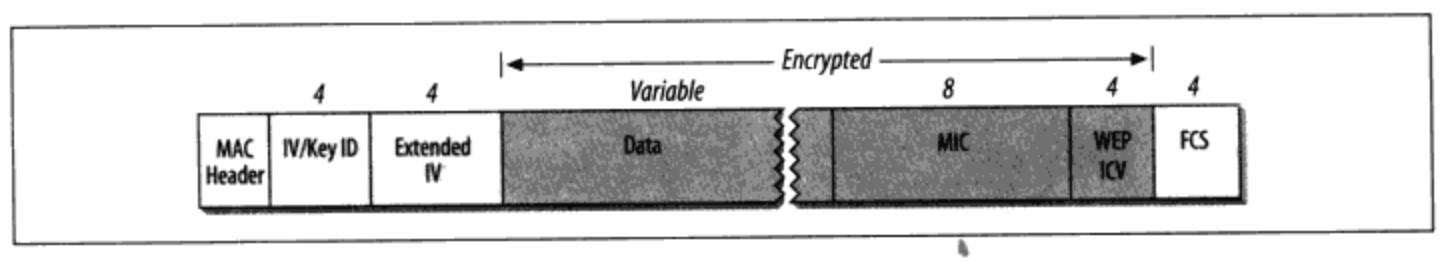


图7-3：TKIP封装格式

TKIP的接收

一旦接收到帧，TKIP就会逆转整个加密与传送过程。作为WEP的扩充版本，TKIP的设计在加密过程中新增了许多检查点（checkpoint），值得详细加以说明。由图7-4的方块图可知，在传递给较上层协议之前，哪些情况下会丢弃帧。

1. 一旦无线接口接收到帧，如果通过帧检查序列确认它不曾损毁，就会将其交付给TKIP做进一步的验证。
2. TKIP采取的第一个步骤是检查序列号以防范重放攻击。TKIP的重放攻击保护机制要求帧的接收必须依循相当严格的次序。如果帧序列号小于或等于最近已接收到的有效帧，就会因为可能遭到重放攻击而被摒弃。不像其他技术允许最近到达的帧可以不必完全依照顺序，TKIP的限制比较严格。不过对这样一种链路层技术而言，坚持依次接收并非无的放矢，因为在这种情况下，未能依序传送的几率应该是微乎其微。
3. 还原用来加密封包的WEP随机数种子。借由发送端地址、临时密钥以及序列号，接收端即可解锁（unmix the key）以恢复WEP随机数种子。
4. WEP随机数种子到手后，就可以除去帧外围所包裹的WEP层，然后还原内容。在还原内容的过程中，WEP ICV必须接受校验。虽然WEP的完整性校验并不牢靠，但还是可以用来防范一些无谓的攻击。

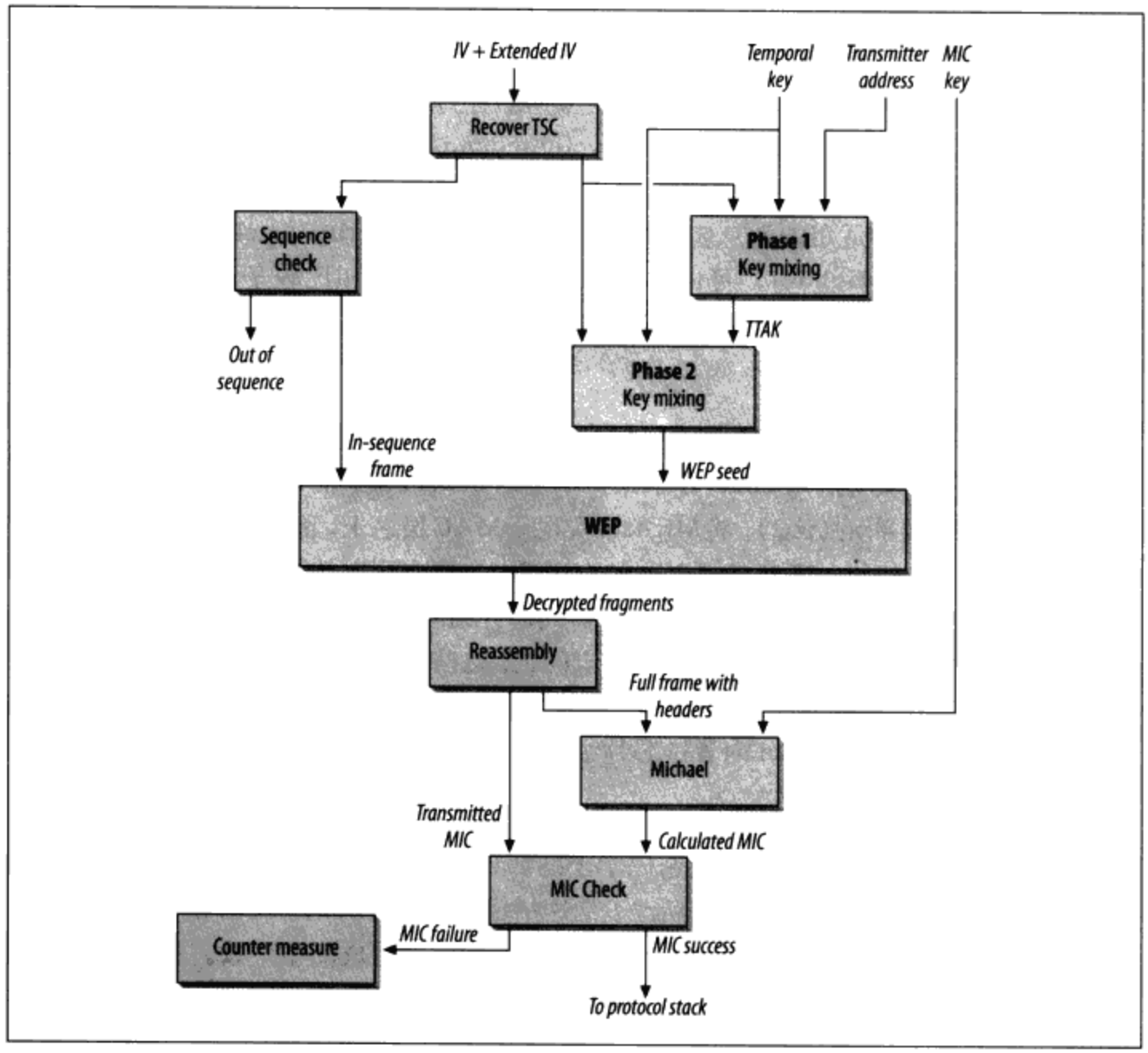


图 7-4：TKIP 的接收过程

5. 如果涉及到帧分段，那么在重组完整有效载荷之前，必须等到所有片段接收完成。不过帧分段在 802.11 中并不常用。

6. 帧重组之后，将会依帧内容计算其 Michael 值。如果所计算出来的值与封包所记载的 MIC 值相符，则会将帧传递给较上层协议并且将序列号设成帧当中所记载的序列号。如果无法通过 MIC 校验，则会触发对策。

保留 WEP 封装的理由之一是为了尽量向下兼容于现有硬件。同时，这种做法也可以避免由于 MIC 校验失败所触发的无谓动作。因无线链路噪声而损毁的帧通常无法通过 802.11 帧校验或者 WEP 完整性校验，因此在触发 MIC 失败对策之前就会被丢弃。

Michael 完整性校验

WEP的最大弱点之一在于完整性校验，而完整性校验原本是用来确保帧在经过无线媒介时不被改变。WEP 采用循环冗余校验（cyclic redundancy check，简称CRC），但经过证明，CRC 并不适合作为完整性校验之用。TKIP 的主要目标之一，即是以较稳固的密码学技术设计出一种适用的消息完整性校验（message integrity check，简称MIC）。最后出炉的算法称为 Michael，可说是多方妥协后的结果。相比较于简单的线性散列，Michael当然比较坚固，由于标准委员会希望尽量减轻实现时的负担，因而使得Michael在设计上受到严重的限制。

从架构的观点来看，Michael被插入在MAC服务层中。换言之，Michael必须处理由上层协议所传递下来的帧。Michael并不保护个别的802.11帧，而是保护经过重组并交给802.11传送的数据单元（注2）。将Michael实现于MAC层之上，而不是将它整合进MAC层的部分理由是，如此一来产品可以非常有灵活性，厂商可以选择以特殊的硬件或是设备上所运行的驱动程序来实现 Michael。旧的芯片组与 802.11 接口并未内置可以支持Michael的特殊硬件，因为当时Michael尚未问世。这些产品可以通过驱动程序或者软件升级的方式来支持 Michael。新款的设备在设计上通常已经将未来的标准考虑在内，如有必要，可以直接将 Michael 内置进芯片组，而不需要通过驱动程序的支持。

开发Michael的动机起因于先前提过的一些攻击。其中最值得注意的即是位翻转攻击与标头篡改攻击。前者是利用CRC在密码学上的弱点。身为一个线性散列算法，只要更改CRC输入的任何位，其输出也会有所改变，这早已是众所皆知的。攻击者可以改变帧中的几个位，同时变更 WEP 完整性校验值，以抵消因此所造成的不一致。在标头篡改攻击中，恶意的攻击者可能会伪造来源或发送端地址，或者更改目的地地址，试图操纵帧的流向。

请别误会，Michael 并不算是特别安全的加密协议。它的设计主要是为了那些有大量设备的用户，让他们在升级现有网络安全性的过渡期可以有点喘息的空间。换言之，它只是未来长期解决方案问世之前的短期措施。

Michael 的数据处理

Michael会对上层传给MAC的帧进行加工处理。当上层帧置于队列待传时，首要步骤即是计算消息完整性校验（MIC）值。Michael 所处理的输入项如图 7-5 a)所示。除了目

注 2：实际上，MAC 服务层与 MAC 协议层之间的区别并非必要。虽然 802.11 允许大小超过 2000 个字节的帧，不过大多数的商业实现均会限制帧的大小，以便与 Ethernet 兼容来避免分割上层的帧。

的地地址（destination address，简称DA）与源地址（source address，简称SA），Michael会在加密数据之前加入4个内容为零的字节。其中，后3个字节保留未用（Reserved），第一个字节则是留给未来标准所使用的Priority（优先级）字段。

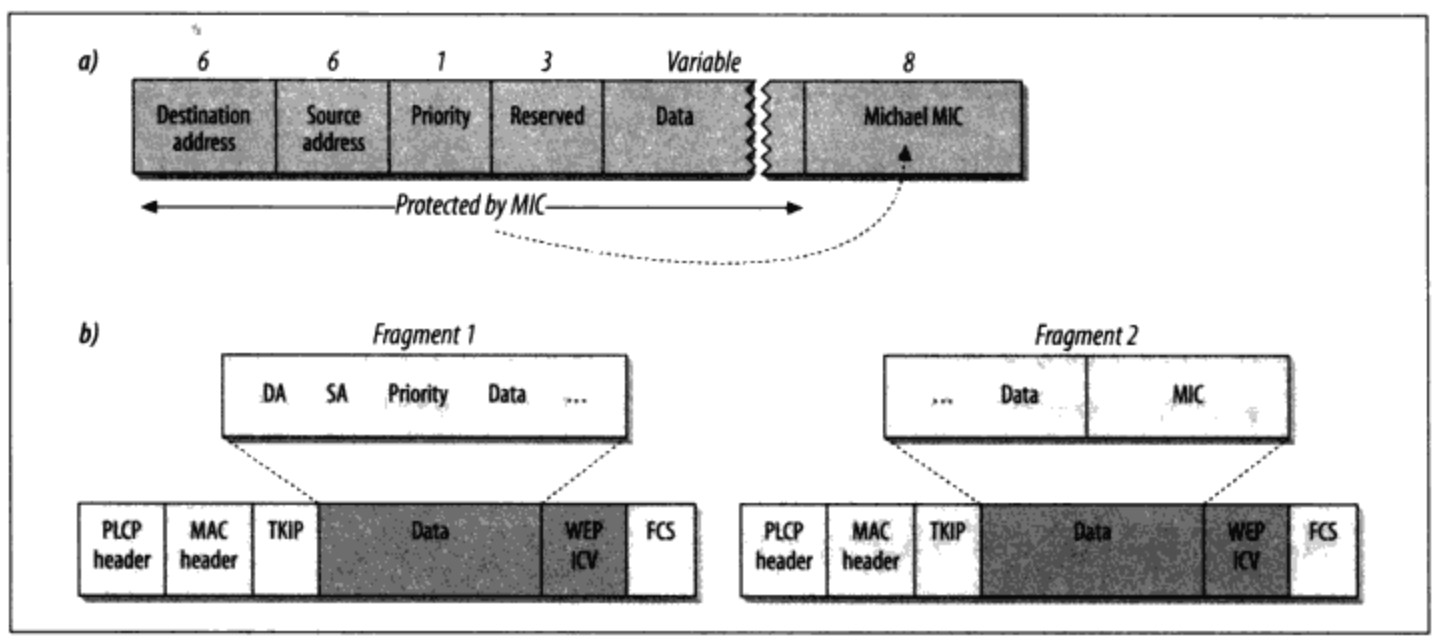


图 7-5：Michael 输入项

Michael是以32位的数据块进行操作的。如果数据并非32位的块的倍数，就会先予以补零。补零只是为了计算MIC，实际上并不会被传送出去。Michael是针对连续的32位数据块所计算出来的MIC值。

计算完成后，将MIC附于数据帧之后，一并交付给802.11来传送。如有必要，就会进行帧分段。在分段过程中，MIC值可能会散置于几个片段中，这是可以接受的。图7-5中，来自上层的数据加上MIC之后经过分段，散置于不同的帧片段中。这是完全可以接受的情况，因为在验证MIC之前这两个帧片段会经过重组。图7-5 b)说明了整个处理过程。来自图7-5 a)的输入项经过分割后分置于两个帧中，然后交付传送。每一层均有自己的MAC与PCLP标头，再由TKIP中的WEP层加以处理。

Michael 对策

Michael防范攻击的能力虽然不强，不过要能支持市面上这么多旧的硬件，看来它已经算得上是梦幻选择了。Michael无法抵挡顽强的主动攻击，因此它纳入了一些对策（*countermeasure*）用来防御。

对策的动作是在MIC校验时进行的。为了执行对策，帧必然已经通过重放攻击防护以及WEP完整性校验值的验证。要能伪造可以通过重放攻击防护与WEP完整性校验的帧并不容易，尤其是后者依赖于混合的每个帧的密钥值。

攻击者若能通过重放攻击防护与WEP完整性校验，就可以针对Michael完整性校验发动暴力攻击（brute-force tack）。为了防止Michael被暴力攻陷，Michael的对策就会停止通信，从而限制对特定密钥的主动攻击的次数。如果攻击持续进行，对策就会更新密钥，同时停止通信。

如果工作站侦测到MIC错误，就会执行下列流程：

1. 标注并登记该MIC错误。在验证MIC之前，此帧必须通过重放攻击防护以及WEP完整性校验。帧如果已送交Michael验证，事情就没那么简单。因此，只要MIC验证失败，就可能发生了安全相关问题，系统管理员必须加以探究。
2. 如果在60秒之内发生两次以上的MIC错误，对策会立即停止所有的TKIP通信60秒。暂停通信的做法可以让攻击者无法立即再次发动持续性的攻击。
3. 更新密钥。工作站删除自己所持有的主密钥副本，然后向认证者请求配发新的密钥，认证者负责产生并分配新的密钥。

虽然802.11i将Michael对策时间设为60秒，不过有些厂商允许将之设定为其他值。

什么是WPA?

Wi-Fi保护访问（Wi-Fi Protected Access，简称WPA）是由Wi-Fi联盟所推行的营销标准。Wi-Fi联盟将打造标准的细节留给其他组织（如IEEE）去费神。不过，作为一个商业组织，Wi-Fi的作用则是确保外界对该产业维持正面的观感。

当WEP的基础首度瓦解之际，IEEE便成立了一个工作组来开发经改良的安全标准。不过，打造安全的加密协议并不简单，也因此802.11i数次推延问世的时间。802.11i规范了两种新的安全协议：TKIP与CCMP。TKIP在设计上主要是为了能够和现有的硬件兼容，而CCMP本质上则是崭新的设计。因此，在CCMP就绪之前TKIP就已经完成了。

为了消除对于安全性的疑虑，Wi-Fi联盟加快脚步致力于TKIP的部署，提出名为WPA的过渡性营销标准。WPA第一版以802.11i第三版草案（2003年中期）为准，WPA第二版则是依循2004年中期最后敲定的802.11i标准。

WPA包含了802.1X身份验证与加密，分为两种：WPA Personal（相当于802.11i的pre-shared key身份验证）以及WPA Enterprise（使用认证密钥模式，从TLS entropy派生密钥）。

计数器模式及密码块链消息认证码协议（CCMP）

TKIP比WEP优秀，不过能够确定的也只有如此。既然WEP以流密码（stream cipher）为基础，后续采用类似机制的做法就无法摆脱众人对其安全性的怀疑。为了消除02.11用户的疑虑，IEEE工作组着手开发一种以高级加密标准（Advanced Encryption Standard，简称AES）的块密码（block cipher）为基础的安全协议。AES的这种密码相当灵活，可用于各种长度的密钥与数据块。为了避免困扰用户，802.11i规定AES使用128位的密钥以及128位的数据块。

802.11i应该使用何种长度的密钥向来就存在某些疑虑。AES可以使用各种长度的密钥。美国国家安全局批准AES可以对“机密”（secret）数据使用128位或更长的密钥，至于更敏感的“最高机密”（top secre）数据，则必须使用192或256位的密钥（注3）。有人据此论断128位的密钥无法提供足够的安全性。姑且不论这些密钥长度的争论依据是什么，128位的AES远比其他长度的RC4更适合用于802.11帧的加密。

这个以AES为基础的链路层安全协议称为 *Counter Mode with CBC-MAC Protocol*（计数器模式及密码块链消息认证码协议，简称CCMP）（注4）。这个名称源自底层所使用的块密码，属于RFC 3610所规范的Counter Mode with CBC-MAC（简称CCM）模式。CCM是一种“组合式”（combined）操作模式，除了以相同的密钥作为加密的方式，同时以它产生出密码学上认定为安全的完整性校验值。

2003年9月，美国国家标准与技术研究院（National Institute of Standards and Technology，简称NIST）开始了一项有关CCM的研究。2004年5月，NIST批准了CCM，这使得802.11i成为安全无线局域网在严苛应用上的基础。

CCMP的数据处理

和其他链路层加密法一样，CCMP以同样的过程支持加密与完整性保护，如图7-6所示。

注3：详见《National Policy on the Use ofthe Advanced Encryption Standard (AES) to Protection NationalSecurity Systems and National Security Information》（Committee on National Security Systems(CNSS) Policy No. 15, Fact Sheet No. 1），网址为 *http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf*。

注4：802.11i标准几经延迟的原因之一，是因为AES算法原本是基于另一种操作模式，称为AES-OCB。基于知识产权的考虑，使得最后的规范采用CCMP而排除了AES-OCB。

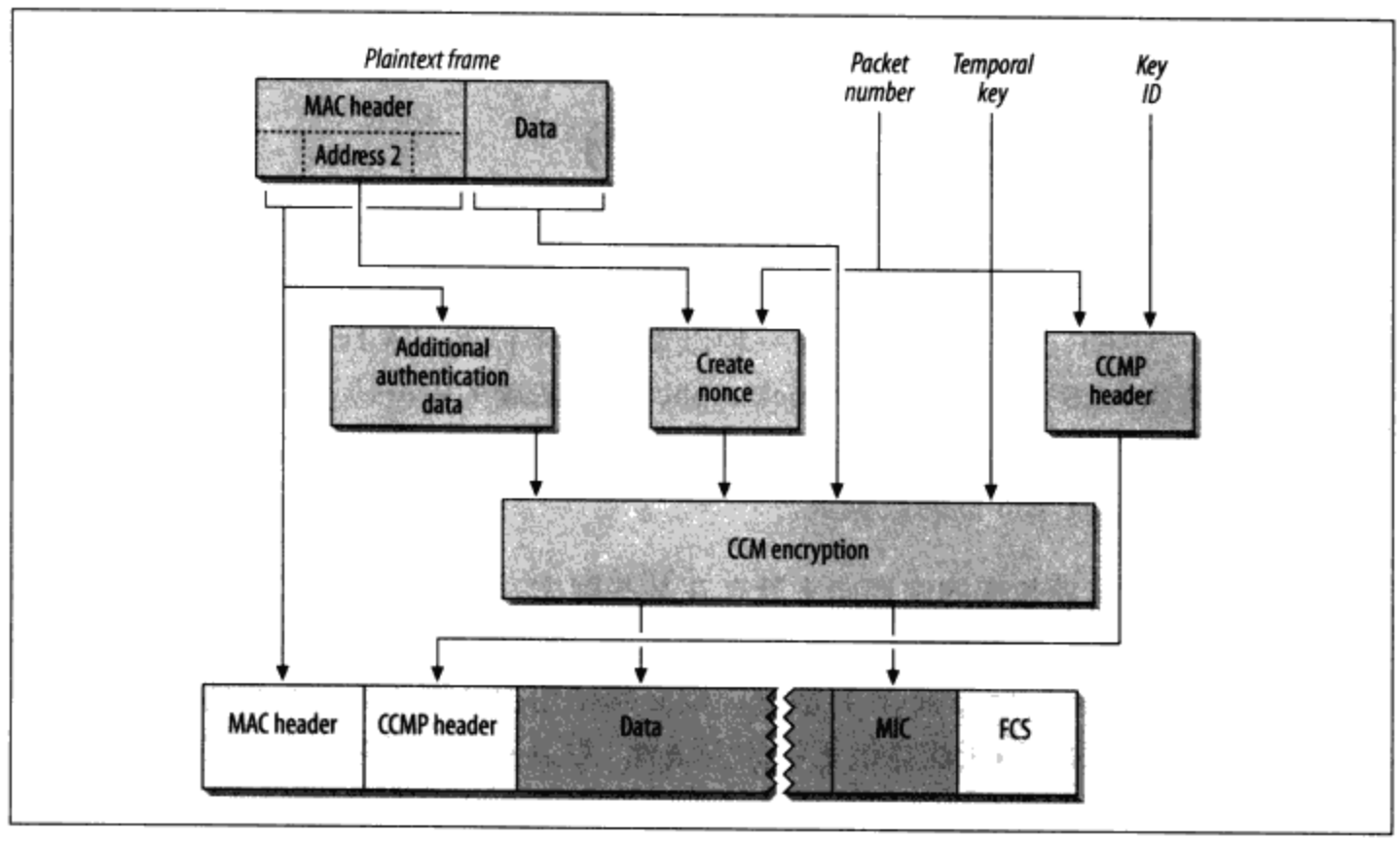


图 7-6：CCMP 帧处理 —— 加密

CCMP 以下列项目作为输入项：

- 帧。
- 临时密钥（*temporal key*），用来加密与确认帧的真实性。这个密钥可同时用来为帧加密并确认帧的真实性。
- 密钥标识符（*key identifier*）。虽然支持多组密钥，不过每个帧只会使用一个密钥。
- 封包编号（*packet number*），用来识别所传送的帧。每传一个帧，封包编号就会累加，不过对于重传帧则维持不变。即重传不会导致封包编号累加。

CCMP 的数据传输

当帧生成且交给 TKIP 待传，就会进行下列过程：

1. 将 802.11 帧置于队列中待传（queued for transmission）。其中包含帧头（frame header）以及有效载荷（payload）。和 WEP 一样，TKIP 只保护 802.11 MAC 的有效载荷，至于 802.11 帧头以及下层协议的标头则原封不动。
2. 赋予一个 48 位的封包号码（Packet Number，简称 PN）。和 TKIP 序列号一样，同一个临时密钥不会重复使用 PN。每次传送后 PN 就会累加，它同时也用来侦测重放攻击。

3. 构造附加认证数据（Additional Authentication Data，简称 AAD）字段。其中包含帧头中的一些字段，这些字段必须通过真实性的校验，但又不能经过加密，否则 802.11 协议便无法进行操作。接收端同样会使用 AAD 字段，以确认这些字段在传送过程中未被改动。AAD 字段会保护 802.11 协议版本、帧类型、分布式系统位以及片段与次序位。它也会保护来自 MAC 标头的地址字段，同时会将序列号（不是片段编号）设为零以保护顺序控制字段。它以两个（可有可无的）选项字段作为结尾：来自 MAC 标头的第四个地址字段（如果使用无分布式系统的话）以及服务质量（QoS）标头信息。

4. 下一步，构建 *CCMP nonce*（译注 1）。所谓 nonce，是指少数的数据位，用以确保加密操作确实作用于某些独特的数据。nonce 不应该在相同密钥中重复使用。在 CCMP 中，nonce 是由封包编号以及发送端地址组合而成，如此一来，不同的工作站也可以使用相同的封包编号。nonce 同时包含 QoS 会用到的优先级数据。

5. 接着，构建 CCMP 标头。它会将构成 PN（封包编号）的 6 个字节拆开，然后将 Key ID（密钥标识符）置于其中。和 WEP 一样，CCMP 中也包含 4 个密钥槽。Extended IV（扩展初始向量）位在 CCMP 中永远被设为 1，因为要能容纳 PN 这么大的字段，必定需要用到 8 个字节的标头。CCMP 标头如图 7-7 所示。

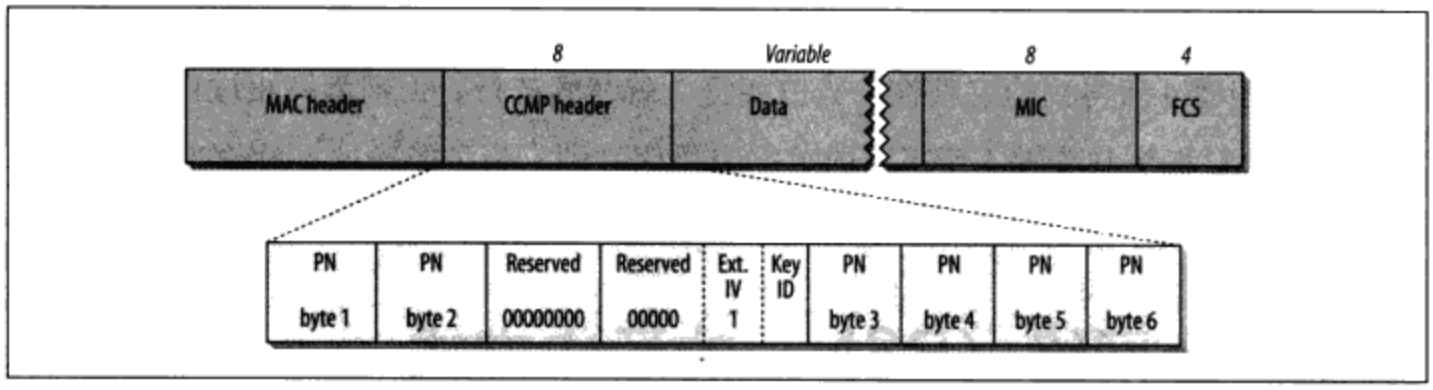


图 7-7：CCMP 封装格式

6. 至此，CCM 加密引擎所需要的输入项均已备齐。它以 128 位的临时密钥、步骤 4 所产生的 nonce、步骤 3 所产生的附加认证数据（AAD）以及帧主体作为输入项。所有这些数据是以长度为 8 个字节的 MIC（消息完整性检查码）来确保其真实性，帧主体与 MIC 也经过加密。整个加密过程如图 7-6 所示。

7. 以原始的 MAC 标头、CCMP 标头与步骤 6 所产生的加密数据来组成待传的加密帧。帧产生之后就会交付无线接口传送，如图 7-7 所示。

译注 1：在密码学中，nonce 是指用过即丢、抛弃式的随机值或随机数。

受到CCMP保护的帧的封装过程相当直接，如图7-7所示。在MAC标头之后，CCMP标头记录了PN（封包编号）与Key ID（密钥标识符）。上层协议的帧及其MIC（消息完整性检查码）加密后置于FCS（帧校验码）之前。

CCMP的接收

当CCMP接收到一个帧，就会逆转整个加密与传送过程。由于没有兼容性的包袱，不必用到WEP引擎，CCMP的解密过程就是图7-6的直接逆转：

1. 一旦无线接口接收到帧，如果通过帧校验序列（frame check sequence）确定它未曾受损，就会将其交付给CCMP进行验证。
2. 从所接收到的帧还原出AAD（附加认证数据）。其中只包含帧头而且未经过加密。
3. 从帧还原出CCMP nonce。其中包含封包编号、发送端地址以及QoS字段的内容，这三者均可自未加密的帧头中取得。
4. 接收端解读密文。此时需要临时密钥、步骤3所还原的nonce、步骤2所得到的认证数据，当然还有加密过的帧主体。此过程完成后，接收端就会得到一份经解密后的帧的副本以及经解密后的完整性校验码。
5. 完整性校验是针对明文数据与附加认证数据进行计算的。如果计算出的完整性校验值与步骤4所得到的完整性校验值相符，就继续进行；否则就终止过程。
6. 由MAC标头与步骤4所还原的数据组成明文帧。为了能通过重放攻击探测校验，其封包编号必须大于或等于最近接收到的通过完整性校验程序的封包编号。

强健安全网络（RSN）的运作方式

除了TKIP与CCMP，802.11i还定义了一组过程，它构建了称为强健安全网络（Robust Security Network，简称RSN）的标准。这些操作主要定义密钥的产生与分配方式。

802.1i密钥层次结构

链路层加密协议使用了两种密钥。成对密钥（pairwise key）用来保护工作站与AP之间往来的数据。组密钥（group key）用来保护AP至所关联工作站之间的广播或组播数据。成对密钥产生自前一章所讨论的身份验证信息；组密钥则是由接入点动态产生然后分配给各个工作站的。

成对密钥层次结构

TKIP与CCMP均使用单一主密钥来产生帧保护操作所需要的其他密钥。利用派生密钥，工作站可以更新加密密钥，而无需重新执行整个认证过程。主密钥本身扮演着秘密根源（root secret）的角色，必须小心保护，因为所有密钥材料（keying material）都衍生于此。密钥分级（key hierarchy）的目的部分是为了派生用来保护临时密钥的传送的密钥。

密钥生成从主密钥开始。在成对密钥体系中，主密钥称为成对主密钥（pairwise master key，简称PMK），长度为256位，如图7-8所示。PMK必然有其来源，在WPA-PSK中，便是使用成对主密钥。在使用认证服务器的情况下，主密钥由RADIUS服务器计算而得，然后以Microsoft Point-to-Point Encryption（简称MPPE）这个厂商特有的RADIUS属性送给接入点。

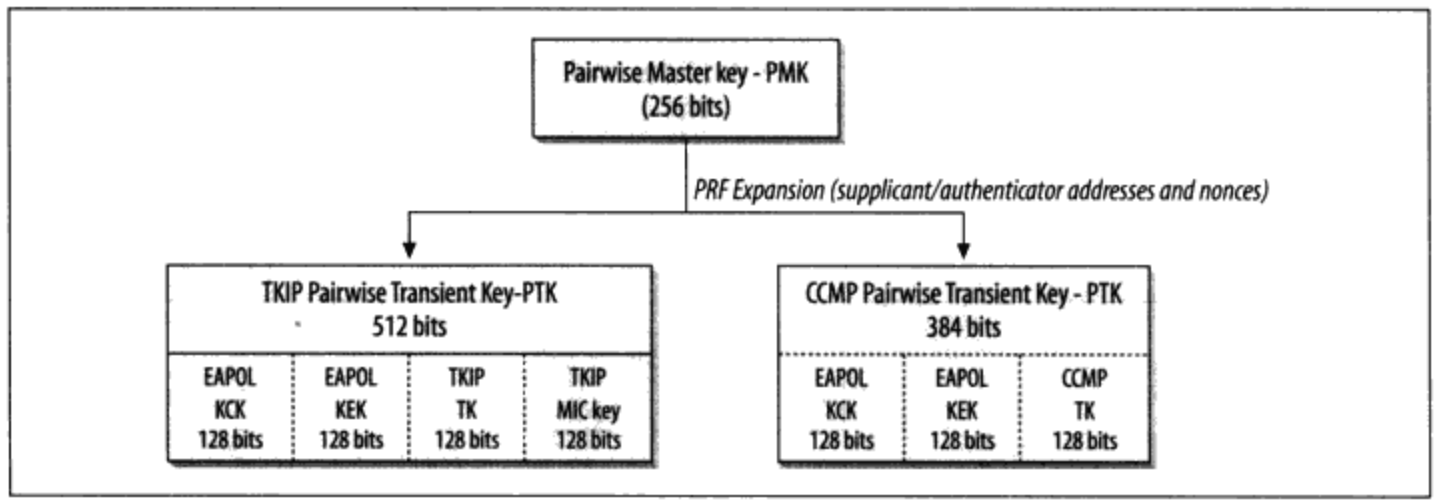


图 7-8：成对密钥的层次结构

为了得到本章之前所提到的临时密钥，必须使用预先定义好的伪随机函数（pseudorandom function）（注5）来展开PMK。为了使数据更为随机，此展开过程是根据预主密钥（pre-master key）、申请者与认证者（supplicant and authenticator）的MAC地址以及两个作为四次密钥交换握手（four-way key exchange handshake）的随机nonce值。

TKIP与CCMP均会使用伪随机函数将256位的PMK展开为成对临时密钥（pairwise transient key，简称PTK）。在TKIP与CCMP体系中，临时密钥的两组128位块在分配过程中被用来保护临时密钥。

这两种密钥体系均始于两个EAPOL密钥，通过前一章所提到的EAPOL-Key消息来保护密钥材料的传送安全。其中使用了两个128位的密钥。第一个是EAPOL密钥确认密钥

注5：许多加密协议会利用伪随机函数，将随机数种子展开为较多的随机数据。TLS或许是最广为人知的例子。

(EAPOL Key Confirmation Key，简称KCK)，用来计算密钥生成消息(keying message)的完整性校验值。第二个是EAPOL密钥加密密钥（EAPOL Key Encryption Key，简称KEK)，用来加密密钥生成消息。两者在四次握手一节均会加以讨论。

TKIP的临时密钥总长度为512位，有附加的256位，其中一半作为TKIP数据处理时所使用的128位临时密钥，一半用于Michael完整性校验。TKIP之所以需要两个附加的密钥，是由于它使用了传统的加密与认证机制，因而会严格区分加密与认证。CCMP的临时密钥只有384位，因为它只使用一个128位的密钥来进行认证与加密。

组密钥的层次结构

链路层安全协议为广播与组播使用了另一组不同的密钥。已关联的每个工作站均拥有不同的预主密钥（pre-master key)，因此无法从认证过程中推衍出组播所需要的密钥。事实上，认证者拥有组主密钥（group master key，简称GMK）以作为临时密钥的基础。通过伪随机函数，组主密钥会被展开成组密钥层次结构，如图7-9所示。在此并未产生密钥加密（key encryption）或密钥确认（key confirmation）密钥，因为密钥交换（key exchange）是以成对EAPOL密钥（pairwise EAPOL key）来分配密钥的。

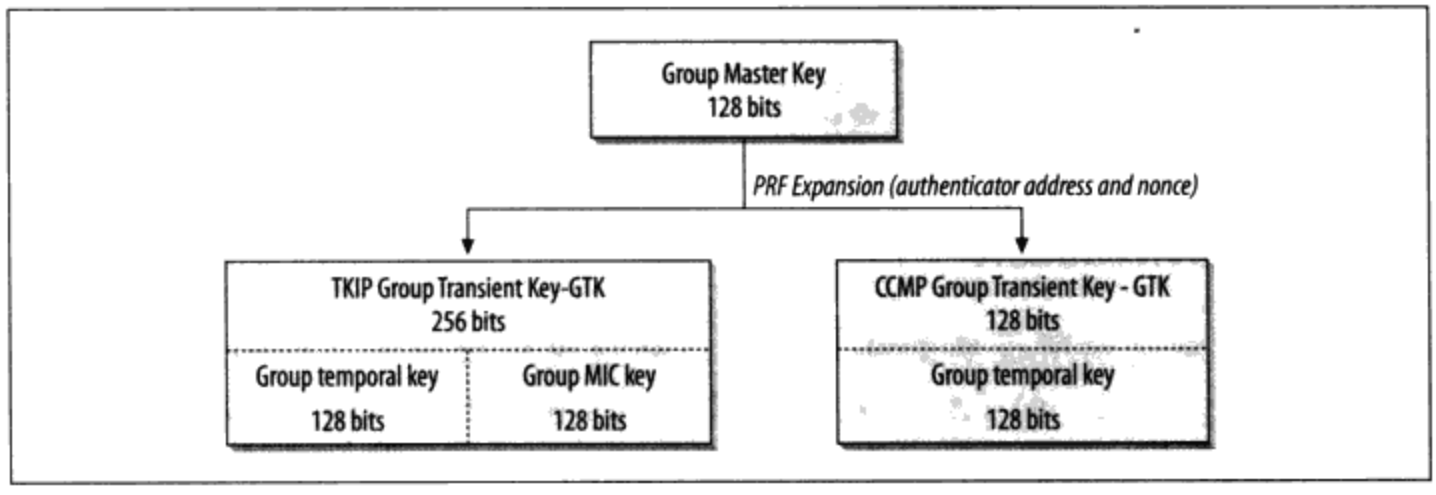


图7-9：组密钥的层次结构

当工作站离开网络，不论是使用完毕或被踢出网络，网络系统即可更新组密钥。在TKIP中，对策也会导致系统重新生成组密钥。

802.11i密钥的来源与分配

802.11i规范了一种派生密钥的机制，而不仅是采用主密钥并以它作为加密协议的输入项。为了防范重放攻击，密钥的交换使用了随机数并且需要经过握手。成对密钥与组密钥分别通过各自的握手加以更新，如图7-10所示。

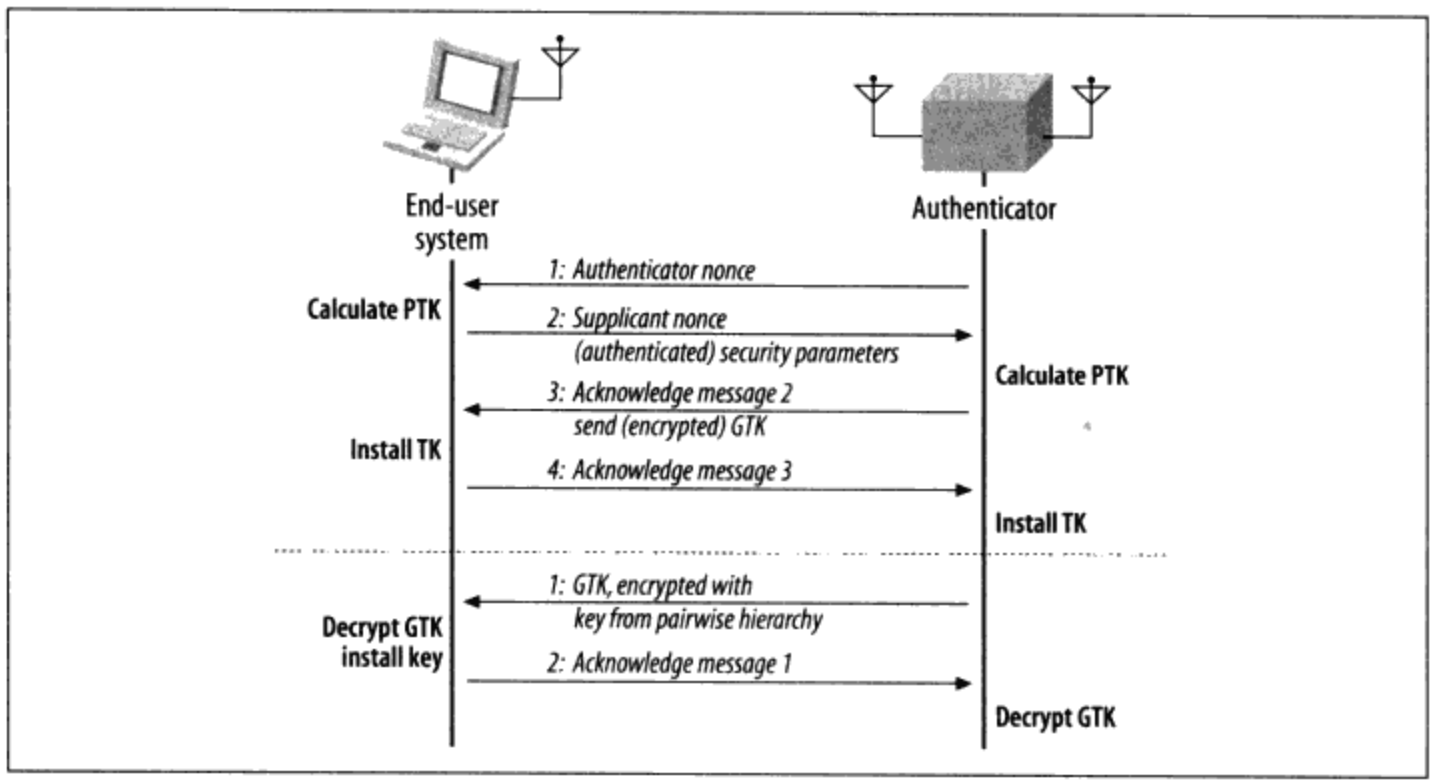


图 7-10：密钥交换握手

更新成对密钥：四次握手

成对（pairwise）或单播（unicast）密钥是通过所谓的四次握手（four-way handshake）加以分配，如图 7-10 所示。申请者（supplicant）与认证者（authenticator）均持有一个共享的成对主密钥。四次握手交换用以产生临时密钥的参数以及确认双方均已准备就绪，可以开始进行加密传送。依序传送的消息由下一个消息来代表确认。

1. 认证者将 *nonce* 传给申请者。nonce 是防范重放攻击的随机值。消息本身并未经过确认，但并没有被篡改的危险。如果消息被人更改，握手就会失败并重新执行。

   至此，申请者就可以将成对主密钥展开成完整的成对密钥层次结构。展开的过程中，需要用到申请者与认证者的 MAC 地址、成对主密钥以及两个 nonce。

2. 申请者所送出的消息中包含申请者的nonce以及初次与网络关联时所取得的安全参数副本。整个消息是经过以EAPOL密钥确认密钥计算而来的完整性校验值验证的。

   认证者接收到消息，取出申请者的nonce，依此衍生出完整的密钥层次结构。此密钥层次结构中包含用来“签署”（sign）消息的密钥。如果认证者无法验证此消息，整个握手即告失败。

3. 此时握手双方的密钥均已就绪，但仍需要确认。认证者会将一个消息传给申请者，此消息代表将被加入的成对密钥的序列号。它同时包含了目前的组临时密钥（group transient key，简称 GTK），以便后续能够更新组密钥。GTK 以 EAPOL 密钥加密密钥来加密，整个消息以密钥确认密钥来认证。

4. 申请者最后会送出确认消息给认证者，告诉认证者已经接收到密钥生成消息，可以开始使用这些密钥。此消息经过密钥确认密钥的认证。

更新组密钥：组密钥握手

组密钥握手（group key handshake）显然比四次握手简单，部分是由于它利用了四次握手得出的部分结果。由于组临时密钥经过成对密钥层次结构中的密钥加密密钥的加密，因此进行组密钥握手之前，四次握手必须已经成功完成。它包含了两个步骤：

1. 认证者送出组临时密钥（GTK）并以成对密钥层次结构中的密钥加密密钥进行加密。此消息也经过密钥确认密钥计算出来的校验值的认证。
2. 申请者送出确认消息，告诉认证者开始使用新的组密钥。此消息也是使用密钥确认密钥进行认证的。

虽然组密钥握手更新的是许多工作站所共享的密钥，但是使用密钥加密密钥来保护数据，意味着此握手过程其实是成对的。当组密钥更新后，每个工作站都必须再进行一次组密钥交换。

虽然组密钥更新一般是由认证者所主导，但是工作站也可以主动送出确认消息来要求更新组密钥。

混合加密类型

为了支持不同加密协议的替换以及适应只支持WEP加密功能的老设备，802.11i定义了一种可信赖的加密协议体系。使用40位密钥的WEP是最弱的加密协议，之后分别是使用104位密钥的WEP、TKIP与CCMP。

作为网络的初始关联的一部分，各个工作站可以协商使用何种加密协议进行单播与组播传送。唯一的限制是组密钥必须使用相同强度或较弱的加密协议。接入点在组密钥上采用了“最小公分母”（lowest common denominator）的做法。在网络上，如果能力最低的工作站只具备动态WEP的能力，就会以动态WEP作为组密钥。不过，其他工作站可以使用较强的单播保护机制。有些接入点支持关联策略控制，用来设定可接受的最低加密强度，以及防止工作站以强度低于网管人员所要求的协议与网络进行关联。

802.11i标准允许混用几乎所有的加密方式，但使用CCMP传送组帧（group frame）的工作站只能以CCMP进行单播帧（unicast frame）的传送，这是唯一的例外。不过，有些驱动程序并不支持所有可行模式。最值得注意的是，驱动程序通常不支持下述的混搭方式，即单播数据（unicast data）使用CCMP以及组密钥（group key）使用较旧的基于RC4的帧加密。

密钥缓存

成对主密钥（PMK）算是802.11i的安全防护基础。如果成对主密钥是通过802.1X交换过程生成的，那么代价其实不斐。大部分的EAP方式都需要用到好几个消息，每个步骤也都需要大量的计算。802.1X认证过程需要花费几秒的时间，此时用户并无法收发数据。位于两个接入点边界的工作站特别容易受到影响，如果它的无线接口因为两个接入点的信号强度相当而在两边来回切换的话。

PMK缓存的动机在于减轻认证负担，如图7-11所示。与接入点进行关联时，工作站会先引用现有关联的成对主密钥安全关联标识符（PMKSA），而非每次都进行完整的802.1X交换过程。如果接入点中存在关联，它就会接受关联且立即进行四次握手。在四次握手过程中，申请者与认证者将会证明各自所缓存的PMK。

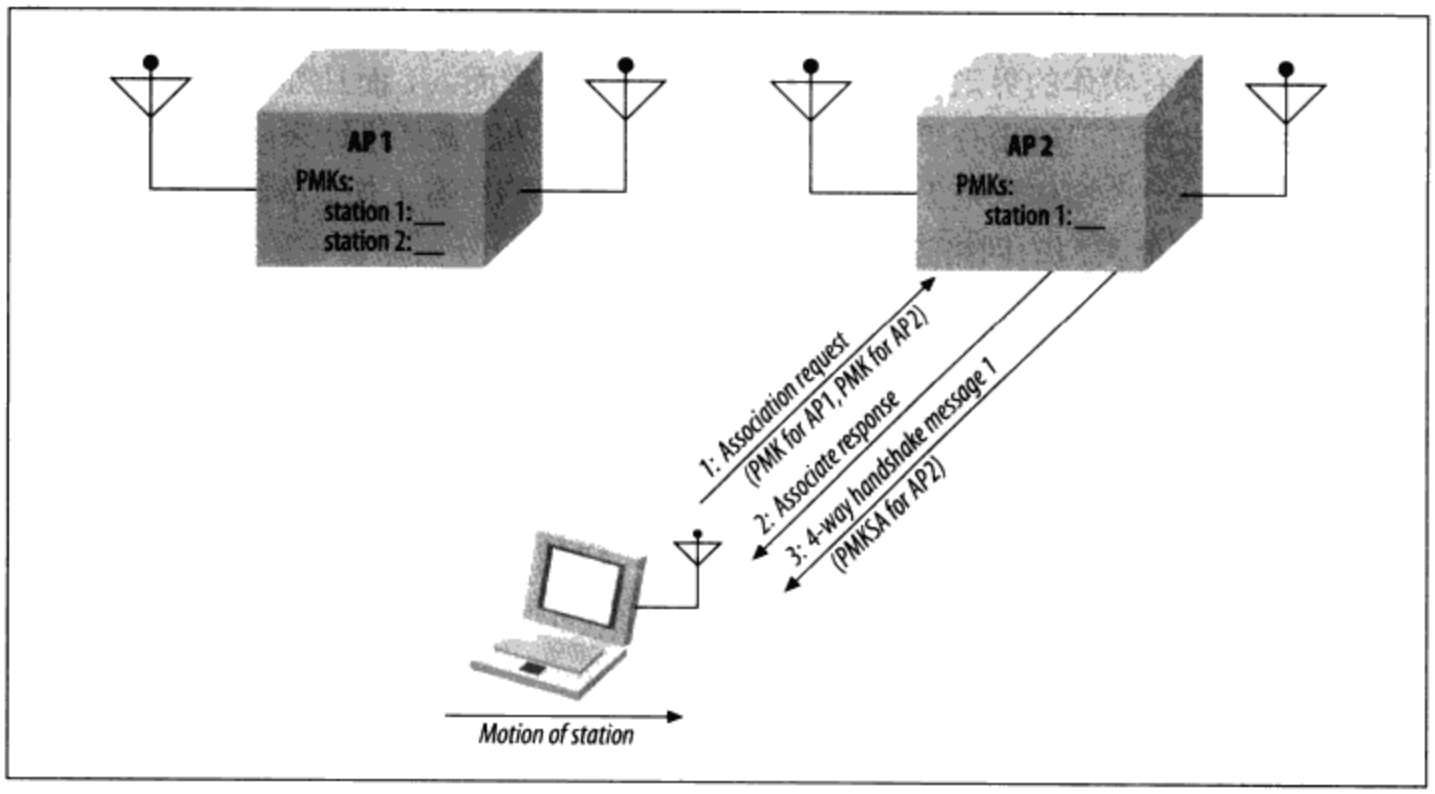


图 7-11：PMK 缓存

没有缓存主密钥的工作站必须进行完整的802.1X认证，这样才能产生主密钥。事先认证（preauthentication）的动机之一，即是在切换（handoff）发生之前，在接入点中产生主密钥备用。事先认证将于下一章讨论。

第八章

管理操作

虽然具备不受有线网络束缚的优势，但无线网络也不是没有任何问题。无线媒介并不稳定，何况既然没有实体的界限，未经授权的用户便可乘虚而入，而且如果所使用的设备以电池供电，电源管理就十分重要。802.11协议的管理功能就是设计来降低这些问题的影响。基本上，管理操作就是无线网络设备在幕后进行的所有工作。借此，无线网络连接感觉上就跟其他类型的网络连接没什么两样。

802.11管理操作是由客户端设备与网络基础设施彼此分工合作。遗憾的是，绝大部分的协议操作均由客户端设备所掌握，但这些设备之间或许差异甚大。有些设备驱动程序允许用户自定义本章所探讨的管理功能。不过应该注意的是，设备驱动程序的功能因产品而异，而且无线网络的市场现况是，有些厂商试图生产功能最丰富的产品，有些则是针对低成本市场致力于生产最简单的产品。要知道可以使用哪些功能，唯一的方法就是了解协议本身具备哪些功能。如此一来，不论面对何种硬件设备，你都可以应付自如。

管理结构

在概念上，802.11管理结构由三个组件组成：MAC层管理实体（MAC layer management entity，简称MLME）、物理层管理实体（physical-layer management entity，简称PLME）以及系统管理实体（system management entity，简称SME）。不同管理实体之间以及其与802.11相关部分之间的关系如图8-1所示。

802.11并未正式规范SME。SME是用户和设备驱动程序跟802.11网络接口交互和取得状态信息的方式。MAC与PHY协议层皆可访问管理信息库（management information base，简称MIB）。MIB包含了许多对象，有些对象可供查询状态信息，有些则可以引发特定的动作。

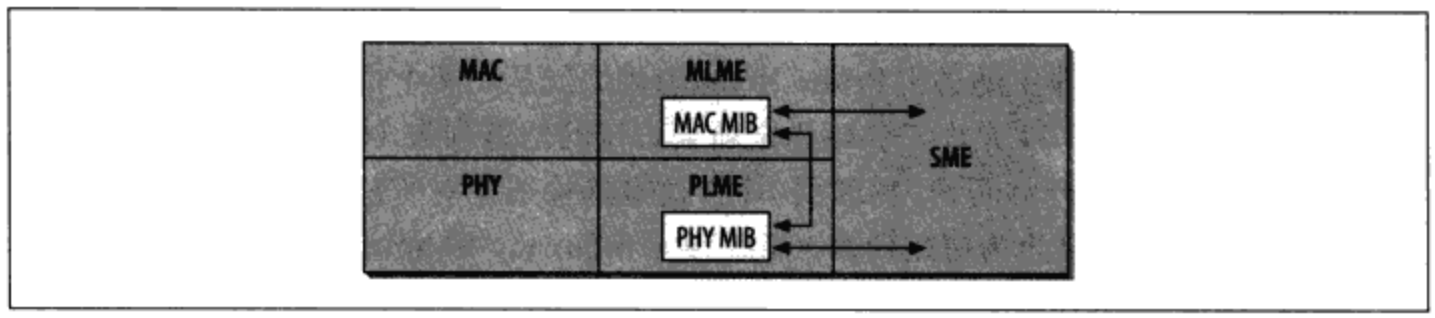


图 8-1：管理实体与 802.11 规范之间的关系

在这些管理组件之间定义了三个接口。SME 可通过 MLME 和 PLME 服务接口来更改 MAC 与 PHY MIB。此外，MAC 有所改变，相对地 PHY 也要有所变动，所以在 MLME 与 PLME 之间必须存在一层接口，让 MAC 可以变更 PHY。

扫描

使用任何网络之前，首先必须找出网络的存在。使用有线网络时要找出网络的存在并不难，只要循着网线或者找到墙上的插座即可。在无线领域中，工作站在加入任何兼容网络之前必须先经过一番识别的工作。在所在区域识别现有网络的过程称为扫描（*scanning*）。

扫描过程中会用到几个参数。这些参数可由用户来指定，有些实现产品则是在驱动程序中为这些参数提供默认值。

BSSType（independent、infrastructure 或 both）

扫描时可以指定所要搜寻的网络属于 independent ad hoc、infrastructure 或同时搜寻两者。

BSSID（individual 或 broadcast）

工作站可以针对所要加入的特定网络（individual）进行扫描，或者扫描允许该工作站加入的所有网络（broadcast）。在移动时将 BSSID 设为 broadcast 不失为一个好主意，因为扫描的结果会将该地区所有的 BSS 涵盖在内。

SSID（"network name"）

SSID 是用来指定某个扩展服务集（extended service set）的位字符串。大部分的产品会将 SSID 视为网络名称（network name），因为此位字符串通常会被设定为人们易于识别的字符串。工作站若打算找出所有网络，应该将之设定为 broadcast SSID。

ScanType（active 或 passive）

主动（active）扫描会主动传送 Probe Request 帧以识别该区有哪些网络存在。被动（passive）扫描则是被动聆听 Beacon 帧以节省电池的电力。

ChannelList

进行扫描时，若非主动送出Probe Request帧，就是在某个信道被动聆听当前有哪些网络存在。802.11允许工作站指定所要尝试的信道列表（ChannelList）。设定信道列表的方式因产品而异。物理层不同，信道的构造也有所差异。直接序列（direct-sequence）产品以此为信道列表，而跳频（frequency-hopping）产品则以此为跳频模式（hop pattern）。

ProbeDelay

主动扫描探测某个信道时，为了避免工作站一直等不到Probe Response帧而设定的延时定时器，以微秒为单位。用来防止某个闲置的信道让整个过程停止。

MinChannelTime 与 MaxChannelTime

以TU（时间单位）来指定这两个值，意指扫描每个特定信道时所使用的最小与最大的时间量。

被动扫描

被动扫描（passive scanning）可以节省电池的电力，因为不需要传送任何信号。在被动扫描中，工作站会在信道列表（channel list）所列的各个信道之间不断切换并静候Beacon帧的到来。所收到的任何帧都会被暂存起来，以便取出传送这些帧的BSS的相关数据。

在被动扫描的过程中，工作站会在信道间不断切换并且会记录来自所收到的任何Beacon的信息。Beacon在设计上是为了让工作站知道加入某个基本服务集（basic service set，简称BSS）所需要的参数以便进行通信。在图8-2中，通过聆听来自前三个接入点的Beacon帧，移动式工作站以被动扫描找出该区所有的BSS。如果该工作站并未收到来自第四个接入点的Beacon，就会汇报目前只发现三个BSS。

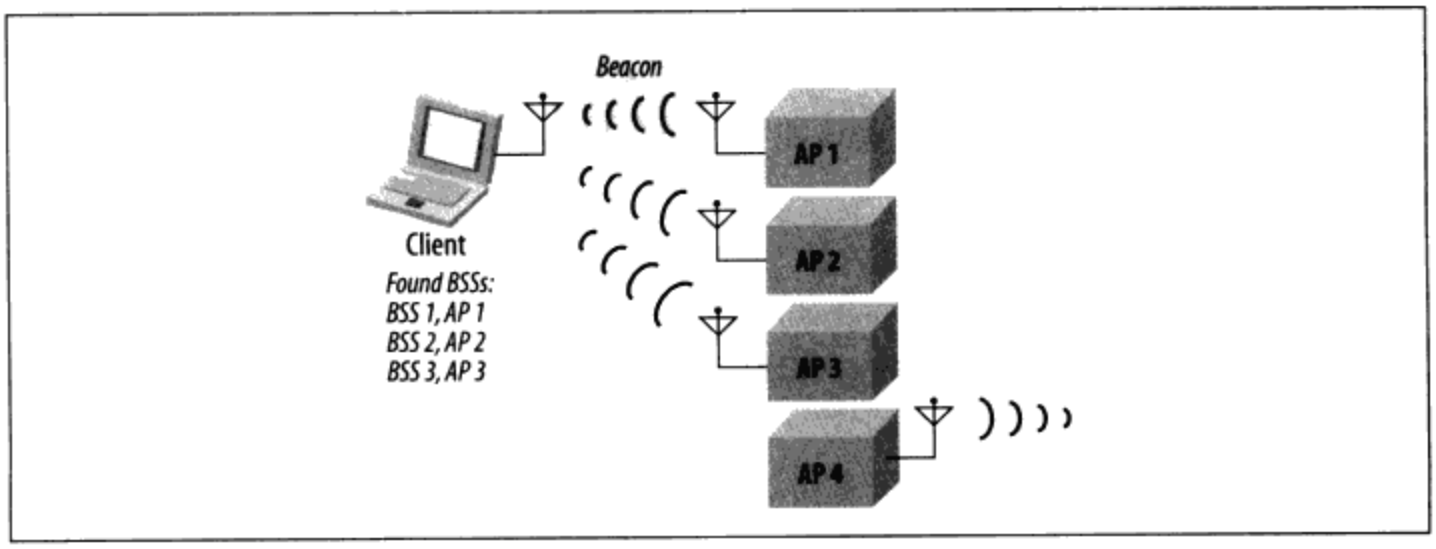


图8-2：被动扫描

主动扫描

在主动扫描（active scanning）中，工作站扮演着比较积极的角色。在每个信道上，工作站都会发出 Probe Request 帧来请求某个特定网络予以响应。主动扫描是主动试图寻找网络，而不是听候网络声明本身的存在。使用主动扫描的工作站将会以如下的过程扫描信道列表所列的每个信道：

1. 跳至某个信道，然后等候来帧指示（indication of an incoming frame）或者等到 ProbeDelay 定时器超时。如果在这个信道收得到帧，就证明该信道有人使用，因此可以加以探测。此定时器可用来防止某个闲置信道让整个过程停止，因为工作站不会一直等候帧的到来。
2. 利用基本的 DCF 访问过程取得媒介使用权，然后送出一个 Probe Request 帧。
3. 至少等候一段最短的信道时间（即 MinChannelTime）。
   a. 如果媒介并不忙碌，表示没有网络存在，因此可以跳至下个信道。
   b. 如果在 MinChannelTime 这段期间媒介非常忙碌，就继续等候一段时间，直到最长的信道时间（即MaxChannelTime）超时，然后处理任何的Probe Response 帧。

当网络收到搜寻其所属的扩展服务集的 Probe Request（探查请求），就会发出 Probe Response（探查响应）帧。为了在舞会中找到朋友，各位或许会绕着舞池大声叫喊对方的名字（虽然这并不礼貌，不过如果真想找到朋友，大概没有其他选择）。如果对方听见了，她就会出声响应，至于其他人根本就不会理你（希望如此）。Probe Request 帧的作用与此相似，不过在 Probe Request 帧中可以使用 broadcast SSID，如此一来，该区所有的 802.11 网络都会以 Probe Response 加以响应。（这就好比在一场舞会中大喊“失火了”，可以确定每个人都会响应！）

每个 BSS 中必须至少有一个工作站负责响应 Probe Request。传送上一个 Beacon 帧的工作站也必须负责传送必要的Probe Response 帧。在 infrastructure（基础结构型）网络里，是由接入点负责传送 Beacon 帧，因此它也必须负责响应以 Probe Request 在该区搜寻网络的工作站。在 IBSS（独立基本服务集）中，工作站彼此轮流负责传送 Beacon 帧，因此负责传送 Probe Response 的工作站会经常改变。Probe Response 属于单播（unicast）管理帧，因此必须符合 MAC 的肯定确认（positive acknowledgment）规范。

单一 Probe Request 导致多个 Probe Response 被传送的情况十分常见。扫描过程的目的在于找出工作站可以加入的所有基本服务区域，因此一个 broadcast（广播式）Probe Request 会收到范围内所有接入点的响应。各独立型 BSS 之间如果互相重叠，也会予以响应。

图 8-3 所示的是 Probe 帧之间的关系以及扫描时可以设定的各种时间间隔。

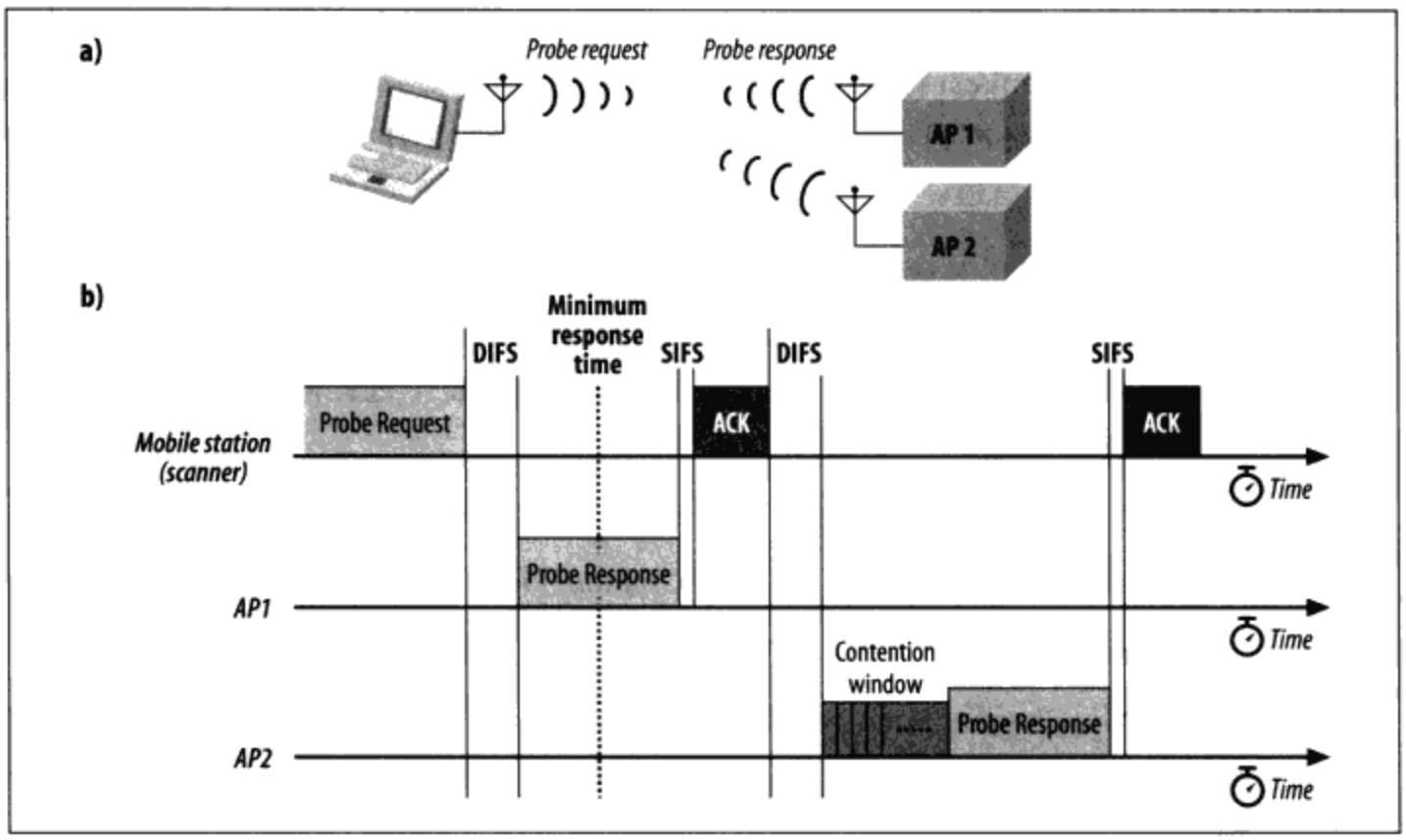


图 8-3：主动扫描过程以及媒介访问

在图 8-3 a)中，某个移动式工作站发出 probe request（探查请求）信息，而有两个接入点加以响应。在媒介（medium）中进行的动作如图 8-3 b)所示。在取得媒介使用权后，进行主动扫描的工作站会送出Probe Request。接着有两个接入点同时以Probe Response（探查响应）加以响应，其中包含它们的网络参数。值得注意的是，第二个Probe Response受限于分布式协调功能（distributed coordination function）的规则，在传送之前必须等待竞争窗口（congestion window）结束。第一个响应在最短响应时间（minimum response time）结束之前即已送出，因此工作站会继续等候至最长响应时间（maximum response time）结束，才会校验所收到的信息。在网络林立的区域，或许必须调整每个信道的最长等候时间（maximum channel time），才有办法处理区域内每个接入点所发出的响应信息。

扫描报告

扫描结束后会产生一份扫描报告。这份报告列出了该次扫描所发现的所有BSS及其相关参数。进行扫描的工作站可以利用这份完整的参数列表来加入（join）其所发现的任何网络。除了 BSSID、SSID 以及 BSSType，这些参数还包括（注 1）：

注 1： 实际输出哪些项目因软件而异。

Beacon interval（信标间隔；整数值）

每个BSS均可在自己的指定间隔（以TU为单位）传送Beacon帧。

DTIM period（DTIM周期；整数值）

DTIM帧属于省电（power-saving）机制的一部分。

Timing parameter（定时参数）

有两个字段可让工作站的定时器与BSS所使用的定时器同步。Timestamp字段代表扫描工作站所收到的定时值，另一个字段则是让工作站能够匹配定时信息以便加入特定BSS的偏移量（offset）。

PHY参数、CF参数以及IBSS参数

这三个网络参数均有各自的参数集，相关细节在第四章已经探讨过了。信道信息（channel information）包含在物理层参数（physical-layer parameters）中。

BSSBasicRateSet

基本速率集（basic rate set）是打算加入某个网络时工作站必须支持的数据传输速率列表。工作站必须能够以基本速率集中所列的任何速率接收数据。基本速率集是由管理帧的Supported Rates信息元素的必要速率组成，细节参见第四章。

加入网络

扫描结果汇总之后，工作站即可选择其中一个BSS加入。加入网络（joining）是建立关联的前置操作，相当于拿起武器。不过此时还不能访问网络。访问网络之前必须经过身份验证以及形成关联。

选择加入哪个BSS和实现有关，有时甚至需要用户的介入。属于相同ESS的BSS被允许采用其本身所决定的方式。通常用来决定加入哪个网络的判断标准是功率电平（power level）与信号强度（signal strength）。外人无法判断一个工作站在何时加入某个网络，因为加入过程纯属节点内部的操作，其中牵涉到调整内部参数以配合所选BSS要求的参数。其中最重要的一项任务就是使移动工作站与网络之间定时信息的同步，此过程在本章的“定时器同步”一节会有更详尽的探讨。

此外，工作站还得匹配PHY参数，此参数用以保证该BSS的任何传送操作均会在正确的信道中运作（定时器同步也可以保证跳频工作站能够在正确的时间切换信道）。使用BSSID可以确保目前与正确的工作站进行传送，同时忽略其他BSS的工作站（注2）。扫

注2：在技术上，只有在工作站遵循接收帧的过滤规则时，这种说法才算成立。试图破坏网络安全的恶意攻击者可以轻易违反这些规则而截取封包，大多数现有产品并未正确实现这些过滤规则。

名称的内涵是什么？（或者，隐藏式SSID的安全性谬误）

SSID是相当重要的扫描参数。工作站进行扫描时会搜寻特定的SSID或者列出可用的SSID供用户挑选。作为网络独一无二的识别名称，SSID通常带有某些安全性的神秘色彩，虽然实际上它并不拥有这些特性。

802.11刚问世时，SSID是通过Beacon帧公开进行广播的，只需要有一个802.11接口对准正确的无线电信道就可以收听到。进入802.11的石器时代以后，有家厂商开始将SSID视为具有安全价值的标志。只要在他们的设备上启用“close network”（封闭式网络）选项，就不会将SSID置于Beacon帧中，借此“保护”网络免遭攻击。为了进一步“保护”SSID不受窥视，这类封闭式网络的接入点对于Probe Request信息也不会响应广播型SSID。

封闭式网络也阻绝了被动扫描，因为不再能够轻易搜集得到SSID。不过为了避免封闭式网络完全拒绝工作站，接入点必须响应那些指定了正确SSID的Probe Request。管理帧并未加密，而且SSID的内容就明确写在Probe Request帧里。严格来讲，封闭式网络或许提供了些微的安全性，因为SSID只有在工作站搜寻网络时才会曝光，而不是每秒钟出现在Beacon帧中好几次。

隐藏SSID可能导致802.11管理上的问题。并非所有802.11接口与驱动程序都能够处理隐藏式SSID。隐藏SSID并不符合标准规范，而且可能导致其他问题，更无法提供真正的安全性。为了顾及互用性，不妨让SSID出现在Beacon帧中，如有必要，应该采用真正的安全解决方案，例如802.1X。

描结果还包含Capability信息，可确认是否使用WEP以及任何的高速功能。工作站必须采用所选BSS的Beacon间隔以及DTIM周期，虽然就能否进行通信而言，这些参数不是那么重要。

身份验证

对所有的恶意侵犯而言，任何无线网络媒介都是开放的，因为攻击者实际上可以隐身于网络媒介之中。只要置身其中，要取得立足之地就十分容易。请各位准备好进入认证的迷离境界（twilight zone）。802.11提供了多种形式的“身份验证”，对真正的安全专家而言，有些根本不值一哂。

提到身份验证，大多数网管人员认为只有强身份验证（strong authentication）才算真正

的身份验证，如果不是以密码学（cryptography）为基础就不能算。只要搭配正确的EAP认证方式，802.1X 身份验证就相当坚固，不过系统必须在关联前先进行低级的 802.11“身份验证”，才可以交换 802.1X 信息。

802.11“身份验证”

802.11 要求工作站在传送帧之前必须确认身份。起初，只要工作站打算连接到网络，就必须进行 802.11“身份验证”。不过应该强调的是，这些并无法提供真正有意义的网络安全。因为不但没有传递或验证任何加密密钥（cryptographic secret），也并未进行相互认证过程。比较正确的看法是将802.11的低级身份验证视为工作站连接到网络时的握手过程的起点，以及一种对网络表明身份的方式。

目前，802.11身份验证有点像是单行道。打算加入某个网络的工作站必须通过身份验证，然而网络方面并无义务对工作站证明自己的身份。802.11的设计者或许认为接入点属于网络基础结构的一部分，因此具备某种特权。

开放系统身份验证

开放系统身份验证（open-system authentication）是802.11 要求必备的唯一方法。称之为身份验证有点曲解这个名词的意义。在开放系统身份验证中，接入点并未验证移动式工作站的真实身份，只是作作表面文章。（想象一下，类似的身份验证应用在银行提款机上是什么样！）网络安全必须建立在现有网络连接的基础之上。开放系统身份验证的过程用到两个帧，如图 8-4 所示。

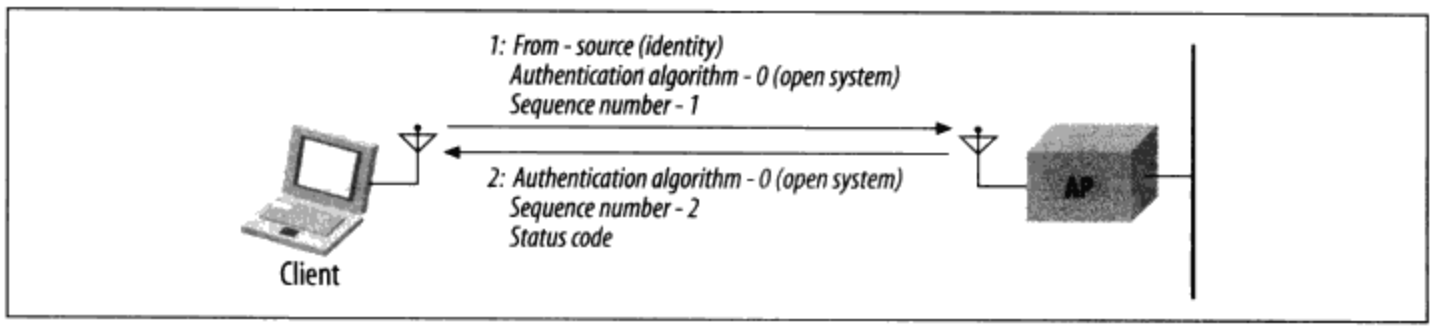


图 8-4：开放系统身份验证的交换过程

由移动式工作站所发出的第一个帧是子类型为 authentication（身份验证）的管理帧。802.11 在规范中并未正式将此帧视为身份验证请求（authentication request），不过它实际上的作用正是如此。在 802.11 中，工作站是以 MAC 地址作为身份证明。和 Ethernet 网络一样，网络上的 MAC 地址必须独一无二，因此可作为工作站的身份证明。接入点以这些帧的源地址作为发送者的身份证明，此外，并没有以该帧的其他字段作为身份证明之用。

身份验证请求包含两个信息元素。首先，身份验证算法标识（Authentication Algorithm Identification）字段被设定为0，代表使用开放系统认证方式。其次，身份验证事务序列号（Authentication Transaction Sequence Number）字段被设定为1，代表该帧实际上为事务序列中的第一个帧。

接入点接着会处理身份验证请求，然后返回结果。和第一个帧一样，响应帧也是子类型为authentication的管理帧。其中包含三个信息元素：身份验证算法标识字段被设定为0，代表使用开放系统身份验证；序列号为2；另外还有一个状态码（Status Code）用来指出身份验证请求的结果。状态码的各种可能值如表4-6所示。

地址过滤（MAC“身份验证”）

802.11并未强制使用WEP，一些早期的产品只实现了开放系统身份验证功能。为了提供更安全的身份验证，有些产品会提供所谓“经授权的MAC地址列表”。网管人员可以输入一组经过授权的工作站地址，只要是列表中的工作站就允许和网络连接。

虽然地址过滤功能聊胜于无，不过还有相当大的改进空间。MAC地址通常可以通过软件或固件加以修改，因此打算访问网络的攻击者可以轻易得逞。此外，要将这些可以访问网络的工作站地址列表传给网络上的所有设备也是件苦差事，何况这份列表的内容还有待商榷。例如购买新的网卡、旧的网卡已经报废、离职员工带走网卡等问题。

授权地址的过滤可作为安全方案的一部分，但非解决方案的关键。尽可能使用802.1X用户身份验证，不要依赖MAC地址过滤。只要网管人员费心验证用户身份，就可以达到标准所提供的安全性。地址过滤只是徒增管理上的复杂度，没有实质利益可言。

旧式的共享密钥身份验证

共享密钥身份验证（shared-key authentication）必须使用WEP，因此只能用于实现了WEP的产品上，虽然目前已经很难找到不支持WEP的产品。正如其名，共享密钥身份验证要求在进行身份验证之前，必须传递共享密钥给工作站。共享密钥身份验证的理论基础是，如能成功响应传给它的质询信息，就证明工作站拥有共享密钥。共享密钥身份验证交换过程使用到4个被归类为authentication（身份验证）的管理帧，如图8-5所示。

第一个帧几乎和开放系统身份验证交换中的第一个帧相同。和开放系统帧一样，其中所包含的信息元素可用于识别所使用的认证算法以及序列号。身份验证算法标识被设定为1，代表使用共享密钥身份验证。

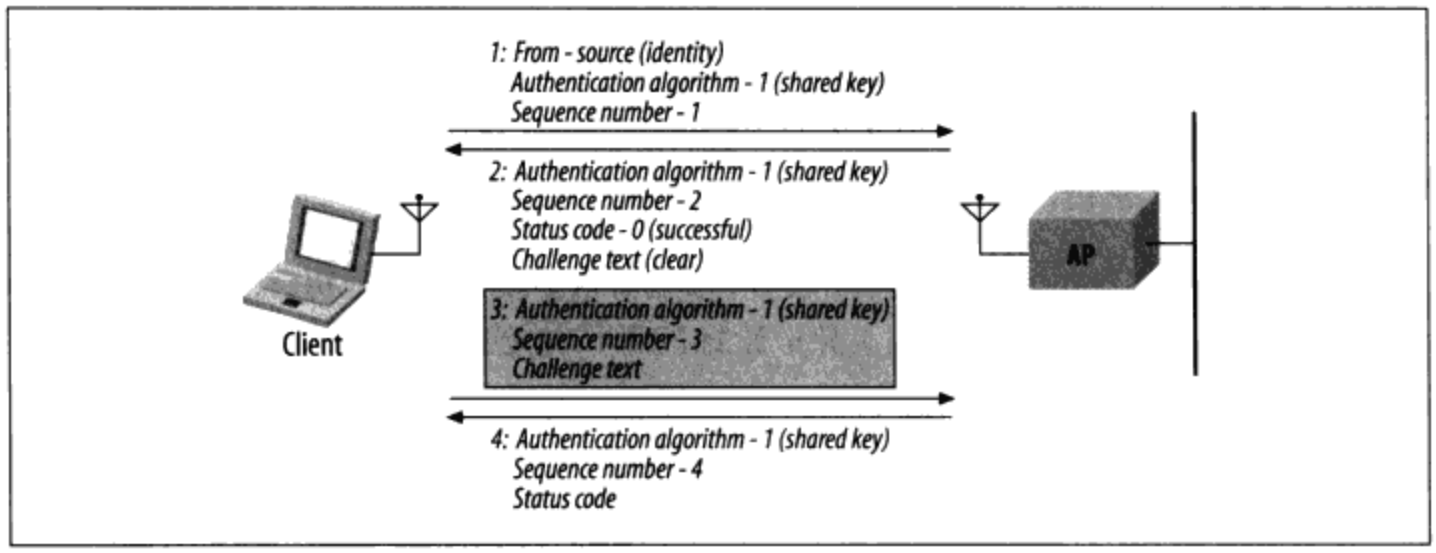


图 8-5：共享密钥身份验证交换过程

共享密钥交换的第二个帧扮演把关的角色，而不是盲目地允许网络访问。第二个帧最多包含 4 个信息元素。通常，这些信息元素包括身份验证算法标识、序列号以及状态码。接入点可能以此帧拒绝身份验证请求，从而中止整个事务过程。要进行下一个步骤，状态码必须为 0（代表成功），如图 8-5 所示。如果状态码显示成功，则此帧还会包含第四个信息元素，即质询文本（Challenge Text）。质询文本的长度为 128 个字节，由 WEP 密钥流生成器（keystream generator）利用随机密钥（random key）及初始向量（initialization vector）产生。

第三个帧是移动式工作站对质询所做出的答复。为了证明本身有访问权限，移动式工作站将会以三项信息元素组成一个管理帧：身份验证算法标识、值为 3 的序列号以及质询文本。在传送此帧之前，移动式工作站将会以 WEP 进行处理它。标头部分会保留不予处理，因为必须利用它来识别其是否为身份验证帧，至于信息元素部分则通过 WEP 予以加密。

收到第三个帧后，接入点会试图予以解密，然后验证 WEP 的完整性。如果可从该帧中解读出质询文本，而且通过完整性校验（integrity check）的验证，接入点就会以成功的状态代码来响应。若能成功解读质询文本，就证明该移动式工作站已经设定好加入该网络所需的 WEP 密钥，因此应该允许它访问网络。如果有任何问题发生，接入点便会返回代表失败的状态码。

破解共享密钥身份验证

共享密钥身份验证很容易屈服于简单的攻击。共享密钥身份验证过程的核心就是质询文本的加密。收到随机的质询信息后，拥有 WEP 密钥的工作站便可从 WEP 密钥产生出所需要的密钥流，然后以之和数据进行 exclusive-OR 运算。不过，关系到质询文本、密钥

流与质询响应的exclusive-OR属于一种可逆的（reversible）运算。只要知道其中两项，就可以逆向推算出第三项。攻击者可以观察质询文本与质询响应，以之推算出密钥流。虽然攻击者可以使用还原的密钥流来响应新的质询信息并且通过网络的身份验证，如果未能还原出WEP密钥，攻击者仍旧无法传送任何数据。

由于攻击共享密钥身份验证只是举手之劳，因此通常不建议使用密钥身份验证。802.11i就不允许以共享密钥通过802.11身份验证的工作站连接到强健安全网络（Robust Security Network）。

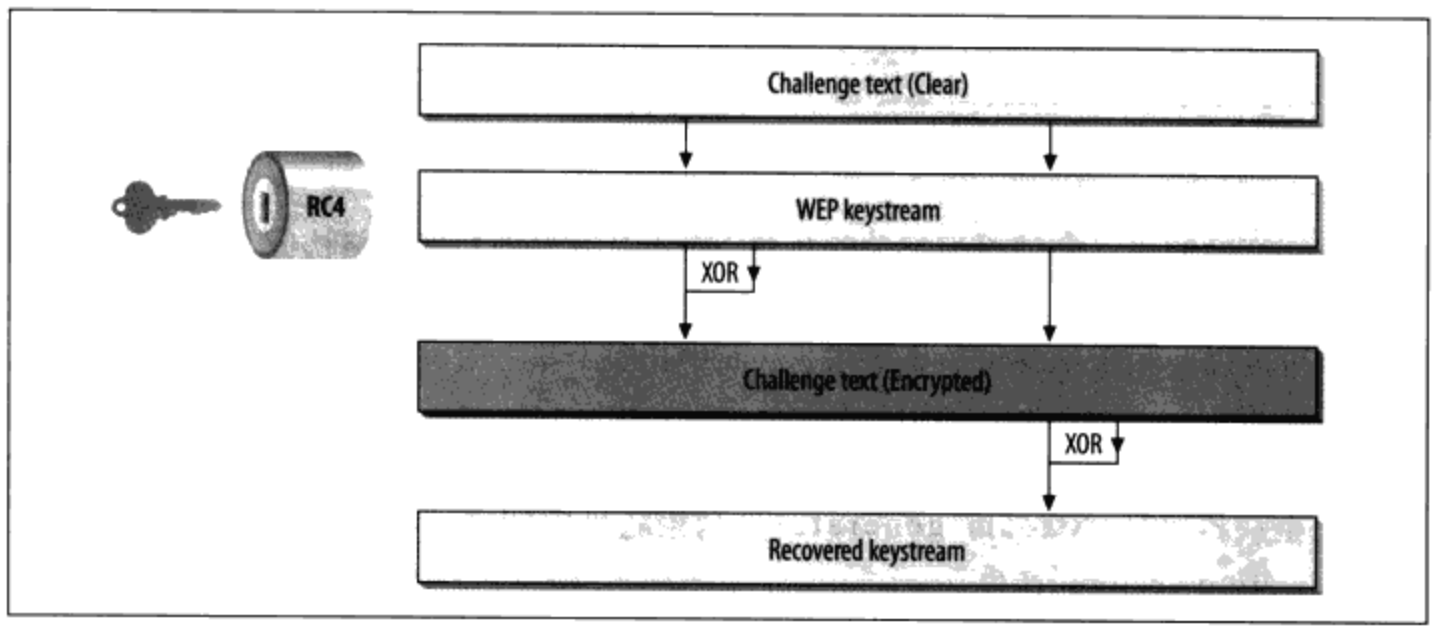


图8-6：破解共享密钥身份验证

预先身份验证

预先身份验证（preauthentication）用来加速关联转移。从工作站决定转移至新接入点，到新接入点开始传送帧给工作站，身份验证是这段期间内最容易造成延迟的因素。预先身份验证的目的就是缩短这段时间，在需要之前先进行这项费时的操作以建立彼此的认证关系。由于低级的802.11身份验证与802.1X身份验证均使用“身份验证”（authentication）这个名词，因此有两种不同类型的预先身份验证。不过，如同网络工程师的习惯用法，身份验证通常是指802.1X身份验证。

802.11预先身份验证

在与接入点关联之前，工作站必须先经过身份验证，不过802.11标准并未要求在低级身份验证之后必须立即进行关联操作。在扫描阶段，工作站可以跟几个接入点进行802.11身份验证，如此一来，当有需要时就可以立即进行关联操作。这种做法称为预先

身份验证（preauthentication）。预先身份验证的好处是，一旦进入接入点的涵盖范围，工作站就可以立即与接入点重新关联，而不必等候认证交换过程。

图 8-7 的左右两边都可以看到，由两个接入点所构成的扩展服务集（ESS）。为了简化起见，此处只会用到一个移动式工作站。假设移动式工作站一开始与图左的 AP1 关联，因为它位于 AP1 的涵盖范围中。当该移动式工作站向右移动时，最后必须跟 AP2 关联，因为它已经离开 AP1 的涵盖范围。

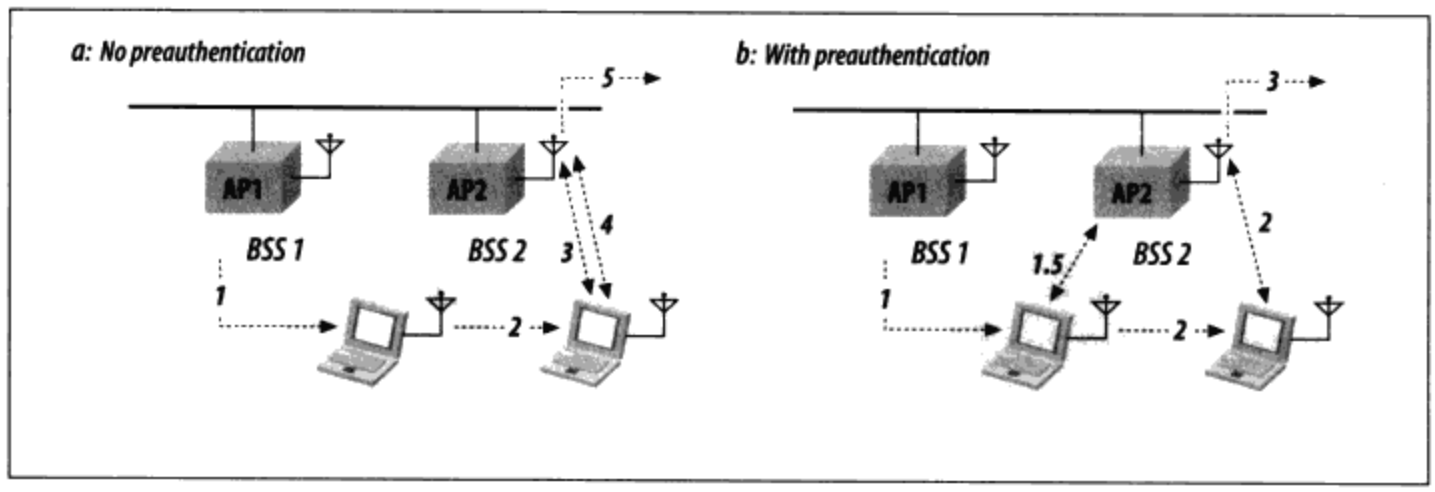


图 8-7：省时的预先身份验证

大多数与 802.11 有关的文字说明都未提到预先身份验证（preauthentication），如图 8-7 a)所示。当移动式工作站移动至右边，来自 AP1 的信号会逐渐减弱。工作站会持续监测来自 ESS 的 Beacon 帧，最后终于注意到 AP2 的存在。至此，工作站或许会选择与 AP1 解除关联，然后与 AP2 进行身份验证与重新关联。这些步骤在图 8-7 a)中已有交代，其中出现的数字为表 8-1 所列的时序值。

表8-1：图8-7的时序

步骤	不采用预先身份验证：8-7 a)	采用预先身份验证：8-7 b)
0	工作站与 AP1 形成关联	工作站与 AP1 形成关联
1	工作站向右移至 BSS1 与 BSS2 的重叠区	工作站向右移至 BSS1 与 BSS2 的重叠区并且检测到 AP2 的存在
1.5		工作站与 AP2 进行预先身份验证
2	AP2 的信号比较强，所以工作站决定与 AP2 形成关联	AP2 的信号比较强，所以工作站决定与 AP2 形成关联
3	工作站与 AP2 进行身份验证	工作站开始使用网络
4	工作站与 AP2 重新关联	
5	工作站开始使用网络	

图8-7 b)显示了采用预先身份验证的工作站会发生什么情况。只要稍微修改软件，让工作站只要检测到AP2，即可与AP2进行身份验证。当工作站离开AP1的管辖范围，就已经同时与AP1和AP2完成了身份验证。当工作站离开AP1的涵盖范围时，省时的效用就出现了：它可以立即跟AP2重新关联，因为已经事先经过身份验证。预先身份验证可以让漫游更为顺畅，因为身份验证可以在需要关联之前完成。图8-7 b)中所显示的每个数字为表8-1所列的时序值。

802.11i预先身份验证与密钥缓存

如果网络采用802.1X进行身份验证，那么从加入802.11网络到能够送出网络协议封包，最费时的步骤就是802.1X身份验证，特别是搭配需要来回传送多个帧的EAP认证方式。预先身份验证让工作站能够在与接入点关联之前事先建立一个安全的操作环境，如图8-8所示。基本上，预先身份验证将关联操作与安全过程加以拆解，让它们能够独立进行。WPA则明确排除了预先身份验证的使用。

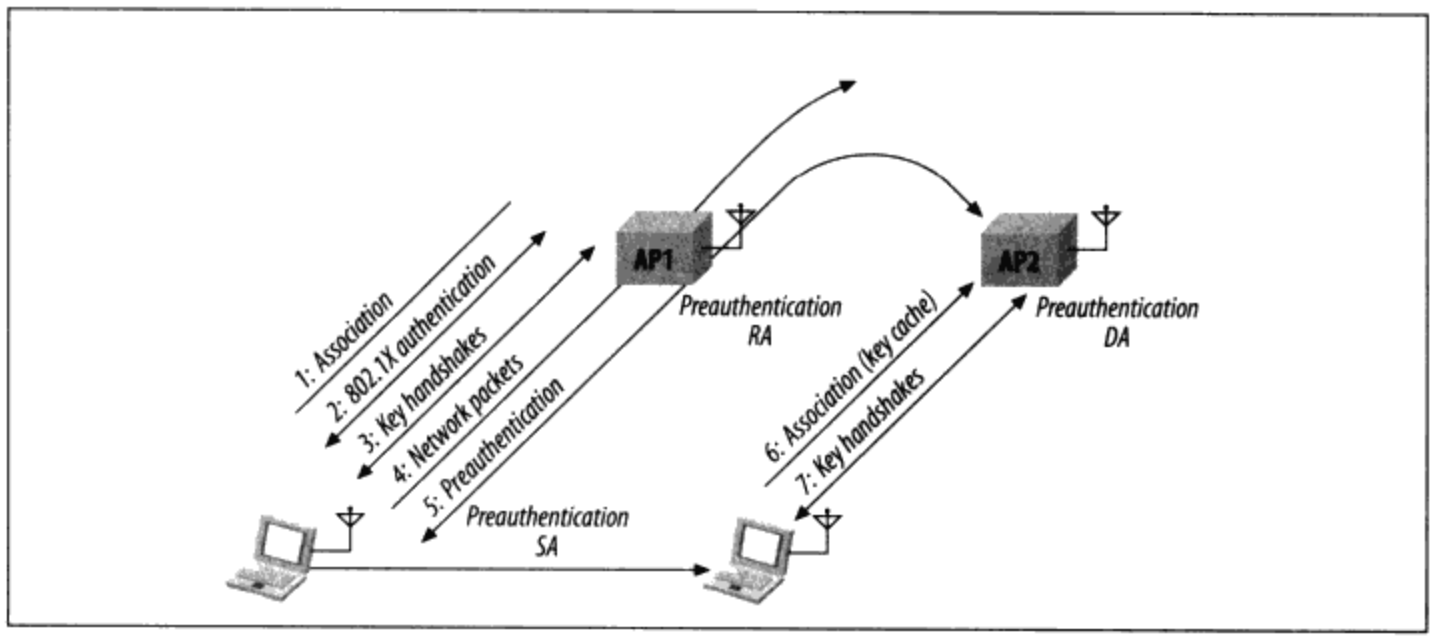


图8-8：802.11i预先身份验证

图8-8显示了如下几个步骤：

1. 工作站关联到它在网络中所发现的第一个接入点。之所以选择与这个接入点关联，是根据工作站固件的判断标准（criteria）。
2. 关联之后，工作站就可以进行802.1X身份验证。这个步骤使用第六章所提到的EAPOL帧，它的Ethertype类型代码为88-8E（十六进制）。接入点会将EAPOL帧转换为RADIUS封包，会话（session）的真实性也经过验证（authenticate）。

3. 双方会分别生成无线电波链路所使用的动态密钥，以四次握手（four-way handshake）生成成对密钥（pairwise key），以组密钥握手（group key handshake）生成组密钥。

4. 当密钥配置完成，工作站就等于“上线”（on the air）了，可以收发网络协议封包。

   工作站软件掌控了漫游的行为，如果对它有利，就可以进行漫游。在移动的过程中，工作站发现AP2似乎是较好的选择，所以开始进行预先身份验证，加快转移到AP2的过程。不过，工作站并不是一并移转所有事项，而是利用预先身份验证缩短收发网络封包因此而中断的时间。

5. 工作站送出一个EAPOL-Start消息给新的接入点，揭开预先身份验证的序幕。工作站每次只能与一个接入点关联，因此预先身份验证帧必须通过旧接入点转达。预先身份验证本身属于完整的802.1X交换。

   a. 预先身份验证帧使用编号范围从88到C7（十六进制）的Ethertype，因为大多数接入点对正常的身份验证Ethertype会做特殊的处理。此帧的源地址为工作站，接收端地址为当前接入点的BSSID（在本例中为AP1无线接口的MAC地址），而目的端地址则是接入点的BSSID（在本例中为AP2的无线接口）。

   b. 由AP1收到以后，帧就会通过分布式系统（distributon system）传给AP2。接入点本身只有一个MAC地址。如果这两个接入点不是位于相同的Ethernet广播域，则必须通过别的方式在两者之间传递预先身份验证帧。

   c. 在整个过程中，工作站仍然与AP1保持关联，也可以使用现有经加密的连接来收发网络封包。由于工作站仍在线，因此不会发生需要进行其他身份验证的情况。

   d. 预先身份验证的结果是与AP2建立起一个安全的操作环境（security context）。工作站与AP2各自产生成对主密钥（pairwise master key），进一步处理后，创建了工作站与AP2之间的密钥。工作站与接入点均将成对主密钥存放于密钥缓存中。

6. 当工作站扣下扳机（pull the trigger），关联就会转移到AP2。作为初始关联过程的一部分，工作站将会提供密钥缓存的副本，告诉AP2它已经通过身份验证。

7. AP2收到身份验证请求并开始搜寻本身的密钥缓存。找出可用密钥之后，便立刻启动成对密钥的四次握手过程。在派生密钥的过程中，短时间内工作站将无法正常收发封包。

当802.11预先身份验证启动费时的802.1X EAP身份验证之际，还是可以通过原本已验证的连接收发网络帧。第一次关联过程较慢，因为需要进行完整的EAP交换过程。使用预先身份验证之后，即可大幅缩短后续关联的切换（handoff）时间。

关联操作

一旦完成身份验证，工作站就可以跟接入点进行关联（或者跟新的接入点进行重新关联），以便获得网络的完全访问权。关联(association)属于一种记录保持(recordkeeping)过程，它让分布式系统（distribution system）能够记录每个移动式工作站的位置，以便将传送给移动式工作站的帧转送给正确的接入点。形成关联之后，接入点必须为该移动式工作站在网络上注册，如此一来，发送给该移动式工作站的帧才会转送至其所属的接入点。其中一种注册方式是送出一个ARP信号，让该工作站的MAC地址得以跟与接入点连接的交换端口形成关联。

关联只限于infrastructure（基础结构型）网络，在逻辑上等同于在有线网络中插入网线。一旦完成此过程，无线工作站就可以通过分布式系统与整个世界连接，而其他人也可以经分布式系统予以响应。802.11在规范中公开禁止工作站同时与一个以上的接入点形成关联。

关联过程

基本的关联过程如图8-9所示。

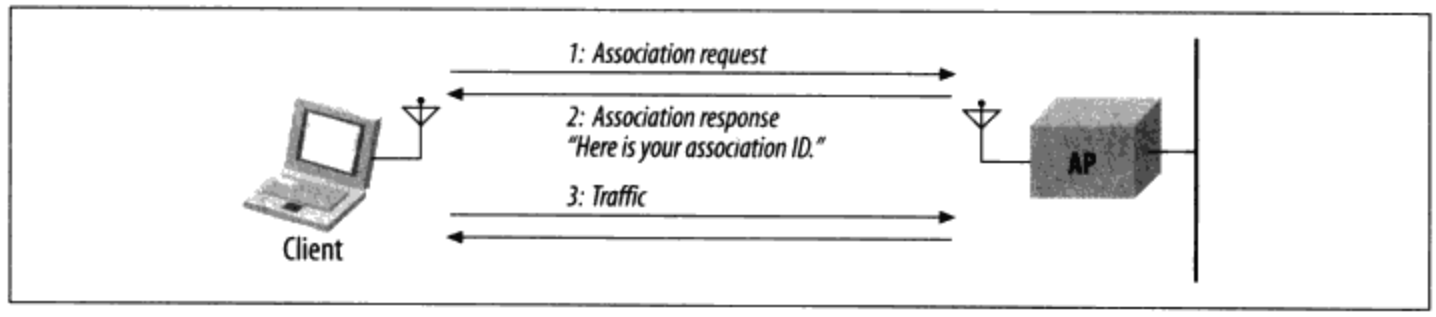


图8-9：关联过程

和身份验证一样，关联操作是由移动式工作站发起的。在此并不需要用到序列编号，因为关联过程只牵涉到三个步骤。其中所用到的两个帧被归类为association管理帧。和单播（unicast）管理帧一样，关联过程的步骤由一个关联帧及必要的链路层响应组成：

1. 一旦移动式工作站与接入点完成身份验证，便可送出Association Request（关联请求）帧。尚未经过身份验证的工作站会在接入点的响应中收到一个Deauthenticaton（取消关联）帧。
2. 接入点随后会对关联请求进行处理。802.11标准并未规范如何判断是否允许关联，这因接入点的实现而异。较常见的方式是考虑帧缓存所需空间的大小。从Association Request（关联请求）帧中的Listen Interval（聆听间隔）字段可以大致上推算出。

a. 一旦关联请求获准，接入点就会以代表成功的状态代码0及关联标识符（Association ID，简称AID）来响应。AID本身是数值形式的标识符，在逻辑上则是用来识别缓存帧所要传递到的移动式工作站。此过程大部分的细节参见本章的“节省电力”一节。

b. 关联请求如果失败，就只会返回状态码并且中止整个过程。

3. 接入点开始为移动式工作站处理帧。在常见的产品中，使用的分布式系统媒介通常是Ethernet。当接入点所收到的帧的目的地为与之关联的移动式工作站时，就会将该帧从Ethernet桥接至无线媒介。如果该移动式工作站处于省电（power-saving）状态，则为之缓存帧。在共享式Ethernet中，该帧会被送至所有接入点，不过只有正确的接入点会进行桥接处理。在交换式Ethernet里，该工作站的MAC地址可以跟某个特定的交换端口（switch port）形成关联。当然，该交换端口必须连接到当前为该工作站提供服务的接入点。

重新关联过程

重新关联（reassociation）是指将关联关系从旧接入点移转至新接入点的过程。在空气中，这个过程几乎和关联（association）没什么两样；不过在骨干网络方面，接入点之间会彼此通信以便转移帧。当工作站从某个接入点的涵盖范围内转移至另一个接入点时，就会进行重新关联过程，以便把自己的新位置通知802.11网络。此过程如图8-10所示。

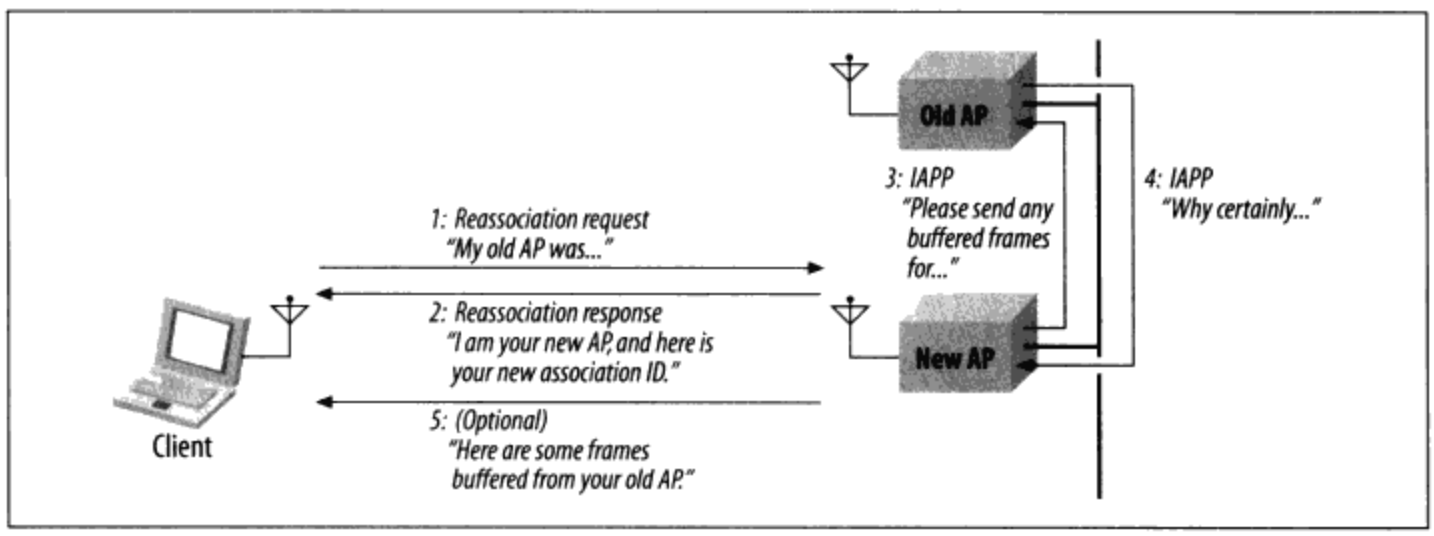


图8-10：重新关联过程

整个过程开始之前，移动式工作站必须已关联至某个接入点。工作站会持续监测从当前的接入点以及同一个ESS中其他接入点所收到的信号质量。一旦移动式工作站检测到其他接入点或许是较好的关联对象时，就会启动重新关联过程。用以作出转换接入点决定的考虑因素因产品而异。所收到的信号强度可根据每个帧加以判断，Beacon（信标）的

传送是否正常也可以作为判断来自接入点的信号强度的基准。在进行第一个步骤之前，移动式工作站必须先与新的接入点完成身份验证过程。

图 8-10 描述了以下步骤：

1. 移动式工作站对新的接入点发出 Reassociation Request（重新关联请求）。Reassociation Request的内容与 Association Request（关联请求）相同，唯一的差别在于Reassociation Request帧中包含了一个用来记载旧接入点地址的字段。新接入点必须与旧接入点取得联系，以判断该工作站之前的关联是否存在。虽然IEEE已经定义出标准的接入点内部协议（inter-access point protocol，简称IAPP），不过有些实现产品还是使用自行开发的专属格式。如果新接入点无法验证旧接入点是否已经对工作站进行过身份验证，新接入点就会响应一个 Deauthenticatoin（解除身份验证）帧，同时中止整个过程。
2. 接入点开始处理Reassociaton Request（重新关联请求）。Reassociaton Request 的处理方式与Association Request类似，以同样的决定因素来判断是否允许重新关联：
   a. 如果Reassociation Request获准，接入点就会返回代表成功的状态码0以及AID。
   b. 如果Reassociation Request 失败，则只会返回状态码，而整个过程也会跟着中止。
3. 新接入点和旧接入点取得联系以完成整个重新关联过程。接入点间的通信属于IAPP 的一部分。
4. 旧接入点把为该移动式工作站所缓存的帧移交给新接入点。802.11标准并未规范接入点之间如何沟通，填补这项遗漏是 802.11 工作组当前的主要任务之一。移交缓存帧后：
   a. 旧接入点为该移动式工作站所缓存的帧均会被移交给新接入点，以便传递给该移动式工作站。
   b. 旧接入点中止其与该移动式工作站之间的关联关系。移动式工作站同一时间只能与一个接入点关联。
5. 新接入点开始为该移动式工作站处理帧。当接入点收到目的地为该移动式工作站的帧时，就会将此帧由Ethernet桥接至无线媒介。如果该移动式工作站处于省电模式，则为之缓存帧。

如果工作站离开之后重新返回某个接入点的涵盖范围，也可以用重新关联过程再次加入该网络，如图 8-11 所示。

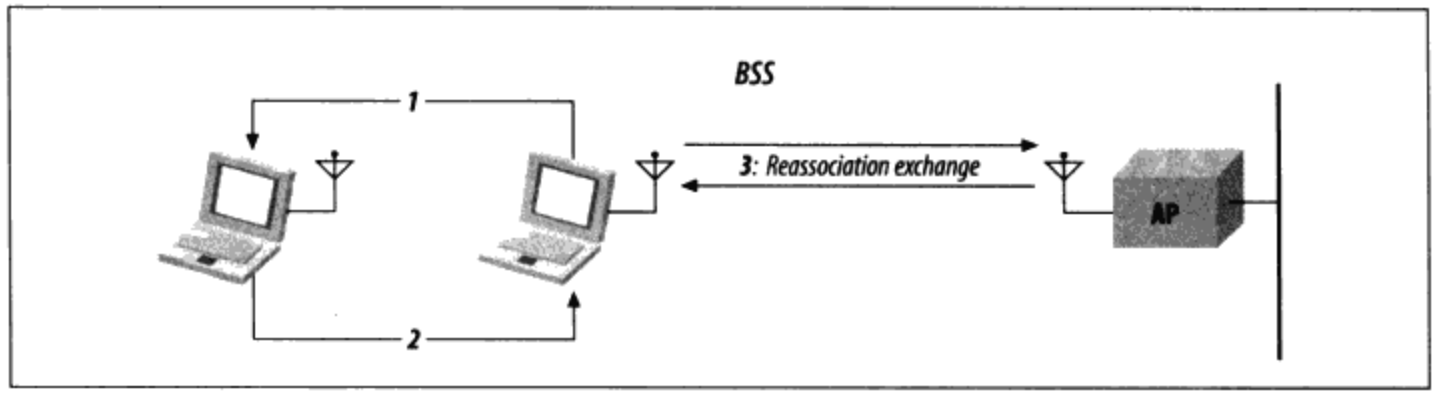


图 8-11：与同一个接入点重新关联

什么是漫游（roaming）？

802.11标准完全没有提到“漫游”(roaming) 这个词（最近才成立一个任务组负责解决漫游问题，但是离见到成果还有一段距离）。不过在谈论802.11时，很多人经常会使用“漫游”这个非正式的名词。一般而言，多数人都认为漫游就是从一个接入点转换到另一个接入点。

过去几年中，漫游一直受困于“名词泛滥”(buzzword overload) 的处境，如今，漫游对不同的用户而言有不同的含义。基本上，漫游是指工作站转换接入点的过程。工作站如何决定是否转换接入点呢？802.11标准对此完全不置一词。决定是否转换接入点完全取决于所使用的软硬件，由各家厂商自行决定。有些客户端设备会选择接口刚启动时最强的信号，然后与之终身厮守，只有在完全收不到信号时才会转换接入点。有些设备永远追随信号最强者，要是有两个信号难分轩轾，就会在接入点之间不断切换。一些其他的设备则会将最近的关联记录纳入考虑，避免在两个邻近的接入点之间进行不必要的切换。工作站如何决定是否以及何时转换接入点，完全视厂商如何决定。原谅我套句Milton Friedman 的话，“不论何时何地，漫游均属客户端现象”(roaming is always and everywhere a client phenomenon)（译注1）。

深究第二层含义，“漫游”意味着工作站如何能够在转换接入点的同时仍然维持原有的网络连接（network connection）。如果涉及IP子网络的界限问题，复杂度就会相对提高，这就必须在所有标准以外加以解决。第二十一章在探讨如何构建一个无线局域网时，还提到了如何实现跨网络拓扑的无间隙漫游。

—待续—

译注1：Friedman是美国著名的经济学家。换个比较通俗的说法，作者的意思是不论何时何地，是否漫游都是客户端的自由。

有时候漫游会被赋予其他意义，意指从某一种网络连接（例如802.11无线局域网）切换到性质截然不同的网络（例如3G移动电话网络）的过程。IEEE已经成立另外的工作组来负责定义可以在不同类型的IEEE 802网络中转移网络连接与状态的漫游操作。

节省电力

无线网络的主要优点在于，当节点访问网络时不必位于特定的位置上。要充分利用移动性的优点，就不能有什么因素限制节点的位置，包括电源的供应。因此，移动性同时意味着移动设备会使用电池供电。不过电池的电力有限，只能够维持一段时间。至少，要求移动用户经常转回以商业用电供电就很不方便。有些无线应用需要较长的电池供电时间，以免影响到网络连接质量（connectivity）。

和其他网络接口一样，在无线网络中关闭收发器（transceiver）能够节省可观的电力。只要关闭收发器，该接口可说是进入休眠（*sleeping*）、假寐（*dozing*）或省电（*power-saving*，简称PS）模式。当收发器再度打开，该接口则可称为重新苏醒（*awake*）、启动（*active*）或者简单称为开机（*on*）。对802.11而言，其节省电源的方式是尽量减少后者所花费的时间，同时尽量延长前者所持续的时间。不过，802.11这种做法并不会牺牲掉网络的连接质量。

Infrastructure（基础结构型）网络的电源管理

在infrastructure网络中，电源管理可发挥最大的效用。所有传送给移动式工作站的数据都必须流经接入点，因此接入点是缓存数据的理想地点。大多数数据均可以被缓存。标准中禁止缓存需要依次传送（in-order delivery）或者设定Order位的帧，因为缓存操作在实现时有可能将帧重新排序。基本上并没有必要设计分布式缓存系统，因为如此一来每个工作站都得实现这项功能，所以不如将整个工作交给接入点负责。在定义上，接入点必须知道每个移动式工作站的位置，而且移动式工作站可以对所属接入点交代本身的电源管理状态。此外，接入点必须随时保持清醒 —— 前提是接入点必须持续有电力供应。因此，在infrastructure网络中，接入点在电源管理上扮演着关键性的角色。

接入点有两项与电源管理相关的任务。其一，因为接入点知道所关联的每个工作站的电源管理状态，因此只要该工作站处于作用（active）状态，接入点即可判断应该将帧传送至无线网络，否则就得为之缓存帧。不过，只是为之缓存帧并不足以让移动式工作站得知应该提取等待中的帧。接入点的第二项任务是定期地声明有帧待传的工作站。在infrastructure网络中周期性地公告缓存状态，对于电力的节省也有贡献。开启接收器聆

听缓存状态远比周期性地送出轮询帧所耗费的电力要少得多。除非收到必要的通知，否则工作站根本不用耗费电力来启动传送器送出轮询帧。

电源管理在设计上是针对以电池供电的移动式工作站的需要。移动式工作站可以休眠一段时间不去使用无线网络接口。在关联请求中与此相关的参数是 Listen Interval（聆听间隔），代表移动式工作站可以选择休眠几个 Beacon 周期。较长的聆听间隔会用掉接入点较多的缓存空间。因此聆听间隔是评估支持某个关联所需的资源时会用到的关键参数之一。聆听间隔可以视为工作站与接入点的一项契约。一旦同意在休眠期间为工作站缓存帧，就表示接入点同意在丢弃这些帧之前必须至少等候聆听间隔所设定的时间。如果在每个聆听间隔之后移动式工作站并未查看缓存帧，接入点就会直接将帧丢弃，而不再另行通知。

缓存单播帧以及使用 TIM 来传递

当有帧被缓存（buffered）时，目的地节点的关联标识符（Association ID，简称 AID）可以在该帧及其目的地之间提供逻辑链路（logical link）。逻辑上，每个 AID 可将缓存帧连接至该 AID 所指定的移动式工作站。组播（或多播）与广播帧被缓存时，会被链接至数值为 0 的 AID。被缓存的组播与广播帧的传递将会在后面说明。

光是做到了缓存还不够，如果工作站一直未能提取为之缓存的帧，那么根本毫无意义。为了通知工作站有帧待传，接入点会产生所谓的传输指示映射（traffic indication map，简称TIM）并且通过Beacon帧传送。TIM本身是由2008位所构成的虚拟位映射表（virtual bitmap）。由于采用offset（偏移量）的处理方式，因此接入点只需传送虚拟位映射表的一小部分。如果只有少数工作站有缓存帧待传，这种做法就可省下不少网络资源。TIM 中的每个位均会对应到特定 AID，设定与特定 AID 相应的位，代表接入点为该 AID 所对应的工作站缓存了单播帧。

无线工作站必须苏醒过来并进入活跃（active）模式，来聆听 Beacon 帧以便接收 TIM。只要查看 TIM，工作站即可判断接入点是否帮助自己缓存帧。要撷取基站所缓存的帧，移动式工作站可以使用PS-Poll控制帧。如果接入点同时为多个移动式工作站缓存帧，这些工作站在传送 PS-Poll 之前必须使用随机 backoff 算法来决定访问顺序。

每个 PS-Poll 帧只用来撷取一个缓存帧。帧从缓存区被移除之前必须得到接收端的肯定确认。肯定确认是必要的，如此一来可以避免第二个或重试的 PS-Poll 被自动当成隐式确认（implicit acknowledgment）。整个过程如图 8-12 所示。

如果接入点为某个移动式工作站缓存的帧不只一个，Frame Control（帧控制）字段的 More Data（更多数据）位就会设定为 1。移动式工作站可以据此发送额外的 PS-Poll 请求给接入点，直到 More Data 位变为 0。在 802.11 标准中对此并无时间限制。

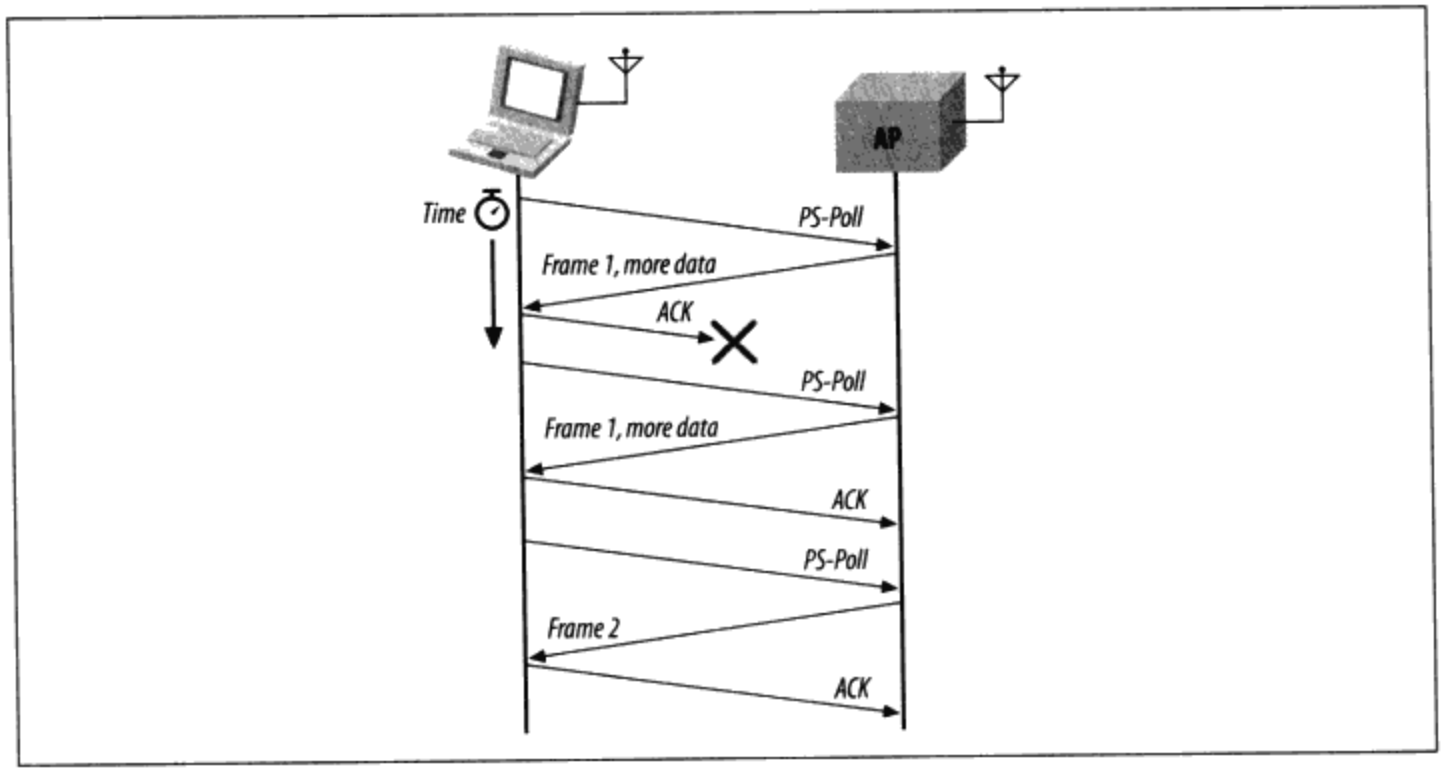


图 8-12：以 PS-Poll 撷取缓存帧

传送PS-Poll之后移动式工作站必须保持清醒，直到整个事务完成或TIM中与自己的AID相应的位已被清除。第一种情况的理由十分明显：移动式工作站已经从接入点成功取得缓存数据，整个事务过程包含工作站即将返回休眠状态的通知信息。第二种情况允许移动式工作站回到省电模式，如果接入点将缓存帧弃置的话。当准备送给某个工作站的所有帧传送完毕或是被接入点丢弃，该工作站即可恢复休眠状态。

整个缓存与递送过程如图 8-13 所示，其中显示了媒介与一个接入点（AP）以及与接入点关联的两个处于省电模式的工作站（Station1 与 Station 2）。时间轴上的垂直坐标代表信标间隔（beacon interval）。在每个信标间隔区间，接入点都会通过 Beacon 帧传送 TIM 信息元素（本图有点简单，还有一种特别的 TIM 信息可传递组播数据，下一节会加以描述）。Station 1的聆听间隔为2，因此每隔2个Beacon周期就得醒来接收TIM。Station 2的聆听间隔为3，因此每隔3个Beacon周期即会醒来处理TIM。工作站轴线上方的线段代表接收端聆听 TIM 的启动（ramp-up）过程。

在第一个信标间隔区间内只有 Station 1 的缓存帧。由于 Station 2 并无帧缓存，因此可以立即返回休眠状态。在第二个信标间隔区间内，根据TIM的指示，接入点同时存在为 Station 1 及 Station 2 缓存的帧，不过此时只有 Station 1 醒着聆听 TIM。Station 1 发出 PS-Poll 帧并且收到缓存帧，接着 Station 1 返回休眠状态。在第三个信标间隔区间，Station 1 与 Station 2 都处于休眠状态。在第四个信标间隔区间，Station 1 与 Station 2 皆醒着聆听 TIM，根据 TIM 的指示，接入点同时存在为 Station 1 及 Station 2 缓存的帧。Station 1 与 Station 2 皆准备好送出 PS-Poll 帧并依照竞争窗口（contention window，

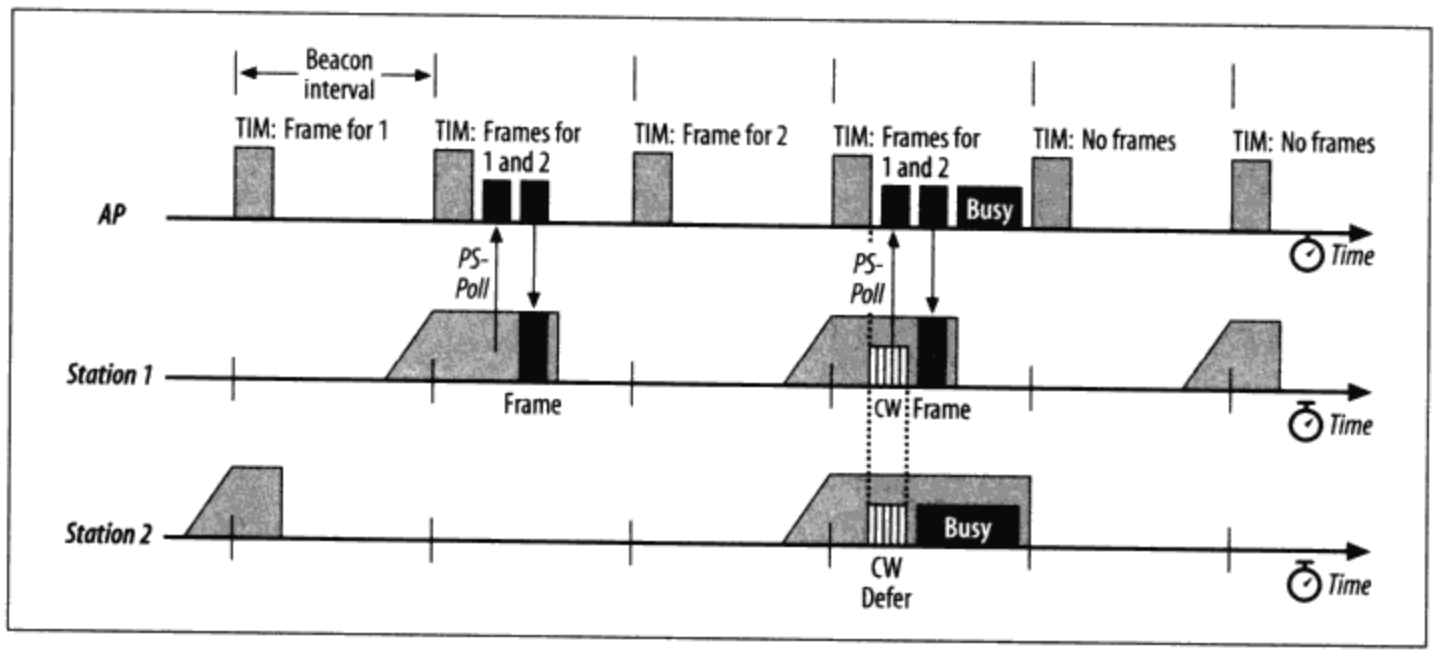


图 8-13：缓存帧的撷取过程

简称 CW）递减计数过程取得媒介使用权（参见第三章）。由 Station 1 先取得媒介使用权，因为它的随机延迟较短。于是 Station 1 发出 PS-Poll 并且收到接入点为它缓存的帧。在此期间，Station 2 会不断推迟。假设在帧传送之后，另外一个图 8-13 中并未显示的工作站取得了媒介使用权，那么 Station 2 必须一直保持清醒，直到下一个 TIM 的到来。如果接入点此时用尽缓存空间，因而丢弃为 Station 2 缓存的帧，第五个信标的 TIM 就会显示并无缓存帧待传，此时 Station 2 终于可以返回省电模式。

工作站可以在任何时候从省电模式切换为活跃模式。膝上型计算机如果使用 AC 电源，通常会充分供应外围设备电源以全力运行，只有在使用电池时才会节省电力。如果一个移动式工作站从休眠状态切回活跃模式，可以不用等候 PS-Poll 即开始传送帧。PS-Poll 帧用以指示某个处于省电状态的移动式工作站暂时切换为活跃模式并且准备接收被缓存的帧。在定义上，活跃的工作站的收发器处于持续运作的状态。切换到活跃模式后，接入点可以假设接收端处于运作状态，就算没有收到任何告知信息。

接入点为移动式工作站缓存帧的时间必须足够长，这样才能让工作站顺利提取这些帧，不过用来缓存帧的缓冲存储器（buffer memory）却是一项有限的资源。802.11 强制要求接入点必须使用某种老化功能（*aging function*），以便判断帧是否缓存过久，能否丢弃。802.11 标准留下了相当大的空间给开发人员自行斟酌，只规范了一项限制。接入点为工作站缓存数据时至少必须保存关联时 listen interval（聆听间隔）所指定的时间，而且标准里还限定，如未超出 listen interval 所指定的时间，老化功能就不能丢弃帧。除此之外，各厂商有相当大的空间可以自行开发不同的缓存管理功能。

传递组播与广播帧：延迟传输指示映射（DTIM）

指定组播地址的帧无法使用论询算法（polling algorithm）来传递，因为在定义上，这些帧是发给某个特定组的。因此，802.11纳入了一种机制，用来缓存与传递广播与组播（或多播）帧。缓存的方式与单播帧一样，但不同于为处于休眠状态的工作站所缓存的帧。经缓存的广播与组播帧是通过AID 0存储的。接入点会将TIM的第一个位设定为0，代表有广播或组播帧被缓存。此位对应于AID 0。

每个BSS均有一个称为DTIM Period的参数。TIM是以Beacon信息来传送的。每当经过几个固定的Beacon interval（信标间隔），就会发送一个特殊类型的TIM，称为延迟传输指示映射（Delivery Traffic Indication Map，简称DTIM）。Beacon帧中的TIM元素包含了一个计数器，用来倒数计时至下一个DTIM来临。在DTIM帧中，此计数器值为0。经缓存的广播与组播数据会在DTIM Beacon之后传送。如有多个缓存帧，则会依次传送。Frame Control字段中的More Data位用以指示是否还有其他帧待传。信道使用权的取得规则也适用于暂存帧的传送。接入点或许会选择暂缓处置所收到的PS-Poll请求，直到传送完缓存区中的广播与组播帧。

图8-14显示了一个接入点及一个与之关联的工作站。接入点的DTIM interval（延迟传输指示映射间隔）被设为3，因此每隔两个TIM就会有一个DTIM。Station 1处于休眠模式，其listen interval（聆听间隔）为3。每3个beacon周期Station 1就会醒来接收经缓存的广播与组播帧。每传送一个DTIM帧，就会接着传送被缓存的广播与组播帧，其后伴随的是与工作站关联的PS-Poll交换过程。在第二个beacon interval（信标间隔）区间，缓存区中只有广播与组播帧，这些帧随即会被传送到BSS。在第五个beacon interval（信标间隔）区间，Station 1还有一个被缓存的（单播）帧。Station 1可以监视DTIM中的指示映射（map），等到被缓存的广播与组播帧传送完毕后再发送PS-Poll信息。

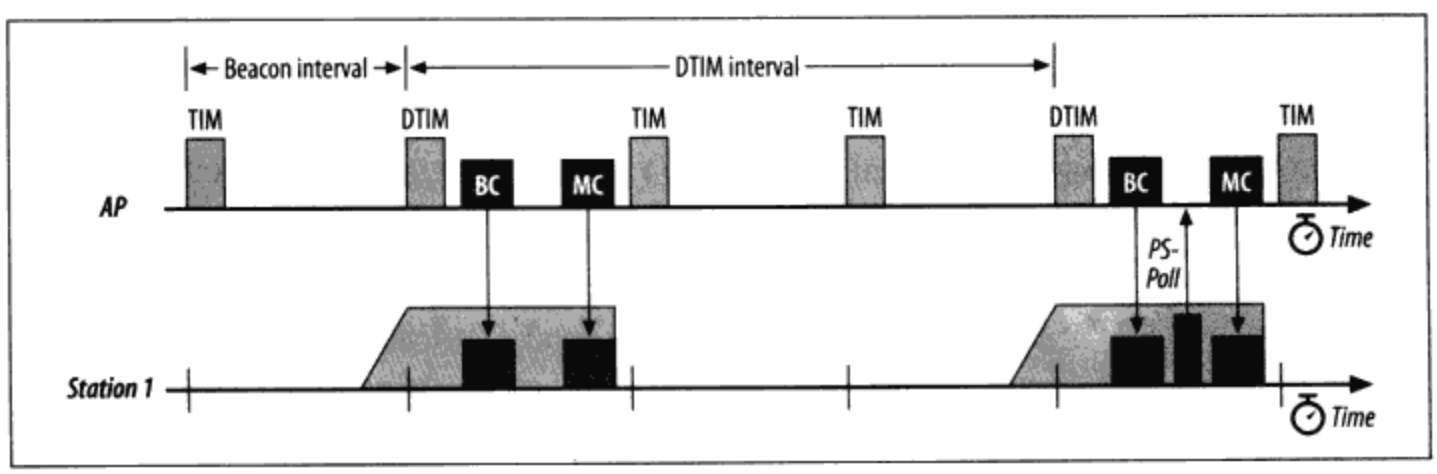


图8-14：在DTIM之后传送广播与组播帧

为了接收广播与组播帧，移动式工作站必须醒着接收DTIM信息。不过802.11标准并未规定infrastructure（基础结构型）网络里进入省电模式的工作站必须醒来聆听DTIM帧。如果系统管理人员认为电池使用时间比接收广播与组播帧重要，可以不用根据DTIM来设定工作站的聆听间隔。有些文献以超低功耗（*extremely low power*）、超省电模式（*ultra power-saving mode*）、沉睡（*deep sleep*）或者类似名词来称之。

有些产品允许设定DTIM interval。将DTIM interval加长可以让移动式工作站休眠一段较长的时间，如此可以延长电池的使用时间，不过代价是无法实时传送数据。较短的DTIM interval强调立即传送，代价则是工作站必须经常开开关关。如果电池使用时间比实时接收广播与组播帧重要，则可以采用较长的DTIM。至于是否适合使用较长的DTIM，取决于需要哪一方面的应用以及能否允许长时间的链路层延迟。

IBSS的电源管理

IBSS的电源管理效率不如infrastructure网络。在IBSS中，发送端必须承受较重的负担以确保接收端处于清醒状态。接收端也必须经常保持清醒，不能像在infrastructure网络中那样休眠太久的时间。

和infrastructure网络一样，independent（独立型）网络的电源管理是以传输指示消息（traffic indication message）为基础。independent网络必须利用某种分布式系统，因为并不存在任何逻辑上的中央协调者（central coordinator）。independent网络中的工作站使用ATIM（announcement traffic indication message，通知传输指示数据指示消息；消息），有时也称为ad hoc traffic indication message（特设数据指示信息），强迫其他工作站保持清醒。在同一个IBSS中，所有工作站都必须在Beacon传送后的特定期间内聆听ATIM帧。

如果有某个工作站为另一个工作站缓存帧，它可以送出ATIM来通知对方。实际上，ATIM帧是让收发器保持开启的消息，因为有数据待传。没有收到ATIM帧的工作站是否要进入省电模式则悉听尊便。在图8-15 a)里，Station A为Station C缓存了一个帧，因此在ATIM传送窗口（transmission window）会送出一个单播式ATIM帧给Station C，目的是告诉Station C不该进入省电模式。不过，Station B可以随意关闭其无线接口。图8-15 b)显示了使用中的组播式ATIM帧。该帧是用来通知一组工作站不要进入低功耗模式。

紧接信标传送之后的一段时间窗口（time window）称为ATIM窗口（ATIM window）。在这期间，每个节点都必须保持清醒。在ATIM窗口中，任何工作站都不准关闭其无线接口。这段周期始于预料信标即将到来，终于IBSS被创建后的某个特定时间点。如果因为流量负载过重而导致信标迟到，ATIM窗口可以使用的时间就会等量缩减。

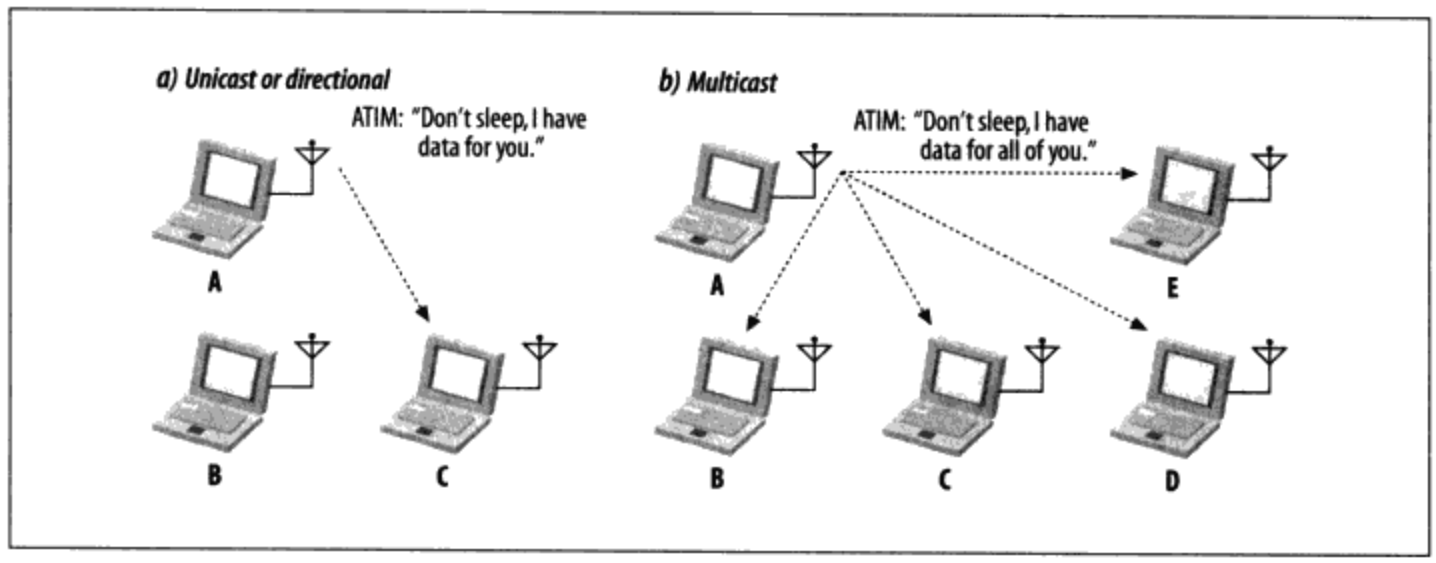


图 8-15：ATIM 的运用

ATIM窗口是创建IBSS唯一必要的参数。将之设定为0即可避免使用任何电源管理。图8-16显示了ATIM窗口与信标间隔之间的关系。其中，第四个信标因为媒介忙碌而迟到。ATIM窗口维持不变，还是从原本预计的信标间隔算起，持续经过一个ATIM窗口。当然，ATIM窗口可使用的时间会因为信标传送的延迟而等量减少。

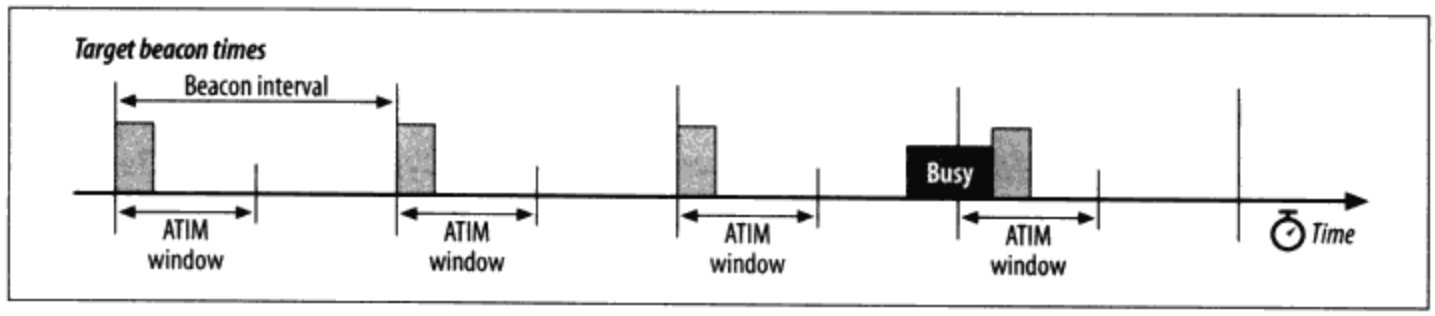


图 8-16：ATIM 窗口

为了监视整个ATIM窗口，工作站必须在信标传送之前醒来。如此一来可能会遇到以下四种情况：工作站送出一个ATIM、收到一个ATIM、无传送也无接收以及同时传送与接收。传送ATIM帧的工作站不能休眠。传送ATIM代表有传送缓存数据的打算，因此也表示准备保持清醒的意识。ATIM帧所针对的工作站也不可休眠，如此才能收到ATIM发送端所要传送的帧。如果一个工作站既传送也接收ATIM帧，就会保持清醒。只有既不传送不会接收ATIM帧的工作站才可以进入休眠状态。当一个工作站因ATIM而保持清醒时，就会一直持续到下一个ATIM窗口结束为止，如图8-17所示。其中，工作站在第一个ATIM窗口清醒。如果该工作站未收发任何ATIM帧，那么等到该ATIM窗口结束即可休眠。如果同时收发ATIM帧，工作站就会一直保持清醒，直到第三个ATIM窗口结束，如图8-17中第二个ATIM窗口所示。

在ATIM窗口中只能传送特定的控制与管理帧，包括Beacon、RTS、CTS和ACK，当然还有ATIM帧。传送时必须依循DCF的规则。ATIM帧之所以只能在ATIM窗口中传

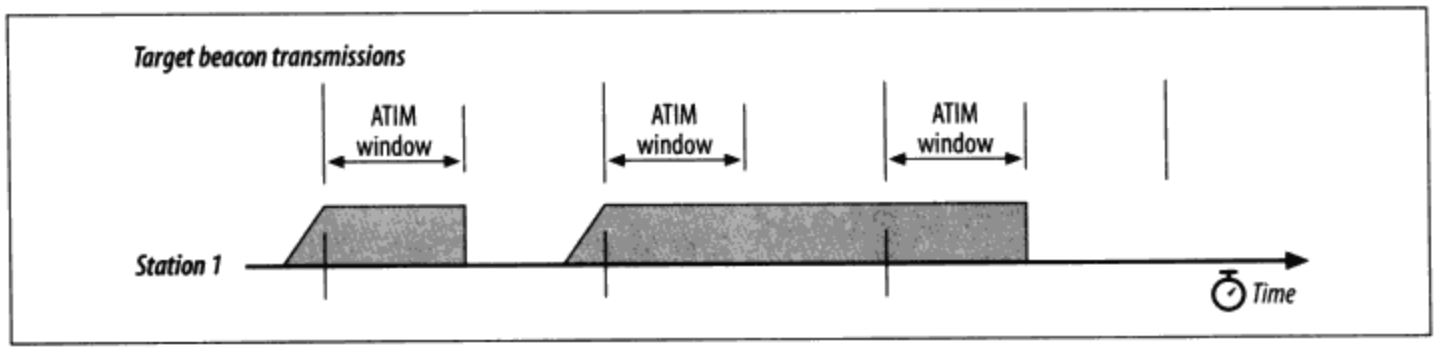


图 8-17：ATIM 对省电模式的影响

送，是因为在这个窗口以外工作站可能处于休眠状态。如果 IBSS 中其他工作站都处于休眠状态，此时送出 ATIM 帧便毫无意义。同样地，单播式 ATIM 帧也需要得到肯定确认，因为这是保证对方的确收到ATIM信息并在信标间隔剩余时间保持清醒的唯一方式。组播式 ATIM 帧并不需要得到肯定确认，因为要一大群工作站同时确认组播帧太没效率了。如果所有 ATIM 帧的潜在接收端都必须进行肯定确认，这些确认信息可能会打断所有的网络服务。

被缓存的广播与组播帧会在ATIM窗口结束后予以传送以符合DCF的约束。广播与组播帧传送之后，工作站可以接着传送 ATIM 所通知的单播帧，同时由接收端得到肯定确认信息。所有由 ATIM 通知的消息传送之后，工作站可以将未被缓存的帧直接传送给已知处在清醒状态的其他工作站。工作站如果送出信标、ATIM 或它不能休眠时，就必须保持清醒。如果争夺媒介使用权的情形十分严重，将导致之前发布 ATIM 的工作站无法如期送出缓存帧，则该工作站必须在下一个 ATIM 窗口开始之后重新发布 ATIM。

图 8-18 显示了以上所提到的某些规则。在第一个信标间隔，Station 1 传送了一个组播式 ATIM 给 Station 2、3 和 4。组播式 ATIM 帧无需得到肯定确认，不过 ATIM 的发布意味着所有工作站都必须保持清醒直到下一个 ATIM 窗口结束，以便从 Station 1 处接收组播帧。当 ATIM 窗口结束，Station 1 即可传送被缓存的组播帧给其他三个工作站。之后，Station 4 可以利用下一个信标到来之前的剩余时间传送一个帧给 Station 1。这个帧并非通过 ATIM 发布，但它知道对方必定处于清醒状态。

在第二个信标间隔区间，Station 2 与 Station 3 均有准备传送给 Station 4 的缓存帧，因此它们会各自送出一个 ATIM，而 Station 4 则分别加以确认。ATIM 窗口结束之后，Station 1 既未传送也未收到任何 ATIM 信息，因此可以进入省电状态，直到下一个信标间隔开始。不过，Station 2 的帧相当长，因此剥夺了 Station 3 传送帧的机会。

当第三个信标间隔开始时，Station 3 仍然有一个被缓存的帧要传给 Station 4。因此 Station 3 会重新传送一个 ATIM 帧给 Station 4，而 Station 4 也会加以确认。此时 Station 2 和任何 ATIM 的交换都没有关系，因此在 ATIM 窗口结束后即可进入省电状态。由于此时已经没有任何缓存的广播或组播帧，因此 Station 3 可以开始传送之前宣布要传给

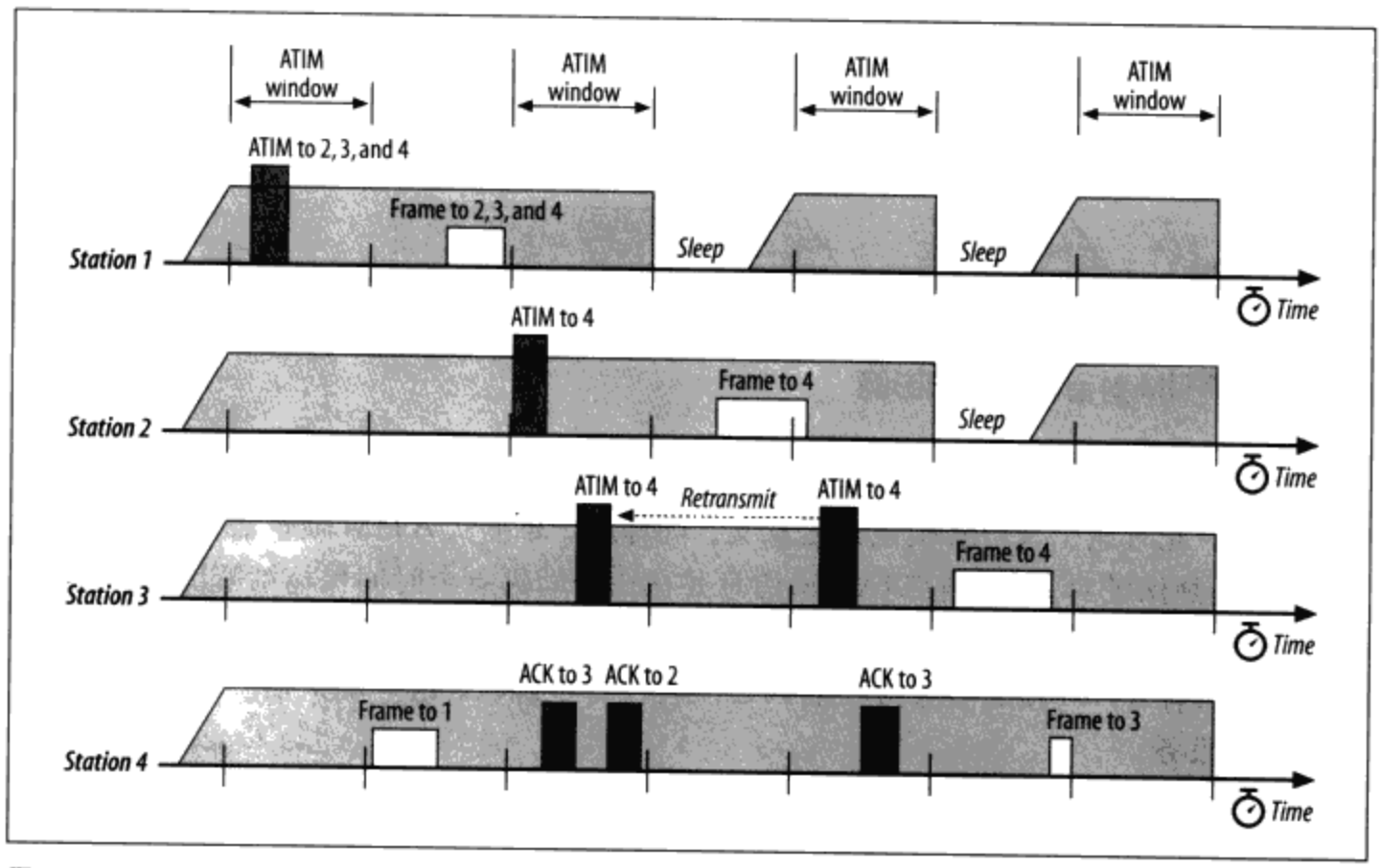


图 8-18：IBSS 网络中 ATIM 对省电模式的影响

Station 4 的帧。帧传送完毕之后，Station 4 可以趁下一个信标帧来临之前传送一个帧给 Station 3，因为 ATIM 交换过程的缘故，可以推论出 Station 3 必然还处于清醒状态。

工作站必须负责维持足够的内存供缓存帧使用，不过要使用多大的缓存区，实际上必须在是否挪作他用之间作出取舍。802.11 标准允许 independent（独立型）网络中的工作站丢弃缓存过久的帧，不过实际判断的算法并不在标准的范围之内。对任何缓存管理功能而言，唯一的要求是缓存帧至少得保存一个信标周期。

定时器的同步

和其他无线网络技术一样，802.11 十分依赖传递给各节点的定时信息。在跳频网络中，定时信息特别重要，因为网络上所有工作站都必须以事先协调好的模式切换信道。在媒介保留机制中也会用到定时信息。

除了工作站内部的定时，基本服务区域中的每个工作站都必须保存一份定时同步功能（timing synchronization function，简称 TSF）的副本，该副本是与基本服务区域中所有其他工作站的 TSF 同步过的本地定时器。TSF 以 1-MHz 的时钟频率运作着，每微秒“作用”（tick）一次。Beacon 帧的另一个作用，就是定期对网络上的工作站发布 TSF 值。

在timestamp（时间戳）字段中，所谓“now”（现在）是指时间戳第一个位到达传送端物理层的时间。

Infrastructure 的定时同步

电源管理在infrastructure网络中相当简单，这是因为有接入点作为数据传输与电源管理功能的协调中心。在infrastructure网络中，定时功能也采取类似的做法。由接入点负责维护TSF时间，任何与之关联的工作站都必须将接入点的TSF视为有效而加以接受。

一旦接入点准备传送Beacon帧，接入点定时器就会被复制到Beacon帧的timestamp字段中。与该接入点关联的工作站会从所收到的Beacon帧中取得该值，不过会稍作调整，将天线与收发器的处理时间纳入计算。与接入点关联的工作站会维护内部的TSF定时器，因此即使漏失掉某个Beacon帧，也可以粗略地与整体的TSF维持同步。无线媒介充满噪声是可以预料的，而Beacon帧无需加以确认。因此，经常会遗失Beacon帧早在预料当中，工作站内部的TSF定时器可以减小偶尔遗失Beacon帧所造成的影响。

为了协助进行主动扫描的工作站符合BSS所要求的参数，定时值也会出现在Probe Resonse（探查响应）帧中。当工作站借由扫描发现一个网络时，就会从该网络的Beacon或Probe Response帧记录下timestamp及收到timestamp时本地定时器的值。为了将内部的定时器调整到与网络定时器相符，工作站会随即从所收到的网络公告中取出timestamp，然后加上收到该timestamp后经过的时间。图8-19显示了整个过程。

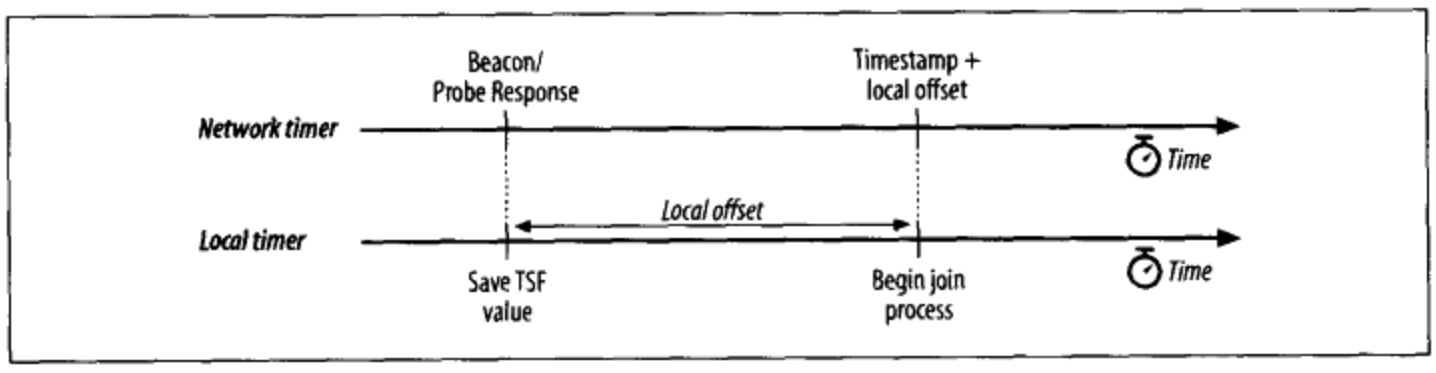


图8-19：让本地计时器与网络定时器匹配

IBSS 的定时同步

IBSS并不存在中央协调单元，因此Beacon是由工作站轮流传送的。TSF的维护工作属于Beacon生成过程的一部分。时间会被切割成相当于信标间定时期（inter beacon timing period）的片段。Beacon帧预期会在信标间隔结束时发送，这就是所谓的目标信标传送时间（target Beacon transmission time，简称TBTT）。independent（独立型）网络是以TBTT作为导引方针。

IBSS中所有工作站会准备在目标时间（target time）传送Beacon帧。当目标时间接近时，所有其他传送都会暂停。Beacon或ATIM除外，所有的帧传送定时器均会中止并等候媒介清空，以便传送更重要的管理帧。IBSS中所有工作站都会为Beacon传送产生一个backoff（退避）定时器。所谓backoff定时器，是介于0与该媒介minimum contention window（最小竞争窗口）两倍时间的随机迟延（时间）。TBTT结束后，所有工作站即将Beacon backoff定时器的值倒数至0。如果工作站在其传送时间之前就收到Beacon帧，预定要进行的Beacon传送就会被取消。

在图8-20中，每个工作站各自选择了一个随机延迟值，Station2所生成的随机延迟值最小。当Station 2的定时器超时，即会传送一个Beacon（信标）帧，此时Station 1与Station 3均会收到该帧。因此，Station 1与Station 3均会取消Beacon的传送。由于定时器同步可以确保所有工作站的定时器均已“对时”，所以同时出现几个Beacon帧并不会造成问题。接收端只要多处理几次Beacon帧，多更新几次TSF定时器即可。

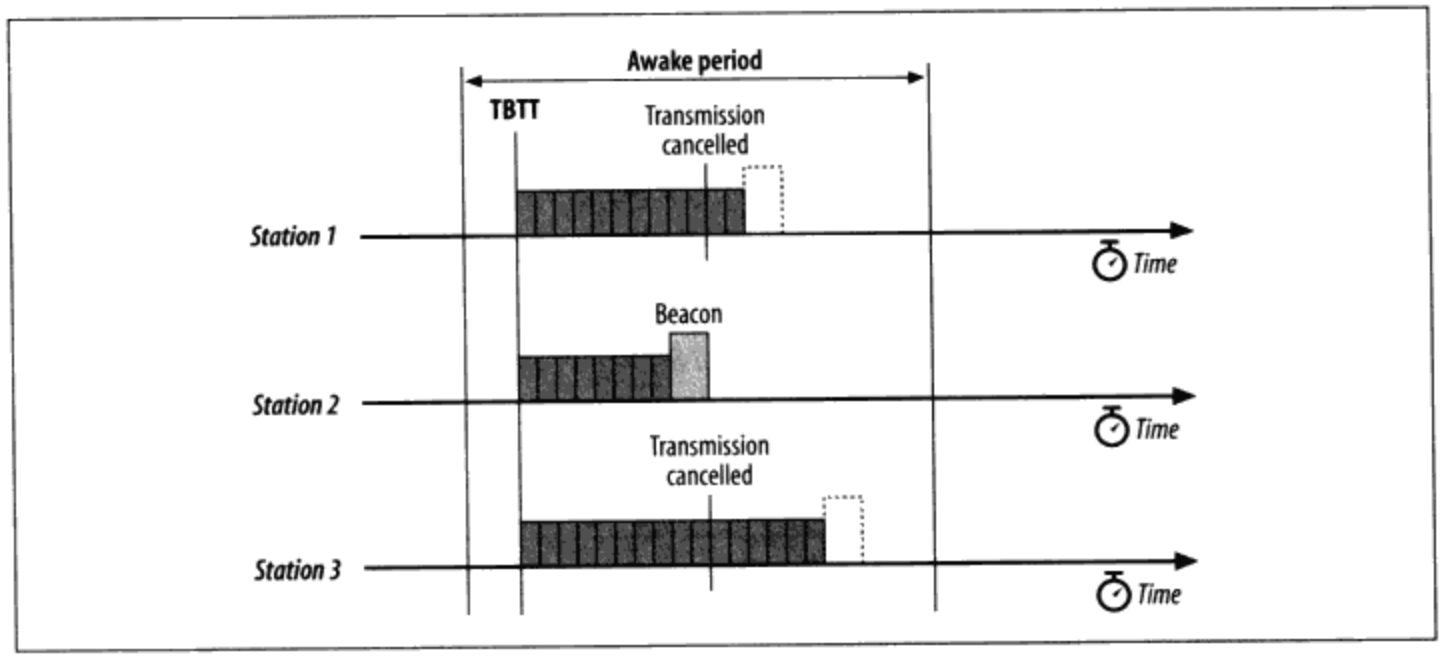


图8-20：轮流产生Beacon

Beacon的生成与电源管理的关系十分密切。Beacon帧的发出时间必须在每个Beacon interval的作用期间，如此一来，所有工作站才能同时醒着处理该帧。此外，帧的发送端不可进入低功耗（low-power）状态，必须一直保持清醒，直到下一个作用周期结束。这个规则能够确保至少有一个工作站处于清醒状态，以便响应正在进行扫描、准备加入网络的新工作站。

在independent网络中，是否采用所收到的timestamp的判断规则比较复杂。既然没有中央标准时间，802.11标准的做法是采用BSS中运行频率最快的定时器。收到一个Beacon帧之后，该timestamp会被稍作调整并计算处理时所耗费的延迟时间，然后与工作站内

部的 TSF 比较。只有当收到的 timestamp 晚于本地定时器，才会以该 timestamp 更新本地定时器。

频谱的管理

802.11a 原本只是针对美国所开发的标准。欧洲对于 5 GHz 频段的管制较为严格，因此若要适用于欧洲，就必须对 802.11 MAC 进行特别的修改。这项操作的开发成果最后在 2003 年成为 802.11h 标准。

传输功率控制（TPC）

欧洲管理者要求使用传输功率控制（Transmit Power Control，简称 TPC）（注 3），是为了确保5 GHz频段的无线电波发射器符合功率限制以及避免干扰特定的卫星服务。能够更精确地控制传输功率同时带来其他好处，其中一些是移动电话产业早已熟知的。高功率的客户端传输可以涵盖非常大的范围。在接入点密集的网络中，高功率工作站的传输距离或许大于所需。传输距离较长不见得都是好事。以高功率运作的无线电波发射器会缩短电池的使用时间。如果传输距离大于所需，额外可及的范围就代表“浪费掉”的功率。功率较大也可能导致网络吞吐量下降，因为客户端设备之间会产生不必要的干扰。

为了说明高功率工作站所导致的问题，请参考图 8-21。图中的网络配置了 9 个接入点（注 4）。Client#1 关联到了位于第一行中央的接入点。如果该工作站设定以最大功率进行传输，那么传输距离将可到达外圈所标示的范围。不过，它和接入点之间的传输只需要用到内圈的功率。两个同心圆之间的差异就是超出的传输范围。无线电波发射器使用高于必要的功率，将会比使用适当功率更快消耗电池的使用时间（为了延长手机电池的使用时间，移动电话网络已经采用功率控制技术多年了）。

控制传输距离也可以让网络运作得更加顺畅。所有传输操作都必须取得无线电波媒介的独家使用权。如果功率过高，传输操作涵盖的范围就会超出所需。位于外圈之内使用 11 信道的任何工作站都会因为Client#1 正在进行传输而受到影响。最佳传输功率与额外功率之间的阴影区表示受到影响的地带，因为 Client#1 正以过高的功率进行传输。例如，Client#2 这时就无法与邻近的接入点进行传输，因为它必须和Client#1 共享无线电波媒介。降低传输功率到适可而止的水平可避免邻近接入点之间产生重叠，从而改善整体吞吐量。

注 3： ERC/DEC/(99)23 可从 *http://www.ero.dk/doc98/Official/Pdf/DEC9923E.PDF* 取得。

注 4： 配置 9 个接入点的网络中只规划了使用三个非重叠信道是不可能的，这就是在接入点密集的环境中应该使用 802.11a 的最佳理由。

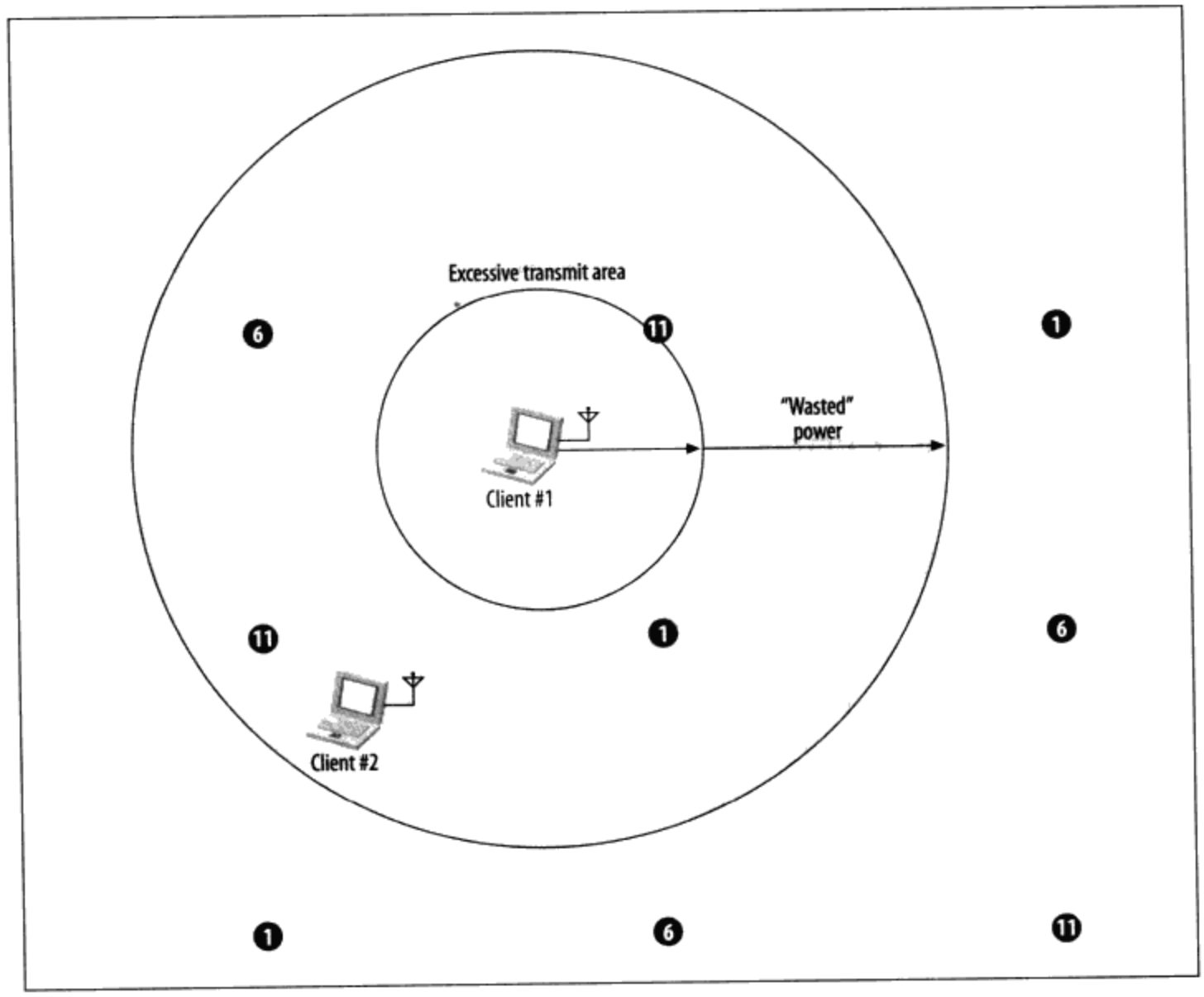


图 8-21：高功率工作站与多个接入点间的干扰

传输功率控制的基本操作方式

传输功率控制（TPC）是一项 802.11 服务，主要是为了尽量降低传输功率至可用水平。除了考虑管理者所允许的最大功率，还会考虑到其他限制。虽然设计上是为了满足管理者的要求，但传输功率控制也会带来其他好处。

任何无线电波传输的绝对上限是由管理者规定，通常列在管理者所出版的相关文档或法规中。最大管制功率可以在接入点或工作站中加以设定，也可以从包含 Contry 信息元素的 Beacon 帧中得知。此外，无线电波的传输或许还有其他进一步限制最大传输功率的规范。欧洲管理者的规定更为严格，他们要求必须至少再降低 3 dB 以避免干扰卫星服务。

最大传输功率是由Beacon帧中的Country信息元素所指定，因此任何关联到网络的工作站均可得知。Contry信息元素用来指定最大管制功率（regulatory maximum power），至

于 Power Constraint 信息元素则是用来指定网络可以使用的最大传输功率（maximum transmission power），这个数值通常较低。

开始操作之前，工作站必须计算出可以使用的最大传输功率。通常，它的计算方式是以最大管制功率减去任何额外的限制。例如，网管人员或许会指定本地网络所允许的最大传输功率以缩短传输距离并避免干扰。

关联过程的改变

当具备频谱管理能力的工作站关联（或重新关联）到接入点时，首先必须在 Power Capability 信息元素中提供最小与最大的传输功率。接入点可以将工作站所提供的信息纳入关联过程中并且任意使用这些信息。至于接入点如何或是否使用这些信息，802.11 标准并未明确规范。功率过高以至于可能违反管理规定的工作站便有可能无法通过相关校验。接入点也可以拒绝传输功率性能太差的工作站，标准认为这会增加隐藏节点的可能性，虽然看上去不至于这样。

变更传输功率

接入点与工作站均可动态调整个别帧的传输功率。接收端可以计算出每个帧的链路边界（link margin），也就是把接收到的功率减去最低可接受值。链路边界就是安全边界。如果接收到的传输功率只达工作站传输的最低可接受值，链路边界就等于零，这代表任何细微的变动均可能导致连接中断。大多数工作站均以缩小链路边界为目标，不过标准并未规定特定链路边界的计算方式以及使用何种特定值。

为了得知传输功率的改变，工作站可以要求进行无线链路测量（radio link measurement）。工作站可以送出一个 Action 帧要求提供传输报告。返回的 Action 帧中包含了一个 TPC Report 信息元素，其中有两项描述性的统计数据。首先，它包含了报告帧（report frame）本身的传输功率。根据此传输功率，接收端可以估算出无线链路的路径损耗（path loss）。其次，此汇报帧中包含链路边界值，告诉接收端已收到功率（received power）与最低可接受功率（minimum acceptable power）之间的比值。举例而言，假设最低可接受功率为 -70 dBm，而实际接收到的为 -60 dBm，那么链路边界即为 10 dB。如果链路边界值“太高”，就可以降低传输功率；如果链路边界值“太低”，就应该提高传输功率。和 802.11 标准的其他组成部分一样，“太高”或“太低”与否均留给软件自行决定。

在设计上，标准是用来确保最大传输功率不致逾越规定，但并未限制功率的选择方式。对于比较高级的功能，标准并没有提出特别的要求。不难理解为何有些支持传输功率控制的高级接入点会去追踪将无线电波送达每个已关联工作站所需要的功率，因为较近的工作站所需要的功率将小于较远的工作站。

动态选频（DFS）

除了传输功率控制之外，欧洲管理者也要求工作站必须避免干扰5 GHz的雷达系统以及将功率展开到所有可用信道中。动态选频（Dynamic Frequency Selection，简称DFS）机制便是用来完成这项任务。

DFS的基本操作方式

动态选频包含了一组步骤，可以让802.11设备根据测量结果（measurement）与管理需求（regulatory requirement）变更无线电波信道。它可以影响一开始的关联过程以及后续的网络操作。

当工作站首次关联到网络，Association Request帧里包含了一个Supported Channels信息元素，其中列出了工作站支持的信道。根据此信息元素的内容，接入点可以选择是否拒绝此项关联操作，虽然标准并未规范这种行为。有种做法是干脆拒绝那些支持“太少”（too few）信道的工作站，理论上是因为它会限制接入点切换信道的能力，因为接入点必须选用所有已关联工作站都支持的信道。

一旦用于实际的网络，DFS就会定期测试信道是否可能干扰其他无线电波系统，特别是5 GHz的欧洲雷达系统。测试信道时会暂停网络的所有传输操作，然后测量潜在干扰，如果有必要，就会广播即将更换信道。

信道静默

无线信道（radio channel）测试是在静默周期（quiet period）或静默间隔（quiet interval）内进行的。静默间隔是指BSS中的所有工作站暂时停止传输的时间，它有助于测量是否存在雷达系统的潜在干扰。静默周期是由Beacon与Probe Response帧中的Quiet信息元素进行安排，指定何时停止传输以及历时多久。唯有最新的Quite信息才算有效。如果同一时间内有好几个Quite信息，则最新的一份信息会取代之前所有已安排的静默周期。在静默间隔内，所有工作站都将网络分配向量（network allocation vector，简称NAV）设为静默周期的长度，确保虚拟载波监听算法会递延所有传输操作。

当已安排的静默周期即将来临，无线信道还是以正常的方式访问无线电波媒介，不过另外附加了一项规则，即在静默周期开始之前任何帧交换必须完成。如果已经排定的帧交换操作无法完成，工作站就会释放信道的控制权，等到静默周期结束后再继续传送。不过，静默周期所导致的帧传送失败会增加重传的次数。当静默周期结束，所有工作站必须再次竞争访问无线信道。没有所谓跨静默周期的信道访问。

在基础结构型网络里，信道静默的安排完全由接入点控制。接入点可以决定静默周期的

长短、静默间隔相隔多久，甚至是完全停用。独立型网络是在网络成立时选择静默周期的安排。轮到新工作站负责发送 Beacon 与 Probe Response 帧时也无法改变静默周期参数，只能沿用之前的参数。

测量

任何时刻都可进行无线信道测量。工作站可以要求其他工作站进行无线信道测量。来自工作站的测量信息对接入点而言特别有用，因为这些提供报告的工作站可能分布在各个不同的地理位置。不论是否在静默期间，均可以进行测量操作。

任何工作站均可要求其他工作站进行测量。此要求是通过 Measurement Request 帧来发送，如图 8-23 所示。基础结构型网络里的所有帧都必须流经接入点。已关联的工作站只能请求接入点提供无线电波信息。只要适时发出请求帧，基础结构型网络里的接入点即可请求单一或一组工作站用于测量。独立型网络并没有中枢控制单元，因此任何工作站都可发出请求给单一或一组工作站。虽然允许使用组地址字段来提出请求，不过接到请求的工作站也可以不予理会。

送出测量请求后，工作站会假设对方需要一些时间来为它的响应搜集数据。送出测量请求后，工作站不得再发送任何其他帧。

接收到 Measurement Request 帧后，工作站必须判断如何响应。Measurement Request 帧非得到响应不可，即使响应的内容是拒绝测量。要进行处理，测量请求必须有足够的时间进行设定与测量。测量请求中会指定进行测量的时间。如果请求被置于队列的同时正在进行冗长的传输，不难想象它会在请求测量的时间点之后才到达目的地。工作站可以不理会这些“迟到”的请求。接收到测量请求的一方必须搜集请求中所指定的数据。能否支持所有请求视接收端的硬件而定。并非所有 802.11 硬件均能够支持多信道操作，虽然这种情况已经日渐减少（注 5）。如今，市面上还是有些卡片不支持多信道操作，因此无法应付测量当前操作信道以外的请求。工作站可以因为其他不明原因而拒绝测量，除非提出的一方强制请求（mark the request as mandatory）。

除了要求进行测量的询问操作，就算无人提出要求，工作站也可以主动发送 Measurement Report 帧，提报相关的统计数据。

雷达扫描

要求信道静默的一个主要理由，是为了搜寻是否存在欧洲所使用的 5 GHz 雷达系统。至

注 5：　例如采用 Radiata 芯片组的 Cisco CB-20 网卡只能够支持 8 个较低的 802.11a 信道。这类卡片就应当拒绝较高的 U-NII 频段的测量要求。

于采用何种搜寻方式，管理者并未强制规定（注6）。管理者只要求当信号强度超过某个特定干扰阈值时，就必须进行雷达检测。

启用无线接口时，必须搜寻所使用的信道是否存在雷达信号。除非“毫无危险”（coast is clear）且确定附近没有雷达会被干扰，否则不允许进行传输。操作过程中必须定期进行雷达检测。一旦检测到雷达信号，网络就必须进行信道切换以避免干扰。

频谱管理服务允许网络切换到其他信道。之所以决定切换信道，或许是因为出现雷达干扰，不过除了用来符合欧洲的无线电管理，信道切换机制还有其他用处。有能力变更操作的信道的网络，可以把对其他802.11设备的干扰降至最低，因此可以优化无线电波的使用计划。信道切换是设计来尽可能将已关联的工作站移往新的信道，不过和其中一些（甚至是所有）工作站的通信还是可能因此而中断的。标准中并未限制该如何选择新信道，只是提到接入点应该尝试选用多数工作站均支持的信道。有些管理者已经草拟出一些规定，强制必须将无线电波能量展开至整个频段，如此一来，管理规定强迫切换的信道有可能无法得到所有工作站的支持。

在基础结构型网络里，操作信道的选择完全由接入点控制。作为关联过程的一部分，接入点会搜集已关联工作站支持哪些信道。接入点将通过管理帧以及Action帧中所包含的Channel Switch Announcement（信道切换声明）信息元素，通知已关联的工作站何时将进行信道切换。为改善接入点传送信道切换声明的能力，可以在PCF帧间间隔（PIFS）之后随即传送信道切换声明。如此一来，相比较于媒介的基本操作，它就具备了较高的优先级。标准建议但并未要求信道切换必须提供充分的准备时间，好让处于省电状态的工作站有机会恢复操作并且接收信道切换声明。

IBSS操作

相比较于基础结构型网络，要在独立型网络中变更操作的信道显然比较困难，因为没有逻辑上的控制单元可以进行频率选择操作。独立型网络并没有接入点内置的功能，而是通过DFS *owner service*（动态选频负责人服务）来协调各个工作站来执行频率选择服务。

网络中会有一个工作站被指定为DFS owner，负责搜集测量报告以及监控信道中是否出现雷达信号。如果独立型网络中有任何一个工作站检测到雷达信号，就会在信道映射的子字段中汇报。一旦被告知检测到雷达信号，DFS owner就会进行切换信道的动作。

DFS owner负责决定使用哪个新信道并且送出信道切换声明帧。有时候也许无法选出一个既符合规范要求，又同时为所有工作站支持的信道。独立型网络并不存在搜集数据的中枢单元，因此就算所有工作站均支某个特定信道，也无法保证DFS owner有办法知道。

注6： ETSI EN 301 893可从*http://www.etsi.org*取得。

在独立型网络中，DFS owner 有可能改变。就像 Beacon 信号的生成，工作站可能在网络来来去去（join or leave the network），DFS owner 也一样。万一 DFS owner 离开网络，所有工作站就会进入 DFS owner 恢复模式（recovery mode）。在这个模式中，可以有好几个工站同时担任 DFS owner 并且安排产生标准所要求的信道切换声明帧。不过，第一个传送信道切换帧的工作站才会成为 DFS owner，其他工作站则会放弃这个角色。DFS owner 恢复的概念类似图 8-20 所讨论的分布式 Beacon 帧的产生过程。

Action 帧

Action（行动）帧用来要求工作站采取必要的动作。频谱管理服务使用 Action 帧提出测量请求、搜集测量的结果以及声明任何必要的信道切换。图 8-22 显示了 Action 帧的格式，基本上它是一个category字段加上category的动作细节。动作细节将会因为category字段值的不同而有所变动。

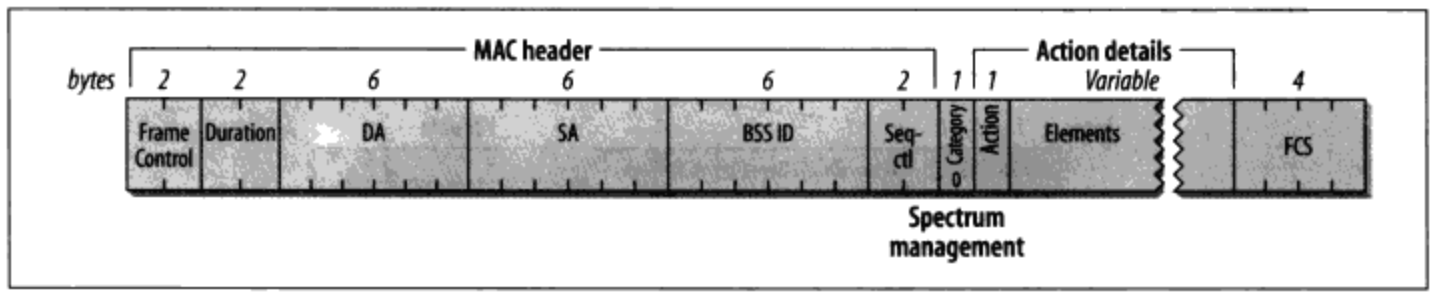


图 8-22：Action 帧

Category（种类）

设定为 0 代表频谱管理。

Action（动作）

所有频谱管理帧均使用动作细节的第一个字节来指定即将采取的动作类型。表8-2列出了 Action 字段所有可能的值，没有列出的值代表保留未用。

Elements（元素）

频谱管理动作帧是以信息元素（Elements字段）来承载信息。多数信息元素的细节详见第四章。一些额外的信息元素定义于 802.1h 并将于本节予以探讨。

表8-2：频谱管理动作帧类型

值	频谱管理动作帧的类型
0	测量请求（Measurement Request）
1	测量报告（Measurement Report）
2	传输功率控制请求（TPC Request）

表8-2：频谱管理动作帧类型（续）

值	频谱管理动作帧的类型
3	传输功率控制报告（TPCReport）
4	信道切换声明（Channel Switch Announcement）

Measurement Request 帧

Measurement Request（测量请求）帧用来请求工作站进行测量并将结果返回。它的格式如图8-23所示。此帧是由一系列测量请求信息元素组成。可测量的项目受到帧的大小而非其他因素的限制。

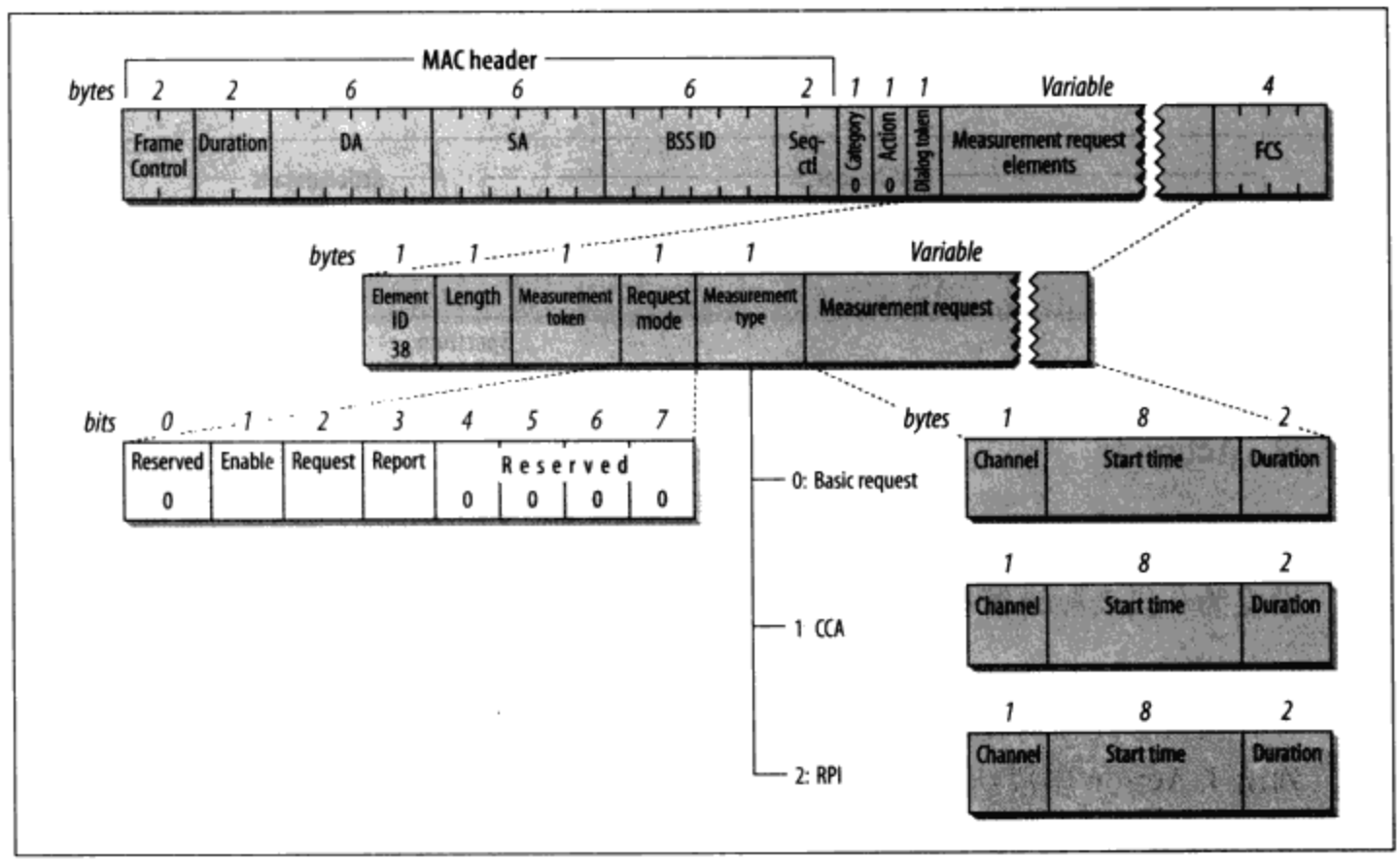


图8-23：Measurement Request 帧

标准允许定期进行测量。如要启用或停用定期报告，可以传送一个测量请求来指示工作站启用或停用定期测量。基础结构型网络里的工作站无法要求接入点停用测量功能。

Category（种类）

设定为0代表频谱管理动作帧。

Action（动作）

设定为0代表测量请求。

Dialog Token（对话标志）

此字段的作用如同序列号。它会被设定为非零值来协助将测量响应对应至现有的请求。

单独一个 Measurement Request 帧可以请求多次测量，只要在帧主体中使用多个 Measurement Request 信息元素即可。如图 8-23 所示，每个信息元素由以下字段组成：

Element ID（元素标识符）

Measurement Request 元素的类型编号为 38。

Length（长度）

此字段之后的信息元素的长度，以字节为单位。

Measurement Token（测量标志）

每个Measurement Request帧可以同时包含好几个请求，只要在帧主体中涵括多个 Measurement Request元素即可。每个请求均会被赋予一个测量标志值，如此才有办法区别不同的请求。

Measurement Request Mode bitmap（测量请求模式位映射）

在 Measurement Request Mode bitmap 中有 3 个位用来指定帧支持哪些类型的频谱管理帧。位编号 2（从 0 开始编号）代表 Request 位，设定为 1 是指传输器将处理传进来的测量请求。位编号 3 代表 Report 位，设定为 1 是指传输器将接受多余的报告。当这两个位都有效时，Enable 位会被设定为 1。

Measurement Type（测量类型）

信息元素中所要求的测量类型，如表 8-3 所示。

Measurement Request（测量请求）

如果有测量请求，就会额外以一个字段来指定定时参数。目前已经标准化的三种测量均有相同的格式，由信道编号、测量开始时间的定时器函数值以及测量持续时间所构成。定时器的初始值如果为零，代表应该立即进行测量。如果所发出的帧是用来启用或停用测量功能，这个字段就不会出现。

表8-3：测量类型值

测量类型值	名称
0	基本测量（basic measurement）
1	空闲信道评估（clear channel assessment，简称CCA）
2	接收功率指示（receive power indication，简称 RPI）柱状图

Measurement Report 帧

Measurement Report（测量报告）帧用来发送测量结果给提出请求者，它的格式如图8-24所示。此帧由一系列测量报告信息元素组成。可测量的项目受到帧的大小而非其他因素的限制。

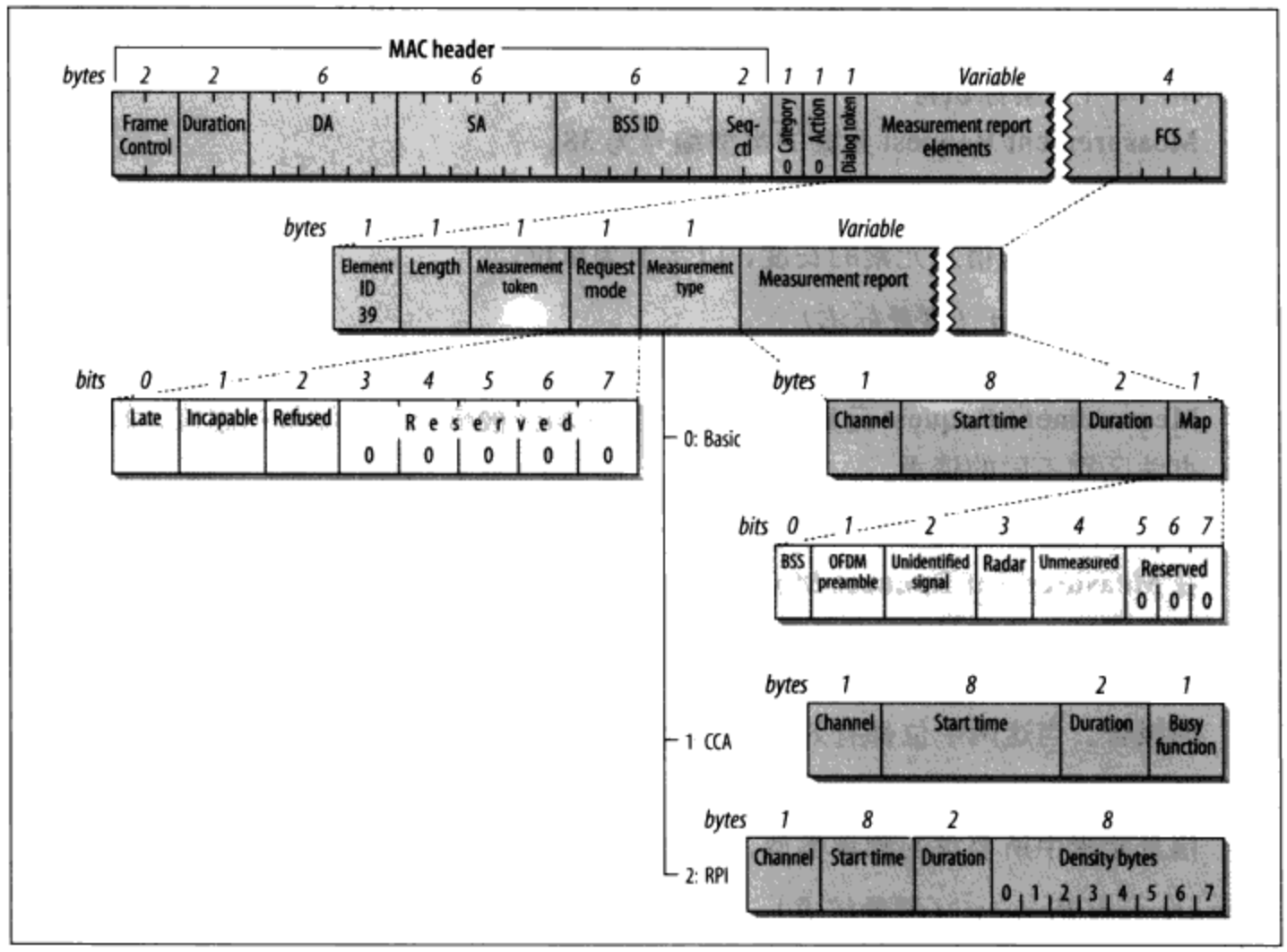


图8-24：Measurement Report 帧

Category（种类）

设定为0代表频谱管理动作帧。

Action（动作）

设定为0代表测量报告。

Dialog Token（对话标志）

如果此测量报告用来响应另一个工作站的测量请求，请求帧中的Dialog Token字段就会被复制到响应信息中。如果此帧是主动发送的报告（unsolicited report），则Dialog Token为0。

单独的Measurement Report帧中可以包含数个测量结果，各自以本身的信息元素进行传

送。为了清楚起见，信息元素标头中只显示了一个信息元素，其所包含的3个可能的报告元素如下所示。

Element ID（元素标识符）

Measurement Report 元素的类型编号为39。

Length（长度）

此字段之后的信息元素的长度，以字节为单位。

Measurement Token（测量标志）

每个Measurement Request帧都可以提出数个请求，只要在帧主体中包含数个Measurement Request元素即可。每个请求均会被赋予一个测量标志值，这样才有办法区别不同的请求。

Measurement Report Mode bitmap（测量报告模式位映射）

在Measurement Report mode bitmap中有3个位用来指定为什么测量请求被拒绝，如果报告帧被用来拒绝测量的话。如果测量请求到达时已经超过指定的开始时间，Late位就会被设定为1。如果工作站能力不足，Incapable位就会被设定为1。如果工作站有能力但不愿进行测量，Refused位就会被设定为1。

Measurement Type（测量类型）

信息元素可以请求的测量类型，如表8-3所示。

Measurement Report（测量报告）

Measurement Report帧包含了请求测量的数据。和Measurement Request不同，每种报告的内容均不相同。所有3种报告均显示于信息元素标头之下。它们共享通用的标头，此标头用来报告测量请求所指定的信道数、开始进行测量的时间以及测量持续时间。不过，每种测量类型的报告方式均不相同。

在*basic*（基本）报告中，显示的数据是一系列跟信道有关的位标记：

BSS（1个位）

如果在测量期间检测到来自其他网络的帧，此位将被设定。

OFDM Preamble（1个位）

如果检测到802.11a的短训练序列，但帧的其余部分并未伴随出现，此位将被设定。HIPERLAN/2网络使用一样的前导码，但帧构造并不相同。

Unidentified Signal（1个位）

当接收到的功率够高，但无法分辨究竟是来自其他802.11网络（因此必须设定BSS位）、OFDM网络（因此必须设定OFDM Preamble位）还是雷达信号（因此必须设定Radar位），此位将被设定。标准并未规范功率电平（power level）多高才应该设定此位。

Radar（1 个位）

如果在测量期间检测到雷达信号，此位将被设定。需要检测哪些雷达系统由管理者规定，而非 802.11 任务小组。

Unmeasured（1 个位）

如果未对信道进行测量，此位将会被设定。如果没有进行测量，当然不会在频段中检测到任何信号，因此前 4 个位均将被设定为 0。

在 *CCA*（空闲信道评估）报告中，主要字段是 CCA Busy Fraction，用来描述空闲信道评估功能被设定为忙碌的时间。它的长度为 1 个字节，因此这段时间会被乘上 255，以范围 0 到 255 的整数来表示，数值较高代表信道经常是忙碌的。

RPI histogram（RPI 柱状图）报告用来汇报接口收到的功率的分布情况。工作站可以请求一份 RPI histogram 报告，用来判断其他工作站从当前网络所取得的信号强度，或者在即将切换操作的信道时使用这项报告来对其他信道进行评估。RPI histogram 报告中包含了收到的信号的强度信息。和单一帧测量不同的是，它能够显示整个测量期间所收到的信号的功率分布情况，让接收端可以了解整体的传输水平。Histogram 包含了 8 个字节，每个字节代表所收到的信号的功率范围，如表 8-4 所示。每个字节的值代表信号落在该范围的功率分数（fraction of power）。所收到的信号落在此字节所代表的功率范围的时间分数（fraction of time）以 0 到 255 范围内的值来表示，这些值的大小因各功率电平所收到的信号的时间分数而定（注 7）。

表 8-4：RPI 功率对应表

RPI 编号	相应功率（dBm）
0	小于 -87
1	-87~-82
2	-81~-77
3	-78~-72
4	-71~-67
5	-66~-62
6	-61~-57
7	-56 以上

注 7：虽然理论上每个字节的值最高只到 255，不过标准中提到，由于取近似值的缘故（rounding effect），有时候可能会累计到 262。

TPC Request 帧与 TPC Report 帧

TPC Request帧与TPC Report帧如图8-25所示。两者都很简单，由频谱管理类型的Action帧组成。每个帧包含其所对应的信息元素，如第四章所述。和其他帧一样，Dialog Token字段用来匹配请求与响应。

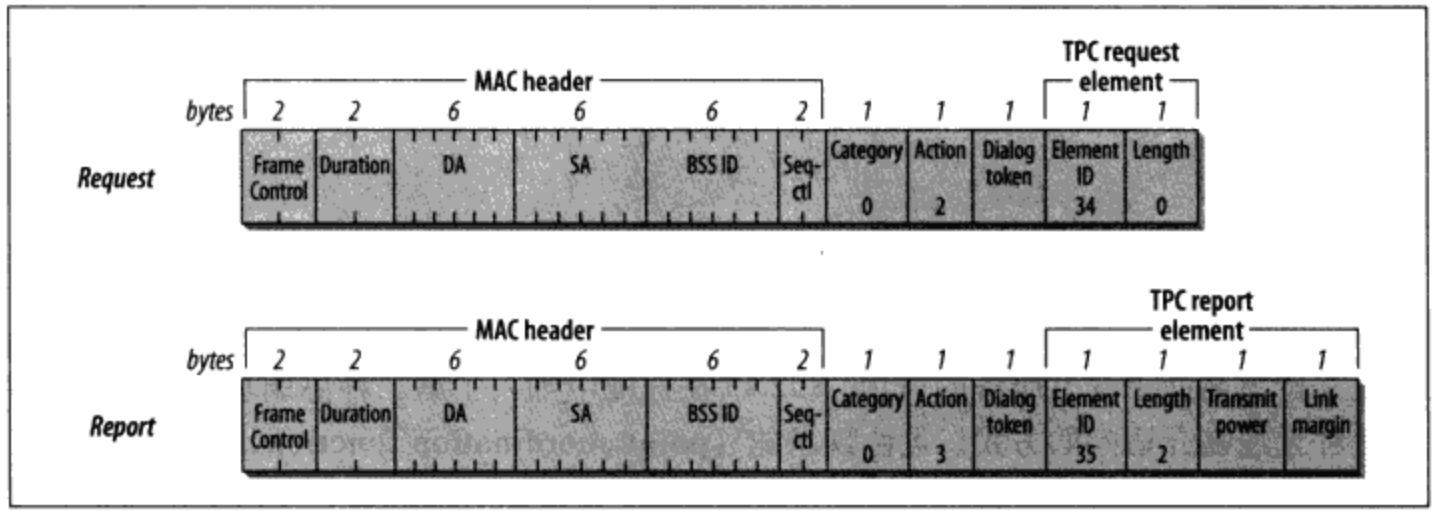


图 8-25：TPC Request 帧与 TPC Report 帧

Channel Switch Announcement 帧

必须变换信道时就得通知网络上各个工作站，让它们准备切换到所指定的新信道。图8-26所显示的Channel Switch Announcement（信道切换声明）帧基本上是以Action帧封装第四章所描述的Channel Switch Announcement信息元素，因此它们都具备信道切换声明元素的所有功能，用来指定网络即将切换至新信道的时间。

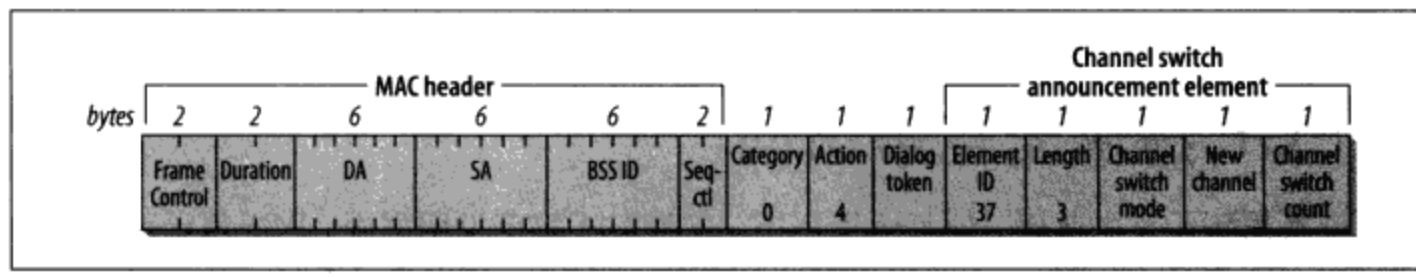


图 8-26：Channel Switch Announcement 帧

第九章

PCF无竞争服务

为了支持需要近乎实时服务的应用，802.11在标准中加入了第二种协调功能，以提供另外一种无线媒介访问的方式。点协调功能（point coordination function，简称PCF）可让802.11网络提供较为“公平”的媒介访问机制。就某些方面而言，以PCF访问媒介有点类似令牌式(token-based)媒介访问控制机制，由接入点掌控令牌。本章主要说明PCF的媒介访问、PCF帧的解析图以及电源管理与PCF的交互操作。

实际上，PCF并未广泛使用。有一款家用媒体服务器（media server）在产品中实现了PCF功能，然而销售情况并不理想。有些企业级产品之所以使用PCF，是因为在控制无线媒介的访问方面，PCF可以赋予接入点更大的权限。就算某些蛮横的工作站使网络陷于无政府状态，PCF也可以协助取回网络控制权。本章对某些读者来讲可能无关痛痒，如果目前使用的产品并不支持PCF功能，就没有必要阅读本章，除非各位对标准本身感兴趣。

以PCF提供无竞争访问

如果需要用到无竞争传输，便可运用PCF。在802.11规范说明书中，PCF属于可选择的(optional)，实际产品不一定非得实现这项功能。IEEE之所以设计PCF，是为了让仅具备分布式协调功能（distributed coordination function，简称DCF）的工作站能够与点协调单元（point coordinator）交互运作，彼此相容。

无竞争服务（contention-free service）并非随时供应。无竞争服务时间的长短是由点协调单元负责仲裁，并与标准的分布式服务（DCF-base service）交相运用。无竞争周期(contention-free period)的长短是可以设定的。802.11规范说明书将无竞争周期描述为“近乎等时的”(near isochronous)，因为无竞争周期并非总是在预期时间内开始，如“无竞争周期的持续时期”（Contention-Free Period Duration）一节所述。

无竞争服务采用中央访问控制机制，只有点协调单元可以访问媒介。所谓点协调单元，是接入点中实现的一项特定功能。与之关联的工作站只有在点协调单元允许的情况下才可以传送数据。在某些方面，通过PCF进行无竞争访问有点类似于令牌式（token-based）网络协议，只是协调单元的轮询（polling）取代了令牌。不过，802.11模型的基础仍在。虽然访问是由某个中央单元控制，但所有传送均需得到确认。

PCF 操作

图 9-1 显示了利用 PCF 进行传送的范例。使用 PCF 时，媒介时间会被划分为无竞争周期（contention-free period，简称 CFP）以及竞争周期（contention period，简称 CP）。无竞争周期的媒介访问受到 PCF 的控制，而竞争周期则是由 DCF 以及第八章所提到的规则所控制。竞争周期不能过短，至少要能够传送一个最大帧（maximum-size frame）及其相关的确认。无竞争服务与竞争服务以固定周期交替，两者合称为无竞争重复间隔（contention-free repetition interval）。

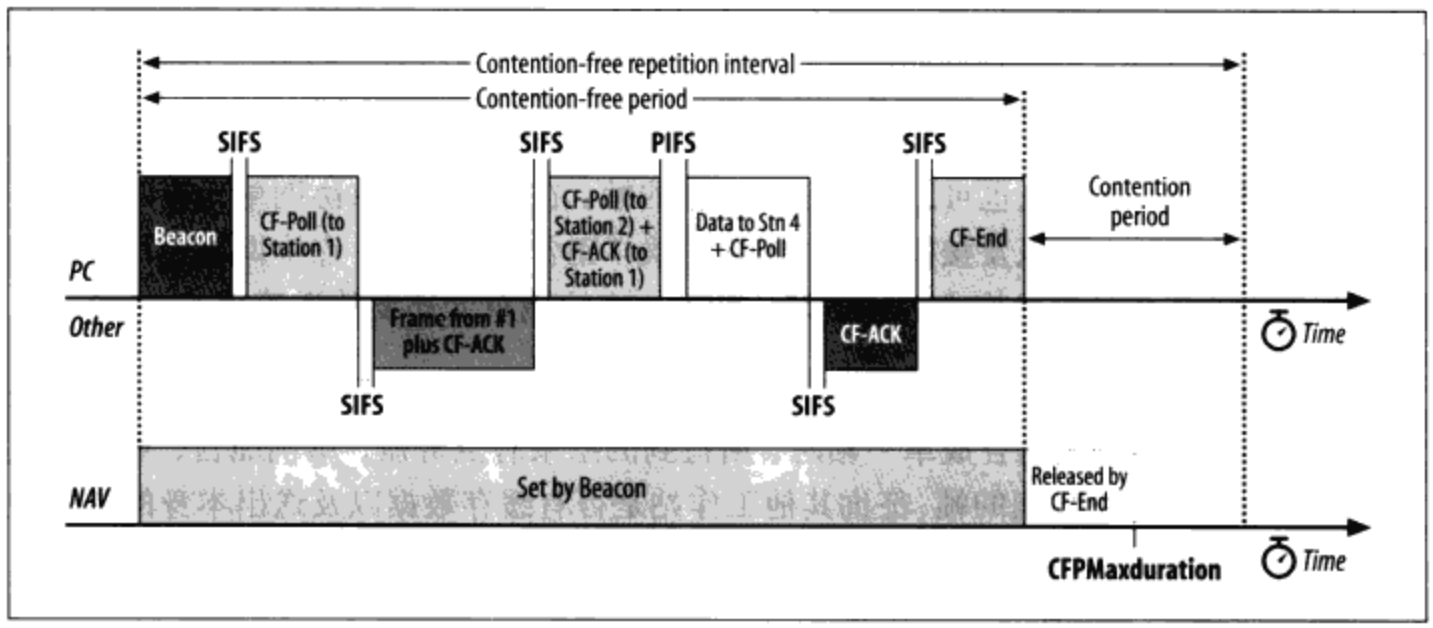


图 9-1：PCF 的运用

于无竞争周期内保留媒介使用权

无竞争周期一开始，接入点就会送出一个Beacon帧。该Beacon帧中的CFPMaxDuration（无竞争最大持续期间）字段，用来标明无竞争周期最长持续多久。所有收到此Beacon的工作站会将 NAV 设定为此时间值，并将 DCF 媒介访问排除在这段期间之外。

为了避免干扰，所有无竞争传输会另外以SIFS（短帧间间隔）与PIFS（PCF帧间间隔）加以隔离防护。这两者都比 DCF 帧间间隔短，因此在 DCF 周期内没有其他 DCF 工作站可以访问媒介。

轮询列表

接入点接管无线媒介之后，会根据轮询列表（*polling list*）分别询问与之关联的工作站是否有数据待传。在无竞争周期内，除非关联以轮询帧提出请求，否则工作站不得传送数据。无竞争轮询帧通常简写为CF-Poll。一个CF-Poll帧代表授权传送一个帧。除非接入点送出多次轮询请求，否则每次只能传送一个帧。

轮询列表所列出的都是无竞争周期内受邀传送帧的特权工作站。工作站一旦与接入点关联，就会被列在轮询列表中。Association Request（关联请求）包含了一个字段，用来表明该工作站能否在无竞争周期内响应轮询。

来自接入点的传输

通常在无竞争周期内，所有传输都只以SIFS（短帧间间隔）加以隔离。为了确保点协调单元掌握了媒介控制权，如果经过一段PIFS（PCF帧间间隔）未得到回复，就会继续询问列表中下一个工作站。如图9-1所示，接入点询问列第二个工作站，但是没有得到响应。等候一段PIFS（PCF帧间间隔）后，接入点会继续询问列表中的第三个工作站。利用PIFS（PCF帧间间隔），接入点得以确保本身持续掌控媒介访问权。

在无竞争周期内，接入点也可以使用不同类型的帧。在此期间，点协调单元有四项主要任务。除了传送缓存帧以及接收工作站响应之类“正常的”任务，点协调单元可以征询轮询列表中的工作站以允许它们传送帧。此外，点协调单元还要传送管理帧。

在无竞争周期内时间十分宝贵，因此可以将确认信息、轮询及数据传送组合在一起以提高效率。当这三种功能结合成单一帧时，所得到的结果有点奇怪。举例而言，单一帧就可以同时确认之前所收到的帧、征询其他工作站是否有缓存数据以及送出本身的数据给轮询列表所列的工作站。

在无竞争周期内可以使用下列帧：

Data（数据）

当接入点要送出一个帧给工作站但是不必确认之前所传送的信息时，就会使用标准的数据帧。标准的数据帧并不会征询对方是否有数据待传，因此不允许接收端传送任何数据。无竞争周期所使用的纯数据（Data-Only）帧和无竞争周期所使用的数据帧完全相同。

CF-ACK（无免竞争周期的确认）

如果没有数据待传，工作站会以此帧确认之前所收到的帧。无竞争周期的确认信息比标准控制帧的确认信息长，因此实现时可能不会使用此帧。

CF-Poll（无竞争周期的轮询）

CF-Poll帧是由接入点发送给移动式工作站的，用来赋予移动式工作站传送一个缓存帧的权力。只有当接入点没有数据要传给移动式工作站时才会使用这个帧。如果尚有数据要传给移动式工作站，接入点会改用 Data+CF-Poll 帧类型。

Data+CF-ACK

此帧结合了数据传送以及确认信息。数据是针对帧接收者发送的；确认信息则是针对之前传送的帧，通常和数据接收者无关。

Data+CF-Poll

接入点使用此帧传送数据给某移动式工作站，然后请求对方传送一个待传帧。Data+CF-Poll 只能够在无竞争周期内由接入点发送。

CF-ACK+CF-Poll

此帧除了会确认接入点最近从某个工作站所收到的帧，同时会要求轮询列表中下一个工作站传送一个缓存帧，虽然所确认的对象可能是任何一个关联此接入点的移动式工作站。

Data+CF-ACK+CF-Poll

此帧将数据传送、轮询功能以及确认信息结合成单一帧，为的是达到最高效率。

CF-End

此帧用来终止无竞争周期以及将媒介控制权交回 DCF 竞争机制。

CF-End+CF-ACK

此帧与 CF-End 帧相同，不过它同时确认了之前所收到的数据帧。

任何管理帧

802.11标准并未限制无竞争周期不能使用哪些管理帧。任何特殊类型的帧只要合乎传送规则，接入点都会加以传送。

无竞争周期的持续时间

CP（竞争周期）再短，至少也要能传送一个最大的帧以及得到相应的确认。不过，基于竞争的服务也有可能超出竞争周期。若基于竞争的服务超出CFP（无竞争周期）预定的开始时间，CFP 就会被压缩，如图 9-2 所示。

如果CFP（无竞争周期）被压缩，在以Beacon（信标）声明无竞争操作开始之前，还是允许正在进行中的帧完成交换。CFP被压缩多少时间，取决于延迟多久。无竞争服务的结束时间不能晚于预定的开始点之后所允许的最长时间，该时间点称为目的信标传送时间（Target Beacon Transmission Time，简称 TBTT）。

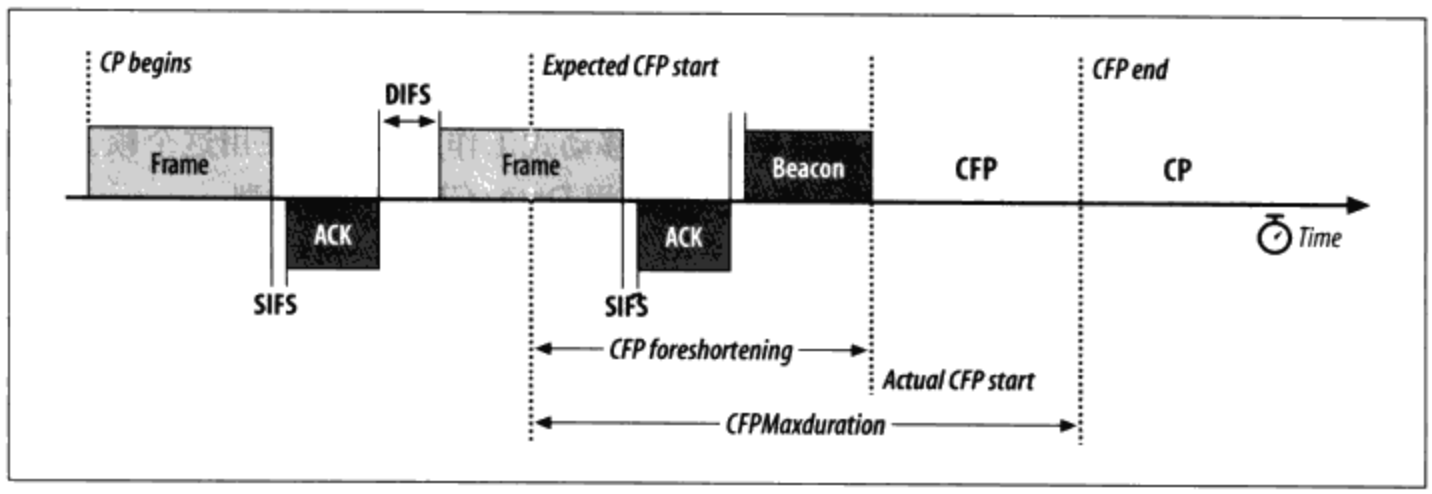


图 9-2：Data+CF-ACK 与 Data+CF-Poll 的用法

点协调单元（point coordinator）也可以送出一个 CF-End 帧，在超过最大持续期间（maximum duration）之前中止无竞争周期（CFP）。它可以根据轮询列表的长短、流量负载或其他接入点认为重要的因素来作出中止决定。实际产品有时候可以选择性地使用 PCF（点协调功能）来交换特定的帧，启用无竞争服务后开始进行帧传送，然后予以中止。

PCF 帧的封装细节

某些类型的帧只能在无竞争周期（CFP）内使用。数据传送、确认与询问可以组合成单一帧。本节主要描述何时使用哪种组合帧，以及在帧交换过程中不同功能之间如何互动。换言之，无竞争帧在单一帧里结合了数种功能。

Data+CF-ACK

Data+CF-ACK 帧结合了两种不同的功能以提高传输效率。此帧除了内含所要传送的数据，也同时确认了 SIFS（短帧间间隔）之前所收到的数据。通常，此帧内含的数据与确认信息是分别针对两个不同的工作站。图 9-3 中，工作站响应之前帧的 CF-ACK（无竞争确认）信息结合了打算传给接入点的数据，不过数据本身可能是要传给 802.11 网络中其他的工作站。

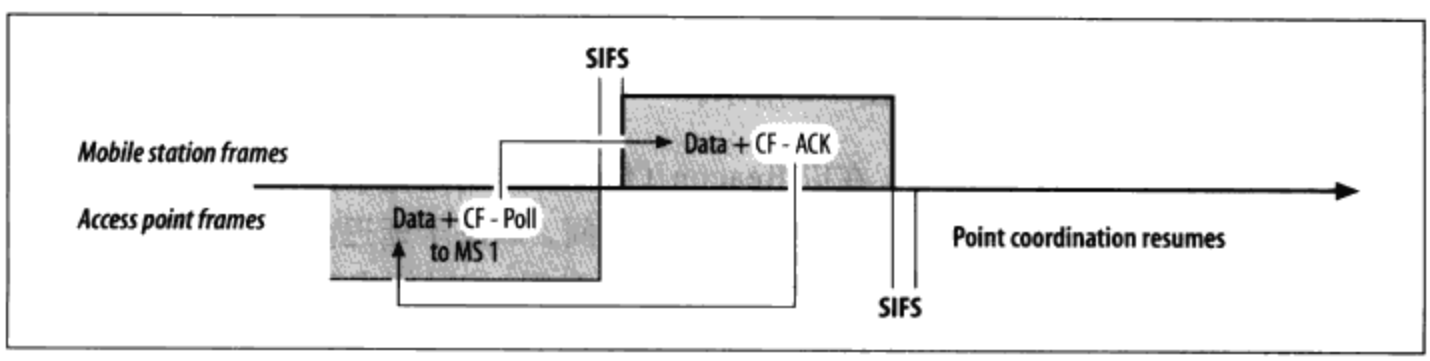


图 9-3：Data+CF-ACK 的用法

此帧只用于infrastructure（基础结构型）网络，因为它只能在无竞争周期内传送。接入点或移动式工作站均可发送此类型的帧。不过在无竞争周期内，接入点必须负责轮询，因此似乎不太可能传送此类型的帧，因为其中并未包含轮询（poll）。

Data+CF-Poll

在无竞争周期内，接入点可以在infrastructure网络中使用Data+CF-Poll帧。当接入点不需要确认任何帧时，就会以Data+CF-Poll传送数据给接收端，同时允许对方传送一个缓存帧作为响应。帧主体所包含的数据必须是给发出询问的接收者，这两种功能不能“分别”针对不同的接收者。图9-3中，接入点使用Data+CF-Poll帧传送一个数据帧给工作站，同时要求对方（传回一个缓存帧作为）响应。

Data+CF-ACK+CF-Poll

在无竞争周期内，接入点可在infrastructure网络中使用Data+CF-ACK+CF-Poll帧。如果接入点必须同时传送数据、确认帧以及探询轮询列表中的工作站，则可以将这些功能组合在一个帧中。图9-4显示了Data+CF-ACK+CF-Poll的用法。如同Data+CF-ACK，Data+CF-ACK+CF-Poll中的组件通常是针对不同的工作站。数据传送与轮询必须针对相同的工作站，而确认信息则是针对前次的数据传送。

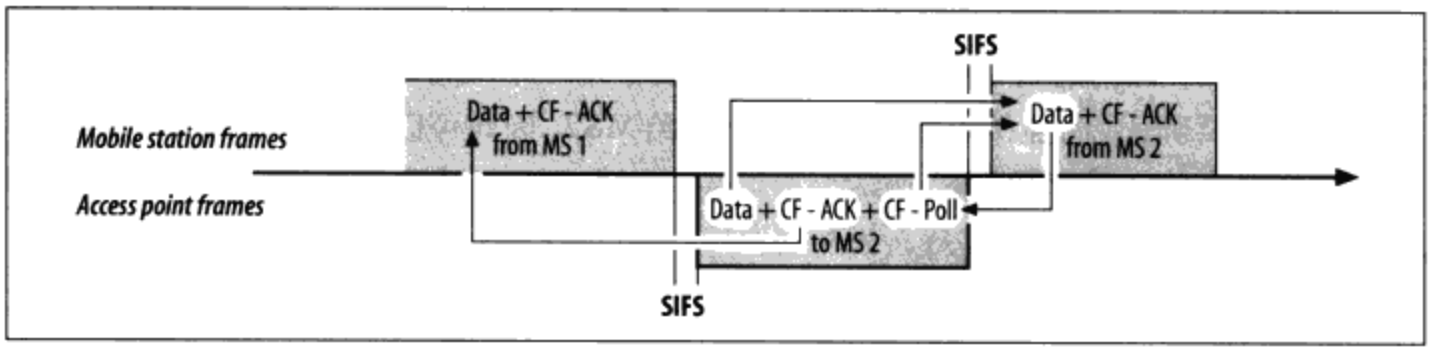


图9-4：Data+CF-ACK+CF-Poll的用法

图9-4中，第一个移动式工作站（MS1）传送了一个Data+CF-ACK帧。Data部分必须送至接入点，不过CF-ACK却是确认接入点之前所传送的数据帧（本图并未显示该帧）。根据轮询列表，接入点随后询问第二个移动式工作站（MS2）是否有缓存帧。然而，此时接入点必须确认来自MS1的数据帧，因此接入点在帧中加入了CF-ACK信息。当时接入点正好有数据要传送，所以将这三者结合成一个多用途的帧。Data与CF-Poll组件是给帧的接收者，而CF-ACK则是给前一个帧的传送者。MS1必须聆听接入点所发出的帧才有办法接收到该确认信息。

CF-ACK（不含数据）

如果只需要确认信息，那么可以传送一个仅含标头及CF-ACK功能的帧。图9-4中，如果MS2没有数据待传，就仅会以一个CF-ACK帧作为响应。

CF-Poll（不含数据）

CF-Poll 也可以独自传送。当然，只有接入点才会使用这项功能，因此 CF-Poll 帧只有在无竞争周期内才会由 infrastructure 网络中的接入点传送。

如果接入点已经没有其他缓存数据要传给接收者，而且不必确认之前所收到的帧，就只会传送 CF-Poll。一种常见的情况是，接入点传送了一个 CF-Poll 进行轮询，但工作站方面并无数据也无响应，这时候便不需要确认信息。如果接入点没有数据要传给轮询列表中的下一个工作站，就只会传出 CF-Poll，如图 9-5 所示。

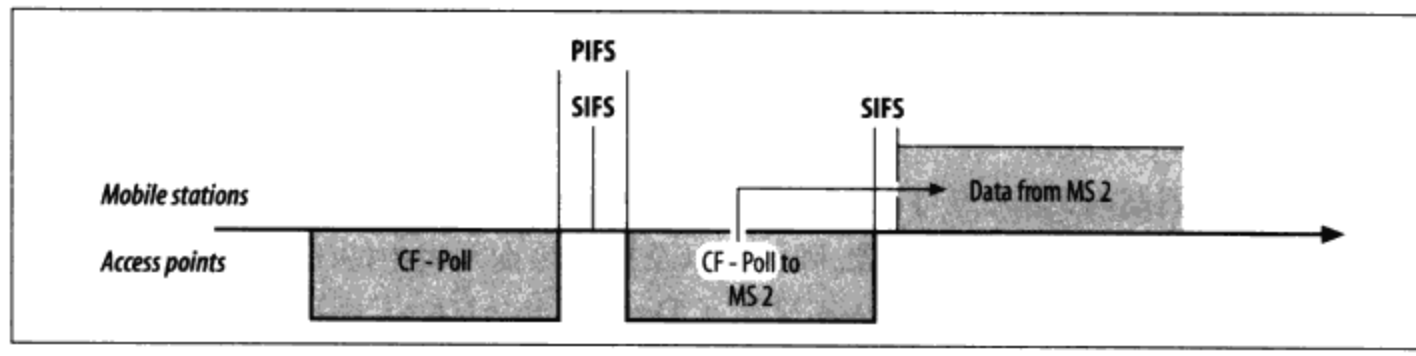


图 9-5：CF-Poll 帧的用法

图 9-5 中，接入点尝试传送数据给 MS1，不过并未收到响应。等候一段 PIFS（PCF 帧间间隔）后，接入点便开始询问轮询列表中下一个项目 MS2。由于没有来自 MS1 的帧需要确认，而且接入点也没有数据送给 MS2，因此可以只发送 CF-Poll 给 MS2，允许对方传送缓存数据。

CF-ACK+CF-Poll（不含数据）

最后一种数据帧类型为 CF-ACK+CF-Poll，也是由接入点发送的。和所有 CF-Poll 帧一样，此帧只用于无竞争周期，而且只能给接入点使用。其中包含了确认以及轮询功能，但是不含任何数据。图 9-6 显示了此帧的用法。

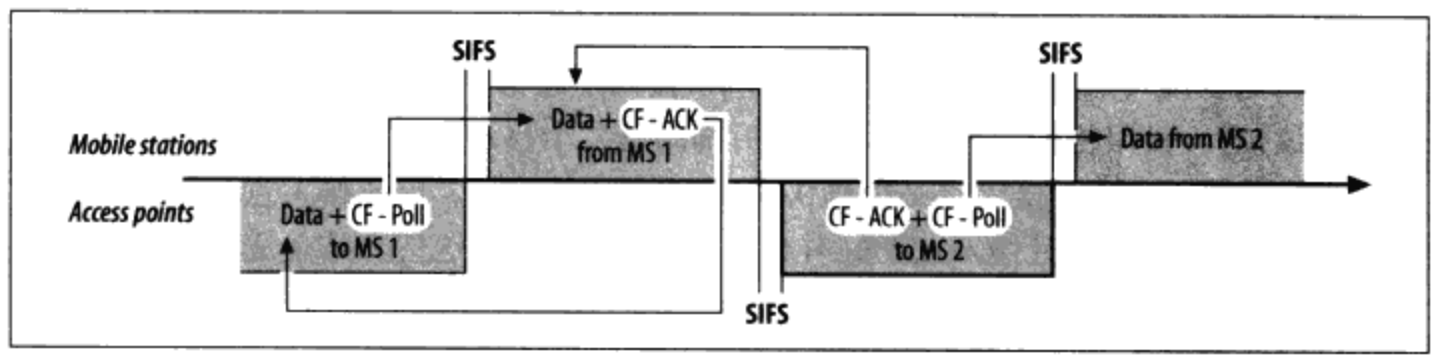


图 9-6：CF-ACK+CF-Poll 帧的用法

此处的情况和之前的设定稍有不同。图 9-6 中，MS1 返回了一个帧，而没有让接入点逾时等候。当接入点取得媒介控制权，就会以 CF-ACK+CF-Poll 确认之前 MS1 所传送的帧，同时通知 MS2，允许它传送缓存数据。

无竞争周期结束（CF-End）

无竞争周期结束时，接入点会送出一个 CF-End 帧，让工作站脱离 PCF 访问规则，然后开始采用基于竞争的服务。CF-End 帧的格式如图 9-7 所示。CF-End 帧的 MAC 标头是由 4 个字段组成：

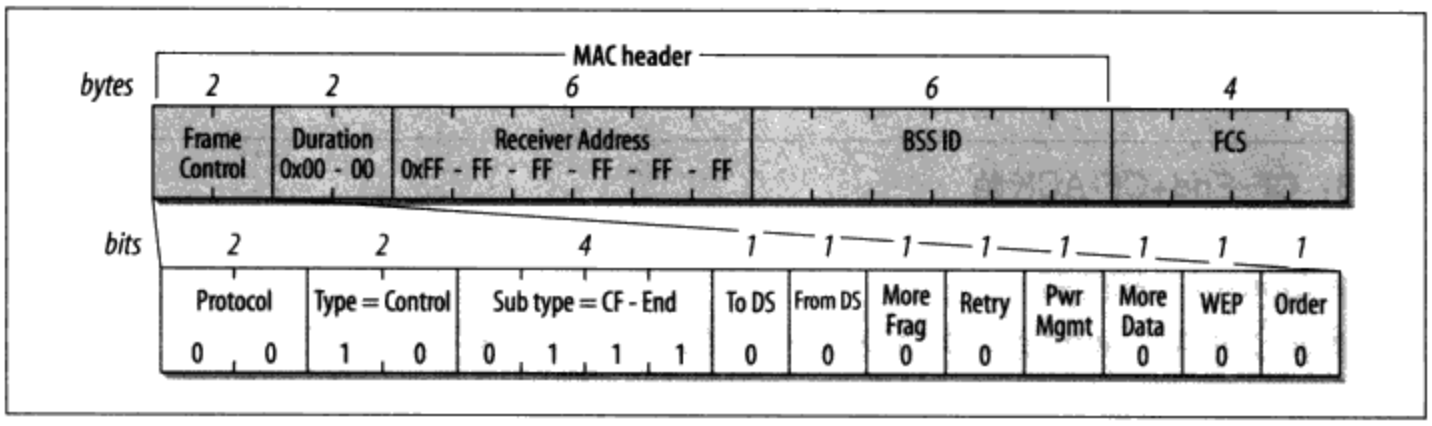


图 9-7：CF-End 帧

Frame Control（帧控制）

帧的子类型（subtype）设定为 1110，代表 CF-End 帧。

Duration（持续时间）

CF-End用来声明无竞争周期的结束，因此不需要延长虚拟载波监听时间。Duration 会被设定为 0。收到 CF-End 帧的工作站会将虚拟载波监听时间截短，以便重新启用基于竞争的访问。

第一个地址字段：Receiver Address（接收端地址）

CF-End 攸关所有移动式工作站的操作，因此接收端地址会被设为广播地址。

第二个地址字段：BSSID

接入点会将CF-End发布给其BBS中与之关联的所有工作站，因此第二个地址字段必须填入 BSSID。在 infrastructure 网络中，BSSID 是接入点的无线接口地址，因此 BSSID 也就是发送端地址。

CF-End+CF-ACK

当无竞争周期结束，接入点会送出一个 CF-End 帧，让工作站脱离 PCF 访问规则，同时以DCF 开始进行基于竞争的服务。如果接入点必须同时响应之前所收到的数据，则可用 CF-End+CF-ACK 帧于结束无竞争周期的同时顺便加以响应。CF-End+CF-ACK 帧的格式如图 9-8 所示。CF-End+CF-ACK 帧的 MAC 标头由 4 个字段组成：

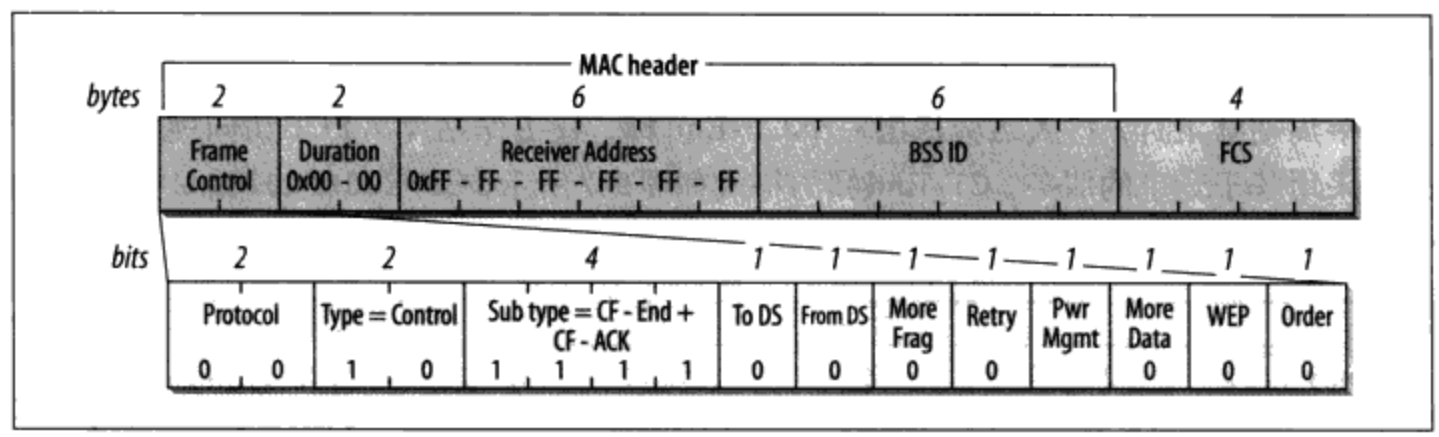


图 9-8：CF-End+CF-ACK 帧

Frame Control（帧控制）

帧的子类型（subtype）设定为 1111，代表 CF-End+CF-ACK 帧。

Duration（持续时间）

CF-End+CF-ACK 用来声明无竞争周期的结束，因此不需要延长虚拟载波监听时间。Duration 字段会被设为 0。

第一个地址字段：Receiver Address（接收端地址）

CF-End+CF-ACK 攸关所有移动式工作站的操作，因此接收端地址会被设为广播地址。

第二个地址字段：BSSID

接入点会将 CF-End+CF-ACK 发布给其 BBS 中与之关联的所有工作站，因此第二个地址字段必须填入 BSSID。在 infrastructure 网络中，BSSID 是接入点的无线接口地址，因此 BSSID 也就是发送端地址。

CF 参数集

支持无竞争操作的接入点可能会在帧中使用 CF 参数集（CF Parameter Set）信息元素，如图 9-9 所示。CF 参数集信息元素若被包含在 Beacon 帧中，可通知所有移动式工作站开始进行无竞争操作。这些参数集信息元素若被包含在 Probe Response 帧中，则可以让工作站明白该 BSS 支持哪些无竞争选项。CF 参数集信息元素由 4 个字段组成：

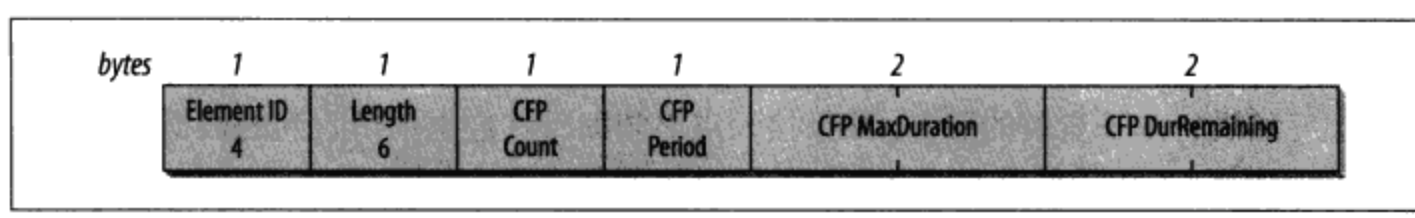


图 9-9：CF 参数集信息元素

CFP Count（CFP 计数器）

此字段占用一个字节，用以告知下个无竞争周期开始前还会传送几个DTIM帧。如果为0，那么当前的帧代表无竞争服务的开始。

CFP Period（CFP 周期）

此字段也占用一个字节，用来指示两个无竞争周期相距多少个 DTIM 间隔。

CFP MaxDuration

这个值是以时间单位（time unit，简称TU）作为计量单位，用来指示无竞争周期最长可以延续多久。移动式工作站会以这个值来设定NAV，表示在整个无竞争周期，媒介均处于忙碌状态。

CFP DurRemaining

这个值也是以TU作为计量单位，用来指示当前的无竞争周期还有多长时间。在整个无竞争周期，移动式工作站会以这个数值来更新NAV。使用DCF服务时，这个值会被设为0。

电源管理与 PCF

无竞争周期节省电力的方式和基于竞争的周期类似，不过有些小小的例外。两者主要的差异为无竞争周期的帧传送必须遵循PCF规则，因此只有在接入点询问时才可以传送缓存帧。不支持 PCF 操作的工作站必须等到基于竞争的服务重新启用时才可以取回缓存帧。

在无竞争周期，不允许列于轮询列表中的工作站进入休眠状态。接入点使用其点协调功能（PCF）时，可以在任何时间询问任何一个工作站。在无竞争周期内，传送给工作站的帧无需缓存，因为这些列于轮询列表中的工作站不可能处于休眠状态。

不论是在无竞争还是基于竞争的服务中，帧缓存的方式都一样。接入点负责维护每个工作站的省电状态，并且为处于低功耗模式的工作站缓存帧。如果与之关联的工作站处于低功耗模式，那么也会为其保留广播与组播帧。

除了与无竞争服务相关的缓存状态，接入点也会针对试图轮询的工作站设定TIM中的几个位标记。之所以要设定这些位标记，与如何传送缓存帧有关。和基于竞争的服务一样，广播与组播帧的传送由DTIM帧所触发。如果传送广播与组播帧所需的时间超过Beacon interval（信标间隔），接入点只会传送相当于 Beacon interval 的时间，之后就会予以中止。由于还有残留帧，因此接入点会继续保留与 AID 0 相应的位标记。

传送了缓存的广播与组播帧之后，接入点会重新查看一次AID（关联标识符）列表，只要其TIM位标记未被取消，就会继续传送残余数据。帧的传送完全依循PCF规则，因此传送前不必加上延迟时间。轮询列表中的工作站会被加到TIM中，因此会参与整个过程。虽然可以传送多个缓存帧，但实际情况得视提供无竞争服务的接入点如何实现。移动式工作站只有在得到接入点允许时才可以进行传送。接收完所有帧之前工作站不能进入休眠状态，除非More Data（更多数据）位为0，代表已无后续数据。当一个工作站空闲下来进入休眠状态，就会沉睡到下一次DTIM传送时。DTIM帧用来声明无竞争周期的开始，因此实际具备PCF功能的工作站必须在每次DTIM传送之前醒来。

在无竞争周期内，如果工作站从低功耗模式醒来，所有为之缓存的帧都会被转移给点协调功能以便进行传送。数据转移后并不会立即传送，不过如果点协调功能允许，接入点可以将这些帧置于队列（queue）准备传送。

第十章

物理层概述

只要静静地站着，每个女人都可以魅力非凡。

—— Hedy Lamarr

通信协议的分层概念（protocol layering）让我们可以针对协议堆栈（protocol stack）的各个部分进行研究、实验或改良。802.11结构的第二个要件为物理层（physical layer），通常简写为PHY。本章主要介绍无线物理层所涵盖的主题与常见的技术，以及描述所有无线物理层的共同问题，之后会就802.11所包含的标准物理层分别加以详细说明。

物理层结构

物理层被分成两个子层（sublayer）：物理层会聚过程（Physical Layer Convergence Procedure，简称PLCP）子层以及物理媒体相关（Physical Medium Dependent，简称PMD）子层。PLCP（图10-1）的功能在于结合来自MAC的帧与空中所传输的无线电波。PLCP同时会为帧加上自己的标头。通常，帧中会包含前导码（preamble）以协助接收数据的同步操作。不过，每种调制方式所采用的前导码均不相同，因此PLCP会为准备传送的所有帧加上自己的标头。接着由PMD负责将PLCP所传来的每个位利用天线传送至空中。物理层还包含了空闲信道评估（clear channel assessment，简称CCA）功能，用来指示MAC是否检测到了信号。

无线链路

802.11最初的版本颁布于1997年，其中包含了三种物理层标准：

- 跳频（Frequency-hopping，简称FH）扩频（spread-spectrum）无线电物理层（radio PHY）

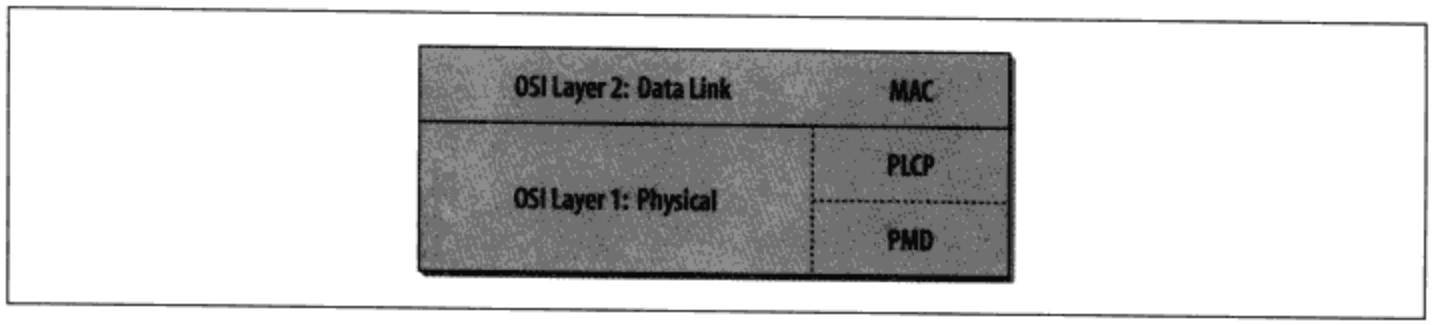


图 10-1：物理层逻辑架构

- 直接序列（Direct-sequence，简称 DS）扩频无线电物理层
- 红外线（Infrared light，简称 IR）物理层

后来，进一步开发了三种以无线电技术为基础的物理层：

- 802.11a：正交频分复用（Orthogonal Frequency Division Multiplexing，简称 OFDM）物理层
- 802.11b：高速直接序列（High-Rate Direct Sequence，简称 HR/DS 或 HR/DSSS）物理层
- 802.11g：增强速率物理层（Extended Rate PHY，简称 ERP）
- 未来的 802.11n，俗称多进多出（MIMO）或高吞吐量（High-Throughput）物理层

本书只会深入探讨其中四种以无线电波为基础的物理层。由于并未广泛使用，因此红外线物理层会略过不谈。就我所知，红外线物理层从来不曾运用在任何商业化的产品中。

IR 物理层

802.11 包含了红外线（IR）物理层的规范。使用红外线代替无线电波似乎有许多优点。红外线连接端口比电波收发器便宜，事实上，它的价格低到每部膝上型计算机均将红外线连接端口列为标准配置。

IR 能够抗拒无线电频率或射频（radio frequency，简称 RF）的干扰，因为无线电波运作在完全不同的频率上。这带来第二项优点：IR 无规则。这样产品开发人员无需费神探究如何让产品符合世界上许多规则机构的规范。

和 802.11 攸关的安全考虑大多围绕在未经授权的用户可能盗连网络的威胁。由于光线只能够局限在某个会议室或办公室，只要将门关上即可，所以以红外线为基础的局域网络具备灵活与易移动等优点，而且安全顾虑较少。不过这并非没有代价。由于红外线局域网络依赖的是随处发散的光线，因此传输距离较短。

— 待续 —

不过，以上纯属学术上的讨论，实际上并没有红外线物理层的相关产品。膝上型计算机配备的红外线端口所符合的标准，是由红外线数据准备协会（Infrared Data Association，简称IrDA）而非802.11所制定的。由于无线电波可以长距离传输而且可以穿透固体，因此灵活性较大，移动性也较好。灵活性与移动性既然是一般采用802.11的最大驱动力，所以就算开发出红外线物理层的相关产品，也无法与无线电波相提并论。

许可证与规则

以往无线通信的做法是将承载信息的信号限制在某个较窄频带，然后尽可能加大信号功率（只要合法即可）。在频带中，噪声不可避免地会造成信号某种程度的失真。在有噪声的情况下，传送信号必须采取强制手段 —— 只要能确保信号的功率远大于噪声即可。

在古典的通信模型中，如何避免干扰其实是属于法律（而非物理）层面的议题。对于窄频高功率的传输，管理者必须制定一套规则以规范如何使用RF频谱。在美国，由联邦电信委员会（Federal Communications Commission，简称FCC）负责管理RF频谱的使用。美洲的其他国家也采用FCC所制定的一些规范。在欧洲，频谱配置是由欧洲无线电通信管理局（European Radiocommunications Office，简称ERO）以及欧洲电信标准协会（European Telecommunications Standards Institute，简称ETSI）负责。在日本，无线电的使用受内务及通信产业省（Ministry of Internal Communications，简称MIC）规范。全球“一致”（harmonization）的规范则由国际电信联盟（International Telecommunications Union，简称ITU）所管辖。ITU的提案被许多国家的管理单位采用。

通常要以特定频率传送电波必须事先取得许可证。许可证限制了可以使用哪些频率与传输功率以及可以传送到哪些地区。举例而言，无线广播电台必须取得FCC的许可证；同样地，移动电话网络也必须取得许可证，方能在某个特定地区与市场使用无线频谱。许可证可以保证特定频率的独家使用权。当信号受到干扰，许可证持有者可以要求管理者介入，通常是通过关闭干扰源来解决问题。故意干扰是一种侵权行为，可能会受到刑事或民事上的处罚。

频率分配与无需许可证的频带

无线频谱可以被划分为许多频带，每个频带针对特定的使用目的。每个频带定义了特定应用可以使用的频率。其中，防护频带（guard band）用来防止传送信号的溢散影响到其他频带。

有些频带是保留给不必使用许可证的应用。举例而言，微波炉使用2.45GHz，在自己家里使用微波炉还得获得FCC的批准并无太大的意义。为了让厂商得以在消费性市场上开发家用产品，FCC（以及其他各国类似的管理机构）指定了一些特定频带给“工业、科学与医疗”设备使用。这些频带通常称为ISM频带。2.4-GHz频带在全世界均可不经授权使用（注1）。不过，无需许可证与无需销售许可证不同。构建、生产与设计802.11设备不必取得许可证，而在美国所有合法销售的802.11网卡必须取得一个FCC认证。在申请过程中，厂商必须提供相当多的信息给FCC。这些信息主要是作为公开记录之用，各位可通过FCC认证上网搜寻。

使用ISM频带的设备通常不必取得许可证，只要这些设备不散发过多的辐射。微波炉属高功率设备，不过通常会加上层层保护以防止电磁辐射。随着新通信技术的发展，这些不必使用许可证的频带近三年来相当受到关注。用户无需通过许可证申请过程，即可使用运作在ISM频带的设备，厂商也无需费神熟悉授权的过程与要求。写作本书时，2.4-GHz ISM频带已经充斥了不少新开发的通信系统：

- 各式802.11系统（跳频层、直接序列层与OFDM系统层）
- Bluetooth（蓝牙），一种短距离的无线通信协议，由Ericsson领军的产业联盟所开发
- 由一些无绳电话（cordless phone）厂商所生产的扩频无绳电话
- X10，家庭自动化设备所使用的一种协议，可以通过ISM频带进行视频（video）传输

遗憾的是，“免证”（unlicensed）并不意味着设备可以“与其他设备融洽相处”（plays well with others）。所有不必使用许可证的设备都必须遵守传输功率的限制。既然没有编码或调制上的管制，因此不同厂商使用频谱的方式可能彼此不兼容。站在用户的角度，解决这个问题的唯一方式就是从中择一使用。因为设备不必取得许可证，因此管理者不会介入。

其他不必使用许可证的频带

其他无需使用许可证的频谱范围位于5 GHz。美国是第一个允许在5 GHz范围内使用

注1： FCC条例（联邦法规第47条）第15.247篇将2.4-GHz频带保留给ISM使用。ETSI则是在ETSI技术规范说明书（ETSI Technical Specifications，简称ETS）300-328中保留该段频谱。

水对微波的吸收峰（Absorption Peak）并不存在

据说微波炉之所以采用2.45GHz，是因为水分子在此频带特别活跃。有时候，这种说法甚至被当成802.11无法长距离传输的理由。如果下雨或者气候十分潮湿时，微波信号会因为大气中的水分蒸发而严重衰减（attenuate），所以802.11就不适合用于长距离传输。

微波中存在能够让水分子特别活跃的频率，这种说法纯属虚构。若是这样，水分必然会吸收相当多的微波能量。如果这些能量被水有效吸收，微波炉就无法加热任何东西，因为微波会被食物表面的水分给吸收尽。既然表面的水分会吸收掉所有能源，食物中央就无法加热变熟。吸收峰（absorption peak）同时意味着大气中的水分蒸发会中断卫星通信，不过情况并非如此。NASA的参考文献1108(02)《Propagation Effects on Satellite Systems at Frequencies Below 10 GHz》论及大气效应预期会造成多少信号的损失，结论是通常频率在10 GHz以上的信号损失较为严重。举例而言，最容易被水分吸收的微波频率为22.2 GHz。

微波炉的运作方式并不是将水分子推至激发态（excited state），而是利用水分子非比寻常的强偶极矩（strong dipole moment）。虽然本身属电中性，偶极矩使得水分子就像是两端各带细微正负电荷的小棒。在微波炉中，不断改变的电磁场会来回扭转水分子。来回扭转之下，连带增加了整个分子的动能，水分子也因此更为活跃，但并未改变水分子的激发态或者成分。

免许可证设备的国家，不过日本与欧洲也随后跟进（注2）。以下是全世界各国允许使用的一系列频谱：

- 4.92~4.98 GHz（日本）
- 5.04~5.08 GHz（日本）
- 5.15~5.25 GHz（美国、日本）
- 5.25~5.35 GHz（美国）
- 5.47~5.725 GHz（美国、欧洲）
- 5.725~5.825 GHz（美国）

注2：欧洲显然不止一个国家，不过全欧洲有一个共同的频谱管理单位。

除了信道宽度与辐射功率，使用5 GHz频带的设备无需遵循其他限制。相比较于美国或欧洲，日本的规范使用较窄的带宽。

扩频

扩频（spread-spectrum）技术是使用ISM频带传送数据的基础。传统无线电通信的焦点在于如何尽可能地在最窄的频带中塞入最多的信号。扩频的运作原理是利用数学函数将信号功率分散至较大的频率范围。只要在接收端进行反向操作，就可以将这些信号重组为窄带信号。更重要的是，所有窄带噪声都会被过滤掉，因此信号可以清楚地重现。

对于无需使用许可证的设备而言，使用扩频技术是必要的。有时候，这是因为管理者要求的；有时候，这是符合管制要求的唯一方式。举例而言，FCC要求使用ISM频带的设备必须使用扩频传输并在一些参数上加以限制。

对传统的窄带接收器而言，传输信号展开至较宽频段之后和噪声没有两样。有些扩频设备厂商宣称扩频可以增加安全性，因为窄带接收器无法接收完整信号。问题是，将之更换为标准扩频接收器是轻而易举的，因此必须强制使用其他安全功能。

这并不意味着扩频是可以解决干扰问题的“万灵丹”（magic bullet）。扩频设备甚至可能与其他通信系统相互干扰，传统的窄带RF设备也是这样。虽然扩频在处理干扰问题上比其他调制技术高明，但问题并未因此而消失。当更多RF设备（不论是否属于扩频）占据无线网络的覆盖范围时，噪声就会增多，信噪比（signal-to-noise ratio）就会因此而降低，可靠的通信范围也会跟着缩小。

为了将（无需许可证的）设备之间的干扰降至最小，FCC限制了扩频传输所能使用的功率。法律上明文限制发射器的输出功率（output power）为1瓦（watt），有效辐射功率（effective radiated power，简称ERP）为4瓦。有效辐射功率4瓦对增益（gain）为6 dB（译注1）的天线而言，相当于1瓦的输出功率；对增益为10 dB（译注2）的天线而言，则相当于400毫瓦的输出功率（注3）。PC无线网卡的发射器与天线显然符合此限制，就算使用商用天线，也不会比较接近。不过，若使用外部的放大器或增益较高的天

译注1：$10\log_{10}4$。

译注2：$10\log_{10}10$。

注3：请记住，传输线属于天线系统的一部分，而系统增益必须将传输线损耗计算在内。因此，增益为7.5 dB的天线如果有1.5 dB的传输线损耗，那么系统整体增益为6 dB。值得注意的是，传输线在UHF频带的损耗通常很高。因此，各位最好让放大器尽可能接近天线。

线，PC无线网卡即可涵盖较大的区域。对于这个问题法律并未明文禁止，不过可以确定的是，无论如何还是必须符合FCC的功率标准。

无意间发明的扩频

奥地利出生的女演员Hedy Lamarr于20世纪40年代初期取得了扩频专利。不过，她之所以举世闻名，却有其他原因。除了在一部名为《Ecstasy》的捷克电影中破天荒全裸出演，好莱坞名人Louis Mayer更称她为“全世界最美的女人”。她同时也是《蝙蝠侠》漫画猫女一角的灵感来源。

在德国纳粹入侵之前，Hedy Lamarr原本是一位奥地利军火商的妻子。她意识到以无线电远程控制鱼雷是当时军火制造商的主要研究领域。遗憾的是，窄带无线电通信容易遭受人为干扰，从而抵消无线导引武器的优势。她从这些讨论中得到一种想法，可以使用一种复杂但预先设定好的跳频模式随时改变控制信号的频率。只要在某个频率稍作停留就可能被干扰，因此频率的变换速度必须很快，才可以避免信号被完全阻绝。Lamarr完成所有细部设计，但不包括如何精确地控制跳频。

移居美国之后，Hedy Lamarr遇到了George Antheil。他是一位美国的前卫作曲家，作品充满不和谐风格（dissonant style），人称“音乐顽童”（bad boy of music）。在著名的Ballet Mecanique（机械芭蕾）中，他控制16部自动弹奏的钢琴，身旁还安排一些人毫无节制地制造噪音。要演奏这个作品，必须能够精确掌控每项元素的时间，这正是Lamarr在控制跳频模式时所遭遇的困难。1942年，他们共同取得该项美国专利，编号为2292387。该专利于1959年失效，没有为他们赚进一分钱。这个贡献一直默默无闻，因为专利上所列的是她结婚时所使用的名字Hedy Kiesler Markey。无线局域网市场在20世纪90年代末期逐渐浮现之后，她的发明也被重新挖掘出来，并被广泛视为奠定当代电信基础的先锋之作。

在古巴导弹危机期间，美国首次将跳频技术应用在封锁古巴的舰队上。电子扩频技术具备商业可行性是多年之后的事。如今，扩频技术不但应用在无线与移动电话上，也应用在宽带无线局域网设备以及使用ISM频带的每一种设备。Hedy Lamarr于2000年初去世，而无线局域网正好在那一年得到市场主流的青睐。

扩频的类型

802.11所采用的无线电物理层使用了三种不同的扩频技术：

跳频（Frequency hopping，简称FH或FHSS）

跳频系统是以某种随机样式在频率间不断跳换，每个子信道只进行瞬间的传输。2-Mbps FH PHY规范于规范说明书第14款。

直接序列（Direct sequence，简称DS或DSSS）

直接序列系统利用数学编码函数将功率分散于较宽的频带。标准中规范了两种直接序列物理层。最初的规范说明书在第15款所提出的是2-Mbps PHY标准，而802.11b则加入了第18款用于HR/DSSS PHY。

正交频分复用（Orthogonal Frequency Division Multiplexing，简称OFDM）

OFDM将可用信道划分为一些子信道，然后对每个子信道所要传送的部分信号进行平行编码。这种技术类似于某些DSL调制解调器所使用的离散多音频（Discrete Multi-Tone，简称DMT）调制技术。802.11a所加入的第17款用来规范OFDM PHY，而802.11g所增加的第18款则是用来规范ERP PHY。基本上ERP PHY跟OPDM PHY没有两样，只不过运作在较低的频率。

这三者中以跳频系统的价格最为低廉。虽然跳频的控制必须精确计时，但不必经过复杂的信号处理即可从无线电波信号中取出位流。直接序列系统需要较复杂的信号处理，即需要消耗更多的电力以及特殊的硬件。直接序列技术所能使用的数据传输率也比跳频系统高。

RF传播与802.11

在固定式网络中，信号只能在电电缆限定的路径中移动，因此网络工程师不必知道电子信号传播的物理特性。只要依循一些规则计算出每个网段所允许的最大电电缆长度，就很少会出现什么问题。RF传播可没那么简单。

信号接收与性能

空气中到处都是随机的电磁波，只要将收音机调整到没有电台的频率就可以轻易听见。无线电通信必须从背景的噪声中分辨出信号。一旦接收条件变差，信号就容易被噪声淹没。性能绝大部分取决于信噪比（signal-to-noise ratio，简称SNR）这个决定性因素。图10-2以信号峰值（the peak of the signal）与本底噪声（noise floor）之间的差异值来表示信噪比。

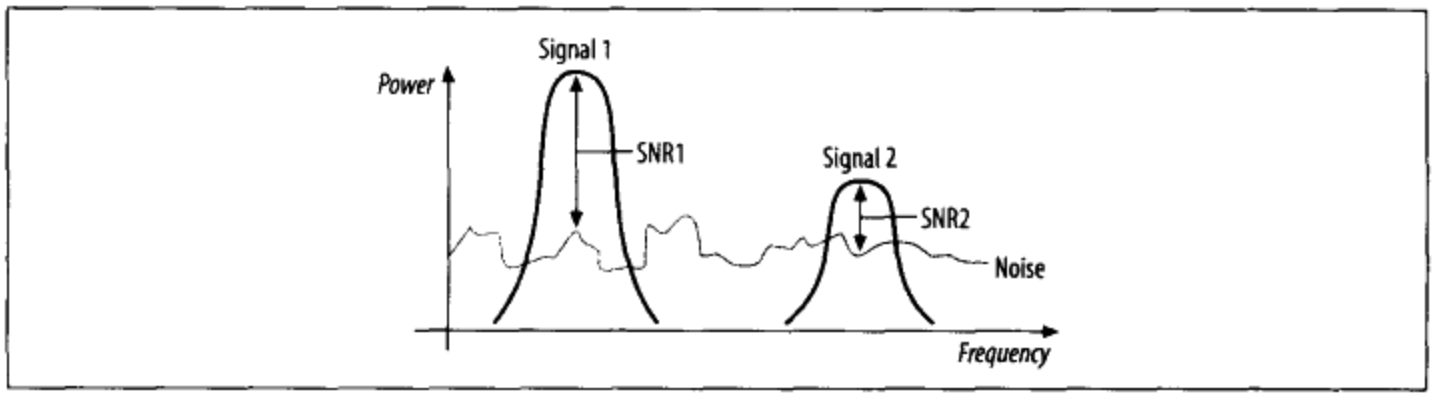


图10-2：信噪比与本底噪声

信号强度十分重要，但不代表一切。在充满噪声的环境中反而难以获取过强的信号。在某些情况下，可以通过加大功率作为对本底噪声太高的补偿。无许可证网络很难采用提高功率的手段，因为受到了严格的管制。因此，业界通常将比较多的精力放在如何降低噪声，即在解读电波信号之前尽量避免产生额外的噪声。

Shannon 极限

值得注意的是，无线电信道能够承载多少数据在理论上并没有极限。1948年，贝尔实验室的研究员Claude Shannon提出Shannon-Hartley定理，用来证明并计算传输信道的性能(capacity)。此定理陈述了传输信道性能在理论上的极限，一般通称此定理为Shannon极限或Shannon性能。原始的Shannon定理把最大性能C（每秒可传输位数）定义成带宽W（以Hertz表示）与信号功率的绝对信噪比的函数。如果以分贝为测量单位，只要在等式中以分贝取代功率比即可。

C=W log2 (1 + S/N)　　（S/N以功率比表示）

C=W log2 (1 + 10^(0.1 * SNR))　（SNR以分贝表示）

图10-3显示了Shannon极限与信噪比的函数关系。Shannon定理反映出无限位率(unlimited bit rate)在理论上的实际情况。要达到无限位率，在设计编码方式时可以任意取用数量很大的信号电平来区别位，不过这些邻近信号间的细微差异将被噪声所吞噬。802.11物理层设计人员的主要目的之一，就是设计出尽可能趋向Shannon极限的编码率。

此外，Shannon定理可以用来推算要达到特定数据率的理论最小信噪比。上述方程式可求解出信噪比：

S/N=2 ^ (C/W) - 1　　（S/N以功率比表示）

SNR=10 * log10 (2 ^ (C/W) - 1)　（SNR以分贝表示）

举一个802.11a的例子。以带宽为20 MHz的单一信道传送信号，数据率最高可达54 Mbps。代入上述方程式，可以求出信噪比为7.4 dB，远低于市面上大多数产品的需要，这反映出现实世界的产品只能以远糟于理想的性能运作（注4）。

注4：　或者另外举个例子。电话网络使用180 Hz至3.2 kHz的频带，信噪比为45 dB。理论上，模拟信号的最大速度可以达到45 kbps。56 kbps调制解调器的秘诀在于下行通道采用数字信号，因此可以得到较高的信噪比。

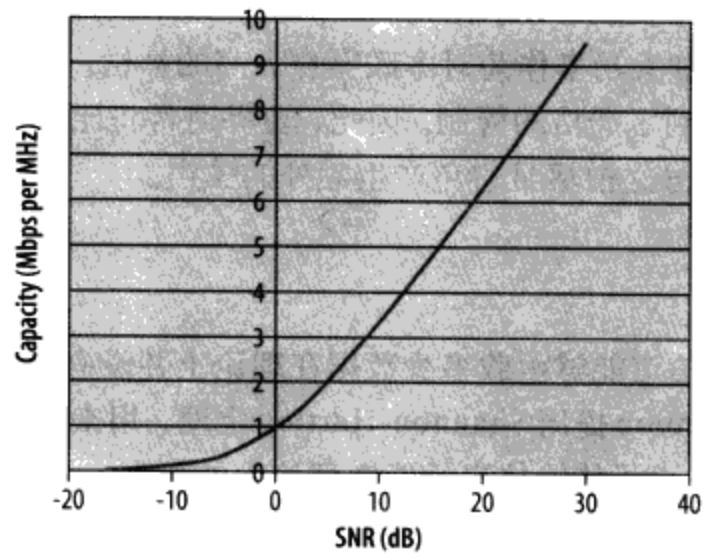


图 10-3：Shannon 极限与信噪比（SNR）的关系

分贝与信号强度

放大器是以能量的数量级（orders of magnitude）来放大信号。放大功率以分贝（decibel，简称 dB）来计算，以便舍弃不必要的 0。

$$dB=10 \times \log_{10}(\text{输出功率}/\text{输入功率})$$

当输出功率大于输入功率，此数值为正；如果输出功率小于输入功率则为负。每 10 dB 的变化量相当于提高 10 倍，而 3 dB 的变化量相当于提高 2 倍。因此 33 dB 的变化量相当于放大 2000 倍。

$$33dB=10\ dB + 10\ dB + 10\ dB + 3\ dB=10 \times 10 \times 10 \times 2=2000$$

功率有时候会以 dBm 计量，即每毫瓦的 dB 值。要计算 dBm 值，只要以 1 mW 代入第一个方程式的输入功率即可。

记住提高 2 倍功率相当于增加 3 dB，这很有用。增加 1 dB，粗略等同于功率提高 1.25 倍。记得这些数字，将可以在脑海中快速计算出大概的增益。

路径损耗、传输距离与吞吐量

在 802.11 中，网络的速度受到距离远近的影响。不同的 802.11 标准定义出了不同的调制方式，速度范围从 1 Mbps 到 54 Mbps。接收器电路必须能够分辨不同的状态，才能将位数据从电波信号中取出。较高速的调制方式在特定时间内可以封装更多的位，因此需要比较干净的信号（以及更高的信噪比）方能成功解码。

电波信号经过空间时会衰减。在802.11网络的有限范围内，本底噪声还不至于有太大的波动。不过距离一长，信号的衰减就会影响接收端的信噪比。当工作站逐渐远离接入点，信号电平就会不断下滑。既然本底噪声不变，信号的衰减就会造成信噪比的下降。这种情况可以通过图10-4加以说明。与接入点间的距离增加，接收到的信号就越趋近本底噪声。距接入点较近的工作站有较高的信噪比。以网络工程而言，当信噪比过低至以于无法使用较高的速率时，工作站就会降速，以便使用信噪比要求较低的数据率。

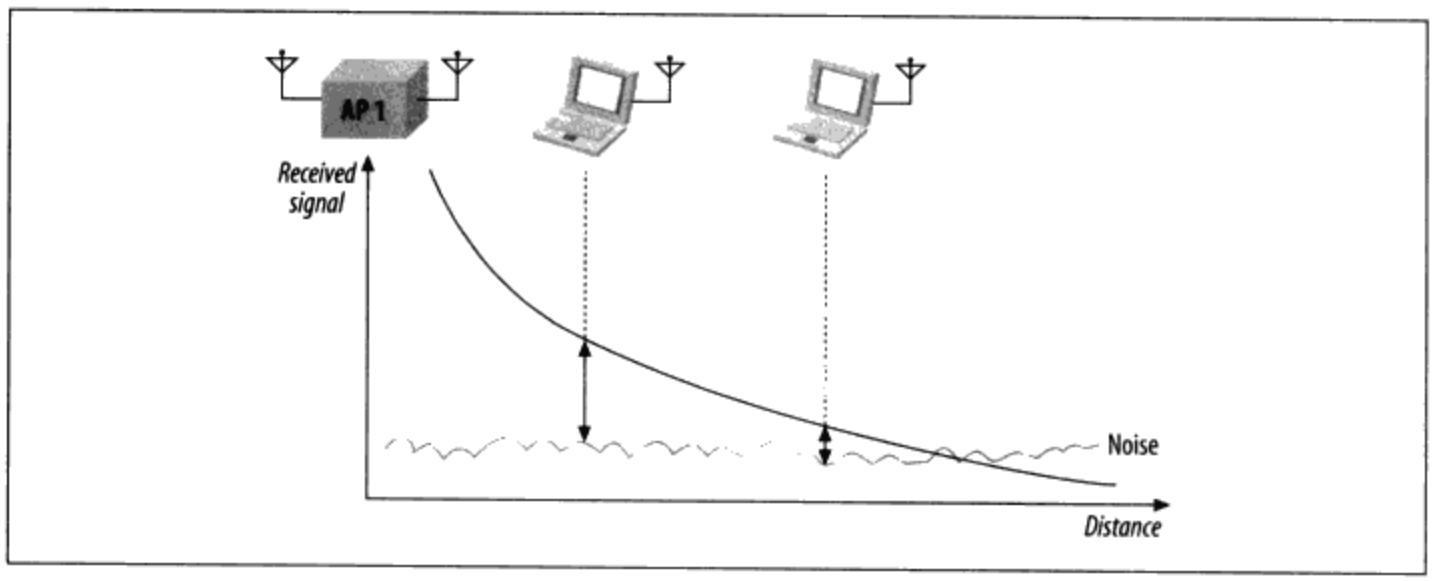


图 10-4：吞吐量与传输距离之间的关系

如果空中没有障碍物阻隔，信号的衰减就可以用下列公式计算。开放空间的损耗有时也称为路径损耗（path loss），因为它是预期中经过特定长度的路径的最小损耗。路径损耗受到距离与无线电波频率的影响。距离越远或频率越高，路径损耗就越大。802.11a的传输距离之所以比802.11b与802.11g的短，是因为802.11a所使用的5 GHz的路径损耗较大。开放空间的路径损耗可以表示成如下等式：

$$路径损耗（dB）=32.5 + 20 \log_{10}F + \log_{10}d$$

其中频率F以GHz表示，距离d以米为单位。不过，路径损耗不仅受距离的影响，墙面或窗户等障碍物也会影响信号，至于天线或放大器则可用来加强信号，补偿传输时的损耗。计算距离时通常会加上一种称为链路边界（link margin）的虚构因素来代表无法预料的损耗。

总损耗 = 传输功率 + 传输天线增益 − 路径损耗 − 障碍物损耗 − 链路边界 + 接收天线增益

多径干扰

虽然有相当简单的公式可以预测无线电波的传播，但也只是针对802.11网络的粗略估

算。除了直线的路径损耗，还有其他现象会影响802.11信号的接收。困扰无线网络的一个主要问题是多径衰落（multipath fading）。波与波之间具有叠加性（superposition）。当多个波聚集于某一点时，所产生的波即是所有波的总和。图10-5显示了一些波与波的叠加范例。

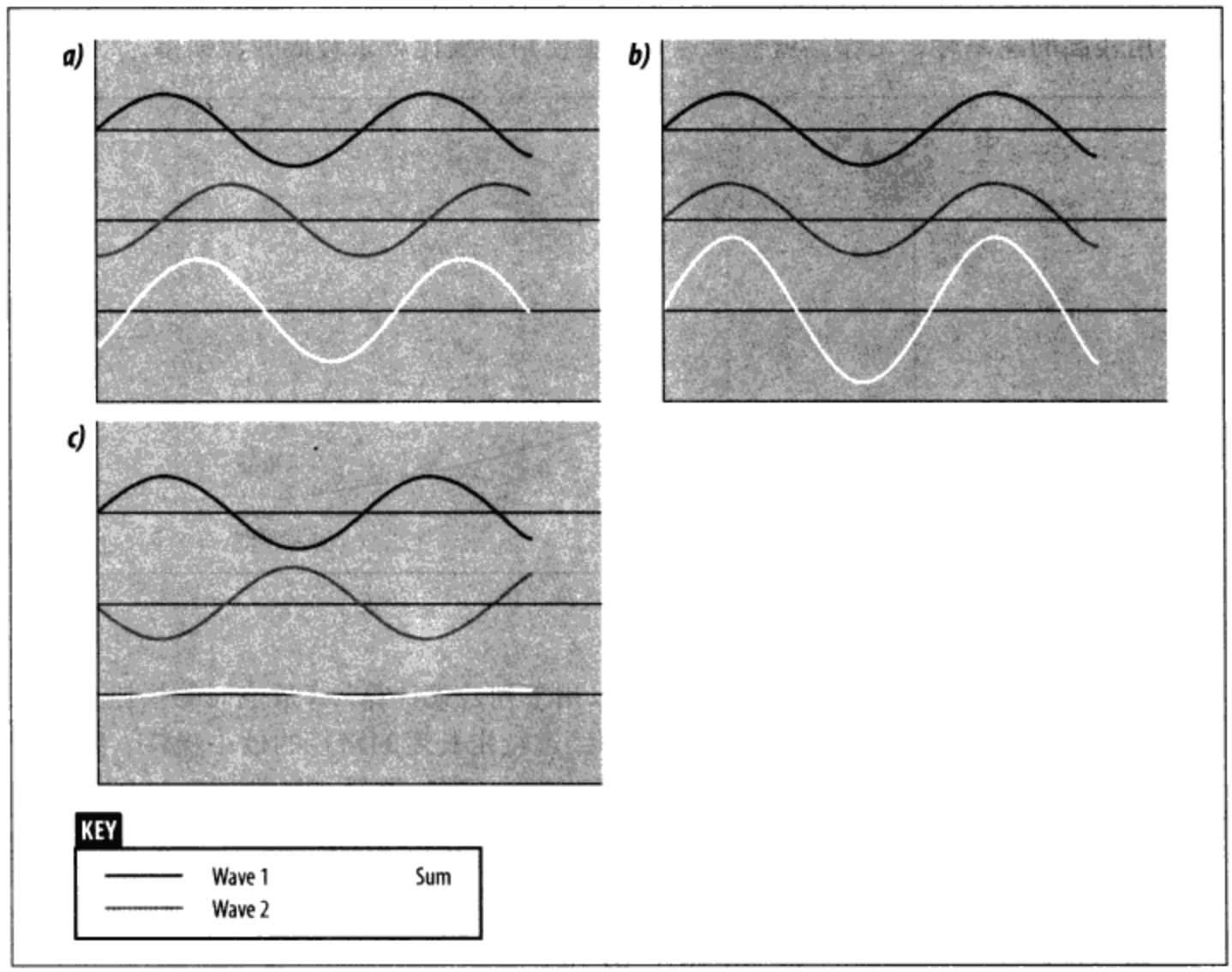


图10-5：波的叠加组合

图10-5 c)所显示的两个波几乎完全相反，叠加之后相当于什么也没有。遗憾的是，这种情况出现在无线网络的次数绝对出乎大家所料。802.11设备大部分采用全向天线，因此RF能量会往所有方向辐射。电波从天线向所有方向发散，在该区中遇到各种物体表面时则会加以反射。图10-6显示了一个经过高度简化的范例，其中有两个工作站位于完全没有阻隔的长方形区域内。

此图显示了从发送端到接收端的三种路径。接收端收到的电波为各种电波的总和。图10-6所显示的路径加起来的净值可能为0，在这种情况下，接收端就无法察觉信号的传输，因为根本没有收到任何信号。

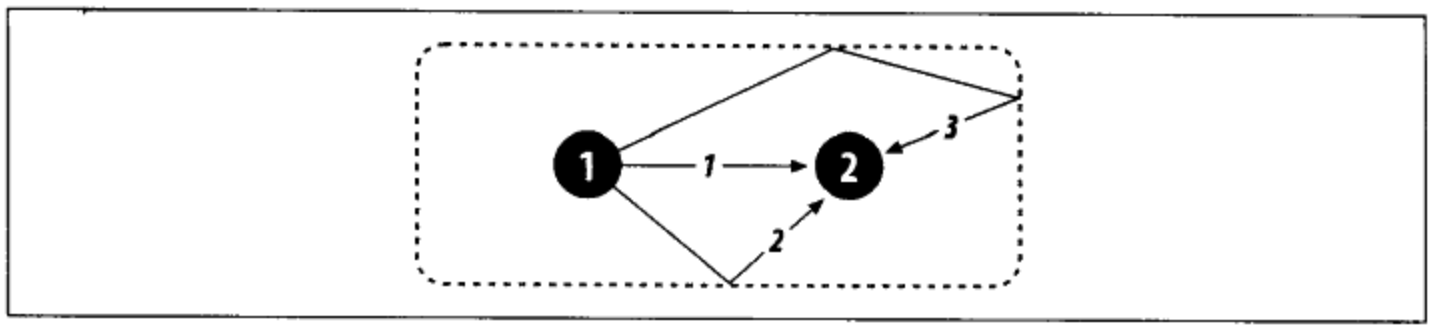


图 10-6：多径

由于干扰是相同的传输在不同路径迟延的结果，这个现象就称为多径衰落（*multipath fading*）或者多径干扰（*multipath interference*）。有时候，调整接收端的方向或摆设位置即可解决多径干扰问题。

符号间干扰（ISI）

多径衰落属于符号间干扰（Inter-symbol interference，简称ISI）的特例。从发送端至接收端，经过不同路径的电波，其路程不尽相同，因此彼此之间会有延迟落差，如图10-7所示。再次强调，波与波之间具有叠加性，因此造成整个波形的混淆扭曲。在实际情况中，来自不同路径的波前（wavefront）会相互叠加。最先到达的波前与最后到达的多径回波，两者之间的时间差称为延迟扩展（delay spread）。延迟扩展较长，就必须采用比较稳定的编码机制。802.11b 网络可以处理 500 ns 以下的延迟扩展，如果延迟扩展较短，性能就会更好。如果延迟扩展实在太长，有些网络就会降低传输速率。有些厂商宣称，若要以 11 Mbps 全速运作而且持有合理的帧错误率（frame error rate），则迟延扩展必须在65 ns以内（如何解读产品规格表将于第十六章探讨）。有些无线局域网分析工具可以直接测量延迟扩展。

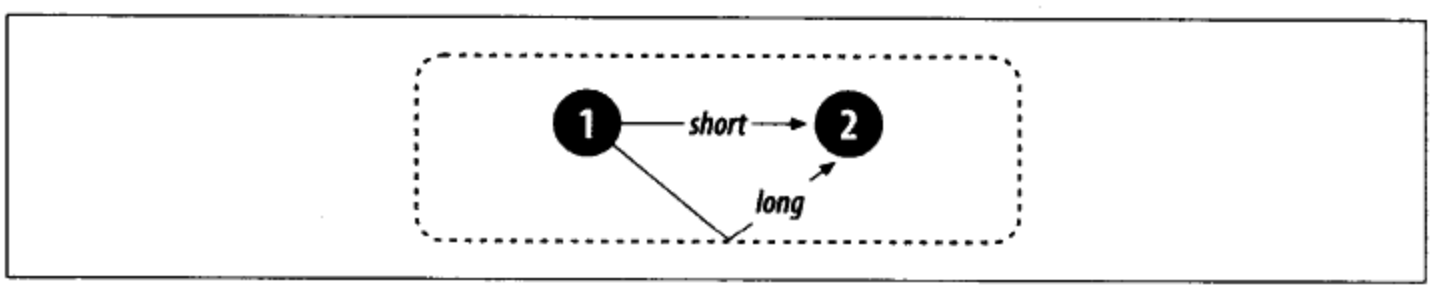


图 10-7：符号间干扰

802.11 的 RF 工程

802.11一直以惊人的速度为人们所采用。过去（习惯性地认为信号必然沿着定义明确的电电缆而行）的网络工程师如今所面对的局域网络是在充满噪声、容易出错而且变化多

端的无线链路上运行。802.11之所以能够在数据网络领域获得成功，与RF工程脱离不了关系。真要介绍RF工程，起码得用上一本书的篇幅，也许还不止。就本书目的而言，我将会粗略地把篇幅浩瀚的RF工程主题分为两个部分：如何产生无线电波以及如何传送无线电波。

RF零件

RF系统不但延伸了有线网络的范围，也和有线网络形成了互补关系。虽然RF系统的零件会因所使用的频率及信号的传送距离而异，不过所有系统基本上是相同的，其所使用的零件也不多。802.11的用户可能会对两种RF零件特别感兴趣：天线与放大器。之所以会对天线感兴趣，是因为在RF系统中，天线是有形的实体。而放大器和天线彼此互补，可以让天线输出更大的功率，在构建不同类型的802.11网络时，用户或许也会感兴趣。

天线

天线（antenna）是RF系统中最关键的零件，因为它们负责将线路中的电子信号转换为电波以及将电波反转为电路信号。在框图中，天线通常是以倒三角形来表示，如图10-8所示。

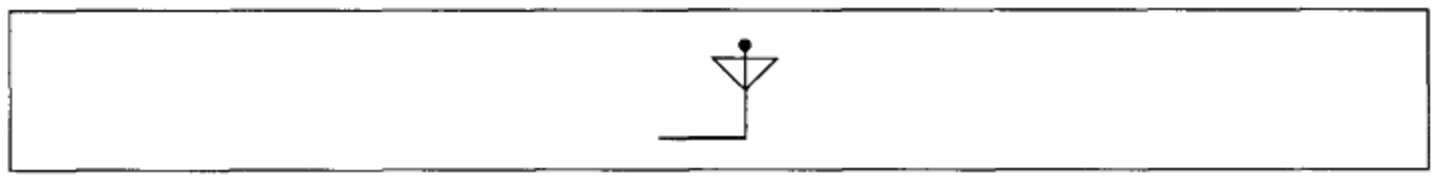


图10-8：天线示意图

天线必须以导电材料制造才能运作。无线电波遇到天线时，电子就会流入导体而产生电流；同样地，在天线施加电流就会在天线周围产生电场。施加在天线上的电流不同，电场也会随着改变。变动的电场会产生磁场，因此形成电波。

天线的长短取决于频率：频率越高，天线越短。每种频率可以使用的最短的简易型天线长度为波长的一半（虽然天线工程师可以运用一些技巧进一步缩短天线）。这个经验法则同时适用于大型无线广播天线以及移动电话所使用的小型天线。使用830 kHz频带的调幅广播电台，其电波的波长约为360米，因此必须使用大型天线。至于使用2.4 GHz频带的802.11网络接口，其波长只有12.5米。利用一些工程技巧即可将天线整合到PC无线网卡里或是膝上型计算机的LCD屏幕中。至于性能更高的外部天线，也可以让各位轻易将其放进背包或者计算机包中随身携带。

在设计上，天线也可以将方向纳入考虑。有些天线属于全向型（omnidirectional），即可以收发所有方向的信号。有些应用则受惠于定向型（directional）天线，这种类型的天线可以针对某个较窄的范围进行收发。图10-9比较了全向型与指向型天线的辐射功率。

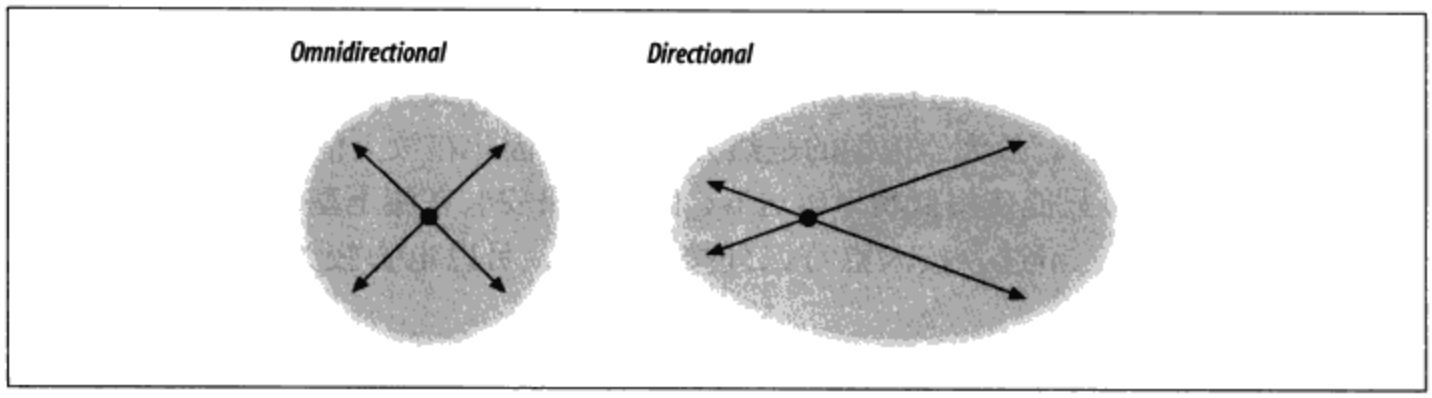


图10-9：全向型与定向型天线的辐射功率

给予等量的输入功率，定向天线可以传得较远，信号也比较清楚。在所指向的方向，它们具备较高的无线信号敏感性。以无线链路取代有线网络时通常会使用定向天线，移动通信业者划分蜂窝（cell）时通常会使用全向天线，虽然也有例外，特别是希望网络可以延伸更远的距离时。同时，应该谨记在心的是，根本没有真正的全向天线。我们通常习惯性地认为，那些垂直悬挂的天线属于全向型，因为当你在天线的水平面移动时，信号并不会有太大的改变。不过如果你以垂直角度（即由上往下或由下往上）观察信号的辐射情况，就会发现这根本是两回事。如果你正为学校校区或公司园区构建网络并且希望将天线置于大楼屋顶，就必须注意此现象。

本节所介绍的所有零件中，以天线最有可能和其他电子零件分隔两地。在这种情况下，你就得使用一条传输线（某种电电缆）连接天线与收发器。传输线通常具备50欧姆的阻抗（impedance）。

就使用2.4-GHz频带的802.11设备而言，通常PC无线网卡会采用内置天线。这种内置天线虽然可以用，但表现平平，最多只能算是中上。天线越大，性能越佳。有些802.11网卡附有外部天线接头。外接天线可以让网卡有更好的性能，不过外观质感就会因此而大打折扣。为了满足改善天线性能的需求，同时不让丑的外接天线占用空间，许多膝上型计算机厂商便将天线内置在屏幕周边的边框里。

放大器

放大器可以增强信号。信号的放大或增益程度是以分贝（decibel，简称dB）作为测量单位。放大器大致上可以分为三种：低噪声、高功率与其他种类。低噪声放大器（Low-noise amplifier，简称LNA）通常与天线连接，用来将收到的信号放大到与RF系统连接的电

子零件可识别的程度。LNA 同时也可以就噪声系数（noise factor）区分等级，噪声系数可用来评定放大器本身所带来的不相干信息。噪声系数越小，接收器就可以识别越细微的信号，因此可以涵盖较长的距离。

至于高功率放大器（High-power amplifier，简称HPA），则是用来将信号提升至最大功率后传送。输出功率是以 dBm 作为测量单位，其与 watt 有关（参见本章对“分贝与信号强度”所做的说明）。放大器依循的是热力学定律，因此在放大信号的同时会产生热量。802.11 PC Card 只能使用低功率传送器，因为如果安装在膝上型计算机中，很快就会耗尽电池的电力。不过，接入点可以外接放大器，另以电力较为充沛的电力设施（power grid）供电。

放大器与天线关系到如何符合管理规定的微妙之处。802.11 设备限定使用 1 瓦的输出功率以及 4 瓦的有效幅射功率（effective radiated power，简称 ERP）。ERP 借由天线增益（gain）减去传输线的损耗（loss），让传送器的输出功率倍增。假设你手上有个 1 瓦的放大器，所使用的天线可带来 8dB 的增益，而传输线的损耗是 2 dB，那么 ERP 即为 4 瓦，整个系统的增益为 6 dB，相当于传送器功率提高了 4 倍。

第十一章

跳频物理层

1977 年 802.11 初稿所提出的物理层标准中，跳频扩频（frequency-hopping spread-spectrum，简称 FH 或 FHSS）是最先得到广泛运用的物理层。支持跳频调制（FH modulation）的电子零件相对比较便宜，而且无需用到多大的功率。起初，采用跳频网络的主要优点在于相同区域内可以同时容纳多个网络，而且这些网络的带宽总和或吞吐量相当高。不过到目前为止，跳频网络多半已经沦为802.11历史的脚注。虽然好歹也是一种标准，不过目前只剩一家厂商仍在生产与销售跳频系统，而且这些产品也渐渐淡出市场。随着规范的高速发展，跳频系统的优势已经逐渐消逝，何况新型芯片组更为省电，功耗更低。

本章描述了 FH PHY（跳频物理层）的基本概念及其所使用的调制技术。此外，还会交代物理层会聚过程（physical layer convergence procedure）如何打造传送至无线链路的帧并简单提及无线媒介本身的一些细节。到目前为止，FH PHY 已经成为802.11历史的脚注，所以各位可以跳过本章，直接阅读下一章所讨论的DS PHY（直接序列物理层）。然而，若能掌握 802.11 的技术演进，可让你更清楚全貌。

跳频传输

所谓跳频，是以一种预定的（predetermined）伪随机模式（pseudorandom pattern）快速变换传输频率，如图 11-1 所示。图中的纵轴将可用频率划分为几个频隙（frequency slot）；同样地，时间轴也被划分为一系列时隙（time slot）。这些隙（slot）的使用方式由跳频模式来控制。本图所使用的跳频模式为{2,8,4,7}。正确掌握跳频时机是关键，发送端与接收端必须同步，这样接收端才可以随时与发送端的频率保持一致。

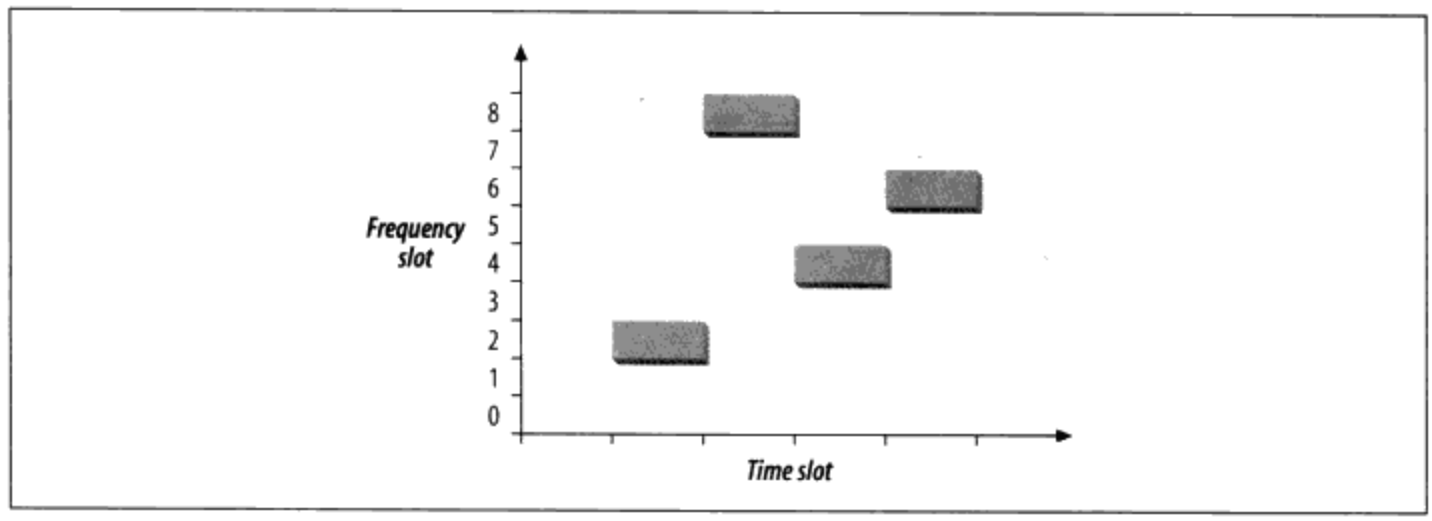


图 11-1：跳频

跳频有点类似于频分复用（frequency division multiple access，简称 FDMA），不过有项重要差异。FDMA 系统会为每个设备分配固定的频率。这些设备共同分享可用的无线频谱，各自使用不同的频率。跳频系统所使用的频率会依时间而有所不同，并非一成不变。每个频率只使用一小段时间，称为驻留时间（dwell time）。

最重要的是，跳频可以避免设备干扰某个频带（frequency band，简称 band）的主要用户。这种做法之所以可行，是因为各个窄频带的主要用户有权使用较高的功率，传送足以覆盖无线局域网络的信号。跳频用户对主要用户只会造成瞬间干扰，因为跳频会将能量分散至较宽的频带（注 1）。同样地，主要用户只会影响扩频设备的某个频隙，就像是瞬间的噪声一样。图 11-2 显示了某个主要用户使用第 7 个频隙时所造成的影响。虽然第 4 个时隙的传送受到损毁，但前 3 个时隙还是可以成功传送。

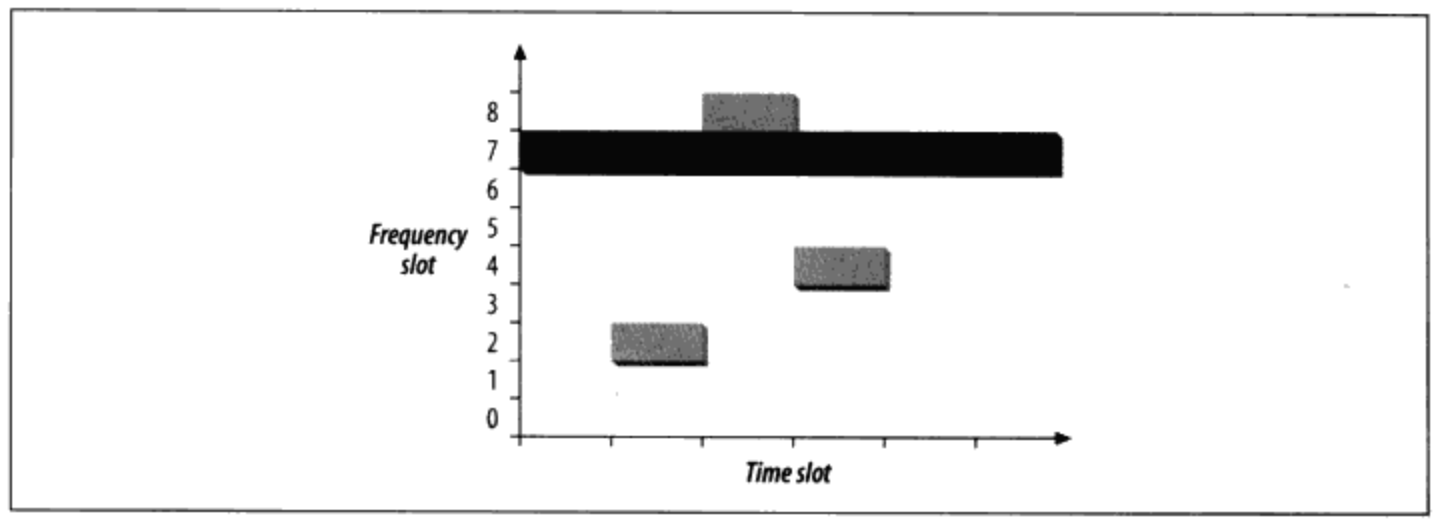


图 11-2：以跳频避免干扰

注 1：　如果某个频带的主要用户遭到其他次要用户的干扰，管理者可以（并且将会）介入予以停用次要用户，所以扩频调制技术必须以低功率进行传输。

如果两个跳频系统需要共享相同频带，可以指定不同的跳频顺序，如此便不会互相干扰。在同一时间内，每个跳频系统必须使用不同的频隙。只要两个系统使用不同的频隙，就不会互相干扰，如图 11-3 所示。和之前的图形一样，灰色方块的跳频序列为{2,8,4,7}，其中加入了跳频序列为{6,3,7,2}的第二个跳频系统。彼此不相重叠的跳频序列称为正交(orthogonal)。在同一区域使用多个 802.11 网络时，正交跳频序列可以使总吞吐量达到最高。

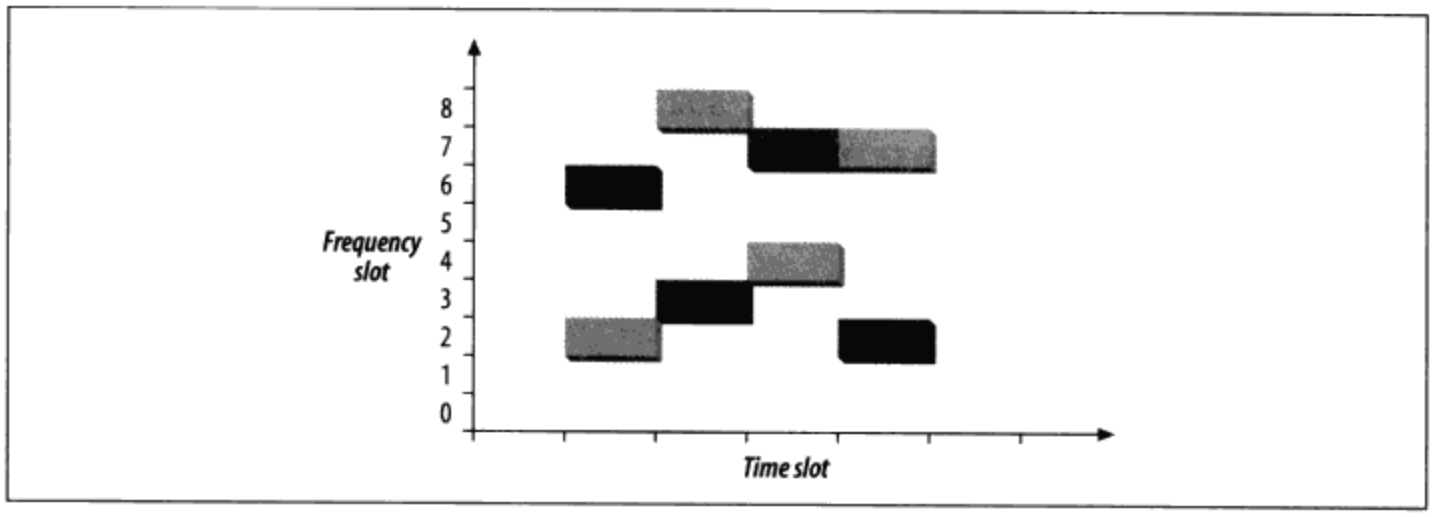


图 11-3：正交跳频序列

802.11 FH 的细节

802.11 将 ISM 微波频带划分为一系列 1-MHz 的信道（channel）。几乎 99% 的微波能量都被限制在信道中。802.11所使用的调制方式会将数据位编码成信道中央所传送频率的偏移量。信道是以中心频率（center frequency）来定义的，信道 0 的中心频率为 2.400 GHz。之后每个信道会依次加上 1-MHz：信道 1 的中心频率为 2.401，信道 2 的中心频率为 2.402，一直到中心频率为 2.495 GHz 的第 95 信道。能够使用 ISM 频带的哪些部分，依管理者的规定而有所不同。主要的管制区（regulatory domain）及其可用信道列于表 11-1。

表 11-1：不同管制区所使用的信道

管制区	可用信道
美国（FCC）	2 至 79（2.402~2.479 GHz）
加拿大（IC）	2 至 79（2.402~2.479 GHz）
欧洲（不含法国与西班牙）（ETSI）	2 至 79（2.402~2.479 GHz）
法国	48 至 82（2.448~2.482 GHz）
西班牙	47 至 73（2.447~2.473 GHz）
日本（MKK）	73 至 95（2.473~2.495 GHz）

802.11 FH 系统所使用的驻留时间为390个单位时间（time unit），相当于0.4秒。当802.11FH PHY在信道间进行切换时，整个跳频过程不能超过224微秒。跳频本身必须符合额外的管制规定，不论是跳频数的多少，还是跳频的发生率。

802.11 跳频序列

用以推算跳频集合（hop set）的数学函数属于FH PHY规范的一部分，记载于802.11规范说明书的14.6.8款。举例而言，北美与欧洲大部分地区所使用的跳频序列1，其跳频顺序为{3,26,65,11,46,19,74,50,22, …}。802.11进一步将跳频序列区分为彼此不重叠的集合，同一集合的成员（即跳频序列）间彼此正交。在欧洲与北美，每种组合包含26个成员。有些地区的管理者会限制可跳频的信道数，因此每个集合包含较少的成员，详见表11-2。

表11-2：每个管制区中跳频集合的大小

管制区	跳频集合的大小
美国（FCC）	26
加拿大（IC）	26
欧洲（不含法国与西班牙）（ETSI）	26
法国	27
西班牙	35
日本（MKK）	23

加入 802.11 跳频网络

跳频序列的标准化使加入跳频网络成为可能。FH 网络的Beacon帧包含时间戳（timestamp）以及FH参数集元素（FH Parameter Set element）。FH参数集元素包含跳频模式编号（hop pattern number）以及跳频索引（hop index）。收到Beacon帧后，工作站就会知道如何同步本身的跳频模式。

工作站可根据跳频序列编号（hop sequence number）得知道自己的跳频次序。举例而言，假设有个工作站收到Beacon帧，表示该BSS使用了编号为1的北美/欧洲跳频序列，而且当前的跳频索引为2。只要查询跳频序列，该工作站就可以判断下个信道为65。跳频时间也有明确的定义。每个Beacon帧均包含一个Timestamp（时间戳）字段，当以时间戳对Beacon帧中驻留时间取模（modulo）的结果为0时，就会发生跳频。

ISM 发射量规定与最大吞吐量

802.11跳频系统受到频谱分配策略的规范。举例而言，以下是美国FCC所提出的三项主要规定（注 2）：

1. 频带必须至少包含 75 个可供跳频的信道，占用 83.5-MHz 的带宽。
2. 跳频信道所使用的带宽不得大于 1 MHz。
3. 设备必须平等对待每个可用信道。30 秒的周期内，每个信道不能驻留超过 0.4 秒。

在这些规定中，以第二项最为重要。不论使用多么神奇的编码机制，任何时刻都只能使用 1 MHz 带宽。虽然因为另两项规定，信道会不断变动，但第二项规定无疑限制了用来编码数据的信号变化量。

如果采用两级编码，每个周期可以编码一个位。以每周期一个位而言，1 MHz 可以提供 1 Mbps 的数据传输率。较复杂的调制与解调制机制可以提高传输率。四级编码可以在一个周期内封装两个位，因此 1-MHz 带宽可以提供 2 Mbps 的传输率。

欧洲电信标准协会（European Telecommunications Standards Institute，简称ETSI）同时也为使用 ISM 频带的扩频设备制定了一组规范，记载于欧洲电信标准（European Telecommunications Standard，简称ETS）300-328。ETSI 规定允许使用较少的信道，只需要20个就够了。不过，ETSI 对于辐射功率的管制就严格得多。实际上，为了同时符合FCC与ETSI的规定，设备通常会使用FCC所要求的信道数搭配ETSI所规定的辐射功率。

干扰效应

802.11 是第二个使用 2.4-GHzISM 频带的标准，因此不得不接受来自其他传输的干扰，这些传输通常有较高的优先级。严重的干扰可能导致某个信道不能使用，不过其他信道却不受影响。以美国和欧洲的大约80个可用信道来讲，一个信道受到干扰，最多会使媒介的原始位率（raw bit rate）降低 1.25%（在 IP 层通常必须付出较高的代价，因为还要将帧间间隔、确认信息、帧头以及物理层会聚过程标头计算在内）。有越多信道受到干扰，传输量就越低。参见图 11-4。

注 2： 这些规定详见 FCC 法规的 15 节 247 款（47CFR 15.247）。

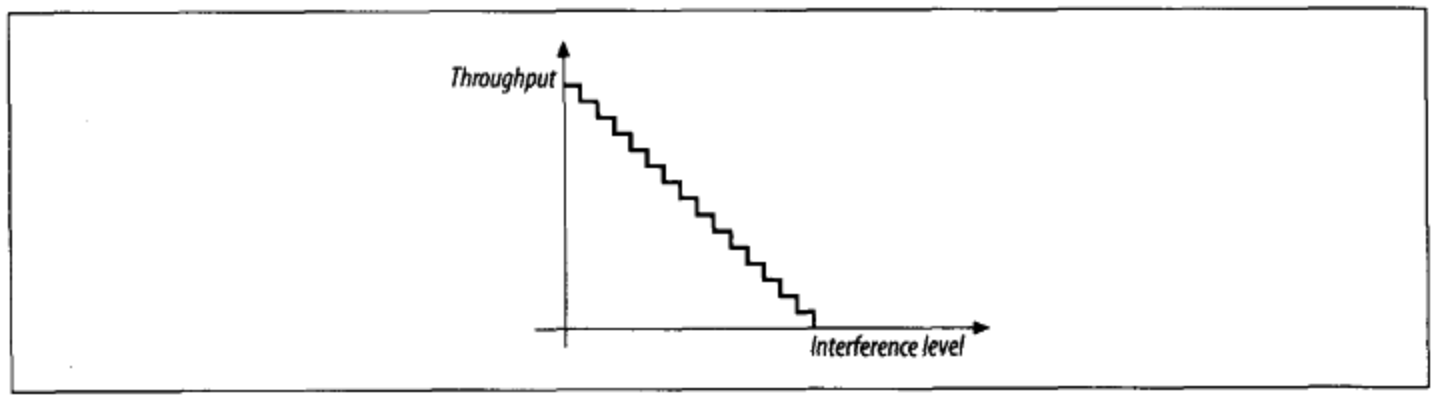


图 11-4：干扰对 FHSS 系统的吞吐量的影响

高斯频移键控（GFSK）

FH PHY 采用了高斯频移键控（Gaussian frequency shift keying，简称 GFSK）（注 3）。频移键控就是将数据编码成载波（carrier）中一系列的频率变动。将数据编码成频率的好处是噪声通常会随信号的振幅而改变，与振幅无关的调制系统（例如，调频广播）通常能够免于噪声的干扰。GFSK 中的“Gaussian”意指电波脉冲的形状（译注 1），GFSK 将能量的发散限定在相对较窄的频带中，因此适合作为频带的再利用（secondary use）工具。防止 RF 能量泄漏的信号处理技术着实不错，对某个频带的再利用者（secondary user）而言尤其如此。借由降低干扰的可能性，GFSK 让 802.11 无线局域网络能够构建在某个频带已经有更高优先用途的地区。

两级 GFSK

最基本的 GFSK 实现称为两级 GFSK（2-level GFSK，简称 2GFSK）。其中使用了两种频率，分别表示为 0 或 1。要传送 1，就会将载波频率提高一个特定量；至于 0，则是将载波频率减少一个特定量。图 11-5 显示了一般的编码过程。实际系统上所使用的载波频移量较小，为了说明编码的运作方式，本图刻意画得比较夸张。

通过系统所传输的数据率称为符号率（symbol rate）。由于必须经过几个周期以后才有办法判断所使用的载波频率以及其所传送的信号究竟为 1 还是 0，通常符号率只是载波频率的零头。虽然载波频率约有每秒24亿个周期，但符号率通常每秒只有一两百万个符号。

注 3：“键控”（*keying*）是电报通信年代残留下来的名词。数据通过电报线路传送时需要按键。虽然现代的数字系统是通过调制技术来传送数据，不过还是继续使用“键控”这个词。

译注 1：即钟形曲线（bell shaped curve）。钟形曲线又称高斯曲线（Gaussian curve）。

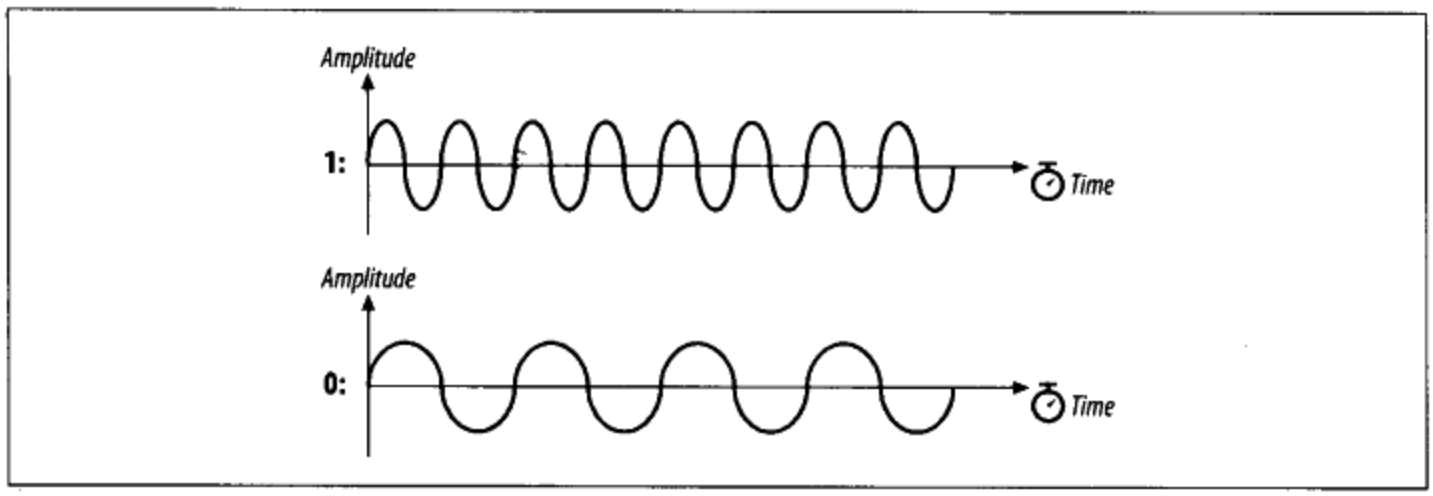


图 11-5：两级 GFSK

GFSK 的频率变动并不剧烈。瞬间频率变动较大则需要使用较贵的电子零件以及较高的功率。较缓和的频率变动可以降低设备的成本，RF 泄漏（leakage）也较低。图 11-6 说明了以2GFSK为字母M（二进制码为1001101）进行编码时的频率变动情况。要特别注意的是，图中纵轴代表传输频率。传送 1时，频率会提升至中心频率以上，相当于中心频率加上特定偏移量。传送0时，频率则以相同偏移量下降。代表时间的水平轴被分割为许多符号周期（symbol period）。在每个周期中点，接收器会对传输频率进行测量，同时将该频率转换为符号（symbol）。（在802.11跳频系统中，较高级的数据在传送前会经过扰频（scrambled），因此要传送给对方的位顺序不一定和空气中的位顺序相符。本图纯粹在说明 2GFSK 的运作原理，不涉及实际的编码。）

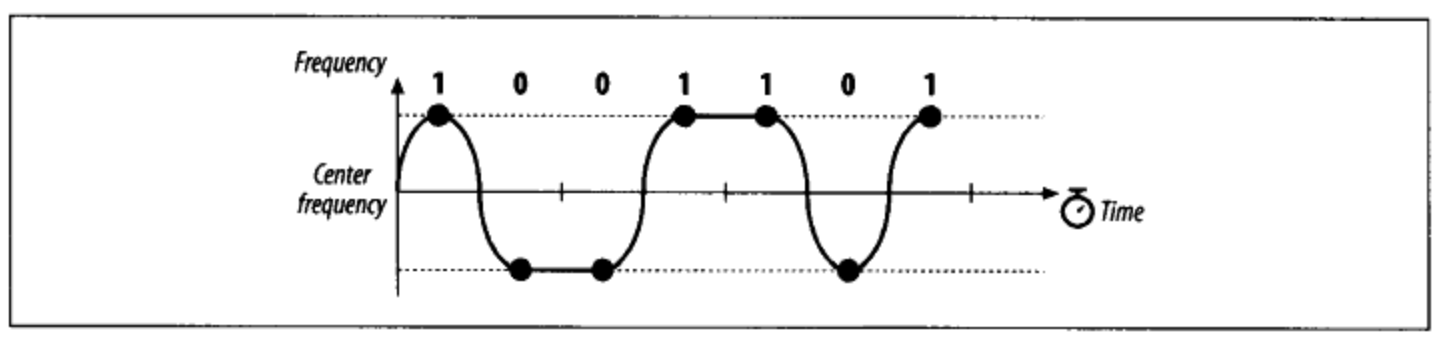


图 11-6：以2GFSK 对字母 M 进行编码

四级 GFSK

利用此机制，你可以有两种传送更多数据的方式：使用较高的符号率，或者在每个符号中编码更多位信息。四级 GFSK（4-level GFSK，简称 4GFSK）基本上和 2GFSK 采用相同的方式，不过使用四种符号。这四种符号（00、01、10 与 11）会分别对应到特定的离散频率（discrete frequency），因此在符号率相同的条件下，4GFSK 可以传送两倍的数据。显然，这并非毫无代价：4GFSK必须使用较复杂的发射器与接收器。符号与频率之间的对应关系如图 11-7 所示。

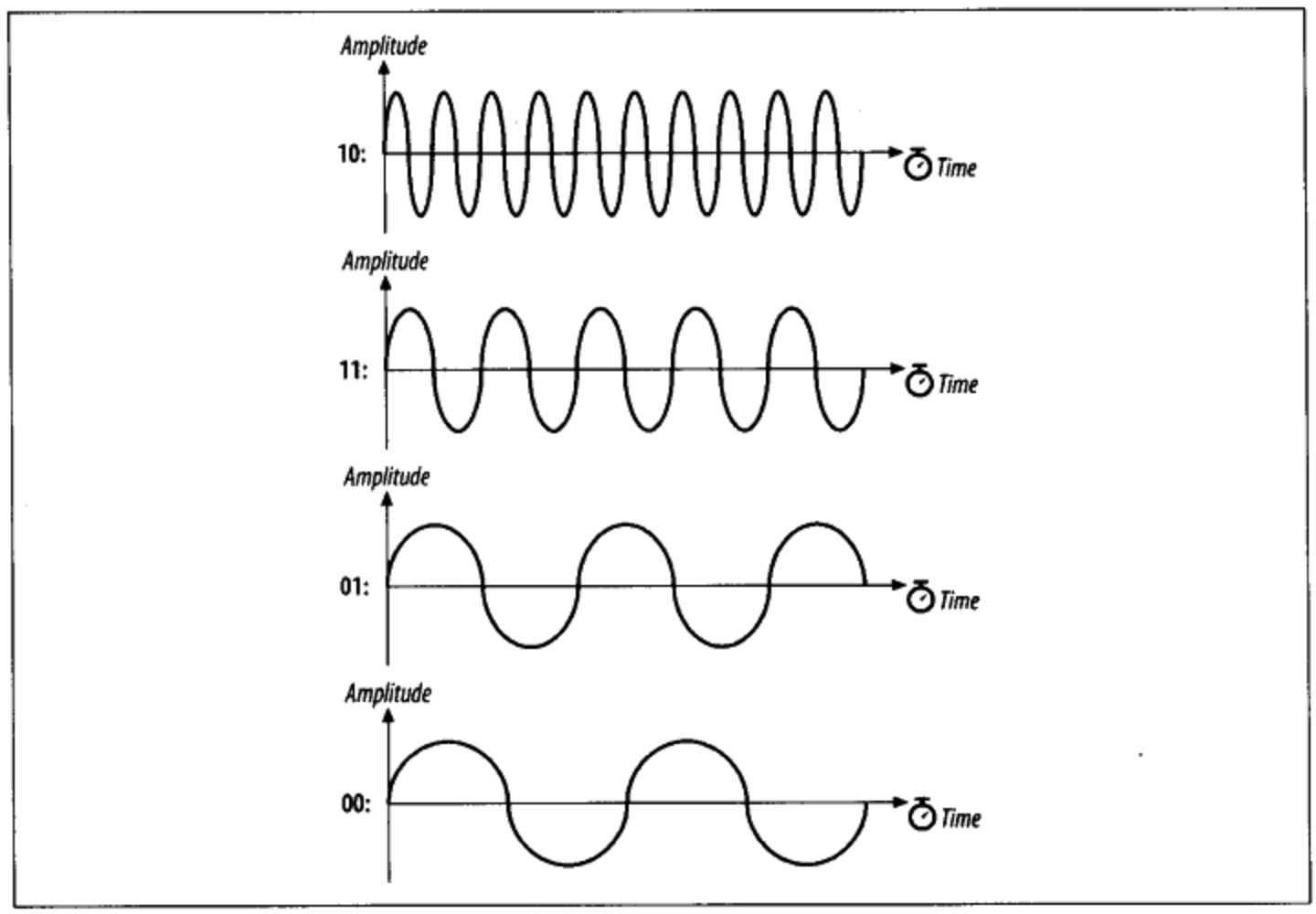


图 11-7：4GFSK 的符号与频率的对应关系

采用比较复杂的信号处理方式，4GFSK 可以在单一符号中封装更多位。图 11-8 说明了如何对字母 M 进行编码。再次强调，纵轴代表频率，横轴分割为许多符号时间。符号的传输是通过频率的变动来完成，每个符号的频率如虚线所示。本图其实暗示了 GFSK 编码方式在提高位率时必须面对的问题。区分两种信号十分简单，四种就比较困难。位率每提高两倍，信号电平也就变为两倍，RF 组件就必须区分更细微的频率变动。实际上，这些限制使得 FH PHY 局限于 2 Mbps。

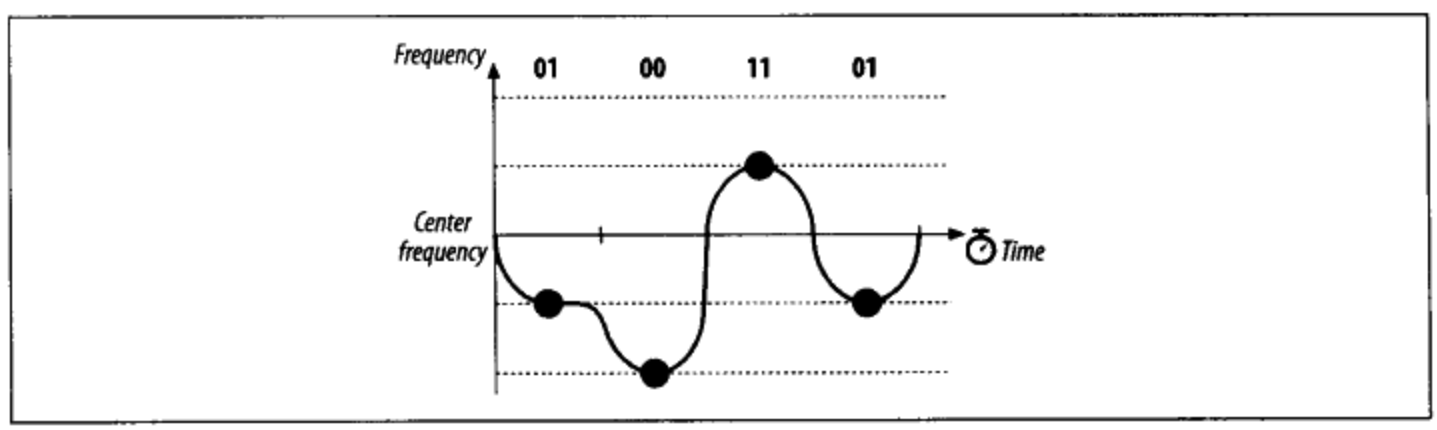


图 11-8：以 4GFSK 对字母 M 进行编码

FH PLCP

在帧被调变至RF载波之前，来自MAC的帧必须先经过物理层会聚过程（Physical Layer Convergence Procedure，简称PLCP）加以处理。不同的物理层可能有不同的需求，因此802.11允许物理层在处理即将传送至空气的MAC帧时可以有某种程序的自由。

成帧（Framing）与白化（Whitening）

FH PHY所使用的PLCP会在MAC传来的帧前面加上标头，其中包含5个字段。PLCP是位于MAC以及PMD（物理媒介相关）无线接口之间的中继站。以ISO参考模型的术语来讲，从MAC传来的帧属于PLCP服务数据单元（PLCP service data unit，简称PSDU）。PLCP的成帧格式如图11-9所示。

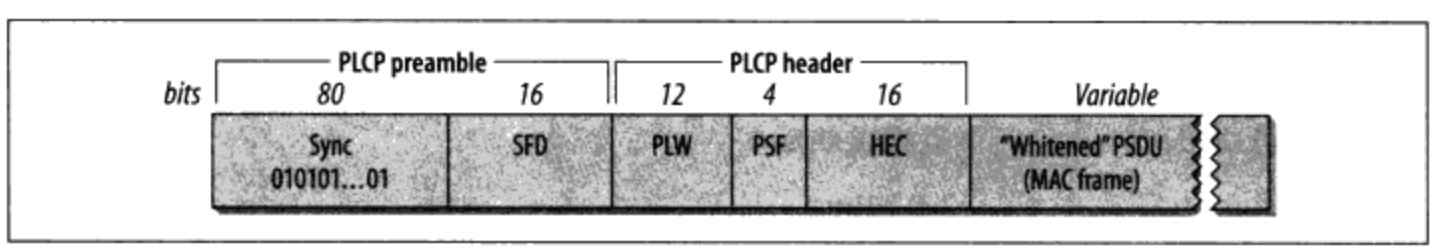


图11-9：FH PHY中的PLCP成帧格式

Preamble（前导码）

和有线Ethernet一样，Preamble（前导码）是用来同步发射器与接收器，以维系两者之间的定时关系。在802.11 FH PHY中，前导码是由Sync（同步）以及Start Frame Delimiter（起始帧定界符，简称SFD）两个字段组成。

Sync（同步）

Sync字段的长度为80个位，由一系列01交替的序列（010101…01）组成。工作站会找寻此同步模式（sync pattern），准备接收数据。除了同步发送端与接收端，Sync字段还有其他三种目的。首先，前导码的出现代表帧即将到来。其次，有些工作站的天线不只一个，这样可防范多径衰落（multipath fading）或其他环境所造成的接收问题。这些工作站可以选用收到最强信号的天线。最后，接收端可以衡量所收到信号的频率是否偏离正常值，如有必要则加以校正。

Start Frame Delimiter（起始帧定界符，简称SFD）

和Ethernet一样，SFD用来指示前导码的结束以及帧的开始。FH PHY采用的是16位的SFD：0000 1100 1000 1101。

Header（标头）

前导码之后紧跟着是PLCP标头。此标头包含PLCP所使用的物理层专属参数。它

由三个字段组成：一个长度字段（PLW）、一个速度字段（PSF）以及一个帧校验码（HEC）。

PSDU Length Word（PSDU 长度字，简称 PLW）

PLCP标头的第一个字段是PLW。PLCP帧的有效载荷（payload）为长度可达4095个字节的MAC帧。这个字段的长度有12个位，用以通知接收器PLCP标头之后的MAC帧的长度。

PLCP Signaling（PLCP 信令，简称 PSF）

位0，即第1个被传送出去的位，目前保留不用而设定为0。位1~3是所承载的MAC帧的传输率编码。由于有几种速度可供选择，因此这个字段可供接收器调整适合的解调制机制。虽然802.11标准允许你使用速度介于1.0 Mbps与4.5 Mbps之间、增量为500kps的数据传输率，但目前只为1.0 Mbps与2.0 Mbps两种速度定义调制机制（注4）。参见表11-3。

表11-3：PSF的意义

位（1-2-3）	数据传输率
000	1.0 Mbps
001	1.5 Mbps
010	2.0 Mbps
011	2.5 Mbps
100	3.0 Mbps
101	3.5 Mbps
110	4.0 Mbps
111	4.5 Mbps

HEC（Header Error Check，头部差错校验）

为了防止PLCP标头错误，因此使用长度为16个位的CRC来校验整个标头的内容并置于此字段。不过此标头并未防范帧的其他部分的错误。

对于Data字段所放置的内容并无任何限制。任何数据均包含一长串连续的0或1，这使得数据看起来不是那么随机。为了让所要传送的数据比较像是随机的白噪音（white noise），FH PHY将会以一种白化算法（whitening algorithm）对MAC帧进行处理。此算法会在电波传送之前对数据进行扰频。接收器则是通过逆向处理来还原数据。

注4：未来似乎不太可能继续开发高速跳频系统。如果需要更高的数据传输率，直接序列是较具成本效益的选择。

FH PMD

虽然PLCP标头里有一个记载MAC帧传输率的字段，不过其中只有两种符合PMD子层标准。这两种PMD之间具有许多共同特性，例如：支持天线分集（即多重天线），允许启用或关闭天线内置的功率放大器，以及使用高斯脉冲成形器（Gaussian pulse shaper）尽量将RF能量限制在狭窄的跳频频带。图11-10显示了802.11跳频网络所使用的收发器的一般设计。802.11标准规定，以1 Mbps或2 Mbps传送时，收发器必须至少具备−80 dBm的灵敏性。

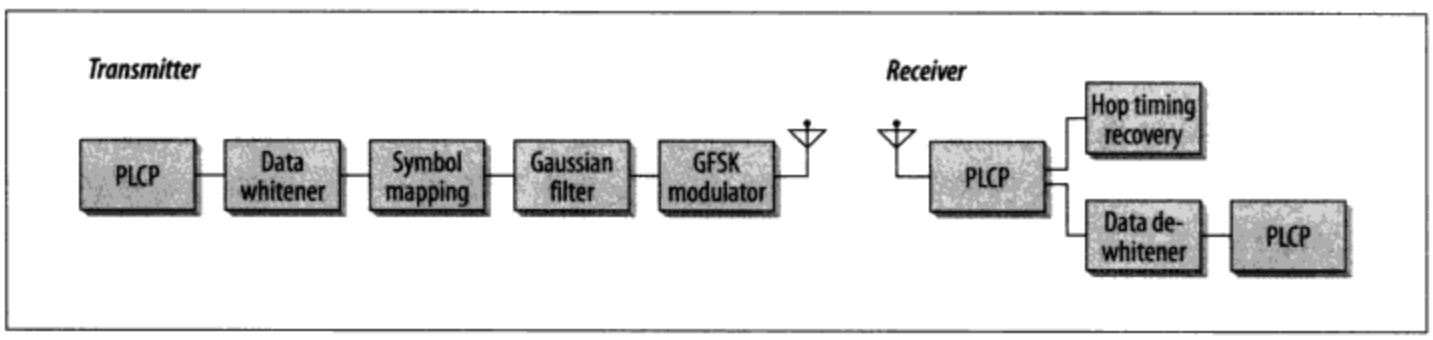


图11-10：跳频收发器

传输率为1.0-Mbps的FH PHY所使用的PMD

基本的跳频PMD（物理媒介相关）允许1.0 Mbps的数据传输率。来自MAC的帧已经附加上了PLCP标头，所产生的位序列会从无线电波接口传送出去。为了符合1-MHz的带宽管制，每秒只能传输100万个符号。由于所采用的调制机制为2GFSK，因此每个符号可以编码1个位。802.11规定所使用的最小功率为10毫瓦，同时要求使用功率控制，必要时将辐射功率限定在100毫瓦。

传输率为2.0-Mbps的FH PHY所使用的PMD

FH PHY还有另外一种较高速的PMD可以使用。和1.0-Mbps的PMD一样，附加上PLCP标头之后，再利用2GFSK以1.0 Mbps的速率进行传输。在PLCP标头中，PSF字段所代表的是帧主体（frame body）的传输率。采用较高的数据传输率时，帧主体则会使用不同于物理层标头的编码方式。管制上要求所有PMD只能使用1 MHz的符号率，因此4GFSK只能用于帧主体。每个符号分别代表2个位，因此每秒100万个符号可以达到2.0 Mbps的数据率。如果信号质量太差无法使用较高速率，支持2.0-Mbps的PMD的固件可以降速而改用1.0-Mbps的PMD。

载波监听/空闲信道评估（CS/CCA）

为了落实802.11的CSMA/CA功能，PLCP包含了一种功能，可借以判断当前无线媒介是否正在使用。MAC不仅使用虚拟载波监听机制，还使用了物理载波监听机制，而物理载波监听是由物理层所负责。802.11并未规范如何决定信号是否存在，只要能够符合标准所要求的性能，厂商可以自由决定如何实现。802.11规定，信号检测能力必须符合最起码的要求，至少要能够检测到具有一定功率且与802.11兼容的信号。

FH PHY的特性

表11-4列出了FH PHY（跳频物理层）里的一些参数值。除了该表所列的标准化参数，FH PHY尚有一些参数可供调整，让802.11跳频系统各部分的延迟能够维持均衡，其中包括MAC、PLCP、收发器等的延迟变量以及收发器电子零件个别变异的相关参数。另外值得注意的是，同一区域所有跳频网络的整体吞吐量（total aggregate throughput）相当高。整体吞吐量是跳频集合大小的函数。在每个跳频集合中，所有序列彼此保持正交关系，不会互相干扰。在北美与欧洲大部分地区，每个区域同时可以构建26个跳频网络。如果每个网络的传输率为2 Mbps，其中有一半时间是用来传递有效载荷数据（user payload data），只要ISM频带没有什么干扰存在，该区的总吞吐量即可高达26 Mbps。

表11-4：FH PHY参数

参数	值	备注
时隙时间	50 μs	
SIFS时间	28 μs	SIFS可用来推衍出其他帧间间隔值（DIFS、PIFS以及EIFS）
竞争窗口的大小（contention window size）	15至1 023个时隙	
前导码持续时间（preamble duration）	96 μs	前导码符号以1 MHz的速率进行传输，因此传输每个符号需时1 μs，96个位则需要96个符号时间
PLCP标头持续时间（PLC pheader duration）	32 μs	PLCP标头有32个位，因此需要用到32个符号时间
最大MAC帧（maximum MAC frame）	4095个字节	802.11建议最多使用400个符号（1Mbps使用400个字节，2 Mbps使用800个字节），以便在不同环境下维持性能的一致性
最低灵敏度（minimum sensitivity）	−80 dBm	

第十二章

直接序列物理层：DSSS与HR/DSSS (802.11b)

1997年首次修订的802.11规范说明书规范了采用直接序列扩频（direct sequence spread spectrum，简称DSSS）技术的第二种物理层。802.11直接序列扩频物理层的数据率为1 Mbps与2 Mbps。虽然动作速度与跳频物理层相同，不过人们很快就发现，直接序列技术有潜力达到比跳频技术还快的速度。因此就算当时两者速度相当，直接序列还是成为了物理层的首选。1999年，802.11b规范了数据率可达5.5 Mbps与11 Mbps的物理层。之前1 Mbps与2 Mbps的物理层通常与后来的5.5 Mbps与11 Mbps物理层合并为单一接口，即使它们的规范并不相同（它通常被称为802.11b，虽然这两个较低的速率并不属于802.11b）。本章将会介绍直接序列物理层（DS PHY）的基本概念以及所采用的调制技术。除了说明PLCP如何处理即将通过电波链路传送的帧，本章还会简短交代物理媒介本身的一些细节。

直接序列传输

直接序列传输是一种不同的扩频技术，可以通过较宽的频带传送信号。直接序列技术的基本运作方式，是通过精确的控制将RF能量分散至某个宽频带。当无线电载波的变动被分散至较宽的频带时，接收器可以通过相关处理（correlation process）找出变动所在。图12-1以比较抽象的方式说明了直接序列的基本运作方式。

位于图左的是传统的窄带无线电信号。信号经过扩频器的处理后，以数学转换公式将窄带输入信号的振幅平坦化，分布至相对较宽的频带。对窄带接收器而言，经过直接序列扩频处理的信号就像一些低电平噪声，因为RF能量已被扩展至较宽的频带。直接序列

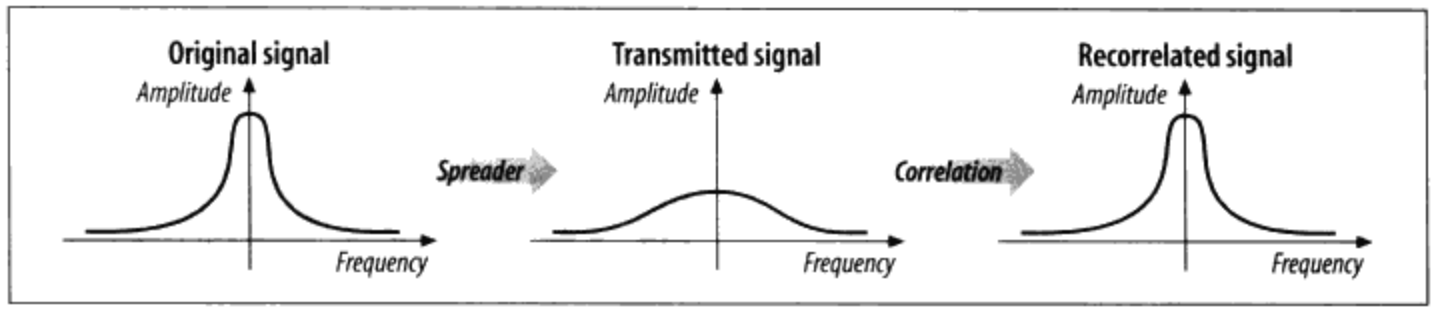


图 12-1：基本的 DSSS 动作方式

传输的关键是 RF 载波的任何调制也同时被扩展至整个频带。接收器可以监视某个宽频带并找寻影响整个频带的变动所在。原始信号可以通过相关器（correlator）还原，只要逆转整个扩频过程即可。

从更高的水平来看，相关器只是在找寻影响整个频带的RF信号变动。相关性（correlation）所提供的防护使得直接序列传输可以抗拒很多的干扰。噪声通常是以突波或脉冲形式出现，相对而言所占的频带较窄。在定义上，这类脉冲并不会影响整个频带。因此，相关函数（correlation function）会将噪声扩展至整个频带，所以经过相关处理的信号完全不受影响，如图 12-2 所示。

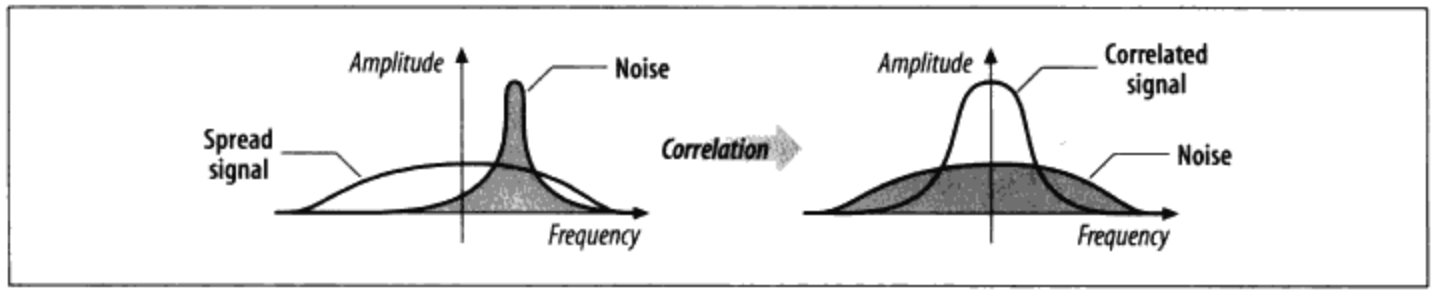


图 12-2：以相关处理扩展噪声

直接序列调制的运作方式是以扩频码（chipping sequence，或译为碎片序列）对数据流进行处理。*chip*（碎片）是扩频过程中所使用的二进制数字。bit（位）属于比较高级的数据，chip（碎片）则是编码过程中使用的二进制数字。bit 与 chip 之间并不存在任何数学上的差异。扩频开发人员之所以采用这个术语，是为了表明 chip 虽属编码与传输过程的一部分，然而本身并未携带任何数据。扩频码也称为伪随机噪声码（PN code），其传输率必须高于底层数据（直接序列物理层的主要功耗在于使用高频振荡器来产生碎片流或者还原数据）。图12-3显示了在直接序列调制的数据传输过程中扩频码所扮演的角色。位于图左的是单一数据位，其值为 1 或 0。每个数据位都会用到好几个碎片。图中，碎片流是由 11 个位所组成的扩频码。扩频码与数据字节合并后产生了携带数据位的 11 个碎片。这 11 个碎片 / 单一数据位序列是通过无线链路来传送。接收端会以同样的碎片流（即扩频码）来比较这 11 个碎片块。如果与扩频码相符，则所还原的数据位为 0；如果不符，则所还原的数据位为 1。

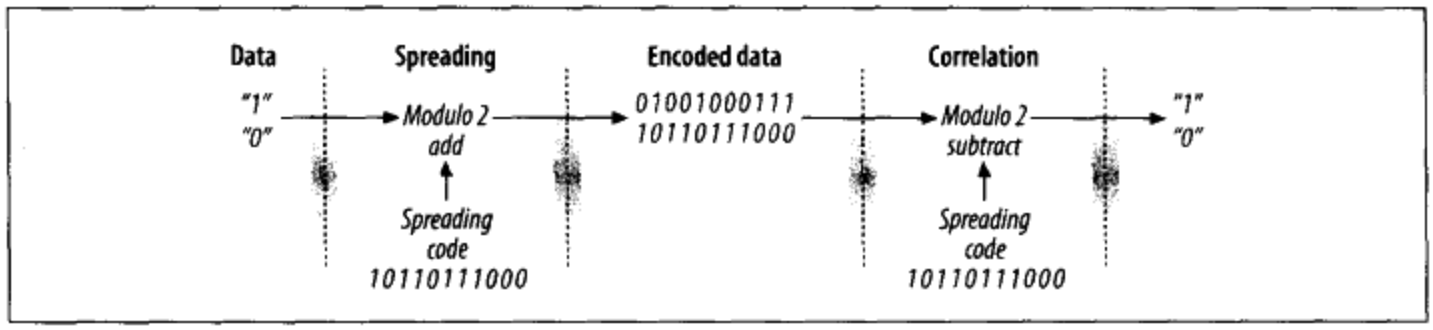


图 12-3：加入扩频码

以较高的碎片率（chip rate）对较低的位率（bit rate）信号进行编码，会产生信号功率被扩展至较宽频带的副作用。直接序列系统最重要的特性之一即是扩频率（spreading ratio），表示传输单一位（bit）必须使用多少个碎片（chip）（注 1）。较高的扩频率可以提高信号的还原能力，不过需要使用较高的碎片率及较宽的频带。将扩频率提高两倍需要用到两倍的碎片率，也需要用到两倍的带宽。增加碎片率需要付出两种成本。直接成本就是必须使用价格比较昂贵、可以在较高频率运作的 RF 零件，而间接成本则是所需要的带宽。因此在设计直接序列系统时应该尽量将扩频率压低，这样在符合设计需求的同时还可以避免浪费带宽。

直接序列调制是以带宽交换传输量。相比较于传统的窄带传输，直接序列调制显然需要更多无线电频谱，速度也比较慢。不过，它通常可以跟其他干扰源共存，因为接收器的相关函数（correlation function）有效地排除了窄带噪声。相比较于跳频，直接序列技术也比较容易提升吞吐量。管理者并未限制频谱的使用量，通常限制的反而是处理增益的最低下限。使用较宽的频带可以达到较高的传输率，不过较宽的频带需要使用较高的碎片率。

802.11 直接序列网络的编码方式

802.11采用11个位的Barker word作为扩频码（PN code）。每个比特位均以Barker word进行编码。Barker word 及其属性的详细探讨已超出本书的范围。对 802.11 网络而言，Barker word的关键属性就是具备良好的自动相关（autocorrelation）性质，即接收器所使用的相关函数在绝大多数环境中的表现均合乎预期，而且相对能够容忍多径衰落。Barker word之所以使用 11 个位，是因为管理者通常要求直接序列系统必须有 10 dB 的处理增益（processing gain）。每个位配置 11 个位的扩频码可让 802.11 符合管制要求，

注 1：扩频率（spreading ratio）关系到所谓的处理增益（processing gain）。有时候，这两个名词相互通用，不过处理增益必须将系统的实际损耗纳入考虑，因此其值稍微低于理想中的扩频率。

而且还留有一点安全边界。以11个位作为扩频码并不算多，因此可以容纳更多的重叠网络。较长的扩频码可以得到较高的处理增益，不过需要使用较大的带宽。

802.11 使用 Barker 序列{+1, −1,+1,+1, −1,+1,+1,+1, −1, −1, −1}作为扩频码。用在802.11时，+1 更换为 1，而 −1 更换为 0。因此 Barker 序列就变成了 10110111000。模2的加法器（modulo-2 adder）会将之运用到数据流的每个位（注 2）。如果编码对象为1，扩频码所有位均会改变；如果编码对象为 0，就会保持不变。图 12-4 说明了整个编码过程。

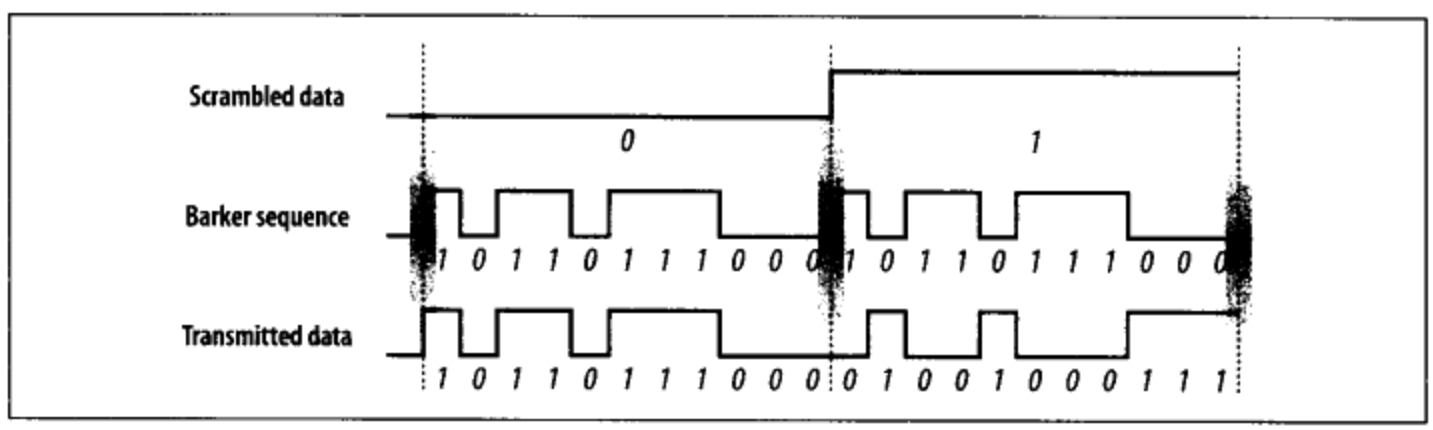


图 12-4：以 Barker word 进行编码

接收器可以定期查看所收到的位中包含多少个 1。Barker 序列本身有 6 个 1 和 5 个 0。只要11个位序列中包含 6 个 1，就代表所传送的是 0；如果其中包含 6 个 0，则代表所要传送的是 1。除了计算 1 与 0 的数目，接收器也可以通过位模式的分析，推论出所传送的位的实际值。

802.11 直接序列网络所使用的无线电频谱

相比较于 FH PHY，DS PHY 所使用的信道较宽。DS PHY 在 2.4-GHz 频带使用了 14 个信道，每个信道的带宽为 5 MHz。信道 1 位于 2.412 GHz，信道 2 位于 2.417 GHz，依此类推至位于 2.472 GHz 的信道 13。信道 14 是特别针对日本所定义的，其中心频率与信道 13 的中心频率相差 12 MHz。表 12-1 显示了每个管理者允许使用哪些信道。北美与欧洲均允许使用信道10，这也就是为什么大部分产品均以信道10作为默认操作信道。

注 2：以Baker序列进行编码的技术和一些无线电话系统所使用的码分多址复用(code division multiple access，简称 CDMA）技术类似。此技术让多个工作站（手机）得以同时访问无线媒介。CDMA 采用相当复杂的数学运算，以确保每部手机的传输对其他位于同一蜂窝的手机而言就像是随机的噪声。其所涉及的数学运算远比固定的伪随机噪声码复杂许多。

表12-1：各管制区所使用的信道

管制区	可用信道
美国（FCC）／加拿大（IC）	1 至 11（2.412~2.462 GHz）
欧洲，不含西班牙（ETSI）	1 至 13（2.412~2.472 GHz）
西班牙	10 至 11（2.457~2.462 GHz）
日本（MIC）	1 至 13（2.412~2.462 GHz）与 14（2.484 GHz）

信道能量的分布

每个信道中，大部分的能量会分布在 22-MHz 的频带。因为 DS PHY 使用的是 11-MHz 的芯片时钟频率，能量会从信道中心以 11 MHz 的倍数分散出去，如图 12-5 所示。为了避免干扰相邻的信道，第一个旁瓣（sidelobe）会经过处理，使之小于信道中心频率能量 30 dB。第二个旁瓣经过处理，使之小于信道中心频率能量 50 dB。这相当于分别将能量降低 1000 倍与 100000 倍。这些限制在图 12-5 中是以 dBr 注记，即与信道中心能量的相对 dB 值。图 12-5 使用的是对数刻度（logarithmic scale）：30 dBr 其实代表 1000，而 −50 dBr 则代表 10 万。

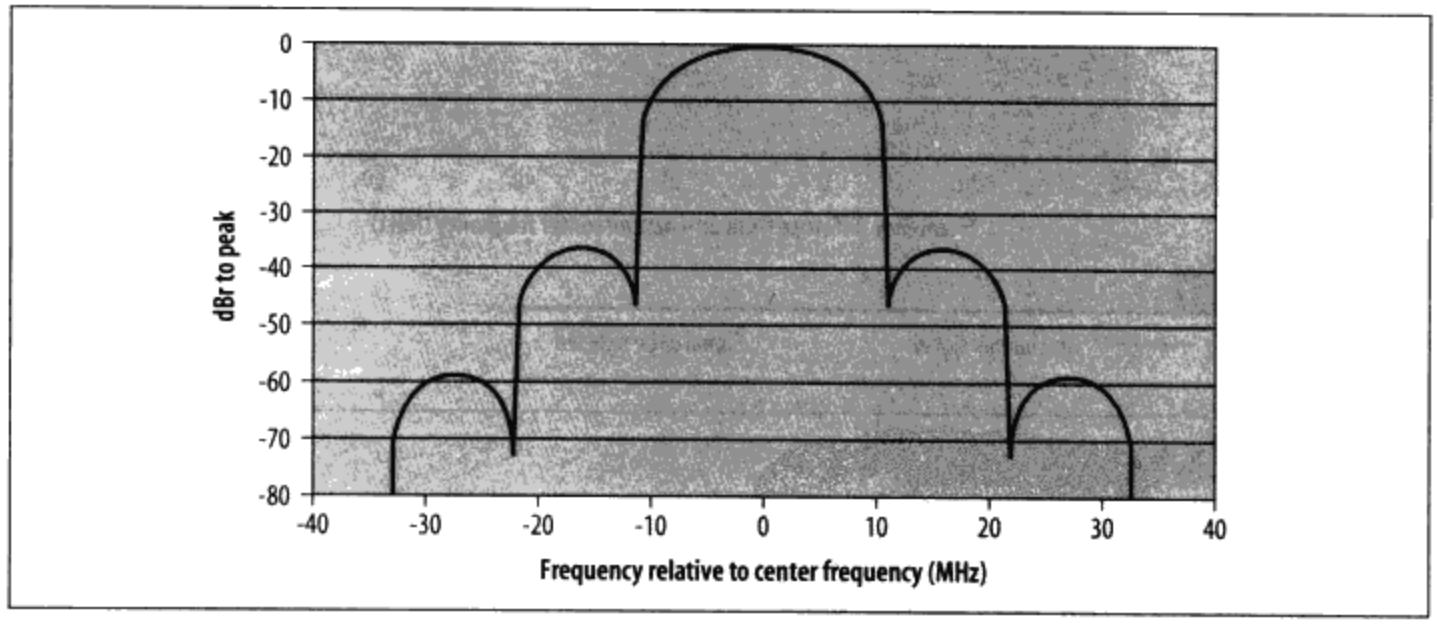


图 12-5：802.11 DS 的各个传输信道的能量分布

通过传送滤波器（transmit filter），可将大部分的 RF 能量限制在 22-MHz 频带。欧洲的管制单位限定最高的辐射功率只能为 100 毫瓦；美国的 FCC 则允许使用 1000 毫瓦的辐射功率。如果使用定向天线，甚至可以将能量集中为更高的辐射功率。

邻道抑制（adjacent channel rejection）与信道隔离（channel separation）

为了避免干扰，必须在频域中对 802.11 设备加以隔离。最初的规范说明书要求相距 30 MHz 的两个邻近信号必须有 35 dB 的抑制值（rejection），不过 802.11b 将相邻信道间距缩短为 25 MHz。要测量邻道抑制值，可以在信道的中心频率输入一个极速信号（maximum-speed signal），如图 12-6 中左边的曲线。它的功率比规定的最低灵敏度高 6 dB，对 802.11b 接收器而言为 −70 dBm。在相距 25 MHz 以上处输入第二个 11 Mbps 的 802.11b 信号，强度提高 35 dB。右边的曲线代表干扰测试信号。只要帧错误率低于 8%，接收器就可以通过测试。请注意，干扰信号的第一个旁瓣（first lobe）与主频（on-channel）信号的中心主瓣（main center lobe）之间存在明显的重叠。

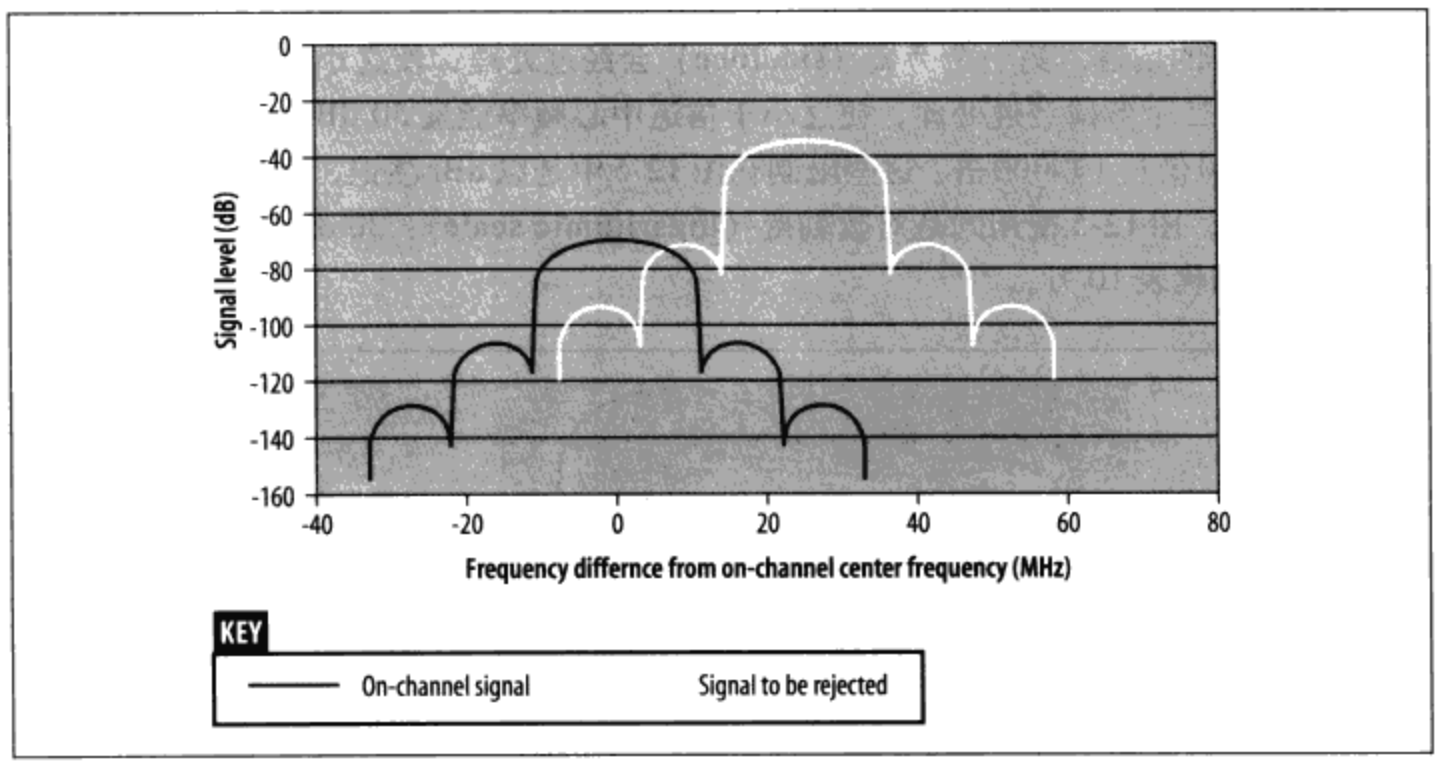


图 12-6：邻道抑制

邻道抑制也会影响同一时间内可用的信道数。虽然使用 ISM 频带的 802.11 网络定义了 14 个信道，不过信道间相当接近，真实信号必须加以隔离以避免干扰。802.11b 标准认为 25 MHz（5 个信道）的间隔就已足够。图 12-7 显示了在所谓的非重叠信道（1、6 与 11）上进行传输时的频谱屏蔽（spectral mask）。相比较于之前的图形，图 12-7 比较容易看出若使用非重叠的信道组合，所有系统组件都必须以最高效率运作。不过在真实世界里，并非所有无线电系统都能够以近似极限的方式拒绝信号很强的邻道传输。

虽然可以使用重叠较多的四道部署方式（例如 1、4、7 与 11），不过这种部署策略并不常见。信道间的重叠部分越多，相邻信道的无线电操作就越容易受到干扰。干扰太多会导致载波监听机制报告媒介处于忙碌状态或者导致传送中的帧损毁。无论如何，个别信

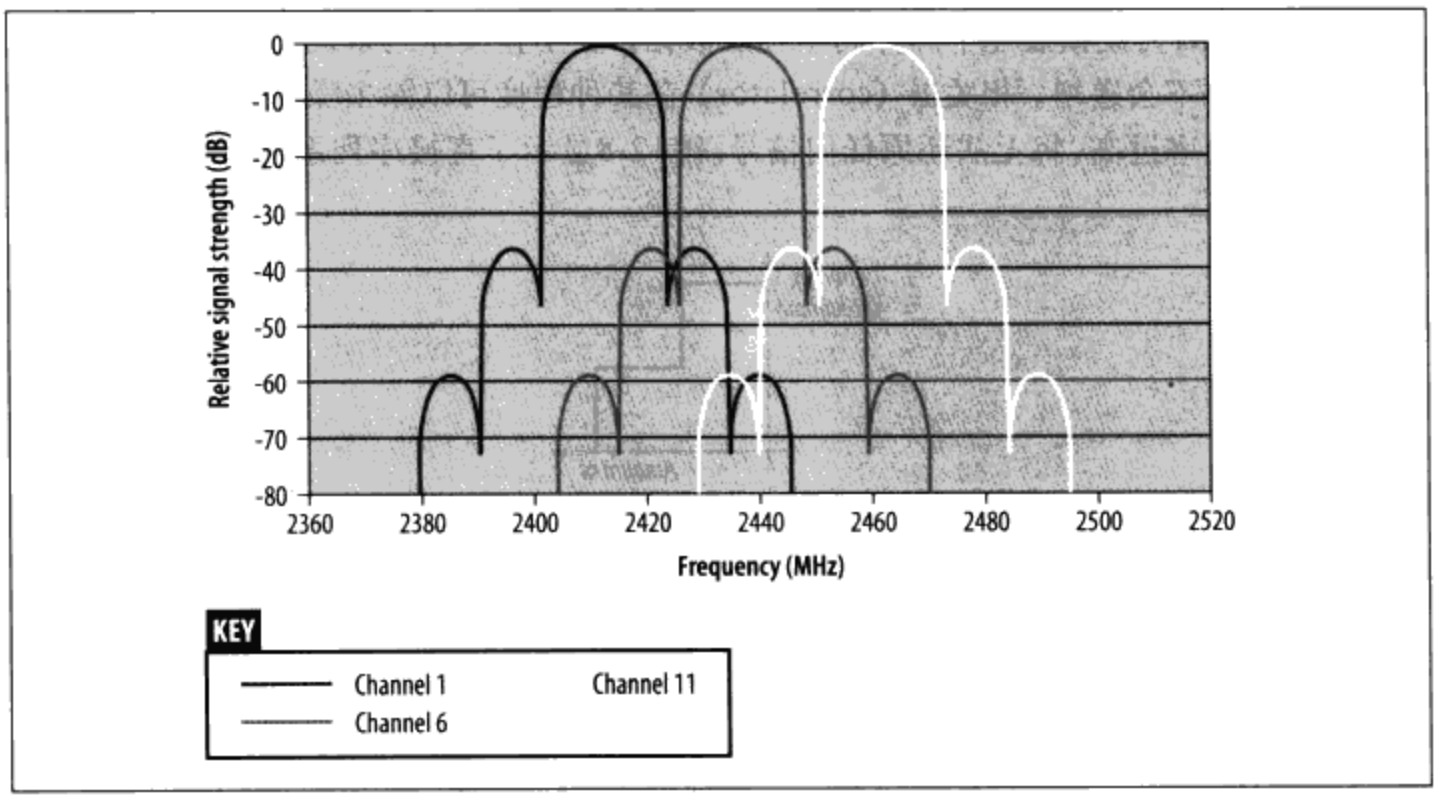


图 12-7：802.11 DS 网络中的信道隔离

道的最高吞吐量都会因此变少。以少许吞吐量换来全区带宽看似划得来，实际上并非如此。

注意： 不论称之为1、6与11，A、B与C，还是Tom、Dick与Harry，在2.4 GHz无线局域网络中，最多只能有三个非重叠信道。

最大吞吐量（理论值）

如果使用DS PHY的信号处理技术，那么最大吞吐量将是所用频率空间的函数。粗略而言，ISM频带的带宽为80-MHz。若扩频率为11，则最大位率大概比7 Mbps稍微多一些。不过，这是指使用一个信道的情况，而且产品必须使用频率为77 MHz的振荡器来产生扩频码。高频设备相当耗费电池的电力，而且使用这么高的编码率必须用掉整个频带，对可用频谱而言这简直是最糟的浪费。要达到较高的吞吐量，必须使用较复杂的技术。802.11b只是稍微增加了符号率，但它使用较复杂的编码技术，在吞吐量方面将可获得更大的进展。

干扰响应

比起跳频信号，经过直接序列调制的信号更能抵抗干扰。相关处理（correlation process）让直接序列系统可以更有效率地解决窄带干扰的问题。每个位（bit）使用11个碎片

(chip)，允许漏失或损毁几个碎片而不损及数据。至于直接序列系统的缺点，在于响应噪声的能力并不会递增。相关器（correlator）在某种程度可以除去噪声，但是如果干扰对频带的遮蔽率过高，将无法还原任何信号。图12-8显示了直接序列系统对干扰的响应。

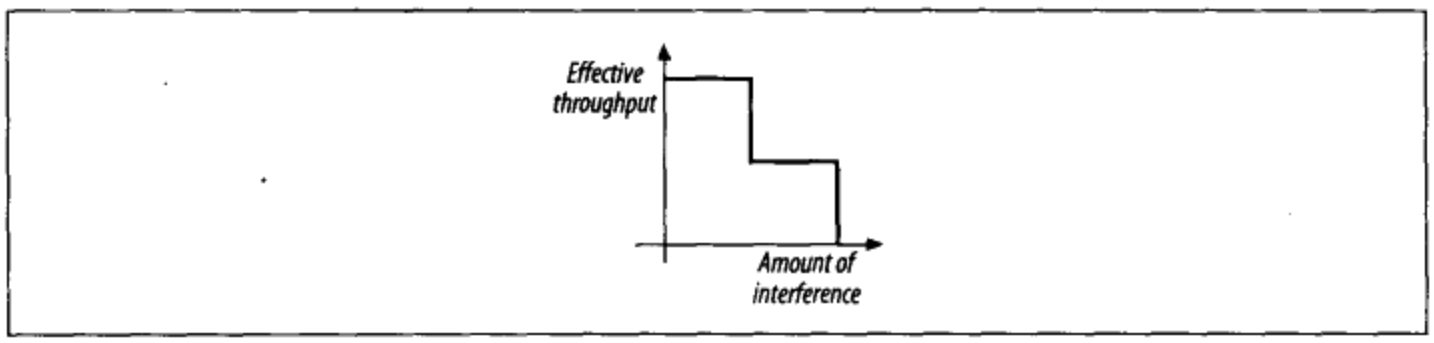


图12-8：DSSS系统中吞吐量对干扰的响应

比起跳频系统，直接序列系统更能有效避免妨碍到频带优先用户（primary user）。经过直接序列处理后，信号比较宽，振幅也比较小，对传统窄带接收器而言有如随机背景噪声。如果同地区的两位用户所选用的直接序列信道相隔太近，使用上就会产生问题。一般而言，不等频带优先用户察觉，直接序列设备相互干扰的问题已事先浮出台面。

差分相移键控（DPSK）

差分相移键控（differential phase shift keying，简称DPSK）是802.11直接序列系统的基础。正如其名，它是以传输信号的相位差对数据进行编码。在PSK中，波形的绝对相位并不重要，重要的是相位的相对变动。和频移键控（调频）一样，PSK也可以抗拒干扰，因为干扰通常只会影响振幅。图12-9显示了两个相同的正弦波彼此之间沿时间轴的相互偏移。两个波形的相同点偏移量即为相位差。

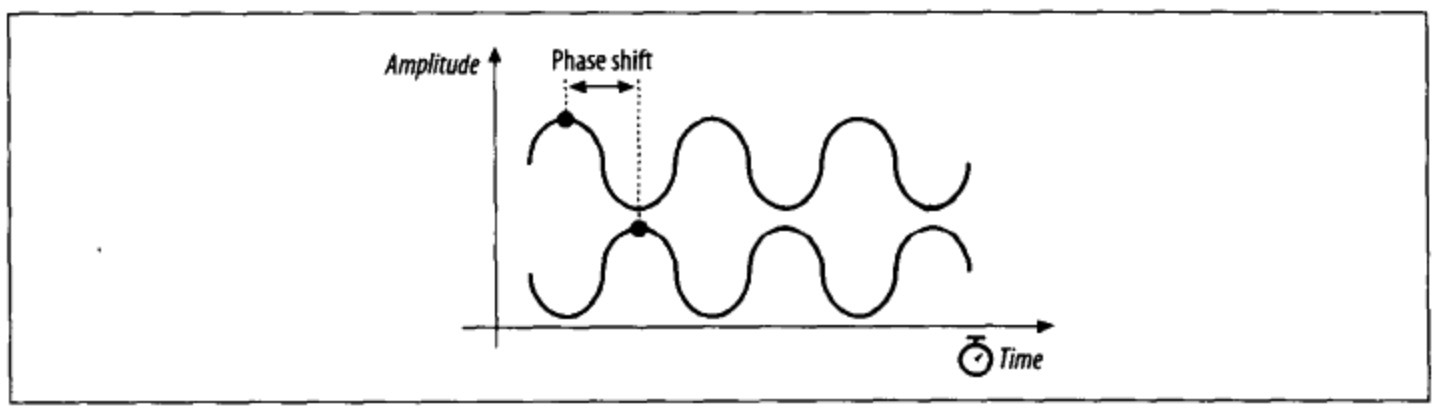


图12-9：两个正弦波之间的相位差

差分二进制相移键控（DBPSK）

形式最简单的 PSK 使用两种载波，它们彼此间偏移半个周期。其中一个波称为参考波（reference wave），所对应的编码为0；偏移半个周期的波所对应的编码为 1。表 12-2 列出了可能的相位偏移。图 12-10 说明了如何借助正弦波的相位差进行编码。

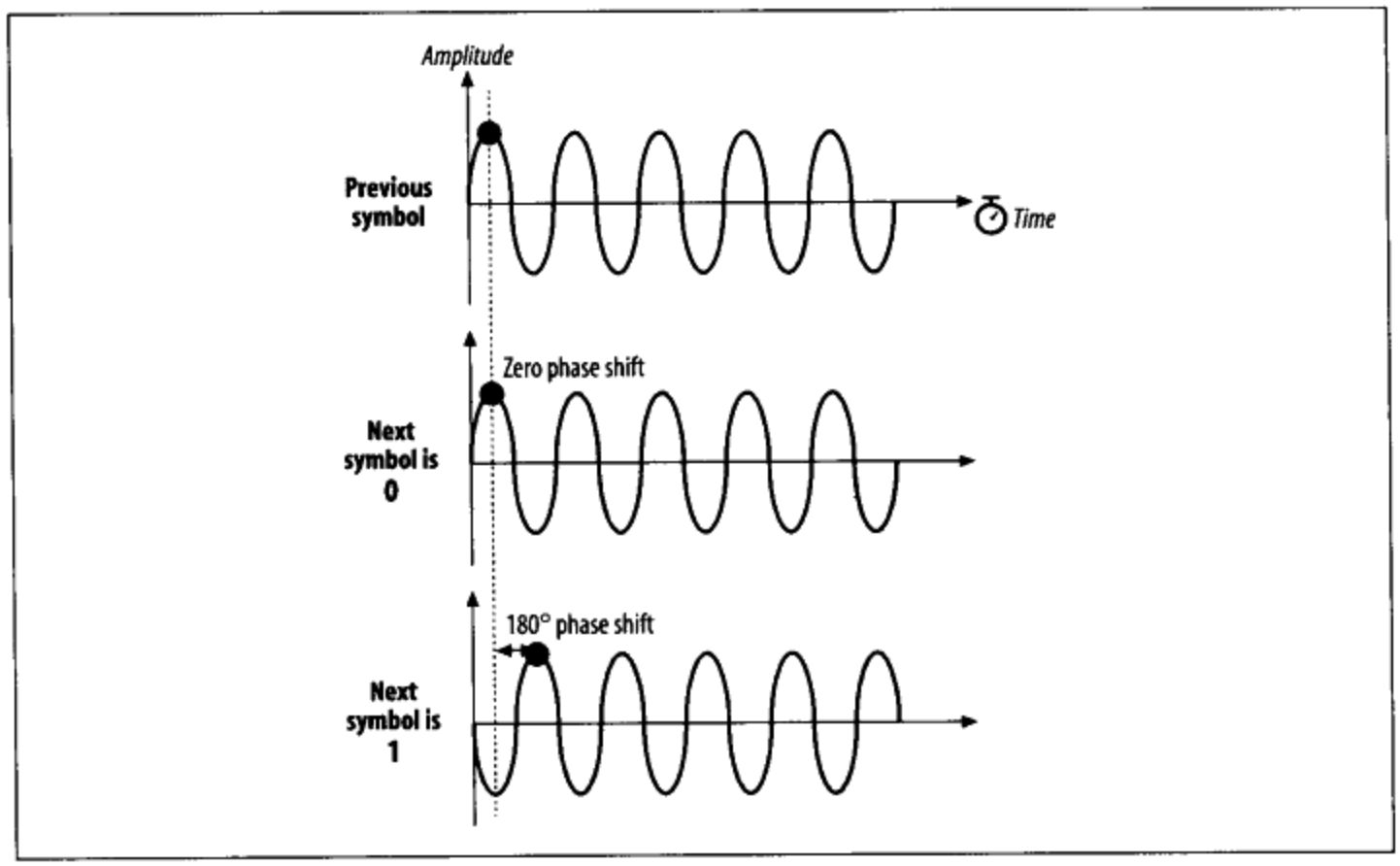


图 12-10：DBPSK 的编码方式

表12-2：DBPSK的相位偏移

符号	相移（相位差）
0	0
1	180 度（π）

举个相同的例子。对字母 M（以二进制数值表示为 1001101）进行编码，相当于将时间轴区分为 7 个符号时间，然后在每个符号范围内以适当的偏移相位传送波。图 12-11 说明了如何进行编码。首先，时间被分割为一系列符号周期，每个周期是由几个载波周期构成。当符号为0，波形如同上一个符号时；如果符号为 1，波形就会偏移半个周期。因此，传送 1 时载波会被“截断”，传送 0 时载波则会平顺地过渡到下一个符号时间。

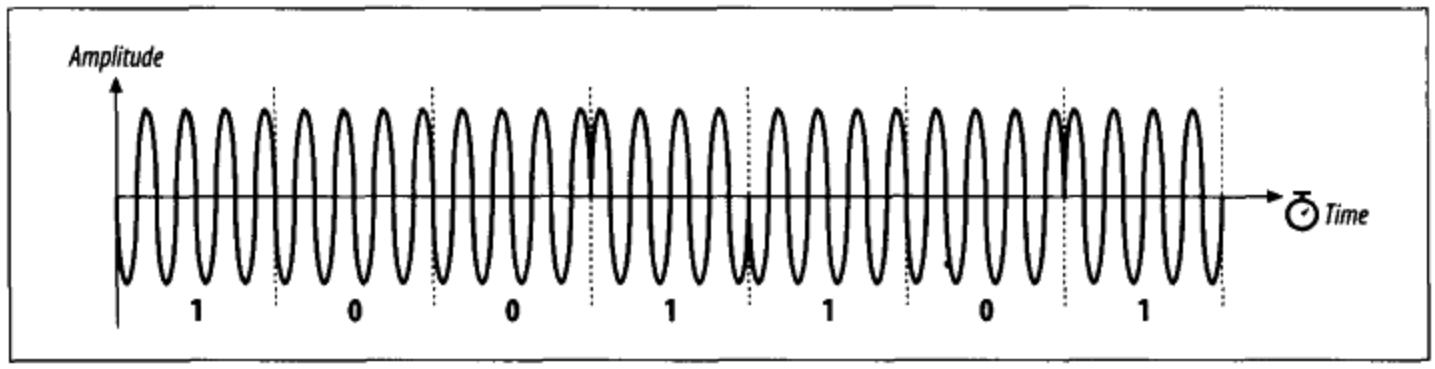


图 12-11：以 DBPSK 对字母 M 进行编码

差分正交相移键控（DQPSK）

和2GFSK一样，DBPSK 也受限于每个符号只能编码一个位。较先进的接收器与传送器可以使用一种称为“差分正交相移键控”（简称DQPSK）的技术，以每个符号编码数个位。DQPSK 并非使用基波与相位差为半个周期的偏移波，而是采用一个基波与三个偏移波，每个波偏移 1/4 周期，如图 12-12 所示。表 12-3 列出了所有可能的相位偏移。

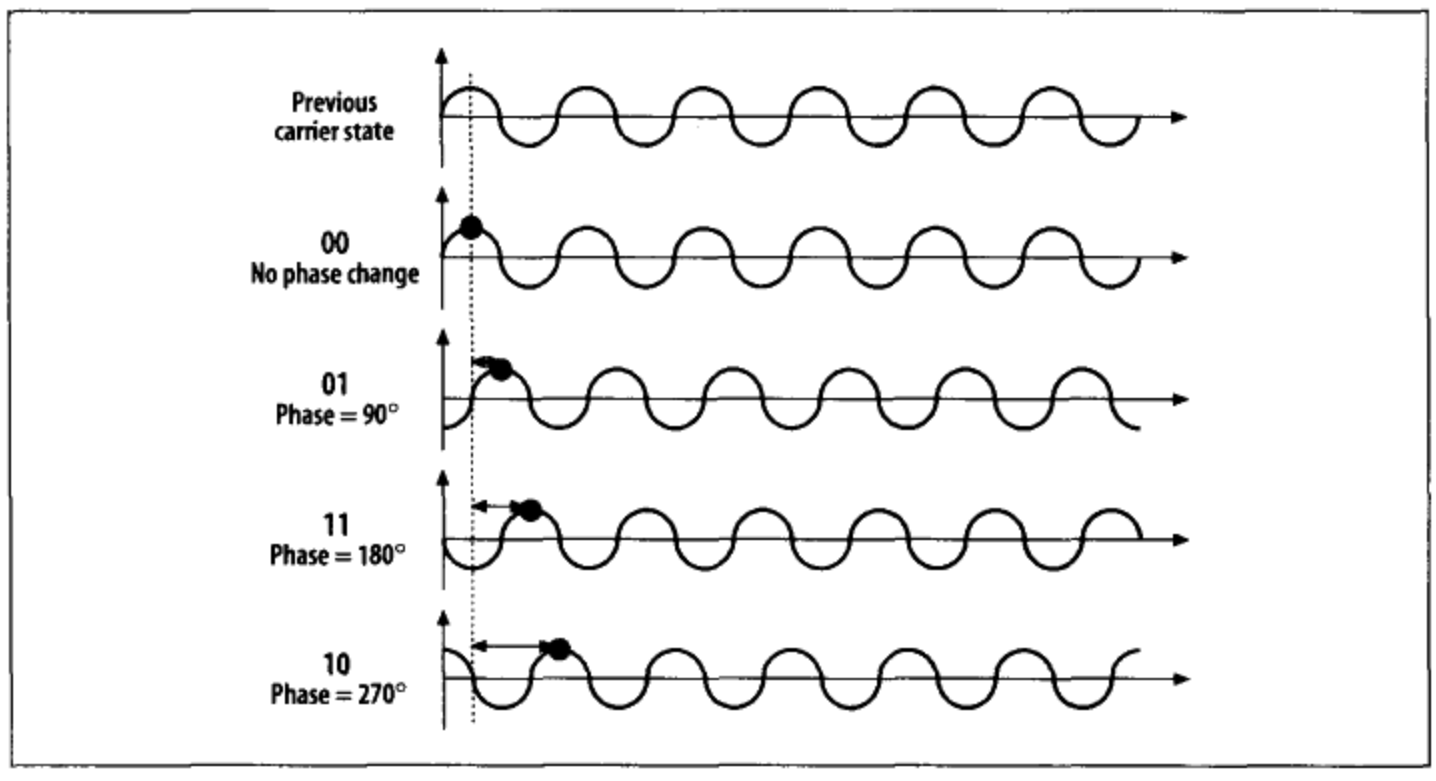


图 12-12：DQPSK 的编码方式

表 12-3：DQPSK 的相位偏移

符号	相移（相位差）
01	90 度（π/2）
00	0

表 12-3：DQPSK相位偏移（续）

讯符	相移（相位差）
11	180 度（π）
10	270 度（3π/2 或 -π/2）

现在以DQPSK对字母M进行编码（图12-13）。在UTF-8字符集中，M是以二进制字符串01001101表示；或者可以将它分割为四个等分，每个等分由两个位的符号组成，即01-00-11-01。在第一个符号周期内，相位偏移为90度。为了清楚起见，本图所显示的偏移量是以纯粹的正弦波为基准。第二个符号不会造成任何相位偏移，因此波形并无任何改变。第三个符号导致180度的相位偏移，因此在最高振幅与最低振幅之间造成剧烈落差。最后一个符号导致相位偏移90度。

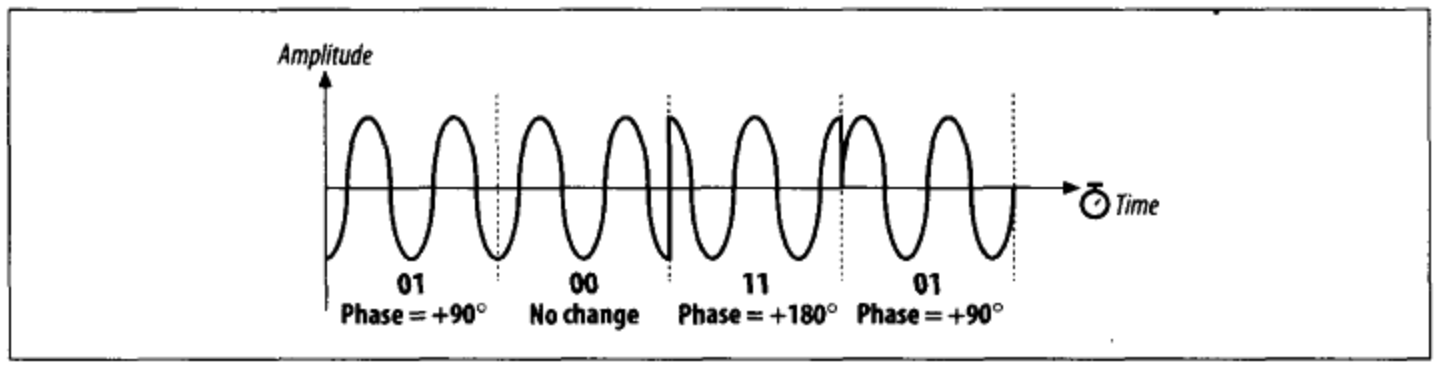


图 12-13：以 DQPSK 对字母 M 进行编码

相比较于DBPSK（两级编码机制），DQPSK所具备的明显优势为四级编码机制可以提供较高的吞吐量。采用DQPSK的代价则是，如果多径干扰十分严重，可能会导致它无法使用。多径之所以发生，是因为信号从发送端分路抵达接收端。每个路径的距离不同，因此从每个路径所接收到的信号相对于其他路径有时间差。时间差所造成的延迟是相位差编码机制的天敌。波前（wavefront）并未附上标签或者以不同颜色标示，因此某个波前可能因为路径太长而迟到，或者太晚传送而产生相位偏移。在多径干扰十分严重的环境下，DQPSK会比DBPSK更早崩溃。

“原本的”直接序列物理层

物理层本身包含了两个组件。物理层会聚过程（PLCP）会在传送之前进行与物理层相关（PHY-dependent）的成帧操作，而物理媒介相关（PMD）则负责帧的实际传送。

PLCP 的成帧（Framing）与处理

DS PHY 所使用的 PLCP 会在 MAC 传来的帧之前加上标头，其中包含了 6 个字段。以 ISO 参考模型的术语来讲，从 MAC 传来的帧属于 PLCP 服务数据单元（PLCP service data unit，简称 PSDU）。PLCP 的成帧格式如图 12-14 所示。

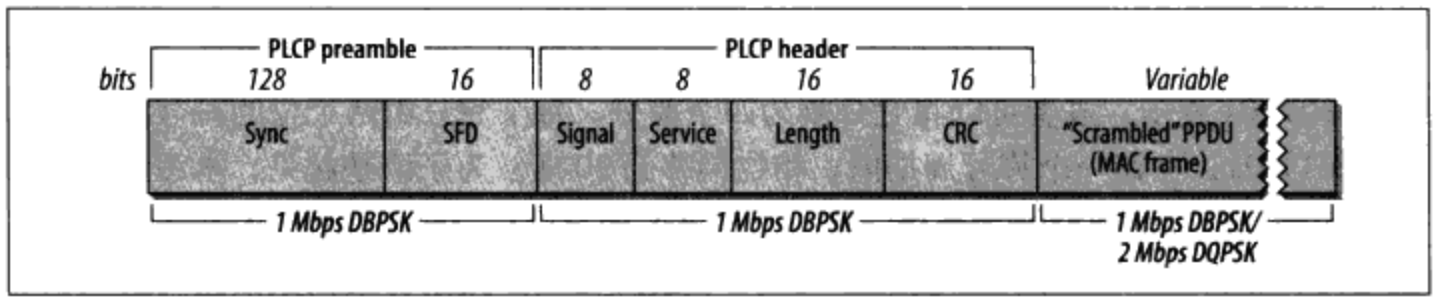


图 12-14：DS PLCP 的成帧格式

FH PHY 使用数据白化器（data whitener）在数据传送之前进行随机化处理，不过白化对象只限于 PLCP 标头之后的 MAC 帧。DS PHY（直接序列物理层）也有类似的功能，称为扰频器（scrambler），只是其扰频范围遍及整个直接序列帧，包括 PLCP 标头与前导码。

Preamble（前导码）

前导码用来同步发射器与接收器，以维系两者之间的定时关系。前导码是由 Sync 以及 SFD 两个字段组成。传送之前，前导码会经过直接序列扰频程序进行扰频。

Sync（同步）

Sync 字段的长度有 128 个位，每个位的值均为 1。和 FH PHY 不同的是，Sync 字段传送之前会经过扰频。

Start Frame Delimiter（起始帧定界符，简称 SFD）

SFD 可让接收器得知帧从何处开始，即便同步位在传送过程中有所遗漏。此字段被设定为 0000 0101 1100 1111，和 FH PHY 所使用的 SFD 有所不同。

Header（标头）

前导码之后紧跟着的是PLCP标头。此标头包含了PLCP所使用的物理层专属参数，由5个字段组成：一个用编码代表速度的信号字段（Signal），一个服务标识符字段（Service），一个长度字段（Length）以及一个帧校验序列。

Signal（信号）

接收器可用Signal字段来识别所封装的MAC帧使用何种传输率。其值若不是设为 0000 1010（0x0A）来代表 1-Mbps 操作，就是设为 0001 0100（0x14）来代表 2-Mbps 操作。

Service（服务）

此字段保留供给未来使用，每个位均设定为0。

Length（长度）

此字段设定为传送一个帧所需要的微秒数，以16位的无符号整数来表示。由最低位开始传送至最高位。

CRC（循环冗余校验）

为了防止标头经过无线链路时受损，发送端会根据前面4个标头字段的内容计算出一个16位的校验码。接收端在对帧做进一步处理之前会先验证校验码。

Data字段所放置的内容并无任何限制。任何数据均包含了一长串连续的0或1，这使得数据看起来不是那么随机。为了让所要传送的数据比较像是随机的背景噪声，DSPHY会以一种多项编码机制将成串的1或0从所传送的数据流中移除。

DS PMD 子层

PMD（物理媒介相关）是相当复杂且冗长的规范，其中包含两种数据率（1.0 Mbps 与 2.0 Mbps）的相关规定。图12-15显示了用于802.11直接序列网络的收发器的一般设计。

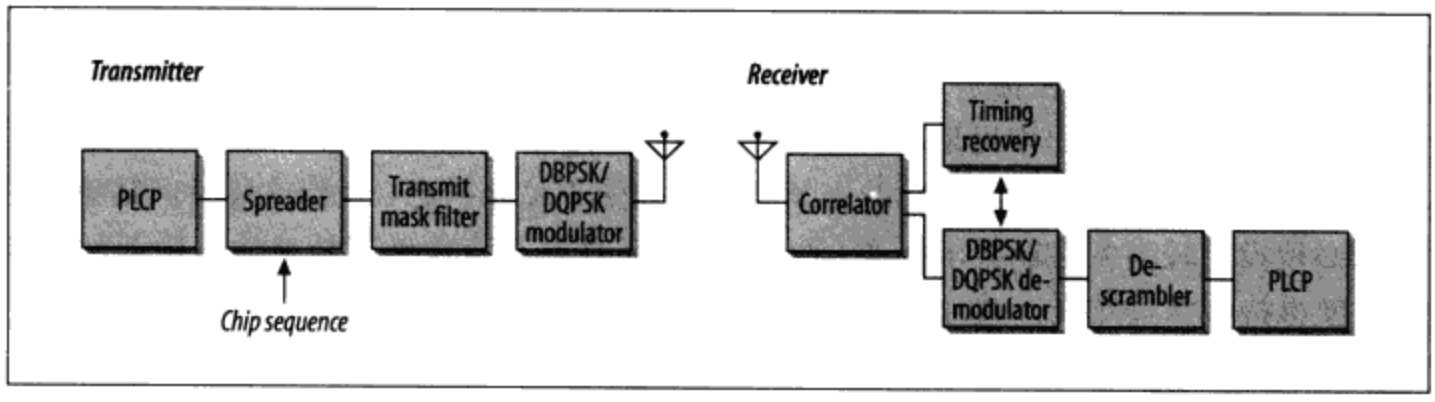


图 12-15：直接序列收发器

以 1.0 Mbps 进行传输

就低数据率而言，DS PMD 可用1.0 Mbps的速率传送数据。来自MAC的帧加上PLCP标头后，即会对整个单元进行扰频。所产生的位序列使用DBPSK以每秒100万个符号的速度进行编码，然后通过物理接口传送。和FH PMD一样，DS PMD有最低功率的限制。如果要符合管制要求，可将功率设定为100 mW。

以 2.0 Mbps 进行传输

和FH PHY一样，以2.0 Mbps进行传输使用了两种编码机制。PLCP前导码和标头使

用DBPSK以1.0 Mbps的速率进行传送。虽然使用较低速率传送标头会降低有效吞吐量，不过 DBPSK 更能容忍噪声与多径干扰。前导码与标头传送完毕后，PMD 就会切换为 DQPSK 调制，开始提供 2.0-Mbps 的服务。和 FH PHY 一样，大多数实现 2.0-Mbps 传输率的产品可以在检测到干扰时切换回低速的 1.0-Mbps 服务。

DS PHY 的 CS/CCA

802.11 允许 CS/CCA（载波监听 / 空闲信道评估）功能以下列其中一种模式运作：

Mode 1

当能量超过能量检测（energy detection，简称 ED）阈值时，它会汇报媒介处于忙碌状态。ED 阈值因传输功率而异。

Mode 2

采用 Mode 2 的实现产品必须搜寻真正的 DSSS 信号。如果检测到，就算信号低于 ED 阈值，也会汇报该信道处于忙碌状态。

Mode 3

Mode 3 结合了 Mode 1 与 Mode 2。所检测到的信号必须具备足够能量，才会向上一层汇报信道处于忙碌状态。

一旦信道被视为忙碌，在预定传输的时间内就会一直处于忙碌状态，即使信号已经遗失。传输持续时间由Length字段取得。汇报媒介是否忙碌必须非常迅速。一旦在竞争窗口时隙的开始检测到信号，CCA 机制就必须报告媒介处于忙碌状态，直到这段时间结束。之所以必须设定较高的性能要求标准，是因为一旦工作站在竞争延迟结束后开始进行传送时，就得持续掌握媒介，其他工作站必须暂缓访问媒介，直到帧传送完毕。

DS PHY 的特性

表 12-4 显示了 DS PHY 中的几个参数值。除了表中所列的标准参数，DH PHY 还有一些参数可供调整，让 802.11 直接序列系统中各部分的延迟得以保持均衡。其中包括 MAC、PLCP、收发器的延迟变量以及收发器电子零件个别变异的相关变量。另外值得注意的是，同一区域中所有直接序列网络的整体吞吐量（total aggregate throughput）比该区所有非重叠的跳频系统低。整体吞吐量是互不重叠信道数的函数。在北美与欧洲的大部分地区，每个区域同时间只能够容纳三个直接序列网络。如果每个网络的传输速率为 2 Mbps，且协议的性能可让用户的数据吞吐量达到额定速率的 50%，该区的总吞吐量即为 3 Mbps，远低于跳频系统的整体吞吐量。

表12-4：DS PHY参数

参数	值	备注
时隙时间（Slot time）	20 us	
SIFS 时间	10 us	SIFS 可用来推衍出其他的帧间间隔值（DIFS、PIFS 以及 EIFS）
竞争窗口的大小（contention window size）	3 至 1023 个时隙	
前导码持续时间（preamble duration）	144 us	前导码符号是以1 MHz的速率传输，因此传输每个符号需时 1 us，144 个位则需要 144 个符号时间
PLCP 标头持续时间（PLCP header duration）	48 us	PLCP标头有48个位，因此需要用到48个符号时间。
最大 MAC 帧（maximum MAC frame）	4 至 8192 个字节	
最低接收灵敏度（minimum receiver sensitivity）	−80 dBm	
邻道抑制（adjacent channel rejection）	35 dB	参见测量注意事项

和FH PHY 一样，DS PHY 中有些属性也可供厂商调整，让系统各部分的延迟时间能够保持均衡。其中包括MAC、PLCP、收发器的迟延变量以及收发器电子零件中个别变异的相关参数。

补码键控（CCK）

802.11 直接序列系统采用了每秒1100万的碎片率（11 million chips per second）。原本的DS PHY将碎片流划分为一系列11位的Barker word，每秒传送100万个Barker word。每个 word 中会根据所使用的是 1.0 Mbps 还是 2.0 Mbps 的数据率，分别编码 1 或 2 个位。要达到更高的数据率以及在商业上具有实用性，就必须在每个符号中承载更多信息，而不只是 1 或 2 个位。

直接进行相移编码无法在每个码字（code word）中携带多个位。DQPSK 所使用的接收器必须能够分辨 1/4 周期的相位差。要增加每个符号所能承载的位数，必须能够处理更细微的相位偏移，例如 1/8 或 1/16 周期的偏移。遇到多径干扰时，检测更细微的相位偏移更加困难，而且还必须使用更复杂（因此也更昂贵）的电子零件。

IEEE 802.11 工作组并未继续采用直接相移键控，转而使用不同的编码方式。补码键控（Complementary code keying，简称 CCK）将碎片流（chip stream）划分为一系列由 8 个位构成的码符号（code symbol），因此底层所使用的传输率是每秒传送 137.5 万个码符号。CCK 采用了复杂的数学转换函数，可以使用若干个 8-bit 序列在每个码字中编码 4 或 8 个位，因此数据总吞吐量为 5.5 Mbps 或 11 Mbps。此外，CCK 所使用的数学转换函数可以让接收器轻易识别不同的编码，即便遇上干扰或多径衰落的情况。图 12-16 显示了 CCK 所使用的码符号。它十分类似低速直接序列物理层所使用的 chipping process（破碎过程），差别在于码字部分是由数据本身推衍而来，并未使用类似 Barker word 之类的静态且具重复性的码字。

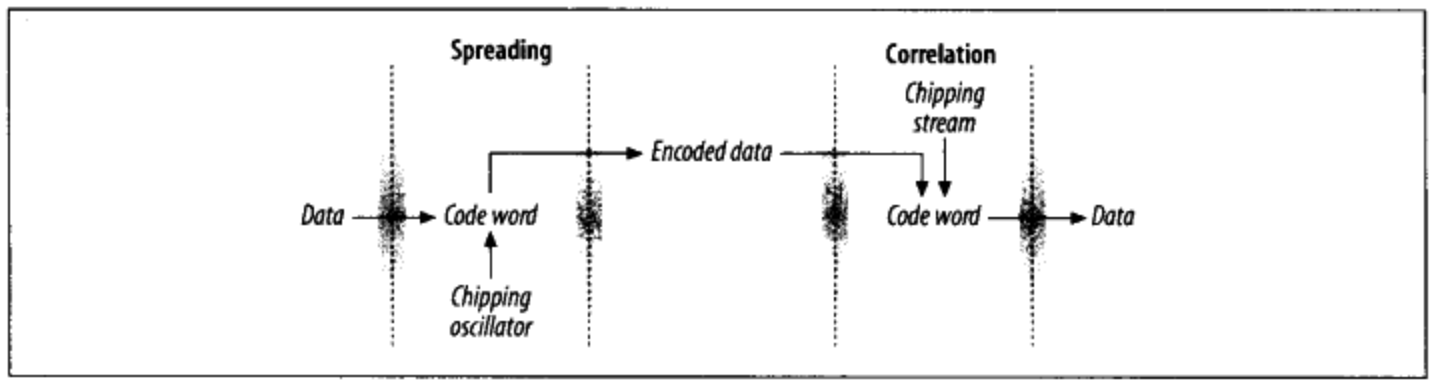


图 12-16：CCK 所使用的编码符号

用于低速直接序列物理层的 Barker 扩频方式，是使用静态编码将信号于可用频带展开。CCK 使用码字（code word）来承载信息以及展开信号。准备这些复杂的 8 个位为一组的码字时必须使用一些不同的相位角（phase angle）。

高速直接序列物理层（HR/DSSS PHY）

为了与原本的直接序列物理层有所区别，以 11 Mbps 运行的高速物理层被简称为 HR/DSSS。和前者一样，HR/DSSS 分成两个部分：PLCP 负责准备传送所需要的帧，PMD 则负责将之转换为无线电波。

PLCP 成帧（Framing）与扰频（Scrambling）

原本的直接序列物理层所使用的长标头会大幅降低性能。802.11 MAC 要求每个数据帧都要得到确认，而 192 微秒的前导码远远长于 MAC 的确认。以 11 Mbps 的数据率而言，传送一个大小为 1500 字节的帧并得到 MAC 确认，前导码与 PLCP 成帧标头就占用了其中 25% 的时间。开发新的物理层时，802.11b 的设计人员采用一种新的“短”帧格式，因此在改善协议性能的同时也提升了吞吐量。使用短标头可将前导码与 PLCP 成帧所造

成的负担删减至 14%。虽然负担仍在，但已有大幅改善。图 12-17 显示了 802.11b 所规范的 PLCP 成帧格式。802.11b 刚问世时并非所有设备都支持短标头，因为当时 2 Mbps 直接序列设备的安装量相当大。目前，几乎所有网卡都已支持短前导码，大多数接入点也以它为默认值。

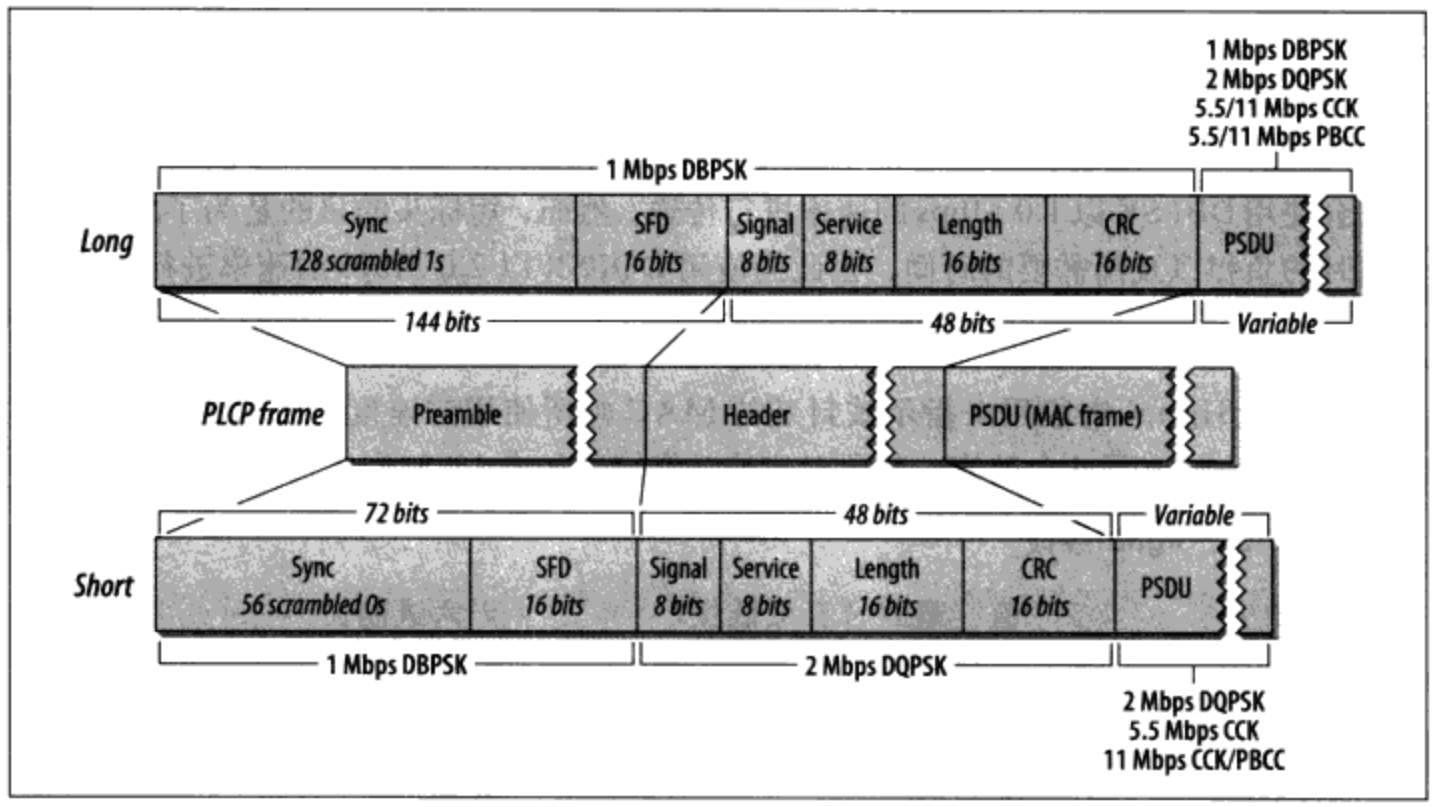


图 12-17：HR/DSSS PLCP 的成帧格式

当然，除非所有工作站都提供支持，否则短帧就无法使用。为了避免支持短帧的网络消失，802.11b 规定，回复 Probe Request（探查请求）主动扫描的工作站必须使用相同的 PLCP 标头加以响应。如果某个只支持长 PLCP 标头的工作站送出 Probe Request，接入点就必须以长标头加以响应，就算该 BSS 设定时使用的是短标头。

Preamble（前导码）

帧始于前导码，它由Sync与SFD字段组成。此前导码会使用DBPSK并以1.0 Mbps的速率进行传送。

Long Sync

Long Sync 字段由 128 个内容为 1 的位所组成。不过在传送之前，此字段会先经过扰频器处理，因此数据内容会有所不同。高速系统使用特定值作为扰频函数的随机数种子（seed），不过也可以向下兼容，支持不指定随机数种子的旧式系统。

Short Sync

Short Sync 字段由 56 个内容为 0 的位所组成。和 Long Sync 一样，这个字段会先经过扰频器处理。

Long SFD

long preamble以SFD来宣告Sync字段的结束。在Long PLCP中，SFD序列为1111 0011 1010 0000。和所有IEEE规范一样，实际的传送顺序是最低的有效位（least-significant bit）优先，因此该字符串是由右至左传送。

Short SFD

为了避免与Long SFD混淆，Short SFD的值正好相反，即0000 0101 1100 1111。

前导码之后为PLCP标头，它是由Signal、Service、Length以及CRC字段所构成。长标头会使用DBPSK以1.0 Mbps的速率进行传送。然而，短标头的目的是为了减少标头传送时的负担以及所需要的时间，因此会使用DQPSK以2.0 Mbps的速率进行传送。

Long Signal

Long Signal字段用来指示被封装的MAC帧所使用的速度与传输方式。目前，802.11b定义了4个数值，其所对应的8位编码如表12-5所示。

表12-5：Signal字段

速度	值（最高位至最低位）	十六进制值
1 Mbps	0000 1010	0x0A
2 Mbps	0001 0100	0x14
5.5 Mbps	0011 0111	0x37
11 Mbps	0110 1110	0x6E

Short Signal

Short Signal字段用来指示被封装的帧所使用的速度与传输方式，不过标准中只定义了3个值。short preamble只能用于2 Mbps、5.5Mbps以及11 Mbps网络。

Service

802.11标准的初版原本是将图12-18所示的Service字段留待未来使用，不过802.11b随即将它应用于高速扩展服务上。首先，Length字段以微秒为单位记录封装帧所需要的时间。传输速度高于8 Mbps时，这个值就有些不明确。因此，Service字段所使用的8个位被用来将Length字段扩展为17个位。其中第3位（clock lock）用来显示该802.11b产品是否使用经锁定的时钟（locked clock）。时钟锁定（clock locking）是指传输频率与符号时钟使用同一振荡器。第4位（Modulation）用来显示封包所使用的编码类型，0代表CCK，1代表PBCC。其他保留位必须设定为0。Service字段的传送是由左至（b0到b7），不论PLCP帧格式的长短都是如此（802.11g做了进一步的改变，相关细节将于第十四章探讨）。

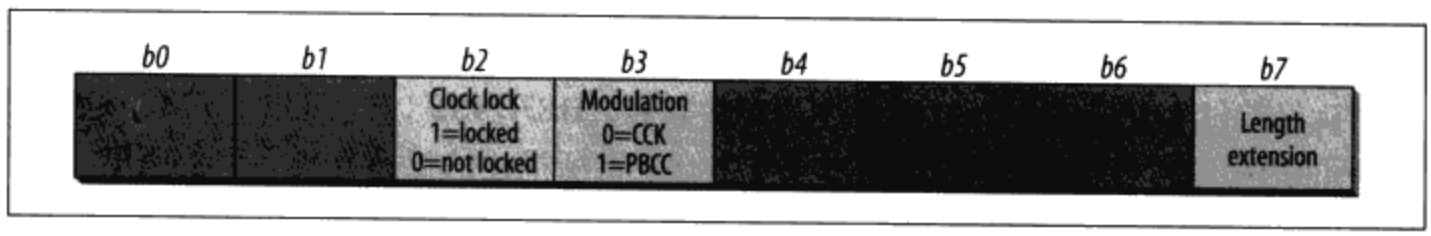


图 12-18：HR/DSSS PLCP 标头中的 Service 字段

Length

Length 字段在 PLCP 短帧与长帧格式中完全一样，代表传送经过封装的 MAC 帧所需要的微秒数。802.11b 标准以将近两页的篇幅描述如何计算 Length 值，不过这些细节已经超出本书的范围。

CRC

CRC 字段在 PLCP 短帧与长帧格式中完全一样。发送端会以 Signal、Service 以及 Length 字段计算 CRC 码。接收端可以利用 CRC 值来确保所收到的标头未经改动，也未在传输过程中损毁。CRC 的计算会在数据扰频前进行。

HR/DSSS PHY 所使用的数据扰频程序几乎与原来的 DS PHY 一样，唯一的差别在于其所使用的扰频函数采用了特定的随机数种子（seed）。PLCP 短帧与长帧分别使用了不同的随机数种子。

HR/DSSS PMD

与 FH PHY 不同，DS PHY 只有一种 PMD 规范。一般收发器的设计如图 12-19 所示。

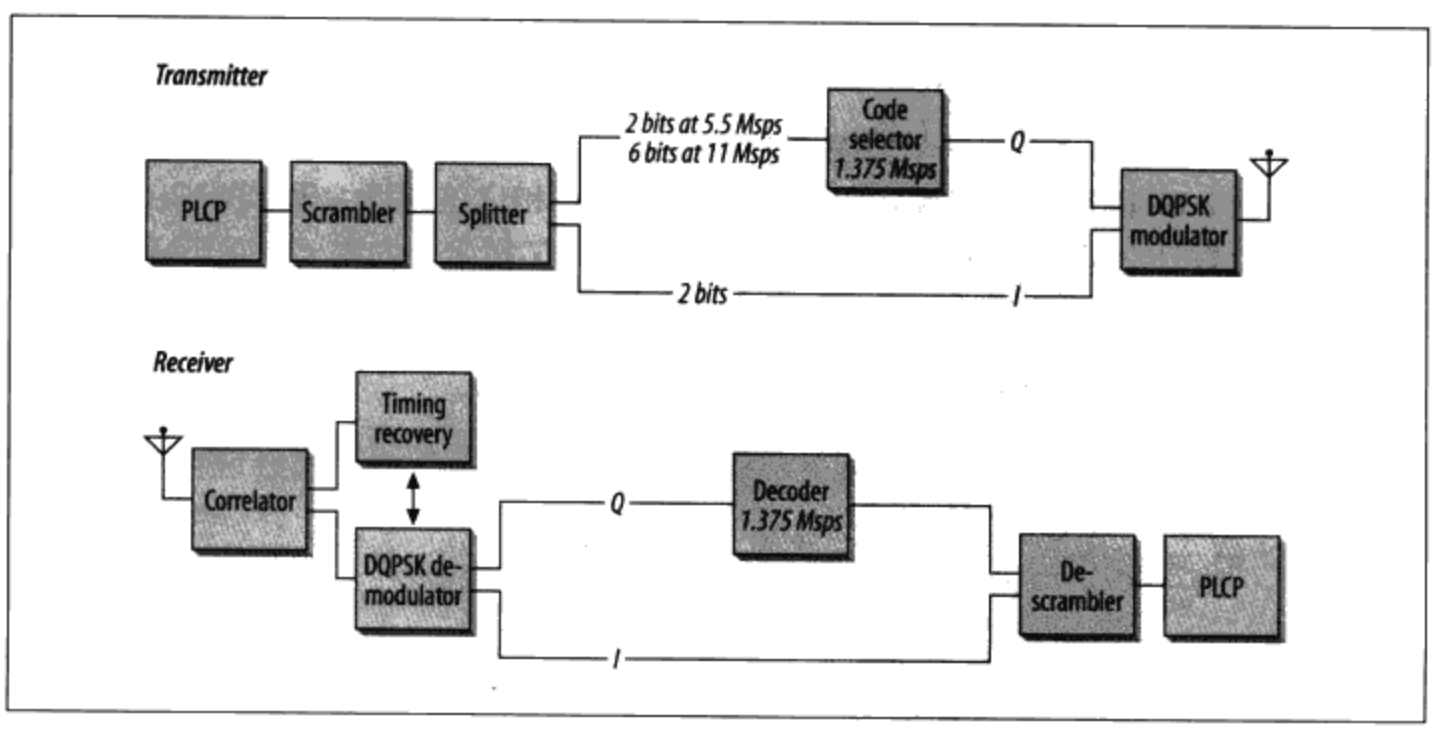


图 12-19：HR/DSSS 收发器

以 1.0 Mbps 或 2.0 Mbps 进行传输

为了确保能够和现有的802.11直接序列硬件兼容，HR/DSSS PHY可用1.0 Mbps或2.0 Mbps的速率进行传输。较慢的传输方式与本章之前所描述的低速直接序列物理层一样。任何低速传输都需要使用长标头。

以 CCK 进行 5.5 Mbps 的传输

高速传输是以基于DQPSK的相移键控（相位差调制）技术实现的。DQPSK在每个符号周期可以传送2个位，这2个位可编码成相应的四种不同相位偏移之一。如果使用CCK，符号字（symbol word）本身可以承载更多信息。5.5-Mbps传输在每个符号中可编码4个数据位。其中2个位使用传统的DQPSK被承载，另外2个位则是通过码字（code word）的内容被承载。图 12-20 显示了整个过程。

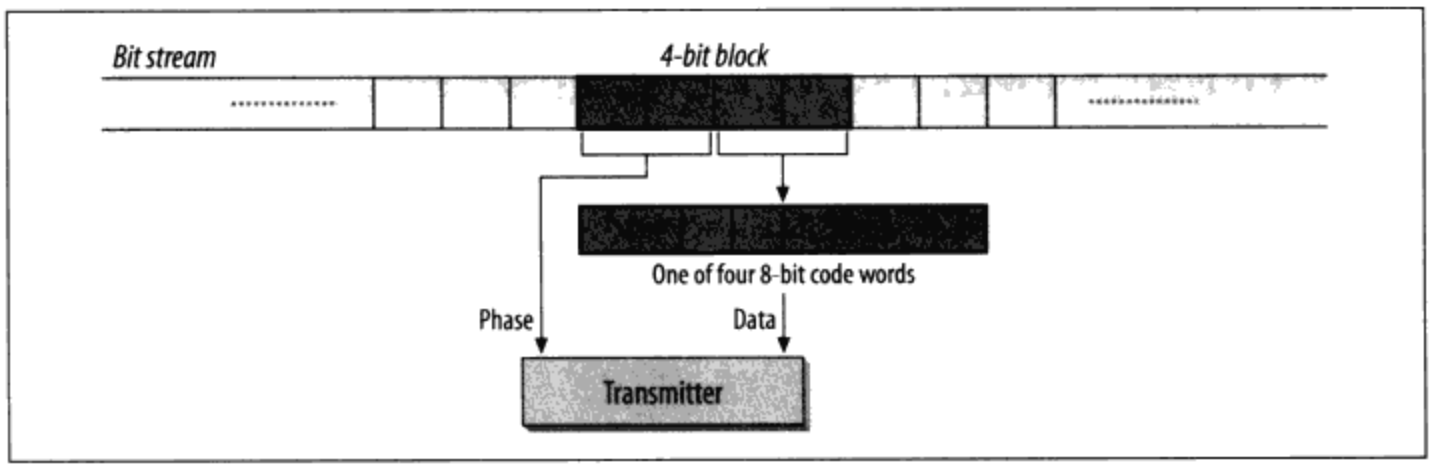


图 12-20：以 5.5 Mbps 进行 802.11b 传输

1. PLCP帧所包含的MAC帧被分割成一连串的4-bit块（block）。每个4-bit块再进一步被划分为2个2-bit段（segment）。
2. 第一个2-bit段是以前后两个符号之间的DQPSK相位差进行编码（表12-6）。偶数与奇数符号之所以采用不同的相位差，纯粹是为了技术上的需要。符号编号从0开始并由第一个4-bit块算起。

表12-6：符号间的DQPSK相位偏移

位模式	相位角（偶数符号）	相位角（奇数符号）
00	0	π
01	π/2	3π/2
11	π	0
10	3π/2	π/2

3. 第二个 2-bit 段可用来将当前符号对应到 4 种代码字（表 12-7）的其中之一。这 4 种代码字可通过 802.11 标准在 18.4.6.5 款中所记载的数学函数推演得知。

表12-7：Mbps码字

位序列	码字
00	i,1,i, −1,i,1, −I,1
01	−i, −1, −i,1,1,1, −i,1
10	−i,1, −i, −1, −i,1,I,1
11	i, −1,i,1, −i,1,I,1

以 CCK 进行 11 Mbps 的传输

为了支持 11 Mbps 的传输，在每个符号中必须编码 8 个位。和其他技术一样，前两个位是以当前所发送的符号与前一个符号之间的相位差来进行编码，其他 6 个位则是使用 CCK。图 12-21 显示了整个过程。

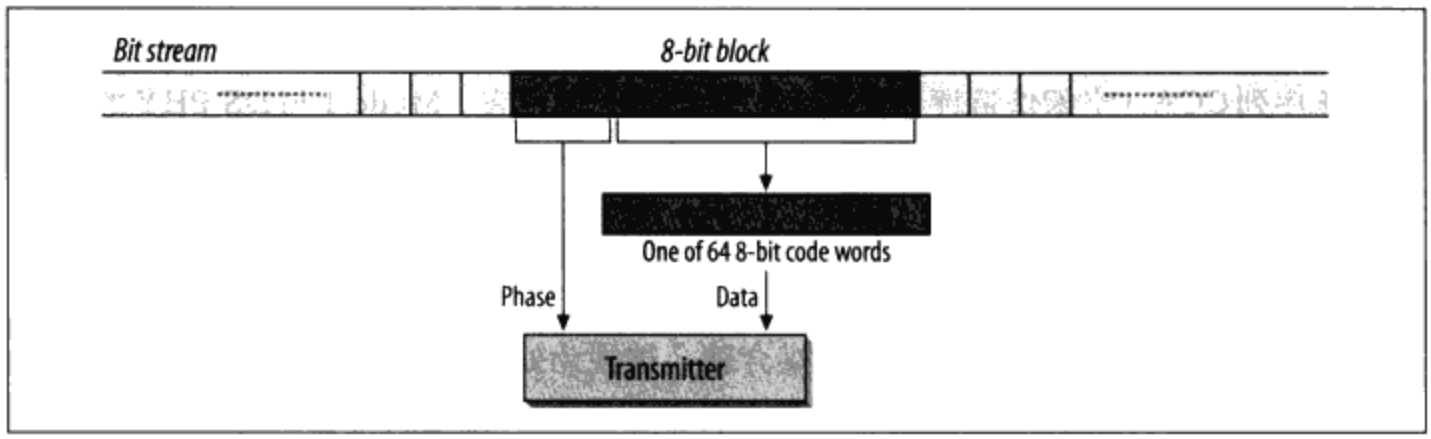


图 12-21：以 11 Mbps 进行 802.11b 传输

1. PLCP帧所包含的MAC帧被分割成一连串的8-bit块（block）。每个8-bit块再进一步被划分为4个2-bit段（segment）。
2. 第一个2-bit段是以前后两个符号之间的DQPSK相位差进行编码。和5.5-Mbps一样，偶数与奇数符号之所以采用不同的相位差，纯粹是为了技术上的需要。符号编号从0开始，由第一个8-bit块算起。此相位偏移与5.5-Mbps传输所使用的完全相同。
3. 其余6个位被分为3组。每一组均对应到表12-8所列的相位角并据此推衍出码字。

表12-8：11-Mbps传输所使用的相位角编码

位模式	相位角
00	0
01	π/2
10	π
11	3π/2

举例说明如何将位序列0100 1101转换为复合码（complex code）以便在802.11b网络进行传输。前两个位为01，以当前符号与上一个符号之间的相位差进行编码。在MAC帧中，如果该符号为偶数符号，相位偏移为π/2；否则，偏移量为3π/2（MAC帧中的符号编号由0开始，所以帧的第一个符号为偶数）。其余6个位被分为3组，每组包含2个位：00、11与01。这3组分别用来对应相位角与码字。下一个步骤是将相位角转换为用来传输的复合码。

空闲信道评估

和原本的DS PHY一样，高速的实现版本在CS/CCA操作模式上也有三种选择。所有这些直接序列CCA（空闲信道评估）模式均来自同一份列表。Mode 1与DS PHY的CCA Mode 1相同，Mode 2与Mode 3只用于原本的DS PHY，Mode 4与Mode 5则是HR/DSSS专属的CCA模式。

Mode 1

一旦超越能量检测（ED）阈值，媒介就会被视为处于忙碌状态。ED阈值因所使用的传输功率而异。典型的直接序列系统也会用到此模式。

Mode 4

实现时Mode 4是用来找寻真实信号。一旦被触发，实现Mode 4 CCA的产品会启动一个3.65 ms的定时器，然后开始倒计时。如果在定时器结束时并未发现有效的HR/DSSS信号，媒介就被视为处于闲置状态。3.65 ms相当于以5.5 Mbps传送最大可能帧（largest possible frame）所需要的时间。

Mode 5

Mode 5结合了Mode 1与Mode 4。所检测到的信号必须有足够的能量，才会向上层协议汇报信道处于忙碌状态。

一旦信道被视为忙碌，在预定传输的时间内便会一直处于忙碌状态，就算信号已经遗失。该信道会被视为忙碌，直到Length字段所记载的时间过去。如果检测到了第二个PLCP标头，找寻有效信号的实现产品有可能会不管此项要求。

802.11b PHY 的非必要功能

802.11b 包含了两种非必要的物理层功能，两者均未受到广泛使用。有人提议使用分组二进制卷积码（Packet Binary Convolutional Coding，简称 PBCC）来达到 11 Mbps 的数据率，不过并未得到广泛使用。有些提案提议在未来版本中采用 PBCC，不过这些提案在 2001 年已被否决。

第二种称为机动跳频（channel agility），它被设计来协助网络避免干扰。机动跳频会定期变更中心信道，以此来避免干扰。机动跳频从未得到广泛使用，因为它并不是特别有用。接收器在干扰出现时跳至其他信道可以提升一些吞吐量，但是这还不如找出干扰源予以移除或者重新分配信道有效率。

HR/DSSS PHY 的特性

表 2-9 列出了若干 HR/DSSS PHY 的参数值。和 DS PHY 一样，HR/DSSS PHY 还有一些参数可供调整，以补偿实际系统各部分所产生的延迟。

表12-9：HR/DSSS PHY参数

参数	值	备注
最大 MAC 帧长度	4095 个字节	
时隙时间	20 μs	
SIFS 时间	10 μs	SIFS 可用来推衍出其他帧间间隔值（DIFS、PIFS 以及 EIFS）
竞争窗口的大小	31 至 1023 个时隙	
前导码持续时间	144 μs	前导码符号是以 1 MHz 的速率进行传输，因此传输每个符号需时 1 μs，144 个位需要 144 个符号时间
PLCP 标头持续时间	48 μs	PLCP 标头的传输时间取决于是否使用短前导码
最低敏感度	−76 dBm	
邻道抑制	35 dB	参见测量注意事项

另外值得注意的是，HR/DSSS网络在某个区域所能提供的整体吞吐量仍然低于非重叠的跳频网络。整体吞吐量是互不重叠的信道数的函数。在北美与欧洲大部分地区，每个区域同一时间可以容纳三个HR/DSSS 网络。如果每个网络的最高传输速率为11 Mbps，假设有效载荷数据的吞吐量为 50%，则该区的总吞吐量即为 16.5 Mbps（译注 1）。

译注 1： 11x3x0.5。

第十三章

802.11a 与 802.11j: 5-GHz OFDM PHY

到西部去吧，年轻人，和这个国家一起成长！

—— John B.L. Soule（注 1）

2.4 GHz ISM 频带十分拥挤，而且经常充斥着非 802.11 信号。为了达到更高的数据率，802.11工作小组制定出另一种物理层标准，使用5 GHz附近的无许可证频谱。除了还有很多未开发的频谱空间，目前也很少有设备使用这个频谱。

802.11a 早在 1999 年就已经成为标准，但是经过很长一段时间后相关产品才开始出现。802.11a硬件最早出现在 2001 年底。目前，Atheros Communications 算是最著名的802.11a芯片组厂商。不论是在形式还是功能方面，802.11a和其他类型的无线网卡均十分类似。大多数网卡采用CardBus接口，不过目前比较常用的反而是其他形状因素(form factor）的网卡。通常数据率越高传输距离就越短，但一般来说，802.11a不论是在数据率还是传输距离方面，都还能够与 802.11b 相提并论。

起初，802.11a 是专门针对美国所做的设计，使用 5-GHz 的免授权国家信息基础设施(Unlicensed National Information Infrastructure，简称 U-NII）频带。802.11a 成功打开美国市场后，其他管理者便着手制定相关法规，允许使用 802.11a。在 802.11 工作组的协助下，最后针对欧洲制定了 802.11h（参见第八章），针对日本制定了 802.11j。

本章首先会介绍OFDM的基础知识。OFDM的做法是将较大的信道分割成数个子信道。这些子信道随后会以平行的方式加以利用，以便达到更高的吞吐量。我预料许多读者会

注 1:　拜 Horace Greeley 所赐，这句话才广为流传。

跳过本章前面的部分，若不是因为这些读者对OFDM已经相当熟悉，就是因为他们只对如何使用频带，以及 PLCP 如何封装所要传送的帧感兴趣。

正交频分复用（OFDM）

802.11a是基于正交频分复用(orthogonal frequency division multiplexing，简称OFDM)的。OFDM的技术并不算新，它的基本架构完成于20世纪60年代末期，而美国则在1970年 1 月批准专利，专利号码为3488445。近年来，DSL（HDSL、VDSL与ADSL）与无线数据应用对OFDM重新燃起兴趣，主要是出现了更好的信号处理技术，使之更为实际可行（注 2）。然而，在做法上，OFDM的确不同于其他近年来出现的编码技术，如码分多址（code division multiple access，简称CDMA）。CDMA通过复杂的数学转换，以单一载波(single carrier)进行多路传送，OFDM则是以多路副载波(multiple subcarrier)进行单一传送。CDMA 的码分所使用的数学运算远比OFDM 复杂得多。

OFDM设备会将一个较宽的信道(frequency channel)分割成几个子信道(subchannel)。每个子信道均用来传输数据。所有这些“较慢”的子信道随后会被复用的方式组合成“较快”的信道。

载波复用

当网管人员请用户对网络设备提供建议时，最常得到的反应就是希望网络的速度能够更快一些。数据传输的需求与日俱增，这带动了一些致力于提升传输速度的技术的发展。在质量上，OFDM 采取类似 Multilink PPP 的做法：当一条链路不够使用时就增加几条平行的链路来处理。

OFDM和传统频分复用（FDM）技术的关系十分密切。两者均是将可用带宽分割为许多称为载波（carrier）或副载波（subcarrier）的片段，同时将这些载波作为个别信道进行数据传输。借由这些副载波的平行运用以及对这些副载波的数据进行复用处理，OFDM可以有效提升吞吐量。

传统的 FDM 被广泛运用于第一代移动电话中，作为无线信道的分配方式。每个用户会被分配到一个专用信道，信道间使用防护频带（guard band）以确保某个信道所溢出的信号不会干扰到相邻信道的用户。图 13-1 显示了传统 FDM 所采取的做法。

注 2：由于对OFDM感兴趣的人并不多，因此参考资料也相当稀少。对其数学背景有兴趣的读者可以参考Richard van Nee与Ramjee Prasad所合著的《OFDM for Wireless Multimedia Applications》（Artech House，2000）一书。

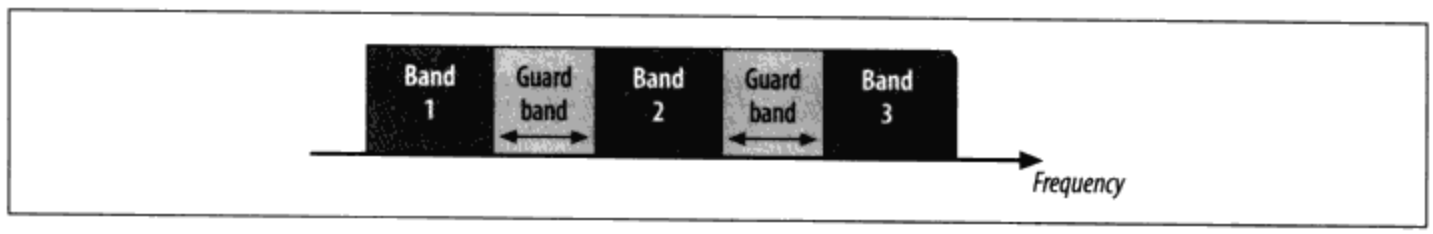


图 13-1：传统 FDM

传统 FDM 的问题在于防护频带不仅浪费带宽，也会减少可用资源（capacity）。为了避免无用的防护频带浪费传输资源，OFDM 使用彼此重叠但不会互相干扰的信道。图 13-2 显示了传统 FDM 与 OFDM 之间的差异。

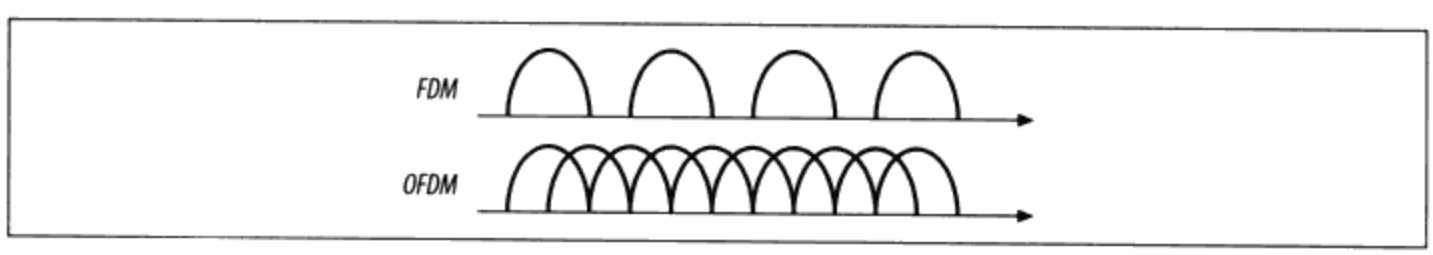


图 13-2：FDM 与 OFDM 的差异

之所以能够使用相互重叠的载波，是因为定义了副载波，因此可以轻易区分彼此。能够区别副载波，关键在于它使用了一种复杂的数学关系，称为正交性（*orthogonality*）。

正交性的意义（不使用微积分）

“正交”（*orthogonal*）这个数学名词源自 *orthos* 这个希腊文，意思是“直接、正确或者真实”。在数学上，“orthogonal”这个单词则是用来描述相互独立的项目。只要对信号进行光谱分解（spectral breakdown），就很容易从频域（frequency domain）中了解正交性的含义。OFDM 之所以能够运作，是因为所选用的副载波频率的波形丝毫不受其他副载波影响。图 13-3 显示了一种正交性的常见观点。图 13-3 中，信号被分为三个副载波。每个副载波的波峰均作为数据编码之用，如图 13-3 上方标示的圆点。这些副载波之间经过刻意设计，彼此之间保持正交关系。注意每个副载波的波峰，此时其他两个副载波的振幅均为 0。

OFDM 会从每个子信道取得编码信号，然后使用快速傅立叶逆变换（inverse fast Fourier transform，简称 IFFT）由每个子信道的振幅产生一个组合波形（composite waveform）。OFDM 接收器随后可以使用快速傅立叶变换（FFT）从所收到的波形中取出每个副载波的振幅。

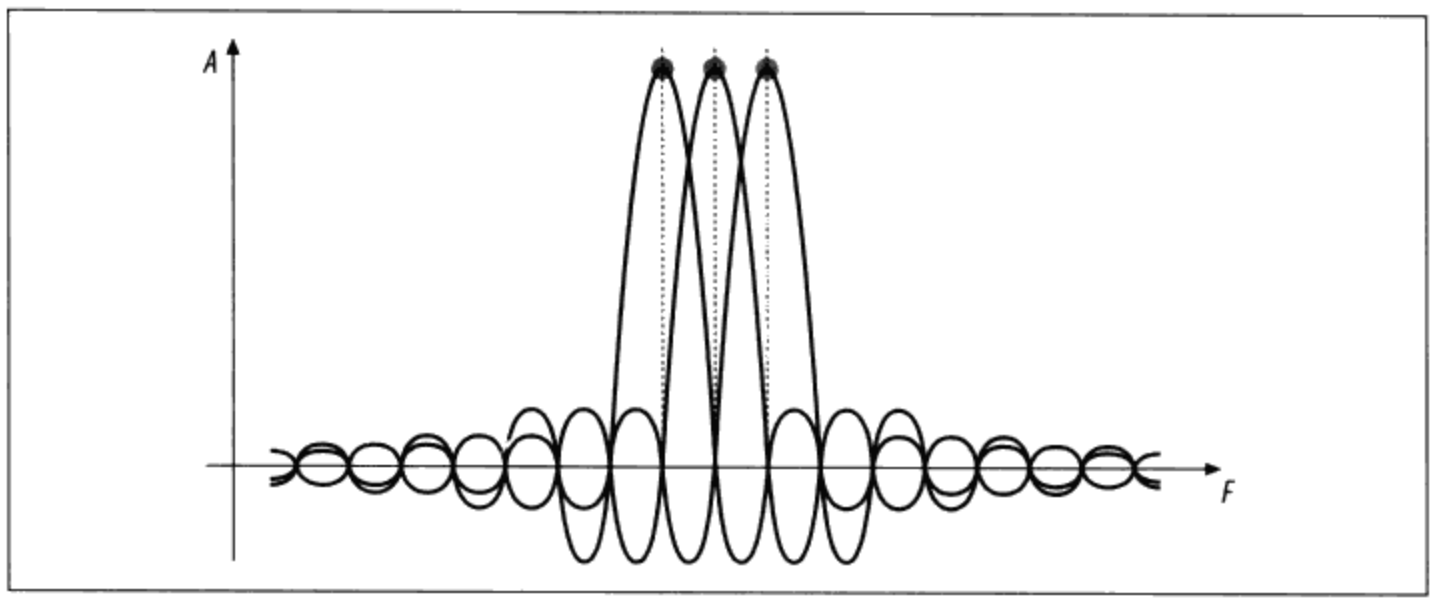


图 13-3：频域中的正交性

防护时间

第十二章讨论物理层时提到，符号间干扰（inter-symbol interference，简称 ISI）是接收器面临的主要问题（图 13-4）。当不同路径之间的延迟差距过大而导致后来所发送的数据副本混叠先前所收到的数据时，就会发生符号间干扰。

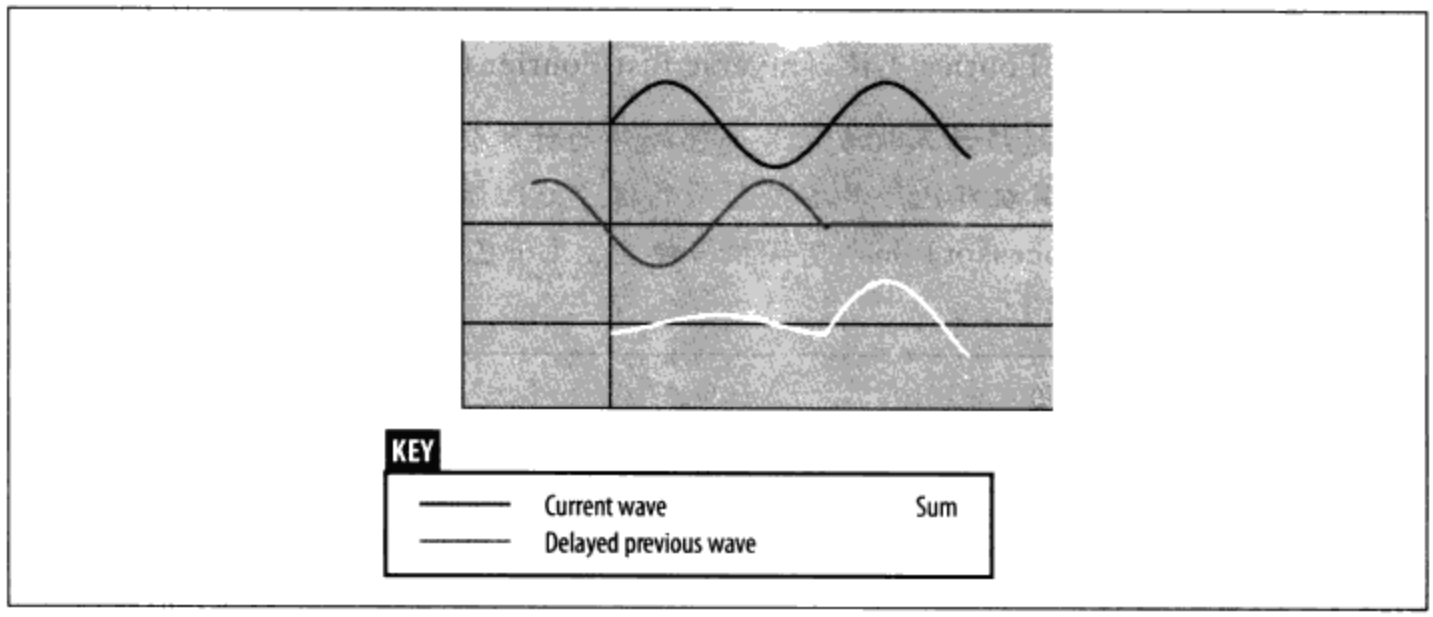


图 13-4：重新查看 ISI

如果采用 OFDM，符号间干扰就不会造成问题。OFDM 所使用的 Fourier 转换会将所收到的波形萃取为副载波的振幅，因此时间偏移就不会造成太大的问题。图 13-4 中，基本的低频载波将有较大的振幅，而迟到的高频部分则可以忽略不计。

Fourier 分析、Fourier 变换以及信号处理

Fourier（傅立叶）变换通常被称为“信号处理的瑞士军刀”。信号处理通常是以构成频率的组件定义行为。不过，接收器主要在处理依时间变动的信号振幅。Fourier 变换是一种数学运算，它会将波形拆解成许多组件。Fourier 分析所处理的则是依时间变化的信号，将之转换为一组构成该信号的频域元素。

信号处理应用程序通常也需要用到反向运算。已知一组频率组件，这些应用程序就可以利用这些频率组件重建出组合波形。从频域中的已知频率组件重建组合波形的数学运算，即为逆 Fourier 变换。

严格来讲，Fourier 分析被应用于类以物理学教科书中所描述的平滑曲线。运用于一组离散数据点时必须使用 Fourier 变换的亲戚，称为离散 Fourier 变换（discrete Fourier transform，简称 DFT）。和 Fourier 变换一样，DFT 的逆运算称为 IDFT（逆 DFT）。

DFT 是一种运算密集的过程，其 order（复杂度）为 N^2，即 DFT 的执行时间与数据点数目的平方成正比。不过，如果数据点的数目是 2 的偶数乘方（even power），就可以利用一些速算法将复杂度降到 order $N \log_{10}N$。如果要处理的数据量相当大，所降低的复杂度可以大大提升算法的速度。因此，数量为 2n 的数据点所采用的 DFT 速算法，就称为快速 Fourier 变换（fast Fourier transform，简称 FFT）。FFT 的逆运算，则称为快速逆 Fourier 变换（inverse fast Fourier transform，简称 IFFT）。

FFT 过去一直应用于超级计算机或信号处理硬件的特殊领域。不过以目前的微处理器速度而言，个人计算机就已经具备了复杂的信号处理能力。特殊的数字信号处理器（digital signal processor）如今变得相当便宜，几乎已经应用在所有东西中，包括 802.11 网卡的芯片组。

虽然有种种好处，但也非全无代价。OFDM 系统使用了多个频率各异的副载波。这些副载波被紧密包裹到一个操作信道中，只要副载波频率有稍许偏移，就会在载波之间造成干扰。这种现象称为载波间干扰（inter-carrier interference，简称 ICI）。频率偏移之所以发生，可能是因为多普勒效应（Doppler effect）或发射器与接收器的频率稍有偏移。

为了同时解决 ISI 与 ICI 的问题，OFDM 收发器会在符号时间（symbol time）开头的部分保留一段防护时间（guard time），而且只在非防护时间进行 Fourier 变换。以符号而言，防护时间以外的部分通常称为 FFT 积分时间（integration time），因为 Fourier 变换只针对该部分进行处理。

短于防护时间的延迟并不会造成ICI，因为频率组件并不会渗透到后续的符号时间中。慎选防护时间是 OFDM 系统设计人员的主要任务。防护时间显然会降低系统的整体吞吐量，因为它减少了可用于传输数据的时间。过短的防护时间不仅无法防止干扰，同时还会降低吞吐量；防护时间如果太长，则会白白浪费许多吞吐量。

循环扩展（循环前缀）

实现防护时间最直接的方式莫过于届时不要传送任何东西，如图 13-5 所示。

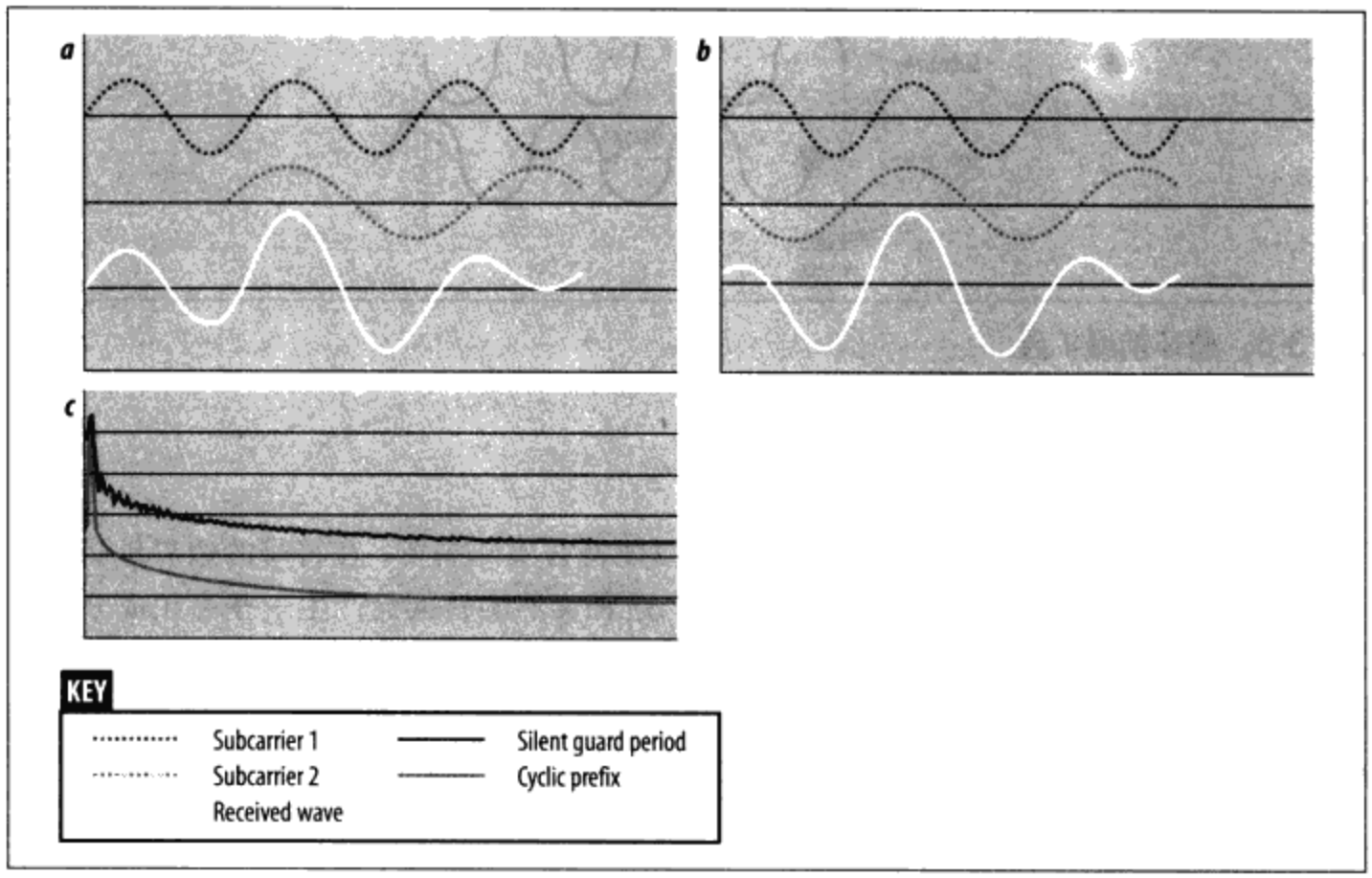


图 13-5：天真的防护时间实现（千万别这么做！）

如此实现防护时间，一旦遇到常见的延迟，就可能将正交性粉碎。OFDM 要求各载波之间的波长数目必须为整数。当防护时间几乎完全静止时，延迟现象就可以轻易摧毁此必要前提，如图 13-5所示。当图中两个副载波叠加在一起时，光谱分析（spectral analysis）显示副载波 1（2 个周期 / 符号）的振幅较强，而副载波 2（3 个周期 / 符号）相对较弱。此外，光谱分析也显示出相当数量的高频成分，使信号更加混乱。这些高频部分是突然“启动”信号所造成的结果。

要解决静止的防护时间所造成的问题十分简单，只要将副载波的FFT积分时间向前延伸至防护时间即可。延长副载波（换言之即是延长整个 OFDM 符号）会使 Fourier 变换只显示出该副载波频率的振幅。这种技术通称为“循环扩展”（cyclic extension），也可以

称为“循环前缀扩展”（cyclic prefix extension）。经过前置延伸的防护时间称为“循环前缀”（cyclic prefix）。

图13-6的循环前缀保留了光谱分析的结果。副载波1并无偏移，因此不会造成问题。副载波2有所迟滞，不过前一个符号只出现于防护时间，因此Fourier变换不会加以处理。由于循环前缀扩展的作用，当副载波2经过Fourier变换的处理时，它在每段积分时间（integration time）就是三个周期的纯波（pure wave）。

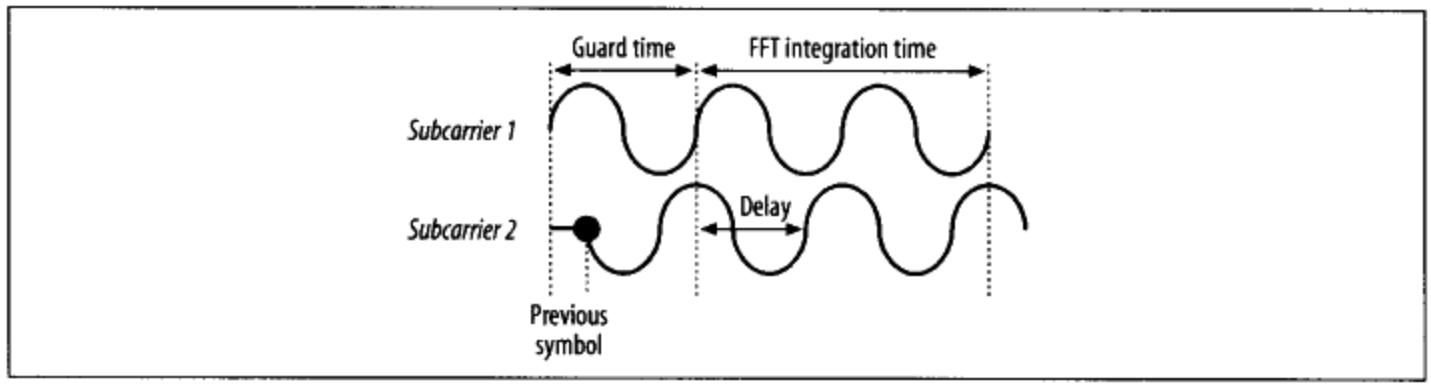


图13-6：循环前缀扩展

加窗法（Windowing）

另外，OFDM收发器可以采用一种加强技术以便符合实际需要。在符号的边界地带，信号的过渡（transition）不尽然都是相当平顺。这种突然的转换会产生一些高频成分（噪声）。为了使OFDM收发器表现良好，通常会在信号前后加上填充位（padding bit），如此一来，收发器在达到完全功率或从完全功率下降的过程中，就能够以“斜升”（ramp up）或“斜降”（ramp down）的方式缓缓升降。使用错误修正码时，填充位通常是必要的。有些文件称填充位为“训练序列”（traning sequence）。

加窗法（Windowing）主要是让新的信号能够缓缓拉升至完全强度以及让旧信号能够逐渐消逝的一种技术。图13-7显示了一种常见的余弦波加窗函数。在符号周期的开始阶段，新的函数根据余弦函数逐渐拉高至完全强度；当符号周期结束，该余弦曲线则是让符号的结束不致过于突然。

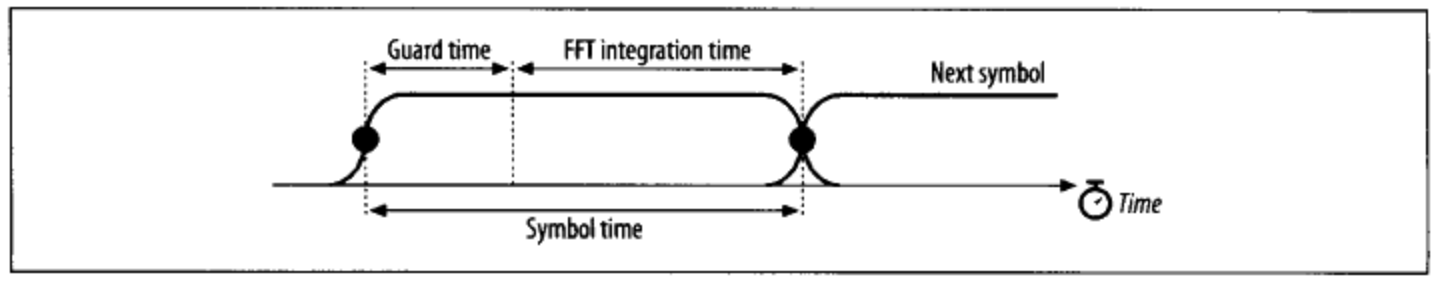


图13-7：余弦加窗（cosine windowing技术）

802.11a 所采用的 OFDM

802.11a 并未彻底运用 OFDM 技术。负责 OFDM 标准化操作的任务组将 OFDM 运用至无线局域网络时采取了中庸之道。

802.11a 所选用的 OFDM 参数

选择 OFDM 参数时通常有三项既定的事实。带宽（Bandwidth）是固定的，这通常由管理者来限制。延迟时间（Delay）取决于 OFDM 系统的操作环境。通常办公大楼的延迟扩展（delay spread）为 40~70 ns，不过在某些环境里，延迟扩展可能高达 200 ns。最后，提高位率（bit rate）通常是设计上所要达到的目标，虽然这通常意味着“在其他参数限制不变的情况下尽量提高位率”。

比较常见的做法是防护时间应该为平均迟延时间的 2 至 4 倍。因此，802.11a 设计人员选用 800 ns 作为防护时间。符号的持续时间应该比防护时间长，不过有值得斟酌之处。较长的符号时间代表该段时间内可以容纳更多的副载波。更多副载波会增加发送端与接收端的信号处理负担，设备的成本与复杂度也会因此提高。比较实际的做法是选择至少比防护时间多 5 倍的符号时间。802.11a 以 800-ns 的防护时间搭配 4-μs 的符号时间。subcarrier spacing（副载波间距）与 FFT 积分时间成反比。802.11a 的积分时间为 3.2-μs，而 subcarrier spacing 为 0.3125 MHz（1/3.2 μs）。

802.11a 中操作信道的带宽为 20 MHz。操作信道使用多少带宽，纯粹是设计时的决定。较宽的信道具有较高的吞吐量，不过可用频谱中只能容纳较少的操作信道。采用 20-MHz 的操作信道，可以为每个信道提供合理的速度（最高为 54 Mbps），以及在所指定的频谱中提供数量合理的操作信道。802.11a 在调制与编码上提供了相当多的选择。采用较稳定的调制方式与较保守的编码率，可以提供较低速但较可靠的吞吐量；选择较细致的调制方式与较激进的编码率，则可以提供较高但不是那么可靠的吞吐量。

操作信道的结构

和 DS PHY 一样，OFDM 物理层将频谱组织为操作信道。每个带宽为 20 MHz 的信道由 52 个副载波组成。其中有 4 个副载波充当导频（pilot carrier），用以监控路径偏移与 ICI，其余 48 个副载波则是用来传递数据。副载波之间彼此相距 0.3125 MHz。信道编号从 −26 至 26，如图 13-8 所示。由于信号处理上的需要，副载波 0 并未使用。

副载波 −21、−7、7 以及 21 被指定为导频。为了避免在 Fourier 变换中出现过强的光谱线（strong spectral line），导频会以 802.11a 所规范的保守调制技术来传送固定的位序列。

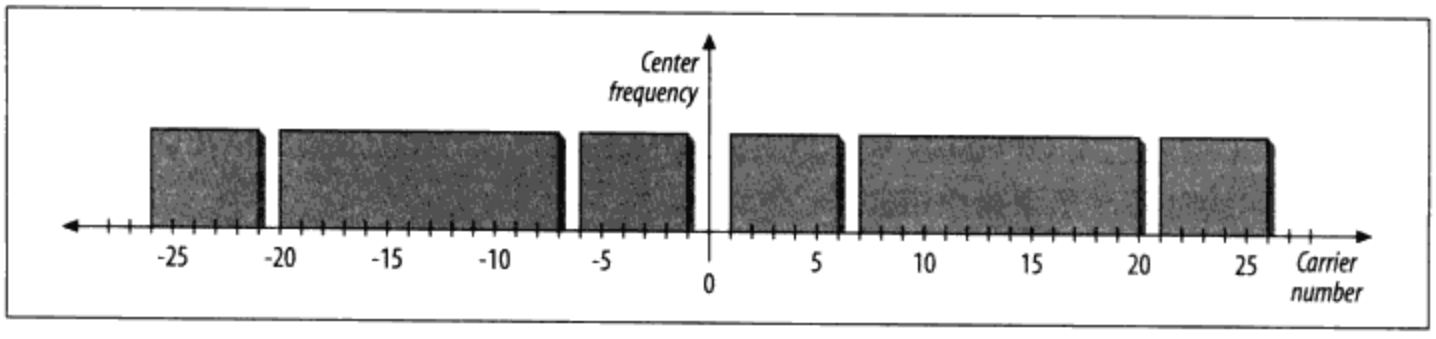


图 13-8：OFDM 信道的结构

子信道调制技术

802.11a在每个子信道上使用正交调幅（quadrature amplitude modulation，简称QAM）技术来传送数据。QAM是在单一载波（single carrier wave）上编码数据，不过该载波是由同相（in-phase）与正交（quadrature）两种信号组成。QAM会同时对这两种信号进行调幅，即根据输入信号的大小调整载波波形。主载波是以同相信号为名，简写为I。正交信号落后1/4周期，简写为Q（也可以用复数来表示其波形，构建出QAM的数理模型）。基本上，这个组合信号的振幅以及相移均用来编码信息（注3）。

QAM被广泛使用于无线电传输系统。以北美的电视系统而言，同相信号用来承载亮度（luminance或brightness）信息，而正交信号则用来承载色彩（color）信息。调幅广播也可以有立体声，一种称为C-QUAM的正交调幅系统就是以正交信号来编码立体声（stereo）信息。

电视和广播通常属于模拟系统。在数字系统中，同相与正交信号经过量子化（*quantized*）被限定在一组特定电平。当两种信号都被限定在一组特定电平时，结果就形成了所谓的星座图（constellation）。星座图通常是在二维平面上描绘出同相与正交信号的可能值。星座图上的每个点代表一种符号（symbol），每个符号代表特定的位值。提到QAM时，通常会在其前面标注星座图中的位数，例如64-QAM。在每个方向，量化值的数目必须是2的乘幂数，因此QAM前面附注的数字也将是2的乘幂数（power of two）。和其他提案一样，802.11a采用方形星座图，即其值必须为2的偶次幂数（even power of two），而此数字恰为正方形（16-QAM, 64-QAM,256-QAM）。

要提高数据率，只要使用点数更多的星座图即可。不过当数据率提高，接收到的信号质量必须足够好，否则就难以区别星座图中的相邻点。如果距离太近，每个点的可接受误差范围就会缩小。802.11a在物理层标准中规范了每个星座点的最大可接受误差范围。图

注3：802.11直接序列物理层（DS PHY）所使用的相移调制属于QAM的特例，它所调制的是相位而非振幅。

13-9 显示了 802.11a 所使用的星座图。BPSK 与 QPSK 的位率最低，它们是直接序列物理层所使用的两种相移键控调制。

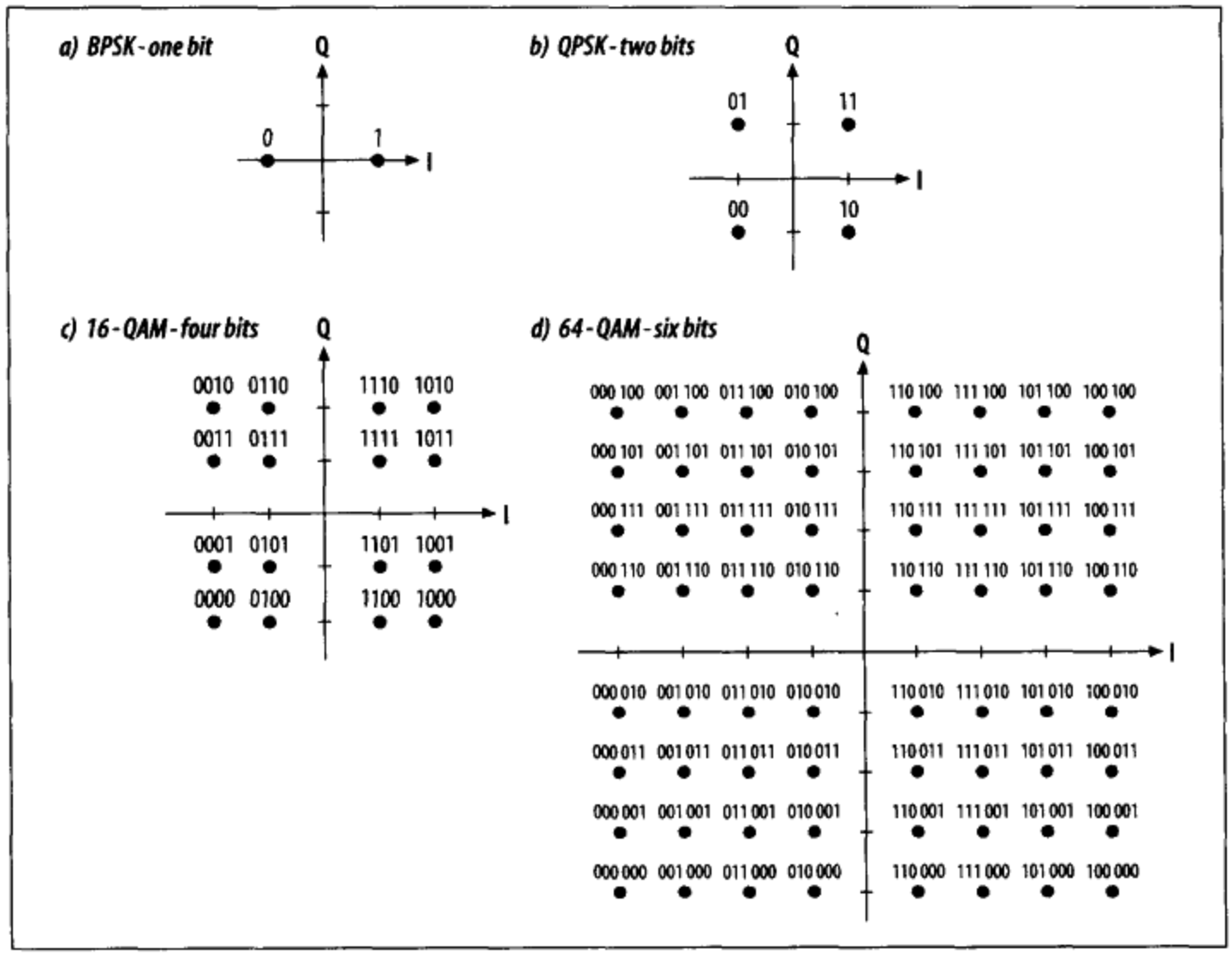


图 13-9：802.11a 所使用的星座图

子信道数乘以每个信道的位数，就可以得出无线电信道的总容量。使用64-QAM时，每个子信道可以承载 6 个位。802.11a使用48个子信道，因此每个信道的容量为288个位。不过，还有另外一个属性必须说明。大多数无线电信道操作不可能没有错误出现，因此必须加入错误修正码。

前向纠错与卷积编码

严格来讲，前向纠错（forward error correcting，简称 FEC）并不属于 OFDM。不过，当信号遭受窄带干扰或者在特定的窄带频率面临所谓的深度衰落（deep fading）时，也可以使用OFDM。一旦发生衰落现象，由于所收到的振幅十分微小，因此信道就会丧失承载数据的能力。为了防止某些衰落的信道造成位错误率（bit error rate）大幅上扬，实

现时可以使用OFDM为所有子信道加上纠错码（error correction code）。搭配纠错码的OFDM有时也称为编码OFDM（coded OFDM）。

编码OFDM会在各个信道使用前向纠错（forward error correction，简称FEC）码。只要遗失或受损的位数不多，FEC系统就可以让接收器检测受损位并加以修复。为了具备纠错能力，必须在数据流中加入冗余位（redundant bit）。FEC码的运作方式，是根据当前所传送的数据位来产生一个状态引擎(state engine)并且将它们编码至多个符号中。以这些符号抹平噪声，就可以把瞬间噪声减至某种程度，使接收器重组位流的能力不至于受误差所影响。

可用的前向纠错码有两种。分组码（*block code*）采用大小固定的输入块，而卷积码(*convolutional code*)则可以应用于任何长度的流。分组码主要用于以固定长度来存储、传输或处理数据的应用。DVD、CD以及硬盘等均使用分组码。不过对无线局域网络而言，卷积码是比较好的选择，因为传输的帧的长度通常并不固定（注4）。

卷积码有两个主要参数。*constraint length*决定了数据位的平均时间。constraint length越长，平均（average）数据位（包含噪声）就需要越多时间，虽然解码器的复杂度会因此而增加，不过这是换取较可靠传输的代价。至于较短的constraint length，则是使用802.11a标准建议的Viterbi算法。之所以有此建议，是因为Viterbi解码器属于最大相似度（*maximum likelibood*）解码器。Viterbi解码器解读出的数据位和原始数据的相似程度最高。并非所有解码器均采用最大相似度算法，虽然它对数字传输系统而言显然是项重要的属性。802.11a所使用的constraint length为7，这个数字是Viterbi解码器实际应用上的极限（Viterbi解码的复杂度会随着constraint length成指数递增）。

第二个参数是编码率（coding rate，简写为R），用来决定加入多少冗余位。它代表每个编码位可以传送多少数据位。R=1/2的卷积码代表每两个编码位传送一个数据位。比较激进的做法可能会加入较少的冗余信息，例如使用3/4的编码率，即当中只有25%的冗余位。选用何种编码率纯粹是工程上的问题。当编码率减少，用来纠错的编码位就比较

注4：在1993年，发现了两组卷积码可以组成所谓的并行级联卷积码（turbo code）。并行及联卷积码的威力十分强大，不过代价是必须付出一些卷积码的延迟时间。如果延迟一些时间无妨，就可以使用并行级联卷积码，例如外层空间与卫星通信。并行级联卷积码的进一步信息可以参考Jet Propulsion Laboratory的网站（*http://www331.jpl.nasa.gov/public/JPLtcodes.html*），其中的报道比较了Voyager与Cassini两次探测所使用的并行级联卷积码与纠错码。并行级联卷积码也用于Qualcomm的3G因特网访问系统1xEV-DO。

多，因此比较牢靠，不过必须付出吞吐量变少的代价。802.11a规范了三种编码率，其中最保守的做法是使用1/2的编码率，至于最激进的做法，编码率甚至高达3/4（注5）。

卷积编码率可以通过收缩（*puncturing*）过程加以改变。收缩码的做法是丢弃某些编码位(coded bit)，从而提高卷积码的编码率。数据编码时应采用较低的编码率。以802.11a为例，最低的编码率是1/2，因此数据变为原先的两倍。要将编码率提高为3/4，可以丢弃其中1/3的编码数据，即将编码数据“收缩”(punctured)。要收缩2/3的编码率，即丢弃30%的编码数据。扣除丢弃的位后才是真正传送的编码数据。在接收端，解码器会在收缩的部分填充无关紧要的位。图13-10显示了将编码率从1/2提高为3/4的收缩过程。使用收缩码的好处是，它可以用软件控制的卷积编码器来实现，而且可以通过软件。使用不同的收缩模式（puncturing pattern）来变更编码率。

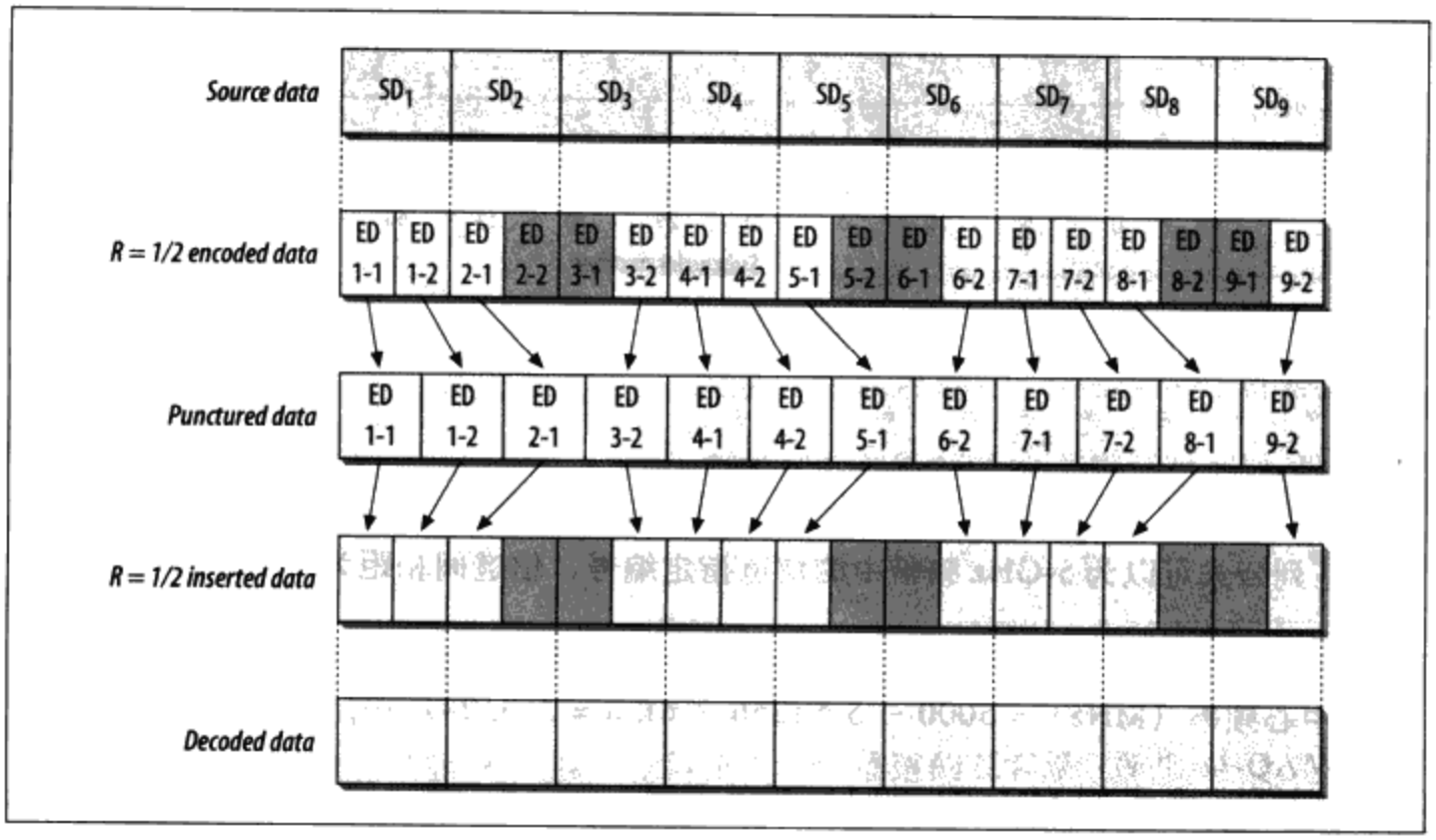


图 13-10：通过收缩过程提高编码率

子信道交错

每个操作信道由48个信道组成。基本上每个操作信道的吞吐量就是48个数据流的总和。所接收到的编码位流必须映射到正确的副载波。802.11a所使用的是一组交错规则，而不是使用简单的round-robin算法来轮流将位映射到副载波，例如第一个位映射到第一个

注5： 802.11a所使用的卷积码长度限制为7，编码率为1/2。Voyager进行深度太空之旅时也是使用卷积码。

副载波，第二个位对映到第二个副载波，依此类推。第一项规则可以确保依次传送的位会被分散至相隔较远的副载波，第二项规则可确保依次传送的位映射至不同的星座点。举例而言，图 13-11 显示了用于 16-QAM 的交错操作，其中共有 192 个位。承载数据的副载波总数为48，每个位都必须映射到其中一个副载波。图形中描绘出了每个副载波所映射的点位，并且清楚地显示出了每个副载波负责 4 个编码位。

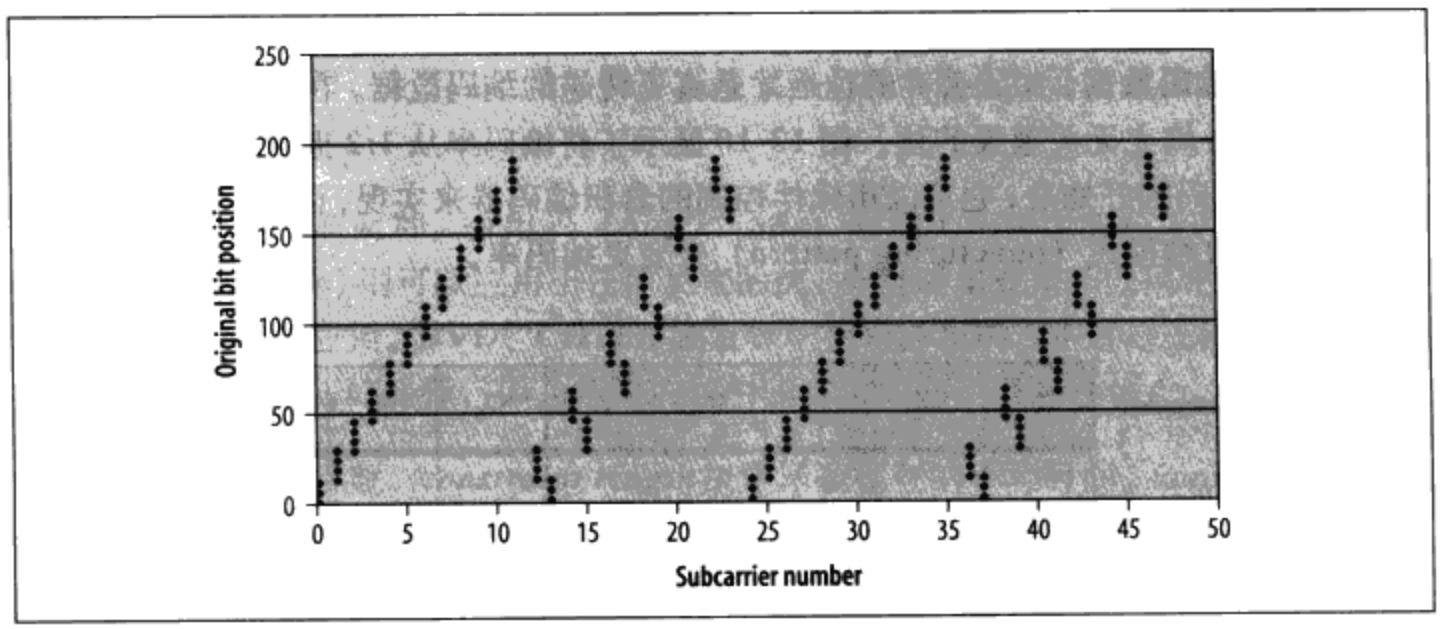


图 13-11：16-QAM 的交错过程

操作信道

根据下列公式可以为 5-GHz 频带中的信道指定编号，信道间相距为 5 MHz：

中心频率（MHz）=5000 + 5 x n, n = 0,1,2, … 199

中心频率（MHz）= 5000 − 5 * (256 − n), n = 240, 241, …, 255

显然，每个带宽为 20-MHz 的 802.11a 信道占用 4 个信道。信道的建议使用方式列于表 13-1。802.11a 原本是针对美国所做的设计。欧洲的信道划分是在 2003 年底被纳入 802.11h，日本的操作信道则是在 2004 年底被纳入 802.11j（注 6）。

注 6：欧洲无线电管制标准是由欧洲邮政电信会议（European Conference of Postal and Telecommunications Administrations，简称 CEPT）负责。相关法规是 CEPT 委托欧洲无线通信委员会（European Radiocommunications Office）制定的。5 GHz 无线局域网管制规定详见 ERC/DEC/(99)23（文件网址为 *http://www.ero.dk/doc98/Official/Pdf/DEC9923E.PDF*）。日本的主管机关是内务及通信产业省（Ministry of Internal Communications，网址为 *http://www.soumu.go.jp/*），相关法规详见 Articles 49.20 与 49.21（*http://www.soumu.go.jp/joho_tsusin/eng/Resources/Legislation/MRA/020226_00.html*）。

表13-1：802.11a/j的操作信道

频率	允许使用地区	最大功率限制[a]	操作信道编号	中心频率(GHz)
4.920~4.980 GHz	日本	250 mW EIRP 且 <1 W，或者 10 mW EIRP	240	4.920
			244	4.940
			248	4.960
			252	4.980
5.040~5.080 GHz	日本	250 mW EIRP 且 <1 W，或者 10 mW EIRP	8	5.040
			12	5.060
			16	5.080
5.15~5.25 GHz	日本	200 mW (<10 mW/MHz)	34	5.170
			38	5.190
			42	5.210
			46	5.230
U-NII 低频带 (5.15~5.25 GHz)	美国	40 mW (2.5 mW/MHz)	36	5.180
			40	5.200
			44	5.220
			48	5.240
U-NII 中频带 (5.25~5.35 GHz)	美国	200 mW (12.5 mW/MHz)	52	5.260
			56	5.280
			60	5.300
			64	5.320
5.470~5.725	欧洲（CEPT）（2003 年 11 月后，也允许在美国地区使用，受 U-NII 的规范[b]）	1 W EIRP	100	5.500
			104	5.520
			108	5.540
			112	5.560
			116	5.580
			120	5.600
			124	5.620
			128	5.640
			132	5.660
			136	5.680
			140	5.700

表13-1：802.11a/j的操作信道（续）

频率	允许使用地区	最大功率限制[a]	操作信道编号	中心频率（GHz）
U-NII 高频带		800 mW	149	5.745
(5.725~5.825 GHz)		(50 mW/MHz)	153	5.765
			157	5.785
			161	5.805

a: 美国允许使用的功率，相当于增益为 6 dBi 的天线的最大输出功率。

b: FCC 03-287 另外开放了这段频谱（*http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-287A1.pdf*），不过在本书即将付印时，测试程序仍在开发当中。未经测试认证，任何设备均不得在美国使用此频谱。

操作频带尚有一些值得注意的功能。和DS PHY一样，OFDM会使用传输屏蔽（transmit mask）来防止功率泄漏至相邻频带。所使用的屏蔽如图 13-12 所示。

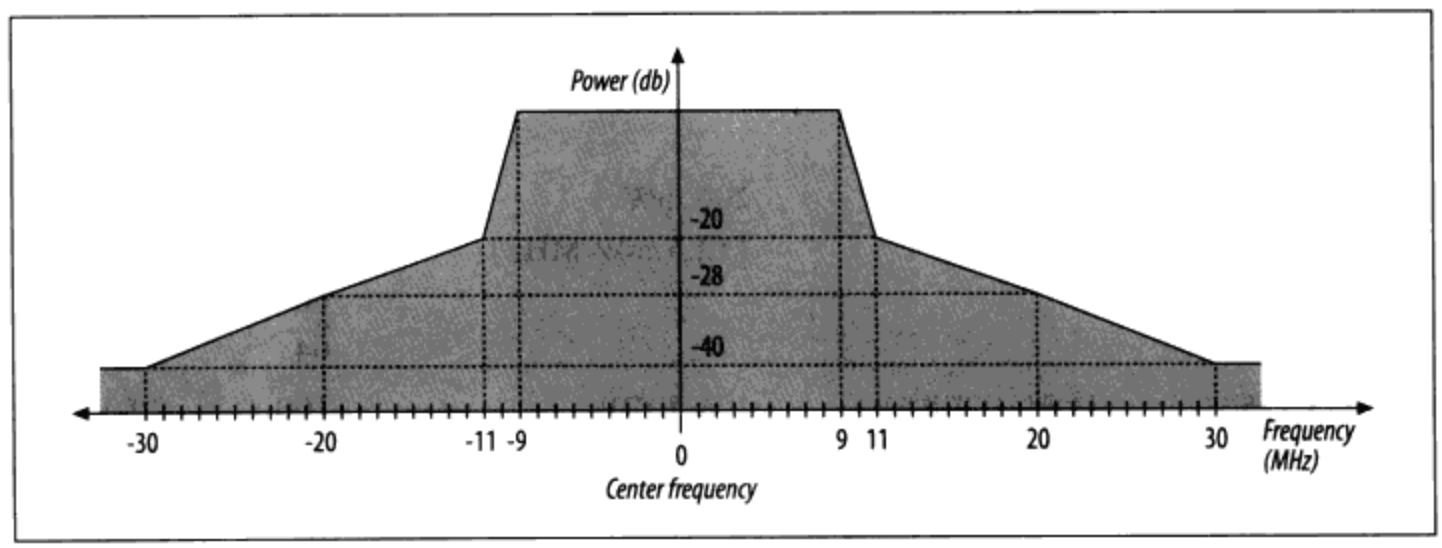


图13-12：802.11a的频谱传输屏蔽

图13-13显示了美国所使用的802.11a信道。在每个U-NII频带（band）中包含4个信道（channel）。在两个较低的频带中允许信道相互重叠，以及在U-NII低频带与中频带两旁使用30-MHz的防护频带。

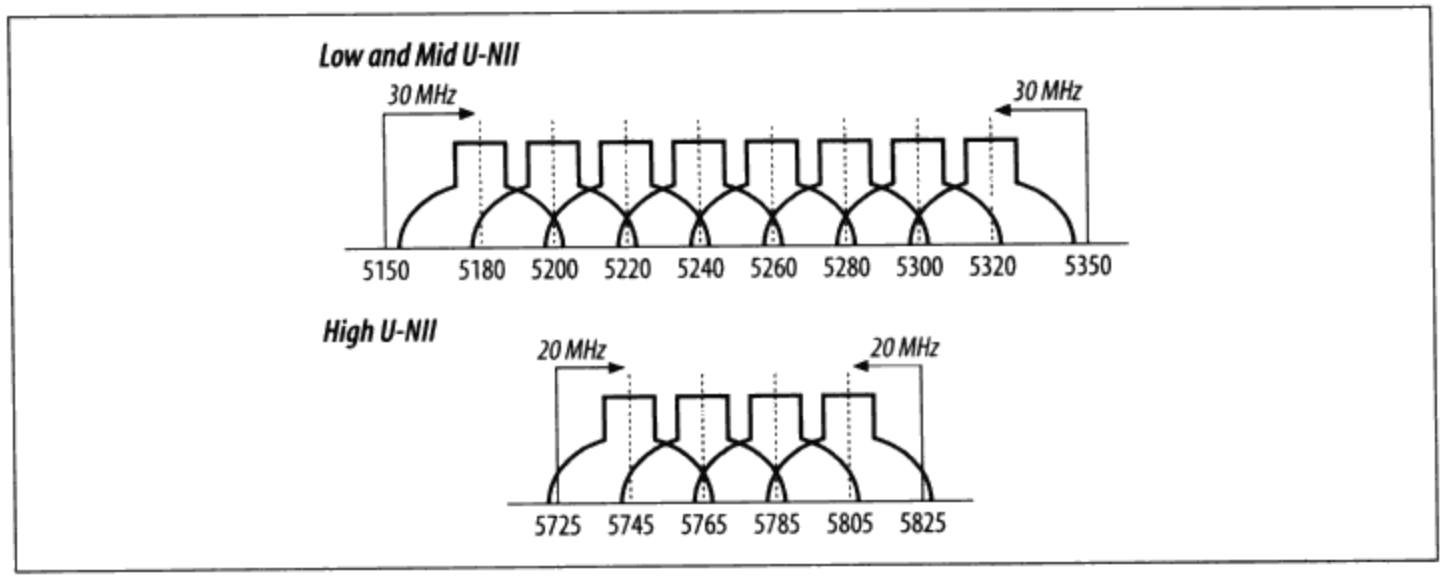


图 13-13：表 13-1 中的操作频带的图示

OFDM PLCP

和其他物理层一样，OFDM PHY 具有它自己的 PLCP，其中包含了该物理层专属的帧参数。

成帧

OFDM PHY 负责添加前导码（preamble）以及 PLCP 标头。此外，它也会添加若干结尾的位以协助所使用的编码机制。本节是以逻辑的方式来区分 PLCP 帧，不过有些组件涵盖协议单元中不同的字段。图 13-14 是我们进行 OFDM 帧讨论的出发点。

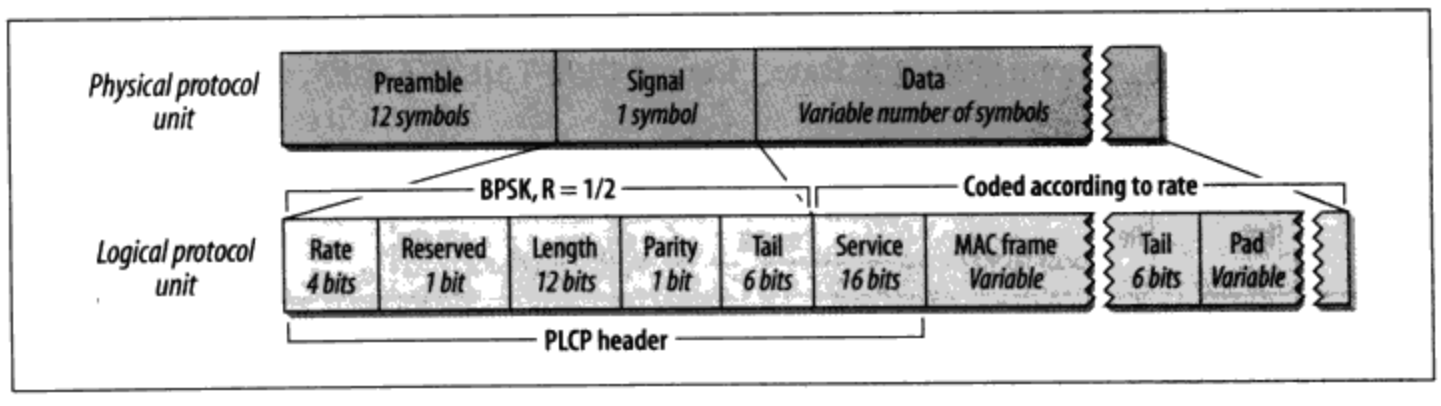


图 13-14：OFDM PLCP 的成帧格式

图 13-15 显示了帧的前半段，其中包含防护间隔（guard interval）以及发射器所使用的加窗法（windowing）。前导码持续了 16 us，平均分配给短训练序列（short training sequence）与长训练序列（long training sequence）。两者之间的区别将于下节探讨。前导码之后，由一个 OFDM 符号携载 Signal 字段，然后由数据符号携载 PLCP 标头的结束

字段，最后是MAC有效载荷（payload）以及结尾位（trailer）。所有符号均使用经过修饰的余弦窗口（cosine window）以确保能够平稳过渡。在用来同步频率的短前导码（short preamble）之后，会使用防护时间（guard time）来防止多径衰落（multipath fading）。

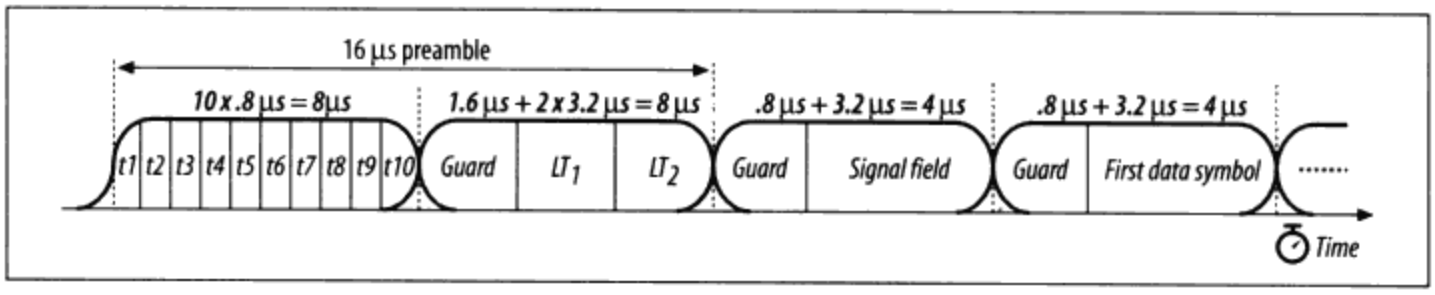


图 13-15：前导码与帧的开始部分

前导码

和所有常见的IEEE 802网络一样（包括所有的802.11物理层），OFDM物理协议单元（physical protocol unit）是以一个前导码（preamble）开始。它是由12个OFDM符号所组成，借以同步发送端与接收端的定时器。前面10个符号是短训练序列（short training sequence），接收器会用它来锁定信号；如果使用多组天线，也可由它来选用天线以及同步开始解码后续符号时所需的大规模时序关系。短训练序列传输时并未使用防护间隔。在短训练序列后面紧跟着两个长训练序列（long training sequence）。长训练序列主要用于微调timing acquisition，同时采用防护间隔来加以保护。

标头

PLCP标头是物理协议单元的Signal字段中传送的，它结合了物理协议单元的Data字段的Service子字段。Signal字段包含Rate、Length以及Tail等子字段，如图13-16所示。

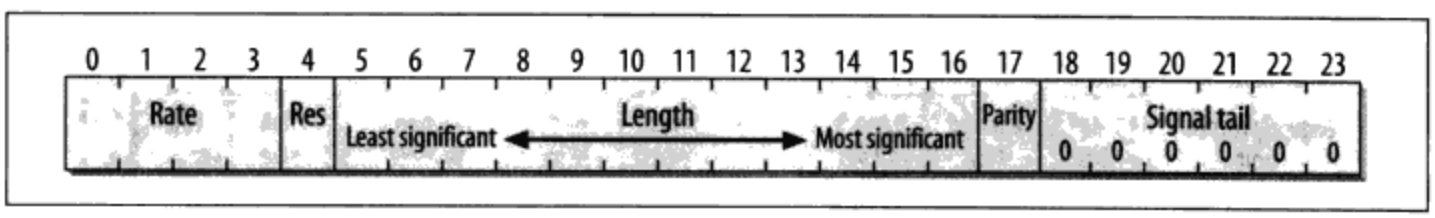


图 13-16：OFDM PLCP 帧的 Singnal 字段

Rate（4个位）

以4个位编码的数据率。表13-2显示了每一种数据率所对应的位编码。每一种数据率所使用的编码与调制机制的详细说明请参阅“OFDM PMD”一节。

表 13-2：数据率及其位编码

数据率（Mbps）	位（依传送次序排列）
6	1101
9	1111
12	0101
18	0111
24	1001
36	1011
48	0001
54	0011

Length（12 个位）

所包含的MAC帧中的字节数，以12个位来加以记录。和大多数字段一样，此字段由最低位至最高位逐一被传送。Length（长度）字段会经过卷积编码以防止错误发生。

Reserved（1 个位）与Parity（1 个位）

位 4 保留供未来使用，必须设定为 0。位 17 是前 16 个 Signal 位的 even parity（偶同位）位，用来避免数据损毁。

Tail（6 个位）

Signal 字段以 6 个值为 0 的结尾位结束以展开卷积码（convolutional code）。因此，在定义上这 6 个位必须交由卷积编码处理。

Service（16 个比特位）

PLCP 标头的最后一个字段是长度为 16 位的 Service 字段。和 PLCP 标头的其他字段不同的是，它是以所包含的MAC帧的数据率通过物理协议单元的Data字段来传送。此字段前 8 位设定为 0。和其他物理层一样，在传送之前，MAC 帧必须经过扰频。前 6 位设定为 0 是为了启动扰频器。剩下的 9 位目前保留，在未来另有他用之前必须设定为 0。

Data

数据所使用的编码机制取决于数据率。在传送之前，数据必须经过扰频，和其他物理层一样。标头的 Service 字段之所以包含在物理层协议单元的 Data 字段，是因为必须以它来启动扰频器。

Trailer

物理协议单元的Data字段会以标尾（trailer）结束（802.11a规范说明书并没有称结尾字段为“标尾”，但它把“标尾”当成术语来看）。标尾由两个字段组成：

Tail（6个位）

和PLCP标头的结尾位一样，附加至MAC帧结尾的位主要是让卷积编码可以平顺结束。之所以需要6个位，是因为卷积编码的长度限制为7。

Pad（位数不定）

802.11a所使用的OFDM是以大小固定的位块来传送数据。Data字段之所以加上填充位，是为了使数据长度与位块的大小一致。位块的大小取决于数据所使用的调制方式与编码率，下一节将会加以探讨。

OFDM PMD

OFDM PHY使用了各种不同的调制机制，数据率可达到6 Mbps至54 Mbps。在所有情况下，物理层在48个子信道所使用的符号率为每秒250000个符号，至于每个符号可以承载几个数据位则视情况而定。单一OFDM符号会分布在所有这48个子信道中。

编码与调制

OFDM PHY的速率有四级：6与9 Mbps、12与18 Mbps、24与36 Mbps以及48与54 Mbps。6、12与24 Mbps是必要的项目，即前三级的最低速率，因此在遭遇干扰时也最稳定。第一级的速率使用二进制相移键控（binary phase shift keying，简称BPSK）在每个子信道编码一个位，或者相当于每个符号48个位。卷积编码（convolution coding）是指这些位中有一半或者1/4是用于纠错的多余位，因此每个符号中实际只包含了24或36个数据位。第二级的速率使用正交相移键控（quadrature phase shift keying，简称QPSK）在每个子信道编码2个位，相当于每个符号96位。去除冗余的卷积码，接收器实际收到的有48或72个数据位。第三与第四级使用BPSK与QPSK的一般形式，称为正交调幅（quadrature amplitude modulation，简称QAM）。16-QAM是以16个符号来编码4个位，而64-QAM则是以64个符号来编码6个位。第三级速率使用16-QAM以及R=1/2与R=3/4的标准型卷积码。不过，为了达到更高速率，64-QAM采用R=2/3与R=3/4的卷积码。表13-3列出了OFDM PHY中每种数据率所使用的编码方式。

表 13-3：各种OFDM数据率的编码细节

速度 (Mbps)	调制方式与编码率（R）	每个子信道所编码的位数[a]	每个符号所编码的位数	每个符号的数据位数[b]
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216
72[c]	64-QAM	6	288	288

a: 每个子信道所编码的位数为调制方式（BPSK、QPSK、16-QAM 或 64-QAM）的函数。

b: 每个符号的数据位数为卷积编码率的函数。

c: 虽然不使用卷积码的情况并未纳入标准，有些产品还是提供这种模式来提升吞吐量。

无线电性能：灵敏度与信道抑制

和其他物理层一样，802.11a 也规范了接收器的最低灵敏度要求，如表 13-4 所示。之前已经提过其他物理层的最低灵敏度。唯一比较值得注意的是802.11a的数据率比较多样，必须针对每个数据率制定最低性能要求。相比较于直接序列物理层，802.11a 所制定的要求算是有过之而无不及。802.11b 要求接收器必须具备 −76 dBm 的灵敏度，相当于 802.11a 中 18 Mbps 与 24 Mbps 这两种数据率（注 7）。

比较值得注意的是信道抑制（channel rejection）的部分。和其他物理层一样，首先在任意信道输入一个比最低灵敏度稍高（3 dB）的信号，然后在相邻或不相邻信道输入第二个信号进行抑制测试。当被测试信道的帧错误率为10%时，注意两个信道间的功率差异。

由此表可知，当数据率越高，接收器所收到的信号就越容易被损毁。如果 802.11a 网络的接入点过于密集，位于相邻接入点间的工作站可能会同时接收到来自两者的54 Mbps 信号，造成工作站的无线电芯片组无法判读。不过 54 Mbps 的传输距离相对较短，因此不太会出现这种情况。此外，虽然有些芯片组的性能优于标准所规定，不过大多数厂商并不会在网卡的规格表中列出邻道抑制的数据。

注 7： 不过 802.11a 所使用的频率具有较高的路径损耗。

表13-4：接收器的性能要求

数据传输率（Mbps）	最低灵敏度（dBm）	邻道抑制值（dB）	非邻道抑制值（dB）
6	−82	16	32
9	−81	15	31
12	−79	13	29
18	−77	11	27
24	−74	8	24
36	−70	4	20
48	−66	0	16
54	−65	−1	15

空闲信道评估

OFDM PHY 规范说明书留下了相当大的空间，让实现人员可以自行选择空闲信道评估（clear channel assessment）技术。信号的强度阈值可用来决定信道是否正在使用中，不过802.11a设备的主要指导原则是设备本身必须符合特定的性能标准。实现时可以使用PLCP 标头的 Packet Length 字段作为空闲信道评估的参数，但并非必要。

传送与接收

802.11a接收器的方块图如图13-17所示。准备传送帧时，802.11a接口会执行下列流程：

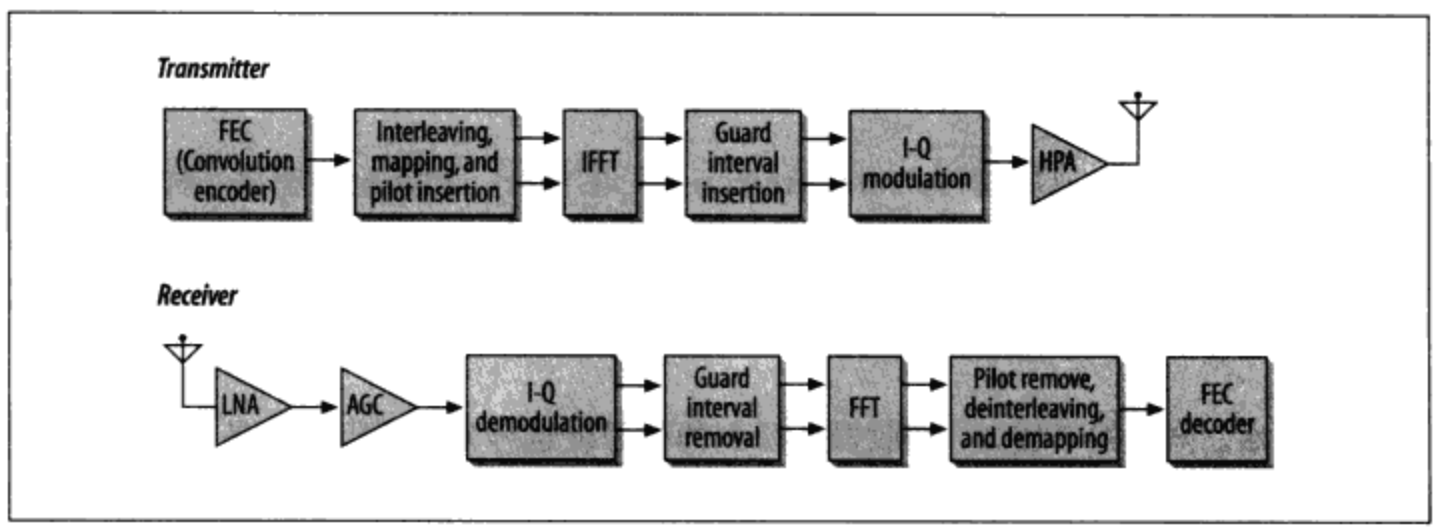


图 13-17：收发器方块图

1. 选择传输率。数据率选择的算法因实现而异，在相同环境下，不同厂商的产品也许会选择不同的速率。速率决定了所使用的调制方式与卷积码以及各个副载波的数据位数。参见表 13-3。

2. 传送 PLCP 前导码，其中包含长短训练序列。
3. 开始传送 SIGNAL 字段中的 PLCP 标头。它并未经过扰频，但经过卷积编码器的编码。
4. 产生封包的数据字段。
   a. 产生 SERVICE 字段，当前这个字段的每个位均设为 0。前面 7 个 0 是用来初始化扰频器，后面 9 位目前保留未用，均设为 0。
   b. 附加数据。
   c. 放置 6 个 0 作为标尾。
   d. 填充位补 0，使之成为副载波块数据位的倍数。
5. 对数据进行扰频，如此可以避免出现长串的 0 或 1。
6. 以卷积编码器进行数据编码。如有必要，再对卷积编码的结果进行收缩处理，以高于 1/2 以上的编码率产生编码后的字符串。
7. 将编码数据（coded data）分成块来处理。块的大小取决于数据符号的调制率。
   a. 执行纠错过程，将块中的位映射到 48 个副载波。
   b. 在操作信道的特定位置插入 4 个导频。
   c. 使用逆 Fourier 变换，将频域数据转换为时域数据进行传送。
8. 重复步骤 5 直到所有数据块传送完毕。

确认

802.11a 标准规定 6、12 与 24 Mbps 是必要的（required）数据率。802.11 MAC 要求每个帧都必须得到确认。传送确认时必须采用已关联工作站均支持的数据率。大多数设备是以 24 Mbps 的数据率传送确认信息，如此不仅可以符合上述要求，也可以将网络的总开销（overhead）降至最低。

OFDM 编码范例

正如读者到目前为止所见到的，OFDM 是个相当密集、由多个步骤所构成的过程。802.11a 对原始规范的一项增补记录于附录七，内容是将席勒的《欢乐颂》（Schiller's Ode to Joy）编码后以 802.11a 网络进行传送。802.11a 发布后不久，IEEE 802.11 工作组在范例中发现了一些错误，因此发布了修正版。如果各位对 OFDM 编码的细节感兴趣，可以参考该范例。

OFDM PHY 的特性

OFDM PHY 特有的参数列于表 13-5。和第十一和十二章所介绍的物理层一样，OFDM PHY 也包含一些参数，可用来调整电子零件不同处理阶段所造成的延迟。最后值得注意的是，额外的带宽提升了不少吞吐量。美国原本有12个信道，最近又清理出其他8个信道。以传输时间的50%计算，20个共存信道可以提供500 Mbps以上的通信量。这个数字是其他物理层标准远远不及的。

表13-5：OFDM PHY参数

参数	值	备注
最大MAC 帧长度	4095 byte	
时隙时间	9 μs	
SIFS 时间	16 μs	SIFS可用来推衍出其他帧间间隔值（DIFS、PIFS 以及 EIFS）
竞争窗口的大小	15 至 1023 个时隙	
前导码持续时间	20 μs	
PLCP 标头持续时间	4 μs	
接收器灵敏度	−65 至 −82 dBm	取决于数据传输速度

和其他的物理层一样，OFDM PHY 中也有些属性可供厂商调整，使系统各部分的延迟时间保持均衡。其中包括MAC、PLCP、收发器等的延迟变量以及收发器电子零件个别变异的相关变量。

第十四章

802.11g：增强速率物理层

当无线局域网首次进入主流运算领域时，实际上没有太多选择。当时802.11b刚成为标准，渴望提供近似Ethernet的速度。平心而论，这种速度在当时并不算快。等到802.11a跨出实验室成为商业产品时，用户开始渴望比802.11b更快的速度，但又能够兼容于现有802.11b硬件的产品。802.11g因此应运而生，它除了提供相当于802.11a的额定速率，也使用原本的微波频带。由于操作频率不及802.11a的一半，相比较于5 GHz的802.11a设备，802.11g设备能够传输更远的距离。

802.11g并非革命性的规范。事实上，只要看过规范说明书的新增条款，就知道它运用了不少现成的技术。其所制定的新物理层是以现有技术为基础，只是稍微做了修改。802.11g规范说明书中绝大部分的篇幅都是用来提供向下兼容性。

802.11g的组件

802.11g其实是将好几种物理层规范合而为一。虽然统称为增强速率物理层（Extended Rate PHY，简称ERP），但是实际上ERP有好几种不同的“口味”：

ERP-DSSS与ERP-CCK

这两种模式向下兼容于第十一章所提到的原始直接序列规范（1 Mbps与2 Mbps），以及第十二章所提到的802.11b规范（5.5 Mbps与11 Mbps）。为了向下兼容，在规范上必须稍做改动。

ERP-OFDM

这是802.11g的主要模式。基本上，它是在ISM频带（2.4 GHz）中执行802.11a，不过为了向下兼容，在规范上必须稍做改动。它所支持的速率如同802.11a：6、9、12、18、24、36、48与54 Mbps。其中6、12与24 Mbps为必要的（mandatory）传输速率。

ERP-PBCC

这是802.11b的PBCC标准的可选增强功能（optional extension），提供22与33 Mbps的数据率。虽然属于标准的一部分，不过市面上大多数芯片组并未实现这种模式，也未得到广泛使用。

DSSS-OFDM

这是一种混合模式，封包数据（packet data）是以DSSS标头进行编码，有效载荷（payload）则是以OFDM进行编码。之所以开发这种模式，部分原因是为了提供向下兼容性。虽然802.11b无法识别经OFDM调制的内容，但可根据标头所提供的信息来判断封包的持续时间。此功能并非必要，也未被广泛实现。

任何实现802.11g的设备均需要支持某些必要模式。为了向下兼容性，802.11g设备必须支持1与2 Mbps的DSSS调制（802.11）以及5.5与11 Mbps的CCK调制（802.11b）。除了基本的OFDM，所有的802.11g工作站也必须支持6、12与24 Mbps的OFDM调制。

兼容性议题

802.11g的必要模式只是稍微修改了现有的物理层，为了顾及向下兼容性，另外做了些许变动。802.11g工作站必须加以配合以便与其他旧工作站并存。现有的规范并未改变，802.11b网卡依然运作如昔。唯一的差别在于802.11g网卡具备某些802.11b所没有的功能。

802.11b设备实现了两种不同的规范：原始802.11标准所规范的较慢的直接序列（DSSS），以及802.11b所规范的高速的补码键控（CCK）物理层。802.11g同时采用这两种标准，只做了少许修改。除了旧式工作站，802.11g工作站也得和其他802.11g工作站通信，因此必须支持802.11g所规范的前导码以及同步操作。更重要的是，802.11g工作站必须支持短前导码，因为它有助于维持较高的吞吐量。802.11g的无线电系统也必须具备更高的信号灵敏度。

此外，802.11g设备必须实现ERP-OFDM，而ERP-OFDM大致上是以802.11a为基础。事实上，它与802.11a几乎完全相同，只有少许显著的差异。最值得注意的是，802.11g采用了802.11b的信道规划，因此仍然只有三个非重叠信道可以使用（相邻信道重叠表详见第十三章。有关三个非重叠信道的注释同样适用于802.11g）。其所使用的帧间间隔

与时隙也兼容于使用ISM频带的旧式802.11工作站。不过，802.11g的管制规定和802.11b的有些差异。例如，日本允许802.11b使用1~14信道，不过只允许802.11g使用1~13信道。

保护机制

保护机制是802.11b与802.11g的一项主要差异。之所以需要保护机制，是因为实现这两种规范的芯片组之间存在一种非对称性（asymmetry）。设计人员面临的一个问题是802.11g所使用的调制机制与802.11b的不同。802.11g芯片必须向下兼容并且能够正确接收与解读802.11b信号。正如同技术领域常见的情况，反之则不然。802.11b芯片组无法解读较高速的802.11g信号。解决方案的第一个部分，是要求802.11g工作站在基本服务集进行传输时使用所有工作站均支持的速率。如果接入点必须同时服务802.11b与802.11g工作站，传送Beacon帧时就不能使用高于11Mbps的数据率。

解决方案的第二个部分，则是要避免802.11g与802.11b网络相互干扰。为了确保802.11b工作站能够得知802.11g正在进行传输，802.11g制定了一种保护机制以保护802.11b工作站免于受到干扰。保护机制的基本运作方式如图14-1所示。为了避免在OFDM帧及其响应信息传送期间造成干扰，必须传送一个较慢的帧来更新NAV。保护机制主要有两种。通常，802.11g工作站是使用反身CTS保护（CTS-to-self protection）机制，如图14-1a)所示。当工作站必须为待传帧采用保护机制时，就会发送一个CTS帧并且将接收端地址设为本身的MAC。换言之，CTS帧的目的地为工作站本身。CTS帧用来更新网络分配向量（NAV），告诉其他正在使用物理媒介的工作站随后将占用无线链路多少时间，以便传送CTS、经OFDM调制的帧以及经OFDM调制的确认信息。虽然工作站是将CTS传送给自己，不过网络上所有工作站都必须聆听CTS帧并且据此更新NAV。CTS帧是以可行的最高速率传送并且使用所有工作站均了解的调制方式。如此一来，吞吐量必然会大幅降低。以最高速率传送最大的Ethernet数据帧及其确认信息总共需要294微秒，不过传送用来清空网络的CTS帧至少需要107微秒。如果使用长前导码，可能需要200微秒以上的时间。

第二种机制是采用完整的RTS/CTS交换，如图14-1 b)所示。完整的RTS/CTS交换在遭遇隐藏节点时比较可靠，不过必须以牺牲一些吞吐量作为代价。以刚才的反身CTS（CTS-to-self）为例，用来预订媒介使用权的兼容性帧可能会比传送数据占用更长的时间。RTS与CTS各占用100微秒，而最大数据帧及其确认信息总共才用掉300微秒。将RTS所需要的额外时间纳入计算，我估计使用完整的RTS/CTS交换会比使用反身CTS减少1/3左右的总吞吐量（注1）。

注1： 详见《When is 54 Not Equal to 54: An Analysis of 802.11g Throughput》一文，网址为*http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html*。

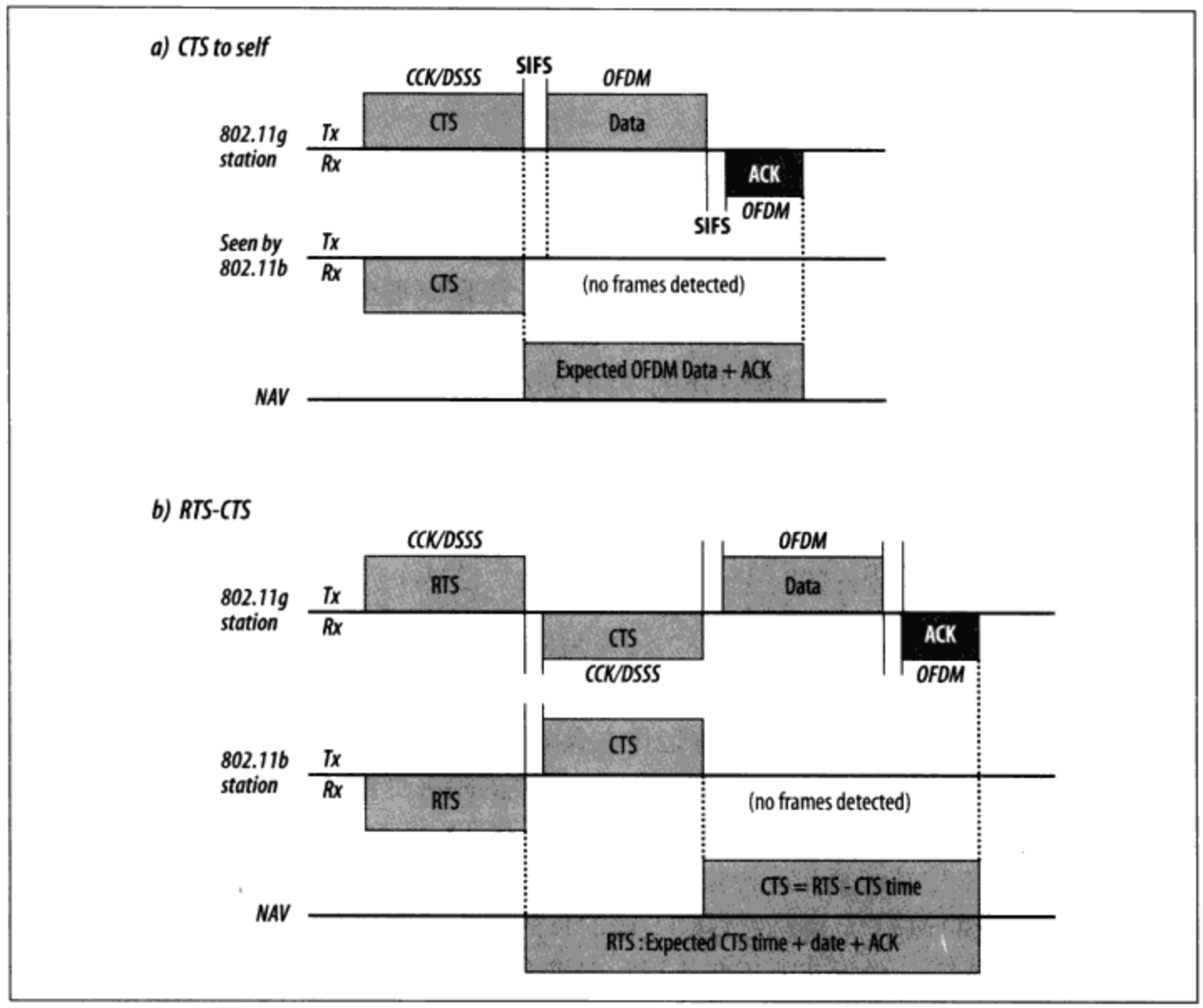


图 14-1：保护机制的基本运作方式

为了确保网络上所有工作站均能接收与处理保护帧，必须依循802.11b规范来传送保护帧。传送时可以使用1 Mbps或2 Mbps的相移键控，或者5.5 Mbps或11 Mbps的CCK。所有802.11b工作站均了解这种调制方式，并能据此更新本身的虚拟载波监听。图14-1显示了所使用的调制方式，而且只显示了802.11b工作站能够理解的兼容调制方式。

注意： 只有保护帧需要以兼容于802.11b的数据率进行传输。保护机制并未要求802.11g工作站在传递有效载荷数据时也必须使用较低的速率，这是一般容易误解之处。

凡是需要确保802.11g工作站不会干扰802.11b工作站的场合，就得启用保护机制。比较明显的情况是802.11b工作站与接入点进行关联时。此时所有与接入点关联的802.11g工作站均会启动保护机制，以确保802.11b工作站不至于受到或造成干扰。比较不明显的场合，像是与802.11b接入点共享信道的情况下也会启用保护机制。因为共享信道的

两个接入点必须分享物理媒介，其他接入点上使用相同信道的802.11b工作站也会触发保护机制。

保护机制是通过Beacon帧中的ERP信息元素来控制。802.11g在Beacon帧的信息元素中加入了一个 *Use Protection* 位。只要此位设定为1，工作站就必须使用保护机制。当一个非802.11g工作站关联到无线局域网时，此保护位就会被设定。负责发送Beacon帧的工作站必须负责判断是否启用保护机制。在基础结构型网络里，保护机制是由接入点所掌控；在独立形网络中，则是由Beacon发送者负责。每当非802.11g工作站关联到网络，或者该区有非802.11g工作站正在进行传输时就会启动保护机制。要判断工作站是否具备802.11g能力，可以由重叠网络所接收到的管理帧（包括Beacon与Probe Response帧）加以推断，观察其中是否包含802.11g所支持的速率。

802.11g网络中的Beacon帧也可以用来控制前导码的长度，借此达到保护的目的。在ERP信息元素中，*Barker Preamble Mode* 位可用来告诉所有已关联的工作站，究竟应该使用长前导码还是短前导码。如果网络上所有工作站均能够使用短前导码，则Barker Preamble Mode位就会被设定为0，并且所有工作站都将使用短前导码以达到更高效率。不过，只要其中一个工作站无法使用短前导码与网络关联，此位就会被设定为1，而且所有保护帧均将使用长前导码。

如同其他必须向下兼容的技术，802.11g也会因此受到限制。如果不启用保护机制，802.11g与802.11a的吞吐量不相上下。一旦启用保护机制，据我估算，大概只剩下50%的吞吐量，这取决于TCP数据段与TCP确认信息两者的比例。通过802.11传输一个完整的1500字节的Ethernet帧并且得到确认需时428微秒；如果使用反身CTS保护机制，所需要的时间就跳升为557微秒；RTS/CTS会增加更多负担，同样的传输需时774微秒。有些802.11g接入点不接受非802.11g工作站的关联请求，主要是为了避免使用保护机制。拒绝那些无法以802.11g的速率关联的工作站，就有更多的机会不启动保护机制。当然，被拒绝的工作站有可能会找到愿意接纳它们且使用相同信道的网络，如此一来仍会触发保护机制。

注意： 虽然802.11g能够达到802.11a的速率，不过保护机制所占用的额外传输时间或许会让有效载荷数据吞吐量腰斩一半。

ERP-PBCC与DSSS-OFDM物理层不需要用到保护机制。两者均使用兼容于802.11b的标头，因此不必传送额外的帧来更新虚拟载波监听与NAV，如图14-2所示。802.11b工作站能够解读标头并且根据标头的内容来更新虚拟载波监听机制。除非媒介解除锁定，否则不允许进行传输。虽然802.11b工作站无法解读帧的内容，但可以根据标头所提供的信息来避免造成干扰。不过，使用ERP-PBCC或DSSS-OFDM并非毫无代价。就某种

意义而言，它们无异于随时使用保护机制，因为它们使用较长的标头。ERP-PBCC 与 DSSS-OFDM 所使用的标头无法丢弃，而且至少占用 96 微秒；相对地，常见的 ERP-OFDM 模式必须使用与 CTS 帧相同的标头，至少需要 107 微秒的传输时间，另外加上 10 微秒的 SIFS 间隔。不过，ERP-OFDM 只有在使用保护机制时才需要付出此代价，但 ERP-PBCC 与 DSSS-OFDM 这两种模式则无法避免。

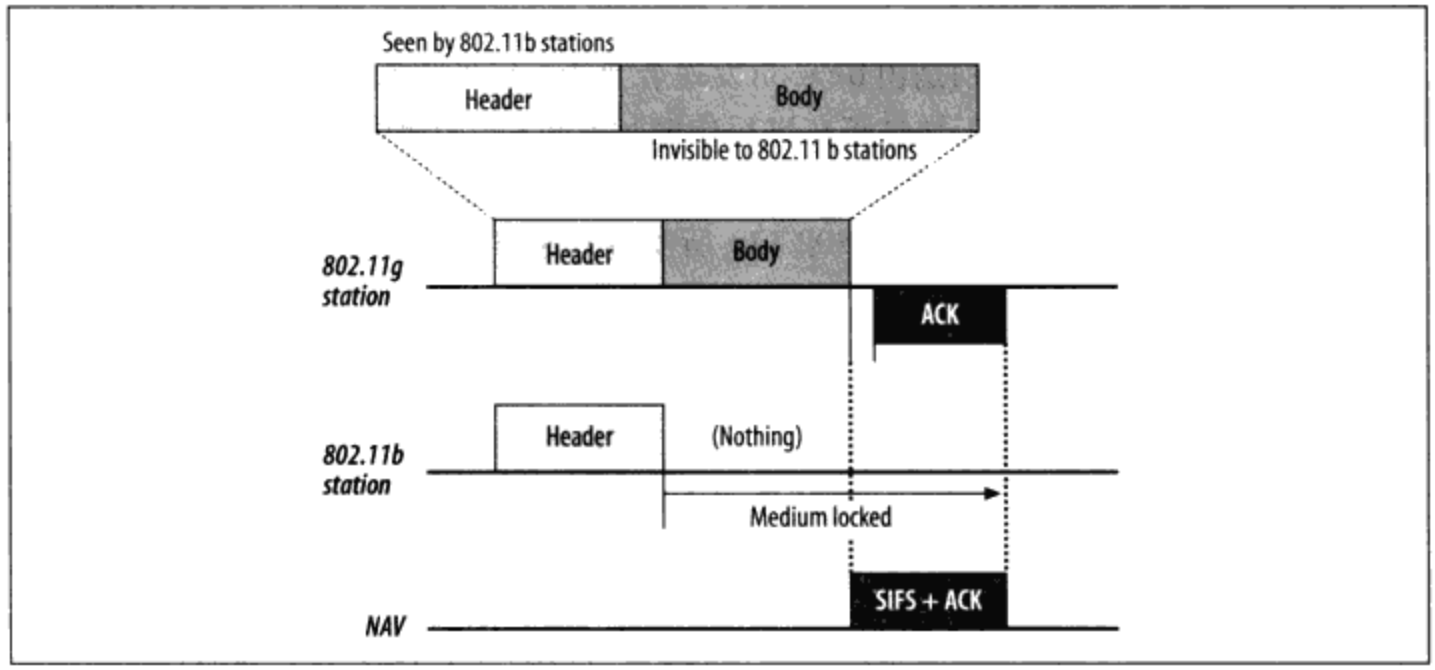


图 14-2：ERP-PBCC 与 DSSS-OFDM 的帧格式

ERP 的物理层会聚过程（PLCP）

ERP PHY 的会聚子层相当复杂。由于操作模式众多，要通过无线电接口将帧传送出去就有好几种不同的方式。本章一开始所提到的各种模式都自有一套物理层成帧。

ERP-OFDM 的成帧

此模式可以说是本规范的核心，所有工作站均需实现此模式。一般所谓“支持 802.11g”即指 ERP-OFDM，因为大多数工作站默认使用此模式。事实上，了解 ERP-OFDM 物理层的成帧有助于了解大多数的 802.11g 传输操作。

ERP-OFDM 物理层所使用的帧格式几乎和 802.11a 完全相同，如图 14-3 所示。ERP-OFDM 使用相同的逻辑协议数据单元，如图 14-3 最上方所示。事实上，它与 802.11a 的唯一差别在于其后伴随 6 微秒的闲置时间。这段用来组装帧逻辑架构的时间称为信号扩展（signal extension），如图 14-3 中第二行所示。之所以需要这个额外的 6 微秒，是为了让时序的计算与帧的速率等同于 802.11a。802.11a 使用 16 微秒的 SIFS，部分时间是用来对上一个帧进行解码。为了向下兼容于 802.11b，802.11g 仍然采用 802.11b 所使用

的10微秒SIFS。因此，为了给解码过程提供充裕的时间，802.11g另外在帧后面加上6微秒，以便保留16微秒的间隔给硬件执行解码过程。当然，此时会一并设定NAV，好让虚拟载波监听机制在信号扩展时间结束之际能够汇报媒介的闲置状态。OFDM传输显示于图14-3的最下方，与802.11a完全相同。

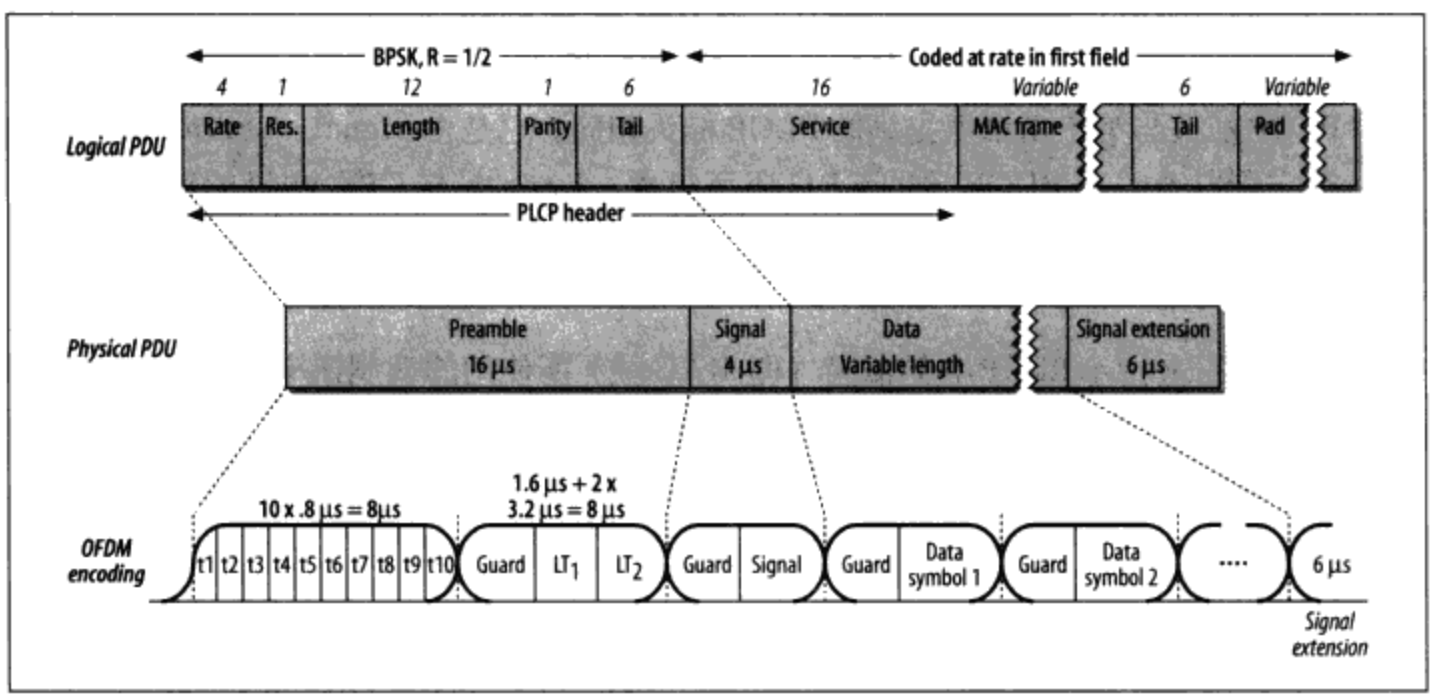


图14-3：ERP-OFDM PLCP帧格式

802.11g的单载波成帧

虽然上一节所提到的OFDM是最常见的调制方式，不过较高速的数据内容也可以使用兼容于802.11b的成帧格式。传统的成帧方式可同时用于封装二进制卷积编码以及DSSS-OFDM物理层。旧式的802.11b工作站也能够解读帧头，因此可以避免在传输进行时访问媒介，也无需用到保护机制。从图14-4中可以看到802.11g如何进行传统的单载波成帧。

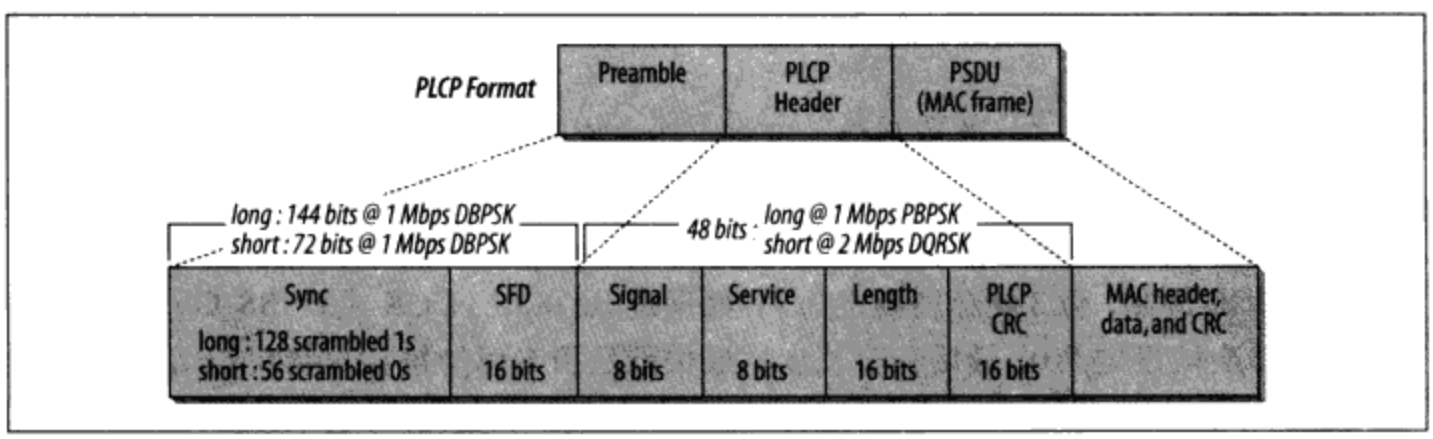


图14-4：采用长前导码的ERP PLCP帧格式

Preamble

Preamble（前导码）与第十二章所提到的802.11b preamble相同，由一个同步（Sync）字段以及起始帧定界符（SFD）组成。它可以是144位的长前导码或者是72位的短前导码。不论长短，Preamble均使用DBPSK调制，以1 Mbps的速率传输。调制之前，数据如同在802.11b中一样会先经过加密编码。

PLCP标头

PLCP标头与第十二章所提到的PLCP标头相同。它是由Signal、Service、Length等字段以及一个PLCP层的CRC码所组成。Length与CRC字段的使用方式与802.11b相同。

Signal字段

此字段用来指示PLCP有效载荷（即MAC帧）所使用的调制速率。起初，它会被定义为100 kbps的倍数。由于此字段只有8位，因此最高只能编码至25.5 Mbps。为了容纳更高的速率，Signal字段改用数值来表示，如表14-1所示。基本上不需要通过Signal字段来告诉接收器DSSS-OFDM帧使用何种编码率，这项任务由OFDM标头负责。

表14-1 ：单载波帧头中的Signal字段值

速率	Signal字段值（十六进制/二进制）	Signal字段值（十进制）
1 Mbps (ERP-DSSS)	0x0A (0000 1010)	10
2 Mbps (ERP-DSSS)	0x14 (0001 0100)	20
5.5 Mbps (ERP-CCK, ERP-PBCC)	0x37 (0011 0111)	55
11 Mbps (ERP-CCK, ERP-PBCC)	0x6E (0110 1110)	110
22 Mbps (ERP-PBCC)	0xDC (1101 1100)	220
33 Mbps (ERP-PBCC)	0x21 (0010 0001)	33
其他的DSSS-OFDM速率	0x1E (0001 1110)	30

Service字段

Service字段包含了一些控制位，用来协助接收器对帧进行解码，如图14-5所示。如前所述，位0、1与4目前保留未用且必须设定为0。所有802.11g工作站的传输与符号时钟（symbol clock）均会被锁定，因此位2必然设定为1。如果帧主体是以PBCC调制，位3就会被设定为1；如果是以DSSS、CCK或DSSS-OFDM调制，则位3会被设定为0。最后三个长度扩展位则是用来协助接收器判断Length字段所记载的帧长度，以字节为单位，指示需要多少微秒来进行传输。标准中有一套复杂

的规则说明应该设定哪些位，不过这些细节已经超乎本书的需要，何况单载波帧封装技术并不常用。

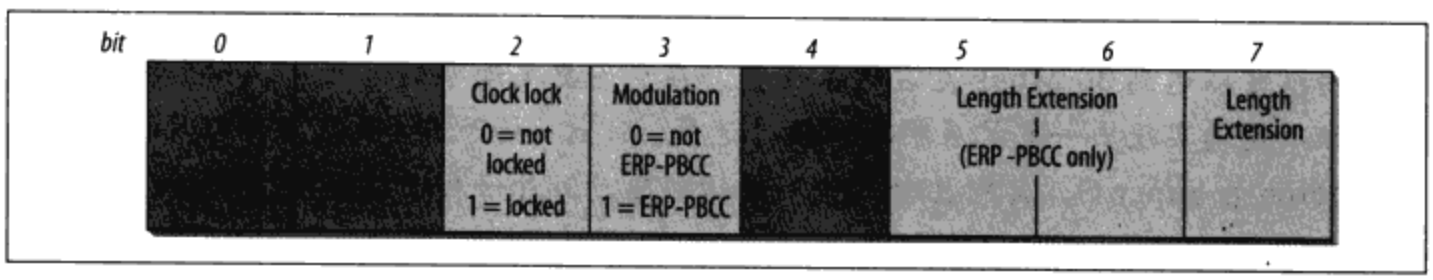


图 14-5：802.11g 的 Service 字段

帧主体

PLCP 帧最后的组件是它的有效载荷，即 MAC 帧，以 PBCC 或 OFDM 进行调制。帧主体的调制细节将在后续几节加以探究。

PBCC 编码

要使用 PBCC 传送帧，帧数据必须先经过卷积编码。帧会被拆解成 2 位一组的元素，经过卷积编码，最后会输出 3 个位。每一组 3 位的块会通过 8PSK 映射到一个符号。接收器只是反转整个过程，将每个相移转换为 8 种符号之一。将符号转换为 3 位序列后，通过卷积编码移除冗余的位，然后还原出原始数据，如图 14-6 所示。

使用这种物理层编码要达到 22 Mbps 的数据率十分简单。符号时钟如同 802.11b 那样维持在 11 MHz，但是每个符号用来传递 2 个位。若要达到 33 Mbps 的数据率，帧的数据部分必须使用 16.5 MHz 的符号率。既然每个符号可以传递 2 个位，因此整体数据传输率即为 33 Mbps。切换时钟速度必须在 PLCP 前导码与其有效载荷之间的空隙内进行。

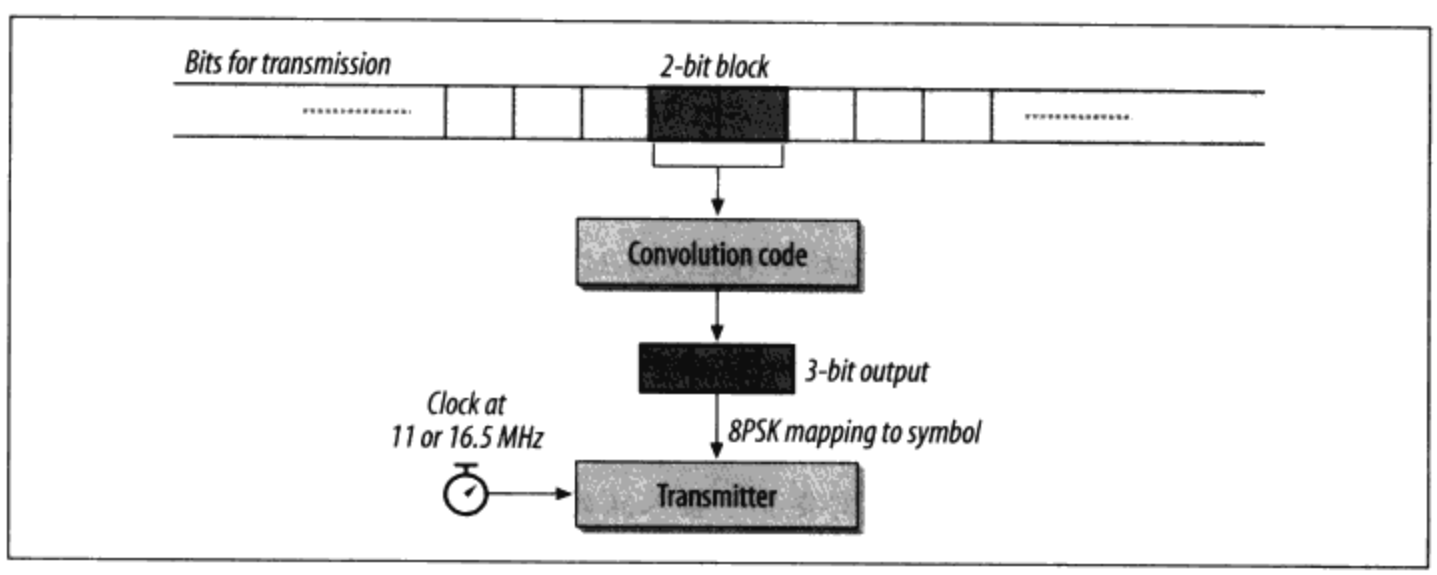


图 14-6：PBCC 处理过程

Atheros "Super G" 扩展功能

虽然过去几年速度已有显著的提升，但无线网络还是不够快。最佳情况下，标准无线网络可以达到30 Mbps左右的吞吐量。在竞逐更高速率的过程中，几乎所有芯片组厂商均实现出一些扩展功能来提升速度。目前，最著名（或恶名昭彰）的算是Atheros的Super G，其中包含三种不错的功能，另外一种功能则颇受争议。

块确认（block acknowledgment，无线也称为帧突发）

在标准的802.11无线链路管理机制中，每个数据帧都必须伴随一个确认信息，之后工作站必须重新竞争媒介的使用权。块确认（block acknowledgment）让工作站得以连续传送几个帧，帧间以短帧间间隔（SIFS）进行区隔，过程中无需竞争媒介使用权。此帧序列伴随一个块确认信息。只要是根据目前的802.11e草案进行开发，块确认通常不至于造成厂商间的互用性问题。

封包集群（packet clustering）

802.11帧可以承载多于标准1500个字节的Ethernet帧的数据。尽可能装满数据有助于改善有效载荷开销比（payload-to-overhead ratio）并且提高速度。

硬件数据压缩（hardware data compression）

传输之前先将数据压缩可以缩短传输时间并且有效提升链路的吞吐量。存在冗余数据（例如未经压缩的文字）时硬件压缩最有效率。传送已压缩的图像时效果就没那么显著了。

信道捆绑（channel bounding，也称为"Turbo模式"）

除了使用22MHz的单一信道，也可以通过信道捆绑（channel bounding）功能使带宽加倍。信号展开时若增加可用频谱，就可以在较宽的信道中塞进更多的位。为了确保使用较大带宽时仍然符合管制规定的限制，有些产品限定只能在第6信道，即中央频带进行信道的合并。

目前，信道合并可说是Super G最具争议的功能。在2003年底，Broadcom指控Super G会干扰其他正常的802.11g传输并在Comdex举办了一场私人展示会（我被拒绝入场）。后续测试显示干扰的确存在，不过发现Broadcom芯片组比其他厂商更容易受到影响。Atheros已经开发出一种监听模式，附近如有其他以802.11g标准进行传输的网络，则停止使用信道合并的功能。

足以为鉴的是，消耗更多稀有频谱的同时，信道合并的功能就更容易造成干扰。容易消耗频谱的传输模式不适用于需要多个接入点的大范围区域，因为原本已经少得可怜的可用信道将由三个缩减为一个。信道合并设备在家中使用无妨，但不要部署在公司网络中。

DSSS-OFDM 成帧

DSSS-OFDM 是一种混合型的成帧技术。较上层封包以 OFDM 编码，经 OFDM 调制的封包则是以传统的单载波标头封装，如图 14-7 所示。标头依 802.11b 标准进行传输（包含 802.11b 所使用的数据扰频器），帧主体则是通过 OFDM 加以调制，如第十三章所提到的 802.11 编码过程。虽然编码方式类似 802.11a，不过 DSSS-OFDM 成帧移除了一开始的短训练序列。此外，它新增了一个 6 微秒的信号扩展字段，以便有充足的时间完成卷积解码过程。PLCP 标头结束后必须从直接序列调制转换为 OFDM，从无线电工程的角度来看颇为复杂，不过这已经超出本书的范围。

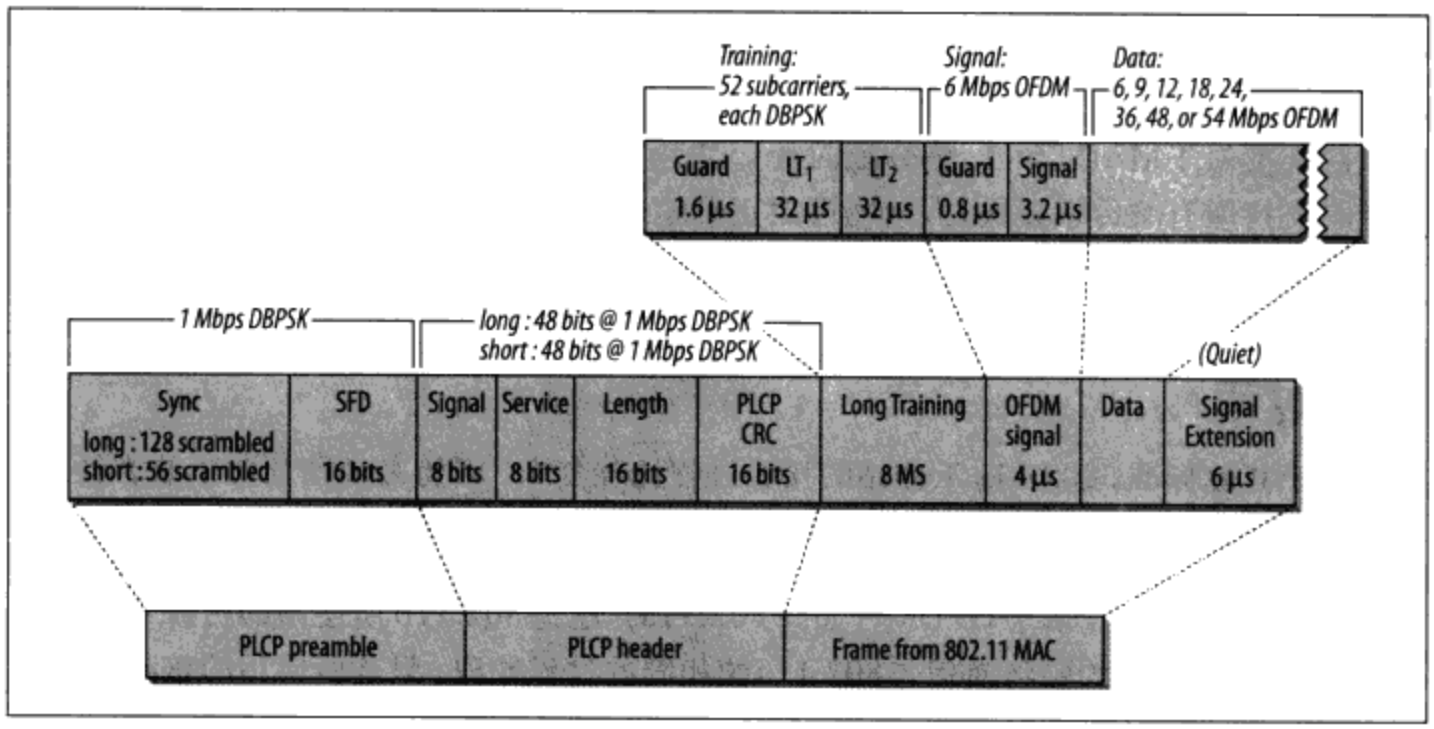


图 14-7：DSSS-OFDM 帧格式

ERP 的物理媒介相关（PMD）

一旦 PLCP 帧准备就绪，便会通过 PMD（物理媒介相关）加以发送。PMD 负责取得数据并经由天线传送。由于可使用的调制机制种类颇多，802.11g 收发器必须实现好几种不同的传输模式（不论完整与否）并在必要时进行切换。不过，有些功能是收发器共享的，与操作模式无关。

空闲信道评估（CCA）

802.11g 只定义了一种 CCA 模式，除了检测能量的最低阈值，也用来解读信号。在传输时隙（transmission slot）开始时，若接收到功率高于 −76 dBm 的信号，则视为有效信

号。在性能要求方面，在特定时间内，物理层正确汇报媒介处于忙碌状态的几率必须大于某个数值。所需要的时间间隔与几率如表 14-2 所示。

表14-2：802.11g的CCA性能需求

	长时隙（20 μs）	短时隙（9 μs）
CCA 时间	15 μs	4μs
检测几率	>99%	>90%

CCA 与PLCP级的虚拟载波监听（virtual carrier sense）机制整合在一起。接收到PLCP标头时，其中会包含 length 字段，显示媒介将忙碌多长时间。这段时间内，物理层将持续汇报媒介处于忙碌状态，就算物理层信号已经漏失（不论是在概念上还是操作上，这种做法都类似于MAC层的网络分配向量）。之所以采取这种做法，部分是因为并非所有实现均支持所有的传输模式，因此物理层正确地避免干扰其所无法解调的传输就相当重要了。

接收过程

相比较于其他标准，802.11g工作站的接收过程比较复杂，因为必须顾及向下兼容性。接收帧时，802.11g 工作站必须使用正确的物理层加以检测与解调。

1. 帧的前导码究竟属于 OFDM（如同 802.11a）还是 802.11b 所使用的传统单载波？以OFDM调制的帧将使用与802.11a帧相同的过程处理，只是所使用的接收频率不同。
2. 如果不是 OFDM 帧，则必须对前导码进行解码，然后在前导码的结尾找出 PLCP Signal 与 Service 字段。
3. PLCP 标头经过解码后，便可以采用适当的调制方式对帧主体进行解调。
   a. 如果 Service 字段显示此帧是以 PBCC 调制的，便会触发 PBCC 接收过程。
   b. 如果Service字段并未显示任何使用PBCC的迹象，便会进一步查看数据率。若数据率为 1 Mbps 与 2 Mbps，则以 DSSS 接收算法进行处理；若数据率为 5.5 Mbps与11 Mbps，则以CCK接收算法进行处理，两者在第十二章均已说明过。
   c. 如果 Signal 字段显示数据率为 3 Mbps，则使用 DSSS-OFDM 接收过程。PLCP 标头结束后即切换为 OFDM 解调器。

ERP 物理层的特性

802.11g 与 802.11a的特性十分相似，只有一项比较值得注意的例外。虽然 802.11g 的信道性能与 802.11a 相当，但只有三个信道可用。就算每个信道以最高速率运行并且达到 50% 的效率，整体吞吐量也只有 81 Mbps。虽然这个数字不差，但仍然无法和 802.11a 相提并论。

表14-3：ERP物理层参数

参数	值	备注
最大 MAC 帧长度	4095 个字节	
时隙时间	20 μs 9 μs	如果网络上只有 802.11g 工作站，便可以缩短时隙时间，从兼容于 802.11b 的 20 μs，缩短为 802.11a 所使用的 9 μs
SIFS 时间	10 μs	SIFS 可用来推衍出其他帧间间隔值（DIFS、PIFS 以及 EIFS）
信号扩展时间	6 μs	每个 802.11g 封包均伴随此信号扩展时间
竞争窗口的大小	15 或 31 至 1023 个时隙	如果工作站只支持 802.11b，为了兼容必须使用 31 个时隙；否则可以使用较短的竞争窗口
前导码持续时间	20 μs	

第十五章

802.11n 前瞻：MRMO-OFDM

802.11任务组N（TGn）的目标很有意思。大部分IEEE任务组的焦点是提升最高吞吐量，让数据能够尽快传输。TGn的目标是在扣除协议管理功能（例如前导码、帧间间隔以及确认信息）所造成的负担后达到100 Mbps的净吞吐量。尽管目标是100 Mbps的净吞吐量，最终提案似乎不难超越原先设定的数字，最佳情况下甚至能够提供好几倍的吞吐量。要达到100 Mbps有两种方式：改善MAC的性能以及将最高吞吐量拉到100 Mbps以上——或两者并行。

TGn任务组总共收到6份完整的提案，不过焦点在其中2份，分别由TGnSync与WWiSE（"World-Wide Spectrum Efficiency"的简称）阵营提出。双方阵营均包括芯片制造商。Atheros、Agere、Marvell与Intel属于TGnSync阵营；Airgo、Broadcom、Conexant与Texas Instruments则是WWiSE的核心厂商。此外，不少用到802.11的电子设备制造商（Cisco、Nokia、Nortel、Philips、Samsung、Sanyo、Sony与Toshiba）也参与规范的制定，但大多倾向TGnSync阵营。

就高层次来看，这两份提案十分类似，尽管强调的重点不同。其中一方强调最高数据率的提升，另外一方则是侧重MAC性能的改善。在许多配置上，两者均采用多进/多出（multiple-input/multiple-output，简称MIMO）技术，并且向下兼容于同频带的旧系统。操作上，两者均支持当前的20 MHz信道，另外渴望使用2倍宽的40 MHz信道来提升吞吐量。

标准之争才在全球的IEEE会议开打，市面上就已经出现所谓的"pre-N"接入点，内部采用Airgo的芯片组。在标准出炉之前购买这类产品，有点像是在赌运气。当初"pre-G"产品问世时，任务组虽然才刚起步，至少只需要与一份提案奋战。目前，TGn还处

于“双份提案”(dueling proposal)的阶段，根本无法保证未来是否能以固件升级的方式更新为最后的802.11n标准。802.11n可能是这10年内最后一份物理层标准。标准的开发既是技术工程，也是行政工程。IEEE要求提案在成为标准的基础之前必须得到75%以上的支持率。本书即将付印时，虽然TGnSync得到大多数厂商的支持，但仍低于必要的75%。预计对立阵营所提出的功能将被整合到未来的提案中，好让支持率提升到必要水平。因此，本章将针对这两份提案的内容提出说明。虽然TGnSync或许将成为802.11n规范说明书的基础，但终究还是会纳入许多WWiSE的功能。

本章会同时描述WWiSE与TgnSync这两份提案。最后的标准将与之类似并将从中挑选出必要的功能。幸运的是，两者所用到的一些基本概念是共通的。当各位阅读至此，切记本章所依据的提案草案尚有可能历经一番变动。

共同功能

虽然这两份提案有所差异，但两者间其实具备不少共同点。实际上，为了达到100 Mbps的吞吐量，有些功能是不可或缺的。

多进/多出（MIMO）

2004年之前，802.11接口仅使用单一天线。虽然有些接口使用两支天线作为天线分集，不过天线分集只是选用信号最好的天线。就天线分集而言，任一时间点都只用到单一天线。就算配置两组以上的天线，也只用到其中一组组件来处理信号或射频链路（*RF chain*）。接收器只有一组输入链路（input chain），发射器也只有一组输出链路（output chain）。

为了进一步超越天线分集，必须将射频链路分配给系统天线。这就是多进/多出（MIMO（注1））操作的基础。任一射频链路均能同时接收或发送，如此可以大幅提高吞吐量。此外，接收器平行处理的好处在于能够解决多径干扰的问题，也可以改善接收信号的质量，远胜过单纯的天线分集。个别射频链路及相应的天线负责传送空间流（*spatial stream*）。单一帧可以被拆解，经过多任务处理后以多组空间流传送，接收器再加以重组。WWiSE与TGnSync提案均采用MIMO技术来提高数据率，虽然两者的应用方式不同。

MIMO的天线配置通常表示成“YxZ”，其中Y与Z均为整数，分别代表传输天线与接收天线的数量。举例而言，WWiSE与TGnSync均将2x2操作列为必要，即使用两组传

注1：MIMO念成“MyMoe”。我曾经参加一场研讨会，一位委员提到，标准委员会曾就“MIMO”的念法进行表决。

输链路、两组接收链路以及两道经过多任务处理的以无线链路传送的空间流。这两份提案中还包含其他必要（required）与可选（optional）模式。预计两者将采用相同的硬件配置在客户端使用两组RF链路以节省电池电力，而在接入点使用三组以上的RF链路。这种配置将使用2x3 MIMO作为上行链路（uplink），以3x2 MIMO作为下行链路（downlink）。

带宽

802.11a目前使用20 MHz信道，因为这是所有管制单位一致允许的带宽。理论上，将带宽倍增为40 MHz，信道的通信量也会因此倍增。虽然渴望在未来开放，但一些管理者目前并不允许40 MHz的操作，日本是最明显的例子。

MAC性能的提升

本书再三强调802.11 MAC性能一向很差。大多数情况下，它很难达到物理层额定位率（nominal bit rate）的50~60%以上。每个待传帧都需要用到物理层帧头以及只会造成负担的前导码。802.11 MAC要求每个帧都需要得到确认，这也是额外的负担。对小型帧而言这些负担更是沉重，因为它们可能比帧数据本身用掉更多的传输时间。MAC的性能定义为各种长度的帧中MAC有效载荷数据（payload data）占额定位率的比例，如图15-1所示。图中所标示的数值代表MAC有效载荷数据。任何网络测量都必须加计额外的LLC数据，经加密的网络也会有额外的负担。此外，大多数网络协议都会提供本身的确认机制，这进一步拖累了实际的性能。图15-1的重点在于：帧越小，性能越差。

TGnSync与WWiSE采用了一些技术来改善无线电信道的性能。虽然概念相似，但是细节不同。两者均采用某种形式的块确认（有时也称为帧突发）。如果不需要个别确认，就可以减少ACK帧、前导码与成帧所造成的负担。块确认虽然有用，但在帧突发期间不能有任何闪失。只要漏掉任何帧或确认信息就会严重影响协议的操作，整个块必须予以重传。

帧聚合（frame aggregation）也同时见于这两份提案。802.11所承载的封包有时很小。交互式网络连接（例如telnet或SSH）的封包通常很小，但需要立即传送。封包较小，帧也就跟着变小。每个小型帧都需要物理层成帧，因此造成额外的负担。将一些小型封包组合成较大的单一帧有助于改善数据开销比（data-to-overhead ratio）。帧聚合通常会搭配MAC标头压缩，因为目的地的相同帧会有相当类似的MAC标头。

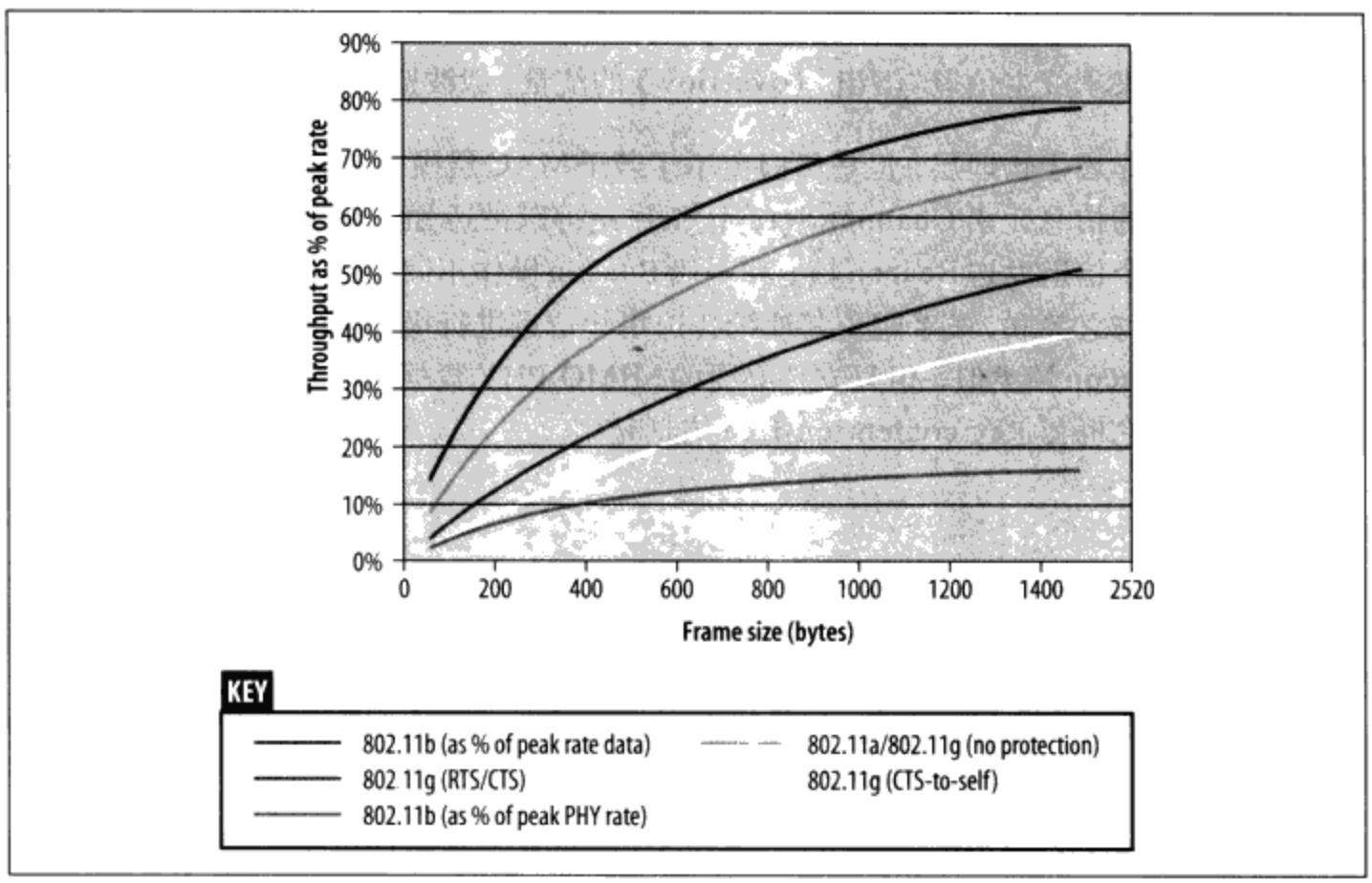


图 15-1：MAC 的性能

WWiSE

WWiSE 联盟的参与者包含了若干著名的芯片制造商：Airgo（首部“pre-N”设备制造商）、Broadcom、Conexant 以及 Texas Instruments。Motorola 于 2005 年 2 月加入此阵营，刚好在本书付印之前。

MAC 的改良

从名称上标榜“频谱效率”（spectral efficiency）即可预料 WWiSE 比较侧重 MAC 性能的改善。为了达到 100 Mbps 的净吞吐量，必须在 960 微秒的时间内传送 12000 个字节（960000 位）。使用两组天线搭配两道数据流的基本配置，WWiSE 的物理层规范可以有 135 Mbps 的数据率，在 711 微秒之内传送所有数据。其余的 249 微秒则是用于前导码、成帧、帧间间隔以及单一块确认。

信道与无线电模式

WWiSE 同时使用 20 MHz 与 40 MHz 两种信道。40 MHz 操作可以使用单一 40 MHz 信道或者一对同时用来发送数据的 20 MHz 信道。其中一个信道作为主信道，使用正常的

操作方式。第二个信道只用于信道聚合(channel aggregation)，不会让工作站与之关联。第二个信道用来承载主信道“溢出”(overflow)的流量。载波监听功能只在主信道进行。

虽然双信道操作属于物理层，但是仍旧免不了若干MAC层操作。主信道的Beacon帧中会加入一个新的信息元素Channel Set，让工作站得以被通知第二个信道的存在。接入点也会在第二个信道发送Beacon帧。和一般Beacon操作不同的是，这么做的目的是为了避免工作站与之关联，或者避免其他设备选用此信道进行操作。第二信道的Beacon帧与主信道的Beacon帧类似，但只支持必要的MIMO PHY数据率。为了进一步避免他人使用此信道，它也会包含contention-free信息元素。

保护机制

如同802.11g，这些新式物理层必须改良现有的保护机制，才能避免干扰现有的工作站。当然，使用2.4 GHz的工作站必须实行802.11g所规范的保护机制，方能避免干扰其他较旧的直接序列或802.11b设备。如果接入点检测到旧式设备，就会启动第十四章所描述的RTS-CTS或CTS-to-self保护机制。

不过，为避免MIMO工作站以802.11a或802.11g设备无法理解的速率进行传输，必须设计一些额外的保护机制。WWiSE提案提出一种OFDM保护机制，允许MIMO工作站以适当的方式设定旧式OFDM工作站的NAV。它相当于第十四章所描述的保护机制，但使用OFDM数据率。

最后，WWiSE提案使用Beacon帧中ERP信息元素里的两个位来指示是否需要用到OFDM保护机制。在某些情况下，可能需要用到OFDM保护机制来协助802.11g网络，但无需提供802.11b工作站保护机制。接入点会监控无线链路以判断是否需要OFDM保护机制。为了协助使用成对信道的工作站，它们也会指示是否使用第二个信道。

帧聚合、帧突发与确认

WWiSE提案把有效载荷数据的最大长度从2304个字节提高到8000个字节以上。有效载荷数据变多相当于提升有效载荷开销比，因此可以提升整体性能，如果较大的帧或帧突发能够顺利传送的话。

帧聚合是将几个较上层网络协议的封包捆绑在单一帧中。每个封包均包含一个带有来源与目的地地址的子帧头以及指定封包大小的长度字段，如图15-2所示。除非所要捆绑的各帧的Address 1（帧的接收端）字段值相同，否则无法聚合帧。在基础结构型网络里，来自接入点的帧的Address 1字段代表目的地，因此接入点只能聚合传给单一工作站的帧。不过，基础结构型网络里的工作站可以聚合传至不同目的地的帧。工作站会在Address 1字段填入接入点地址，因为传递至骨干网络之前，所有帧都必须经过接入点

的处理。聚合帧时，目的地地址是“下一跳”（next hop）处理工作站，源地址则是帧的产生者。拆解帧时，各个子帧（subframe）将根据各自的帧头进行处理。由于接收端地址必须相同，因此无法同时聚合单播、组播与广播数据。提案中并未规范何时该聚合帧。

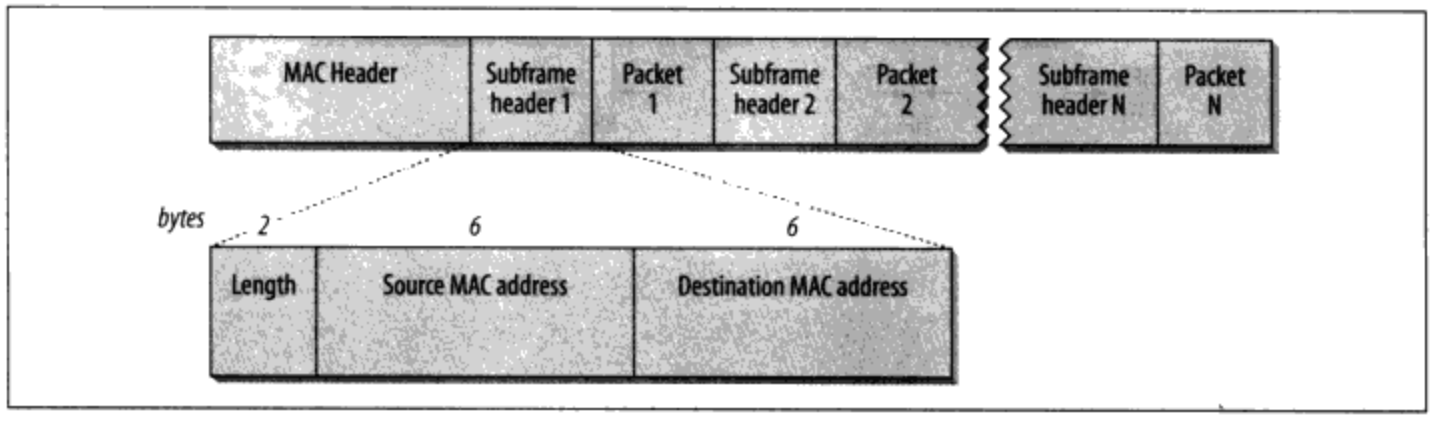


图 15-2：WWiSE 的帧聚合

帧突发（bursting）是与帧聚合相关但稍有不同的概念。帧聚合汇集了较上层协议的封包，以较大的数据量进行传输。帧突发在物理层采取同样的做法。一旦工作站付出相当的代价取得了信道的控制权，就可以持续进行传输。相对于较上层的帧，使用多个物理层帧的优点在于能够指定各个帧的来源与目的地地址。帧突发可以包含传送到不同目的地地址的传输操作。帧突发另外定义了两种帧间间隔，称为零帧间间隔（Zero Interframe Space，简称ZIFS）与缩短型帧间间隔（Reduced Interframe Space，简称RIFS）。传输功率相同的连续帧，可以用ZIFS立即传送；如果帧的传输功率有所变动，则使用RIFS。然而RIFS短于其他帧间间隔，这让工作站得以持续掌控信道。图 15-3 中，第一个帧无法被聚合，必须等到传送者掌控信道后方能传送。一旦取得控制权，它就可以在允许的时限内持续掌控信道。第二与第三个帧使用相同的传输功率，因此在ZIFS后进行传送。此外，它们的Address 1字段值相同，因此被捆绑到同一个聚合帧。要传送下一个帧，必须调整所使用的传输功率，因此得使用RIFS。第四与第五个帧可以聚合，作为单一聚合帧传送。等到队列中的数据传送完毕，工作站随即释放信道的控制权。

802.11 MAC 的最初版本规定，每个单播数据帧必须得到一个肯定确认信息（positive acknowledgment）。WWiSE 移除了此项限制，允许使用较灵活的确认策略。除了“标准的”策略，帧的传送可以不用得到确认或者使用块确认来代替。

WWiSE MIMO 物理层

WWiSE 提案是从802.11a演变而来，使用MIMO技术。基本的信道访问机制维持不变，OFDM编码方式亦然。从高层次来看，WWiSE PHY 主要是用来为各个位指定不同的天线。

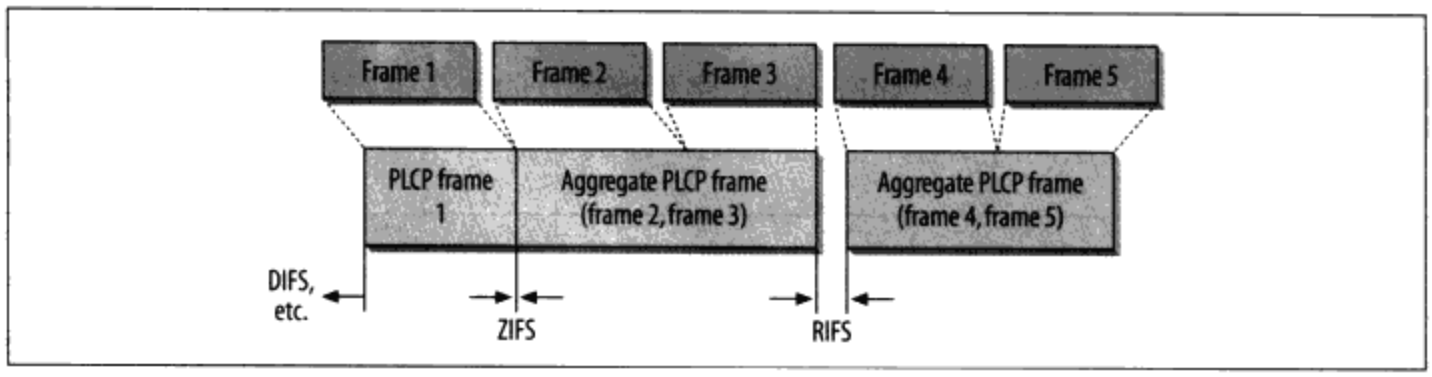


图 15-3：WWiSE 的帧突发

操作信道的结构

如同802.11a，无线电信道的划分是以0.3125 MHz为副载波间隔。和802.11a的信道分割一样，在WWiSE提案中，20 MHz信道被划分为56个副载波，40 MHz信道则被划分为112个副载波。40 MHz信道并非必要（optional），也只能用于5 GHz频带，因为ISM频带根本挤不出几个40 MHz信道（如果各位认为以3个信道进行网络规划已经很难，不妨试试看2个信道的情况）。图15-4显示了WWiSE提案中所规范的20 MHz与40 MHz操作信道。

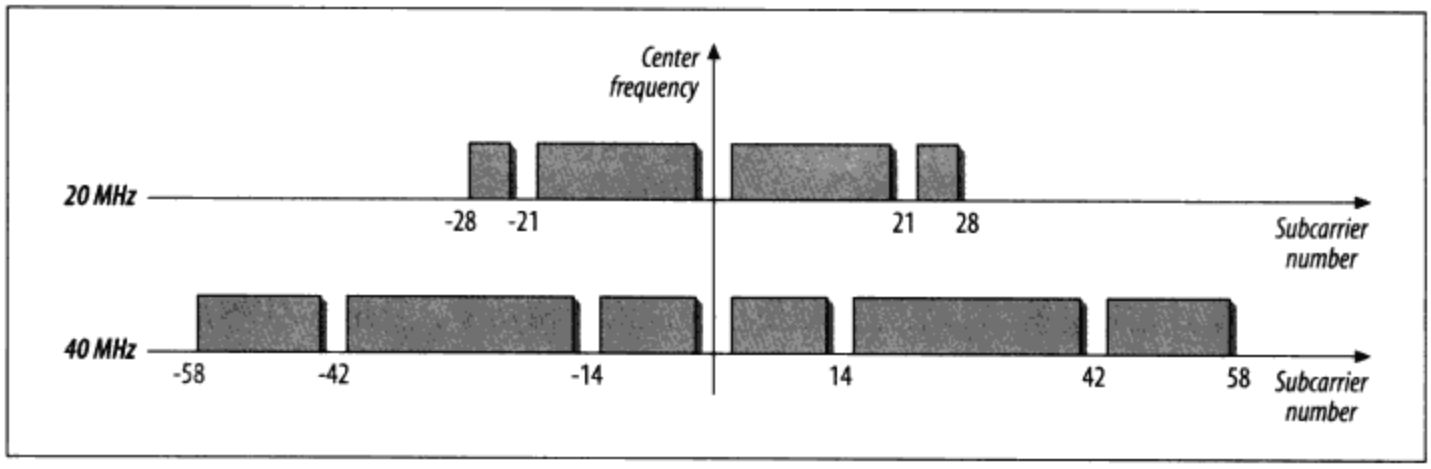


图 15-4：WWiSE 的导频结构

如同802.11a，其中有几个副载波（subcarrier）会被设为导频（pilot carrier），用来监控无线链路的性能。MIMO系统用到较少的导频，因为导频涵盖好几个接收链路。20 MHz的802.11a信道使用了4个导频。在WWiSE提案中，20 MHz的信道只需要2个导频，因为每个导频是由2个接收链路处理，效果相当于以单一接收链路处理4个导频。由于导频数较少，多出来的副载波就可以用来传递数据。20 MHz的WWiSE信道有54个数据副载波；40 MHz信道则有108个，刚好是前者的2倍。

调制与编码

WWiSE 提案并未规范新的调制速率。它广泛使用 16-QAM（4 位）与 64-QAM（6 位）调制技术，但不需要十分精确的调制星座图（modulation constellation）。

至于编码方面则有所改良。WWiSE 新增 5/6 的卷积编码率。如同 802.11a 所定义的 2/3 与 3/4 编码率，5/6 编码是从输出收缩（puncture）得来的较高编码率定义而来。WwiSE 还定义了低密度奇偶校验（low density parity check，简称 LDPC）码的用法。

交错器

在 802.11a中，交错器（interleaver）负责为各位指定其所使用的副载波。MIMO 交错器比较复杂，因为除了指定位在信道本身的位置，还需指定位所使用的空间流。WWiSE 交错器从前向错误编码器（forward error coder）取得传送位，然后轮流分配给每个空间流。第一位指派给第一个空间流，第二个位指派给第二个空间流，依此类推。交错器也负责每个空间流中编码位的扰频事宜。

空时分组编码

通常，每道空间流由一组天线来传递。不过有时候天线数可能远多于空间流数。举例来说，如果接入点使用 3 组天线，而工作站使用 2 组天线，就会出现所谓的“额外”传输天线，即两道空间数据流必须指派给 3 组天线。通过多组天线来传送单一空间流称为空时分组编码（space-time block coding，简称 STBC）。

将一道空间流划分给几组天线的基本规则，就是以不同天线传送两道相关流。如第十三章对 802.11a 所做的说明，无线电波是由同相（in-phase）与正交（quadrature）两种信号组成，正交信号落后同相信号 1/4 周期。在数学上，其相移表现为星座图中复数的虚数部分。两个复数共轭指的是它们的实数部分相同，但虚数部分的正负号相反。实际上，由共轭复数所形成的无线电波具备相同的同相信号，不过正交信号的相移刚好相反。如果有多余的天线，WWiSE提案要求必须使用同一对天线来传送空间流及其共轭复数。使用规则如表 15-1 所示。分割空间流的规则与带宽无关，但 40 MHz 的空间流显然能够承载更多位的数据。

表 15-1：天线数大于空间流数时WWiSE 所采用的编码规则

传输天线	空间流	第一道空间流	第二道空间流	第三道空间流
2	1	跨天线 1 与 2 编码	N/A	N/A
3	2	跨天线 1 与 2 编码	在第三组天线上正常传送	N/A
4	2	跨天线 1 与 2 编码	跨天线 3 与 4 编码	N/A
4	3	跨天线 1 与 2 编码	第三组天线	第四组天线

调制速率

WWiSE PHY 定义了 24 种数据率以及 49 种不同的调制选项。为了节省空间，此处只列出数据（传输）率的基本公式，不再列出表格：

数据率（Mbps）= 0.675 × channel bandwidth × number of spatial streams × coded bits per subcarrier × code rate

channel bandwidth（信道带宽）

20 MHz 信道的带宽为 20，40 MHz 信道或成对信道的带宽为 40。

number of spatial streams（空间流数）

空间流数可以是 1、2、3 或 4。它必须小于或等于传输天线数。提案规定，必须至少支持两道空间流。

coded bits per subcarrier（每个副载波的编码位数）

大多数情况下，64-QAM 为 6 位而 16-QAM 为 4 位。BPSK（每个副载波编码 1 位）与 QPSK（每个副载波编码 2 位）只能用于 20 MHz 且只有一道空间流的信道。

code rate（编码率）

16-QAM 可以搭配 1/2 或 3/4 的编码率，64-QAM 可以搭配 2/3、3/4 或 5/6 的编码率。

要达到相同的数据率，有几种不同的方式。例如，有 4 种方式可以达到 108 Mbps：

- 使用 4 道 20 MHz 的空间流，以 16-QAM 搭配 1/2 的编码率（R=1/2）。
- 使用 2 道 20 MHz 的空间流，以 64-QAM 搭配 2/3 的编码率（R=2/3）。
- 使用 1 道 40 MHz 的空间流，以 64-QAM 搭配 2/3 的编码率（R=2/3）。
- 使用 2 道 40 MHz 的空间流，以 16-QAM 搭配 1/2 的编码率（R=1/2）。

在使用单一空间流的基本模式中，信道的通信量（capacity）稍高于802.11a，因为所使用的导频数量较少。单一信道调制最高可达 60.75 Mbps，而非 802.11a的 54 Mbps。如果将所有参数调至极限（4道40 MHz的空间流，以64-QAM搭配5/6的编码率），WWiSE 提案的吞吐量最高可达 540 Mbps。

MIMO 与传输模式

之前的 802.11 物理层规范使用相当简单的传输模式。WWiSE 提案提出了 14 种传输模式，使用哪一种取决于三项因素：

- 传输天线数，以 xTX 表示，其中 x 代表传输天线数。其范围从 1 至 4，不过单一天

线只能用于40 MHz信道。所有20 MHz的信道必须至少使用2组天线，但可以只使用一道空间流。

- 将帧用于Greenfield（简称GF）模式或mixed mode（混合模式，简称MM）的环境。混合模式使用向下兼容于其他OFDM PHY的物理层标头，GF模式则是使用速度较快的物理层标头。
- 信道的宽度，可以是20 MHz或40 MHz。

表15-2列出了所有14种传输模式。每一种模式各自定义了几种不同的物理层编码方式，将于PLCP相关章节探讨。有源天线（active antenna）数与空间流数只有粗浅的关联。以4TX40MM模式进行操作的系统有4支天线，但可以仅使用2道或3道空间流。

表15-2：WWiSE的传输模式

	20 MHz 信道	40 MHz 信道
Greenfield 模式	2TX20GF	1TX40GF
	3TX20GF	2TX40GF
	4TX20GF	3TX40GF
		4TX40GF
混合模式	2TX20MM	1TX40MM
	3TX20MM	2TX40MM
	4TX20MM	3TX40MM
		4TX40MM

WWiSE PLCP

PLCP必须能够操作于两种模式。操作于Greenfield模式时，PLCP不会使用向下兼容的物理层标头。Greenfield的访问比较简单：它可以不用向下兼容。图15-5显示了1TX40GF、2TX20GF与2TX40GF所使用的PLCP封装格式。

帧中各个字段的名称与用法类似于本书其他章节所提到的其他PLCP帧。

MIMO-OFDM PLCP Preamble 字段

此字段包含已知的位序列，协助接收器锁定信号。Preamble可能划分为几个部分，取决于采用何种传输模式。它通常同时包含长短两种训练序列（training sequence）。在WWiSE提案中，所有天线均会传送相同的前导码，但有稍微的时间差。在图15-5中可以看到双天线传输模式所使用的训练序列。虽然训练序列包含不同位，但时间差是一样的。当然，单天线40 MHz模式仅会使用一组有源天线来传送一组前导码。

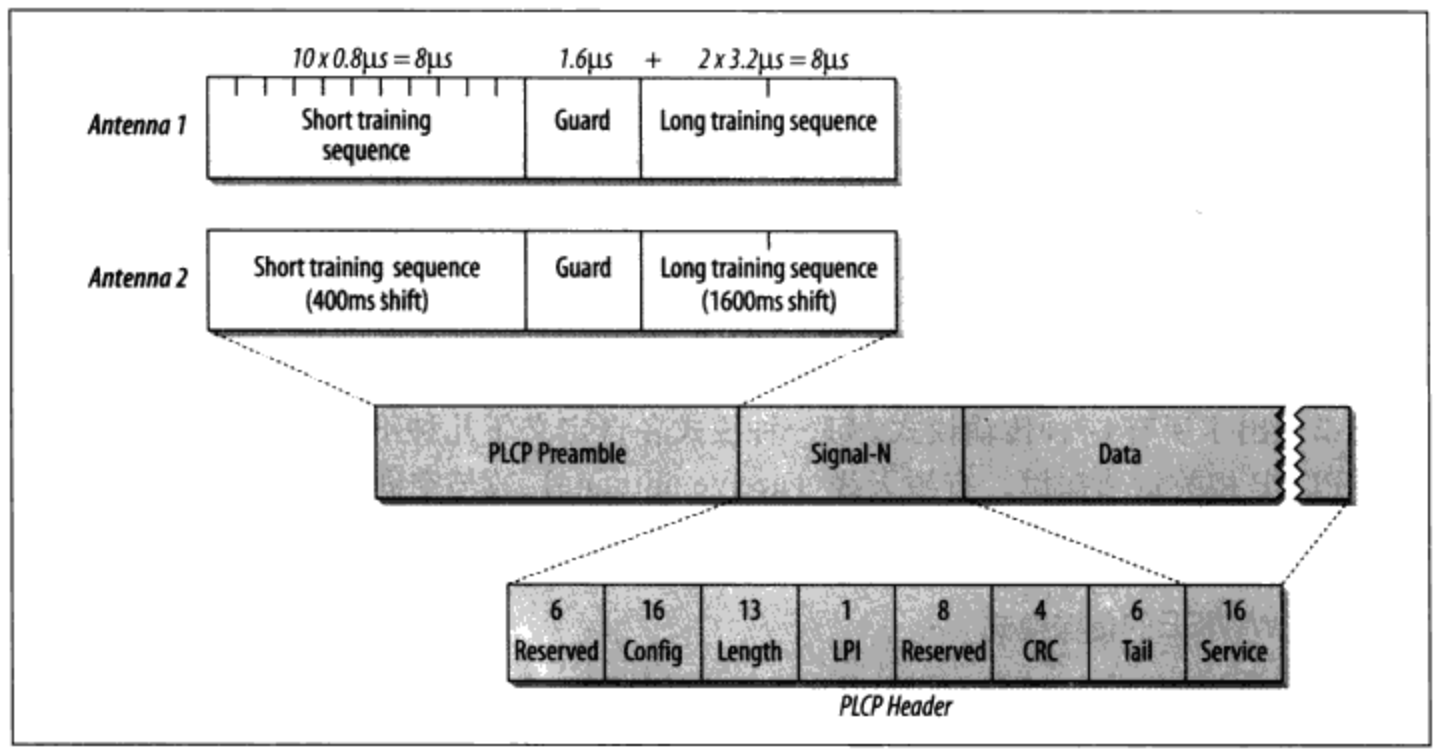


图 15-5：Greenfield ITX40 与 2TX20/2TX40 模式

Signal-N 字段

Signal-N 字段中包含解读数据流时所需要的信息。它通常以 QPSK、R=1/2 的编码率进行传送，而且未经扰频。其中包含空间流数、带宽、调制与编码的相关信息以及一个 CRC 码。稍后将更详细说明 Signal-N 字段的相关细节。

Service 字段

Service 字段与 802.11a 的用法相同。不同于 PLCP 标头的其他字段，它位于物理协议单元的 Data 字段中，以内嵌的 MAC 帧的数据率进行传送。前 8 位设定为 0。和其他物理层一样，传送 MAC 帧前会先经过扰频。前 6 位设定为 0，是为了初始化扰频器。其余 9 位目前保留未用，另有他用之前必须设定为 0。

Data 字段

最后一个字段是一系列历时 4 微秒的符号，用来承载数据。最后 6 个设定为 0 的结尾位，用来结束纠错码并以填充位（pad bit）使得符号块的长度值变为偶数。

Signal-N 字段

Signal-N 字段用于所有传输模式。其中包含从数据符号（data symbol）还原位流（bit stream）所需要的信息。Signal-N 字段如图 15-6 所示。

Config 子字段

Configuration 子字段由 6 个字段组成。

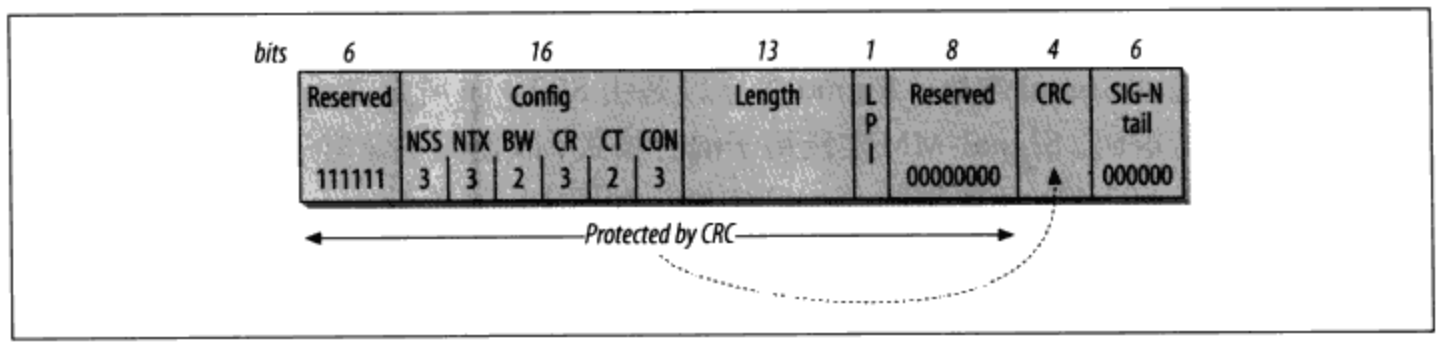


图 15-6：WWiSE Singal-N 字段

NSS（空间流数）

3 个位用来指示所使用的空间流数。此数值从 0 起算，因此范围从 0 至 3。

NTX（传输天线数）

3个位用来指示使用多少天线来承载空间流。此数值从0起算，因此范围从0至3。

BW（带宽）

2 个位用来指示所使用的带宽：20 MHz 以 0 表示，40MHz 以 1 表示。

CR（编码率）

3 个位用来指示所使用的编码率（code rate）：1/2 以 0 表示，2/3 以 1 表示，3/4 以 2 表示，而 5/6 以 3 表示。

CT（编码类型）

2个位用来指示所使用的编码类型（code type）：0代表卷积编码（convolutional code），1 代表非必要的 LDPC。

CON（星座图类型）

3 个位用来指示所使用的星座图类型（type of constellation）：0 代表 BPSK，1 代表 QPSK，2 代表 16-QAM，而 3 代表 64-QAM。

Length

长度为 13 位，用来记载物理层帧的有效载荷的数据位数。其范围从 0 至 8191。

LPI（最终 PSDU 指示）

在帧突发期间，最后一个帧会设定 LPI 位，告诉其他工作站此次突发已经结束。

CRC

除了 CRC 与 Tail 位，将根据其他所有字段计算出 CRC 值。

Tail

长度为 6 位的结尾位，用来关闭卷积编码器。

在其他传输模式中，preamble（前导码）会被分割成好几个块，如图 15-7 所示。在这些块之间有可能包含 Signal 字段。Signal-N 字段是由 802.11n 所定义，只有 802.11n 工作站才会对其进行解码。Signal-MM 字段用于混合模式，以便向下兼容于旧式的 OFDM 工作站。它等同于 802.11a 所使用的 Signal 字段，如图 13-16 所示。

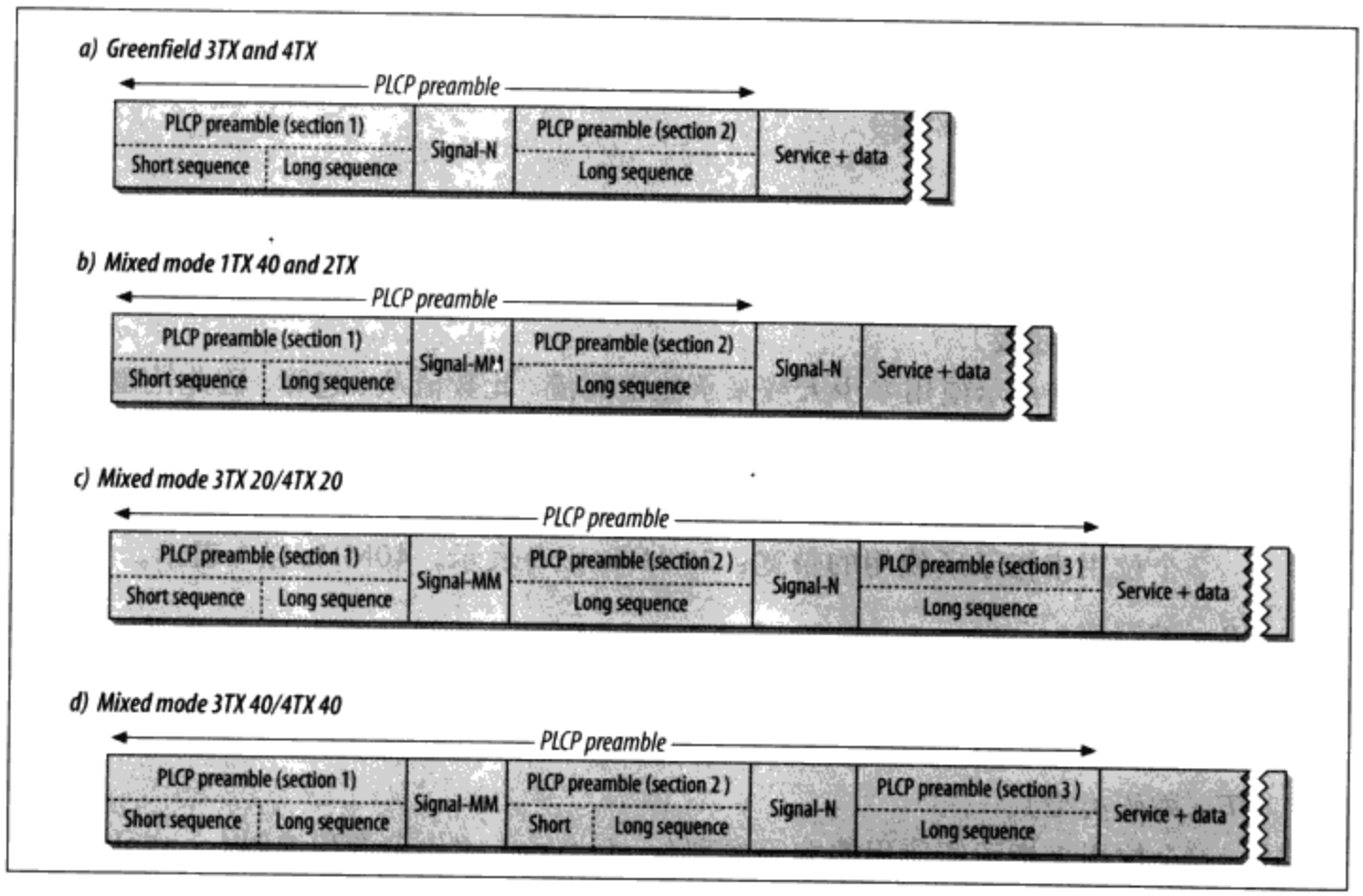


图 15-7：其他传输模式所使用的 PLCP 帧格式

WWiSE PMD

WWiSE 收发器的基本构造如图 15-8 所示。基本上，它和 802.11a 收发器没有两样，只不过具备多组传输链路（transmit chain）。交错器（interleaver）主要负责将已编码位分配给不同的传输链路以及空间流。

提案所规范的灵敏度等同于 802.11a 对接收器的要求。表 15-3 列出了所需要的灵敏度。至于邻道抑制，提案中并未加以规范。

表 15-3：WWiSE 接收器的灵敏度

星座图	编码率	灵敏度（dBm）	802.11a 的灵敏度（dBm），参考值
BPSK	1/2	−82	−82
BPSK	3/4	−81	−81

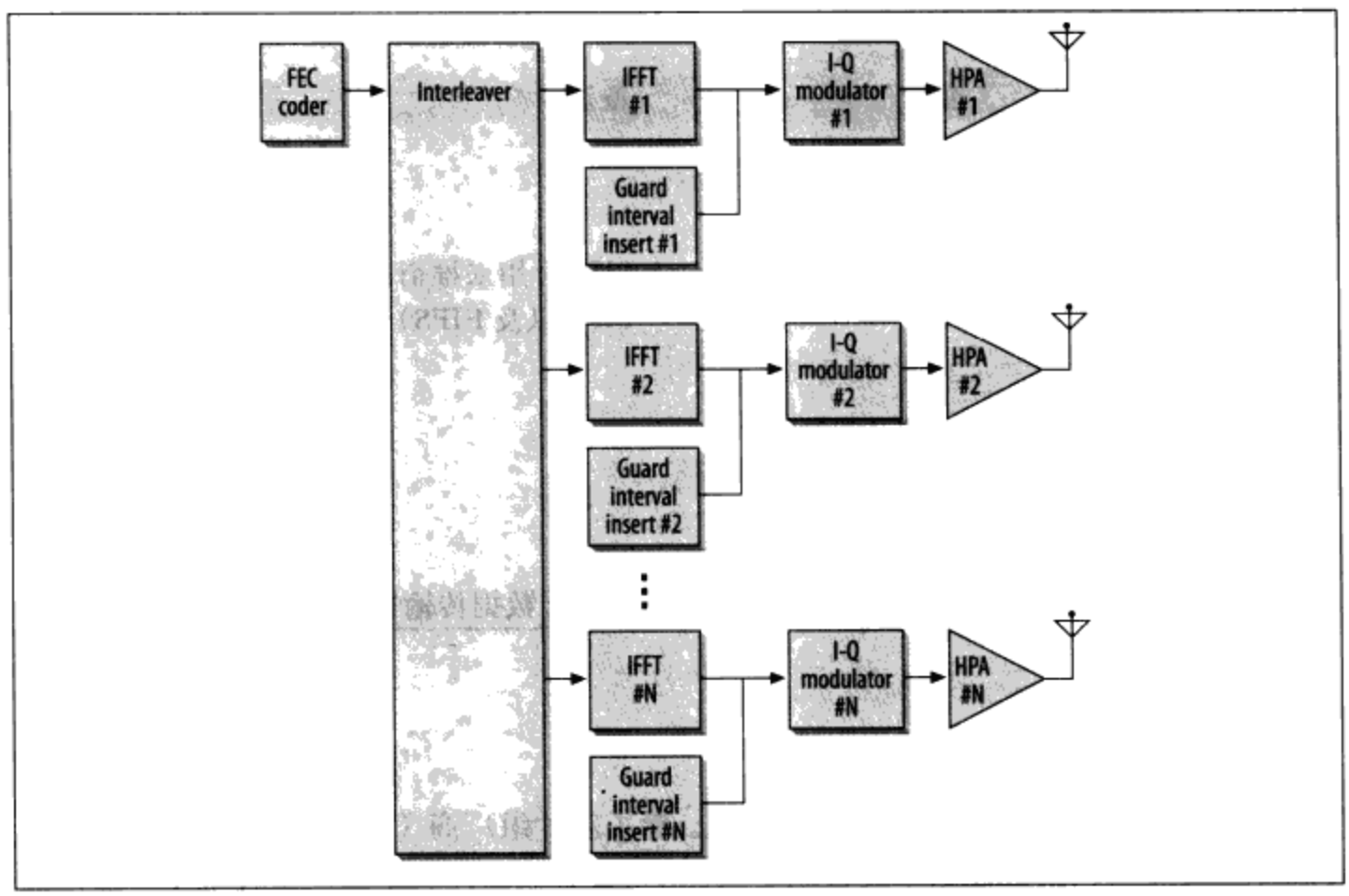


图 15-8：WWiSE 收发器

表 15-3：WWiSE 接收器的灵敏度（续）

星座图	编码率	灵敏度（dBm）	802.11a 的灵敏度（dBm），参考值
QPSK	1/2	−79	−79
QPSK	3/4	−77	−77
16-QAM	1/2	−74	−74
16-QAM	3/4	−70	−70
64-QAM	2/3	−66	−66
64-QAM	3/4	−65	−65
64-QAM	5/6	−64	N/A

WWiSE PHY 的特性

WWiSE PHY 特有的参数列于表 15-4。和其他物理层一样，WWiSE PHY 也包含了一些参数，可用来调整电子零件不同处理阶段所造成的延迟。

表15-4：WWiSE MIMO PHY参数

参数	值	备注
最大MAC帧长度	8191字节	
时隙时间	9 μs	
SIFS时间	16 μs	SIFS可用来推衍出其他帧间间隔值（DIFS、PIFS以及EIFS）
RIFS时间	2 μs	
竞争窗口的大小	15至1023个时隙	
前导码持续时间	16 μs	
PLCP标头持续时间	4 μs	
接收器灵敏度	−65至−82 dBm	取决于数据传输速度

TGnSync

TGnSync联盟是由各式各样的公司所组成。除了芯片组厂商（Atheros、Agere、Intel与Qualcomm），还包括其他电子设备制造商。网络设备制造商甚至是消费性电子产品厂商均列名其中。TGnSync的目标之一，就是支持能够自成网络的家用设备。宣传时提到如何通过无线网络来传送HDTV或DVD视频流，这或许可以说明为何此阵营将焦点放在如何提升最大数据率（peak date rate）上。

TGnSync MAC的改良

虽然TGnSync提案意在提供较高的最大数据率，但此阵营并未完全忽略MAC的改良。性能的改善主要是通过帧的聚合与突发机制以及确认策略的改变。旧式传输的保护机制有些是在MAC层进行。值得注意的是，有些改良是设计来节省电池电力，这点可以从此阵营的成员略窥一二。

信道、无线电模式与共存

TGnSync提案将对40 MHz信道的支持列为必要项目，虽然有些管理者并不允许。如果未来它获得采用，TGnSync芯片组将同时支持20 MHz与40 MHz信道，即使后者在某些管制区域并不允许使用。TGnSYnc提案还加入了若干MAC功能，让网络得以服务同时具备20 MHz与40 MHz能力的工作站。如工作站有大量数据待传，可以暂时协调使用较宽的信道，传送完毕后再恢复为20 MHz的操作方式。

MAC的操作模式也可以根据网络中的工作站类型加以分类。纯模式（*pure mode*）网络只包含802.11n工作站，因此没有必要为了旧式802.11a与802.11g工作站启用保护机制。此外，TGnSync 802.11设备可以运行于传统模式（*legacy mode*），如同802.11a或802.11g工作站。不过，大多数操作将采用混合模式（mixed mode），TGnSync网络必须与旧式网络共存（coexist）并使用相同信道，也可以接受旧式802.11a或802.11g工作站的关联。

不同模式对关联请求采取不同的处理方式。纯模式网络会完全忽略来自旧式工作站的关联请求，其所发送的Beacon帧带有一项信息元素，指示已关联工作站只能使用新的802.11n传输模式。纯模式网络使用TGnSync的高速PLCP来传送Beacon帧，因此旧式设备无法判读。旧式设备可以识别混合模式接入点，因为它们使用旧的格式来传送Beacon帧。

要与旧设备共存，必须使用混合模式（如果802.11g的部署经验有任何参考价值的话，大概可以推论出802.11n设备在大部分时间将以混合模式运作）。混合模式可以进一步细分为几种分支。自行混合（*mixed capable*）网络允许旧设备关联，但并未区分传统传输与高速传输的时间。管制混合（*managed mixed*）网络的接入点则会主动区分高速传输与传统传输的时间。有点类似无竞争周期与竞争周期的区别（参见第九章），操作于管制混合模式的接入点允许旧工作站拥有自己的传输时间，但使用类似保护机制的做法，在某些时段只允许MIMO工作站进行传输。

聚合与突发

原始的802.11工作站通常依接收顺序来传送帧。基于吞吐量的考虑，通常希望能够对帧加以排序，以便将它们塞进更大的聚合帧。在TGnSync中，聚合操作属于MAC层的功能，负责将数个MAC帧绑成单一PLCP帧进行传送。

图15-9所示为包含了数个MAC层帧的单一物理层帧的基本格式。数个MAC帧被塞到同一个PLCP帧中，并以适当的定界符（delimiter）作为区隔。此定界符包含了一个保留字段、一个记录后续MAC帧大小的length字段、一个用来保护定界符的CRC以及一个可用来协助将聚合帧还原成个别帧的独特样式（unique pattern）。置入聚合帧的MAC帧并未改动且包含完整的标头与MAC CRC。就算聚合帧中漏失了某个MAC帧，也可以成功地还原其余的帧。

除非信道经过设定，否则无法进行聚合帧的交换。整个交换过程如图15-10所示。聚合帧的发送端称为启始者（*initiator*），必须传送一个启始者聚合控制（Initiator Aggregation Control，简称IAC）帧。IAC帧的作用类似RTS帧，但包含额外的字段，用来协助控制信道。启始者可以要求进行信道测量、提供不同类型的编码方式以及接收

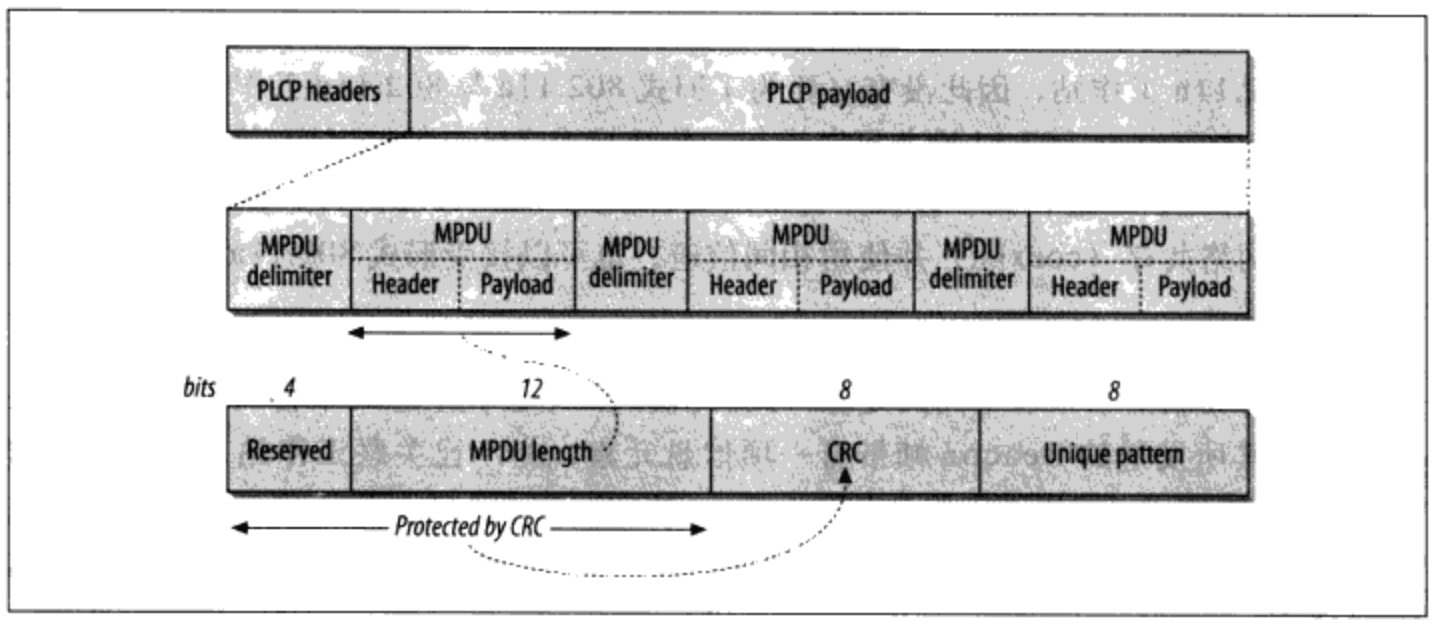


图 15-9：TGnSync 帧合并

聚合帧。一旦接收到IAC，称为响应者（*responder*）的目的端系统就会产生一个响应者聚合控制（Responder Aggregation Control，简称RAC）帧。RAC帧的作用类似CTS帧：除了告诉发送端已经接收到聚合帧，还得完成必要参数的协商。聚合帧必须伴随确认信息。TGnSync定义了一种新的确认信息，称为BlockACK（块确认），用来确认聚合帧中所包含的每个MAC帧。

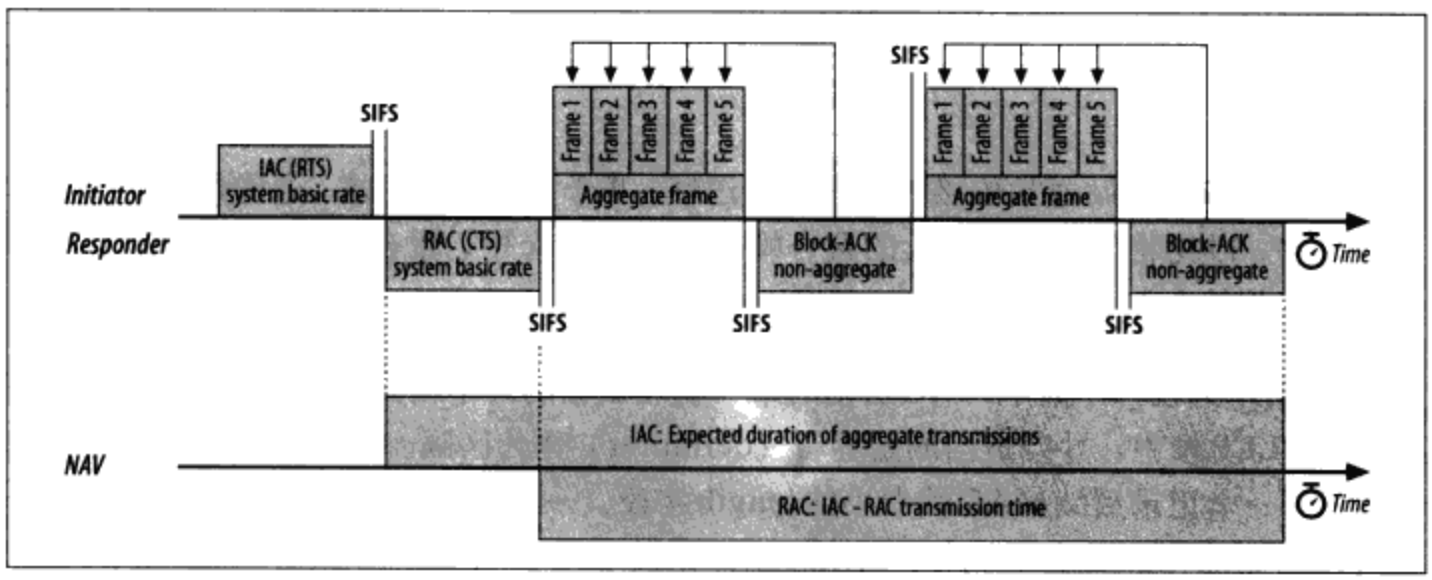


图 15-10：TGnSync 块确认

为了进一步改善MAC性能，TGnSync定义了一种MAC标头压缩算法来搭配聚合帧使用。它的用法类似拨号时所使用的Van Jacobsen标头压缩。传送于两个端点间的帧，其MAC标头中的字段大多相同，比较明显的是封包中的MAC地址。因此，MAC帧所包含的3个MAC地址组合就可以用长度为1个字节的标头标识符（Header ID，简称HID）来代替。HID还可以省略Duration字段，因为聚合帧自己就拥有Duration以及用来控制

QoS 的 2 个字节。当帧的发送端与目的端相同，就以相应的单一 HID 来取代，无需重复传送相同的 22 个字节的标头信息。MAC 帧的标头压缩方式如图 15-11 a)所示。首先，包含完整标头的标头帧被传送至目的端并且被赋予一个 HID。HID 可用来代替之前的完整标头，只要传送 1 个字节，就可以索引出之前所传送的 Duration、寻址与 QoS 数据相关的信息。

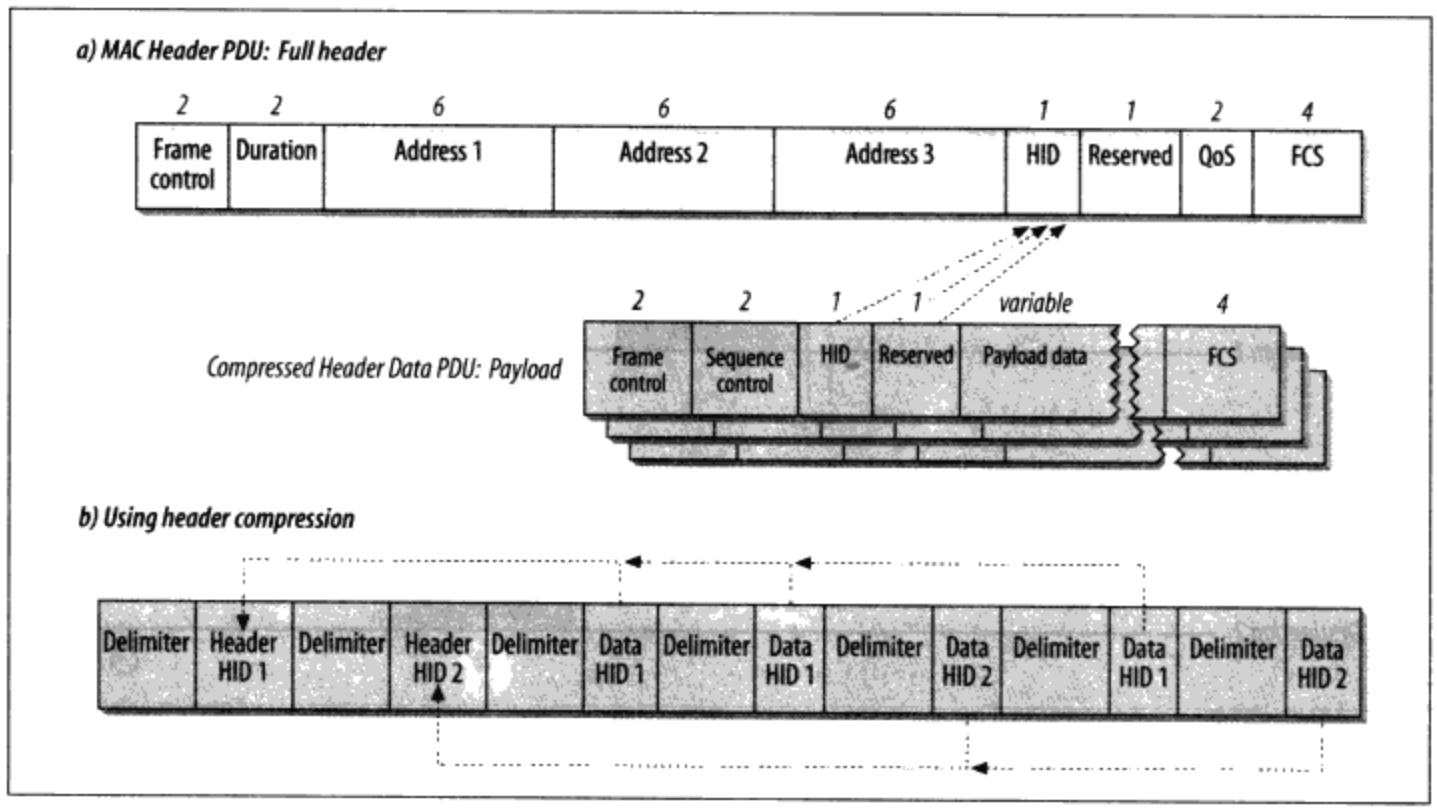


图 15-11：TGnSynx MAC 标头压缩

标头压缩的用法如图 15-11 b)所示。打算分送至两个目的地的 5 个 MAC 帧被聚合成单一帧后交付给物理层传送。此系统会对标头进行压缩，而不会在组成聚合帧的各个 MAC 帧中附上完整的标头。既然有两个目的地，就会有两种不同的 MAC 标头。它们各自被赋予一个 HID 编号，然后被传送出去。随后的 5 个数据帧各自使用适当的标头编号。HID 编号的独特性只存在于单一聚合帧的环境中。相比较于 5 个帧均传送完整标头，如此可将 MAC 成帧所造成的负担减低一半以上。

如果聚合帧所包含的几个帧的来源与目的地相同，标头压缩就特别有用。不过，TgnSync 聚合操作的好处并不限于点对点传输。单一接收者的聚合操作也是必要的（required）。另外一种非必要的扩展功能（optional extension）允许聚合帧包含传送给不同接收者的 MAC 帧，这种情况称为多接收者聚合（Multiple Receiver Aggregate，简称 MRA）帧。单一聚合帧可以包含几个 IAC 帧。每个 IAC 会指定传送对聚合帧的响应的时间差（offset），这些响应通常就是块确认响应。为了区别多接收者聚合帧与单接收者聚合帧，多接收者的帧是以称为多接收者聚合描述符（Multiple Receiver Aggregate Descriptor,

简称MRAD）的控件作为启始字段。启始者的聚合帧始于MRAD，其后才是分送至各目的地的聚合帧。帧之间是用IAC帧加以隔离。

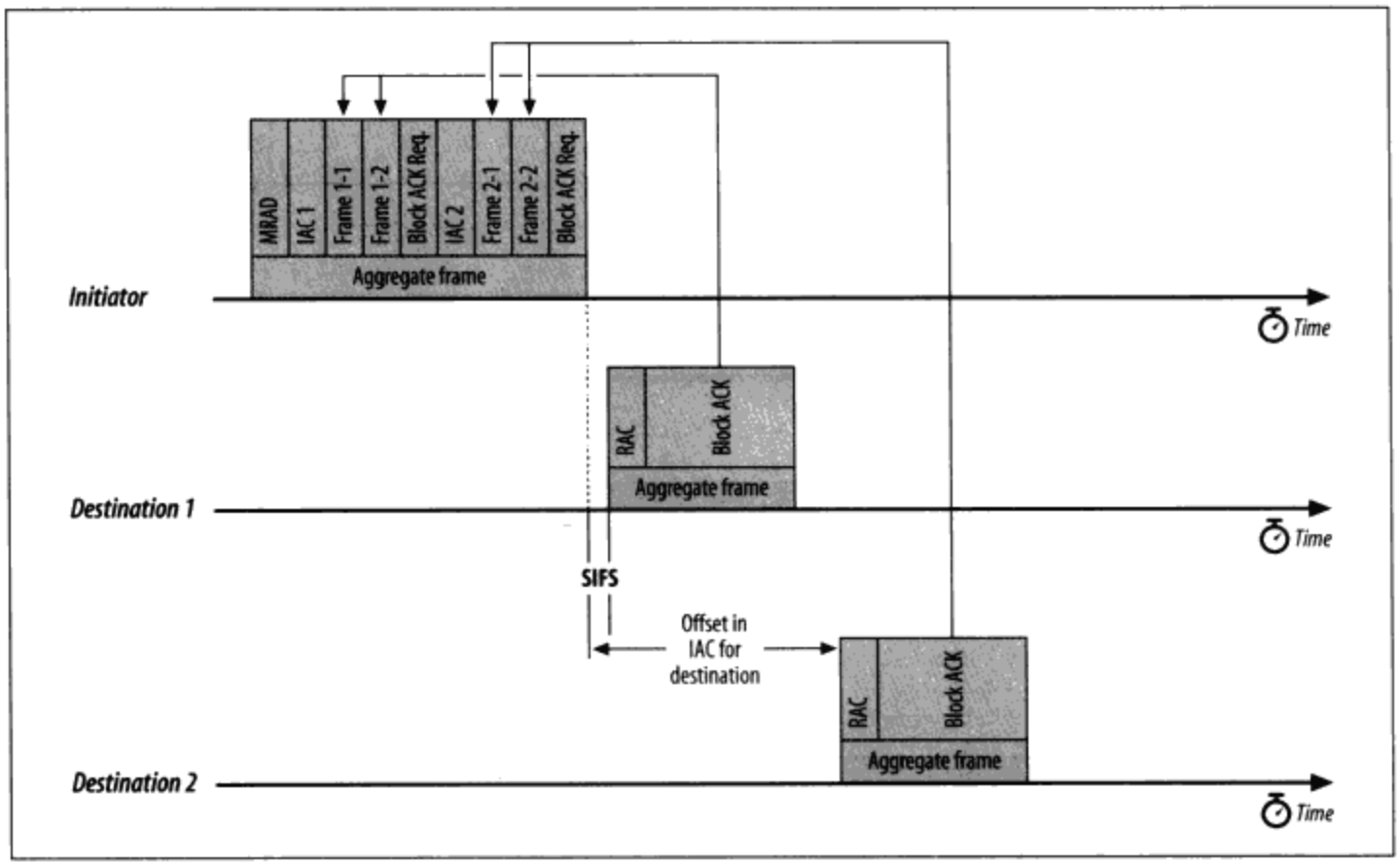


图15-12：TGnSync MRA

保护机制

如同市面上的各式物理层，TGnSync提案也提供保护机制以避免干扰旧的物理层。TGnSync提案的保护机制主要有两种形式。第一种是以MAC的虚拟载波监听机制与网络分配向量为基础。第二种是以“欺骗”（spoofing）机制为基础，使用现有的PLCP标头格式来承载duration信息。工作站可以自行判断应该使用何种机制。

以长NAV值来保护帧交换过程，只是借用802.11g保护机制并稍作调整。帧交换一开始会在RTS帧中设定够长的NAV值，以便保护整个帧交换过程。RTS帧是以“传统”（legacy）速率进行传输，现有的OFDM接收器也可识别。目的端工作站会发送一个CTS信息作为响应，当中也包含一个长NAV值。根据MAC的基本访问规则，在RTS/CTS清空期间，其他工作站必须推迟访问媒介，此时双方就可以使用旧工作站无法理解的调制方式以较高数据率交换帧。CF-End帧可用来提前结束LongNAV周期。这种保护机制用于聚合帧时，必须以IAC取代RTS并以RAC取代CTS。不过，操作的基本原则还是跟以前一样，参见图15-13。

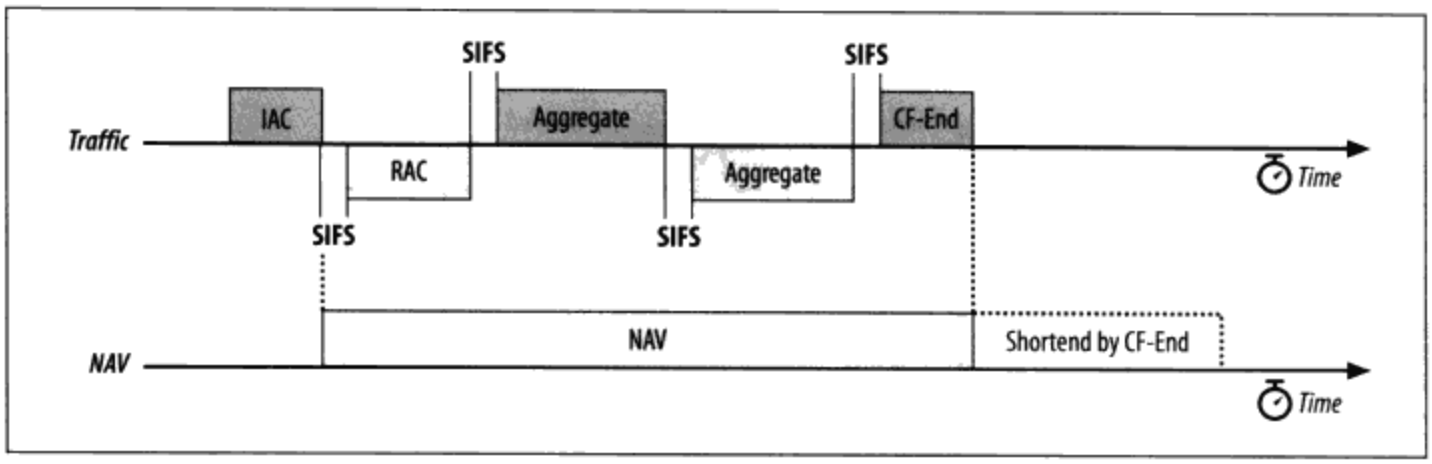


图 15-13：TGnSync 保护机制：LongNAV

第二种保护机制称为“欺骗”（spoofing），主要是设定 PLCP 标头中的 length 字段来实现保护的目的。TGnSync 沿用第十三章所提到的 OFDM 标头。由于和 802.11 a/g 格式相同，因此 spoofing 会影响所有工作站。OFDM PLCP 标头包含两个数值，接收端可以借此判断传输需要多长时间。Signal 字段（如图 13-16 所示）将帧主体（body）的数据率及其长度编码成几个位。工作站会解码 Signal 字段，并用位数除以数据率得出大概需要的传输时间（注 1）。为了取得 spoofing 所需要的最长时间，传统 Signal 字段的数据率一律设为最小值，即 6 Mbps。

交叉欺骗（pairwise spoofing）时，两个工作站会各自传送一个长度与速率均不正确的帧，所以旧工作站会在此帧及其响应期间进入接收模式。TGnSync 工作站会忽略旧的 Signal 字段，只使用 802.11n Signal 字段。交叉欺骗机制如图 15-14 所示。传送 Frame 1 后，可利用交叉欺骗将帧的接收时间设定至 Frame 2 结束。TGnSync 工作站会将此欺骗解读为较长的 NAV，相当于将 NAV 设定至 Frame 2 结束。此时，响应者（responder）附近的工作站将进入接收状态。若有隐藏节点存在，此 NAV 也可以保护整个传输过程，直到 Frame 2 结束。802.11a/g 工作站会将这段欺骗时间解读为接收时间，就算它们不在第二个帧的接收范围。Frame 2 传送完毕后，同样使用交叉欺骗来保护 Frame 2 与 Frame 3。

如果单一帧必须得到多方响应，或许就需要较长的媒介锁定时间，此时可以使用单方欺骗（*single-ended spoofing*）。使用单方欺骗时，交换过程的第一个帧会使用欺骗机制来保护整个交换过程，好让所有响应信息能够在保护时间内到达。搭配帧聚合操作的单方欺骗机制如图 15-15 所示。第一个聚合帧有多个接收端，必须得到其他两个工作站的响应。它将欺骗时间设定为预计完成整个交换过程所需要的时间。TGnSync 工作站在第一个帧设定期间会进入接收模式，这相当于将 NAV 设定至欺骗时间结束。传统设备在整个欺骗期间也会进入接收模式。

注 1：　尽管会根据帧间间隔稍作调整，不过概念是一样的。

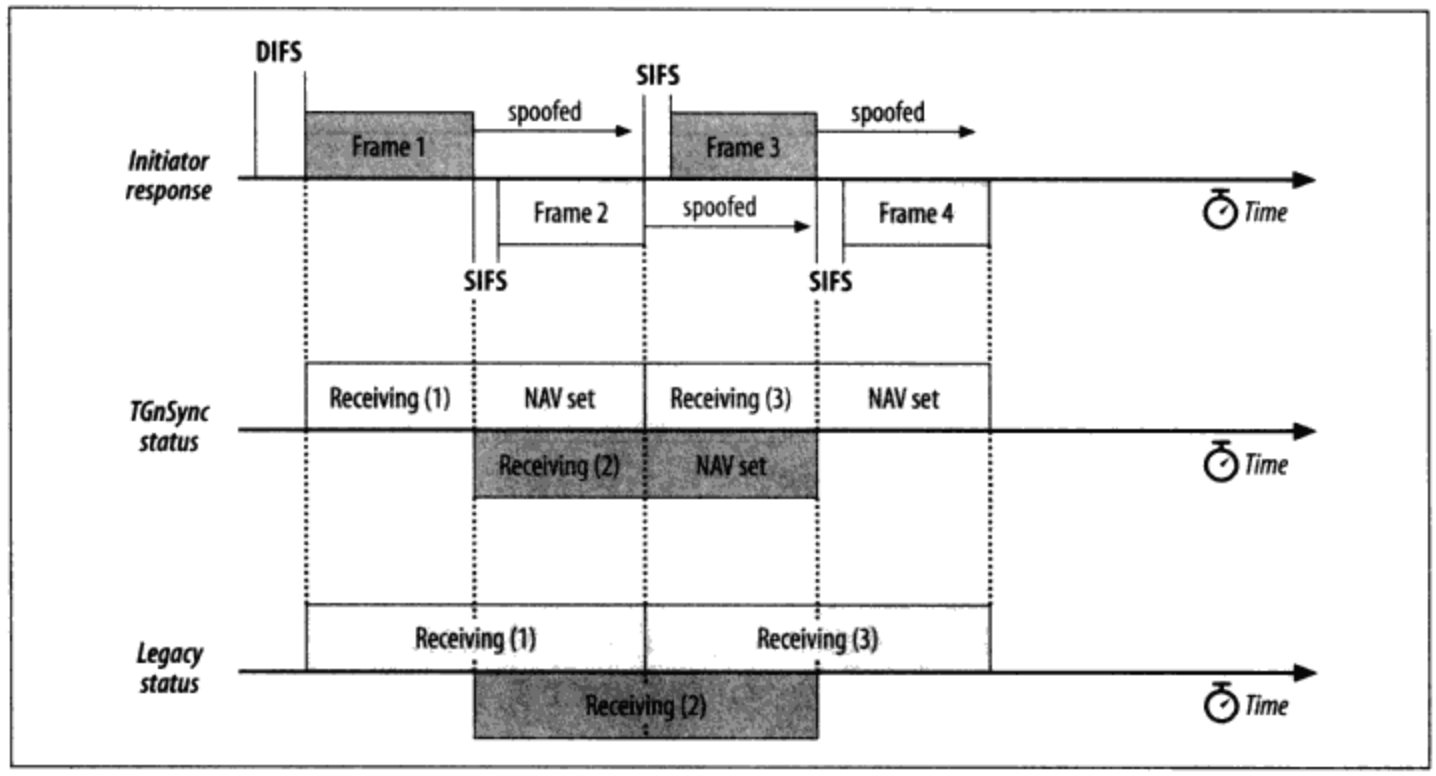


图 15-14：TGnSync 保护机制：交叉欺骗

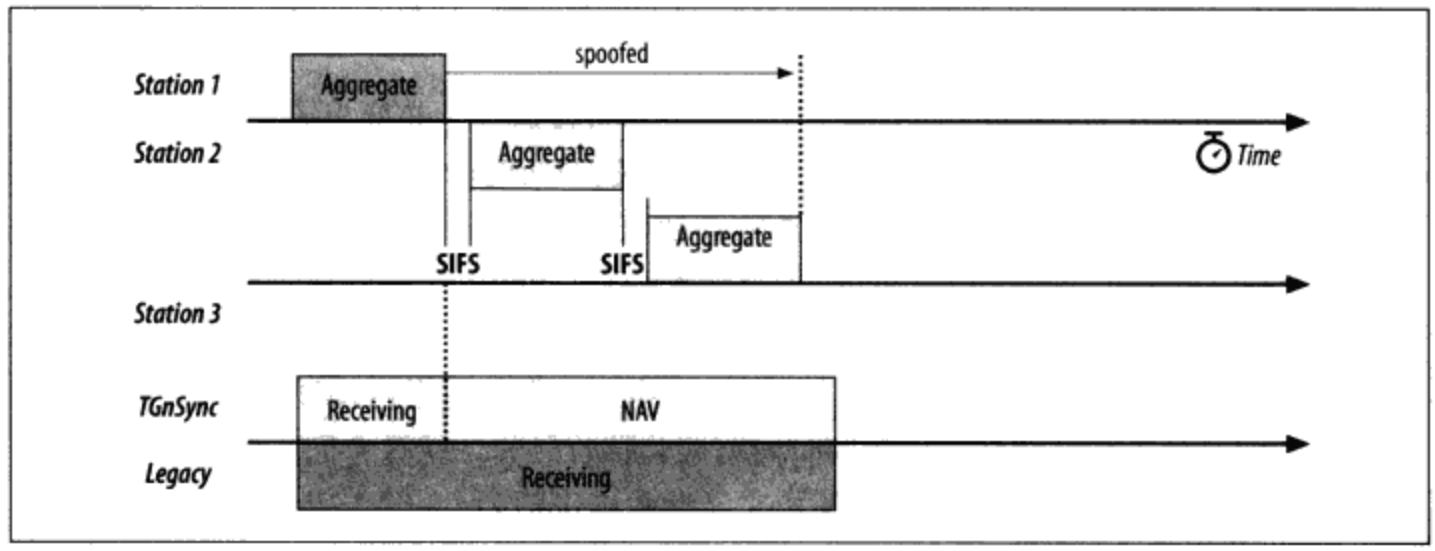


图 15-15：TGnSync 保护机制：单方欺骗

省电机制

TGnSync 定义了定时接收模式切换（Timed Receive Mode Switching，简称 TRMS）协议，用来节省能量并延长电池使用时间。传统的 802.11 省电机制是将接口完全关闭并且在接入点缓存帧。在单进 / 单出（single-input/single-output）接口只有一组射频链路可以关闭。在 MIMO 系统中，如果关闭未用的射频链路，而只留下其中一组来监视无线链路，必然可以省下可观的电力。这两种系统状态分别称为 MIMO 启用（MIMO enabled）

与MIMO停用（MIMO disabled）。前者会启用所有接收功能；后者则会关闭所有RF链路，只留下其中一组。

工作站可以在关联请求中以一项信息元素来启动TRMS省电功能。TRMS省电机制的主要参数为hold time。工作站传送一个帧后，会在hold time所记载的持续时间内保持清醒。后续传送的帧会不断更新hold timer至所需要的时间。将hold time设定为0，代表工作站在进入睡眠状态前会持续运作一个时隙时间（slot time）。

在基础结构型网络里，由接入点负责为每个工作站维护TRMS定时器。时间一到，接入点即推断工作站已经进入MIMO停用状态，这会促使它启用睡眠接收链路。在独立型BSS中，每个工作站必须为所有其他工作站维护hold timer。

此定时器是一个可调参数。如果被设定为较大的值，工作站将会用掉较多的电力来维持接收器全力运作。虽然吞吐量会因此而较高，但代价是必须牺牲一些电池电力。有时候，网络性能不受是否使用省电模式的影响。使用NAV进行保护的网络必须以兼容于所有OFDM工作站的单天线模式来进行最初的RTS/CTS交换，因此不需要传送额外帧，工作站就会以MIMO启用模式来操作。不过，较先进的传送模式将受困于此，因为它们需要使用多天线模式来进行帧交换，这样才能够完全发挥它们的作用。

TGnSync PHY的改良

为了达到较高的最大数据率，TGnSync提案采用类似WWiSE的技术。帧被划分为数个空间流后，以MIMO配置中的多组天线进行多路传输。为了提升数据率，TGnSync使用较激进的编码方式，包括较大的星座图、较高的卷积编码率以及缩短的防护时间间隔。此外，TGnSync也需要使用较宽的信道。TGnSync兼容设备必须支持40 MHz信道，这在WwiSE中则非必要。

信道的结构

如同802.1a，20 MHz与40 MHz信道的划分是以0.3125 MHz为副载波间隔。20 HMz信道与802.11a信道完全相同，如图15-16a)所示。TGn（图15-16 b)）建议使用的40 MHz信道是20 MHz结构的一些修正。捆绑两个20 MHz信道后，再将其划分为128个子信道。这两个旧的20 MHz信道的中心频率会被放在+/－32。这两个旧的20 MHz信道，会在－6与+6之间加上频谱屏蔽（spectral mask），而且频带两端的传输振幅有下滑（roll off）的现象。如果使用单一连续信道，则不需要使用频谱屏蔽，而且频带中央可以用最大功率进行传输。在频带中央以最大功率传输可以增加8个副载波。使用单一连续的40 MHz频带可将原本浪费掉的副载波回收使用。因此在TGnSync中，40 MHz信道的最

大吞吐量不只是20 MHz信道的2倍，而是2.25倍。为了进一步提升吞吐量，这两个20 MHz信道所使用的导频（pilot carrier）也被分别移除了一个，因此40 MHz信道只用掉6个而非8个导频。

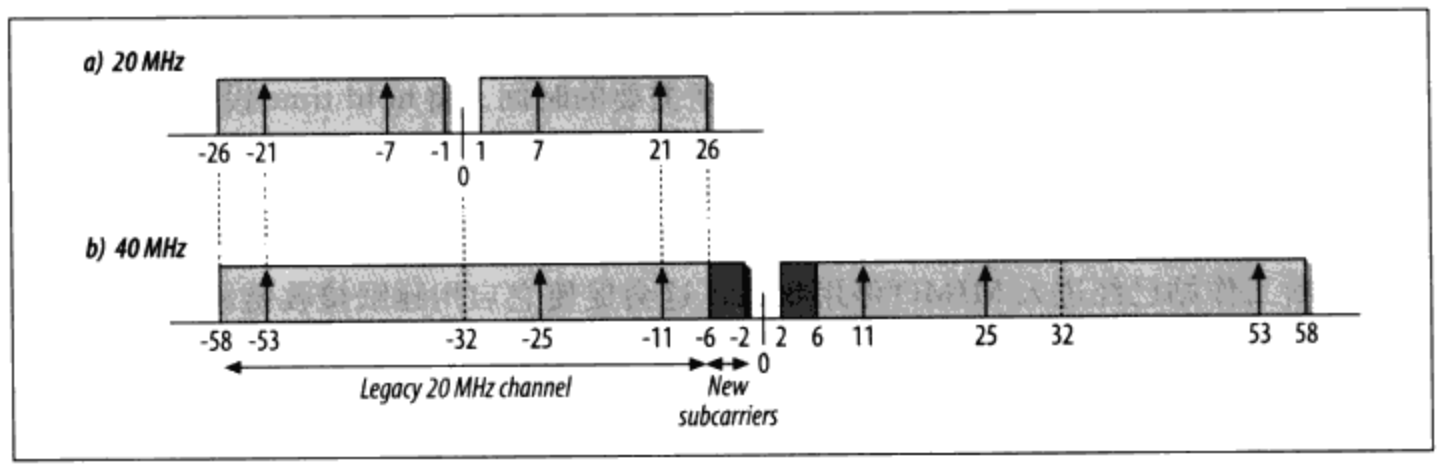


图15-16：TGnSync的信道结构

基本的MIMO速率

TGnSync PHY定义了32种调制与编码配对方式。在基本的MIMO模式中，每道空间流均需使用相同的调制技术，因此数据率即为个别空间流数据率的倍数。为了节省空间，以下仅列出数据率的计算公式，不再以表格列出：

数据率（Mbps）= 12 × channel bandwidth factor × number of spatial streams × coded bits per subcarrier × code rate × guard interval factor

channel bandwidth factor（信道带宽系数）

信道至少为20 MHz，带宽系数设定为1。40 MHz信道可以承载两倍以上的数据，因此带宽系数设定为2.25。

number of spatial streams（空间流数）

空间流数可以是1、2、3或4。它必须小于或等于传输天线数。至少必须支持两道空间流。

coded bits per subcarrier（每个副载波的编码位数）

64-QAM为6，16-QAM为4，QPSK为2，BPSK为1。

code rate（编码率）

搭配BPSK可以使用1/2的编码率；搭配QPSK或16-QAM可以使用1/2或3/4的编码率；搭配64-QAM可以使用2/3、3/4或7/8的编码率。

guard interval factor（防护时间间隔系数）

基本防护时间间隔为800 ns，其系数设定为1。400 ns的防护时间间隔可以稍微提升吞吐量，其系数设定为1.11。

在使用单一空间流的基本模式中信道性能与802.11a相同，不同的是可以使用7/8的编码率达到63 Mbps的数据率。如果将所有参数调至极限值（4个40MHz信道、64-QAM搭配7/8的编码率以及短防护时间间隔），TGnSync建议的吞吐量最高可达630 Mbps。

传输模式

TGnSync提案要求支持三种MIMO模式。在必要的基本模式中，空间流数等于天线数。每道空间流使用相同的调制与传输方式。每个信道使用相同的调制方式来编码，然后以相同的传输功率来传送。任何传输率的变动均是为了对漏失的确认信息所做的调整。

另两种非必要的模式会利用从所谓的“闭环”（closed-loop）操作得到的信息。TGnSync设备会互相传送“探测”（sounding）帧以测量链路的性能。根据探测与校准（calibration）所搜集到的信息，可以使用波束形成（*beamforming*）来提高信号质量。较高的信号质量意味着既定的数据率可以传输较远的距离。在信噪比不变的情况下，以波束形成进行传输可以承载更多数据。波束形成并非必要的协议功能。并非所有客户端设备都能够以波束形成进行传输，但所有客户端设备都必须能够接收波束形成帧。

在搭配波束形成的基本MIMO模式中，每个信道都必须以相同方式编码。开始传输之前，必须先交换探测帧以校准无线电信道。根据探测帧所得到的信息，可进一步为空间流选用传输功率与编码方式。基本波束形成模式（basic beamforming mode）要求所有空间流以相同的功率和相同的编码方式进行传输。不论空间流数小于还是等于传输天线数，均可使用基本波束形成。不过，当传输天线数远多于接收天线数时，信号处理上才会有比较明显的优势。如果空间流数小于传输天线数，就会使用空间引导矩阵（spatial steering matrix）为每个位指定传输天线。

此外，TGnSync还定义了一种可选的称为高级波束形成MIMO（advanced beamforming MIMO，简称ABF-MIMO）的模式。它的运作方式类似基本波束形成模式，但具备额外能力，可以在每一道数据流中使用不同的传输功率以及为每一道空间流使用不同的调制与编码方式。如同基本波束形成模式，它必须搜集无线电波状态信息来校准信道。高级波束形成模式中有一种可选模式，就是如果双方均支持的话，允许双方同时采用波束形成。ABF-MIMO模式还包含了一种新的星座图：256-QAM，每个副载波可以传递8个编码位。

要得到高级波束形成模式的吞吐量，可以使用上一节的公式来分别计算每个空间流的吞吐量，然后再予以求和。以256-QAM而言，每个副载波使用8个编码位，它只能搭配R=3/4的编码率。

可选编码

除了原始OFDM规范说明书所支持的卷积码（convolutional code），TGnSync提案也包含了两种可选的纠错码。第一种技术使用（开发于20世纪60年代）Reed-Solomon码。它被广泛使用在许多数字应用中，特别值得注意的是CD与DVD所使用的纠错码。TGnSync提案以传统方式结合了Reed-Solomon码与现有的卷积码。首先以Reed-Solomon码进行数据流的编码，然后将编码的结果交给卷积编码处理（注2）。这两种编码方式彼此互补。卷积编码是将错误于时间轴展开，能够处理比较零散的错误；Reed-Solomon编码擅长于更正瞬间突发的错误。Reed-Solomon/convolutional编码组合的替代方案是低密度奇偶校验（low-density parity check，简称LDPC）码。

短防护时间间隔选项

为了进一步提升MAC的性能，TGnSync提案允许使用短防护时间间隔（short guard interval）。802.11a与802.11g标准以及WWiSE提案使用800 ns的防护时间间隔。第十三章曾经提到，防护时间间隔应为延迟扩展的2至4倍。800 ns的防护时间间隔容许200 ns的延迟扩展，远高于实际情况所需。大多数办公室与家庭的延迟扩展远低于此，大概是50~100 ns左右。在这种情况下，使用400 ns的防护时间间隔可以提升大约10%的吞吐量。

TGnSync物理层传输（PLCP与PMD）

在TGnSync提案中，PLCP的基本帧格式如图15-17所示。它使用与现有OFDM相同的标头，因此不需要用到会造成严重负担的保护机制来避免干扰802.11a或802.11g网络。图中前置“L-”的字段属于802.11a与802.11g共享的旧式字段，相关细节请参阅第十三与十四章。

旧式标头

TGnSync PLCP帧的前三个字段与802.11a/g PLCP标头相同。

L-STF（旧式短训练序列字段）

此字段与802.11a中的定义相同，持续时间为8微秒。

L-LTF（旧式长训练序列字段）

此字段与802.11a中的定义相同，持续时间也为8微秒。

注2：分组编码器（block encoder）搭配卷积编码器的组合特别受欢迎，一向广泛应用于深度太空探测（deep-space probe）。Galileo、Cassini、Mars Pathfinder以及Mars Rover均使用Reed-Solomon/convolutional编码组合。

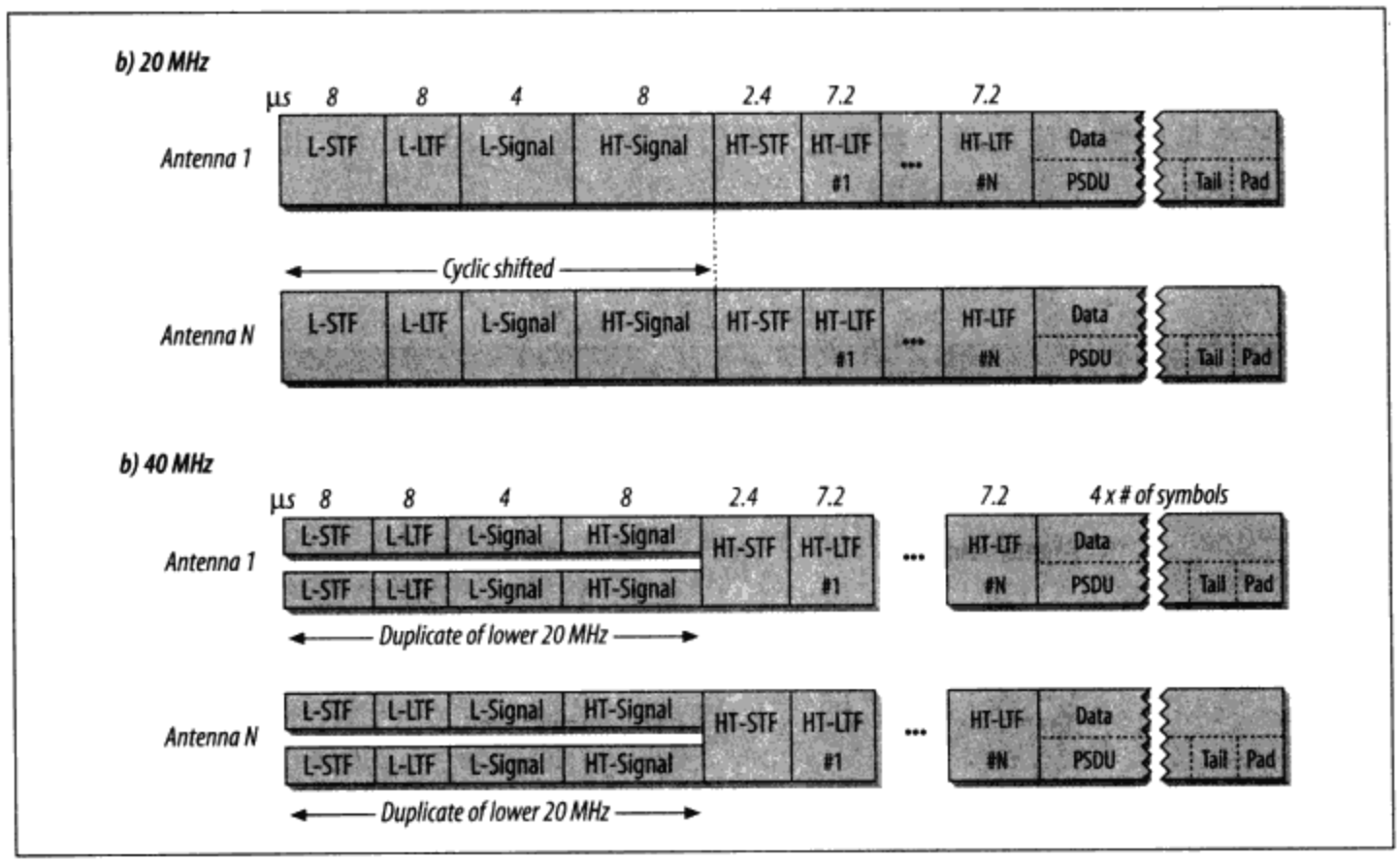


图 15-17：TGnSync PLCP 帧的格式

L-SIG（旧信号）

这三个字段与802.11a相同，802.11g也使用相同字段，相关细节详见图13-16。此字段是以BPSK、R=1/2进行调制与编码。

TGnSync工作站会忽略L-SIG字段的内容。使用欺骗机制进行保护时，L-SIG字段的内容并不明显。TGnSync工作站会在旧标头之后的high-throughput标头中找寻所承载MAC帧的真正长度与编码方式。

为了利用空间分集（spatial diversity）的好处，即以多组天线传送相同的旧标头，TGnSync提供了一种非必要的周期延迟（cyclic delay）。每组天线传送旧帧时，会对周期前置时间稍作改动，让总延迟时间偏移50 ns。

使用40 MHz信道时，会同时在每个20 MHz子信道上传送旧标头。换言之，编号−58至−6（位于较低频带的20 MHz子信道）以及编号+6至+58（位于较高频带的20 MHz子信道）的副载波均被用来传送旧式802.11a标头。

High Throughput 标头

紧跟在旧式前导码之后的是TGnSync提案特有的“hight througput”标头。此标头的主要成分为hight throughput signal（简称HT-SIG）字段，如图15-18所示。HT-SIG字

段是用来检测帧是否承载以高数据率传递的经TGnSync编码的数据，还是只是旧式数据帧。HT-SIG 字段采用较保守的调制方式，以 Q-BPSK、R=1/2 进行调制与编码。Q-BPSK在星座图中使用两个数据点，但出现在正交（quadrature）组件中。图 15-18b) 比较了 Q-BPSK 与 BPSK 星座图。

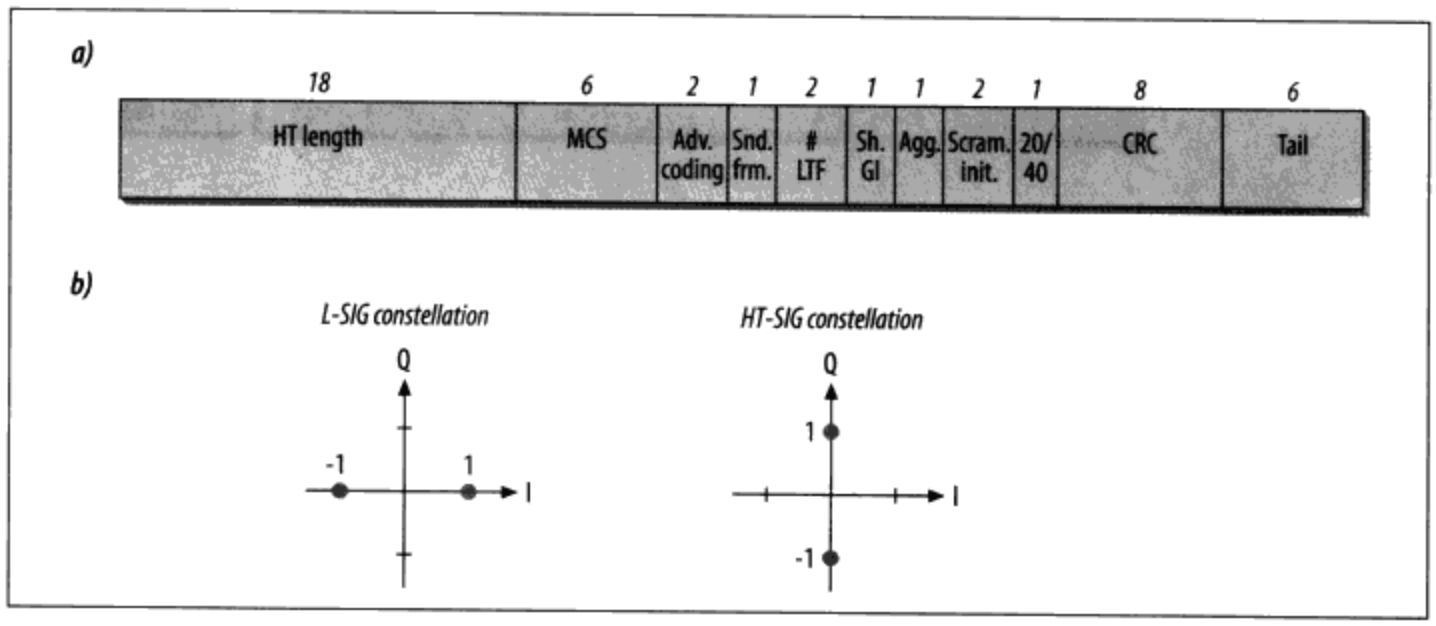


图 15-18：TGnSync HT-SIG 字段

长度为3个字节的high throughput标头是由数个字段组成并且依出现的次序加以传送，最先传送的是每个字段的最低位。

HT-Length（18 个位）

此字段是PLCP帧的有效载荷的长度。进行聚合操作时，如果有效载荷中包含好几个全尺寸的 MAC 帧，此字段的值就会很大。

Modulation and Coding Set（简称 MCS；6 个位）

MIMO的缺点之一是其中包含了种种选项，除了有不同的调制机制、不同的空间流数，还有不同的编码率。MCS 字段是用来选择调制与编码机制以及空间流数。基本 MIMO 模式使用 0~31 的数值范围，33~60 则是留给高级 MIMO 模式使用。

Advanced Coding（2 个位）

此字段的长度为2位，用来指示是否使用可选的高级编码选项。0代表不使用高级编码；1代表使用 LDPC；2代表使用 Reed-Solomon 编码；3目前保留未用。

Sounding packet（1 个位）

用来测量信道性能的请求与响应帧会设定此位。一旦设定此位，代表天线正在传送各自的空间流；如果未设定此位，就不该使用此帧来测量信道的相关信息。

Number of HT-LTFs（2 个位）

紧跟在HT-Signal字段之后的是high-throughput training字段。每道空间流均需要具备一个 training 字段。

Short Guard Interval（1 个位）

如果此位标记设定为 1，代表 400 ns 的短保护时间间隔会被用在帧的 Data 字段中的 MIMO 符号中。

Aggregation（1 个位）

如果此位被设定为1，代表PLCP帧承载了聚合突发（aggregate burst）的几个MAC帧。

Scrambler initialization（2 个位）

这 2 个位用来作为扰频器的随机数种子。

20/40 BW（1 个位）

如果设定为 1，表示使用 40 MHz 信道；如果设定为 0，表示使用 20 MHz 信道。

CRC（8 个位）

CRC 用来保护 L-SIG 字段以及之前的 HT-SIG 字段中的所有字段。

Tail（6 个位）

HT-SIG 字段受到卷积码的保护。如同以往，需要 6 个位来关闭（ramp down）卷积编码器。

High-Throughput Training 字段

紧跟在 high-throughput 标头之后的是 high-throughput 长与短训练序列字段。单一短训练序列（short training）字段会延伸至整个操作信道。在20 MHz信道中，high-throughput short training 字段（简称 HT-STF）的带宽为 20 MHz。如果使用较宽的 40 MHz 信道，则HT-STF的带宽为40 MHz。short training 字段用来微调MIMO操作所使用的接收器。

当数道空间流通过数个链路进行传输时，精确控制接收信号的放大操作就十分重要。high-throughput long training 字段（简称 HT-LTF）用来进一步调整各个接收链路。每道空间流各自使用一种HT-LTF。在基本 MIMO 模式中，每道空间流对应到一个接收器链路；在高级模式中，接收器链路的数目多于空间流的数目。

Data、Tail 与 Padding

Data 位是根据 high-throughput 标头所定义的调制与编码方式被编码。和其他的 OFDM 物理层一样，在传输之前数据必须经过扰频，使用high-throughput标头中的扰频器来初始化位。数据之后是长度为 6 位的标尾（tail），用来关闭卷积编码器并且加入足够的填充位（padding），让待传的数据长度与符号块的大小相等。

TGnSync PMD

TGnSync 收发器的基本设计如图 15-19 所示，图中所显示的是波束形成发射器（beamforming transmitter），而非基本的MIMO发射器。接收到扰频帧后随即交给前向纠错（forward-error correction，简称FEC）编码器处理，它通常就是卷积编码器。来自FEC编码器的编码位随后被空间解析器（spatial parser）送至不同的空间流。空间解析器的任务是负责将单一位流分割为子流以便进行传输。每道空间流均被收缩（puncture）为预计传送的速率。在波束形成模式中，每道空间流均接受收缩处理并且可以使用不同的速率。基本型发射器必须以同样的速率对各道流进行收缩处理（逻辑上，基本型发射器的收缩过程可以先于空间解析器发生）。此时，每道空间流均包含一系列编码位，准备由交错器（interleaver）映射到OFDM载波。经过交错器处理后，每个位块会被星座图映射器（constellation mapper）映射至单一符号。在基本MIMO模式中，每道经过交错的空间流均由单一传输链路处理；高级模式则会使用空间引导矩阵（spatial steering matrix）把每个符号指派给任一传输链路。图 15-9 中所显示的空间引导矩阵可以用一对一的接口替代，介于空间流处理器与用于基本MIMO操作的传输天线之间。每个传输链路取得本身的符号序列后，会把它调制成波段（airwave）。规范说明书中并未提到邻道抑制（channel rejection）或灵敏度性能（sensitivity performance）的相关规定。

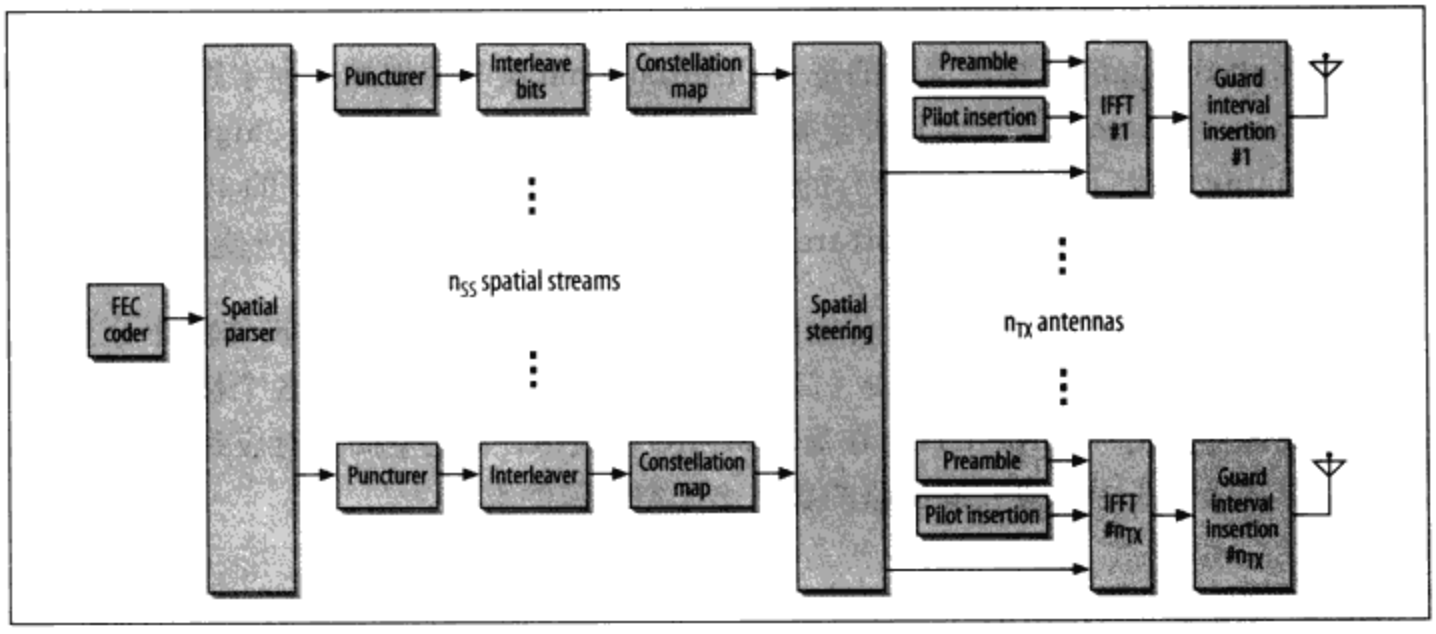


图 15-19：2X2 TGnSync MIMD 收发器

比较与结论

基本上，WWiSE 与TGnSync这两份提案算是802.11a物理层的MIMO修订版。两者均要求支持2x2模式，即发送端与接收端分别具备两组收发器。不过，根据最后出炉的

802.11n标准（不论是否与提案相似）所开发的大部分产品，可能会至少支持几种可选模式。基于成本的考虑，客户端设备可能会限制它们只能使用两组收发器模式，但接入点将使用较多收发器。基本型接入点可能只会使用两组收发器，但大多数昂贵的企业级接入点将使用三组或四组收发器。

表15-5列出了这两种提案的各种空间流模式的数据率。增加空间流可以达到较高的数据率，但会增加芯片成本。TGnSync提案能够达到较高的数据率，但是必须使用较激进的编码率。要达到WWiSE的135 Mbps的数据率，必须使用64-QAM搭配R=5/6的编码率；要达到140 Mbps，TGnSync必须使用7/8的编码率并且将保护时间间隔减半（如果不使用短保护时间间隔，TGnSync的数据率仅达126 Mbps）。高级波束形成模式则采用较大的256-QAM星座图。虽然TGnSync的数据率较高，但我预料采用较激进的编码率将导致传输距离变短。

表15-5：802.11n的两份提案的最高传输速率（两道空间流）

	20 MHz 信道	40 MHz 信道
WWISE	135 Mbps	270 Mbps
TGnSync		
基本模式	140 Mbps (+3.7%)	315 Mbps (+16.7%)
高级波束形成模式	160 Mbps (+18.5%)	360 Mbps (+33.3%)

频谱的运用方式是两个阵营的主要争论点。WWiSE强调MAC效率甚于数据率，甚至认为不先改善MAC性能就径自使用40 MHz信道来提升数据率，根本就是浪费稀有的免许可频谱。这不无道理，TGnSync使用40 MHz信道的做法的好处是可以回收信道中央的频谱。WWiSE使用40 MHz信道时只能够让吞吐量增加一倍，但TGnSync可以在相同的信道中挤出两倍以上的吞吐量。这两种方式各有其缺点。TGnSync提案或许会导致芯片组永远以40 MHz操作，带来额外的成本与复杂度，而且管理者可能不允许使用40 MHz信道。允许使用40 MHz信道的国家当然会欣然接受更快的速度，但在限制使用40 MHz信道的地区，额外衍生的成本就不是芯片厂商所乐见的。另一方面，WWiSE认为不需要高速信道，似乎等于拒绝让数据率提升5倍的可能性。

为了达到最高速率，TGnSync要求使用闭环（closed-loop）操作。要在芯片中实现闭环操作并不容易。除了以探测帧测量信道，还必须搜集响应信息以便校准无线信道。WwiSE只使用开环(open loop)操作，这在实现上比较简单。不必使用闭环操作，WWiSE提案就能够将单一编码流展开至多组天线。如果闭环操作在芯片的实现上有其困难，802.11n标准将再度延迟推出。

为了实现802.11n最终标准所设定的远大目标，帧聚合在其中扮演着重要的角色。不过要完全发挥帧聚合的优势，需要在目前所实现的队列机制（queuing）中加入更多智能。802.11n能否大幅提升速度，取决于所改善的队列算法能否将较小的封包整合成较大的聚合封包。这两份提案均未规范队列机制，因此性能的提升程度将因厂商而异。

TGnSync所设计的聚合功能比较聪明，虽然差距不会太大。MAC标头的Address 1字段值相同时WWiSE才允许帧聚合。在基础结构型网络里，Address 1字段即为BSSID。工作站传给接入点的任何帧均可予以合聚合，因此这两份提案在上行部分是相同的。在下行方面，WWiSE必须通过物理层帧突发来变换方向。任何新方向都必须使用新的PLCP标头。TGnSycn可以使用一个多接收器聚合帧来减少负担（overhead）并从聚合帧中搜集来自各接收器的响应。

802.11的省电模式向来无人重视，构造也过于简单。TGnSync试图为新的MAC架构提供扩展的省电功能，WWiSE则没有。或许是因为TGnSync联盟包含许多设备厂商，而WWiSE阵营则完全由芯片厂商组成。虽然速度与电池电力的取舍会因应用而异，而且不见得合理，但标准制定单位能够未雨绸缪未尝不是件好事。

第十六章

802.11 硬件

制定规范时，重要的是为创新留点诠释的空间。标准过于严苛，实现起来就会死气沉沉；标准过于宽松，则无法顾及互用性。本章主要探讨标准未曾明确规范的事项。例如：标准在硬件上如何实现？在协议的实现上，有哪些地方是标准允许自行斟酌的？对网管人员而言，这又代表什么？

802.11 接口的一般结构

图16-1是一般无线局域网络接口的方块图。这并不是特定厂商的产品，只作为讨论网卡结构的参考指南。网卡必须实现出实体接口以及操作系统所需要的链路层控制。

就像其他使用无线电技术的产品，无线局域网络接口同样内含天线。大多数802.11接口使用两组天线作为天线分集（antenna diversity），以便在多径干扰的环境下改善接收情况。接收到无线电信号时，无线电系统会自动选择信号最强的天线来进行收发。天线分集可以改善多径干扰，就算信号微弱是因为多重信号所造成的自相干扰，至少还有一支天线可以接收到信号。如果信号微弱是因为距离太远所造成的，天线分集就帮不上忙了，因为两支天线所接收到的信号同等微弱。天线分集有各种类型，目前最常见的实现方式是只在接收帧时才会使用天线分集。几乎市面上的所有产品都不会在传输帧时使用天线分集，仅使用“主要”（primary）天线进行传输。

早期的天线分集虽有帮助，却因为实现上过于简单而有其限制。多进/多出（multiple-input/multiple-output，简称MIMO）技术可以达到更高的数据率与更好的性能。不过MIMO的细节已经超出本书的范围。基本上，它舍弃了单一天线的做法，而是同时使用两组天线来提升接收的性能。

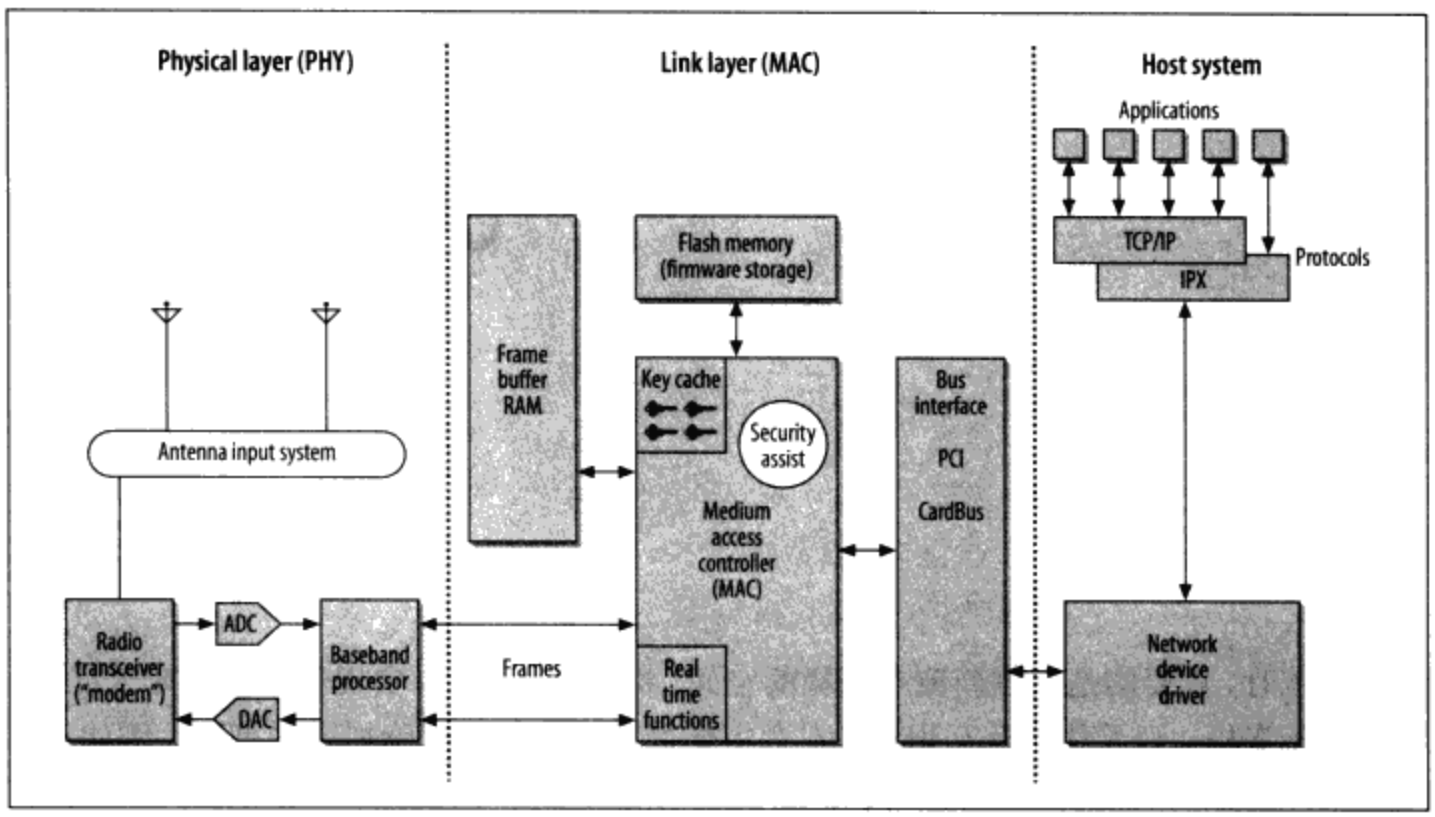


图 16-1：一般无线网卡的结构

天线将无线电信号传给收发器。以无线电通信常用的调制解调器（modem）来模拟，收发器（transceiver）有时也被称为无线电“调制解调器”（radio“modem”）。收发器使用放大器（amplifier）来强化对外传送的信号，或者将接收到的信号放大以便进行后续的处理。无线电收发器还会通过从高频载波中取出数据位的方式，将高频信号转换成比较容易处理的信号。收发系统通常需要加以屏蔽以防止高频信号干扰其他系统组件。这就是为什么无线电接口通常会有一层金属屏蔽，它占据了整张接口卡的不少面积。

收发器之后是基带处理器（baseband processor），它是无线局域网络系统中数字与模拟组件之间的接口。将位转换成无线电波称为调制（modulation）；反之则称为解调（demodulation）。基带处理器负责处理复杂的扩频调制以及检测物理载波。当所接收到的电波能量超过一定的阈值，基带处理器就会加以解调。目前，无线局域网络可以使用多种不同的调制技术。802.11b工作站之所以无法察觉802.11g的传输操作，原因之一在于802.11b 所使用的旧式基带处理器无法解调OFDM 信号。

媒介访问控制器（medium access controller，简称MAC）是整个接口的核心，负责从主机操作系统的网络堆栈中取出所接收到的帧以及决定何时通过天线将帧传送出去。MAC 会通过系统总线接口从操作系统取得帧。大多数的无线局域网络接口采用的是CardBus 标准，有些则是使用 Mini-PCI。MAC 的另外一端与基带处理器相连，由它传送帧给无线电系统。

MAC 可能会同时处理许多帧，它可以配置少许的 RAM 缓冲区来缓存这些正在处理的帧。之所以要对帧进行处理，最常见的原因是为了让主机操作系统摆脱安全处理操作的负担。具备安全处理功能的 MAC 可以从驱动程序接收准备以特定密钥加密的帧，而不必在传送帧之前通过主系统的 CPU 进行加密。MAC 中通常内置密钥高速缓存（key cache）来存储密钥。传送之前，驱动程序会将帧置于队列，同时指定以 key 1 进行加密，随后主系统就可以将加密的重担交给 MAC。旧式的 MAC 芯片有能力处理 WEP 所使用的 RC4 加密，而且升级后也可以处理 TKIP，至于最新型的 MAC 芯片，则可以在硬件中进行 AES 加密。

除了用来缓存帧的 RAM 缓冲区，大多数接口还会使用少许的闪存来为 MAC 存储固件。供电之后，MAC 就会从闪存中取出程序代码并加以运行。若要实现类似 TKIP 的新式安全协议，只要将新的固件写入闪存，然后重新启动 MAC 即可。相比较于不容易变更的专用集成电路（application-specific integrated circuits，简称 ASIC），遇到 802.11 这类变动快速的协议时，使用固件只需要搭配一般的通用型处理器就行了，这对开发过程提供了不少帮助。大部分的 802.11 MAC 芯片实际上就是一般的通用型微处理器。

实现时，有些 MAC 会针对需要立即响应的项目提供一个“实时”（real-time）单元。如此一来，这类帧就可以由 MAC 自动产生，不需要交由主机操作系统响应相关的省电轮询（power-save polling）操作或者传送确认信息。有些系统则是将这类实时功能交给基带处理器处理（目前 MAC 与基带处理器通常已经整合为一个芯片，因此这种区别就无关紧要了）。

图 16-1 的方块图只作为参考之用。为了降低成本与复杂度，有些系统会使用将 MAC 与基带处理器整合在一起的芯片，有些解决方案甚至会将无线电收发器也整合进去。使用 Atheros 芯片组的接口不需再使用额外的闪存来存放固件，因为 Atheros 芯片是在驱动程序启动 MAC 时才加载程序代码。固件通常是指存储于硬件中的程序代码，Atheros 设备可以通过系统软件进行编程。

软件定义无线电：离题插播

802.11 所面临的两个主要问题除了有 MAC 效率不高而导致总传吞吐量受限，还有物理层技术变动太快而导致产品生命周期缩短。面对效率不高的自然反应，通常是针对特定部分进行优化或者在现有的硬件上采用新的协议功能，对沉浸于技术领域的工程师而言尤其如此。

无线局域网络通常无法自行定义接口的功能。出于速度上的考虑，通常会直接将基带处理器或者基带处理器的功能直接实现于集成电路中，因此无法任意变更。所谓专用集成电路（ASIC），是以本身的电路来实现特定的逻辑，因此无法用于原本的设计目的以外。

此外，无线局域网络接口所使用的无线组件通常已经针对管理者所配置的频率做过优化处理。

不过，未来的无线电将是可重新编程的（reprogrammable）。设计人员可以使用“可编程逻辑”（programmable logic）设备，例如FPGA，来取代基带处理器这类特定硬件。无线电波是承载数字数据的模拟电波。在某些情况下，无线电波只需要进行可编程信号处理，就可以使用数字信号处理器（digital signal processor，简称DSP）芯片。不论使用何种可编程逻辑，最终目的都是一致的。采用可编程逻辑的无线电波可以随时通过新的软件来更换调制方式、编码方式与位率，而不必在设计阶段迁就固定的调制方式。较具灵活性的代价就是可编程逻辑设备的体积较大，运行速度较慢，而且比较耗电（也因此会产生较多的热量）（注1）。使用可编程设备将可以任意调整电波的行为，只要加载新的软件即可。无需更改硬件，就可以实现新的调制方式、位率甚至是新的频带（注2）。

完全以软件（或者可编程逻辑）控制的无线电接口称为软件定义无线电（software-defined radio）或者通用无线电（universal radio）。它们在调制与编码方式经常或快速变动的环境中十分好用。SPEAKEasy算是最早的软件定义无线电项目，由美国军方所推行。美军以单一的软件定义无线电来取代10组调制方式各异的无线电系统，它不但具备10组无线电系统所有的功能，体积也变得更小了。软件定义无线电必须符合美国的认证法规（certification rules），厂商必须采取相应措施以避免软件遭篡改而被使用在核准范围以外的频带（注3）。

虽然软件定义无线电是个有趣且值得注意的发展，不过802.11设备大概不会完全以可编程逻辑来实现（目前，Broadcom与Atheros的芯片组只具备有限的可编程性）。可编程逻辑较贵，市场也不会接受此类802.11设备的价格。它或许可以搭配802.11在使用了多种无线链路的实现产品中找到立足点。

注1：可编程逻辑设备通常用来设计特殊应用设备。经过设计与完整的测试之后，再将FPGA重新设计为特殊应用设备。最后出炉的固定逻辑设备有时也称为之前的可编程版本的“硬拷贝”（hard copy）。

注2：值得注意的是，开放源码社群已经开始采用可编程逻辑。就像SourceForge（*http://www.sourceforge.net*）之类的软件，OpenCores（*http://www.opencores.org*）已经成为硬件设计的宝库。

注3：与软件定义的无线电的认证相关的FCC法规详见FCC 01-264附录B，可以从*http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/2001/fcc01264.pdf*取得。最早通过认证的软件定义无线电，由Vanu所开发的GSM接入点，是在2004年11月取得认证的。

802.11 硬件实现时的议题

写作本书当时，市场上有四家主要的芯片组厂商。依字母顺序，他们分别是：

Atheros

大多数包含 802.11a 的接口均会采用 Atheros 芯片组。有些 802.11g 设备也会采用 Atheros 芯片组。

Broadcom

目前，大多数非 Centrino 的内置 802.11g 接口均会采用 Broadcom 的 802.11g 芯片组。Apple 的 AirPort Extreme 亦然。

Conexant（Prism）

被 Conexant 收购之前，Prism 产品线曾经转手过好几家公司。

Intel（Centrino）

许多膝上型计算机内置的无线局域网络接口均会采用 Intel 的 Centrino。就技术而言，Centrino 是泛指一整组 Intel 芯片的营销名词，其中也包含系统 CPU。例如，Intel/PRO 2200 网卡即为 Centrino 802.11g 接口。

比较值得注意的一家新芯片组厂商是 Airgo Networks，他们所开发的 MIMO 芯片组为目前市面上所谓的 802.11n 预标准（prestandard）产品所采用。

知道网卡采用何种芯片组十分有用。大多数芯片组厂商均会提供参考设计（*reference design*，俗称“公版”）给客户。参考设计通常包含软件和硬件方面。802.11 网卡制造商拿到参考设计后，只要稍微（或根本不用）修改，为产品贴上新的标签就可以开始销售。很少有网卡厂商会大幅修改驱动程序，通常只是将公版驱动程序重新包装。当然，每家厂商的口碑与评价不一。有些经常更新驱动程序，有些则不是。知道网卡的芯片组由谁提供，将比较容易取得公版驱动程序或者使用相同芯片组的网卡所提供的最新驱动程序。当然，要为开放源码操作系统找到可用的正确驱动程序，必定得先知道网卡使用何种芯片组。

进一步认识网卡：FCC 文件

套句管制机构的术语：802.11 接口属于有意辐射体（intentional radiator）。在设计上，802.11 接口本身会主动发射无线电波，因此不能仅仅符合电磁辐射管制的标准限制。有意辐射体必须送测并且要符合各国的管制规定，因此需要很多文书工作。

在美国，无线电设备是由 FCC 所管理，无线电传输设备必须经过测试并且符合 FCC 法规。在合法销售设备之前必须取得校验编号。看看各位手上的网卡，就可以找到上面的 FCC ID。

FCC ID分为两个部分：前三个字母称为申请人代码（*grantee code*），之后的数字称为产品代码（product code）——最多可达14个字符。每个组织有不同的申请人代码（代码也许以空白或破折号分隔，也许没有）。例如，Lucent金卡的FCC ID是IMR-WLPCE24H。其中，“IMR”是Lucent的申请人代码，WLPCE24H则是该金卡专属的产品代码。

作为测试过程的一部分，厂商必须提出测试报告、产品照片以及其他文件，这些文件将被公开登记。要查询网卡的相关信息，可以到FCC工程技术部（Office of Engineering and Technology）所维护的搜索引擎查询，网址是 *http://www.fcc.gov/oet/fccid/*。

要知道某片网卡使用何种驱动程序，FCC ID十分有用。大多数产品均会提供内部照片，可以借此得知该产品使用何种芯片组。譬如你手上有张Proxim a/b/g三合一金卡，想知道它采用何种芯片，只要在FCC的数据库以它的ID进行搜索（HZB-8460），就可以看到该网卡的内部照片，在主板上清楚显示该网卡使用的是Atheros芯片组。

实现上的差异

802.11并非严格的标准。标准的某些部分比较宽松，留给实现相当大的空间。大部分实现产品上市不久，有时会有出人意外的行为。我曾经参与过几次测试，使用几台相同的计算机、相同的操作系统，也使用完全相同的无线局域网络硬件与相同版本的驱动程序。虽然位于相同地点，各台计算机的配置设定也完全相同，但表现上还是会出现显著的差异。

重新启动接口卡

802.11是个复杂的协议，何况它还附带许多选项。使用最新的协议，通常可以发现最新的软件瑕疵。802.11接口使用通用型微处理器来运行软件。既然软件成分居多，网卡如果出现问题，就可以通过“重新启动”（rebooting）来清除存储在MAC处理器中的任何协议状态。外接式网卡可以通过插拔（removing and re-inserting）加以重新启动；内置的网卡则必须通过系统软件以冷开机（power cycling）的方式重新启动。只是重载驱动程序并没有用，因为我们的目的是要清除无线局域网络接口中的所有状态。

要排除无法正常运作的问题，也许必须重新启动网卡。如果有以下情况发生，首要步骤就是重启网卡：

- 客户端系统已经关联，但无法发送数据。如果此为加密网络，问题通常出在加密密钥没有同步。这个问题通常出现在漫游时，因为接入点之间的任何变动均会导致密钥的重新发送。

- 看不到扫描结果。如果确定附近有网络存在，但客户端软件却无法加以显示，可能是这片网卡正处于无法提供扫描结果的状态。
- 发生一连串身份验证/关联失败的现象。当网络被列在连接的“偏好”(preferred)列表，但客户端系统软件所处的状态使其无法连接成功，就会进行一连串的重试动作。

扫描与漫游

在搜寻可连接网络以及判断是否切换接入点方面，每片网卡的表现不尽相同。802.11并未限制客户端设备如何决定是否切换接入点，而且不允许接入点以任何直接的方式影响客户端设备的决定。大多数客户端系统以信号强度或质量作为主要依据，并试图与信号最强的接入点进行通信。

大多数网卡会随时监测收到的帧的信噪比，并以目前所使用的数据率来判断何时应该漫游到新的接入点。如果数据率已经很慢且信噪比又低，客户端系统就会开始寻找其他接入点。有些客户端系统会尽量拖延切换的时间，部分是因为寻找其他接入点的过程需要转换到其他信道，因此会有通信中断的情况发生。一直连接着某个接入点不放的客户端系统称为罹患“捕虫灯症候群”(bug light syndrome)。一旦连接到某个接入点，它就与之终生厮守，就像虫子受到捕虫灯的吸引一样。就算客户端系统距离接入点越来越远，而且信号强度持续滑落，大部分网卡也不会开始进行漫游过程，直到几乎收不到信号为止。

802.11的漫游机制完全取决于客户端的决定。何时何地送出Association Request帧完全取决于客户端系统的驱动程序与固件，对此802.11规范说明书完全没有任何限制。就算客户端决定与信号最差的接入点连接，虽然这是相当糟糕的做法，却仍旧符合802.11的规范(由此产生的不幸后果，就是为了解决问题而更新驱动程序也会出乎意料地改变客户端系统的漫游行为)。接入点中并没有相关的协议操作可以影响客户端该于何处连接以及是否应该离开。当需要争取时效(time-critical)的流应用开始运用于802.11，如何实现出更好的漫游技术将成为802.11的首要任务。

注意： 借用Milton Friedman的话：不论何时何地，漫游均属客户端现象(roaming is always and everywhere a client phenomenon)。

速率的选择

802.11为各种速率需求制定了基本规则，但是将速率选择算法留给接口上所执行的软件自行决定。一般而言，接口在降速之前会试着以较高的速度传送几次。这部分只能算是

普通常识。同样传送有1500字节有效载荷的帧，以11 Mbps传送比1 Mbps快8倍，就算启动保护机制，以54 Mbps的802.11g传送也将快20倍。（如果不用保护机制，甚至快40倍！）如果因为偶发状况造成帧损毁，在接受降速的惩罚之前当然应该试着重传几次。

降速算法通常十分类似。重传帧数次但仍然失败的话，就退而使用较低速率。大部分网卡一次只降一级，直至收到响应为止，虽然没有规定非得如此。如果刚开始碰到问题就降至最低速，也算是有效的速率选择算法。升速算法的运作方式刚好相反。如果接收到的“些许”帧的信噪比优于当前的速率所需，接口就可以考虑往上升速一级。

解读规格表

早期有关802.11设备的测试通常将焦点放在传输距离（range）与吞吐量（throughput）上，因为其他没有什么好测量的。在某些环境下，传输距离会是一项重要的因素。传输距离的多少，部分可以从网卡规格表加以判断。

大致上，传输距离可说是接收灵敏度（receiver sensitivity）的函数。所谓接收灵敏度，是指接收器能够正确将信号转换为数据的最微弱信号。灵敏度越高，传输距离就越长（提高灵敏度也有助于改善其他性能，不过传输距离是最便于讨论的一个）。大多数厂商将焦点放在改善性能上，成果发表时（如Atheros的XR与Broadcom的BroadRange）也颇为自豪。

不过，并非所有厂商都会提供完整的规格表。其中，Cisco就揭露了相当多的信息。对所支持的每个频带，Cisco提供了各个数据率的接收灵敏度（这片网卡在5 GHz上的性能稍微受到频率的影响）。许多厂商只提供所支持的数据率，完全没有提到灵敏度。

灵敏度比较

以下就以几张常见的802.11b网卡为例，比较它们的灵敏度。灵敏度是由802.11物理层所决定的。以直接序列而言，它被定义为：接收1024字节的帧时，帧错误率（frame error rate）为8%的接收功率。标准要求11 Mbps的灵敏度需为−76 dBm或者更佳，2 Mbps的则是−80 dBm（注4）。灵敏度的数值越低越好，因为这代表网卡可以接收到比规定的更微弱的信号。

表16-1所显示的灵敏度报告取自各家的规格表与使用手册，其中包括4片著名的802.11b网卡以及1片较新的a/b/g网卡。Cisco的Aironet 350在微弱信号的处理上有不错的评

注4： 相当于.001%（10^{-5}）的位错误率。

价，这点完全可以从以下数据得到佐证。在 11 Mbps，它可以接收到比 Orinoco 金卡弱上一半，比 Microsoft 网卡弱上 3/4 的信号。不过，科技的进展已经使得高位率的灵敏度有所改善。所有上一代的网卡均无法与采用 Atheros 芯片的 Cisco 三模（tri-mode）网卡相比。

表 16-1：不同网卡的灵敏度（以 dBm 为单位）比较

网卡	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Cisco 350	−85	−89	−91	−94
Orinoco Gold (Hermes)	−82	−87	−91	−94
Linksys WPC11 (Prism)	−82	−85	−89	−91
Microsoft MN-520	−80	−83	−83	−83
Cisco CB-21 (a/b/g)；只测 802.11b 的性能	−90	−92	−93	−94

延迟扩展

当无线电波碰到物体，接收端就会汇聚许多折射或反射波。最早与最后到达的两个波之间的时间差称为延迟范围（*delay spread*）。接收端可以在噪声中捡拾信号，前提是延迟扩展不能超过限度。有些厂商会在规格中列出最大迟延扩展。表 16-2 列出了 3 片网卡的延迟扩展。

表 16-2：不同网卡的迟延扩展（以 ns 为单位）

网卡	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Cisco 350	140	300	400	500
Orinoco Gold (Hermes)	65	225	400	500
Cisco CB-21 (a/b/g)；只测 802.11b 的性能	130	200	300	350

延迟扩展较大的网卡能够处理较严重的多径干扰。于此再次证明 Cisco Aironet 350 不愧是当今的超级网卡，相比较于采用 Hermes 芯片组的网卡，它可以容许两倍以上的延迟时间。

第十七章

802.11 与 Windows

不论你是直接跳过第三至十六章，还是已经读过所有理论性的章节，从现在开始，让我们卷起袖子，着手安装设备。

802.11管理接口的发展同样步上其他Windows应用程序的后尘。起初，每家厂商各自开发不同的用户接口。等到逐渐流行，Microsoft就将802.11的配置设定集成到操作系统里，将各家厂商的管理工具统合为一个整体结构。

从系统与网络管理人员的角度来看，802.11的操作与Ethernet并无不同。安装802.11驱动程序几乎和安装Ethernet驱动程序一样，而且无线网络接口的运作方式也几乎和Ethernet接口相同。802.11接口会产生ARP缓存，甚至其他软件也会将无线接口视为Ethernet接口。不过和Ethernet驱动程序不同的是，在802.11驱动程序中有一些高级的选项与功能，其中包含了第八章所提到的额外管理功能。

本章主要探讨如何在Windows XP与Windows 2000操作系统上设定无线网卡。个人强烈建议使用Windows XP，除了使用上比较容易，也因为它实际上额外支持了一些较新的协议。第三方（third-party）的认证申请者（supplicant）通常会将系统内置的认证申请者停用。不过，有时候驱动程序会拒绝使用Microsoft安全协议栈（security stack）以外的安全系统。

Windows XP

Windows XP延续了视窗操作系统长久以来的传统，将原本只由第三方所提供的功能集成到操作系统中。Microsoft打造了一个标准的配制设定工具，能够设定大多数网卡，称为Windows Zero Configuration（也称为ZeroConfig、ZeroConf或WZC），不再依赖802.11网卡厂商自行提供的设定工具。尽管网卡厂商还是必须提供驱动程序，不过配置

设定则交由一致的窗口界面处理，不再通过个别网卡所提供的设定程序。本节之所以探讨ZeroConfig，是因为它呈现出了一种与网卡无关的配置设定观点，因此得到网管与客服人员的青睐。

安装网卡

着手安装网卡之前，最好从网卡厂商的网站下载最新的驱动程序。其他网络技术远比802.11成熟，所以不用经常更新驱动程序。遗憾的是，无线领域的产品随时推陈出新，驱动程序的变动也因此十分频繁。

在主要厂商的网站上，通常可以找到“support”（产品支持）或者“download”（软件下载）的网页。有些规模较小的厂商只是将公版（reference design）重新包装，也许并未在网站上提供驱动程序。遇到这种情况，通常可以使用芯片组厂商所提供的公版驱动程序。

有些驱动程序包在安装程序里面，我通常避而不用。有些网卡厂商会另外支付许可证，使用第三方所开发的802.1X协议栈，不过可能会与ZeroConf相冲突。安装网卡之前，最好的做法通常是从网卡厂商的网站取得最新的驱动程序。

第三方的802.11X协议栈与驱动程序更新过程

市面上有许多第三方（third-party）所开发的802.1X协议栈。在Windows操作系统上，它们通常被实现成网络协议栈的一层，在硬件与网络协议之间拦截EAPOL帧。有些网卡厂商无法忍受内置的Microsoft supplicant开发进度的落后，转而采用第三方所提供的协议栈来支持802.1X。许多第三方所开发的协议栈与ZeroConfig并不兼容。它们通常需要额外的软件设定工具，并非通过ZeroConfig来设定参数。这些协议栈可能也需要额外的认证申请者（supplicant）软件来支持比较高级的协议。

要避免使用这些附带的802.1X协议栈，更新驱动程序时就不要使用厂商所提供的安装程序。最好的做法是从厂商的网站下载驱动程序，解压缩后利用设备管理器（device manager）的更新驱动程序按钮为操作系统更换新版驱动程序。图17-1显示了如何仅更新驱动程序。只要点击硬件属性页面的“Driver”标签页，就可以看到“Update Driver”按钮。

要避免安装第三方的802.1X协议栈有两个小技巧。有些驱动程序的可执行文件其实是自行解压缩的ZIP文件，可以用解压缩（*unzip*）软件开启。将驱动程序解压缩到临时文件夹，然后以个别文件进行更新。另外一种方法是以安装程序进行安装，然后立即运行卸载程序。大多数卸载程序只会移除配置设定工具以及第三方的802.1X协议栈，但会留下新版的驱动程序。

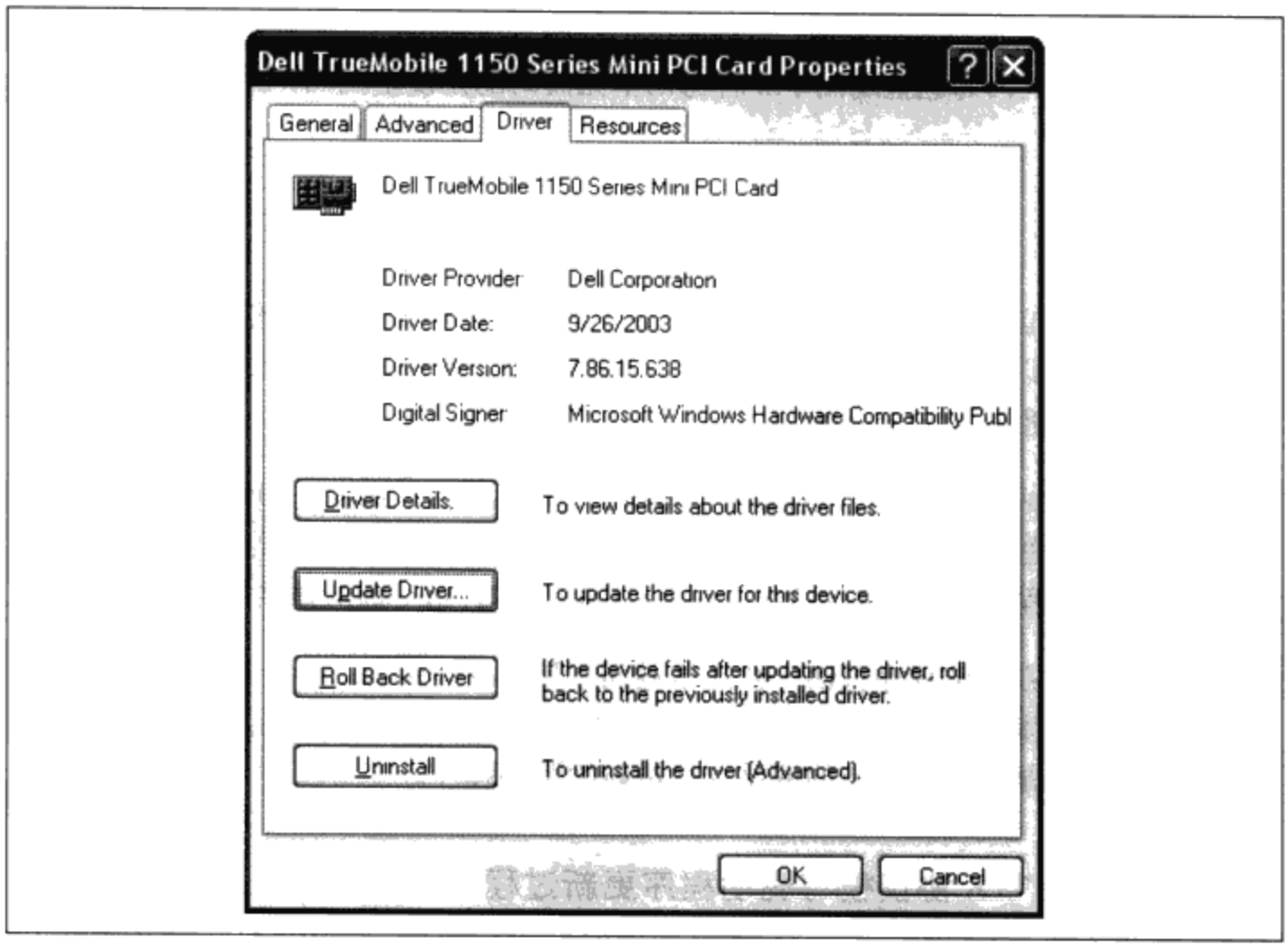


图 17-1：只更新驱动程序

Cisco 客户端软件

Cisco 网卡还有另外一个隐患。保护型 EAP（Protected EAP，简称 PEAP）是仍在开发中的标准。虽然它由 Cisco 与 Microsoft 双方代表所制定，但两家公司的实现版本并不兼容。业界所发布的大多数 PEAP 产品通常会自动检测系统使用的是哪个版本（注 1）。甚至连 Cisco 的认证服务器 CiscoSecure ACS 中也有一个选项，可以设定与 Microsoft 的 PEAP 实现兼容。

Microsoft 的 PEAP 实现版本支持以 EAP-MS-CHAP-V2 与 EAP-TLS 作为内层身份验证协议（inner authentication protocol）；Cisco 的 PEAP 实现版本则支持 EAP-SIM 与 EAP-GTC。大部分使用 Windows 的组织会倾向使用现有的用户数据库，例如 Active Directory，如此一来，就只能以 EAP-MS-CHAP-V2 作为内层身份验证协议。

作为软件包的一部分，Cisco 会以本身的 PEAP 软件取代系统所使用的标准（Microsoft）PEAP。如要使用 Microsoft PEAP，必须先移除 Cisco PEAP 驱动程序，然后以 Microsoft

注 1: Funk 与 Meetinghouse 客户端软件均可自动检测，Radiator RADIUS 服务器亦然。

PEAP取代。由于整个系统只能使用一套PEAP软件，因此安装Cisco PEAP会影响当前系统中所有的卡，而不只是Cisco的网卡。参见表17-1。

表17-1：内层EAP的认证方式

EAP认证方式	Cisco或Microsoft PEAP?	身份验证证书	备注
EAP-MS-CHAP-V2	Microsoft	共享密码（或者密码的MD4散列值）	用于Windows域的身份认证；易搭配Active Directory
EAP-TLS	Microsoft	用户证书	通常不用
EAP-SIM	Cisco	用户识别模块（SIM）卡	GSM移动电话身份验证方式；尚未广泛使用
EAP-GTC（一般令牌卡）	Cisco	通过加密隧道（encrypted tunnel）传送的明文验证字符串	可用于令牌卡以及作为通用的静态密码

有些膝上型计算机厂商已经在系统中预先安装好802.11网卡，而且也加载与设定好相关软件。如果配备Cisco网卡，系统中可能已经预先安装Cisco PEAP，那么你的组织就必须调整系统的构建过程，以便回头使用Microsoft PEAP。要回头使用Microsoft PEAP，必须重新安装最新的更新包（service pack），以Microsoft的PEAP驱动程序覆盖Cisco的PEAP驱动程序。

选择网络

Windows启动后，ZeroConfig系统就会尝试找出附近的所有网络。ZeroConfig会自动连接到目前已有配置文件的网络。如果尚未设定任何网络，无线接口上将会出现如图17-2所示的气泡（bubble）窗口。

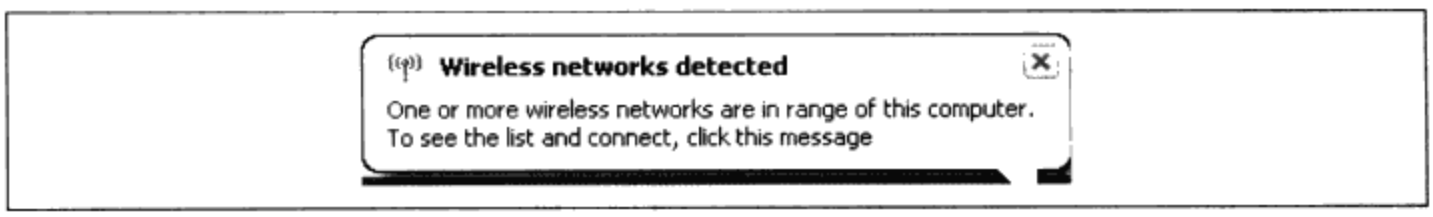


图17-2：提示侦测到了附近的无线网络

只要点击该窗口或者以右键点击无线接口并选取“View Available Wireless Networks”，就会列出所检测到的无线网络（图17-3）。任选其中一个网络加入，Windows就会自动

尝试正确的配置设定。不过，它无从选择适当的EAP认证方式，因此通常不能自动连接至加密网络。连接到未加密的网络十分容易，不过系统会提示即将连接至不安全的网络，要求用户确认。

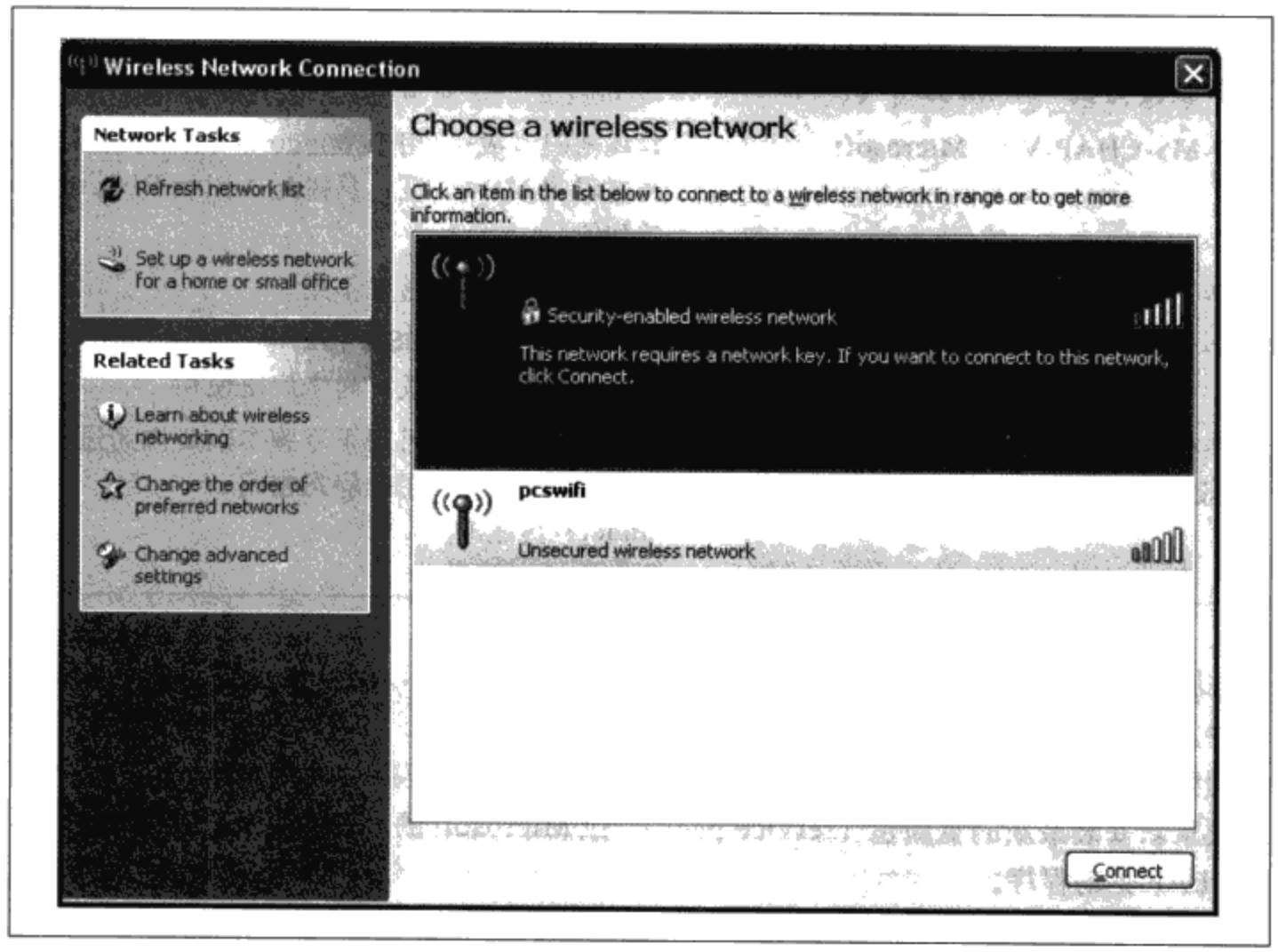


图 17-3：查看现有的无线局域网络

安全参数与 802.1X 的配置

有时候，网络的安全属性必须通过手动方式设定。Windows能够自动选用默认的加密与身份验证方式，不过还是可能出错。802.1X通常默认使用EAP-TLS，虽然EAP-TLS并不常用。要更改安全参数，可以点击“Change Advanced Setttings”进入接口属性页面，然后点击“Wireless Network”标签页（图 17-4）。

要新增一个网络，可以点击“Preferred Networks”，然后选择“Properties”，或者也可以指定一个网络名称然后手动加入，如图17-5所示。如果要手动加入网络，必须从头开始设定正确的属性。如果Windows已经自动设定好网络，它将会从可用的协议中挑选安全性最高者。

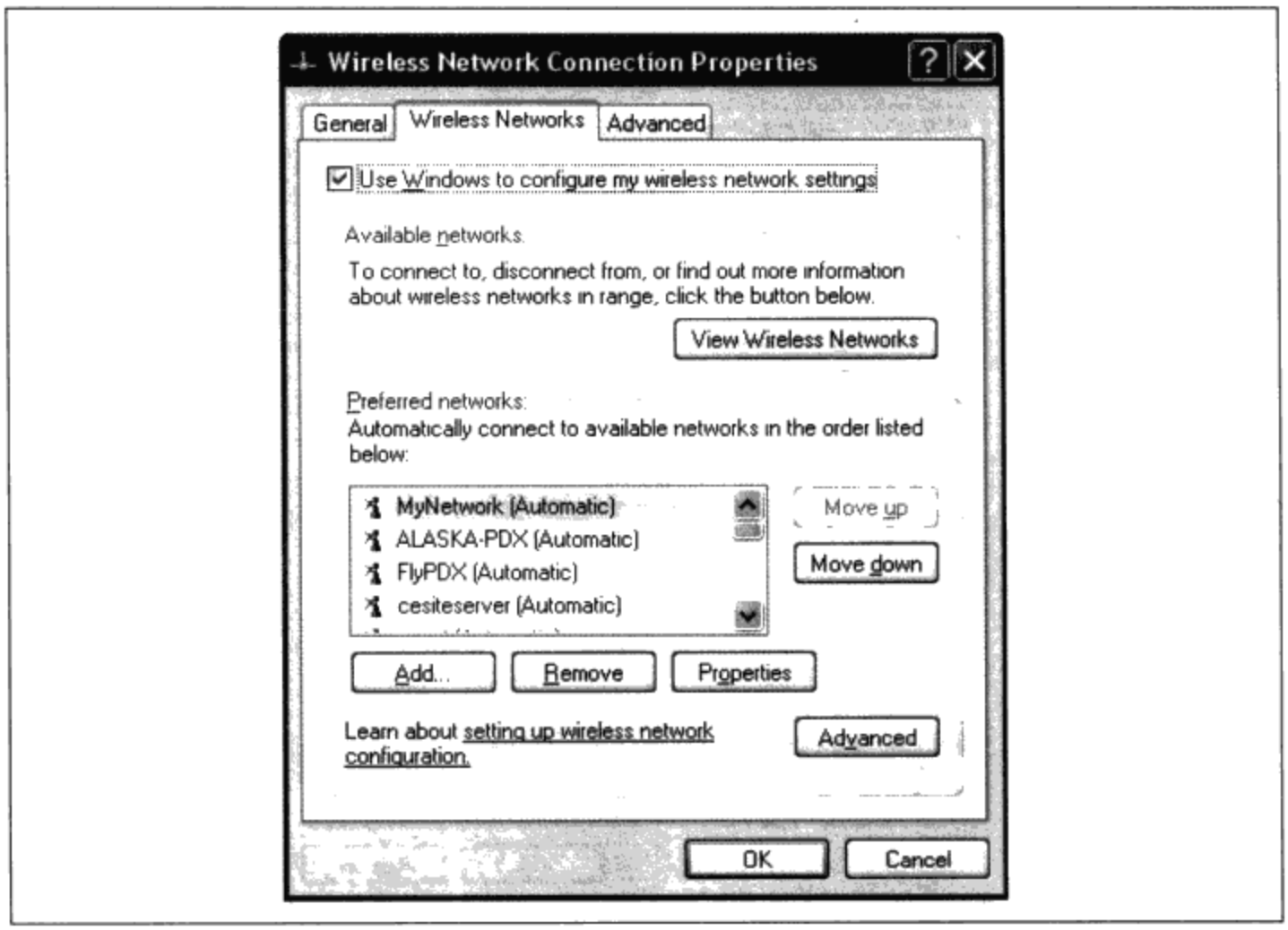


图 17-4："Wireless Networks"标签页

ZeroConf的优点之一，就是可以同时维护多个不同无线局域网络的属性，然后连接至已经设定无误的网络。

首先必须决定的是你打算使用的身份验证类型。图 17-5 中只显示出WPA，不过其实有四种选项：

Open authentication（开放系统身份验证）

用于完全不进行身份验证以及使用旧式动态WEP的网络。使用这个选项，代表一开始所进行的链路层身份验证使用的是第八章所描述的开放系统验证方式。实现开放系统验证的网络可以搭配 802.1X，但非必要。

Shared authentication（共享密钥身份验证）

这个选项用于以共享密钥WEP进行身份验证的网络。它会要求用户在"Network Key"字段输入密钥。以共享密钥WEP进行身份验证并不是十分牢靠，也无法提供严密的保护。除非所要连接的接入点要求，否则没有理由使用这个选项。

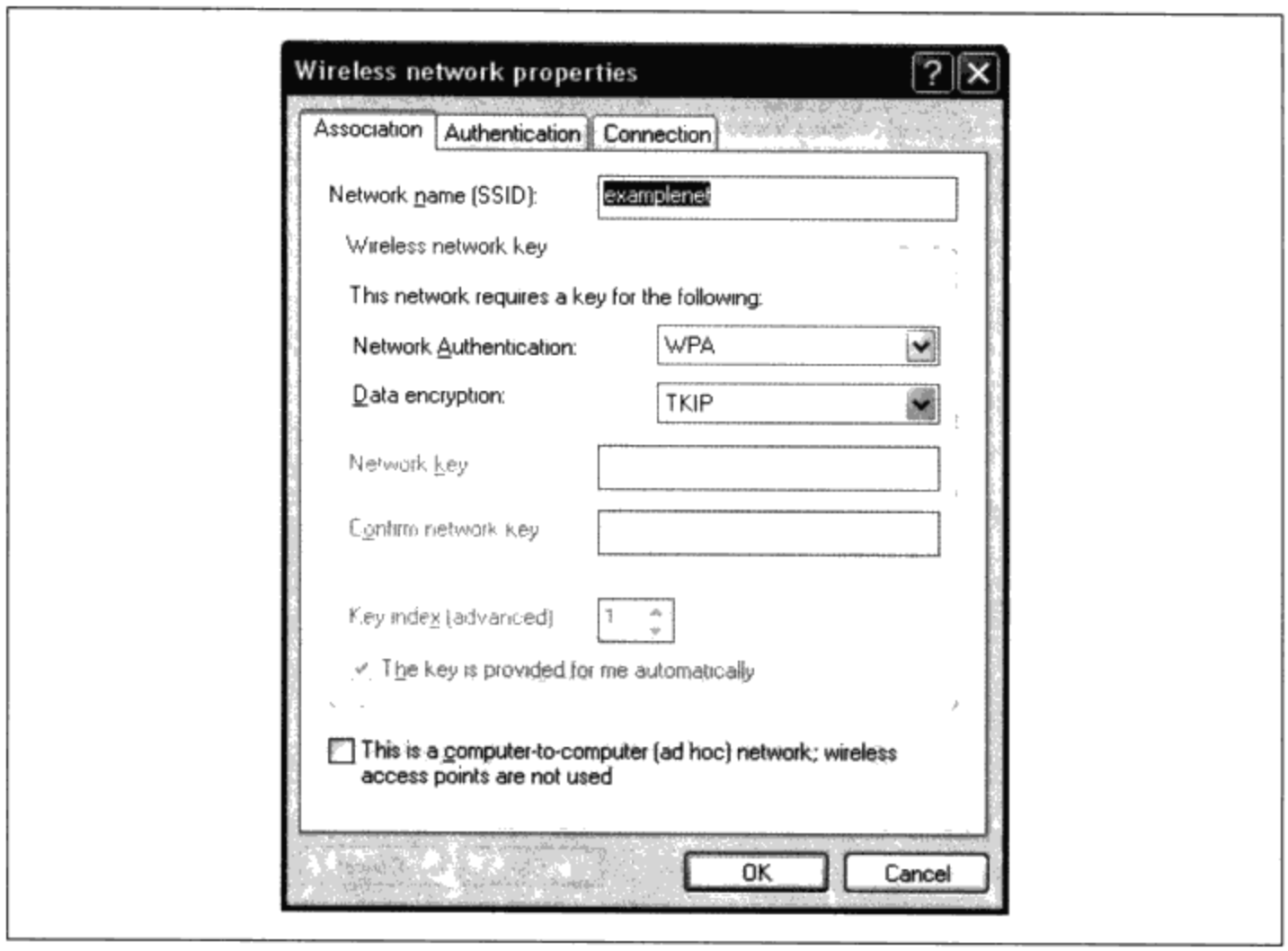


图17-5："Association"属性标签页

WPA authentication（WPA身份验证）

这是WPA Enterprise的简称。它使用802.1X进行用户身份验证，同时使用802.11i所定义的验证密钥模式。除非已经安装WPA软件且驱动程序支持WPA，这个选项才会出现。

WPA-PSK authentication（WPA-PSK身份验证）

这是WPA Personal的简称。此验证方式使用预共享主密钥（preshared master key），而非使用衍生的主秘钥（master secret）。链路加密密钥是由此预共享密钥以及客户端与接入点之间所交换的随机值所衍生。

选好身份验证方式之后，接下来需要选择链路所使用的加密方式。

Disabled（停用）

这个选项用于不采用链路层加密的开放网络。有些802.11热点（hot spot）会使用这个选项，虽然未来应该会提供较坚固的加密方式。

WEP

这个选项包括手动与动态密钥。要使用动态 WEP，则勾选“The key is provided to me automatically”选项。手动设定 WEP 密钥则不需勾选这个选项，只要输入密钥即可。

TKIP

这个选项用于 TKIP，这是 WPA 网络的默认值。

AES

Windows 并未提到 CCMP，在 ZeroConf 配置中是以 AES 称之（注 2）。这是目前无线网络上最坚固的加密方式。

此对话框也提供手动输入密钥或者使用自动提供密钥的选项。使用802.1X时会自动提供密钥，所以这个选项就不让用户勾选。使用WPA身份验证的网络必须使用自动密钥；使用WPA-PSK的网络则必须在此输入预共享密钥。表17-2整理出了目前已支持的加密与身份验证选项。

表17-2：加密与身份验证方式一览表

身份验证框架	所支持的加密方式	身份验证方式
Open	Disabled（不使用 WEP）	802.1X 为非必要的
	WEP（指定密钥）	
	WEP（自动提供密钥）	
WPA	WEP（自动提供密钥）	802.1X 为必要的
	TKIP	
	AES（视网卡是否支持）	
WPA-PSK	WEP（自动提供密钥）	不使用 802.1X
	TKIP	
	AES（视网卡是否支持）	

设定好 Association 属性后，接下来设定 Authentication 属性。图 17-6 所显示的“Authentication”属性标签页是用来选取EAP认证方式的画面。画面中显示这部机器有三种选项：PEAP、EAP-TLS（“Smart card or other Certificate”）以及TTLS（“SecureW2”）。点击“Properties”按钮之后，接着对所选的EAP 认证方式进行设定。

注 2： 或许是因为知识产权的考虑，导致最后以 AES 加密算法取代 802.11i 草案时期所使用的 CCMP。

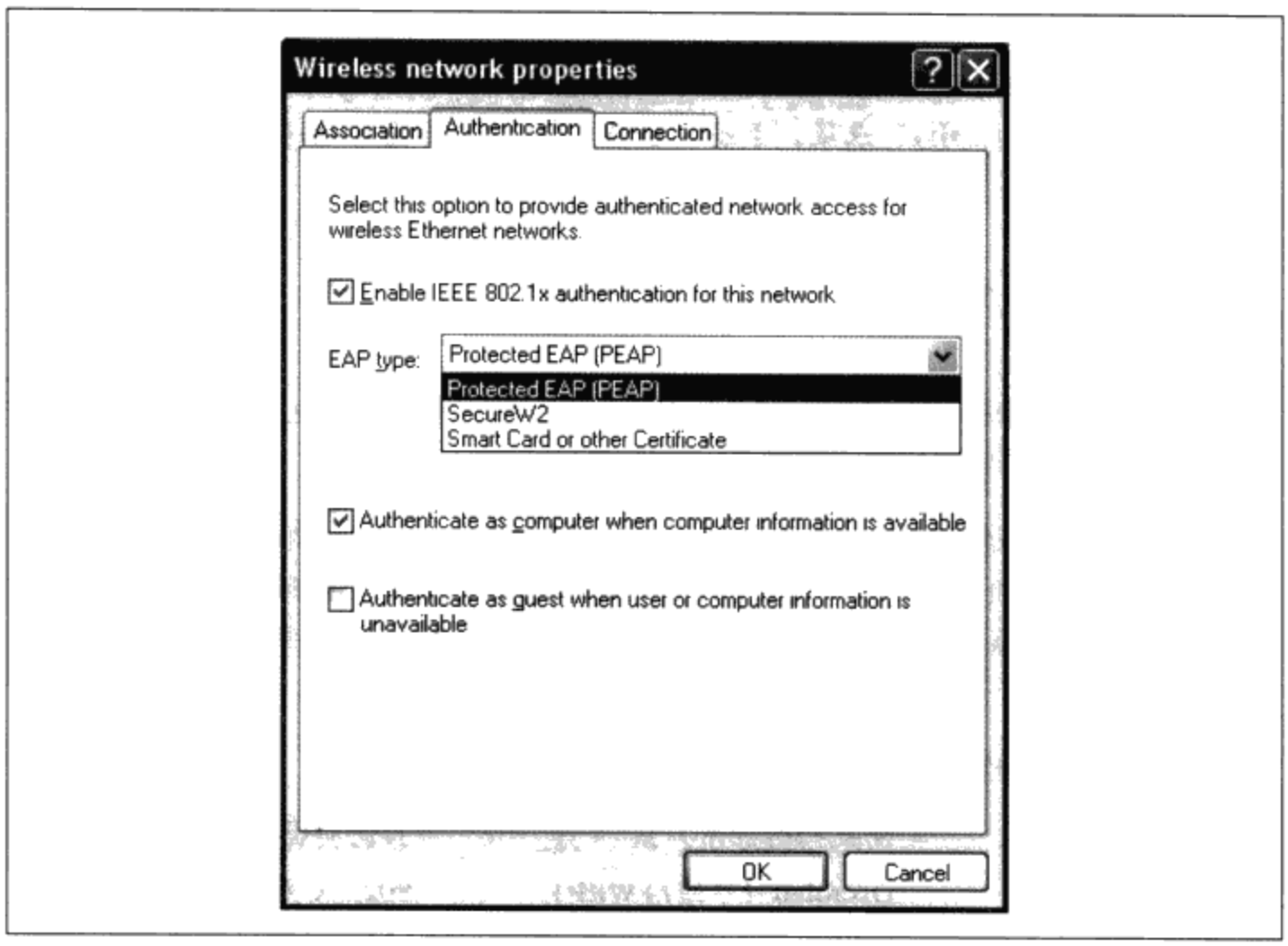


图 17-6："Authentication"属性标签页

在"EAP type"选项框下面，有一个"Authenticate as computer when computer information is available"复选框。勾选这个项目表示允许系统在网络上使用机器凭证（machine credential）进行身份验证，如此可以在验证用户之前，让 Windows 域进行一些必要的操作。此过程的运作方式将留待本章稍后探讨。

设定 EAP 认证方式

虽然可以在"Authentication"标签页选择一种 EAP 认证方式，但配置设定还是通过点击"Properties"按钮来进行。并非所有出现在"Authentication"属性标签页的认证方式均由 Microsoft 提供。第三方所提供的软件也会在下拉式菜单中加入其他 EAP 类型。"EAP type"选项框中所显示的文字可用来判断目前究竟使用的是 Microsoft 还是 Cisco 的 PEAP。Microsoft PEAP（技术上称为 PEAPv0）显示为"Protected EAP (PEAP)"，而 Cisco PEAP 仅显示为"PEAP"。

EAP-TLS

图 17-7 显示了选用 EAP-TLS 时所出现的设定画面。最上方的选项指出用来验证用户的客户端证书（client certificate）究竟存储于智能卡还是由 Windows 所维护的证书存放区（certificate store）。大型机构会发智能卡给员工，有时就嵌入在员工识别卡当中。中小型公司则比较倾向于发行机器证书（certificates stored on each machine）。

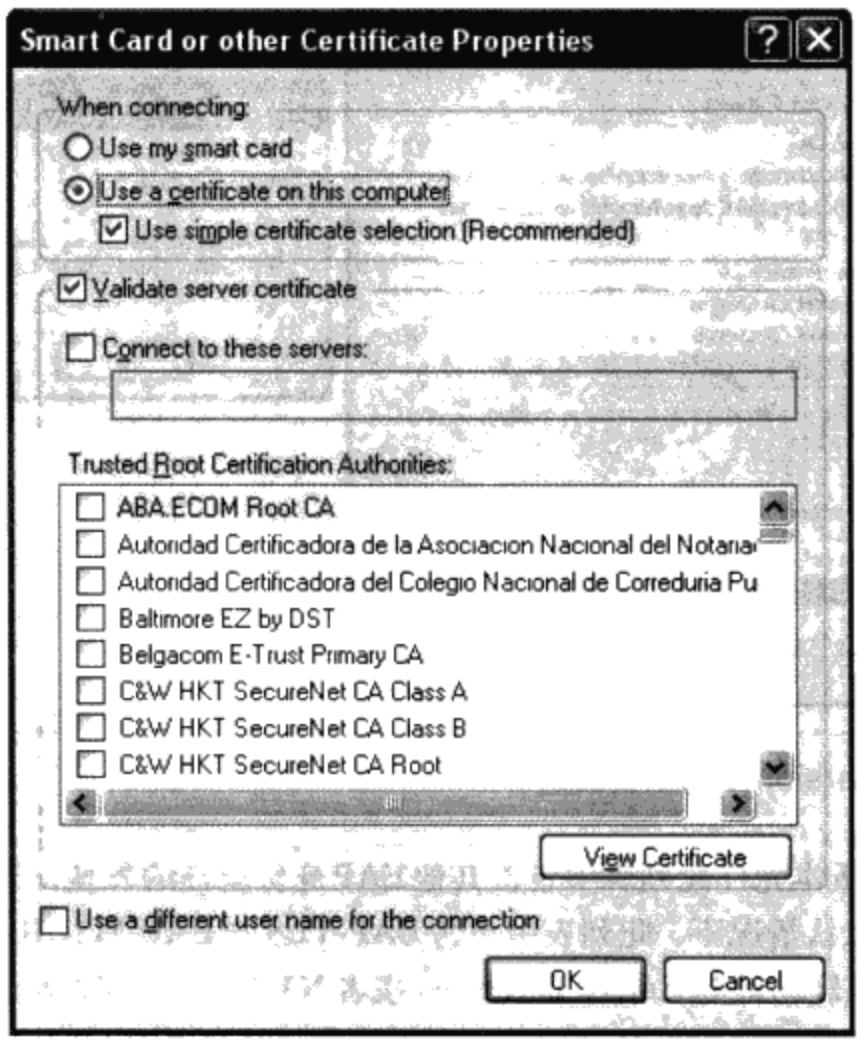


图 17-7：EAP-TLS 的配置设定画面

服务器验证是打造安全网络的关键。Microsoft 认证申请者允许两种不同层次的身份验证。当认证服务器对客户端展示证书时，客户端可以验证该证书是否发行自可信任的证证机构。如果使用自行签署的证书，就不该勾选这个“Validate server certificate”。如此一来，认证申请者便会信任所收到的任何证书，门户便因此而洞开。验证列于服务器证书上的名称以确定它的确来自已知的 DNS 域，可提供额外的保护。

PEAP version 0

图 17-8 所显示的 Microsoft PEAP 配置设定与 EAP-TLS 类似。服务器验证不变，应该予

以启用。主要的设定项目是于保护隧道（protected tunnel）中所使用的内层身份验证方式（inner authentication method）。表 17-1 对这些选项有简短的说明。

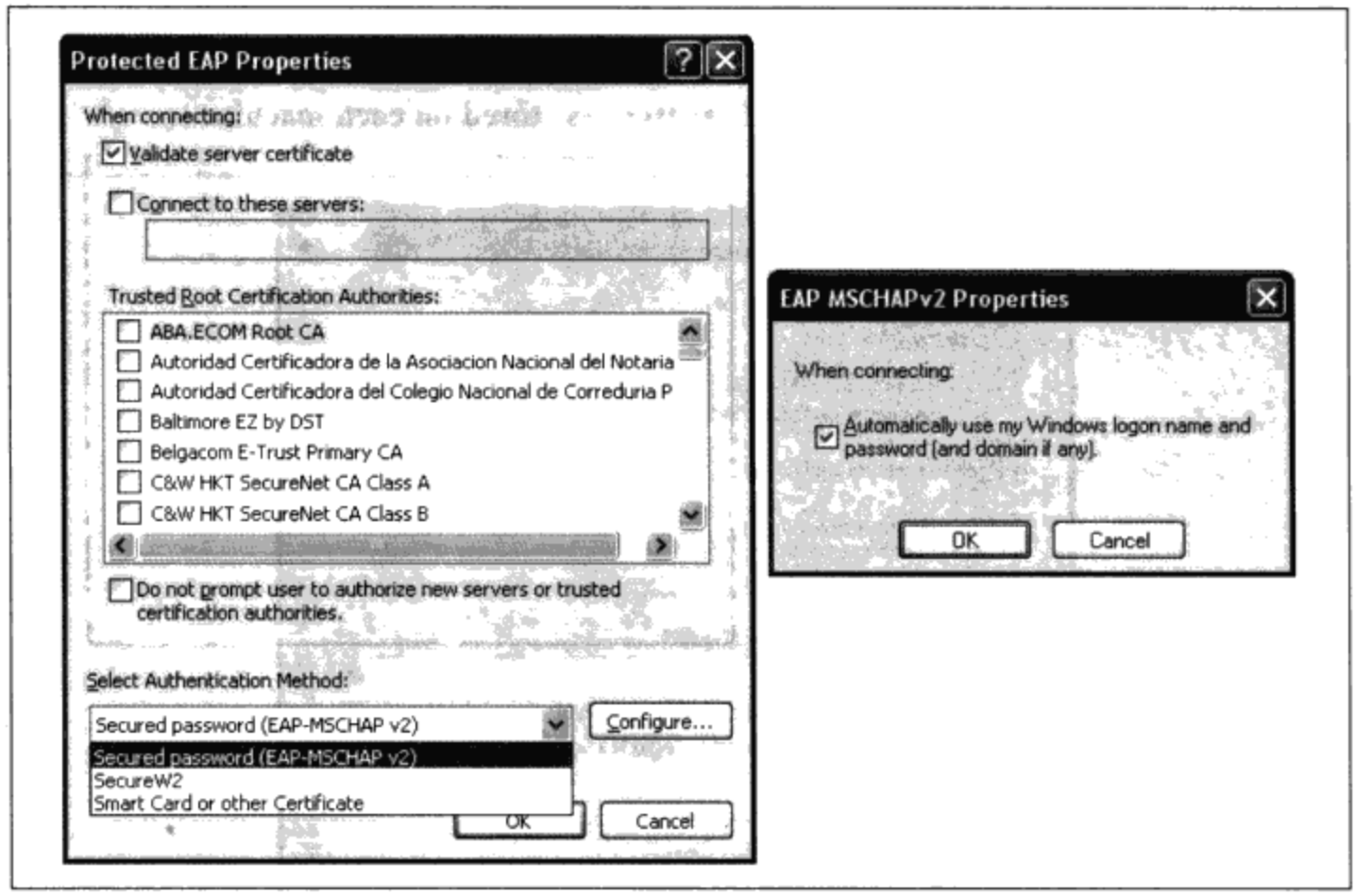


图 17-8：PEAP version 0 的配置设定

Microsoft的实现版本允许此列表中包含其他EAP身份验证的外挂（EAP authentication plug-in）选项。默认情况下，此列表中包含EAP-TLS与EAP-MSCHAP-V2。后者比较常见，因为它可以轻易地与Active Directory或者NT Domain用户账号整合在一起。每种内层身份验证方式都可以有自己的子设定页。以EAP-MSCHAP-V2为例，子设定页只有一种选项。一旦勾选这个选项，Windows登录证书（logon credential）将被自动转送至网络上。这个选项有时也称为PEAP单点登录（*single sign-on*），因为接下来认证申请者会自动送出登录证书，不会再提示终端用户输入账号密码。

清除系统注册表中的证书

如果不使用单点登录，用户的密码将会存储于系统注册表（registry）中。当用户首次连接至某个网络，系统便会提示用户输入用户名称、密码以及Windows域。如果身份验证成功，证书就会被保存在系统注册表中供以后使用。以后，每当用户选择与此网络连接，Windows就会自动传送之前已经验证成功的证书。

虽然十分方便，不过证书高速缓存功能还是有所不足，主要是缺乏一种便利的方式，可以清除不再需要的用户证书。许多无线网络采用现有的身份验证方式，然而大型网络通常均实行定期更换密码的策略。当密码被迫更新，系统注册表中的证书高速缓存就会因而失效，用户必须将它从系统注册表中清除之后才能变更密码。

用户证书存放在系统注册表的*HKCU\Software\Microsoft\EAPOL\UserEapInfo*下，如图17-9所示。不使用单点登录进行PEAP身份验证的网络接口会分别以不同的标识符来表示。标识符是一连串字母与数字所组成的长字符串。

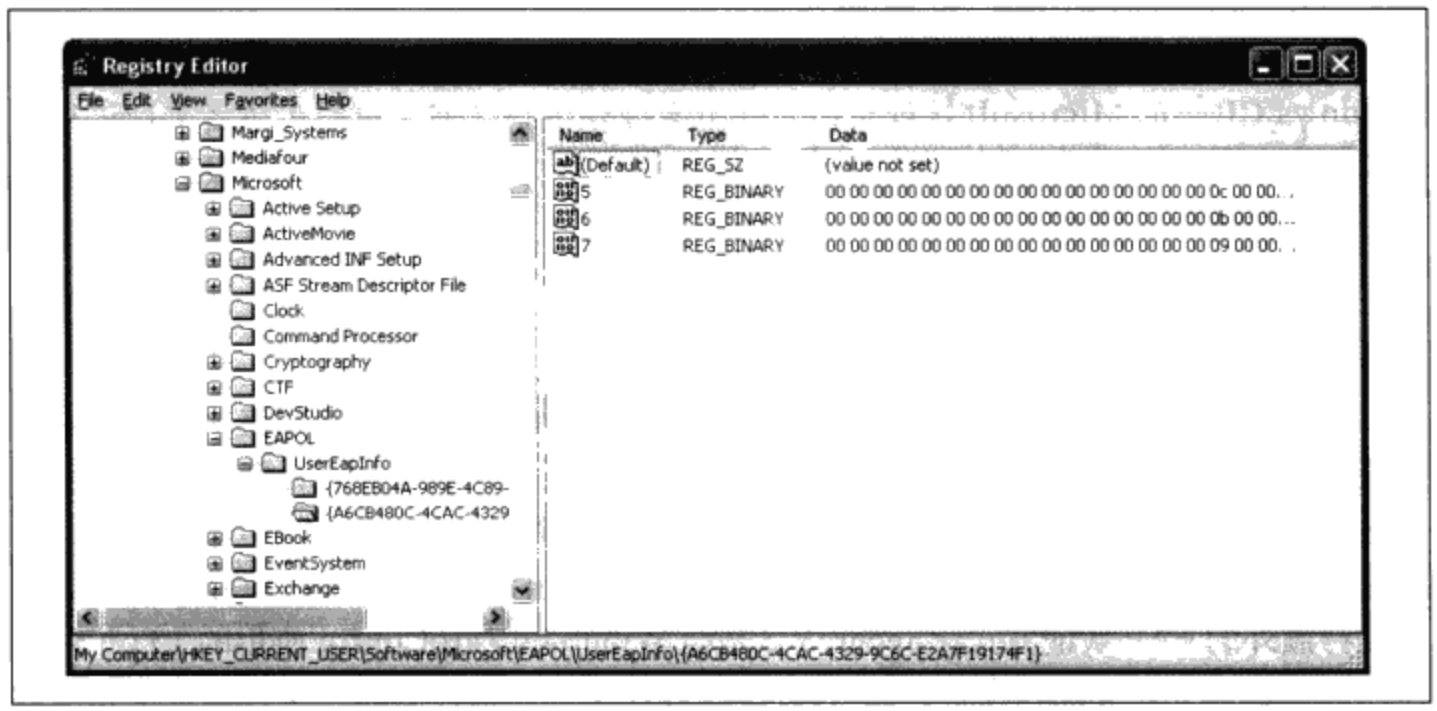


图 17-9：系统注册文件中所存放的用户证书

每个网卡均会有一个标识符。在图17-9中，标识符为{768EB04A-989E-4C89-9B85-93DF52F5EDE6}的接口存放了三个之前缓存的网络密码。要移除某个网络的缓存密码，可以删除相应的注册表键（registry key）。

要找出哪个字符串对应到哪个网络接口，请先找出*HKLM\Software\Microsoft\WindowsNT\CurrentVersion\NetworkCards*，然后查看该值底下的注册表键。图17-10显示该字符串对应到“ORiNOCO 802.11abg ComboCard Gold”。

将用户密码存储于系统注册表会有损要求用户输入密码的Windows认证申请者的可用性。Microsoft方面辩称密码缓存是相当方便的功能，用户可以不需要一再输入密码，同时也指出使用现有Active Directory用户账号与自动使用Windows证书的好处。不过，其他厂商所提供的认证申请者则是将用户密码存储在更方便访问的地方。

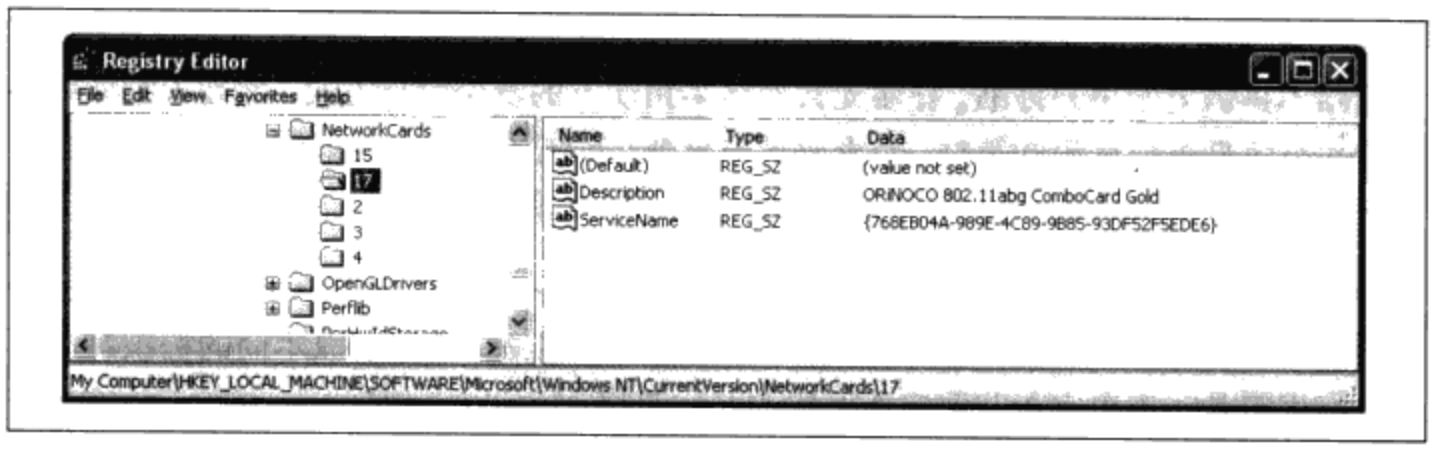


图 17-10：系统注册表中接口所对应的名称

Windows CE 上的 Microsoft 认证申请者并不会缓存用户证书。每当申请者重新进行身份验证时，就会提示用户输入证书（即账号密码）。大多数 Windows CE 设备并没有键盘，很难快速输入证书。

SecureW2: TTLS 与 ZeroConfig

第三方所提供的申请者软件让网管人员陷入困难的抉择。用户通常习惯使用Windows接口来设定无线网络，不过 TTLS 功能通常只能通过第三方所开发的软件提供，但是要使用这些软件却得停用ZeroConfig。所幸并非没有别的解决方案。ZeroConfig提供了一个编程接口（programming interface），可以通过实现特定认证方式的外挂程序（plug-in）来支持额外的EAP 认证方式。SecureW2 是给 Windows ZeroConfig 使用的TTLS 外挂程序。它是一个开放源码项目，以 GPL 授权方式发行。源代码与可执行包可从 *http://www.securew2.com* 下载。

要访问外挂程序SecureW2的配置设定，也是通过 EAP-TLS 与 PEAP 所使用的画面。初次点击“Properties”按钮时，SecureW2就会显示配置设定主画面（图17-11）。SecureW2的配置设定数据会被汇集到一个配置文件（profile）中。ZeroConfig所存储的每个无线网络均会关联到一个SecureW2配置文件。不同的网络可能分别关联到各自的SecureW2配置文件。管理人员可以使用安装程序包装工具（packaging tool）来产生所需要的SecureW2 安装程序（installer），将配置文件包含在安装程序中。

配置文件是由画面中四个标签页来定义的。其中，“Connection”标签页用来指定 TTLS 在第一阶段所使用的身份，如图 17-12 所示。如果不勾选这个项目，则第一阶段将会使用第四个标签页所指定的用户账号。外层身份（outer identity）默认会使用匿名（anonymous）选项。

服务器认证是通过第二个标签页“Certificates”来设定的，如图 17-13 所示。这里不会列出一长串的证书供用户挑选，用户必须自行输入每个认证中心（certificate authority）。

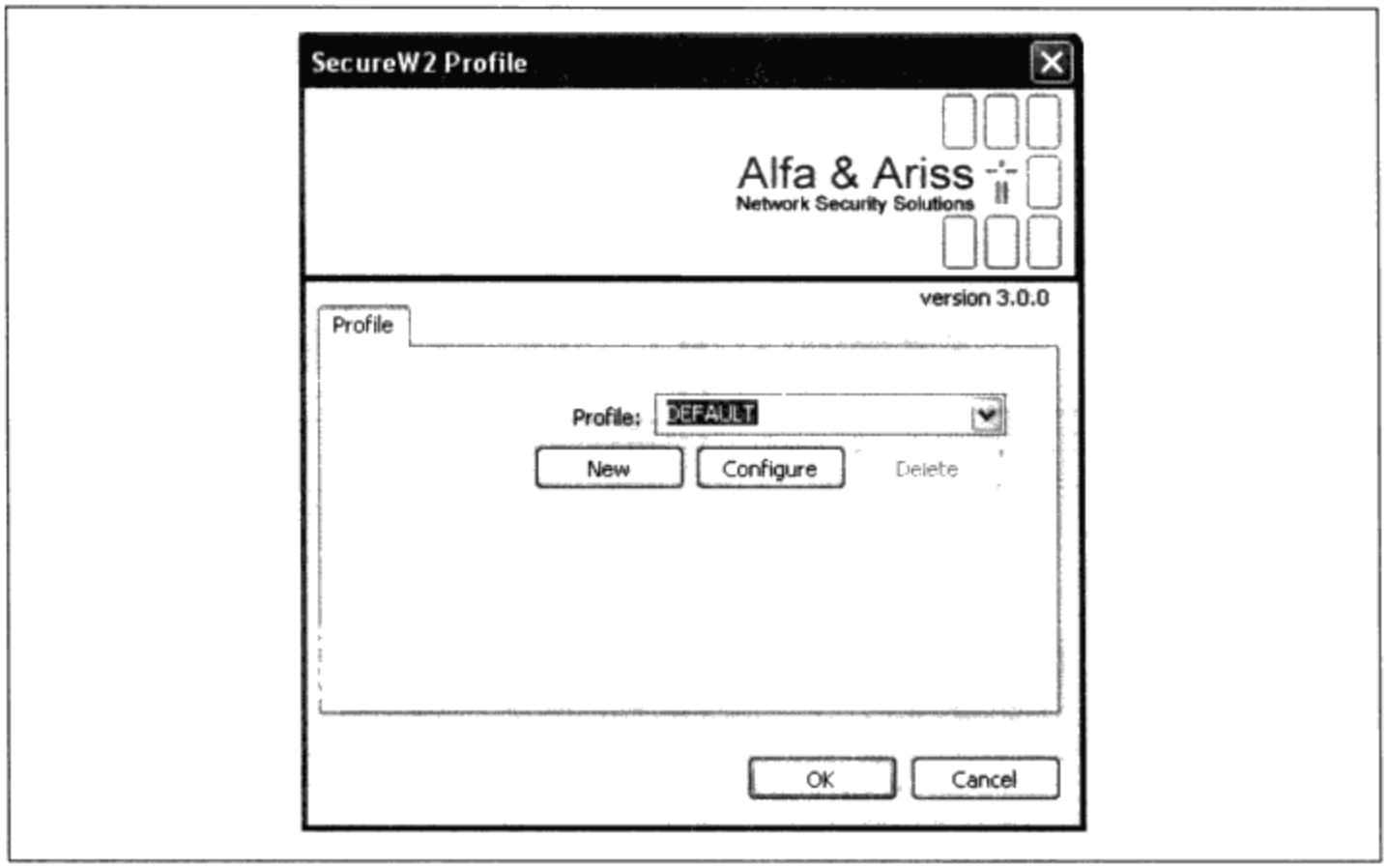


图 17-11：SecureW2 主画面

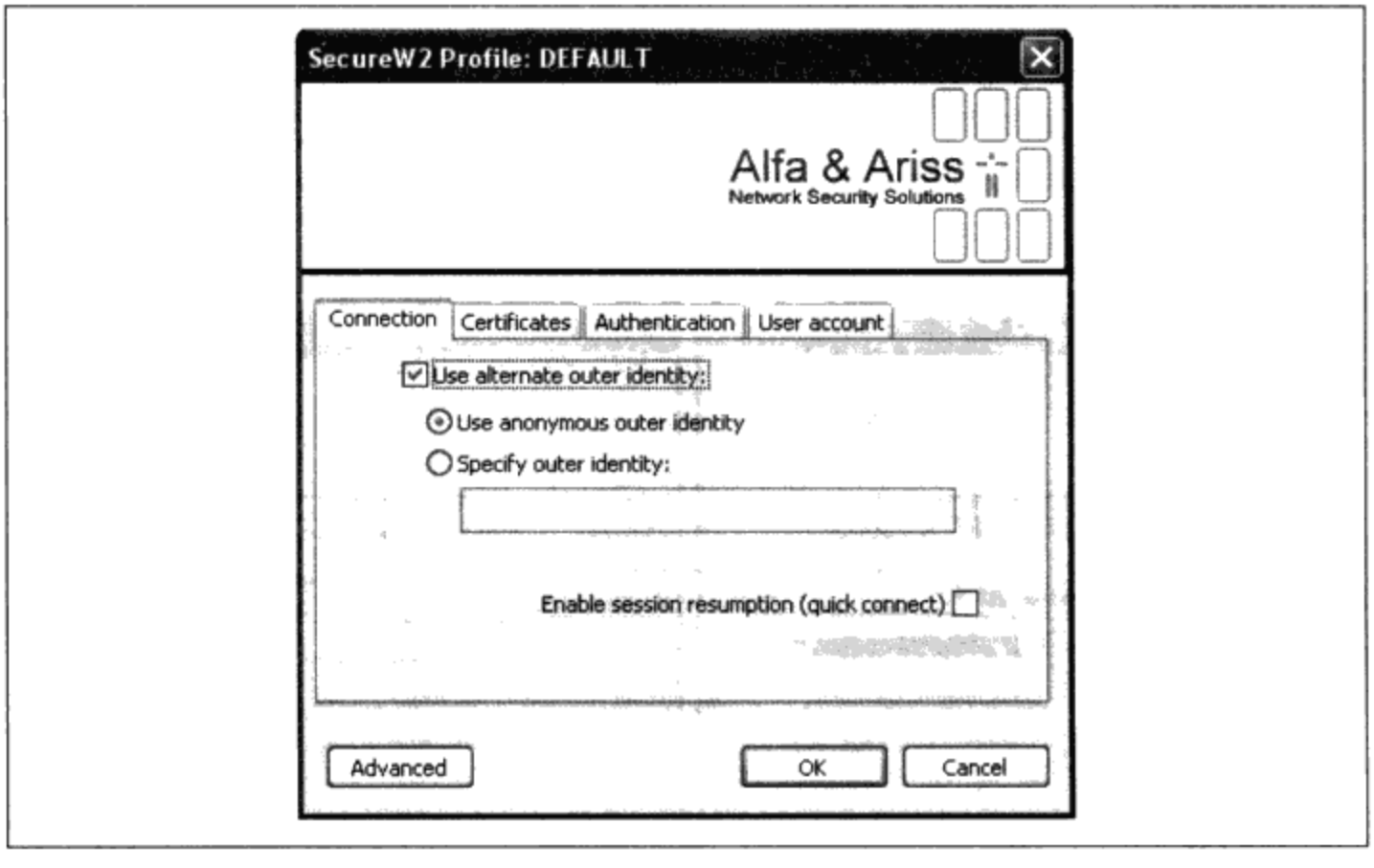


图 17-12：产生 SecureW2 配置文件

只要点击“Add CA”按钮就会显示证书授权单位的列表。在XP Service Pack 2中，此处所列的名单取自计算机的证书存放区（certificate store）。和Microsoft认证申请者一样，用户还可以验证证书中的服务器名称是否相符。

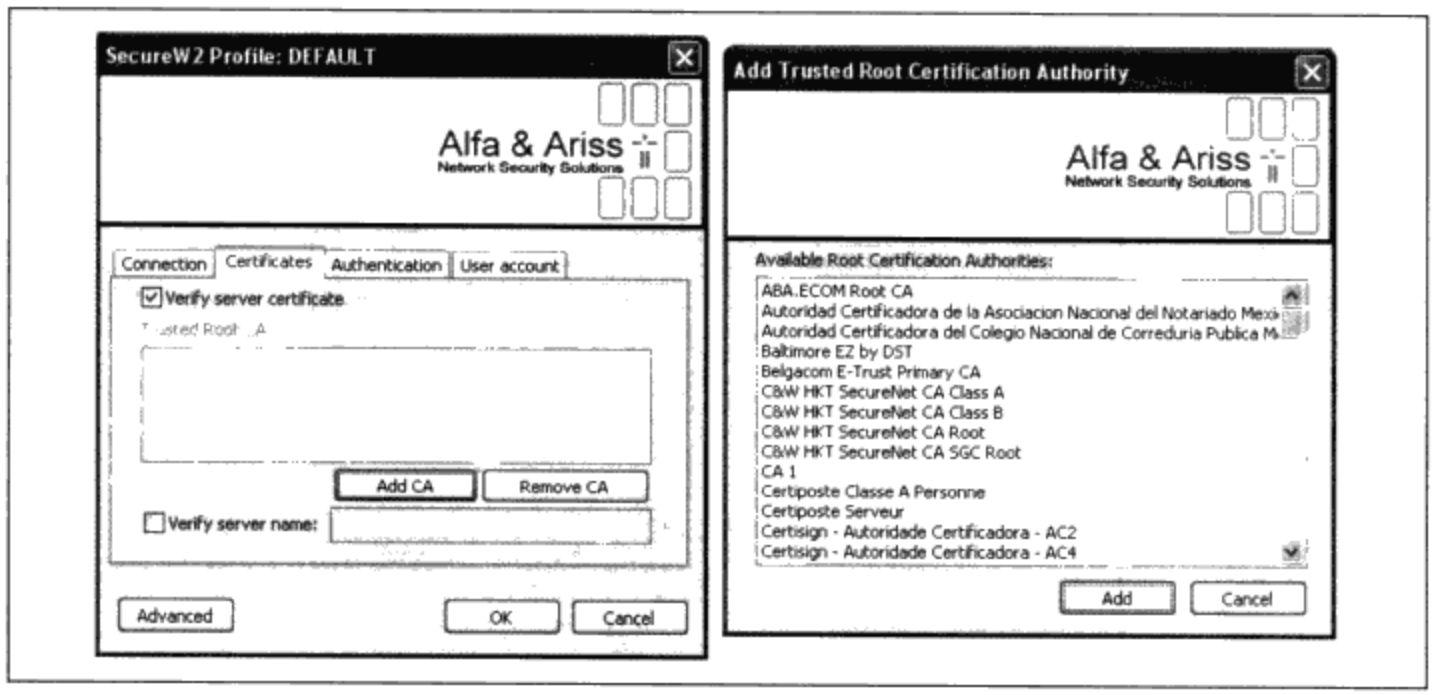


图17-13：SecureW2证书的配置设定

设定好外层用户名称与网络身份验证后，接下来就是设定内层身份验证所需要的用户账号。身份验证类型是通过“Select Authentication Method”下拉式菜单来设定的（如图17-14所示）。之所以使用TTLS，通常是因为需要使用明文密码进行身份验证。在这种情况下，必须将Select Authentication Method设为PAP。第四个标签页用来设定用户账号。

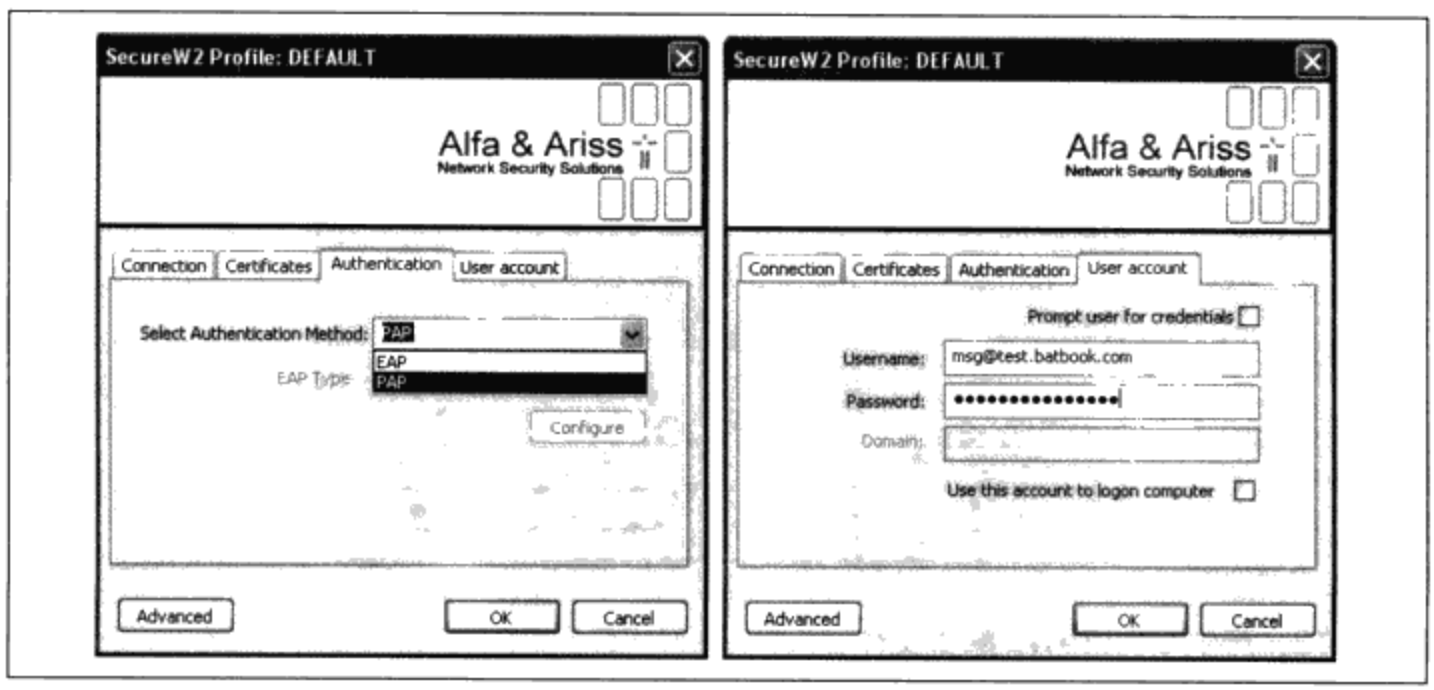


图17-14：SecureW2身份验证方式与用户帐号画面

WPA 的配置与安装方式

Wi-Fi 保护访问（Wi-Fi Protected Access，简称 WPA）是大多数组织所认可的安全底线。Windows XP Service Pack 2 内置 WPA，XP Service Pack 1 则需要另外下载补丁文件（patch）。使用 WPA，相当于在 WPA 与 WPA-PSK 这两种身份验证方式当中选择其一。Microsoft 并未在其他操作系统版本中实现 WPA，要在其他操作系统上使用 WPA，必须使用第三方的认证申请者软件。

要使用 WPA，必须得到整个系统的支持。除了操作系统，硬件及其驱动程序都必须支持 WPA。驱动程序不会显示未支持的选项。以 Dell TrueMobile 1150 无线网卡为例，并没有所谓的 AES 选项，因为该网卡只支持 RC4 加密。如果 WPA 在使用上不如预期，在联络厂商的客户支持部门之前，记得确认是否已经安装最新的驱动程序。

Windows 200

Windows 2000仍然广为使用。为了省钱，许多旧机器并未升级到Windows XP，Windows 2000 依然是可用的操作系统。Windows 2000 上的无线网络设定比 Windows XP 复杂，绝大部分是因为在无线网络的选择以及相应的安全设定上缺乏实质的整合。

从一开始，Windows 2000 就不支持 802.1X。802.1X 是在 Service Pack 3 之后才出现的补丁文件（patch）（注 3），后来集成到 Service Pack 4 中。Microsoft 并未将 WPA 功能移植到 Windows 2000，不过在 Windows 2000 上可以使用 Wireless Security Corporation（*http://www.wirelesssecuritycorp.com*）所开发的 WPA 客户端程序。有些观察家认为让 Windows 2000 支持 802.1X 算不上 Microsoft 的优先事项，如今它居然出现在最近发布的更新包中，显然，要说服用户升级操作系统已经越来越难。

虽然已经将802.1X的配置集成进驱动程序层，Windows 2000还是必须使用工具程序来设定系统所要连接的网络。对必须往返于加密与未加密网络的用户而言，这样特别容易造成问题。虽然使用工具程序进行网络切换很简单，不过通常需要手动启动或停用安全选项。Windows 2000 为网管人员带来困难的抉择。如果软件设定工具包含第三方所提供的 802.1X 协议栈，就必须额外付出精力来区分两者。

动态 WEP 的配置设定

Windows 2000的无线配置设定服务（Wireless Configuration Service）只支持动态WEP加密。至于TKIP，则必须通过第三方的申请者软件提供支持。要设定动态 WEP，必须

注 3：　如何下载此补丁文件，详见 Microsoft knowledge base article 313664。

通过网卡所提供的工具设定WEP密钥。网卡设定程序在乎的是目前是否使用手动设定的WEP密钥。驱动程序会将帧传给网卡并且使用网卡的密钥缓存中的密钥为之加密。不过，无线配置设定过程会依网络所设定的安全性策略将新的密钥塞进网卡。

手动WEP密钥无需加以设定，只要长度正确即可。在使用128位WEP的网络上，必须输入26个十六进制的数字作为密钥，例如12345678901234567890123456。这个假密钥（dummy key）永远派不上用场，因为802.1X身份验证成功后，就会被动态产生的密钥所取代。

就我经验所及，Windows 2000的无线配置设定服务不如Windows XP稳定。有些漏洞（bug）导致此服务即使在身份验证成功后依然会失灵。值得注意的是，这类情况所表现出的症状是初次连接可以成功，之后重新进行身份验证时连接就会中断。没有软件负责处理802.1X帧，任何尝试重新进行身份验证或者更换密钥的操作都将失败。

Windows计算机验证

当初设计Windows身份验证子系统时，是通过网络连接传送用户证书（user credentials）给域控制器（domain controller）来进行验证。当网络子系统开始运作，如果所使用的协议需要，就会取得一组网络地址，然后联系域控制器。除了验证用户身份，域还会提供若干其他的服务。网络管理人员可以定义域策略（domain policy），用来规范域内任何系统的行为，也可以定义登录脚本（login script），将自定义用户环境纳为登录过程的一部分。

在有线世界中，域服务不成问题。用户只要连上网络，系统本身就会开始发送封包。当初设计Windows启动程序时，还不存在任何方式可以对有线网络连接进行身份验证。然而，在无线世界中，用户必须通过身份验证才能启动无线连接，网络身份验证就有点变成“鸡生蛋，蛋生鸡”的问题。只要在登录窗口输入账号和密码，用户当然可以通过无线网络身份验证。不过，若一开始无网络连接可以将封包传送给域控制器，又如何验证这些证书呢？Windows NT、2000与XP以证书缓存提供部分解决方案。只要用户成功登录是Windows域成员的计算机，就会将用户证书置于缓存中供未来使用。

证书缓存只是部分的解决方案，因为这意味着必须先以有线方式登录计算机。Microsoft后来开发出比较好的解决方案，称为计算机证书（*computer certificate*）或机器证书（*machine certificate*）。当系统初次启动，计算机便向无线网络验证其身份。当无线网络开始启用并运作时，计算机就可以从域下载必要的信息，然后与域控制器进行用户身份验证。如此一来就算过去从未登录，系统中也不存在证书缓存，用户还是能够进行登录。

有相当多的功能都依赖是否可以在开机启动过程及早取得网络连接。除了域服务，网络磁盘驱动器映射（drive mapping）也进行得相当早，如果计算机没有通过身份验证，这些操作就会失败。在大多数情况下，Windows计算机验证都应该被视为网络能否运作顺畅的必要条件。

要使用 Windows 计算机验证，后端必须有部 Active Directory 服务器。每部计算机在 Active Directory 中必须有自己的账号，而且必须具备拨入权限（Dial-In permission）。

运作方式

计算机验证在开机过程中额外加入了 802.1X 身份验证过程。一开始计算机会先验明正身。从登录窗口取得用户证书（账号与密码）后随即进行802.1X交换，对用户进行身份验证。整个过程如图 17-15 所示。

本图说明了整个开机过程的主要步骤。当计算机开机并且启动它的网络系统时，便会开始此过程。进行其他系统启动任务的同时开始通过 802.1X 验证机器。

1. 机器验证开始。它可以始于申请者所发出的一个EAPOL-Start帧，也可以始于认证者所发出的一个 Request/Identity 帧。
2. 网络得知机器的身份。进行初次验证时，“用户”（机器）身份是以`host/ComputerName.ActiveDirectoryDomain`的格式出现，`ComputerName`与`ActiveDirectoryDomain`可以通过系统属性得知。
3. 计算机与RADIUS服务器上的计算机账号（或是RADIUS服务器后面的数据库）进行验证。这个过程或许需要来回进行多个回合，因为必须交换证书、产生加密密钥等。

   计算机验证与用户验证使用相同的EAP 认证方式。如果用户验证使用 EAP-TLS，则计算机也必须有自己的证书；如果用户验证使用 PEAP，计算机则会使用EAP-MSCHAP-V2作为内层认证方式。内层认证所使用的“密码”是在计算机加入域时产生的，其他软件无法使用。
4. 一旦验证成功，计算机就会与网络连接。它会从认证者方面接收到EAP-Success帧，在无线局域网络上则是接收到 EAPOL-Key 帧，提供连接所需要的密钥。

   验证完成后，计算机就会与网络连接并且可以收送封包。送出DHCP请求之后，计算机就可以加入网络并且通过 NetBIOS over TCP/IP 找到最近的域控制器。在开始进行用户身份验证之前，计算机可以跟域控制器建立一种关系。用户按下Control+Alt+Delete组合键开始登录过程。系统将会通过其与域控制器的连接加载用户登录脚本（user login script）、设定 Windows 域策略以及进行其他登录操作。

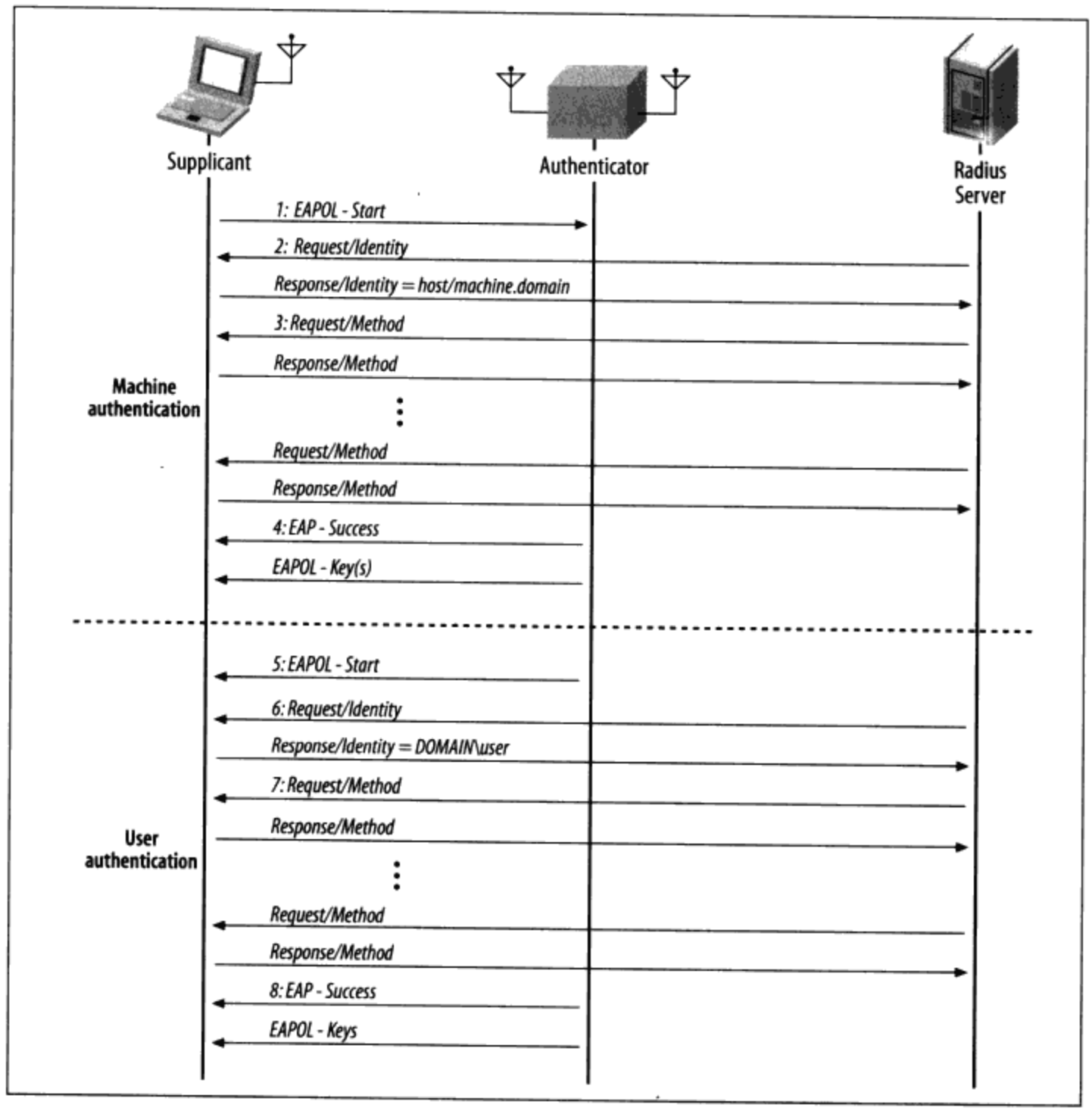


图 17-15：运行 Windows 计算机验证的开机过程

5. 当用户桌面即将启动时开始进行第二道身份验证。终端用户的身份验证必须由操作系统启动。通常，一开始所建立的机器验证只会被使用几分钟，之后就开始进行用户身份验证。

6. 网络要求终端用户表明身份。在 Windows 网络上，通常采用 *DOMAIN\user* 形式的身份格式，其中包含 Windows NT 风格的域名以及用户账号。

7. 申请者以用户证书进行身份验证。就 Windows 申请者而言，计算机验证与用户验证必须使用相同的 EAP 外挂程序。和上一个步骤相同，必须经过几个回合，才能够建立安全的加密信道。

8. 用户验证成功，同时取得连接所需要的密钥。这些密钥有别于计算机密钥，因为来自不同的TLS 会话（session）。

计算机验证和用户验证可以分开处理。这两种验证的授权可以各自进行。例如，在动态指定VLAN的网络中，可以分别为计算机账号与用户账号指定不同的VLAN。早期版本的Microsoft申请者在验证成功后不会触发DHCP请求，从而造成用户无法收送封包。目前已有补丁程序可以解决这个问题。

第十八章

802.11 与 Macintosh

Apple Computer 向来是 802.11 设备市场上开疆辟土的主要造势者。大部分 802.11 厂商在标准委员会的参与以及技术开发方面有所贡献。Apple 的贡献则是以简驭繁，将复杂的技术萃炼为易用的形式并发挥大众营销的专长。

1999 年时，802.11 技术相当被看好，也在一些应用市场中证明其价值。当时，802.11 接口卡的售价约为 300 美元，接入点则叫价 1000 美元左右。Apple 看出 802.11 技术的发展潜力，因此态度十分积极，推出价格只有 300 美元的接入点以及 99 美元的接口卡。当竞争者突然以三分之一的价格介入市场，其他厂商只好大幅降价以为应对，整个市场随即起飞。从那时起，价格就开始一路下跌。

Apple 以 AirPort 作为无线网卡的品牌名称。第一代 802.11b 网卡就叫做 AirPort，新一代的 802.11g 硬件则称为 AirPort Extreme（由于 Apple 主推 SOHO 市场，因此并未销售 802.11a 的相关产品）。本章将只讨论 AirPort Extreme 产品，不过两者在配置设定与管理方面的差异不大。不论是无线接口还是 Apple 802.1X supplicant（认证申请者），其设定均十分容易。802.1X supplicant 首度出现于 OS X 10.3，不过大家可能比较熟悉这个版本的代号：Panther。

AirPort Extreme 网卡

Apple 所提供的系统整合程度相当高，因为软硬件在设计上完全由自己实现。和纷乱的 IBM 兼容系统不同，Apple 必须完全为软硬件负责，而他们的确办到了。几分钟内用户即可安装好软硬件并且连上现有网络。如果在系统安装过程中将 AirPort 网卡插入，上述步骤就会被整合到初次配置设定过程中。

软件安装

OS 9.1 之后的操作系统均内设 AirPort 驱动程序，因此无需下载与安装驱动程序。系统第一次启用之前，如果已经安装 AirPort 网卡，首次启动配置设定工具就会让用户设定 AirPort 接口卡，选择所要使用的网络名称以及 TCP/IP 相关设定。如果使用 DHCP，整个设定过程只需几个画面而已。

已经启用的系统若要加装 AirPort 网卡，可以稍后使用 AirPort Setup Assistant 程序（注 1）来加以设定。插入网卡后，运行 Setup Assistant 程序。程序开始运行后，可看到如图 18-1 所示的对话框。

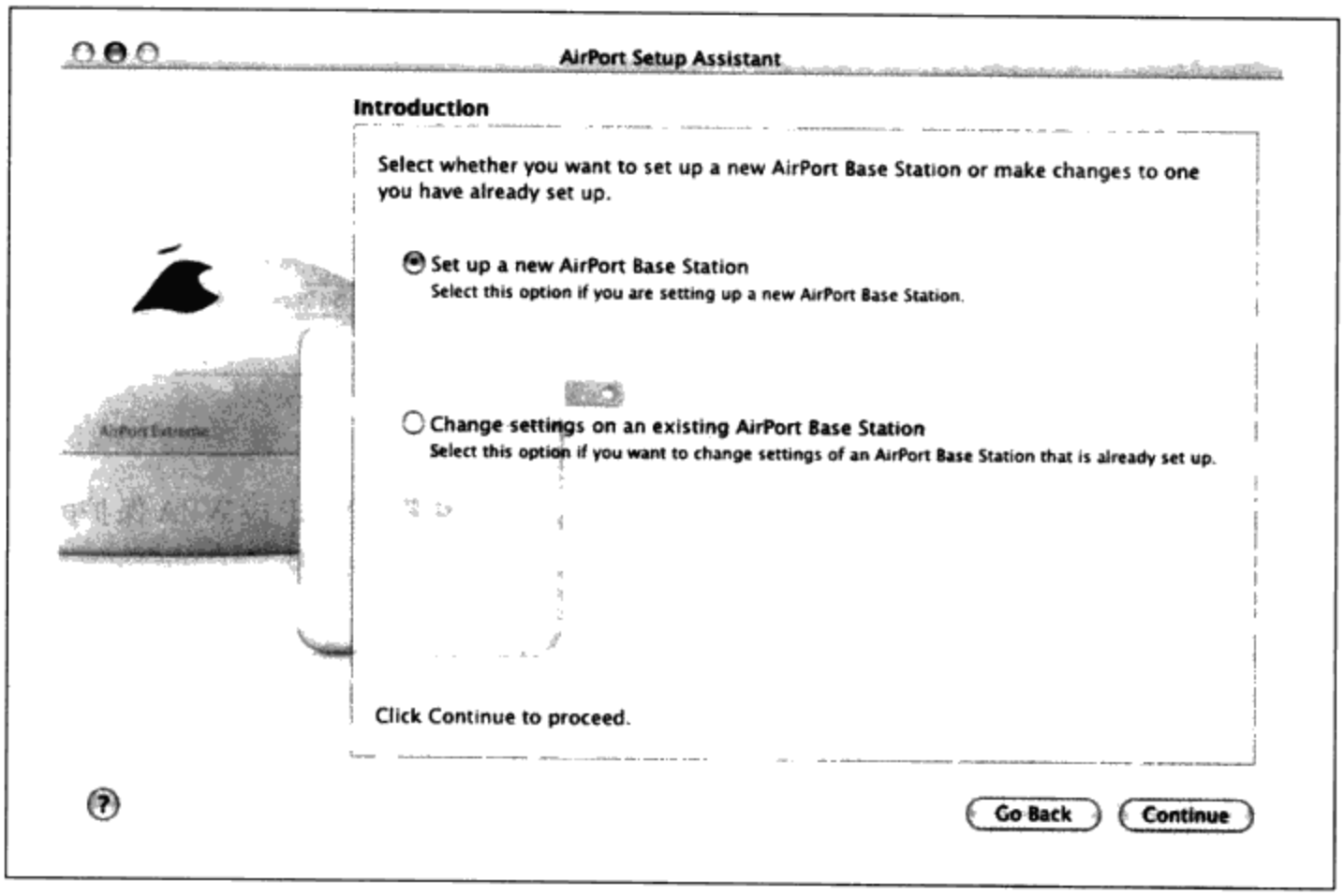


图 18-1：AirPort Setup Assistant 的启始画面

选择设定 AirPort 网卡配置，然后点击“Continue”按钮。下个步骤是选择所要加入的网络，如图 18-2 所示。信号覆盖范围内所有网络均显示于弹出式菜单（pop-up menu）。图 18-2 显示用户选取了 *secure.utah.edu* 网络。

注 1：网卡也可以通过 System Preferences 应用程序加以设定。本章之所以将 Setup Assistant 的讨论置于 System Preferences 之前，主要是为了在监控与变更配置设定各方面力求内容的完整性。不过，没有理由不能直接以 System Preferences 应用程序进行配置设定。

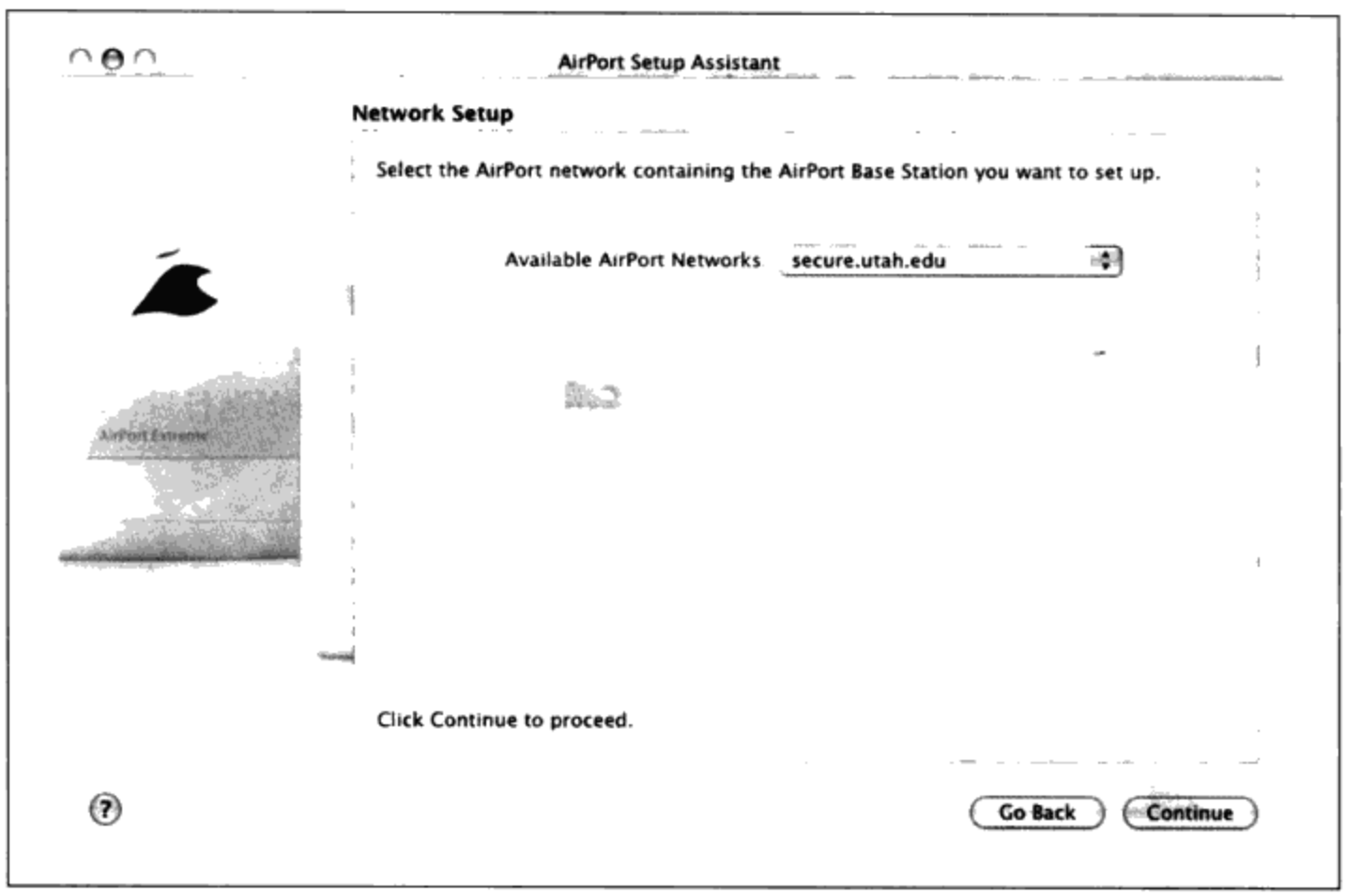


图 18-2：选择 AirPort 网卡所要加入的网络

选好网络后，开始进行第三个步骤：输入网络密码，这只用于以 WEP 或 WPA 保护的网络。802.1X 配置必须在 Internet Connect 中设定，本章稍后将会述及。

进行网络连接时，有好几种不同的安全性设定可供选择，如图 18-3的对话框所示。在下拉式菜单(drop-down box)中有几种安全性选项可供选择：WPA Personal(WPA-PSK)、WPA Enterprise（WPA 搭配 RADIUS 身份验证）以及 WEP。为了让用户更容易上手，Apple 允许网管人员以任意长度的密码设定 WEP 密钥。之后，这些 ASCII 文字所构成的密码会经过散列函数的处理，成为长度适中的 WEP 密钥。WEP 密钥也可以是十六进制的数字，输入时只要在字符串前加上“$”即可，例如 `$EB102393BF`。十六进制密钥的长度若非 10 位数（40 个位），就是 26 位数（104 个位）。只要在所输入的密钥前后加上双引号，就可以强制系统以 ASCII 码来解释（注 2）。

设定与监视 AirPort 接口

有时候，你或许需要变更 AirPort 的配置、在不同的 802.11 网络（ESS）间移动或更改

注 2： 进一步的信息请参阅Apple的知识库(Knowledge Base，位于*http://kbase.info.apple.com*)中编号 106250 的文章。

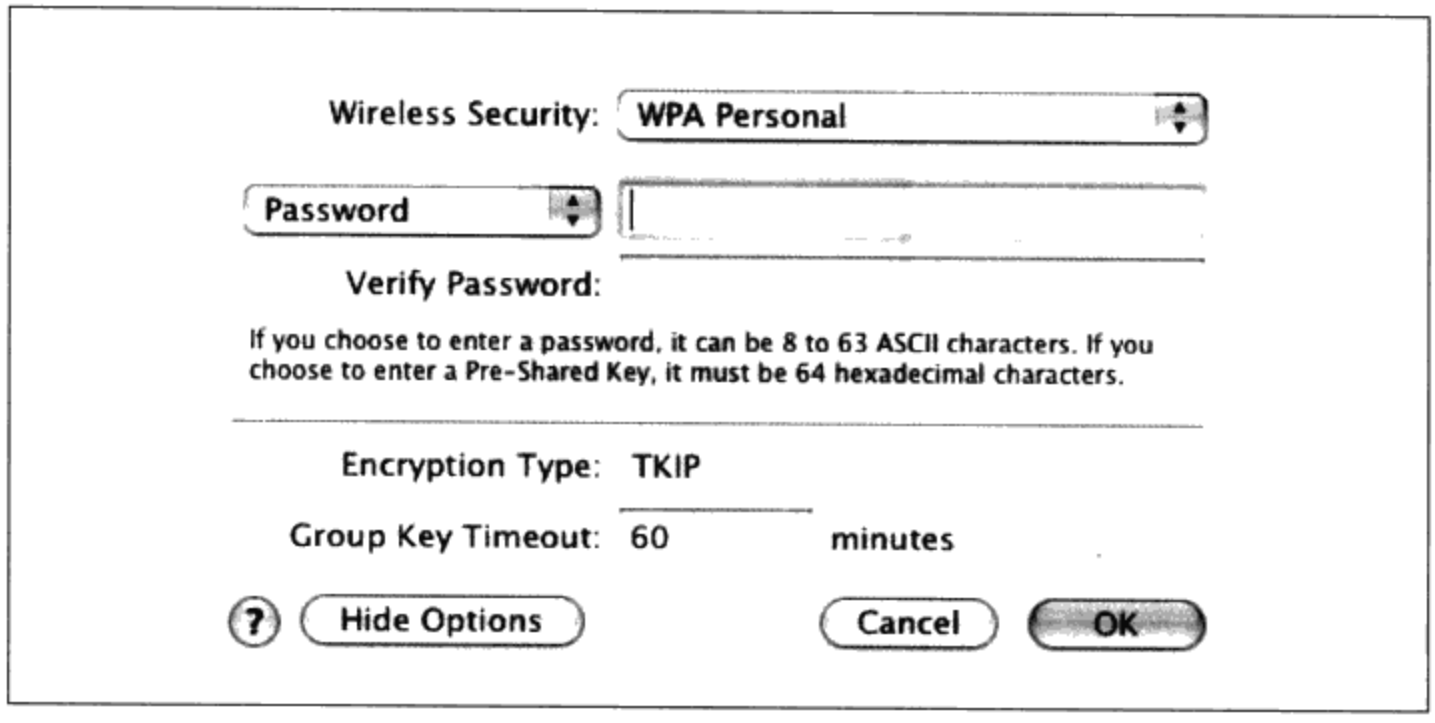


图 18-3：AirPort 网络密码输入画面

WEP密钥与IP的设定值。安装好网卡后，可通过OS X所提供的工具来变更配置。Apple的设定程序不允许用户变更比较复杂的802.11参数。举例而言，加入某个网络所需要的一切信息均广播于Beacon帧。Apple认为，在大部分情况下，只要告诉用户网络名称，要求他们选择安全性设定就够了。

以 AirPort 状态图标进行基本配置设定

配置设定完毕之后，AirPort状态图标（status icon）就会出现在屏幕右下角，位于音量、电池与时钟的图标旁 —— 如果之前没有关闭这些图标的话。AirPort图标同时会显示信号强度。图 18-4 中，图示上会出现一些实心波阵面（solid wavefront）。如果离接入点远一点，信号就会减弱，线条也会减少。点击状态图标后，会出现一个下拉式命令菜单，可以开启或关闭AirPort网卡的电源、选取或新建网络以及运行Internet Connect应用程序来监视无线接口。可以随意开关网卡对用户而言相当方便。当用户离开网络的覆盖范围或不需要使用网络时，即可关闭网卡电源以节省电力。

在图18-4中，信号覆盖范围内有两个网络："Little Green Men"与"Luminiferous Ether"。"Little Green Men"旁边有"V"符号，代表用户目前正与之联机。用户可以随意在两个网络间进行切换。如果尚有其他网络，可以选择"Other..."选项，然后输入网络名称。

要新建一个IBSS网络，可以通过"Create Network"选项，选择如图18-5所示的基本无线参数。该计算机准备设立一个名为"Very Independent BSS"的IBSS网络，使用预设的11个无线电信道之一。在北美或欧洲，这11个信道可以任意使用。每台加入IBSS的计算机都必须使用相同的信道。IBSS网络只能使用WEP加密。

图 18-4：AirPort 状态图标

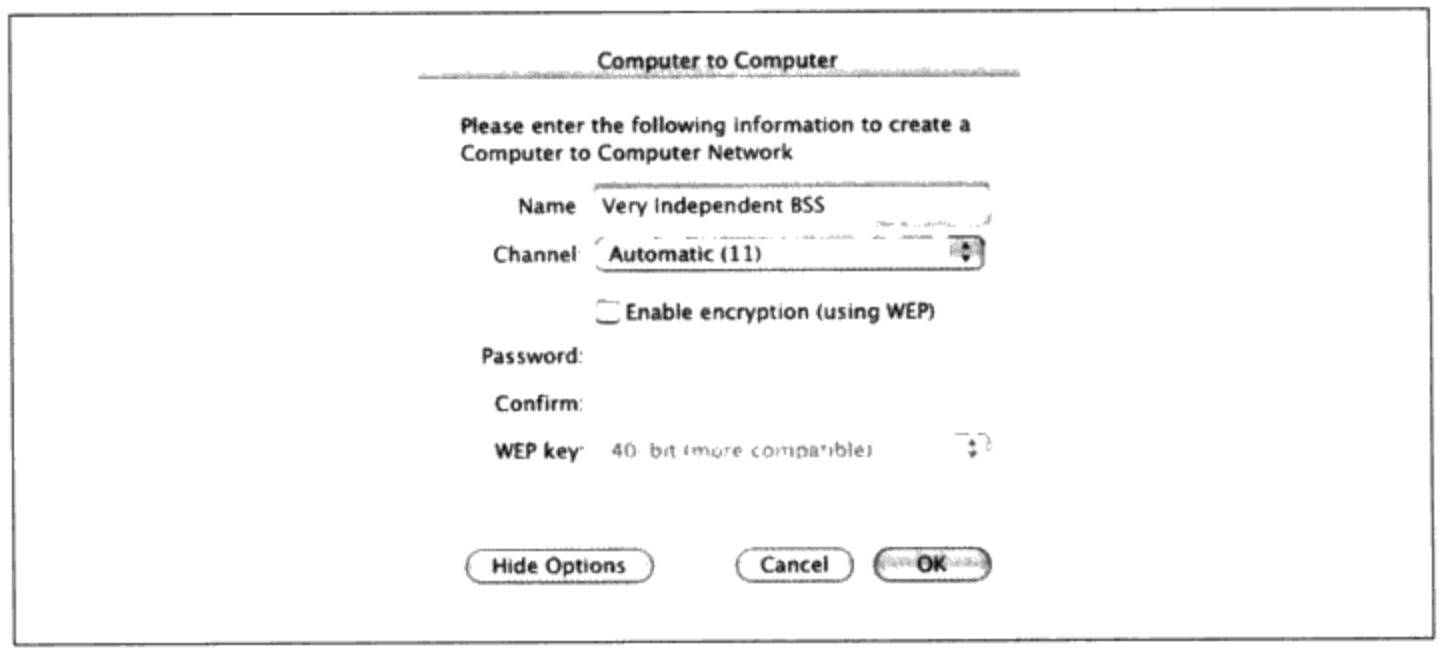


图 18-5：IBSS 参数的设定

设定完成后，系统就会在下拉式菜单中新增一个名为“Computer to Computer Networks”的项目，如图 18-6 所示。AirPort 状态图标也改变为 pie wedge 形，表示目前所使用的是 IBSS 网络，而非 infrastructure 网络。

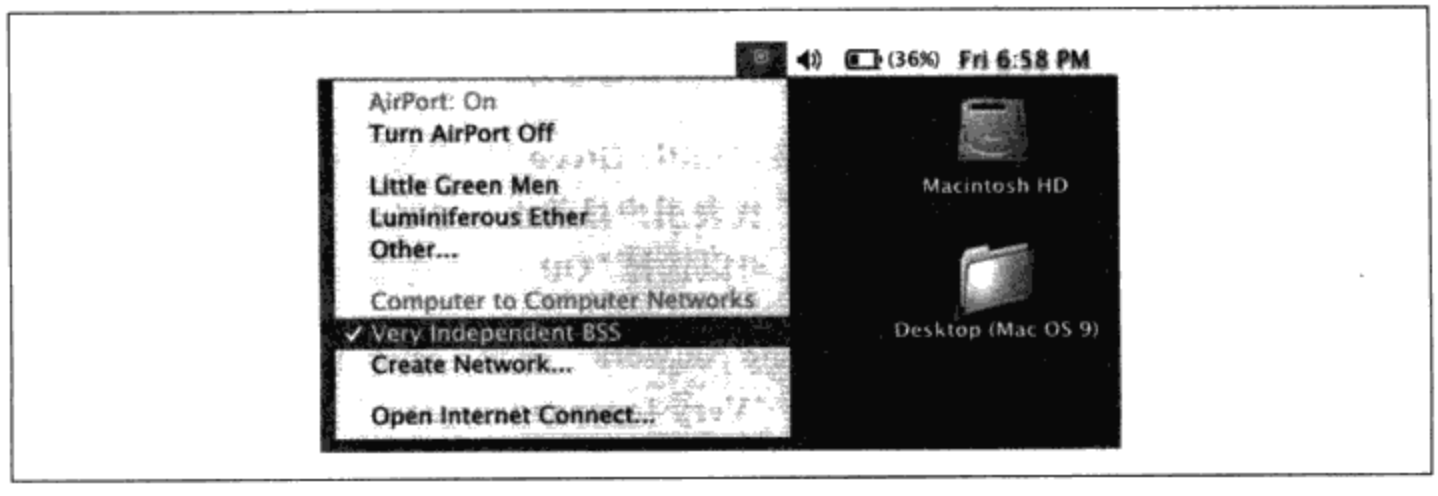


图 18-6：当关联至 IBSS 时 AirPort 所显示的状态图标

以 System Preferences 应用程序进行设定

如果想在不同的ESS之间移动，你可以为每个网络创建一个“位置名称”（location）并以此设定相应的“ESS－密码”对，此后只要移动至某个不同位置，就可以从菜单中点选使用。就算目前不在所要加入的网络范围内，也可以预先设定好“ESS－密码”对。

System Preferences（系统参数设定）应用程序允许用户设定许多系统属性，包括网络方面的属性。图 18-7 显示了 System Preferences 应用程序的 Network Preferences（网络参数设定）面板。Show 弹出式列表（pop-up list）可以被设定成系统中的任何一个网络接口。此处当然是设定成 AirPort，如图所示。默认的参数设定标签为 TCP/IP（图 18-7），可以手动设定接口卡，也可以通过 DHCP 或 BootP 自动设定。设定为 DHCP 时，会显示出所取得的地址，如图 18-7 所示。虽然我的网络上的 DHCP 服务器会提供 DNS 服务器的IP地址，但此处并未显示出来（不过，一般Unix系统会将它置于*/etc/resolv.conf*文件中）。

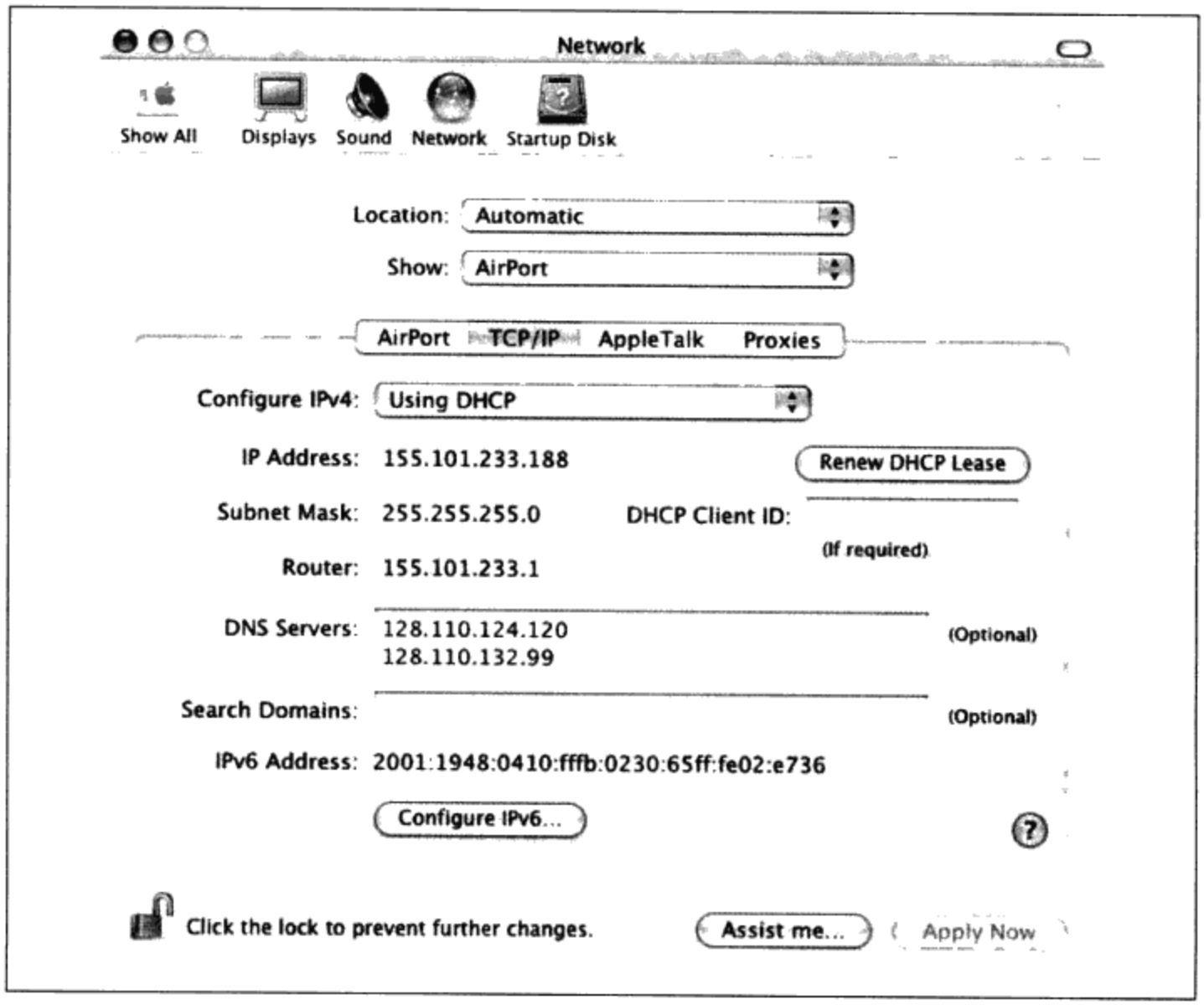


图 18-7：Network Preferences 面板的 TCP/IP 参数设定标签

其他值得注意的参数设定标签是“AirPort”（图 18-8），用来设定预计要加入的网络。大部分情况下，应该将它设定为 Automatic，这让工作站得以在已设定好的网络中进行搜寻。如有必要，“Automatic”选项可以参考Internet Connect 中已设定好的安全性配置。

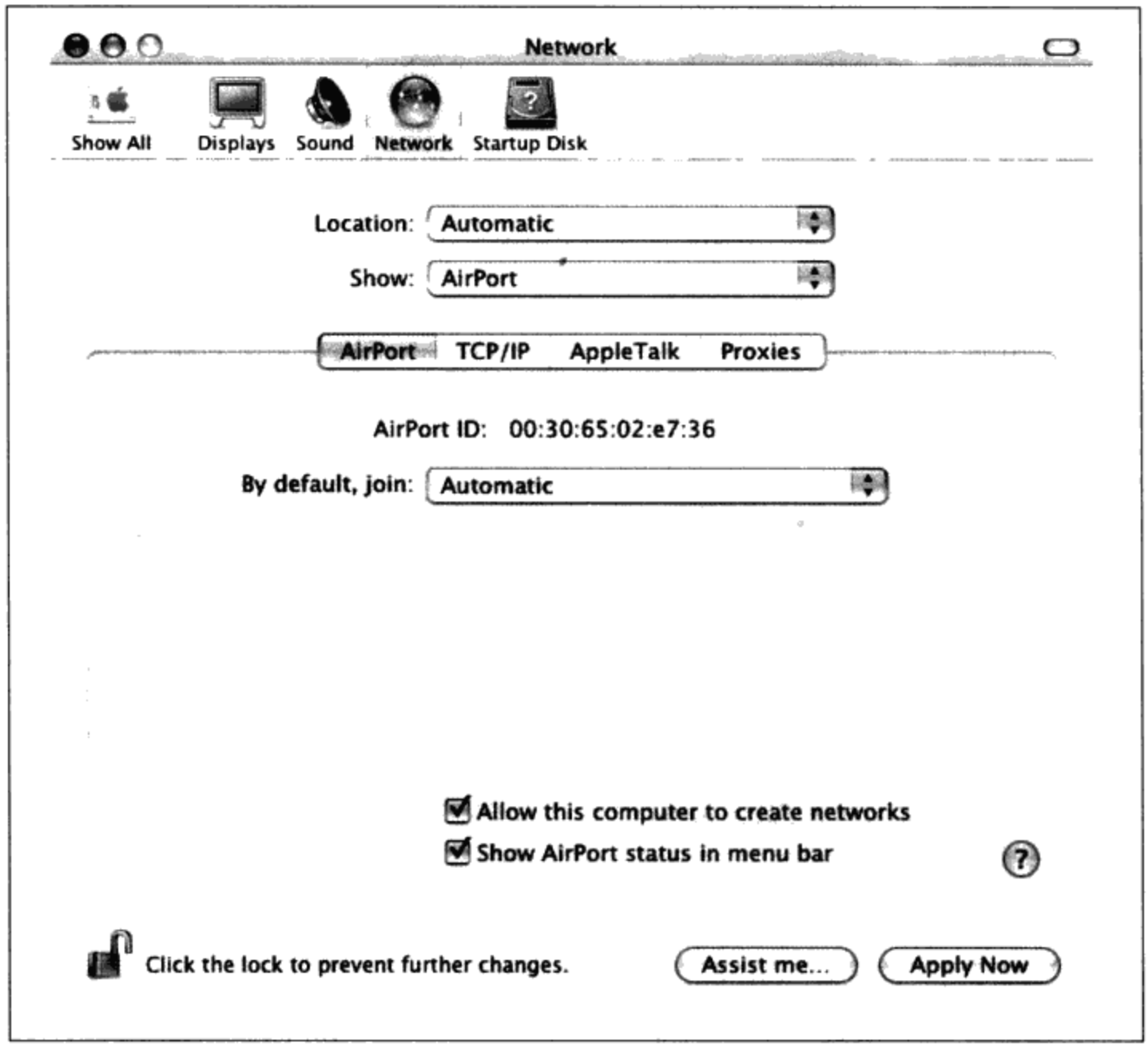


图 18-8：Network Preferences 面板的 Airport 参数设定标签

监控无线接口

无线接口的使用状态可通过Internet Connect应用程序加以监控。Internet Connect应用程序可从硬盘上的Applications文件夹中或由AirPort状态图标来执行。它可以显示距离最近的接入点的信号强度并切换至所要关联的网络。如果切换至到别的网络，它将会参照任何必要的 802.1X 配置设定以便进行身份验证，如图 18-9 所示。

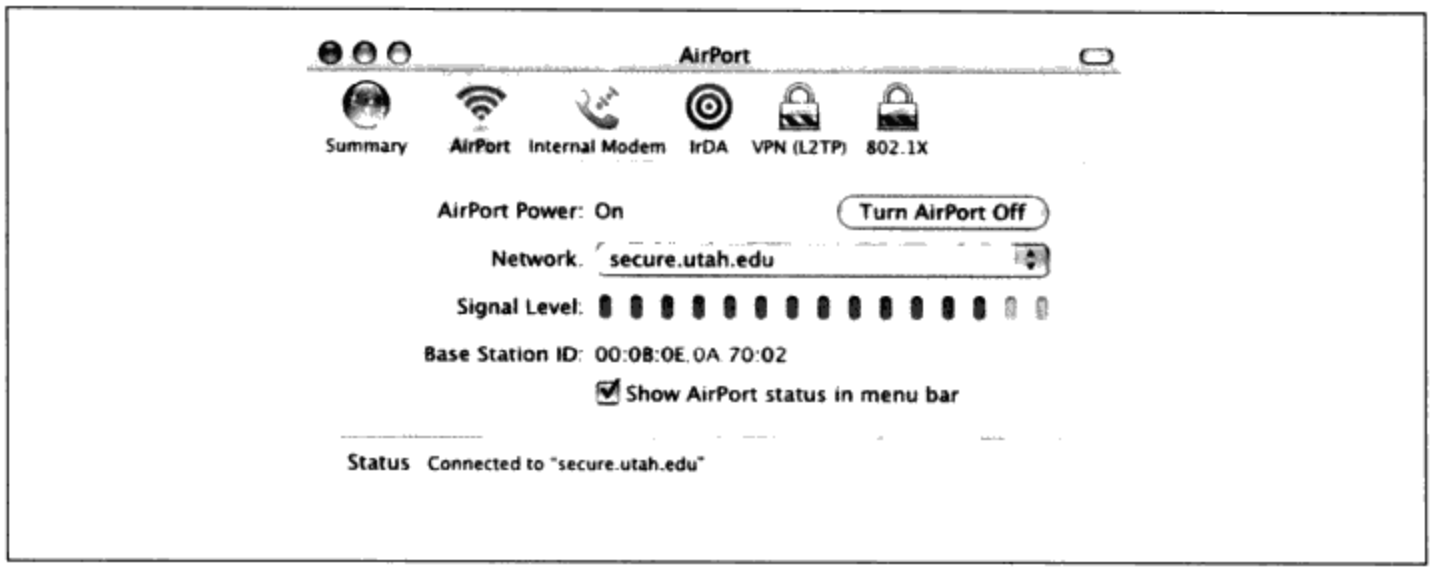


图 18-9：Internet Connect 监控程序

在 AirPort 上使用 802.1X

在 Panther 操作系统上，802.1X 是通过 Internet Connect 应用程序来设定。Internet Connect 可以由 AirPort 状态图标的下拉式菜单（或是直接从硬盘）来执行。

要查看 802.1X 的配置设定，可以点击标示为 802.1X 的锁头图标。如果画面中并未出现该图标，请由“File”菜单点击“New 802.1X Configuration”或直接按Command+Shift+X组合键。一旦启用过 802.1X，该图标就会永远出现在顶端的菜单画面中（如图 18-10 所示）。

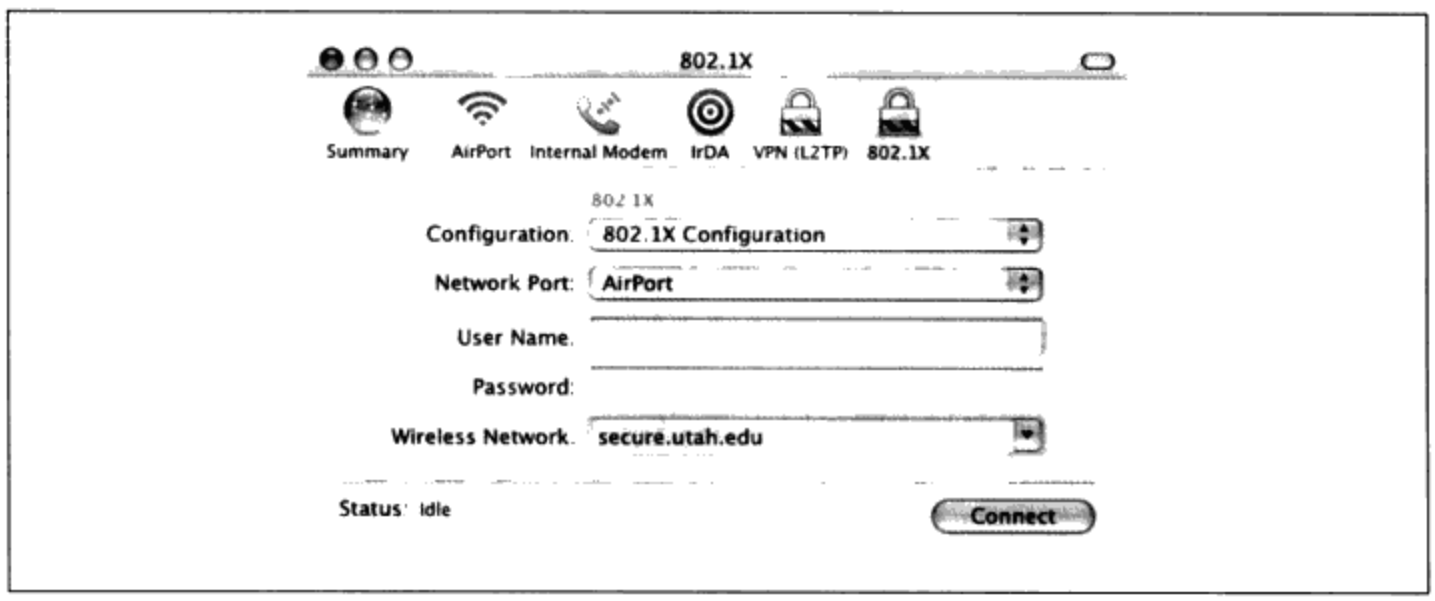


图 18-10：Internet Connect 中的 802.11X 配置设定

要查看完整的配置设定，可以选择“Configuration”下拉式菜单，然后点击“Edit Configuration...”，这样就会显示配置设定主画面（图 18-11）。而最简单的做法是直接编辑现有的配置，由此进入配置设定画面。输入 username 与 password 之后，就可以点击想要使用的身份验证协议。此画面允许用户选择要在哪个网络接口上使用802.1X。大多数情况下，这项设定是针对 AirPort 网卡的，不过 802.1X 在有线网络上也逐渐得到广泛应用。username 与 password 的设定十分直接，“Wireless Network”选项也是。默认情况下，“Wireless Network”下拉式菜单会列出 AirPort 侦测到的所有加密网络，不过用户也可以自行输入 SSID。

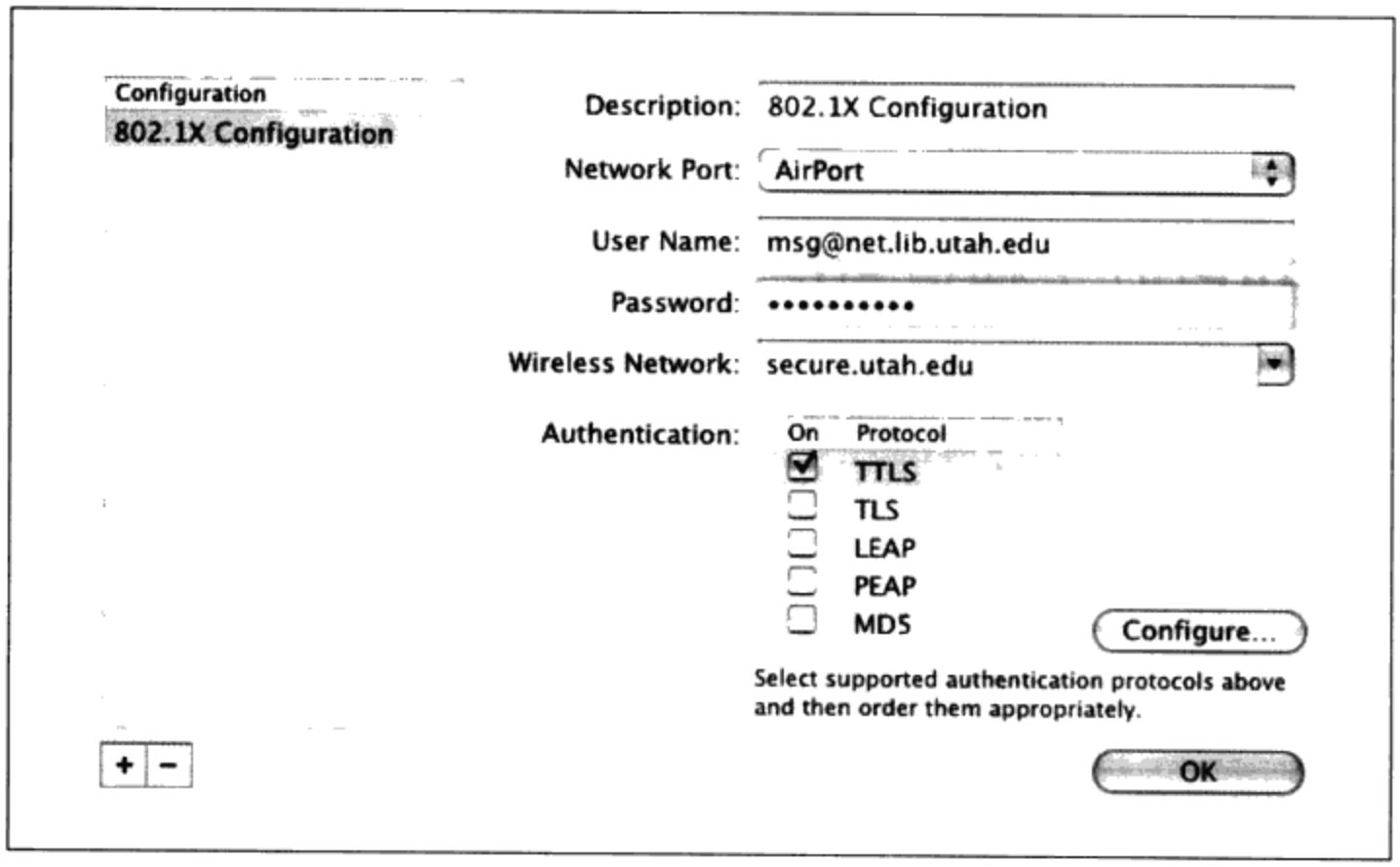


图 18-11：802.11X 的配置设定画面

输入账号与密码后，接下来可能需要设定身份验证方式。每一种认证方式各有不同的配置设定画面，稍后会加以说明。

回到 Internet Connect 主画面后，就可以点击“Connect”按钮进行网络连接以及必要的 802.1X 身份验证。画面下方的状态栏（status bar）将会经历下列阶段：

Idle（闲置）

AirPort 尚未关联到任何网络。

Connecting（连接中）

AirPort 正与所选择的 SSID 进行连接中。

Authenticating（身份验证中）

AirPort 与 AP 或交换器正在交换 EAPOL 帧，尝试验证用户身份。

Connected via (EAP method)（已通过 EAP 方法连接）

如果通过身份验证，状态栏将会显示系统已经联机以及所使用的 EAP 方法以及通过身份验证的时间。

EAP 方法的配置设定

每一种EAP方法均有不同的配置设定方式。除非必要，否则Mac supplicant通常会将比较复杂的设定隐藏起来。

TTLS 配置设定

TTLS有两种可能的配置设定选项，如图18-12所示。第一种属于内部的身份验证，此为必要（mandatory）选项。大多数情况下应该会将这个选项设为PAP，不过也可以使用CHAP、MS-CHAP 或者 MS-CHAP-V2。和大多数 supplicant（认证申请者）一样，Macsupplicant也可以通过设定一个匿名的（anonymous）外部身份（outer identity）来隐藏用户身份。

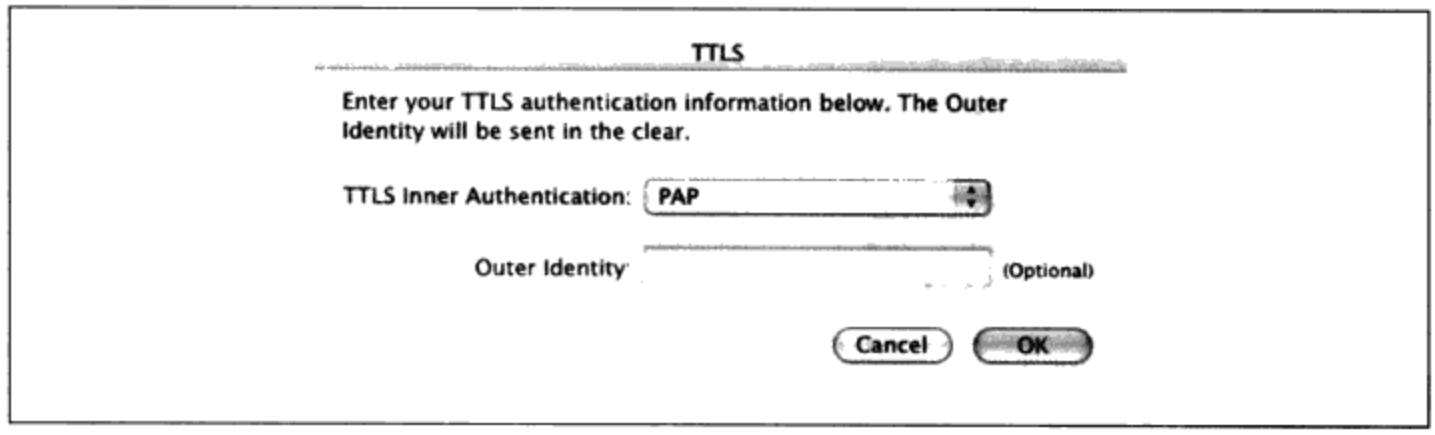


图 18-12：TTLS配置设定画面

PEAP 配置设定

Mac supplicant只支持以EAP-MSCHAP-V2作为内部身份验证方法。如此即可与以MD4散列或明文格式存储的用户账号互用。这种方法的主要用处是支持存储于Windows网络的用户账号。在图18-13的配置设定画面中，只有一个用来设定外部身份以便隐藏用户身份的选项。

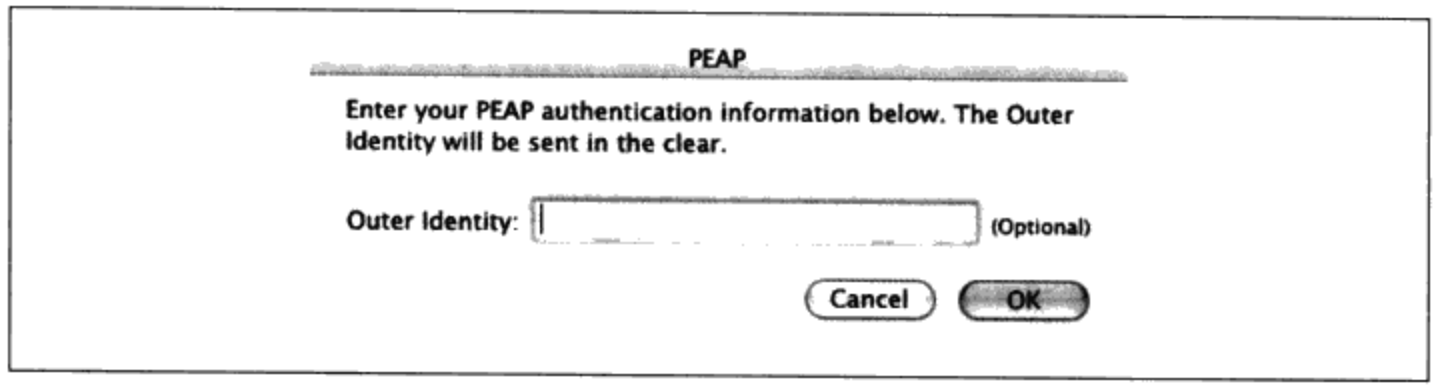


图 18-13：PEAP 配置设定画面

密钥链

在 Mac OS 中，密码与证书存储于密钥链（*keychain*）之上，用来集中保管安全相关信息。登录后，用户有权执行的应用程序即可使用网络身份验证所需要的证书与识别信息。简单的密钥链如图 18-14 所示，其中包含 RADIUS 服务器证书（certificate）、签署该证书的 CA 以及某个网络的 802.1X 配置设定。密钥链提供了访问控制以保护配置设定。

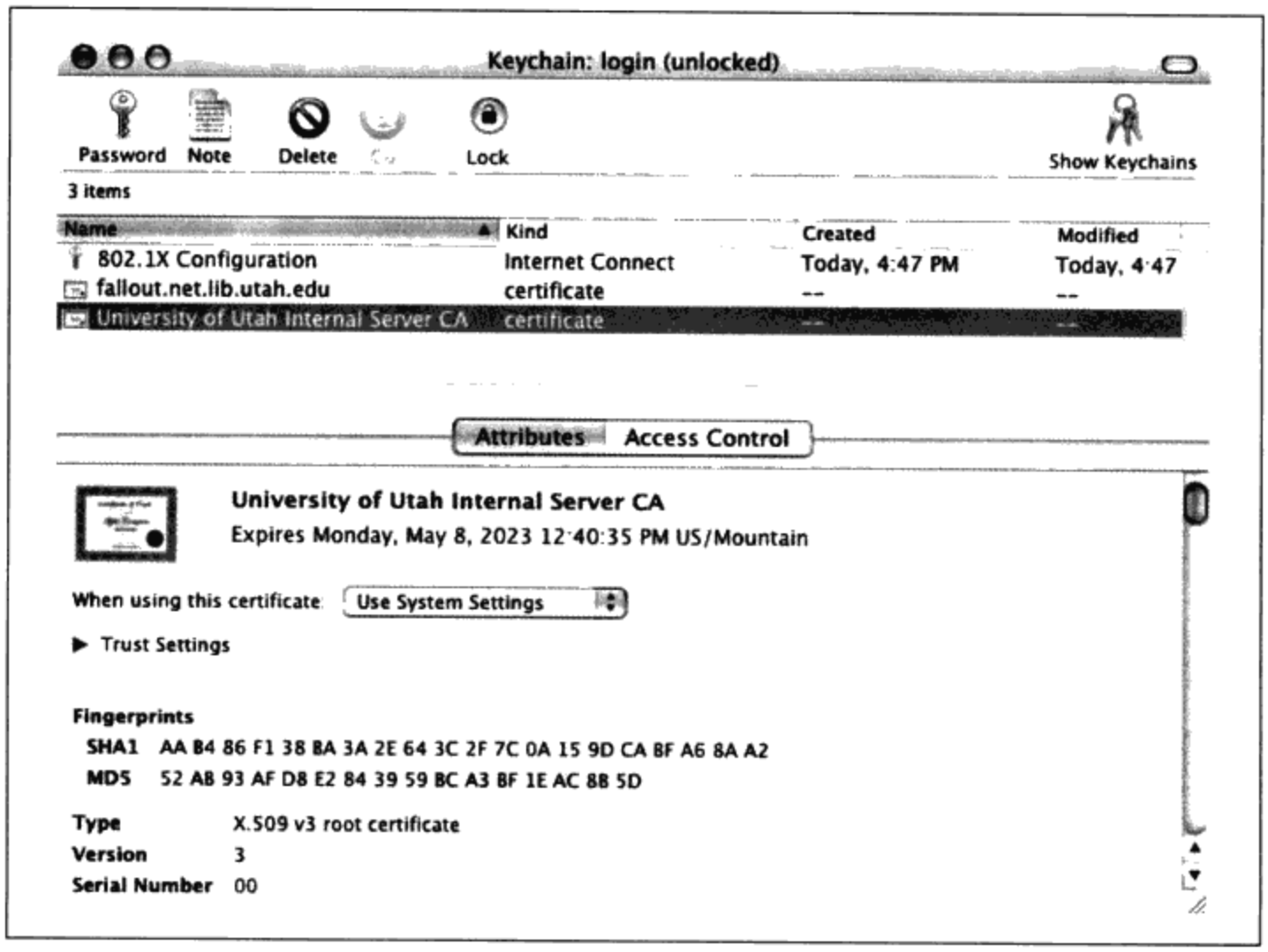


图 18-14：密钥链查看器

将证书加入密钥链

第一次连接至受802.1X保护的网络时，任何未被信任的证书均会导致身份验证失败。不过，supplicant会向用户出示证书内容，而非自行判定身份验证失败，如图18-15所示。检查过证书后，用户即可决定是否信任该证书。比较可能出现的情况是，信息科技部门将系统交付给一般用户之前，会在无线网络上先行测试账号与密码，同时将它们添加至相关的证书。

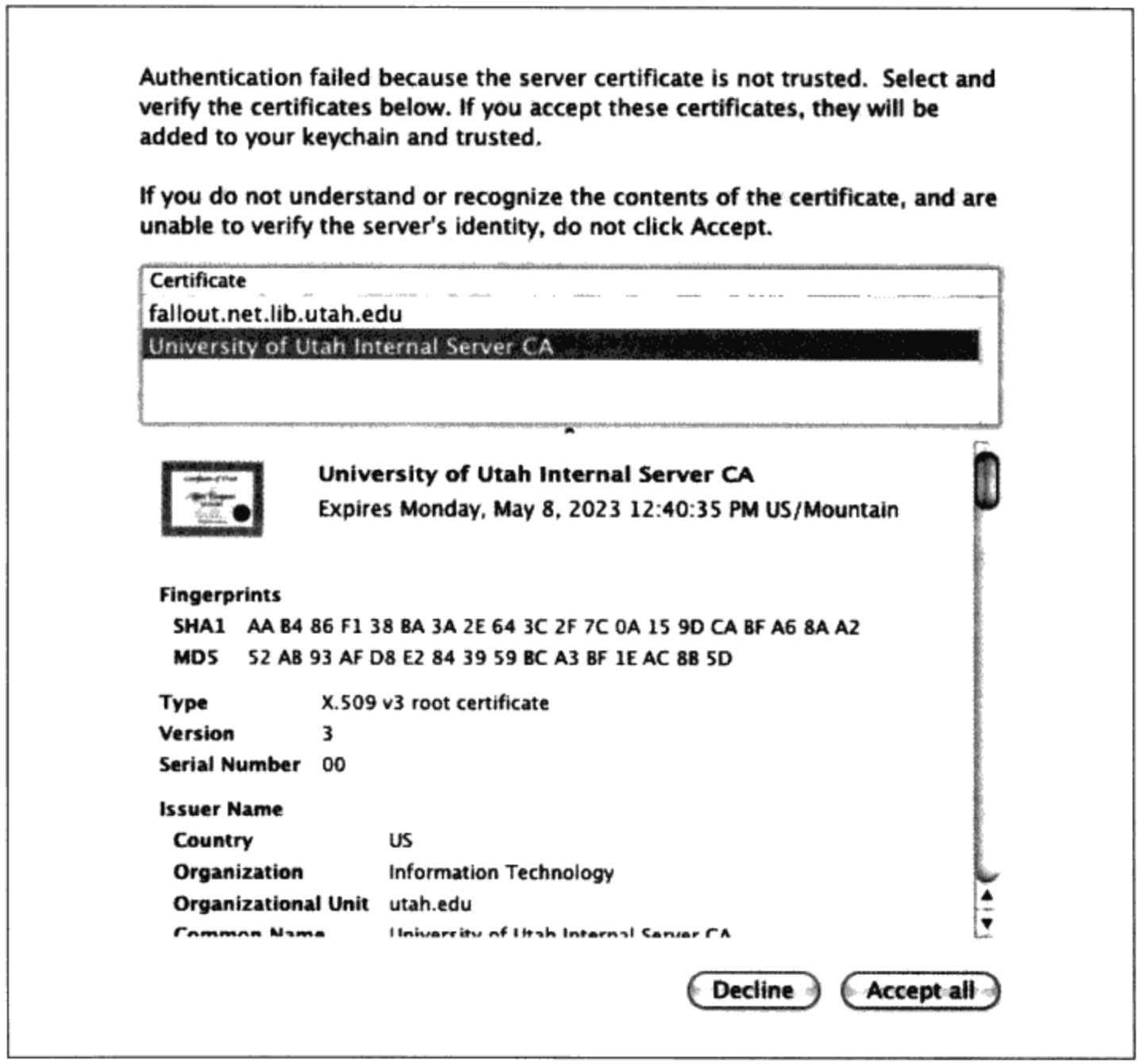


图 18-15：将证书添加至密钥链

故障排除

如果802.1X身份验证失败，所出现的错误信息（图18-16）并不能提供多少线索。错误码无法提供详细的诊断信息，告知失败的真正原因。

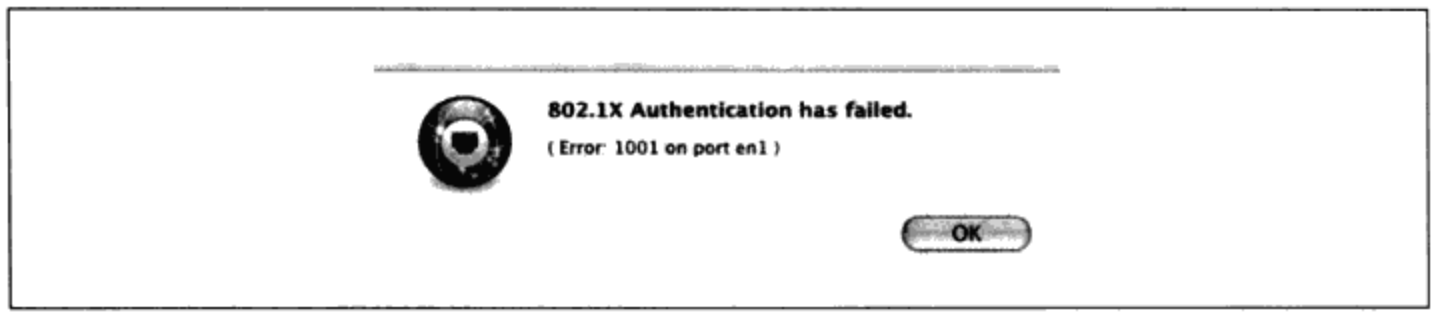


图 18-16：身份验证失败对话框

幸好，supplicant会提供额外的调试记录。如果*/var/log/eapolclient*目录不存在，请先手动创建。如果此目录已经存在，而且在Internet Connect执行时已经设定了*NSDebugEnabled*环境变量，用户所发送的EAPOL帧就会被记录在*/var/log/eapolclient/uid(number)-(network interface).log*文件中。举例而言，如果UID 501试图在AirPort（通常为*en1*）使用802.1X，该日志文件即为*uid501-en1.log*。Internet Connect必须从命令行执行，这样才能自终端机中取得环境变量。

```
Mac:~$ sudo mkdir /var/log/eapolclient
Mac:~$ NSDebugEnabled=YES; export NSDebugEnabled
Mac:~$ /Applications/Internet\ Connect.app/Contents/MacOS/Internet\ Connect
```

对于送出与接收的每个帧，调试日志文件会同时以ASCII与十六进制（hexadecimal）两种格式加以记录。至于经过加密的EAP方法，则不会列出相应的解密帧。举例来说，802.1X身份验证成功后会收到两个如下的EAPOL-Key帧：

```
----------------------------------------
2005/02/15 17:00:42.903841 Receive Packet Size: 75
Ether packet: dest 0:30:65:2:e7:36 source 0:b:e:a:70:2 type 0x888e
EAPOL: proto version 0x1 type Key (3) length 57
Signature: 6c 08 b3 97 b1 74 f2 ec  0e 2c 1f 66 ff 40 78 42 is valid
EAPOL Key Descriptor: type RC4 (1) length 13 Broadcast index 2
replay_counter: 42 11 48 e2 00 00 00 18
key_IV:         ca 7e d9 ff d4 47 80 ba  9e eb 33 c8 82 17 02 7c
key_signature:  6c 08 b3 97 b1 74 f2 ec  0e 2c 1f 66 ff 40 78 42
key:            fc 7a 7c 67 f6 f6 f5 7d  a5 94 cb 49 1a
----------------------------------------
2005/02/15 17:00:42.960436 Receive Packet Size: 64
Ether packet: dest 0:30:65:2:e7:36 source 0:b:e:a:70:2 type 0x888e
EAPOL: proto version 0x1 type Key (3) length 44
Signature: ce b3 45 05 47 72 5a 98  7c 64 0c d8 52 0d 8f 78 is valid
EAPOL Key Descriptor: type RC4 (1) length 13 Unicast index 0
replay_counter: 42 11 48 e2 00 00 00 19
key_IV:     45 e5 2a ad 1c 9c ea 8f  3c 58 a4 c4 6a e0 fa 82
key_signaturece b3 45 05 47 72 5a 98  7c 64 0c d8 52 0d 8f 78
EAPOL:          2 bytes follow body:
00 00 00
```

在 Mac 上同时使用 WEP 与 WPA

本书即将付印之际，Mac supplicant 当中依然存在一个攸关互用性的瑕疵，即无法同时使用两种加密方式。同时用到动态 WEP 与 TKIP（WPA）的情况十分普遍。支持 TKIP 的工作站通常会用它传送单播（unicast）数据，而以动态 WEP 来加密广播（broadcast）数据。只支持动态 WEP 的工作站则同时用它加密单播与广播数据。

在混用 WEP/TKIP 的环境中，Macintosh 便无法联机至网络。supplicant 可以在关联的过程中得知网络同时支持 WEP 与 TKIP 并且接受相关的安全参数。不过在进行密钥握手（key handshake）时，supplicant 坚持只能使用 TKIP。既然关联过程与配钥过程所使用的安全参数有所差异，依照标准规定，接入点应该认定密钥握手失败并将工作站踢出网络。

欲解决此问题，你可以降低网络的安全等级来只使用动态 WEP；或是设定两组无线网络（一组使用 WEP，另一组使用 TKIP），让 Mac 只使用 TKIP 网络；或是强迫使用动态 WEP 的所有设备退出网络，直到它们完全使用 TKIP。

第十九章

802.11 与 Linux

写作本书第一版时，802.11 才刚走向 Linux。当时能够完整支持无线网卡的开放源码的驱动程序很少，也跟不上 Linux 内核（kernel）的更新脚步，因此在选购时必须特别小心。如今支持Linux 已经成为主流，许多厂商开始主动赞助驱动程序开发项目，至少也会提供协助给那些针对本公司硬件所做的努力。Broadcom 算是少见的例外。

大多数 802.11 设备是由 PCMCIA 系统提供支持。和 Windows 驱动程序一样，在 Linux 上安装无线网卡就会创建 Ethernet 接口。有些 Linux 驱动程序会通过内核提供 Ethernet 接口。大多数驱动程序甚至会以*eth*为前缀来替这些接口命名。应用程序会通过Ethernet 接口在链路层收发数据，并由驱动程序负责处理 Ethernet 与 802.11 之间的转换操作（注 1）。其中有许多事情和大家对Ethernet接口的期待相当。ARP的运作方式与之相同，IP的配置设定也可以利用操作系统发行包所提供的相同工具程序。Ifconfig 甚至可以用来监控接口状态以及查看数据的收发。

Linux 所支持的 PCMCIA

起初，无线网卡大多是 PC Card 规格的附加卡（add-on card）（注 2）。PC Card 通过运

注 1　802.11的数据有两种主要的封装格式。RFC 1042用于IP并且得到广泛的支持。Windows 与 MacOS 以 802.1H 支持 IPX 与 AppleTalk。并非所有 Linux 驱动程序均支持 802.1H。

注 2　国际个人计算机存储卡协会(Personal Computer Memory Card International Association，简称 PCMCIA）是制定PC Card 标准的产业团体。起初，这些卡片被称为“PCMCIA cards”，不过后来就简称为“PC Card”。我同时使用两者，是因为 Linux 仍然支持这些网卡使用较长的“PCMCIA”。因为又长又难念，有人戏称 PCMCIA 为“无法招架计算机产业术语的家伙”（People who Can't Manage Computer Industry Acronyms）。

作于 8 MHz 的 16 位控制器与系统总线连接。虽然性能受限于和 16 位 ISA 相当的总线，不过 PC Card 已经足够应付相对较慢的 802.11b 无线局域网络。至于性能较高的 802.11a 与 802.11g 网卡，就必须用到 CardBus 接口（在 33 MHz 驱动 32 位总线）。CardBus 提供了大幅提升的性能，可以满足带宽需求较高的网络接口。在外观上，CardBus 和 PC Card 网卡看起来没什么两样，而且使用同样的插槽。可想而知，两者均可使用 Linux PCMCIA 工具程序进行配置设定与管理。

附带天线的外接式网卡通常会有部分凸出膝上型计算机的机壳，外观并不讨喜。因此膝上型计算机厂商另外替“内置”（built-in）的无线设备选择了一种截然不同的造型，称为 Mini-PCI。Mini-PCI 是 PCI 接口的缩小版，长度只有几英寸。Mini-PCI 接口卡可以内置各种不同功能，不过目前 Mini-PCI 插槽最常见的用途，就是用来让膝上型计算机添加无线网络功能。大多数 Mini-PCI 无线网卡是由 PCI-to-Cardbus 桥接器与 CardBus wireless LAN 接口所组成，因此可以通过 Linux PCMCIA 系统进行配置设定与管理。

PCMCIA Card Services 概观

Card Services（网卡服务）主要是为了简化系统配置。也就是说，主机系统为 PC Card 维护了一组资源，必要时才加以配置，而不是为个别设备提供专属的系统资源。图 19-1 显示了每个网卡在 Linux 操作系统上的配置设定过程。

网卡插入时，*cardmgr* 系统程序负责指挥整个设备的配置设定过程，如图 19-1 所示。整个过程中，会将系统资源、内核组件以及内核驱动程序模块通过存储于 */etc/pcmcia* 的配置文件组合在一块。大致而言，主机会采取下列步骤：

1. 某个网卡被插入一个空的 PC Card 插槽，*cardmgr* 会被告知此事件。除了一些硬件上的操作（例如，为该插槽提供电源），*cardmgr* 会查询该网卡的卡信息结构（card information structure，简称 CIS），判断所插入的网卡种类以及所需要的资源。关于 CIS 的更多信息，请参阅附文“网卡信息结构”。
2. *cardmgr* 接下来会尝试辨识该网卡以及加载适当的内核模块作为支持。位于 */etc/pcmcia/config* 的 PCMCIA 网卡数据库主要把 CIS 数据库映射到驱动程序。驱动程序也可以通过硬件识别表（hardware identification list）自动加载。硬件识别表属于模块的一部分，存放在模块映射表中（*/lib/modules/(kernel version)/module.*map*）。辨识网卡的主要目的是为了将网卡归类。就配置网卡的目的而言，重点在于网络类别（network class）后续还需要一些额外的网卡配置操作。网卡的种类会在步骤 1 借由 CIS 数据加以辨识，而网络类别的设定则在主要系统配置文件中。至此，*cardmgr* 会发出“哔”声。如果辨识成功，所发出的“哔”声的音调较高，否则所发出的“哔”声的音调较低。

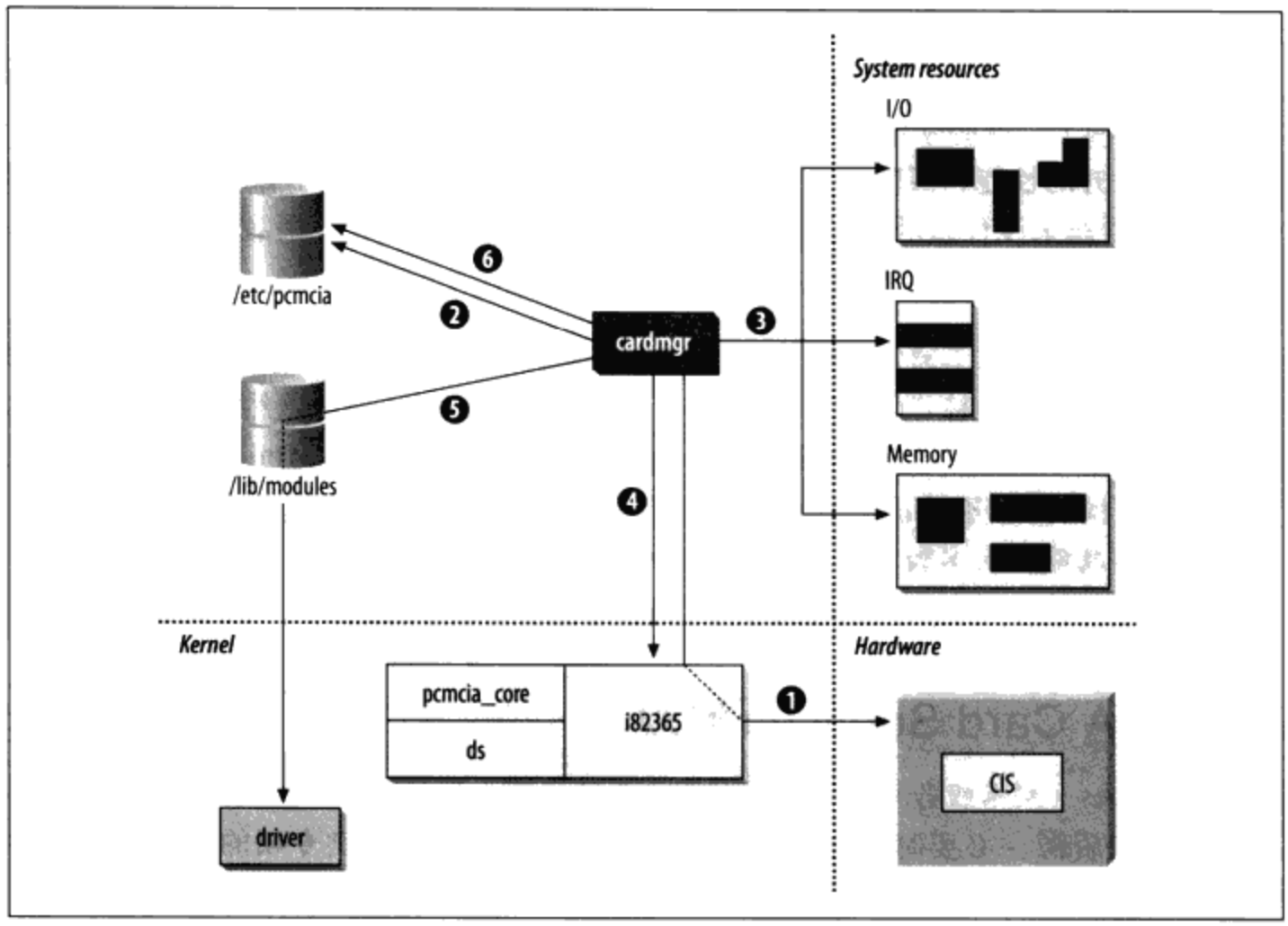


图19-1：Linux PCMCIA配置系统

3. *cardmgr*判断有哪些资源可以分配给网卡。在主要配置文件中会保留系统资源块给PCMCIA网卡使用，而且*cardmgr*会将所需要的资源发送给网卡。I/O端口的编号以及所需内存的大小从CIS取得。

4. *cardmgr*所分配的资源会在PCMCIA控制器加以设定，如图19-1所示，该控制器会与设备驱动程序交互。Intel的i82365SL PCMCIA控制器是目前市面上最常见的芯片，这就是为什么此内核模块会标示为“i82365”。新的PCMCIA系统采用的是*yenta_socket*（而非特定芯片组）驱动程序。PCMCIA控制器负责将网卡所需要的资源映射到可用的系统资源。网卡或许会要求中断，但实际指派的中断与此无关。在操作过程中，网卡仅会要求PCMCIA控制器发出中断信号，而控制器的响应则是找出指派给插槽的中断以及触发正确的中断线路。

5. 在步骤2搜寻来的配置信息中，有一部分是使用刚插入网卡时应该加载的设备驱动程序的名称。PCMCIA网卡的驱动程序被实现成了内核模块。插入网卡的过程中，驱动程序会在步骤4被告知分配到的资源。只要正确设定模块的依赖关系，即可使用模块堆栈来加载多个模块。

6. 更进一步的用户空间配置根据设备类别（device class）加以设定。举例来说，网卡可额外以 */etc/pcmcia/network* 脚本（script）加以设定，只要编辑 */etc/pcmcia/network.opts* 即可。如果设定成功，就会发出一声高音“哔”，否则发出一声低音“哔”。此外，Linux 的热插拔系统（hotplug system）也可能会进行一些额外的配置设定。

Linux 所使用的接口名称

驱动程序创建网络接口之后，就会赋予它一个由前缀（prefix）与数字（number）所组成的名称。有些驱动程序会以 *ethX* 作为新增网络接口的命名格式，其中 *X* 代表顺序编号。目前大多数膝上型计算机均已内置 Ethernet 接口，开机时即启用为 *eth0*，因此无线接口通常从 *eth1* 开始命名。旧版的 WaveLAN 驱动程序以 *wvlan* 为前缀，不过当前的版本已经改用 *eth*。采用 Atheros 芯片组的网卡则使用 *ath* 为前缀。

以热插拔系统进行自动配置设定

Linux 采用“hotplug configuration”项目的工作成果来进行自动配置设定，该项目的网址为 *http://linux-hotplug.sourceforge.net/*。插入设备时，热插拔系统在为接口进行配置设定之前，会先调用必要的 PCI 配置命令。如果有不少网络接口需要设定或是希望进行自定义的配置操作，就可以使用 Hotplug 脚本完成系统的自动配置。有些较新标准的无线设备在产品推出后，开发工作仍然持续进行。更换新软件后，网卡就可以支持新的协议或者修正已发行版本的错误。配置时可以要求 Hotplug 在插入特定网卡时自动更新软件。

PCMCIA Card Services 的安装

2.4 版以后，PCMCIA 功能被集成到了内核，各位所使用的发行包（distribution）或许早已安装了这项功能。升级核心的 PCMCIA 功能并非必要。虽然不能没有网卡驱动程序，但是 PCMCIA 功能也要够新，方能支持各位手上的无线接口卡（较老的发行包可以通过发行维护单位（distribution maintainer）的软件包（package）来更新 PCMCIA 软件，或者使用 *http://pcmcia-cs.sourceforge.net/* 的源代码自行编译）。

大多数的配置设定信息不难从环境中自动侦测得知。根据所使用的发行包以及安装选项，或许必须在系统配置文件中设定 PCIC 变量来告诉 PCMCIA 软件目前 PCMCIA 插槽使用何种控制器。核心的 PCMCIA 软件会将这个变量值设定为 *yenta_socket*。使用独立 PCMICA 模块的系统如果将此变量设为 *tcic*，就代表使用 Databook TCIC-2 芯片组；如果设为 i82365，就代表使用 Intel i82365SL 芯片组。Slackware 提供了一个“probe”选项，可以自动侦测并加载相关模块。

卡信息结构

为了能够自动进行配置设定，每个PC Card都内含了一段数据，让网卡得以向主机系统交代本身所具备的功能。这段数据称为卡信息结构（card information structure，简称CIS），其所具备的格式为link-list（链接串行）。CIS的基本构建单位称为*tuple*，因为它们具有三项组件：用以表示tuple类型的类型码、长度字段以及一系列数据字节。所以tuple格式可以十分简单，也可能相当复杂，这就是为什么本书并未试图进一步为之分类的原因。勇于求知的读者可以向PCMCIA协会订购一份规范说明书，并利用Linux平台上的*dump_cis*工具读出插入的网卡的CIS。

在自动配置设定过程中，CIS会向主机操作系统描述本身所具备的功能。举例来说，网络接口卡会表明身份，其中的CIS可以让Card Services（网卡服务）软件分配适当的资源，如I/O端口以及中断请求（IRQ）线路。在Linux操作系统中，系统管理员可以使用配置文件来匹配CIS数据与驱动程序。

监控网卡

用来控制PCMCIA子系统的主要工具是*cardctl*命令。它具有一些副命令（subcommand），可用来查看信息或配置设定状态。每个自变量（argument）也可以指定插槽编号。有些膝上型计算机配备两个PCMCIA插槽，编号分别是0与1。为了携带方便，有些笔记型计算机只配备一个插槽，因此只有插槽0。

除了以硬件方式退出系统，还可以用*cardctl*来移除驱动程序，只要送出“网卡已经移除”（card is removed）的通知信息即可。移除相关驱动程序以及关闭插槽电源之后，可以传送一个“插入网卡”的软件通知信息来重新启动网卡。通过软件进行控制，不需要实际插拔即可“重新启动”（reboot）网卡。

```
[root@bloodhound]# cardctl eject 0
[root@bloodhound]# cardctl insert 0
```

选择使用何种驱动程序主要是根据CIS数据。要查看网卡的CIS内容，可以插入网卡等它启动，然后使用*info*或*ident*副命令来查看识别信息。以下是Proxim 8480 Gold card的信息。它和其他802.11a网卡一样，所采用的是Atheros芯片组。你甚至可以看到这个卡片采用Atheros的公版设计（reference design）：

```
root@bloodhound:~# cardctl info 0
PRODID_1="Atheros Communications, Inc."
PRODID_2="AR5001-0000-0000"
PRODID_3="Wireless LAN Reference Card"
PRODID_4="00"
```

```
MANFID=0271,0012
FUNCID=6
root@bloodhound:~# cardctl ident 0
  product info: "Atheros Communications, Inc.", "AR5001-0000-0000",
"Wireless LAN Reference Card", "00"
  manfid: 0x0271, 0x0012
  function: 6 (network)
```

除了以 *cardctl* 查看 CIS 信息，也可以使用 *dump_cis* 命令列出完整的 CIS 结构。除了网卡识别信息，CIS 中也包含速率支持的相关信息。以 Proxim 8480 为例，虽然它也兼容于 802.11b，不过却只显示出了所支持的 802.11a 速率：

```
root@bloodhound:~# dump_cis
Socket 0:
  manfid 0x0271, 0x0012
  config_cb base 0x0000 last_index 0x01
  cftable_entry_cb 0x01 [default]
    [master] [parity] [serr] [fast back]
    Vcc Vnom 3300mV Istatic 25mA Iavg 450mA Ipeak 500mA
    irq mask 0xffff [level]
    mem_base 1
  BAR 1 size 64kb [mem]
  vers_1 7.1, "Atheros Communications, Inc.", "AR5001-0000-0000",
    "Wireless LAN Reference Card", "00"
  funcid network_adapter [post]
  lan_speed 6 mb/sec
  lan_speed 9 mb/sec
  lan_speed 12 mb/sec
  lan_speed 18 mb/sec
  lan_speed 24 mb/sec
  lan_speed 36 mb/sec
  lan_speed 48 mb/sec
  lan_speed 54 mb/sec
  lan_speed 72 mb/sec
  lan_media 5.4_GHz
  lan_node_id 20 00 4d a6 d4 0a
  lan_connector Closed connector standard

Socket 1:
  no CIS present
```

将网卡插入系统后，就可以使用 *status* 副命令进行查看。*config* 副命令也会报告由系统所指派的系统中断。以我为例，我的膝上型计算机使用 PCI 到 Cardbus 的桥接器，因此网卡沿用指派给 PCI 总线的 IRQ。

```
root@bloodhound:~# cardctl status 0
  3.3V CardBus card
  function 0: [ready]
root@bloodhound:~# cardctl config 0
  Vcc 3.3V  Vpp1 3.3V  Vpp2 3.3V
  interface type is "cardbus"
```

```
irq 11 [exclusive] [level]
function 0:
```

没有用的灯光显示

有些驱动程序同时支持好几种硬件，而且各家厂商对于网卡上的灯的数量与用途在定义上并不相同。通常会有一个灯表示网卡已经启动，第二个灯闪动时表示网卡正在进行传输，至于响应来自其他工作站的数据时则可闪可不闪。少数网卡会有第三个灯来指示关联状态。

Linux驱动程序通常不会以厂商所定义的方式来控制网卡上的灯，内置的网卡也许根本没有灯光显示。如果你的网卡上的灯显示方式异常，请勿惊慌。请先检查与接入点是否已经建立关联，若已关联，则网卡的运作即为正常，只不过灯的显示方式不同。

排除资源的冲突

PCMCIA网卡厂商所宣称的神话之一是，在IBM PC兼容的硬件中，用户再也不必负责维护低级的硬件配置。就某些方面而言，这个神话有点过度吹嘘，因为用户还是必须负责维护PCMCIA Card Services所使用的资源，所以用户仍然必须熟悉硬件配置。Card Services为用户管理三种资源：IRQ线路、I/O端口以及DMA（直接存储器存取）信道。不过，网卡并不需要用到DMA信道，因此本节将略过不谈。

IRQ

必须周期性用到CPU的设备就会用到IRQ。接口之所以会使用IRQ，是因为一旦缓冲区已满，就必须通知系统CPU清空缓冲区。PC架构的限制之一是只有15个IRQ可用，而且其中有些已经被标准硬件所占用。表19-1显示了IRQ的一般用途，这或许可以帮助读者判断有哪些IRQ可供PCMCIA卡使用。停用额外的组件可以释放IRQ。表19-1同时显示了PC硬件上一般的IRQ设定。依经验法则，在大部分机器上，IRQ 3、5与10通常是空闲可用的。

表19-1：常见的IRQ设定

IRQ编号	一般用途	使用目的
0	系统定时器	每秒钟振荡18次以维持粗略的计时
1	键盘	让操作系统得以监测用户是否按下任何键
2	级联（Cascade）	使用两个中断控制芯片。第二个控制芯片主要负责控制IRQ 8到15并与第一个控制芯片的IRQ 2相级联

表19-1：常见的IRQ设定（续）

IRQ 编号	一般用途	使用目的
3	第二/第四串行端口（serial port）	第二与第四串行端口（在 Windows 中为 COM2 与 COM4）均使用 IRQ 3。如果只用到一个串行端口，那么 IRQ 3 即可供其他扩展设备使用
4	第一/第三串行端口	第一与第三串行端口（在 Windows 中为 COM1 与 COM3）均使用 IRQ 4。通常，提供 IRQ 4 给其他扩展设备使用并不恰当，因为如此一来就无法使用终端仿真软件了
5	第二并行端口（parallel port）	大部分系统均只配备一个并行端口，不过 IRQ 5 通常保留给声卡使用
6	软盘控制器	所有系统均配备软盘，对便携式计算机而言尤其重要
7	第一并行端口	膝上型计算机通常可以将此并行端口停用而不致产生任何问题，除非此并行端口用于打印
8	RTC	负责维持较精确的计时
9	显卡（旧式系统）	旧式系统必须为显卡保留一个 IRQ，通常使用 IRQ 9。如今大部分显卡均使用 PCI 总线，因此不需要特别配置一个 IRQ
10		通常用于扩展设备
11	通常供 PCI 总线或 SCSI 控制器使用	扩展设备一般无法使用此 IRQ
12	通常供 PS/2 鼠标连接端口使用	一般无法移作他用
13	FPU	用于浮点运算单元的 IRQ，专供数学协处理器使用，即使 CPU 本身已经内设数学协处理器，如 Pentium 系列
14	主要 IDE 信道	主要供主系统硬盘使用，因此在便携式系统中 IRQ 14 通常无法移作他用
15	次要 IDE 信道	便携式系统通常将 IRQ 15 供 CD-ROM 使用，因此无法移作他用

I/O 端口

I/O 地址主要用于系统与外围设备之间的双向通信。它们的设计通常不很好，何况有些设备的默认值会相互重叠。每个I/O端口可以在外围设备与CPU之间传送一个字节的数

据。大部分的设备都需要具备一次传递多个字节的能力，因此需要为设备指派一组 I/O 端口。最小的端口编号也称为I/O 基地址（base I/O address）。另外一个参数用来描述 I/O范围的大小。表 19-2 列出了一些常见的I/O端口设定值。至于IR端口、USB控制器、PCMCIA 控制器以及其他需要用到主板资源的设备，请参阅硬件厂商所提供的说明文档。

表19-2：常见I/O端口

设备名称	I/O 范围（大小）
通信端口	
第一并行端口	0x3bc~0x3bf(4)
第一串行端口	0x3f8~0x3ff(8)
第二串行端口	0x2f8~0x2ff(8)
磁盘驱动器	
主要 IDE 信道	master：0x1f0~0x1f7(8)
	slave：0x3f6~0x3f7(2)
次要 IDE 信道	master：0x170~0x177(8)
	slave：0x376(1)
软盘控制器	0x3f0~0x3f5(6)
输入设备	
键盘	0x060(1)
	0x064(1)
多媒体 / 游戏	
声卡	0x220~0x22f(16)
	FM Synth：0x388~0x38b(4)
	MIDI：0x330~0x331(2)
游戏杆 / 游戏端口	0x200~0x207(8)
系统设备	
中断控制器	0x020~0x021(2)
	0x0a0~0x0a1(2)
DMA 控制器	DMA 信道 0~3：0x000~0x00f(16)
	分页缓存器：0x080~0x08f(16)
	DMA 信道 4~7：0x0c0~0x0df
CMOS/ 实时时钟	0x070~0x073(4)
喇叭	0x061
数学协处理器	0x0f0~0x0ff(16)

Linux 无线扩展功能与工具

802.11 接口一旦启动，它们的行为表现就跟 Ethernet 接口没什么不同，不过它们比 Ethernet 接口多出一些配置设定选项，因为底层使用无线电技术。为了让所有驱动程序实现相同的功能以及使用相同的配置设定命令，而不必各自实现本身的配置设定工具与报告机制，因此有了 Extension API 的开发。无线扩展功能（wireless extension）对需要通过此接口取得详细信息的应用程序开发人员相当有帮助，因为如此一来，信息的取得就与设备无关（device-independent）。例如，*xsupplicant* 将会利用无线扩展功能设定接口上的 WEP 密钥，因此你就不必了解各家驱动程序设定密钥的方式（本书付印时，WPA 产生密钥的系统调用尚未纳入官方发布的无线扩展功能）。

编译与安装

无线局域网络扩展功能是通过 *CONFIG_NET_RADIO* 内核配置选项来启用。启用了 *CONFIG_NET_RADIO* 功能的内核会搜集无线统计数据，并且提供多数驱动程序所使用的额外数据结构。大多数 Linux 发行包所包含的内核如果具备无线扩展功能，通常也会包含无线工具。如果需要最新的版本，可以从 *http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux* 下载，不过等候 Linux 发行包将最新版本纳入内核源代码再予以重建可能会比较简单。

以无线工具和 iwconfig 来配置接口

管理具备无线扩展功能的驱动程序，主要是通过 *iwconfig* 这个命令行工具，它原本就是设计来作为“无线网络的 *ifconfig*”的。使用 *ifconfig* 设定传统网络参数前，可以用它来设定无线接口参数。

不带任何参数时，*iwconfig* 会列出所有系统接口。非无线接口将会报告它们没有无线方面的数据，无线接口则会报告所有数据。并非所有的驱动程序均会实现完整的功能。例如，在使用旧式 Orinoco 网卡以及 Atheros CardBus 网卡的系统上运行 *iwconfig*，其结果可能会像这个样子：

```
[root@bloodhound]# iwconfig
lo      no wireless extensions.
eth0    no wireless extensions.
eth1    IEEE 802.11-DS  ESSID:"11b-is-slow"  Nickname:"HERMES I"
        Mode:Managed  Frequency:2.457GHz  Access Point:00:E0:03:04:18:1C
        Bit Rate:2Mb/s Tx-Power=15 dBm Sensitivity:1/3
        RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off
```

```
          Link Quality:46/92 Signal level:-51 dBm  Noise level:-94 dBm
          Rx invalid nwid:0  invalid crypt:0  invalid misc:0
ath0      IEEE 802.11  ESSID:"11a-is-very-fast"
          Mode:Managed  Frequency:5.28GHz  Access Point: 00:0B:0E:00:F0:43
          Bit Rate:36Mb/s Tx-Power:off Sensitivity=0/3
          Retry:off RTS thr:off Fragment thr:off
          Encryption key:E452-94AC-09DB-2200-1256-6D7D-74  Security mode:open
          Power Management:off
          Link Quality:31/94  Signal level:-64 dBm  Noise level:-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0 Missed beacon:0
```

这两个网卡均会报告操作频率以及与接收质量相关的统计数据。Atheros 网卡并未报告 Orinoco 网卡所报告的“nickname”（昵称），因为 Atheros 驱动程序并未实现此项功能（此昵称预设为“HERMES I”，这是以 Orinoco 网卡所使用的 Lucent 芯片组来命名的）。

无线扩展功能将会以两种方式来报告链路质量（link quality）信息。它会列出本底噪声（noise floor）以及信号电平（signal level），两者均由驱动程序所提供。这两种方式之间的差异在于信噪比（signal to noise ratio，简称 SNR）。上例中，*eth1* 的 SNR 为 43 dB，*ath0* 的 SNR 则是 31 dB。驱动程序所提供的 Link Quality 统计数据会显示出 RSSI（相对信号强度）以及本底噪声。上例中，*ath0* 的 RSSI 为 31 dB，本底噪声为 −94 dBm。

搜寻可用网络

有些驱动程序支持列出该地区所有网络的无线扩展功能。设定之前，可以使用 *iwlist* 命令从网卡取得相关信息。使用 *iwlist* 时需要指定接口以及一个副命令。*scan* 这个副命令将会显示出该地区被发现的可用网络信息。要取得扫描数据必须具备 root 权限。

```
root@bloodhound:~# iwlist eth1 scan
eth1      Scan completed :
          Cell 01 - Address: 00:07:50:D5:CE:88
                    ESSID:"LuminiferousEther"
                    Mode:Master
                    Frequency:2.417GHz
                    Quality:0/10  Signal level:-70 dBm  Noise level:-256 dBm
                    Encryption key:on
                    Bit Rate:1Mb/s
                    Bit Rate:2Mb/s
                    Bit Rate:5.5Mb/s
                    Bit Rate:11Mb/s
          Cell 02 - Address: 00:09:5B:72:12:58
                    ESSID:"Mom's House"
                    Mode:Master
                    Frequency:2.467GHz
                    Quality:0/10  Signal level:-22 dBm  Noise level:-256 dBm
                    Encryption key:on
                    Bit Rate:1Mb/s
                    Bit Rate:2Mb/s
```

```
          Bit Rate:5.5Mb/s
          Bit Rate:11Mb/s
Cell 03 - Address: 00:0D:72:9B:FE:69
          ESSID:"2WIRE086"
          Mode:Master
          Frequency:2.442GHz
          Quality:0/10  Signal level:-28 dBm  Noise level:-256 dBm
          Encryption key:on
          Bit Rate:1Mb/s
          Bit Rate:2Mb/s
          Bit Rate:5.5Mb/s
          Bit Rate:11Mb/s
          Bit Rate:22Mb/s
          Bit Rate:6Mb/s
          Bit Rate:9Mb/s
          Bit Rate:12Mb/s
```

设定网络名称

要与网络连接，首先必须选择打算加入的网络。做法是以*essid*（注1）参数来设定SSID。如果网络名称中包含空白，则必须在前后加上引号。此时网络接口或许尚未启动，因此必须先用*ifconfig*命令启动之后方能进行网络搜寻。要查看扫描的进度，可以连续运行几次*iwconfig*，然后查看扫描至哪个频率。例如，要搜寻使用第56信道的接入点，你可以这么做：

```
[root@bloodhound]# iwconfig ath0 essid "Space Cadet"
[root@bloodhound]# ifconfig ath0 up
[root@bloodhound]# iwconfig ath0
. . .
Mode:Managed  Frequency:2.412GHz  Access Point: 00:00:00:00:00:00
. . .
[root@bloodhound]# iwconfig ath0
. . .
Mode:Managed  Frequency:2.447Hz  Access Point: 00:00:00:00:00:00
. . .
[root@bloodhound]# iwconfig ath0
. . .
Mode:Managed  Frequency:5.17GHz  Access Point: 00:00:00:00:00:00
. . .
[root@bloodhound]# iwconfig ath0
. . .
Mode:Managed  Frequency:5.28GHz  Access Point: 00:0B:0E:00:F0:43
. . .
```

注1：本书会使用“SSID”这个名词来称呼网络名称，包括WaveLAN在内的一些驱动程序则是使用“ESSID”。两者之间的差别在于ESSID是指派给extended service set（扩展服务集）的网络名称，而非固有的service set（服务集）。

一旦网卡发现网络，就会与接入点关联，然后在 *iwconfig* 输出中显示接入点的MAC地址。与网络关联只是第一个步骤。在进行逻辑网络连接之前，也许还需要进行其他配置设定。

如果信道已经通过自动配置方式（automatically configured）设定完成，则会对某些驱动程序造成问题。如果信道已经“设死”（hard set），驱动程序可能就不会进行搜寻。要解决驱动程序卡死在特定信道的问题，可以先以 *cardctl eject* 命令停用网卡，重新设定SSID，然后用 *ifconfig* 重新启用接口。

设定网络信道

不同网卡支持不同的操作频率。采用Atheros芯片组的网卡支持整个ISM频带，最高至第14信道以及三个5 GHz频带。驱动程序如果支持此项操作，就可以使用 *iwlist* 命令列出得到支持的信道：

```
root@bloodhound:~# iwlist ath0 channel
ath0    255 channels in total; available frequencies :
        Channel 01 : 2.412 GHz
        Channel 02 : 2.417 GHz
        Channel 03 : 2.422 GHz
        Channel 04 : 2.427 GHz
        Channel 05 : 2.432 GHz
        Channel 06 : 2.437 GHz
        Channel 07 : 2.442 GHz
        Channel 08 : 2.447 GHz
        Channel 09 : 2.452 GHz
        Channel 10 : 2.457 GHz
        Channel 11 : 2.462 GHz
        Channel 12 : 2.467 GHz
        Channel 13 : 2.472 GHz
        Channel 14 : 2.484 GHz
        Channel 34 : 5.17 GHz
        Channel 36 : 5.18 GHz
        Channel 38 : 5.19 GHz
        Channel 40 : 5.2 GHz
        Channel 42 : 5.21 GHz
        Channel 44 : 5.22 GHz
        Channel 46 : 5.23 GHz
        Channel 48 : 5.24 GHz
        Channel 50 : 5.25 GHz
        Channel 52 : 5.26 GHz
        Channel 56 : 5.28 GHz
        Channel 58 : 5.29 GHz
        Channel 60 : 5.3 GHz
        Channel 64 : 5.32 GHz
        Channel 100 : 5.5 GHz
        Channel 104 : 5.52 GHz
        Channel 108 : 5.54 GHz
```

```
Channel 112 : 5.56 GHz
Current Frequency:5.28GHz (channel 56)
```

操作频率有三种选择方式。如果以之前所描述的方式进行，大多数网卡就会开始搜寻SSID。至于不支持扫描功能的网卡，可以使用*freq*参数直接设定操作频率；或者使用指定适当信道编号的*channel*参数，驱动程序会将信道编号自动转换为相应的频率。以下两道命令可以达到相同的目的：

```
[root@bloodhound]# iwconfig ath0 freq 2.432G
[root@bloodhound]# iwconfig ath0 channel 4
```

设定网络模式以及关联接入点

通常802.11工作站若不是处于ad hoc网络，就是处于infrastructure网络。*iwconfig*将这两种模式分别命名为*Ad-hoc*与*Managed*。你可以使用*mode*参数从中挑选一种模式：

```
[root@bloodhound]# iwconfig ath0 mode Ad-hoc
[root@bloodhound]# iwconfig ath0 mode Managed
```

处于infrastructure网络的工作站可以使用*ap*参数来请求与所指定的MAC地址关联。不过，工作站并不是非得一直与所指定的接入点保持关联，如果信号强度衰减过多，也可以选择漫游至其他接入点：

```
[root@bloodhound]# iwconfig ath0 ap 01:02:03:04:05:06
```

设定数据率

大部分网卡均支持几种不同的位率。*iwconfig*允许管理人员用*rate*参数从中挑选。位率可以在*rate*参数之后指定或者使用*auto*这个关键字，如此一来，在信号质量较差的信道中，网卡就会自动降速至较低的位率。如果*auto*和某种位率结合使用，驱动程序就会使用低于指定速率的任何传输率：

```
[root@bloodhound]# iwconfig ath0 rate auto
```

设定静态WEP密钥

key这个参数用来控制驱动程序的WEP功能。密钥的输入可以使用十六进制数字所构成的字符串。所输入的字符串可以不带任何分隔字符，也可以每4个数字一组，每组数字以破折号隔开或是以冒号区分每个字节。下列命令是等价的：

```
[root@bloodhound]# iwconfig ath0 key 0123456789
[root@bloodhound]# iwconfig ath0 key 0123-4567-89
[root@bloodhound]# iwconfig ath0 key 01:23:45:67:89
```

许多驱动程序也支持104个位的WEP密钥。104个位刚好是13个字节或是26个十六进制字符：

```
[root@bloodhound]# iwconfig ath0 key 12345678901234567890123456
[root@bloodhound]# iwconfig ath0 key 1234-5678-9012-3456-7890-1234-56
[root@bloodhound]# iwconfig ath0 key 12:34:56:78:90:12:34:56:78:90:12:34:56
```

虽然可以在中括号里指定编号来输入多个密钥，但并不是所有网络均会使用这项功能。通过802.1X来指定动态WEP密钥是比较简单的做法，不但可以使用多个密钥，也比较安全。

```
[root@bloodhound]# iwconfig ath0 key 0123-4567-89
[root@bloodhound]# iwconfig ath0 key 9876-5432-01 [2]
[root@bloodhound]# iwconfig ath0 key 5432-1678-90 [3]
```

一旦输入多个密钥后，可以直接以索引编号来选用特定的密钥，而无需使用密钥值：

```
[root@bloodhound]# iwconfig ath0 key [2]
```

要启动或停用WEP处理，可分别用*key on*与*key off*参数加以指定。这些参数可以在选取新的WEP密钥时与索引编号搭配使用：

```
[root@bloodhound]# iwconfig ath0 key [3] on
[root@bloodhound]# iwconfig ath0 key off
```

WEP的处理方式可以区分为两种。*open*（开放）系统接受以明文方式传递的数据帧，而*restricted*（受限）系统会将明文形式的数据帧丢弃。这两个参数均可与索引编号搭配使用：

```
[root@bloodhound]# iwconfig ath0 key [4] open
[root@bloodhound]# iwconfig ath0 key [3] restricted
```

*key*这个参数也可以用*encryption*（可缩写为*enc*）参数来替代。我比较喜欢使用*key*这个参数，因为对我而言比较清楚，不过你可以选择自己喜欢的方式。

调整802.11参数

*iwconfig*允许用户调整RTS与fragmentation阈。大多数驱动程序将RTS阈设为2347，这个值可以有效停用RTS清空功能。在可能有隐藏节点的环境里，可以使用*iwconfig*设定*rts_threshold*（可缩写为*rts*）参数。

```
[root@bloodhound]# iwconfig wvlan0 rts 500
```

fragmentation阈的默认值是2346。在噪声较多的环境里，降低fragmentation阈以减少数据量是值得的，因为当帧漏失或因冲突而损毁时，就必须加以重传。可以使用*iwconfig*

配合*fragmentation_threshold*（可缩写为*frag*）自变量来指定此阈。其值可介于256到2 356之间，不过必须是偶数值。

```
[root@bloodhound]# iwconfig ath0 frag 500
```

802.11工作站本身维护了几个重试计数器。当帧重传“太多”次或等候传输“太久”时，就会被弃置不用。工作站所维护的重试计数器有两种。长帧重试计数器以*retry*参数来指定，代表比RTS阈长的帧的重传次数。短帧重试计数器以*retry min*参数来设定，代表比RTS阈短的帧的重传次数。和一些驱动程序不同的是，*iwconfig*也允许以*retry lifetime*参数来设定每个帧的最长存活时间。要以毫秒（millisecond）或微秒（microsecond）指定时间，可以分别在时间值后加上“m”或“u”：

```
[root@bloodhound]# iwconfig ath0 retry 4
[root@bloodhound]# iwconfig ath0 retry min 7
[root@bloodhound]# iwconfig ath0 retry lifetime 400m
```

Agere (Lucent) Orinoco

无线网络的历史远比802.11标准悠久。一些专属系统在20世纪90年代初期就已经发布并且在市场上取得了一定的占有率。其中最值得注意的产品是NCR的WaveLAN，发布时，NCR还是AT&T的一个部门（注2）。Lucent在1996年由AT&T独立出来时，WaveLAN部门和其他AT&T所生产的通信产品一样被划归为Lucent所有。

早期的WaveLAN硬件完全是封闭的专属系统。802.11在1997年正式成为标准后，符合标准的新硬件才以WaveLAN品牌对外销售。为了区别两者，符合标准的网卡称为“WaveLAN IEEE”网卡，专属系统则只称为“WaveLAN”网卡。

当802.11硬件市场逐渐发展时，Lucent决定将WaveLAN部门以其他品牌重新命名。“Orinoco”这个新名称来自于全世界第三大河流。由于南美的多雨气候，Orinoco汇集了两百条以上支流的水量。在河水高涨时，该河会膨胀为10英里宽，水深达300英尺。1300英里长的Orinoco河有将近1000英里可以航行，难怪这条河的名称原意为“可划船之地”。

在开放源码平台上，Lucent原本采取的策略是提供不同的驱动程序方案。Lucent提供了两种驱动程序。*wavelan2_cs*是封闭源码的专属的二进制驱动程序，此驱动程序提供完整功能。此外，功能较少的开放源码驱动程序*wvlan_cs*以GPL方式授权使用。*wvlan_cs*驱动程序是以封闭源码驱动程序所提供的低级链接库为基础的，不过已经面临发展的死

注2：创办于1884年的NCR（National Cash Register Company）在1991年被AT&T所并购。一家收款机公司会对无线网络产生兴趣，依我推论大概是因为如此一来收款机就可以任意摆放而不必拉线了。

胡同。放弃延续传统路线之后，*wvlan_cs*的低级控制层经过重新改写，成为Linux2.4版内核中的*orinoco_cs*。（*orinoco_sc* 原本称为*dldwd_cs*，代表 David's Less Dodgy WaveLAN Driver！）

除了WaveLAN以及其他OEM版本的WaveLAN网卡外，*orinoco_cs*为一些使用PRISM-2芯片组的网卡以及使用相同MAC控制芯片的Symbol网卡提供了基本功能。2.4.3版内核以后，*orinoco_cs* 成为了 Linux 发行包的一部分。

编译与安装

所有采用2.4版以上内核的Linux发行包均随附了*orinoco_cs*驱动程序。在某些情况下，可以直接使用内核所附的驱动程序。如果打算运行xsupplicant或是需要应用密钥管理功能则另当别论，这些议题将于稍后探讨。

PCMCIA 的配置设定

许多随附*wvlan_cs*驱动程序的旧版发行包仍然还在使用中。要更换发行包所使用的驱动程序，只要换掉系统 PCMCIA 配置的模块即可。*orinoco_cs* 的编写者提供了一个名为*hermes.conf*的文件，其中包含 *orinoco_cs* 所支持的网卡的网卡定义。因为*hermes.conf*以*.conf*为结尾，因此可以在负责读取所有*.conf*文件的*/etc/pcmcia/config*文件的末尾处被导入。不过为了避免绑定上有所冲突，你必须注销所有*wvlan_cs*所使用的部分，以防其与新插入的网卡绑定在一块。另一种做法是先以*dump_cis*读出网卡的识别数据，然后编辑无线网卡的定义以便与 *orinoco_cs* 绑定：

```
# in hermes.conf
#
card "Lucent Technologies Wavelan/IEEE"
   version "Lucent Technologies", "WaveLAN/IEEE"
   bind "orinoco_cs"
# from standard /etc/pcmcia/config
#
# card "Lucent Technologies WaveLAN/IEEE"
#    version "Lucent Technologies", "WaveLAN/IEEE"
#    bind "wvlan_cs"
```

自行编译

这部分涵盖在内核当中，因此通常无需进行安装，除非是为了修复特定的缺陷或者增强某些功能。之所以要重新编译驱动程序，通常是为了支持动态WEP以及802.1X身份验证。xsupplicant发布了一个补丁程序来产生动态密钥。固件或许也得更新才有办法支持动态密钥。我所使用的固件版本为8.42。我确定8.42以上的版本可以正常运作，较老的版本就不见得了。

自行编译的方法十分简单。程序代码本身可以从*http://ozlabs.org/people/dgibson/dldwd/*下载。请确定手上的补丁程序可以修补所有你感兴趣的功能（0.15rc2版不需要rekey补丁）：

```
gast@bloodhound:~$ cd orinoco-0.13e
gast@bloodhound:~/orinoco-0.13e$ patch -p1 < ../rekey_patch_orinoco-0.13e
patching file orinoco.c
patching file orinoco.h
msg@bloodhound:~/orinoco-0.13e$ make
   （省略构建信息）
root@bloodhound:/home/msg/orinoco-0.13e# make install
if [ -d /etc/pcmcia ]; then install -m 644 -o 0 -g 0 hermes.conf /etc/pcmcia/hermes.
conf; fi
mkdir -p /lib/modules/2.4.26/kernel/drivers/net/wireless
for f in hermes.o orinoco.o orinoco_cs.o orinoco_plx.o orinoco_tmd.o orinoco_pci.o;
do \
   if test -e /lib/modules/2.4.26/pcmcia/$f; then \
       install -m 644 -o 0 -g 0 $f /lib/modules/2.4.26/pcmcia/$f; \
   else \
       install -m 644 -o 0 -g 0 $f /lib/modules/2.4.26/kernel/drivers/net/wireless/
$f; \
    fi; \
done
depmod -a
```

编译完成后，系统将会产生几个系统内核模块：*orinoco_cs.o*（PCMCIA接口）、*orinoco.o*（硬件驱动程序）以及 *hermes.o*（MAC 芯片驱动程序）。

设定 orinoco_cs 接口的配置

orinoco_cs 的配置与 *wvlan_cs* 的配置相同。插入网卡之后就会运行 */etc/pcmcia/wireless* 脚本，同时会用到 */etc/pcmcia/wireless.opts* 文件中记载的配置选项。wireless脚本其实不过是 *iwconfig* 程序的前端。编辑 *wireless.opts* 文件中的字段，实际上就是在设定 *iwconfig* 的自变量。设定 *iwconfig* 选项的细节，请参阅上一节论及 *wvlan_cs* 驱动程序的部分。

采用 Atheros 芯片组的网卡与 MADwifi

802.11a 是高速、高密度的 802.11 网络的最佳选择，市面上大多数的 802.11a 设备均会采用 Atheros 芯片组（注 3）。它的驱动程序项目称为“Multiband Atheros Driver for WiFi”，简称为 *MADwifi*，网址为 *http://sourceforge.net/projects/madwifi/*。

注 3：似乎所有支持802.11a的网卡均会使用Atheros芯片组。与其列出一张马上就会过时的名单，我建议各位参考*http://customerproducts.atheros.com/customerproducts/*上所列的客户名单。

安装WEP密钥后的重置动作

在Linux上使用动态WEP时，802.1X supplicant会从认证交换过程中产生WEP密钥，然后将其加载至驱动程序。1999年之前，有些网卡并不支持动态密钥，必须重置（reset）网卡中的微控制器方能让新的密钥生效。当初编写驱动程序时通常会以此为前提，因此更新密钥的程序代码会负责重置硬件。

对动态WEP而言，每次更换新的密钥便重置硬件是无法接受的。一旦身份验证完成，就必须进行密钥的安装。如果驱动程序在密钥安装完成后即进行重置，连接就会中断。接入点注意到连接中断后会要求重新进行身份验证。一旦申请者侦测到连接状态改变，将重新进行身份验证以产生新的密钥。当身份验证再度完成，supplicant又会重置网卡以便安装新的密钥，就这样陷入死循环。

大多数接口卡目前都已提供固件更新，解决安装密钥后必须重置硬件的问题。软件更新为正确版本后，必须将驱动程序一并更新成不会送出重置命令、具备动态WEP能力的版本。

如果动态WEP无法正常运行是因为网卡在身份验证后的重置动作，那么除了查看源代码外，也可以到在线论坛确定网卡驱动程序是否有更新版本或者需要进行修订。

虽然以支持802.11a著称，但Atheros其实推出了好几款不同的芯片组。该公司的芯片组分为三代。第一代芯片组称为5210，只支持802.11a。之后就是第一套双频芯片组5211，加入了对802.11b的支持。目前市面上大多数设备均使用5212，它属于双频（dual-band）/三模（tri-mode）芯片组，同时支持802.11a、802.11b以及802.11g。此外，下一代的产品将能够处理更复杂的安全防护操作。MADwifi支持上述所有芯片组。

驱动程序架构与硬件访问层

MADwifi分为两部分：其一是开放源码驱动程序，其二是称为“硬件访问层”（Hardware Access Layer，简称HAL）的封闭源码链接库。Atheros芯片组相当有灵活性，经过调整后也可以使用非免许可证频带，因为它们使用了某种特定形式的软件定义无线电。

对于FCC的管制规定，Atheros的解读是不得公开硬件访问层（HAL）（在市场上推出类似芯片组的Broadcom也采取同样的解释）。FCC规定要求SDR（软件定义无线电）不得让用户可自行将其变更成运行在非FCC核准的频带。违反FCC认证条款的设备就可

能受罚。如果原本用于免许可证频带的设备突然能够干扰有许可证的（licensed）通信，设备的供应商也将一并受罚（注 4）。

对商业产品而言，要确保软件不致逾越免许可证频带的范围并不困难，只要编译与发布的程序代码不会破坏规定即可。用户无法更动编译后的程序代码，也就无从破坏规定。开放源码改变了整个游戏，发布合乎规定的程序代码不见得可以防止有心人士的恶意篡改。

Atheros 面临一项抉择：是要释放完整的驱动程序源代码并且承担可能遭管制当局禁止销售芯片的处罚措施的风险，或是找出某种可以保护无线电频谱的方式。Atheros 最后显然实行了后者。它通过 HAL 的 API 来访问无线电波，而不让开放源码驱动程序直接访问无线电芯片组。HAL 是相当普遍的做法，其他操作系统也经常借此开发开放源码驱动程序。它们完全独立于主机系统软件，虽然还是离不开主机硬件的指令集。HAL 支持 X86 架构（32 与 64 位）、ARM、MIPS、PowerPC 以及 Xscale。虽然开放源码社群对封闭源码通常怀有疑虑，我认为 Atheros 此举已经体现了他们对于 Linux 平台的承诺，亦即该公司愿意支持驱动程序的开发。

先决条件

MADwifi 广泛使用了无线扩展功能，而且通常以最近的版本进行开发。你可以使用支持最新版本的发行包或者将内核升级至最新版本。

驱动程序通常会用到其他内核功能，MADwifi 自然也不例外。设置 MADwifi 需要用到一些内核头文件以及执行内核所需要的配置文件。如果内核是你针对所使用的硬件平台自行打造的，你手上应该已经有内核源代码以及相关的配置设定。不过内核源代码与配置设定并非所有发行包的默认安装选项，有时候可能必须自行找出正确的软件包。

要取得 HAL，你还需要用到 UUCP 工具。为了能够在任意网络路径上安全地传输 HAL 程序代码，该程序代码需经过 uuencode 的编码。MADwifi 的 *make* 脚本会调用 uudecode。uudecode 可能属于 shell archive utilities 软件包（*sharutils*）或者属于 UUCP tool 软件包，这取决于你所使用的发行包。

注 4： Illinois 大学 Urbana-Champaign 校区的 Christian Sandvig 教授在一篇名为“Hidden Interfaces to ‘Ownerless’ Networks”的论文（*http://www.spcomm.uiuc.edu/users/csandvig/research/Hidden_Interfaces.pdf*）中对 FCC 规则的 SDR 诠释提出反对意见。

构建驱动程序

MADwifi 仍然在继续进行开发，而且经常更新。它是以 CVS 进行维护，而不是定期发布更新的包。要取得最新版本，可以通过 CVS：

```
root@bloodhound:~# cvs -z3 -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/madwifi
co madwifi
```

这道命令执行后，源代码以及编码过的HAL文件便会被下载至*madwifi*目录。要构建驱动程序，可以输入下列开放源码常用的标准命令：

```
root@bloodhound:~# cd madwifi
root@bloodhound:~/bloodhound# make
...
root@bloodhound:~/bloodhound# make install
```

主要的模块是*wlan.o*、*ath_pci.o*以及*ath_hal.o*。其他的一些加密模块会在需要时被加载以支持特定的加密模式。如果MADwifi构建系统无法在文件系统中侦测到正确的安装位置，你就必须手动将这些必要的模块放置于正确的地点，然后执行*depmod -a*来更新模块。

驱动程序的使用

最新版的MADwifi驱动程序会将所支持的网卡列表提供给内核，在检查模块依赖性时就可以看见。此列表包含了一些厂商标识符为0x168c的设备，这个标识符即属Atheros所有。如果模块依赖性正确无误，就没有必要修改 PCMCIA 配置设定脚本。

加载驱动程序会创建一个前缀为*ath*的接口。如果系统中只有一个Atheros网卡的话，通常命名为*ath0*。旧版的 MADwifi 使用 *wlan* 作为前缀。如果接口名称为 *wlan0*，请更新驱动程序。

MADwifi已经与Linux热插拔系统整合无误。插入网卡模块时，热插拔系统会尝试注册该接口。几乎可以确定的是，发行包所使用的启动脚本（start-up script）必然需要修改。使用开放系统的无线网络可能只需稍作修改；使用 802.1X 则需要大幅修改，因为在DHCP 程序运行之前，接口必须已经通过验证。

在 Linux 中使用 xsupplicant

过去几年，我有幸担任Interop Labs无线安全制定小组的志愿者，可以就近体验互用性。2004 年，Open1X 项目的开发人员参加了互用性测试大会，将开放源码带到之前只有产品制造商能够参加的会议。当无线网络逐渐普及时，众人也越来越有兴趣为Linux 系统提供安全的无线局域网络解决方案。*xsupplicant*算是这些802.1X实现产品中的佼佼者。

在 Linux 中使用 Windows 驱动程序

并非所有网卡厂商均承诺支持Linux。释出驱动程序源代码可能侵犯知识产权是主要的考虑因素，必须提供额外人力来撰写、维护与支持释出给用户群的驱动程序则是另外的考虑。

针对 Linux 量身订做的驱动程序通常比较受欢迎。不过，即使网卡厂商尚未提供 Linux 驱动程序，还是可以通过封装程序（wrapper program）来使用 Windows 驱动程序。目前有两种软件包可以运行 Windows NDIS 驱动程序，将 Windows 系统调用转换为Linux 系统调用。NDISWrapper项目（*http://ndiswrapper.sourceforge.net/*）提供了完整的开放源码实现。另外一家名为 Linuxant 的公司则开发出了一套称为 DriverLoader的商业程序（*http://www.linuxant.com/driverloader/*）来提供相同的功能。试用版是免费的，如要继续使用就必须付费。

先决条件

考虑使用xsupplicant之前，最重要的工作是确定802.11已经运作无误。有些“无线”问题实际上是PC Card的问题。当然，除非你已经构建与设定好xsupplicant，否则无法连上已经验证的网络，但是插入无线网卡时系统应该能够辨识得出。辨识出网卡时，Card Service 通常会发出一个高音“哔”声，代表资源已经成功分配，驱动程序也已经加载（后续或许会出现一个低音“哔”声，代表配置设定失败，不过这并没有关系。有可能你希望最后再使用自己的配置设定来运行xsupplicant，因此一开始没有配置设定的支持是可以接受的）。成功加载驱动程序后就可以运行*iwconfig*，以便从驱动程序取得相关的统计信息。

不过就算可以驱动网卡，最好还是要确认一下能否支持动态WEP。虽然动态产生密钥的WEP系统的绝对安全性尚有争论，但它的安全性比单一密钥WEP系统高是毫无疑问的。要使用 xsupplicant 的话，网卡必定得支持动态密钥功能。2003 年初以后发行的网卡均已提供支持动态 WEP 的驱动程序，不过一些较老的网卡就需要进行修补。常见的 Orinoco 802.11b 网卡（使用 Hermes 芯片组）即属后者。编译驱动程序时，你可能还需要重新构建内核（或者至少取得一份内核的配置设定），这得视驱动程序而定。

最后，xsupplicant还需要用到一个链接库。如前所述，大多数的EAP认证方式均以TLS为基础。xsupplicant 使用的是 OpenSSL TLS 实现产品。请安装 0.97 或者之后的版本。从 *openssl.org* 取得源代码之前，请确定你的发行包是否提供该软件包。

编译与安装 xsupplicant

xsupplicant的编译与安装仍是遵循开放源码包的标准例程。你可以从*http://sourceforge.net/projects/open1x/*取得已发布的源代码并以标准 Unix 程序进行编译：

```
root@bloodhound:~# tar -xzvf xsupplicant-1.0.1.tar.gz
root@bloodhound:~# cd xsupplicant
root@bloodhound:~/xsupplicant# ./configure
root@bloodhound:~/xsupplicant# make
root@bloodhound:~/xsupplicant# make install
```

本书即将付印时，xsupplicant1.0.1已经发布好几个月了，CVS版本中已经累积了不少补丁（本节所使用的是最新的2004 CVS版本）。除了一些补丁，这个CVS版本初步支持WPA。CVS版本可以从任何匿名CVS服务器取得，同样是以标准的Unix程序进行编译：

```
root@bloodhound:~# cvs -z3 -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/
xsupplicant co xsupplicant
root@bloodhound:~# cd xsupplicant
root@bloodhound:~/xsupplicant# ./configure
root@bloodhound:~/xsupplicant# make
root@bloodhound:~/xsupplicant# make install
```

构建完成之后，你会在系统中安装三个可执行文件，其中最可能用到的就是*/usr/local/sbin/xsupplicant*。

xsupplicant 的配置设定

运行时，xsupplicant 会在*/etc*目录中搜寻配置文件。默认情况下并不会安装*/etc/xsupplicant. conf*这个配置文件，请自行将它复制到指定位置。

```
root@bloodhound:~/xsupplicant# cp etc/xsupplicant.conf /etc/
```

配置文件中指定了身份验证方式、用户标识符，有时也会指定密码以及证书所在位置以便进行网络验证。网络的证书验证也可以停用，只要将证书位置设为NONE即可，但是不建议这么做。设定网络时，你或许需要将证书转换为其他格式。OpenSSL可以轻易将其转换为各种不同的格式，只要在命令行指定所需格式即可。

```
root@bloodhound:~# openssl x509 -inform DER -outform PEM -in MyCA.der -out MyCa.pem
```

密码以未加密的格式存放在配置文件中，但是你或许希望系统提示你输入密码，而不是将敏感的数据摆在配置文件里。如果配置文件中没有所要连接的网络的密码，xsupplicant就会提示用户输入密码。

配置文件中，每个SSID都可以拥有一份自己的设定描述。在下面的配置文件范例中，一个名为*batnet*的网络上使用了PEAP以及EAP-MSCHAP-V2内部认证方式。xsupplicant可以被设定成在认证完成之后执行命令或是让操作系统上的脚本来执行。

```
### GLOBAL SECTION

logfile = /var/log/xsupplicant.log
network_list = all
default_netname = batnet

first_auth_command = dhcpcd %i

###  NETWORK SECTION

batnet{
  # allow_types = eap_tls, eap_md5, eap_gtc, eap-otp
  allow_types = eap_peap

  # Phase 1 ("outer") identity
  identity = msg
  # Alternative, but common specification is to not reveal username
  # identity = anonymous

  eap-peap {
      # It is a good idea to validate the certificate and not do "none"
      # root_cert = NONE
      root_cert = rootCA.pem
      root_dir = /etc/xsupplicant.d
      chunk_size = 1398
      random_file = /dev/random

      # ** Inner method configuration
      allow_types = eap_mschapv2

      # Inner method configuration
      eap-mschapv2 {
        username = msg
        password = imnottelling
      }
  }
}
```

产生伪随机数

和其他安全协议一样，EAP认证方法需要有“好的”随机数来源。Linux提供两种随机数设备：*/dev/random*与*/dev/urandom*。前者所返回的随机位是从系统的熵池（entropy pool）取得。如果目前没有足够的熵可用，读取动作就会一直等候。后者则会立即返回目前可用数据，代价是牺牲数据的质量。

网络连接与身份验证

要访问经802.1X保护的网络，首要步骤就是与之关联。xsupplicant进行关联的方式与系统有关。初始的配置设定告诉网卡必须使用加密帧，虽然密钥本身并不重要。设定一个假密钥（dummy key）来告诉驱动程序应该使用加密模式。xsupplicant将在身份验证成功后调用wireless extension链接库以便替换密钥。最常见的连接设定方式，就是利用*iwconfig*设定密钥及网络，然后以*ifconfig*启用网络接口及搜寻网络。当然，这些命令可以在插入无线网卡时由配置系统脚本加以执行。

```
root@bloodhound:~# iwconfig ath0 key 1234567890123456789012345 6
root@bloodhound:~# iwconfig essid essid "batnet"
root@bloodhound:~# ifconfig ath0 up
```

系统与网络关联之后就可以运行xsupplicant。*-i*选项指定要在之上运行的接口。调试功能可以通过*-d*选项启动，后续选项则是用来指定要显示出多少信息。*-f*选项可以将log消息显示在控制台（console）。下面是经过删节的原始封包倾印（dump）。

```
root@bloodhound:~# /usr/local/sbin/xsupplicant -i ath0 -dasic -f
Using default config!
network_list: all
Default network: "default"
Startup command: "echo "some command""
First_Auth command: "dhclient %i"
Reauth command: "echo "authenticated user %i""
Logfile: "/var/log/xsupplicant.log"
Allow Types: ALL
ID: "msg"
peap root_cert: "NONE"
peap chunk: 1398
peap rand: "/dev/random"
PEAP Allow Types: ALL
mschapv2 username: "msg"
mschapv2 password: "imnottelling"
Interface ath0 initalized!
```

至此，xsupplicant已经读取了配置文件并且查看了无线接口是否已经与接入点关联。若已关联，则开始进行身份验证过程。

```
[INT] Interface ath0 is wireless!
[INT] The card reported that the destination MAC address is now 00 0B 0E 00 F0 40
[INT] Working with ESSID : batnet
[CONFIG] Working from config file /etc/xsupplicant.conf.
[STATE] (global) -> DISCONNECTED
[STATE] Processing DISCONNECTED state.
[STATE] DISCONNECTED -> CONNECTING
[STATE] CONNECTING -> ACQUIRED
[STATE] Processing ACQUIRED state.
```

一旦系统已经与接入点关联，就会开始进行身份验证。

```
Connection established, authenticating...
[STATE] Sending EAPOL-Response-Identification
[STATE] ACQUIRED -> AUTHENTICATING)
[STATE] Processing AUTHENTICATING state.
[STATE] Sending EAPOL-Response-Authentication
****WARNING**** Turning off certificate verification is a *VERY* bad idea!
You should not use this mode outside of basic testing, as it will compromise
the security of your connection!
[AUTH TYPE] Packet in (1) :
20
[AUTH TYPE] Setting Key Constant for PEAP v0!
[INT] Interface eth0 is NOT wireless!
Userdata is NULL!  We will probably have problems!
[STATE] (global) -> DISCONNECTED
[STATE] Processing DISCONNECTED state.
[STATE] DISCONNECTED -> CONNECTING
[STATE] Processing AUTHENTICATING state.
[STATE] Sending EAPOL-Response-Authentication
```

当双方开始对话并且来回交换与验证证书时，就会出现一些调试信息。一旦建立起TSL隧道，调试信息就会显示内部身份验证。以EAP-MSCHAP-V2为例，RADIUS服务器会送出一个质询信息。有了质询信息与共享秘钥，就可以产生响应信息。

```
 [AUTH TYPE] (EAP-MSCHAPv2) Challenge
[AUTH TYPE] (EAP-MS-CHAPv2) ID : 2F
[AUTH TYPE] Authenticator Challenge : C6 02 26 BE C3 E0 44 03 13 6E 1F BA F0 B3 1D 5A
[AUTH TYPE] Generated PeerChallenge : 28 62 AA A2 8C 8E EB 82 D1 9B 2F 9A 54 67 93 2C
[AUTH TYPE] PeerChallenge : 28 62 AA A2 8C 8E EB 82
[AUTH TYPE] AuthenticatorChallenge : C6 02 26 BE C3 E0 44 03
[AUTH TYPE] Username : msg
[AUTH TYPE] Challenge : 48 E7 AA 53 54 52 98 62
[AUTH TYPE] PasswordHash : C5 A2 37 B7 E9 D8 E7 08 D8 43 6B 61 48 A2 5F A1
[AUTH TYPE] Response : 4D 96 51 8C 18 3A F7 C7 70 15 47 13 19 D8 D6 9B 36
00 AD E8 FA 9A 0F 28
[AUTH TYPE] myvars->NtResponse = 4D 96 51 8C 18 3A F7 C7 70 15 47 13 19 D8
D6 9B 36 00 AD E8 FA 9A 0F 28
[AUTH TYPE] response->NT_Response = 4D 96 51 8C 18 3A F7 C7 70 15 47 13 19
D8 D6 9B 36 00 AD E8 FA 9A 0F 28
[AUTH TYPE] (EAP-MSCHAPv2) Success!
[AUTH TYPE] Server authentication check success!  Sending phase 2 success!
```

一旦通过身份验证，接入点将提供密钥给系统。密钥本身会被“来自第一阶段TLS交换的共享加密密钥”所加密与验证。总共会送出两条密钥信息，其中一条信息包含工作站所使用的单播密钥（unicast key），另外一条信息包含所有工作站共享的广播密钥（broadcast key）。xsupplicant会使用wireless etensions API来设定驱动程序中的密钥，这些密钥可以使用 *iwconfig* 来查看 。

```
Processing EAPoL-Key!
[INT] Key Descriptor = 1
[INT] Key Length = 13
```

```
[INT] Replay Counter = 41 2F BB 2D 00 00 00 D5
[INT] Key IV = 69 4C 45 D7 CF C3 DD CD 2A 3A F3 CB 04 7A F4 A3
[INT] Key Index (RAW)  = 01
[INT] Key Signature  = C2 05 6C 3A EB 25 E9 B9 8E FC 60 D6 77 44 57 22
[INT] EAPoL Key Processed: broadcast [2] 13 bytes.
[INT] Key before decryption : ED 5D 03 D2 7A DE B4 60 29 FD FD F5 42
[INT] Key after decryption : FB BB AC D3 6F 7D 0A 3F FF 2A CF 33 4E
[INT] Successfully set WEP key [2]
Processing EAPoL-Key!
[INT] Key Descriptor = 1
[INT] Key Length = 13
[INT] Replay Counter = 41 2F BB 2D 00 00 00 D6
[INT] Key IV = 66 15 69 E2 B2 8C 0E 89 7C D3 94 8C 93 25 43 1B
[INT] Key Index (RAW)  = 80
[INT] Key Signature  = 49 C1 15 B8 E9 D0 87 53 A6 FD 5D 76 CB 51 9D 65
[INT] EAPoL Key Processed: unicast [1] 13 bytes.
[INT] Using peer key!
[INT] Successfully set WEP key [1]
[INT] Successfully set the WEP transmit key [1]
```

有些驱动程序实现了用自己的系统调用来报告密钥。使用MADwifi驱动程序的 Atheros 网卡可以用 *iwlist ath0 key* 命令列出密钥；有些驱动程序也会在 *iwconfig* 中显示单播密钥。

Linux 上的 802.1X 商用软件

除了 xsupplicant，市面上还有一套由 Meetinghouse Data Communications 公司发行的商业软件。Meetinghouse 的 AEGIS 客户端程序支持相当多的EAP认证方式(MD5、TLS、TTLS、PEAP及LEAP)。不过因为很难跟得上发行包的脚步，因此只为RedHat8与9两个版本提供官方支持。Linux版的Meetinghouse supplicant并未支持WPA，理由和xsupplicant所持的一样：缺乏标准的WPA keying API (WPA动态密钥应用程序开发接口)。

Linux 上的 WPA

通常Linux上并无WPA功能，因为没有一种标准的方式可以取得“进行四次握手”所需要的信息。xsupplicant在用户空间运行，然而计算四次握手所需要的数据却必须从驱动程序取得。每一种驱动程序各自定义了访问这些数据的系统调用，如此一来申请者就必须追踪个别驱动程序所定义的系统调用的后续发展。未来发布的 wireless extensions API将会支持必要的系统调用，到时WPA就会出现在开放源码以及商业产品中。

第二十章

使用802.11接入点

就算是最简单的802.11网络，正确设定接入点（access point）也是一件重要的事。网络接口没设定好，根本就不会有任何数据被桥接至有线网络。

早期的802.11接入点十分简单。通过接入点内设的一组接口，可以将无线设备连接到现有的有线局域网络。早期的接入点相当于无线与有线领域之间的桥梁，另外附带一些其他功能。第一代无线局域网络产品刚上市时，可粗略区分为便宜的家用网关与昂贵的商用产品。这些产品具备同样的功能，不过后者通常采用比较高档的组件，除了保障升级的灵活性与设备的投资，也提供大规模安装所需要的管理工具。

802.11刚问世时，接入点通常设计成独立的设备。早期无线局域网络虽然提供无线访问的功能，但是缺乏牢靠的安全性以及管理方面的能力。虽然这些网络中的孤岛偶尔互相往来，但因为所需要的协议尚未开发完成或未经过大规模的测试，所以通常不被视为大规模网络系统的一部分。当无线网络逐渐普及且规模逐渐扩大，传统上将接入点设计为独立设备的做法开始浮现缺点。

察觉到这股商机，有些厂商开始打造第二代无线网络硬件。新式的做法是将接入点的管理与支持功能整合到具备Ethernet交换器基本功能的机器中，如此一来就只需要配备具有无线接口的傻瓜型（dumbed-down）接入点。虽然做法不同，但业界通常将这种以“轻量级”（lightweight）或者“精简型”（thin）接入点搭配中央控制系统的做法称为“无线交换器”（wireless switch）。自从2002年底开始流行之后，这种交换式（switch-based）架构就引起各方的兴趣，不过基本上它还是提供等同第一代接入点的功能。

本章主要探讨如何使用接入点。除了了解Cisco 1200系列的接入点，本章也会提到Apple的AirPort Express。Cisco 1200属于全功能的独立设备，因为功能很多，所以设定上并不容易。

接入点的基本功能

大致而言，市面上的接入点可以分为两种价位。家用低价机设备过零售管道直接销售给一般用户。这些低价设备属于特殊运算平台，其内存（memory）与外存（storage）能力有限（注1）。高价设备内设一些额外的功能，可以支持较大规模的安装。通常，这些设备配备额外的内存与外存能力并且使用更多通用型（general-purpose）硬件。这两种价位的产品之间的差异在于高价设备能够协同运作自成系统，构建出更加可靠、安全与可管理的网络。举一个稍嫌简单的例子。逐渐延伸到家庭或小型办公室的小型无线局域网络就像无绳电话（cordless phone）。它们可以在有限的距离内延伸网络的使用范围，但仅止于此。大型无线局域网络则像移动电话（cellular telephony），可以在更严苛的环境下维持连接质量。应付经常移动的用户以及接入点间的切换（hand-off）操作只是起码的要求，其所使用的管理与故碍排除工具也比较高级。

然而不论市场如何区分，这些设备还是必须提供一组通用的功能，以达成802.11标准对这些服务所做的承诺。虽然每家厂商配置设定的方式各有不同，不过各家产品在功能与设计上其实极为相似。

最明显的是接入点乃是扮演无线与有线世界之间的桥梁。既然如此，接入点也就具备网络桥接器的所有功能。接入点至少具备两个网络接口：其中的无线接口通晓802.11相关细节，而另一个接口则是连接至有线网络。我还未曾见过不以Ethernet作为有线后端（wired back-end）的接入点，虽然标准的确不曾这样规定。当无线局域网络逐渐普及时，一些高端接入点开始在网络上行链路（uplink）功能方面支持VLAN。有些低端接入点会提供第二个Ethernet端口作为WAN端口，供电缆调制解调器（cable modem）或DSL使用，不过有少数产品只提供支持拨号调制解调器的RS-232串行端口。

所有无线接口都必须支持802.11信道访问的基本规则，不过它们之间的共同点仅止于此。早期的接入点是在网络的边陲地带实现所有802.11协议；新式设备则是把一些802.11功能自网络边陲地带移开，将802.11 MAC分解为跨系统的组件。大多数接入点均可以加装外接天线来微调传输距离与覆盖范围。

桥接器中内设了一些缓冲存储器，可容纳行经两接口间的帧，此外亦会将每个端口所关联的MAC address存储于内部的桥接表。当然，桥接表（bridging table）的实现方式各有不同，业界并无一套放诸四海皆准的做法。功能最大众化或价格最便宜的设备通常认为自己是网络中独一无二的接入点或桥接器。如果接入点支持漫游功能，有时候就必

注1：为了降低成本，低价产品中有许多使用精简版的Linux，这向来都是喜欢自行修改软件（software hacking）人士的最爱。例如HyperWRT（*http://www.hyperwrt.org*）与wifi-box（*http://sourceforge.net/projects/wifi-box*）等项目。

须在接入点间进行联机或用户数据的转移。比较高端的接入点或许需要新增一份基本的桥接表，用来记录有线接口上的 VLAN 信息以及用户如何进行身份验证的相关信息。

商用级的产品在设计上会考虑到设备间的协同运作。最常见的功能是各厂商专属的漫游方式可在接入点间转移关联数据，同时维持链路层的连通性。商用级的产品在网管功能方面通常较为复杂，让网络工程人员得以管理覆盖范围相当大的数十甚至数百台设备。

起初，通过 TCP/IP 网络接口管理接入点属于基本功能。过去几年，一项重大的创举是开发出了所谓的“精简型”（thin）接入点解决方案，将接入点的管理功能集中交由特定设备负责。

根据其所针对的目标市场，接入点可能为无线用户提供不同的服务。其中最受欢迎的服务要算是 DHCP，无线工作站在关联后会被自动赋予一个地址。大型网络中，设备通常使用现有的 DHCP 服务器以确保接入点间的一致性。有些接入点也提供网络地址转换（network address translation，简称NAT），特别是可以连接调制解调器及拨号到ISP的“家用网关”之类的产品。

早在802.11取得成功之前，安全问题一直是无线网络管理人员所关注的焦点。出于安全性的考虑，接入点本身占据了相当特殊的地位。既然接入点是有线网络的网关，在此实施安全策略就再理想不过。除了第一代的安全防护（像MAC地址过滤），目前大多数产品均已实现较坚固的用户身份验证（user-based authentication）。大多数家用产品可以使用预共享密钥来执行“Wi-FI 保护访问”（Wi-Fi Protected Access，简称 WPA），大型企业也可以安装身份验证服务器与之配合。目前，有些高端设备已能完美地整合到现有的有线网络。什么是使用这些功能来扩展有线网络的最佳做法将留待下一章探讨。

管理接口通常无法尽如人意。设定接入点之所以具有挑战性，主要是因为接入点在生产上必须尽可能便宜，而低价设备所具备的处理能力通常难以支持易于配置的引擎所需要的条件。大部分厂商会使用轻量级的操作系统运行于能力较弱的硬件上，然而这种做法的缺点是无法提供足够支持更多功能的程序设计环境。早期的接入点通常会同时提供命令行接口以及基于 Web的管理接口。近来“Wi-Fi 交换器”（Wi-Fi switch）的发展为网管人员带来不少希望。所谓的“傻瓜型”（stripped-down）或“精简型”（thin）接入点是通过少数中央控制交换器来管理，不像过去那样必须分别管理每一个独立的接入点。这些交换器具备较强的运算能力与功能，可以提供更多功能与更完善的管理接口。

调试与故障排除工具如同管理工具一般先进，不幸的是，这意味着它们通常留给网络管理人员一堆难以判别或者毫不相关的信息。理想上，这些产品必须维护网络活动的详细日志，不过时常会见到一些无用的记录，让人难以洞察问题所在。除非维护得当，否则计数器也帮不上什么忙。*ping* 与 *traceroute* 之类的工具程序十分常见，不过网络分析软件及封包捕获工具则不然。

接入点的种类

大致而言，接入点可以分为三种。知名的接入点中有许多是通过各主要消费性电子产品卖场进行销售的低价产品。虽然此类接入点占市场销售的大部分，不过并不适合用于大规模的网络安装。就像消费性电子产品级的 Ethernet 交换器不适合用来构建主要网络，便宜的接入点也无法提供构建主要无线网络所需要的功能。高价设备具备许多重要的功能，主要是针对企业市场。

家用：家庭网关

低价设备包含一般所谓的家庭网关（residential gateway）。家庭网关在设计上尽可能的节省成本，因此只提供一些小型或家庭办公室所需要的基本功能。为了进一步降低成本，大多数家用产品均采用802.11 芯片制造商所提供的“参考设计”（俗称“公版”）。设备制造商也许会（也许不会）更改开版本或外壳，然后贴上自家品牌后就开始销售。

家庭网关通常具备如下特征：

- 大部分设备均内设 DHCP 服务器，便于 plug-and-play（即插即用）的配置设定。
- 用户通常会被部署一个可路由（routable）的 IP 地址，因此使用 NAT 的做法十分常见（注2）。有些接入点使用PPPoE或DHCP动态指定可路由的外部地址（routable external address）。
- 依据家庭网关所面向的客户不同，其所配备的WAN接口有可能是调制解调器、串行端口甚至是DSL（有些家庭网关产品会使用Ethernet端口作为连接端，以便与电缆调制解调器或者 DSL 调制解调器转接）。
- 它们通常自成一个独立的单元并且内设天线。如果找不到适合的安置地点，通常必须重新摆放。
- 有些产品宣称具备 IPSec 通透（*pass-through*）功能，允许通过 NAT 使用 IPSec。根据所选用的 IPSec VPN 解决方案的不同，其支持的程度会有所差异。
- 家庭网关的配置设定通常是通过默认的内部（internal）IP 地址。首次开机时，可以通过 Web 浏览器指定默认地址，然后输入用户名称和密码。有时候，同一家厂商生产的设备会使用相同的默认地址。常见的默认网址是 192.168.0.1，亦即 RFC

注 2：这种NAT实现通常功能有限。它可以将许多内部设备对应到外部IP地址的连接端口，或者将外部 IP 地址的固定连接端口对应到特定的内部地址（例如向内送出的 Web 或 SSH 请求）。有些厂商称之为“端口地址转换”（port address translation，简称 PAT）而非 NAT。

1918在传统的class C保留的第一个内部地址。不过随着无线局域网络的逐渐普及，有些厂商考虑到设备的共存性，就会任意挑选一个地址或者测试该地址是否已被占用。

- 这些产品通常会直接销售给一般用户，因此在设计上极尽美观之能事。不过对一些用户而言，这些炫目的视觉设计反而使他们无法将家庭网关与其他网络设备配合在一起使用。不过，有些厂商刻意设计出只能与自家产品配合使用的产品。
- 小型网络设备的安全性设定选项通常有限。较旧的家庭网关通常只提供MAC地址过滤或静态WEP，因此购买二手设备时必须特别小心。目前，几乎所有市面上销售的产品均已使用WPA的预设共享密钥身份验证搭配动态加密密钥。
- 大多数家用型的无线电系统都很简单。它们通常只配备单一无线接口，使用802.11g或802.11a。前者在家用产品上比较常见，因为802.11g所使用的2.4 GHz频带覆盖范围较广。家庭网络通常受限于Internet的上行链路带宽，因此没有必要以缩小覆盖范围、增加接入点数目来提升带宽。

写作本书当时，家庭网关的价格大约介于35至100美元之间。常见的厂商有D-Link、Linksys与Netgear。Apple的AirPort有时候也被归于此类，不过它的价格显然较高，也具备较多功能。

一般商用：企业接入点

尽管有各种不同的称谓，“企业网关”（enterprise gateway）这个名词意味着用户比较侧重考虑产品的功能，而非产品的价格。除了提供家庭网关（residential gateway）所具备的功能，企业网关还具备一些在大规模环境中所需要的额外功能。企业网关通常具备如下特征：

- 需要在较大的范围内提供移动性且必须有几个接入点彼此合作。企业级产品支持某种协议，可以在接入点间转移联机。
- 企业级产品着重可升级性，目的是尽可能延长产品的使用年限。它们通常采用功能较强的通用型硬件并以软件实现大部分的高级功能，因此相当容易升级。它们也可能采用抽换方便的无线接口。早期企业级接入点使用的是PC Card接口，因此要从802.11b切换到802.11a只要更换网卡即可，顶多配合软件的升级。随着零件价格不断下降，无线网卡通常已经无法升级，不过软件可以。
- 以高级软件控制企业级接入点的好处之一，就是可以随时通过软件更新的方式将最新的安全功能加入接入点。任何称得上企业级的接入点均支持WPA，有些厂商承诺可以通过软件轻易升级至802.11i。当新的安全功能成为标准，不必更换硬件就可以将它们添加到现有网络。企业级接入点通常是以逐层添加的方式新增安全功

能，如此一来，新旧安全机制便可并存共享。通常只有更高档的产品才会抢先以硬件更新安全功能。当初芯片组开始以硬件支持更快的 AES 加密时，就是高端设备最先采用。有些企业级接入点可以同时支持多种安全标准。

- 企业级的部署通常是在相当大的区域内提供地毯式覆盖（coverage blanket）服务。接入点所在之处不见得方便供电，但配线柜（wiring closet）的电力供应通常不会匮乏。所有企业级接入点均支持 IEEE 802.3af 标准，可以通过 Ethernet 获取所需要的电源。
- 高端接入点所使用的无线接口通常比低价产品来得复杂。大多数企业级接入点均提供天线接头，可以加装各式外部天线，根据实际需要来调整覆盖范围或信号质量。有些接入点已经开始采用相当先进的天线技术，允许以非常精密的方式控制传输模式，或者让好几个MAC芯片共享单一天线。传输功率通常可以任意调整，以便扩大或缩小覆盖范围。有些企业级接入点甚至可以使用单一天线支持多组虚拟无线网络。
- 除了可以调整无线电波，企业级接入点也支持某种形式的虚拟接入点。只要设定多组SSID，就可以指定个别SSID的身份验证与加密设定。这项功能通常用来创建安全等级不同的平行网络，除了可以容纳老设备，也可以为新式设备提供最高的安全性。
- 企业级接入点原本就是设计来整合到现有网络的。在安全性方面，这意味着它们必须整合到现有的安全架构中，通常是安插到现有的用户数据库。当用户成功通过网络的身份验证，就可以充分利用网络所提供的服务。第二个整合点，就是企业级接入点用来扩展有线网络现有访问控制与用户权限的方式。
- 在整合到现有网络的同时，也扩展了整个数据平面（data plane）。大多数企业级接入点可以根据身份验证服务器所提供的用户属性来动态指定虚拟局域网络(VLAN)。
- 通常，企业级产品会附带 site survey（实地勘探）工具，网络管理人员可以根据覆盖范围的信号质量来规划大型的部署计划。这些工具的复杂程度不一，有些只能提供一些历史统计数据；有些则十分先进，可以从实际环境中勾勒出网络分布图。
- 为符合管理上的需要，企业级设备的配置设定通常是通过简易的命令行接口或SNMP来完成，而其监控与管理机制也较家庭网关来得完备。有些产品也可以整合到大型管理架构当中，如此一来，只需要一位网管人员就能够监控与设定数以百计甚至数以千计的接入点。
- 企业网关通常是整批安装。任何摆放都必须符合办公空间对于美观上的要求，因此这些设备通常提供较具灵活性的摆放方式。有些是设计成悬挂于天花板之上，而且

可能是阻燃的（*plenum rated*）（注 3）。出于安全上的考虑，安装于风道（air duct）与空调场所（air-handling spaces）的设备均得符合严格的排烟规定。有阻燃的接入点几乎可以安装在任何场所，未取得相关认证的产品就只能安装在某些特定区域。

不过，天下没有白吃的午餐。大多数企业级接入点的价格通常介于 500 至 1000 美元之间，虽然通常会有不少折扣。过去一段时间，高端接入点的价格的确有所下降，但不像家用产品一般有降价压力。Cisco1200与Cisco 1100是企业级接入点中比较经典的产品。两者均使用比较通用的硬件，搭载完整版的 Internetwork Operating System，每隔一段时间就会加入新的功能。Proxim、Symbol、3Com 以及 HP 均提供具备类似功能的竞争性产品。

大型商用：无线交换器

本书第一版问世以来，最大的变化就是“无线交换器”（wireless switch）或“精简型”（thin AP）架构的出现。在此架构中，功能比较简单的几个轻量级接入点由一个中央交换器加以控制。之所以会发展出精简型接入点或无线交换器架构，是为了提供比第一代产品更高的效率。更高的效率，部分来自所使用的技术本身。精简型接入点架构将处理工作从接入点抽离，交由专职设备全权负责。从接入点移除处理工作意味着移除接入点的组件，因此降低了接入点的成本，也增加了接入点的使用年限。如果一并移除接入点的配置设定，就可以进一步减少需要管理的网络设备。

将功能集中在控制器也同时提高了灵活性。同样的成本，将硬件集中于控制器可以提供更强大的处理能力，这样又何必将资源分散给接入点处理。透过各接入点间的协调，网管人员可以平衡各接入点的流量负载、集中监控无线电波的活动情形以及轻易扩展现有的网络功能。

以无线交换器作为解决方案的成本绝大部分取决于网络规模的大小。大多数厂商推出各种不同款式的控制器，能够控制几个甚至数百个接入点。最早推出的解决方案是Symbol的Mobius无线交换器。后续推出的解决方案的厂商，包括Airespace、Aruba以及Trapeze。

以 Ethernet 供电（PoE）

如果希望网络的规模可大可小，以 Ethernet 供电（Power over Ethernet，简称 PoE）就极为重要。设计无线网络时应该从无线电波的传播（而不是以电源供应）的角度考虑接入点的摆放位置。

注 3：焰色试验（flame test）的相关信息参见 *http://www.houwire.com/catalog/technical/cable_flame.asp*。

第一波销售的接入点产品与其他计算设备采用同样的供电方式，亦即将电源线插入最近的AC电源插座。糟糕的是，有些产品所使用的变压器居然会挡到隔壁的插座。接入点的摆放受制于附近是否有电源插座，而不是考虑哪些地点能够提供最佳的服务。如果受限于必须靠近电源，接入点的位置变更就不是那么容易。

由于电气方面的工作有其危险性，所以有些地方的法律规定必须聘请合格的技师操作。有些机构也会与行业协会协商，要求提供有经验的电工。这时候，变更接入点的摆放位置就可能所费不菲。但在有些地方，Ethernet之类的数据线由网络技术人员拆装即可，因此接入点可以由非行业协会成员进行安装或变更摆放地点（注4）。

PoE的种类

市面上有各种不同的电源设备，其中有许多符合IEEE 802.3af标准。802.3af所定义的传输标准是可以在整段Ethernet电缆中供应48伏特的直流电，最高可达15瓦。这份标准可以从IEEE Get802网站下载，进一步的信息可从*http://www.poweroverethernet.com/*取得。

它们最基本的差别在于通过Ethernet电缆中的哪几对线供电。数据通常是通过数据线（第1、2对和第3、6对）传送。标准中，A版本以数据线供电，而B版本则是通过其他未使用的线（第4、5对和第7、8对）供电。以数据线供电时，正负极有两种配置方式，如图20-1所示。脚位的安排如表20-1所示。以非数据线供电时必须使用特定的极性。并非所有厂商均将第一对线当作正极，值得一提的例外是Cisco早期的专属电源装置，其所定义的极性只供自己公司的设备使用。

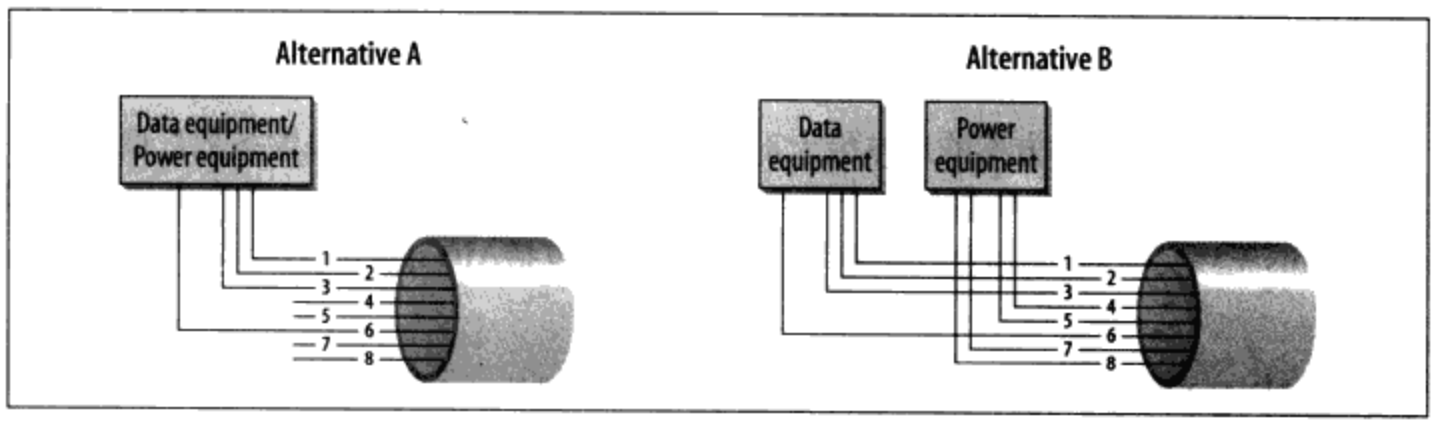


图20-1：电源线路图

注4：有些行政部门将Ethernet定义为“低压布线”(low-voltage wiring)，必须由电工来安装。华盛顿州的雷德蒙市将低压布线视为构建许可证过程的一环予以课税。

表20-1：802.3af的线路定义

线号	第几对线	版本 A（MDI-X）	版本 A（MDI）	版本 B
1	1-数据	−	+	
2	1-数据	−	+	
3	2-数据	+	−	
4	3（未使用）			+
5	3（未使用）			+
6	2-数据	+	−	
7	4（未使用）			−
8	4（未使用）			−

电源设备的种类可以从电源供应的角度做进一步区分。电源设备如果内设于交换器，就称为终端（*endpoint*）电源。另一种方式是使用馈电器（*power injector*）来提供电力，称为中跨（*mid-span*）设备。目前大多数802.11网络安装均使用馈电器或所谓的中跨设备。如果交换器厂商所生产的电源设备（power blade）得到更广泛的使用，终端供电就会更加普及。图20-2显示了两种不同的选择。中跨式选项的馈电器可以是独立设备，也可以是具有好几个供电端口的“电源插线板”（power patch panel）。Gigabit数据链路只能够使用终端供电，虽然这对802.11而言尚无重大影响。

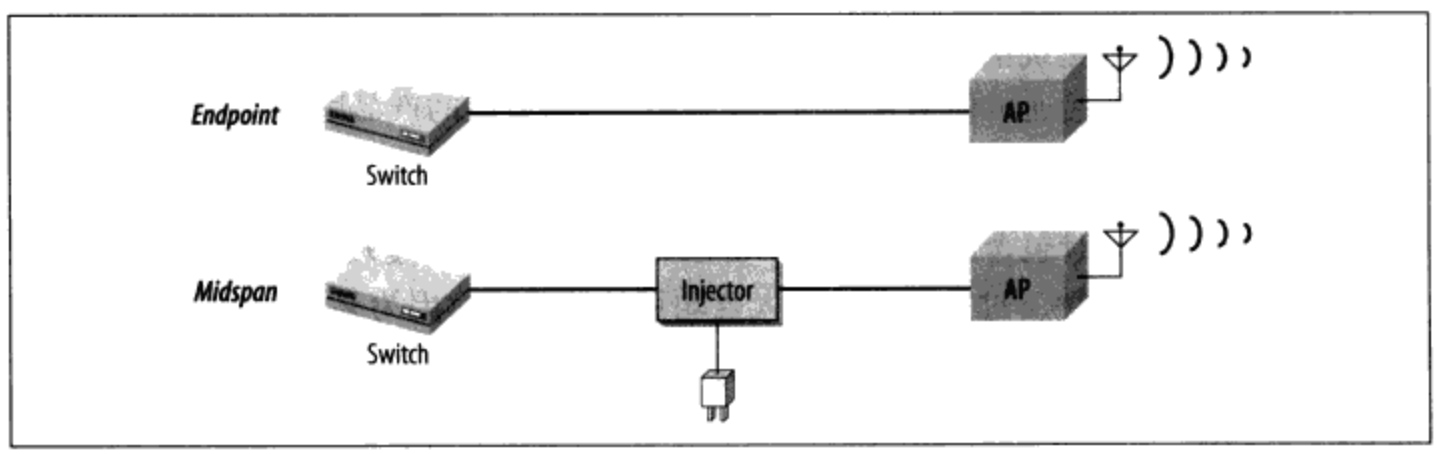


图 20-2：终端电源与中跨馈电器

802.3af提供电源侦测机制，可避免烧毁插入供电端口的设备。早期的PoE设备随时提供全电压，规格不符的设备可能因此而烧毁。为了安全，802.3af提供了一种握手机制，可以逐步提升电压。如果初次侦测得不到任何反应，就会停止供电以保护终端设备。

馈电器通常配备两个Ethernet端口以及一条电源线。其中一个Ethernet端口用于连接网络，第二个Ethernet端口则为之供电。值得一提的例外是Cisco的AIR-PWRINJ-FIB，它使用Ethernet端口供电，但以100BASE-FX光纤作为网络连接。

选购接入点

选购接入点时，必须将一些因素纳入考虑。随着802.11成为主要标准，是否符合标准已经不再是主要考虑因素。任何打算构建大型网络的厂商都必须提供符合当前所有标准的兼容性，而且通常需要承诺支持未来制定的重要标准。有些机构已经推出测试方案来验证互用性。其中最著名的就是Wi-Fi联盟的Wi-Fi认证，虽然其他机构眼见无线局域网络逐渐普及，也推出类似方案与其争抢这个市场。目前业界最严谨的测试方案是由New Hampshire大学的互用性实验室（Inter-Operability Lab，简称IOL）所推行的。IOL的测试方案不如其他商业性测试方案出名，因为它的目的是协助开发更好的产品，而不是提供营销上的“认可盖章”（seal of approval）给厂商。如同以往，研究认证方案时，最好确定厂商已经通过你所感兴趣的相关测试。

部署无线网络时，安全性通常是主要考虑的。既然WEP已遭彻底破解，在选购接入点时最好确定它支持802.1X与802.11i安全功能。小型网络部署可以使用预共享密钥身份验证，不过比较侧重安全性的网络部署就应该采用完整的RADIUS整合方案。在比较大型的环境中，选用能够提供多个虚拟接入点同时允许不同加密与身份验证组合的产品，或许比较值得。

有时候，如何供电给接入点是部署时会遇到的头痛问题。为了覆盖较大的范围，通常必须将接入点置于电源所不及之处。使用较长的天线可能使信号质量降至可接受的水平以下，因此最好还是就地提供电源。安装新的电源插座通常十分昂贵。这些工作必须由合格的技师完成，况且建筑消防法规也有额外的限制。有些产品可以通过Ethernet电缆提供电力。较便宜的产品通常使用专属的电源设备，价格较高的产品则使用符合标准的电源设备。网络线没有电源线那么多的限制，网管人员可以自行布线。

有时候，使用环境同时包含室内与户外。要在一个区域提供密度较高的覆盖率，外接天线通常可以派上用场。不过并非所有接入点均可外接天线，因为必须付出额外的成本。就算接入点配备外接天线接头，也无法保证可以找到适合的天线。802.11只规范外接天线的转接头必须具备50 ohms的标准阻抗。如果外接天线对整个部署计划而言十分重要，最好确定有足够类型的天线可供使用，不论其来自802.11厂商还是其他。户外安装通常需要使用“耐候”（environmentally“hardened”）的接入点或以耐候材料包裹。

校验接入点需要符合哪些条件时，也必须将环境因素纳入考虑。安装于空调场所的设备必须是阻燃的（plenum rated）。认证时会在受测的设备上点火，然后检测所产生的烟雾浓度。浓烟可能会通过通风系统与管线弥漫到整座建筑物，遮蔽紧急出口标志且造成伤亡。阻燃的设备所采用的材料不会产生浓烟，而烟雾通常容易造成危险。即阻燃的接入

点之所以比较安全，是因为不至于产生浓烟遮蔽出口，而不是因为它的烟雾不具毒性。安装在天花板上面的设备通常不需要是阻燃的，除非天花板上方就是换气口。配备气道的建筑物通常不必使用阻燃的接入点，但有些建筑校验单位可能会误认有此必要，而有些地区的建筑法规也的确有此要求。

如果漫游十分重要，就必须从不同技术与做法中挑选合适的解决方案，因为不同厂商提供的产品之间或许无法顺利漫游。确保各家产品间的互用性的最佳方式，就是选购以“动态 VLAN 分配”（dynamic VLAN assignment）作为漫游与切换（handoff）基础的系统。工作站进行身份验证时，将可以通过相同的“逻辑附接点”（logical point of attachment）连接至网络。

802.11在标准中包含了一些省电功能，这些功能绝大部分不具强制性。如果在部署时主要是使用以电池供电的设备，那么最好评估一下该设备提供了哪些省电功能。此外，最好先试试看，如果启用省电功能，电池可以持续多久时间。

设备管理也必须加以考虑。无线网络属于新的服务，对于新的硬件，网络人员必须加以规划、评估、采购、部署以及维护。大型部署可能会用到数十甚至数百个接入点，若无适当工具，那么对网络管理而言这将是一项头痛的问题。厂商是否提供接入点管理工具来平行配置许多设备？接入点的管理是否能够整合到现有的网管基础架构中，以便使用已安装完成的工具？这些管理工具是否够安全？许多产品只能够以明文协议（clear-text protocol）加以管理，这无疑会危及或违反目前既定的安全策略。经验显示，网络设备软件升级十分频繁。那么，软件该如何升级？升级又可以提供多少功能？新的协议功能是否能够通过软件加以升级？

在采购之前，可以根据部署的规模加以评估。看看自己是否可以感受每个接入点所能覆盖的范围，或使用一些常见的网卡加以测试。802.11网络的负载能力完全取决于无线链路，不过你或许希望确定是否有其他的负载限制。如果启用安全性协议，接入点是否能够提供最大的负载能力？有些产品针对所有协议提供加密加速机制（cryptographic acceleration），有些则无。仅靠单一加密处理器来运行安全系统的产品，在升级至较快的物理层标准后或许会不够使用，也有可能受限于上行链路带宽。目前，Fast Ethernet 虽然足够应付802.11a/g网络所需，不过未来就可能成为802.11n标准的瓶颈。试着架设一个测试网络，感受一下如果要将接入点整合至现有网络，应该如何配置。

和所有采购决策一样，有些“软”因素是不容易量化的。产品的保证、与厂商的关系以及技术支持的质量，种种因素都会影响到采购的决策。因为软因素既不属于技术层面，也不容易量化，所以在此不予置评。

真的需要接入点吗？

无线网络不见得需要配置接入点。无线工作站可以彼此形成独立型网络，根本用不着接入点。设置一台Unix机器来作为Ethernet与无线网络间的路由并不困难，况且所需要的硬件可以从旧机器堆中回收使用。那么，为什么要用接入点呢？

既然家用网关的价格已经跌破100美元，对只需单一接入点的网络而言，构建一台Unix路由器已经不符成本效益。只要想想必须花费多少工时成本，就知道构建一台Unix路由器算不算是浪费。何况，接入点的硬件与通用型平台相比亦有其优点。接入点设备较小，无其他琐碎零件。因此，它们所耗费的电力较少，也不会产生多少热量。Apple所提供的“软件基站”（software base station）算是例外，它可以将任何台式计算机转变为桥接用的接入点。只要稍加设定，一台台式计算机就可以摇身一变成为接入点。

以Unix主机充当路由器在较大型的部署上不具效率，主要是因为无法支持移动性。有效的漫游需要通过桥接（而非路由器）来访问不同地理位置的链路层。不过，在802.11中，除非接入点之间能够彼此沟通，借此追踪无线工作站的行踪，否则也无法提供漫游。未来或许会出现开放源码的Unix包，可以提供接入点的所有功能：访问802.11网卡基本参数的低等能力、Ethernet的桥接能力以及IAPP。在此之前，商用级产品还是无可替代的。

Cisco 1200 接入点

Cisco1200系列接入点是独立式（standalone）接入点的典型代表。它所运行的是Cisco的IOS操作系统。1200系列原本采用的是基于VxWorks的系统，不过后来Cisco发布了IOS，可用来升级1200。升级工具可以从Cisco的网站下载。目前VxWorks的版本已经停止开发，也不再增加新的功能。

Cisco 1200可以通过Web接口或IOS命令行接口单独设定。设备数量较多的话，则可以通过Wireless LAN Solutions Engine（简称WLSE）进行管理。通过一条使用Cisco RJ-45脚的串口电缆，就可以进入命令行接口；或者等到网络接口就绪后，以telnet或SSH登录。

设定 1200 接入点

1200的硬件设定十分简单。它可以使用本身的电源供应器（power supply）或者Cisco专用的馈电器（power injector），两者的电路相同。电源供应器的输出为48伏特，和馈电器一样。

Unix-Based 接入点

打造一个Unix-based接入点的先决条件之一，就是启动无线网卡上的接入点功能。其中一个困难所在，就是必须重写802.11标头。在基础结构型网络（infrastructure network）中，所有流量均会流经接入点。接入点必须重写802.11标头中的传送端与接收端的地址。此外，可能还会用到其他的管理功能。举例来说，802.11规范包含了基础结构型网络所使用的一些省电机制，不过必须通过接入点实现，方能使用这些功能。

此外，还有一些非技术性的障碍。有些厂商会十分积极，相当支持自家网卡的Unix开放源码驱动程序的开发工作。毕竟，厂商是通过销售硬件获利，可以将网卡销售给所有的客户系统当然是件好事，就算使用在开放源码的Unix平台上亦然。不过，接入点则不然，厂商们通常不愿支持将网卡变更为接入点模式的接口。因为接入点比较有利可图，而如果为网卡提供驱动程序接口，使之可以支持接入点的功能，无疑会妨碍接入点的销售。

就某些方面而言，要将采用Intersil芯片组的网卡转变为接入点，唯一的方法是向Intersil购买公版（此公版附带具备接入点功能的固件，而该固件并未分开销售）。Intersil所销售的工作站固件，当中的确包含所谓的“Host AP Mode”（仿AP模式）。在此模式下，PRISM-2芯片组会自动处理一些“低级的”工作，例如传送Beacon帧及响应Beacon帧。Jouni Malinen所开发的驱动程序可以在Linux kernel 2.4中使用Host AP Mode。连同内核所实现的Ethernet桥接功能，此驱动程序可用来构建一个接入点。该驱动程序可从*http://www.epitest.fi/Prism2/*下载。

以驱动程序目前的现状而言，构建一个Unix-based路由器不无可能（在此，我学术性地称“路由器”为“第三层网络设备”）。其中一个接口可像以往一样连接至有线网络，而第二个无线接口可以IBSS模式运行。Ross Finlayson利用一个FreeBSD-based路由器，已经在加州Mountain View一家咖啡馆中构建了一套小区网络。该项目的网址为*http://www.live555.com/danastreet/*，该路由器也有专属的网页*http://www.live555.com/wireless/unix-base-station.html*。

1200使用了一个“桥接－组虚拟接口”（Bridge-group Virtual Interfac，简称BVI）。BVI是IOS所使用的一种软件功能（construct），可以允许同一个接口上的协议的路由（routing）与桥接（bridging）。接入点需要将802.11帧桥接到802.3，但也需要路由IP封包进行管理操作，因此BVI就成为理所当然的选择。必须在全局配置提示符（global configuration prompt）下方能设定BVI的IP地址。接入点的IP地址可以手动指定，也可以通过内置的DHCP客户端程序取得：

```
ap1200# configure terminal
ap1200(config)# interface BVI1
ap1200(config-if)# ip address 192.168.1.5 255.255.255.0
ap1200(config-if)# ip address dhcp client-id FastEthernet0
```

要检查接口的状态以及确认是否已经指定地址，可以使用 *show ip interface* 命令：

```
ap1200# show ip interface brief
Interface              IP-Address     OK? Method  Status  Protocol
Dot11Radio0            unassigned     YES TFTP    up      up
FastEthernet0          unassigned     YES NVRAM   up      up
Virtual-Dot11Radio0    unassigned     YES TFTP    down    down
BVI1                   192.168.5.191  YES DHCP    up      up
```

无线接口的配置设定

1200 配备了两个无线接口。Radio 0 为 2.4 GHz 的无线电，通常使用 802.11g，不过较旧的硬件可能还是使用 802.11b。Radio 1 是 5 GHz 的无线电。每个接口均可使用接口配置设定命令分别加以设定。数据率（传输率）可以只用 *speed* 命令来设定或者加上 *basic-* 前缀。在下面的范例中，第一个speed命令允许使用所有传输率。第二个命令指定1 Mbps 与 2 Mbps 操作为必要的，但也允许 5.5 Mbps 与 11 Mbps 操作。最后两个命令比较特别。*speed range* 允许使用所有传输率，不过只有最低速率为必要的。*speed throughput* 会将所有传输率设为必要的。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# speed 1.0 2.0 5.5 11.0
ap1200(config-if)# speed basic-1.0 basic-2.0 5.5 11.0
ap1200(config-if)# speed range
ap1200(config-if)# speed throughput
```

以 milliwatt（毫瓦）为单位设定“本地最大功率”（local maximum power）即可对每个接口进行传输功率配置设定。和传输率一样，*power* 这个命令会因接口而异。802.11 b/g 接口最高只允许使用 100 mW 的功率。由于 OFDM 芯片设计上的限制，802.11a 接口最高只能够设定到 40 mW。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# power local 100
```

除了功率设定外，还可以使用 *channel* 命令为每个接口设定操作信道。*channel* 之后必须提供以 MHz 为单位的频率作为自变量。另外一种做法是在 *channel* 命令之后输入 *least-congested* 关键字，让接入点自行挑选最合适的信道。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
```

```
ap1200(config-if)# channel 2412
ap1200(config-if)# channel least-congested
```

接入点可以使用两种 802.11b 前导码。长前导码兼容性较好，不过短前导码性能较佳。一般而言，应该将这个选项设为 short，除非网络中存在一些老设备。要停用短前导码，可以使用 *no preamble-short* 接口命令。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no preamble-short
```

Beacon 帧用来宣告网络的存在，DTIM 信息元素则是用来宣告有暂存帧。通过 Beacon 帧间间隔的微调，可以使用 *beacon period* 与 *beacon dtim-period* 命令在暂存帧的传送与电池的消耗之间找出平衡点。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# beacon period 100
ap1200(config-if)# beacon dtim-period 5
```

除了 Beacon 帧间隔，也可以设定 RTS/CTS 阈值。较低的设定值将导致 RTS/CTS 握手过程开始进行。根据所处的环境，以下面的命令来调整帧的重传次数或是进行帧分割的阈值可能会有所帮助：

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# rts threshold 2000
ap1200(config-if)# rts retries 2
ap1200(config-if)# packet retries 8
ap1200(config-if)# fragment-threshold 1500
```

网络互联

不同客户端将会以不同的方式封装帧。到目前为止，最常使用的是 RFC 1042 所规定的 SNAP 封装格式，这是本接入点的默认值。IOS 也允许使用 802.1H。这个设定只能针对无线接口做全局设定，无法针对个别协议。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# payload-encapsulation snap
ap1200(config-if)# payload-encapsulation dot1h
```

随着“动态VLAN分配”(dynamic VLAN assignment)的出现，在有线网络中使用VLAN已经日渐普遍。1200 的 IOS 同时支持原生（native）与标记式（tagged）VLAN。重点在于必须在相同的 IP 网络中将 VLAN 1（即 native VLAN）指定给网络上的其他设备，以确保能够通过所谓的 native VLAN 进行通信。要指定 native VLAN，可以在子接口的 encapsulation 命令之后加上 *native* 关键字。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# interface fastethernet 0.1
ap1200(config-subif)# encapsulation dot1q 1 native
```

其他的VLAN 可以用同样的方式来设定，但省略掉 native这个关键字。常见的做法是将子接口编号作为VLAN tag。举例来说，要设定VLAN 10，可以用下面的命令。要设定VLAN 20，只要将 10换成 20 即可。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0.10
ap1200(config-subif)# encapsulation dot1q 10
ap1200(config-subif)# interface fastethernet 0.10
ap1200(config-subif)# encapsulation dot1q 10
```

安全性的配置设定

接入点所广播的SSID代表无线网络。在1200中，每个SSID就代表一个独立运作的虚拟接入点。每个SSID均有自己的安全性配置设定以及自己的VLAN映射方式（VLAN mapping）。值得注意的是，这些VLAN的映射方式显得有些冗杂。默认的VLAN可以被指派给SSID。如果所使用的RADIUS服务器返回不同的VLAN，客户端设备将会被重新映射到所指定的VLAN（注5）。不过，只有当RADIUS服务器完全不提供任何VLAN时，才会使用这种指派给每个SSID的默认值。（这种做法不如市面上其他产品来得纯粹，亦即若非使用默认VLAN，就由RADIUS服务器提供）。

每个SSID的身份验证使用authentication命令进行配置设定。一般而言，这个命令会将身份验证的方式设定为“开放”（open），但可能会加上EAP作为认证方式选项。下列命令会把名为babefish的SSID映射到VLAN 42，并且要求对服务器组 *rad_eap* 进行EAP身份验证。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid babelfish
ap1200(config-ssid)# vlan 42
ap1200(config-ssid)# authentication open eap rad_eap
```

要定义用来进行EAP身份验证的RADIUS服务器，首先得指定有哪些服务器，然后将它们加入一个组。默认情况下，如果没有指定UDP端口，RADIUS服务器就会使用老式的RADIUS端口（1645与1646），因此必须加以指定后才能使用新的端口号。

注5：设定时必须提供一组RADIUS隧道属性（tunnel attribute）给Cisco接入点，而且必须加以标记（tagged）。在Cisco接入点中，Tunnel-Type属性必须设为VLAN，Tunnel-Medium-Type属性必须设为IEEE-802，而Tunnel-Private-Group-ID属性则必须设为VLAN ID。

```
ap1200# configure terminal
ap1200(config)# radius-server host 192.168.200.187 auth-port 1645 acct-port 1646
key MySecret
ap1200(config)# radius-server host 192.168.200.188 auth-port 1812 acct-port 1813
key MySecret
ap1200(config)# aaa group server radius rad_eap
ap1200(config-sg-radius)# server 192.168.200.187 auth-port 1645 acct-port 1646
ap1200(config-sg-radius)# server 192.168.200.188 auth-port 1812 acct-port 1813
```

WPA-PSK 的配置设定

WPA 预共享密钥是通过 SSID 命令来设定的。以 SSID 命令设定好 WPA 密钥管理功能后，就可以指定 WPA 所使用的 ASCII 或十六进制预共享密钥。

```
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid LuminiferousEther
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii Thisisaverylongsecretpresharedkey!
```

监控

欲列出所有已关联的工作站，可以在一般提示符下输入如下的命令（这是一项基本的监控工具）：

```
ap1200> show dot11 association

802.11 Client Stations on Dot11Radio0:

SSID [LuminiferousEther] :

MAC Address  IP address        Device      Name        Parent      State
0002.2d6e.abda 192.168.200.150 -           -           self        Assoc
```

要查看特定关联的详细资料，可以指定对方的MA 位址，如此就会列出完整的关联记录，包括所使用的加密方式。下面这个已关联的工作站以TKIP 作为加密的方式：

```
ap1200> show dot11 association 0002.2d6e.abda
Address              : 0002.2d6e.abda Name          :
IP Address           : 192.168.200.150  Interface   : Dot11Radio 0
Device               :  -  Software Version         :
CCX Version          :
State                : Assoc  Parent                : self
SSID                 : LuminiferousEther  VLAN      : 0
Hops to Infra        : 1  Association Id            : 120
Clients Associated   : 0  Repeaters associated      : 0
Tunnel Address       :0.0.0.0
Key Mgmt type        : WPA PSK  Encryption          : TKIP
Current Rate         : 11.0 Capability              :
Supported Rates      : 1.0 2.0 5.5 11.0
Signal Strength      : -39  dBm Connected for       : 1463 seconds
```

```
Signal Quality      : 79 % Activity Timeout        : 55 seconds
Power-save          : Off  Last Activity           : 4 seconds ago
Packets Input       : 535  Packets Output          : 245
Bytes Input         : 61629  Bytes Output          : 137018
Duplicates Rcvd     : 0  Data Retries              : 18
Decrypt Failed      : 0  RTS Retries               : 0
MIC Failed          : 0
MIC Missing         : 0
```

故障排除

IOS 提供了一些额外的调试工具，可用来排除问题。*debug* 命令用来启用追踪功能，然后可以指定所要追踪的对象。追踪信息默认会被送到控制台（console）。如果通过网络关联到接入点，就必须以如下的命令将调试信息导入当前的登录画面：

```
ap1200# terminal monitor
```

采取安全防护措施的802.11网络最容易出现问题的地方，就是一开始的关联与密钥传递阶段。这些问题的故障排除可以通过 *debug dot11* 以及相关副命令来达成。一些常用的“故障排除”调试命令如表 20-2 所示。

表 20-2：Cisco 1200调试命令

调试范围	命令	附注
EAP 身份验证	debug radius authentication	显示 RADIUS 封包，解码
	debug dot11 aaa authenticator process	属性，解释行为
	debug dot11 aaa authenticator state-machine	显示服务器逾时或失败
MAC 地址过滤	debug dot11 aaa authenticator mac-authen	显示 MAC 地址以及身份认证系统的响应信息
WPA	debug dot11 aaa authenticator process	显示密钥交换过程
	debug dot11 aaa authenticator state-machine	
	debug dot11 aaa manager keys	

关闭调试功能十分简单，只要输入如下命令即可：

```
ap1200# undebug all
```

Apple AirPort 接入点

目前 Apple 在市面上推出了 AirPort Express 与 AirPort Extreme 两款接入点，两者均采用 802.11g 规范。AirPort Extreme 在设计上比较像是家用网关，而且具有一个调制解

调器端口与外部天线接头。虽然价格比市面上其他产品高出不少，但它的功能较多，得到许多小型办公室的青睐。

初次设定

和设定新的无线接口一样，初次设定也是使用同一套 AirPort Setup Assistant 应用程序。AirPort 接入点会对外宣告本身的存在，Mac OS 用户端可据以设定联机参数。连接到 AirPort 接入点并且点击配置设定画面后，就会出现如图 20-3 所示的网络安全性设定画面。图中的配置设定画面显示目前采用WPA pre-shared key安全性设定。如要设定WEP，同样是通过这个画面。

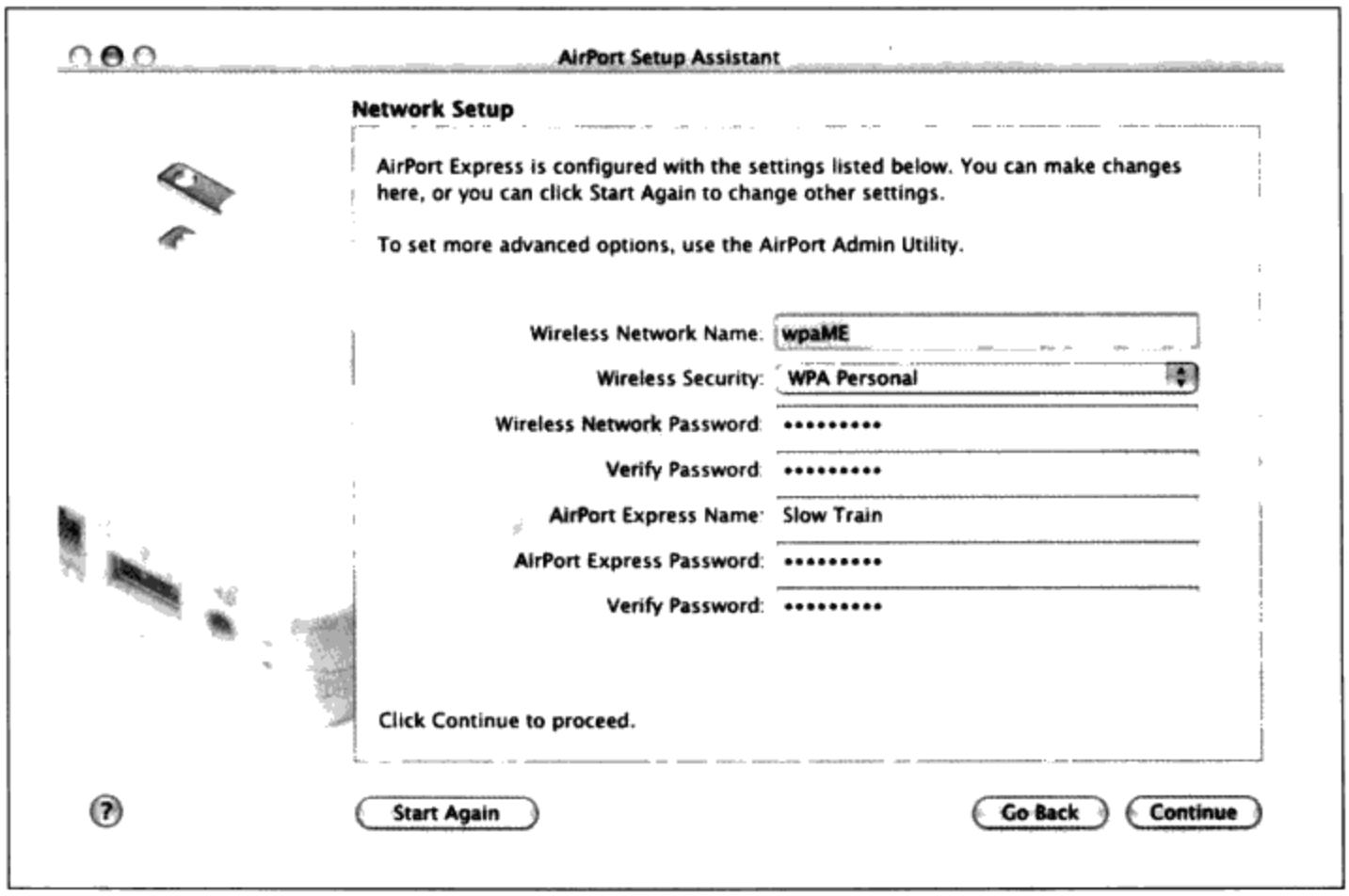


图 20-3：网络安全性设定

管理界面

一旦以 Setup Assistant 完成初次配置设定，AirPort 接入点便会出现在网络上，此时必须以 AirPort Utility（图 20-4）加以设定。这是另外一套设定工具，如果你看过 Lucent 的 AP Manager，必然会感到相当熟悉。程序开始运行后，AirPort Admin Utility 会搜寻网络中所有 AirPort 接入点并且以列表方式显示。只要挑选个别的接入点，就可以进

一步加以设定。配置变更之后，接入点必须重新启动，变更才会生效。上方所显示的“Other”按钮可用来设定任何 AirPort 接入点，只要管理人员能够送出 IP 封包至该接入点。距离较远的接入点可能不会出现在列表中，不过只要点击“Other”按钮的同时输入 IP 地址，即可设定任何以 IP 相连的接入点。

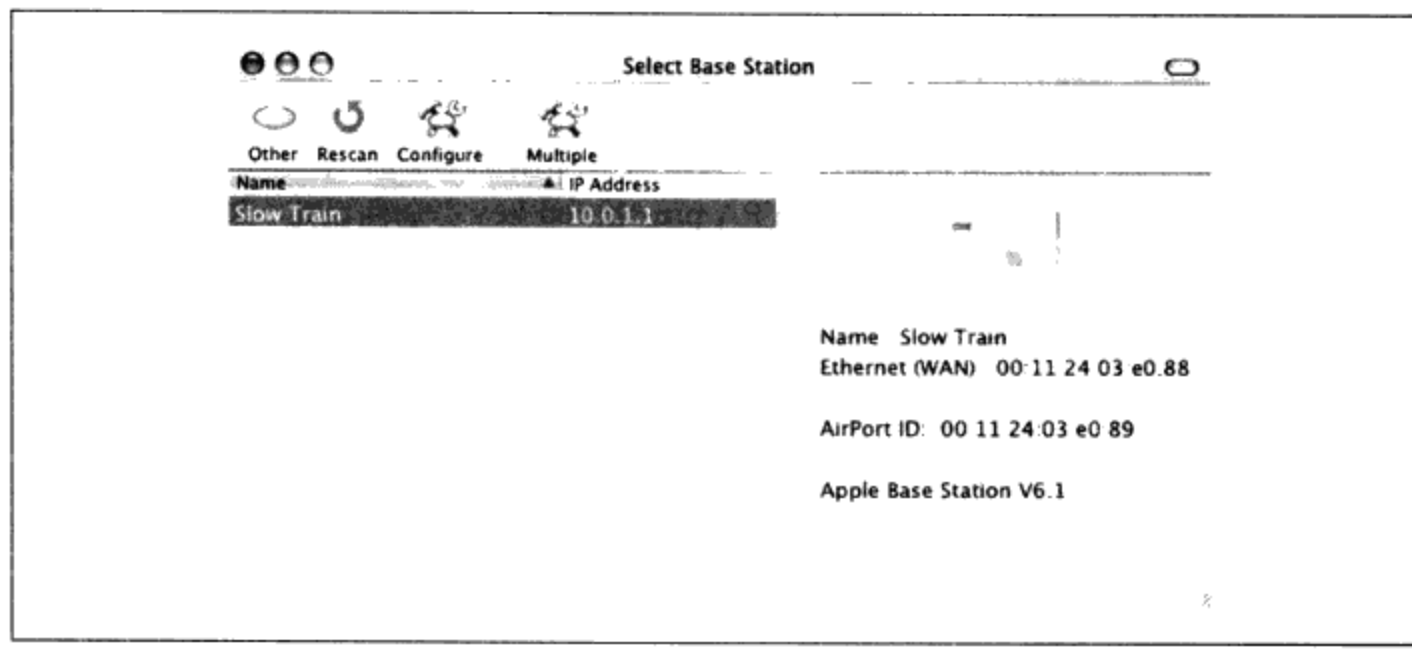


图 20-4：AirPort Admin Utility 主画面

设定无线接口

为所选定的接入点进行配置设定时，会出现配置设定画面。配置信息以标签页（tab）区分为各种逻辑单元，默认选用无线接口配置设定（wireless interface configuration）标签页。画面上方有一些按钮可用来重新启动接入点（Restart）、更新软件（Upload）、还原出厂设定（Default）以及更改密码（Password）（新软件通常随 Admin Utility 包一起发布，如果管理软件发现有新的版本，就会自动进行软件升级）。

AirPort的配置设定过程如图20-5所示。安全性设定类似之前图20-3所显示的。“closed network”选项会移除Beacon帧中的SSID信息元素，想要关联到网络的工作站时必须自行指定。这个有点像是消遣性质的安全性选项（toy security option），因为它并无法提供真正的封闭式网络。既然同时支持802.11b与802.11g，就可以将它设定为b/g兼容模式，或者禁止使用802.11b设备以避免保护机制带来的负担。

设定 LAN 接口

AirPort 可以当作 NAT 设备使用，这时候它会把来自无线设备的 IP 数据翻译为它的 Ethernet 接口地址。管理人员可以手动为其他工作站设定静态地址，或以内设的 DHCP 服务器将特定范围中的地址分配给其他工作站。当NAT被用来让多部计算机使用同一个

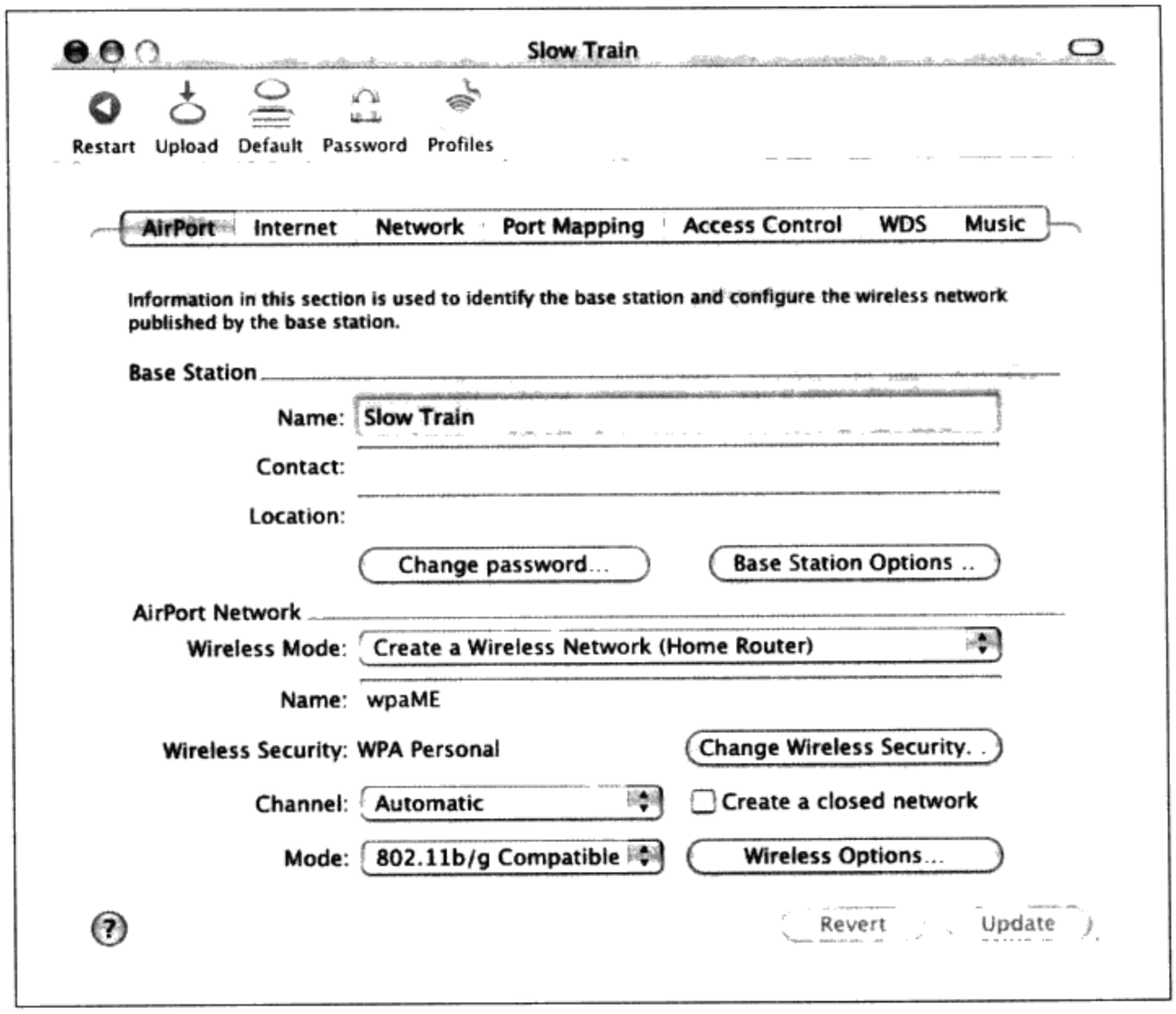


图 20-5：无线接口的配置设定

IP 地址时，“Internet”选项所指定的地址就会被当作对外的公开地址。有线局域网络接口的地址会被设定为不对外公开的私有地址 10.0.1.1，而 DHCP 所释出的私有地址介于 10.0.1.2 与 10.0.1.200 之间（在这种情况下，无法手动指定由 DHCP 服务器所分配的地址范围）。如果不使用 DHCP 服务器，AirPort 接入点可以使用内设的 Fast Ethernet LAN 端口连接至有线网络。

如图 20-6 所示的“Port Mapping”标签页可用来新增内部（inbound）静态连接端口映射关系。公开的端口号会被转换为私有 IP 地址与相应的端口号。本图所显示的地址转换是将内部的 Web 服务传送至 10.0.1.201 主机上的 80 端口。

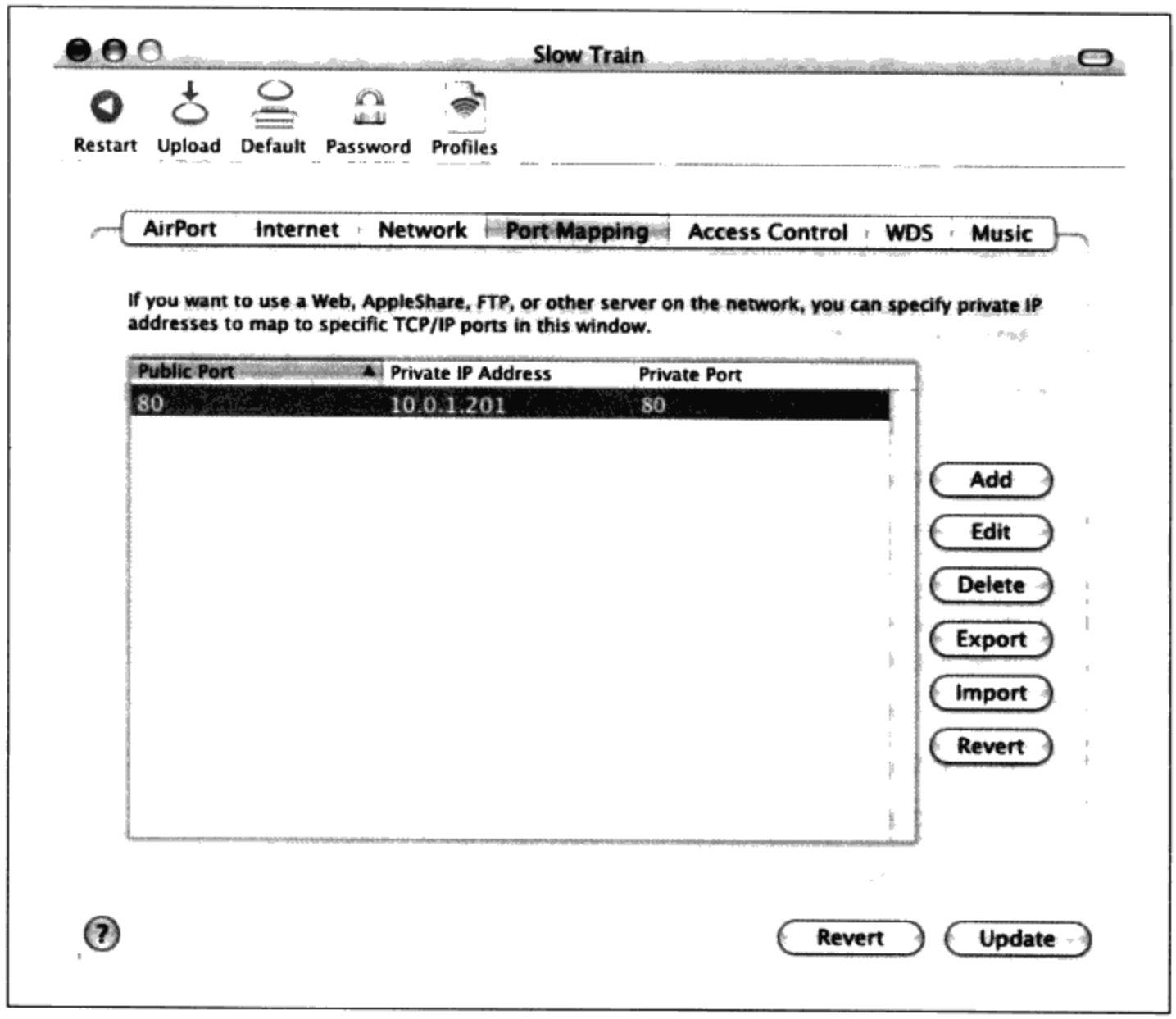


图20-6："Port Mapping"标签页

访问控制

和大部分其他产品一样，AirPort接入点也支持MAC地址过滤的功能。"Access Control"标签页可通过AirPort ID（MAC地址）来辨识工作站，请求将它列入允许访问的工作站列表并且填写工作站的相关描述。

第二十一章

无线网络逻辑架构

无线局域网络的安装规划并不简单，因为横跨许多原本毫不相干的学科。本章会先从网络架构的角度探讨无线局域网络的部署。网络设计就是在几个因素之间做取舍，包括成本（cost）、可管理性（manageability）、可用性（availability）与性能（performance）。至于无线网络，得另外将移动性（mobility）纳入考虑范围。

无线网络通常是现有有线基础设施的延伸。有线基础设施或许十分复杂，特别是其范围涵盖工作园区里好几座建筑时。无线网络必须以牢靠、稳定、设计完备的有线网络为基础。如果现有网络不够稳定，无线部分也必然岌岌可危。

本章主要探讨构建无线局域网络的四种做法。本章将从技术的观点探讨足以影响网络设计的无线局域网络功能。无线局域网络的功能如何影响网络拓扑结构？除了802.11设备，部署网络时还需要哪些器材？如何让逻辑网络的移动性达到极致？

评估逻辑架构

详细列举各种网络拓扑结构之前，让我们先来探讨如何评估网络构建方案。本章所提到的网络拓扑结构各有其优缺点。网络拓扑结构的选择取决于几个决定性因素。以下是我认为比较重要的评估因素。

移动性

可移植性（portability）能够提高生产力，因为方便用户随处访问信息。不过，可移植性只免除了连接的实体限制。膝上型计算机方便带着四处游走，因此有很多人这么做。不过到达新地点后仍然必须重新连接，实际的连接动作还是无可避免，何况设备一经移动，原本的网络连接就无法使用了。

举例而言，远程挂载文件系统后，让膝上型计算机进入休眠状态。带至别处唤醒膝上型计算机后，该文件系统已经不存在。必须等到之前开启的文件或操作逾时，才有办法重新取得计算机的控制权。DHCP客户端可能造成更常见的限制。一般DHCP客户端在更新租期时会尝试取得之前所使用的地址，因此可能要进行好几回合的DHCP交换过程，才有办法在新的IP子网络上取得地址。

相较之下，移动性就较具威力：它进一步解除了许多限制，主要由逻辑网络架构着手。就算设备正在移动，网络连接也不会因此中断。这对需要一致而持续的连接的应用来说特别重要，例如数据库的应用。服务人员经常会访问录有问题与解决方案的追踪数据库(tracking database)，对于医疗机构所使用的追踪软件而言亦然。通过无线网络访问数据库可以提高生产力。如此一来，位于不同地点的用户均可就地新增信息，而用不着每次都与数据库重新连接。另外一个例子是库存应用，这也是为什么零售业（retail）与物流业（logistics）是率先采用802.11的市场。以库存应用为例，就地计算产品或包装盒数量，然后将数据通过无线网络传回，比起先将数据记录在纸上，然后再录入数据要来得合理（注1）。

传统的有线Ethernet只能够提供可移植性。用户可以带着膝上型计算机至园区各地，然后插上网线（如果愿意忍受低速连接，甚至可以从世界各地接回公司网络）。不过，每次访问网络时都必须从头开始。就算只移动了几英尺，也必须重新建立连接。然而用户所期盼的是，每当走进会议室时，不需要任何动作即可连接上公司网络。

“移动性”的定义

无线网络与移动性密不可分。缺乏移动性，人们就不会对无线网络特别感兴趣。移动性意味着不论计算机位于何处，应用程序都能够运作。遗憾的是，要构建不受空间限制的网络，需要具备相当多的知识以及设定不少与位置相关的配置。

要将移动性从高层的定义落实为技术细节，有几种不同的方式。有些技术可以为网络用户提供移动性，但并非所有技术均能带来好处。要提供真正“不需人为介入”(transparent）与“不受应用限制”（independent of application）的网络传输，必须满足下列条件。

1. 一致的链路层网络连接。要具备移动性，现有的数据链路层必须不受位置(location)的影响。通过若干额外的工程，便可以在802.11中提供链路层的移动性。
   a. 接入点间的自动切换（transparent handoff）。用户或许一开始还是必须设定配置并选择某个网络加入，但不必参与切换的决定。如果信号强度过低，内设的软件必须能够自动寻找更强的信号并进行转移，不需要用户介入。目前，几乎

注1：事实上，无线局域网络技术的早期用户主要是移动医疗、物流与教育方面的机构。

所有网卡均可在同一个网络的接入点间进行切换。802.11在设计之初即考虑到此项需求，各位所购买的任何无线局域网络设备应该都符合这项要求。

b. 如果接入点位于不同的广播域（broadcast domain），接入点间的切换操作就可能会失败。假设两个工作站正在交换帧，但其中一个工作站却移往另一个接入点，此时802.11就无法保证这两个工作站位于相同的广播域。如要改善这种情况，厂商可以为所有接入点指定相同的SSID，如此一来，无线局域网络中的工作站不论置身何处，均可位于相同的广播域，就算这些接入点各自连接至不同的区域广播域。

c. 要在两个接入点间漫游，必须为加密与完整性防护操作设定一组新的安全性参数，或将安全性参数自原来的接入点转移至新的接入点。802.11并未规范这种过程，这取决于所使用的硬件。建立新接入点的安全上下文（security context）的过程可能相当费时。传送大批数据时影响或许并不明显，但传送语音数据时就很容易察觉。

2. 对工作站而言，并没有必要变更网络堆栈（network stack）的配置设定。通常，这意味着工作站移动时仍可保有相同的网络地址。在大多数网络中，此地址即IP地址，虽然有些应用或许需要保留其他类型的网络地址。为了提供网络层的移动性，实际上需要一些额外的工程，特别是在IP领域，因为传统的IP并无法提供网络层的移动性。如何保有相同的网络地址乃是网络工程的主要挑战，特别是需要跨越不同的IP子网络时。

a. 论及如何保有相同的地址之前，工作站必须先取得一个地址。初次连接至无线局域网络时，工作站必须先取得一个地址，通常是通过DHCP。连接过程中必须使用同一个地址。对客户端而言，在网络中移动时它仍可保有同一个IP地址，就算连接至其他接入点，也无需更换地址或其他堆栈信息。

b. 当工作站跨越不同接入点的覆盖区域或者突然遇到无线电链路问题，无线网络就可能会出现中断的情形。此时，接入点必须掌握足够的联机信息，这样工作站才能够轻松地重新联机。接入点也必须为工作站暂存帧，让工作站能够访问中断时所收到数据。

c. 同样重要的是工作站必须能够维持本身的地址。如果工作站连接至某服务器，那么在连接期间工作站的地址必须维持不变。此外，网络系统所保存的状态信息通常与IP地址脱离不了关系。有许多网络会使用NAT来访问Internet，每笔NAT记录关联到工作站的IP地址。

d. 视应用的不同，有时必须保存逻辑网络的路径。帧必须通过相同的路径传送，这样才有办法控制。不论位于网络的何处，工作站都得像连接到同一个接入点才行。

没有任何一种技术能够同时满足所有移动性的要求。虽然802.11在链路层提供不少功能，但仍需要一些标准以外的功能。在接入点间转移连接关系通常不难。在未使用链路层安全防护的网络中，将连接信息转移给其他接入点只需要几毫秒至数十毫秒的时间。重新建立链路层安全上下文（link-layer security context）可能需要数百毫秒，这取决于身份验证服务器的反应速度。有些公司投入了不少资源，希望打造出能够加速建立安全上下文的产品。新型的“Wi-Fi交换器”产品可以加速整个漫游过程，将工作站的连接记录集中管理，如此一来就不必在接入点间进行转移了。

有几种不同的做法可以提供网络层的移动性。一些早期的设备使用NAT。NAT并非一种移动性协议。以较上层的协议作为网络的基本架构，只要转换操作失灵，应用就会无法运作了。有些应用几乎无法与NAT兼容，例如H.323；有些则必须使用特殊的协议，例如Ipsec必须使用NAT Traversal。有些设备极度依赖NAT来提供移动性，最好不要使用。

通点对点隧道协议（tunneling protocol）常用来提供与应用无关的移动性。客户端设备寄存于某个网络，如果它无法直接访问根网络（“home” network），接入点内部协议会自动将流量导回寄存所在地。点对点隧道协议必须定义于网络层，这样隧道（tunnel）方能够跨网络传递数据。不过，点对点隧道协议本身也可以运作于链路层（让VLAN连接点遍及全网络）或网络层（让IP地址可路由至全网络）。目前，Mobile IP点对点隧道协议是业界唯一的开放标准（详见本章稍后的附文）。

网络设计人员经常面临的一项挑战是究竟要提供多大范围的移动性。小规模的部署十分简单，有些技术已经可以支持25个接入点。真正的挑战来自于如何为大规模部署或者分散在不同区域的组织提供移动性。要设计成功的移动性解决方案，部分关键在于判断用户的需求。有哪些任务需要IP地址维持不变？Telnet与SSH这类具有交互性的终端联机即属此类。有些应用在重新连接网络时可以启动新的连接，而且重新连接的过程完全不需要用户的介入。一般而言，大多数用户并不希望当他们搭乘汽车、火车或飞机时，IP地址还能够维持不变。静态、大型、分散的园区则需要高于一般的移动性支持。

注意： 移动性的“汽油”（dinosaur juice）定律：如果移动时用到燃料（fossil fuels），IP地址的改变就可以接受。

安全性

当全世界的网络融合为全球性的单一网络时，安全性就更加重要。对一些较有安全意识的组织而言，无线局域网络曾是祸害的根源。随着新工具的出现，构建具备显著安全防

护的网络已经变得比较简单。除了传统的安全性议题，例如用户组间的流量区分与维护适当的访问权限，无线网络还带来新的挑战，例如私设接入点与未经授权的工作站。

Mobile IP

802.11在MAC地址上采用了一个策略：工作站以MAC地址进行通信，仿佛就像固定的Ethernet工作站一般。然而，接入点还会注意到附近的移动式工作站，并且会通过电波转送来自有线网络的数据给它。移动式工作站与哪个接入点关联并无关紧要，因为负责的接入点会进行必要的转送操作。有线网络上的工作站可以直接与无线工作站进行通信，就好像它位于有线网络一般。

Mobile IP对IP地址使用类似的花招。外部使用的IP地址看似位于固定的地方，称为归属位置（*home location*）。不过，位于归属位置（归属地址，*home address*）的IP地址是由所谓的*home agent*（归属代理）提供服务，而非用户的系统。和接入点一样，home agent负责追踪移动式节点当前所在的位置。当移动式节点“位于归属地”(at home)，就可以直接传送封包。如果移动式节点连接至不同网络，称为外地网络（*foreign network*）或拜访网络（*visited network*），就会向home agent登记所在的外地位置，好让home agent知道如何传送数据给它。

举例而言，有两个无线局域网络分别位于不同的IP子网络。对于归属子网络(home subnet)，无线工作站可以“正常”收发数据。

如果无线工作站从其归属子网络移动至另一个子网络（“外地”），它会通过正常的流程连接至该网络。与接入点关联的同时，该工作站或许还会从DHCP服务器取得一个IP地址。如果无线工作站无法使用Mobile IP，由于IP地址突然改变，之前的连接必须中断，所有进行中的TCP连接均告无效。

不过，配备Mobile IP软件的无线工作站只要向home agent登记，就可以维持连接的状态。home agent可以为移动式工作站接收封包，检查登记表，然后将封包送至移动式工作站目前所在的位置。实际上，移动式工作站其实有两个地址。在归属网络，移动式工作站可以使用home address进行连接。在外地网络，则使用该网络所指派的地址。TCP连接状态仍然有效，因为移动式工作站并未停止使用其归属地址。

当然，系统管理人员通常不喜欢在终端用户的系统上安装新的软件(这没有错)。另一种做法是使用“移动式IP代理”（*proxy mobile IP*），将代理软件的功能整合到接入点设备。将Mobile IP功能移到接入点，就不必安装客户端软件了，虽然这种做法会增加接入点本身的复杂度。

—待续—

此处省略了许多协议操作的细节。要让工作站随时随地联机，又能够同时使用其归属地址，在协议的设计上必须下相当的工夫。比较显著的还有安全问题，尤其是协议操作的认证以及归属网络与外地网络之间的封包转送安全问题。要维护传统的Internet网关转送表及Mobile IP代理的路由信息的正确性，已经是莫大的挑战。何况，该协议必须同时和IPv4与IPv6兼容。想要对Mobile IP有更进一步的了解，我大力度推荐Charles Perkins所著的《Mobile IP: Design Principles and Practices》（由Prentice Hall出版）。

逻辑架构的安全性之所以错综复杂，和加密与身份验证协议的选择脱离不了关系。不过，架构本身还涉及其他安全因素，例如接入点所使用的技术。

传统的接入点是属于独立网络组件的自主设备（autonomous device）。接入点被放置于用户所在区域，而且通常没有物理防护。不幸的是，随着802.11越来越受欢迎，放置于公共场所的接入点很容易成为遭窃取的对象。传统的接入点包含自身的软件与配置设定，攻击者能够从配置设定中取得敏感的安全信息（例如RADIUS共享秘钥），因此容易成为令人垂涎的目标。新式的“精简型”接入点移除了大部分的接入点功能，并将这些功能置于可以被锁在配线柜的控制器上。

攻击者也有可能移除某些接入点来取得额外的网络权限。在一些架构下，接入点必须连接至权限较高的网络连接端口。举例来说，如果无线网络提供好几个VLAN，有些接入点就要求与骨干网络连接的接入点必须标记所有可用的VLAN。在这种配置下，攻击者只要移除其中一个接入点并取得连接端口，就可以直接访问骨干网络。

另外一个顾虑是许多政府网络在设计上必须符合管制规定与最佳实践。美国国家标准与技术研究院（National Institute of Standards and Technology，简称NIST）负责开发美国联邦政府所使用的computing标准，这些标准被称为“联邦信息处理标准”（Federal Information Processing Standards，简称FIPS）。在这份FIPS-140标准中，列出了安全的网络设计必须符合哪些条件。FIPS-140规定一些特定的数据必须经过加密。较为显著的是，FIPS-140同时规定必须使用业经核准的加密模式与算法。并非所有安全性协议与标准都具备同等地位，只有某些网络设计符合FIPS-140的要求。除了大多数的联邦机构，FIPS对联邦机构的供货商与合约商也有相当大的影响力（FIPS的要求将于第二十二章详细探讨）。

性能

虽然有移动性的好处，但无线网络并非不用付出任何代价。简单来讲，不能期待无线网络提供类似有线网络的性能。相较于有线局域网络，无线网络的名义位率（advertised

bit rate）较低。更糟的是，华而不实的文章浮夸数字，但对协议所造成的沉重负担完全避而不提（注 2）。根据经验法则，表 21-1 列出了各种技术的最大吞吐量。

表21-1：各式802.11技术的最大吞吐量

技术	名义吞吐量	估计最大连续吞吐量	以 5:1 多路复用系数估计最大可使用吞吐量
单模系统			
802.11b	11 Mbps	6 Mbps	30 Mbps
802.11a	54 Mbps	30 Mbps	150 Mbps
802.11g，未使用保护机制	54 Mbps	30 Mbps	150 Mbps
802.11g，使用保护机制	54 Mbps	15 Mbps	225 Mbps
双模系统			
802.11a+802.11b	11+54 Mbps	36 Mbps	180 Mbps
802.11a+802.11g（未使用保护机制）	54+54 Mbps	60 Mbps	300 Mbps

不同于有线网络，无线网络的速度取决于其与最近的网络上行链路之间的距离。工作站离接入点越远，信号就越微弱、操作速度就越慢。吞吐量取决于距接入点的距离以及设备所处的位置。对有线网络的用户而言，这些都是陌生的概念。

信号必须足够强而且距接入点不能太远，方能达到表21-1所列的吞吐量。事实上，大多数无线局域网络是以覆盖范围为主要考虑。在边缘地带，只能达到最低的速率，而非最高的速率。典型的情况如图21-1所示。距接入点较近的工作站使用较高的数据率进行连接，距接入点较远的工作站必须花费较长的时间，才能传送等量的数据。即使无线电波媒介处于正常使用状态，图 21-1 中连接至接入点的工作站的最大吞吐量也将远低于 6 Mbps。

虽然图21-1所显示的最大数据率不高，但可以通过神奇的多路复用技术（multiplexing），让这个数字看起来高一些。网络的基本原则是，用户的流量通常时高时低（bursty）。虽然用户通常希望能以每秒一兆位以上的速率传送数据，但实际上网络经常处于闲置状态。网络只需要在用户接收电子邮件或下载网页时提供最大数据率；当连接处于闲置状态时，其他用户就可以享受每秒一兆位的服务。虽然802.11b网络的速率只有6 Mbps，但可以给 20 至 30 个用户提供每秒数兆位的服务需求，因为很少有应用需要持续服务（语音应用例外）。表 21-1 最后一栏显示多路复用系数（multiplexing factor）为5:1时的有效吞吐量。取决于应用的方式与经验，有时你需要在网络上提高或降低此系数。

注 2：　有效吞吐量实际上更低。要将这些协议所造成的负担加以量化十分困难。相关计算详见 *http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html*。

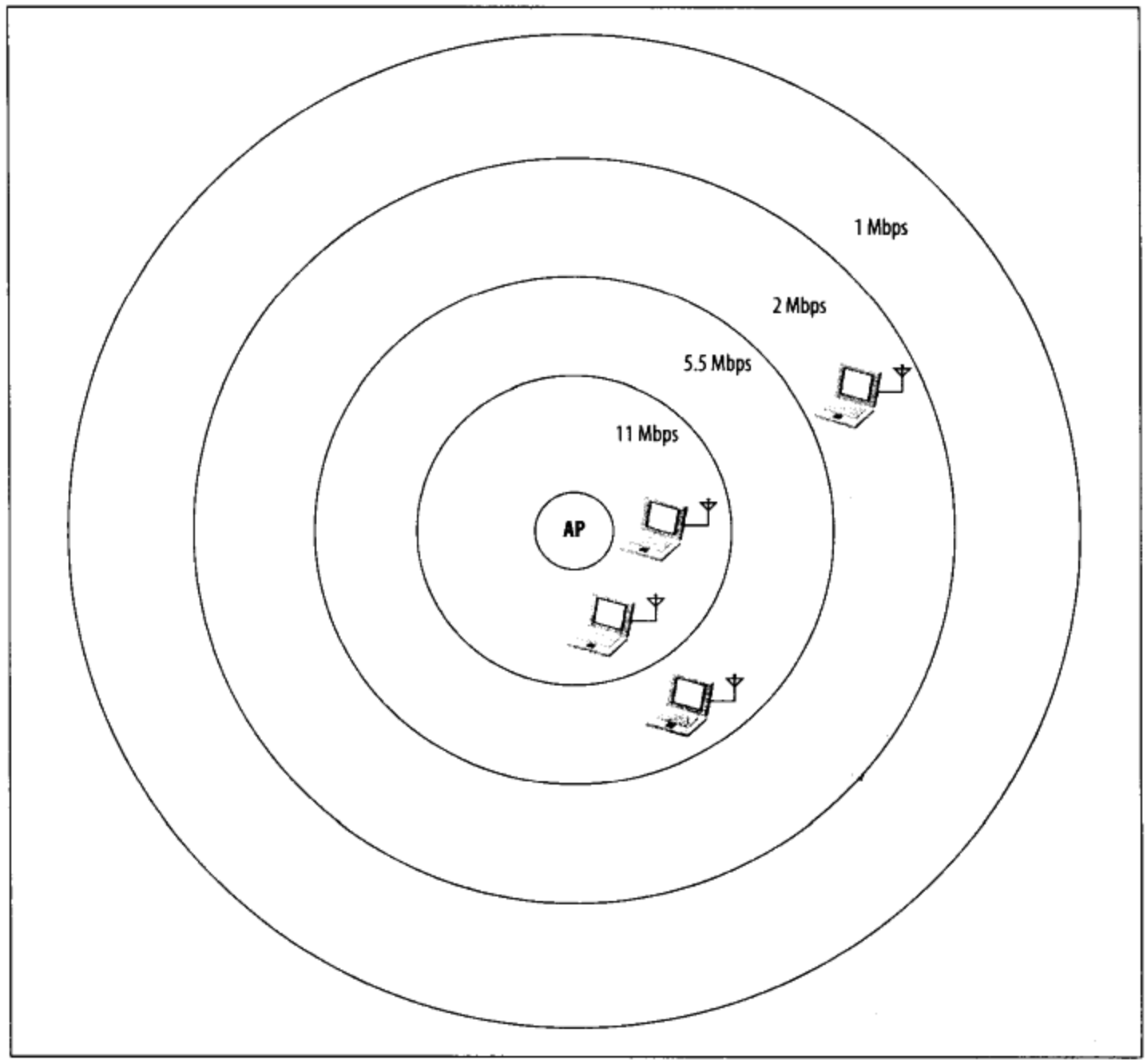


图21-1：性能与距离的关系

图21-1从定性的（qualitative）观点说明网络速度如何随距离而改变。从定量的（quantitative）观点看，可以借助计算开放空间损耗（free-space loss）来掌握网络的传输距离与传播特性。开放空间损耗（或称路径损耗）是指在没有障碍物的情况下，信号在空间中传输时的损耗。路径损耗（path loss）是一种“理想”值，用来描述电磁波随距离在信号强度方面的衰减，至于一些与设置802.11网络相关的因素则忽略不计。室内网络必须处理墙壁、门窗以及大多数信号并非呈瞄准线（line of sight）传送的问题。开放空间损耗计算的基本假设是：本底噪声（noise floor）低到某种程度时，接收器的灵敏度将成为限制因素。在许多环境中，2.4 GHz ISM频带存在过多的免许可证设备，以至于本底噪声超过许多接收器的最低限制。

开放空间损耗受到两种因素的影响："信号的频率"与"覆盖的距离"。频率越高或距离越长，衰减就越严重。

开放空间损耗(以 dB 为单位)= 32.5 + 20 × [$\log_{10}$(频率，以 GHz 为单位)+ $\log_{10}$(距离，以米为单位)]

表 21-2 所列的数值是针对 2.4 GHz 与 5 GHz 无线局域网络所计算的开放空间距离。在 ISM 频带，是以 2.437 GHz 或第 6 信道的中心频率来计算；在 5 GHz 频带，则是以 5.250 GHz 或 U-NII 低中频带的中点来计算（一些早期的 802.11 网卡只能够使用两种较低频带，因此有些网络限制只能使用 802.11a 的前 8 个信道）。此表假定在 2.4 GHz 频带是以最大功率 20 dBm（100 mW）进行传输，至于 802.11a 设备，则是以 14 dBm（25 mW）的最大实际功率进行传输。在接收器方面，是使用 Cisco CB-21 a/b/g 无线网卡的规格表（data sheet）所列出的接收灵敏度。此表直接列出灵敏度，是假设本底噪声远低于灵敏度字段所列出的数值。不要期望能够得到此表所列的距离，毕竟此处所计算出的最大距离纯属理想值。不过它可作为参考，用来比较不同的调制速率以及不同的频带。

表21-2：开放空间中不同调制速度的传输距离

调制方式与速度	灵敏度（Cisco CB-21）	开放空间最大传输距离（米）	相对于最大速度的开放空间距离	最大传输距离调制的百分比
2.4 GHz				
1 Mbps DSSS	−94	4850	13.9	100%
2 Mbps DSSS	−93	4300	12.3	89%
5.5 Mbps CCK	−92	3850	11.0	79%
11 Mbps CCK	−90	3050	8.7	63%
6 Mbps OFDM	−86	1930	5.5	40%
9 Mbps OFDM	−86	1930	5.5	40%
12 Mbps OFDM	−86	1930	5.5	40%
18 Mbps OFDM	−86	1930	5.5	40%
24 Mbps OFDM	−84	1530	4.4	32%
36 Mbps OFDM	−80	970	2.8	20%
48 Mbps OFDM	−75	550	1.6	11%
54 Mbps OFDM	−71	350	1.0	7%

表21-2：开放空间中不同调制速度的传输距离（续）

调制方式与速度	灵敏度（Cisco CB-21）	开放空间最大传输距离（米）	相对于最大速度的开放空间距离	最大传输距离调制的百分比
5 GHz				
6 Mbps OFDM	−89	630	7.0	100%
9 Mbps OFDM	−89	630	7.0	100%
12 Mbps OFDM	−89	630	7.0	100%
18 Mbps OFDM	−85	400	4.4	63%
24 Mbps OFDM	−82	280	3.1	44%
36 Mbps OFDM	−79	200	2.2	32%
48 Mbps OFDM	−74	110	1.2	18%
54 Mbps OFDM	−72	90	1.0	14%

另一个需要注意的地方是，无线网络的性能不同于有线网络。大多数有线网络是由交换器构建而成，因此可以独立交换不同的流量。无线网络基本上属于一种共享媒介。在接入点的覆盖范围内，同时间只能有一个工作站进行传输。无线网络通常是以覆盖范围为主要考虑因素。无线网络越受欢迎，网管人员就越需收缩每个接入点的覆盖范围，以避免竞争带宽的情况出现。通过收缩覆盖范围来防止带宽竞争，乃是大多数“Wi-Fi 交换器”所采取的做法。

无线媒介的物理特性对性能与服务质量有负面的影响。为了顾及可靠性，802.11 要求MAC层必须得到确认信息，却因此造成帧的传输延迟。封包漏失与重传的可能性更增加了延迟的变动性，称为*jitter*（抖动）。在某些应用上，用户并不会察觉延迟的情况。可用容量（available capacity）比服务质量（service quality）更容易影响大批数据的传输。不过，如果计划以无线网络提供语音服务，就得花费一些工夫才有办法提供可接受的服务质量。语音服务需要少量但稳定的数据，带宽高低反而不是重点。本章所探讨的架构中有一些比较适合于需要高质量网络服务的应用。

传统服务质量的排队（queuing）与控制（control）之所以重要，是因为不仅符合无线信号少量而稳定的需求，也因为带宽有限。既然接入点每秒只能传送数百万个位，只要有一个行为不良的工作站，就可能榨干所有带宽。有些接入点提供较佳的流量控制方式，让工程师自行分配稀少的无线媒介资源。此外，有些逻辑架构较适合于需要高带宽的应用。

如同许多其他网络工程任务，要构建符合预期性能的无线局域网络，必须分析打算在局

域网络上执行的应用的类型并且尽量移除可能的瓶颈。有时候，构建足够的网络资源来满足用户的需求的确可能。至于其他应用，则可能必须使用流量管理工具来管理资源的分配。

骨干工程

接入点位于不断扩张的网络的边界。大多数情况下，它们并未提供新的网络服务，只是让现有服务更易于取得与使用。作为边界设备，接入点必须接入网络核心，才能够使用户与资源互相连接。将无线网络加入局域网络的边界地带时，网络核心额外的配置设定势不可免。

在802.11刚成为标准且产品刚问世时，除了网络工程师所规划的，尚无法提供移动性，也没有针对流量加以区别。其移动性完全是拜网络工程师所赐。将接入点置于单一链路层网络才有所谓的移动性可言，否则，移动性纯粹是一种幻想。早期无线局域网络的要求是，网络的架构必须围绕着一个交换式核心，这样横跨整个园区的单一子网络便可用来连接所有接入点。许多新型网络的构建也是围绕着一个交换式核心，但旧式网络通常有限制，无法构建纯粹的交换式核心。

第一代产品问世后，业界开始生产可以将用户附接到多个VLAN的设备。虽然这些产品允许多个用户组同时存在于无线与有线骨干网络，但是较具影响力的其实是骨干网络的配置。每个VLAN都必须被扩展至园区里的所有接入点，而不是以单一VLAN来连接园区里的所有接入点。Wi-Fi控制器的目标之一，就是通过允许使用较简单的接入点连接配置来进一步减少骨干工程。

Beacon、BSSID以及VLAN整合

目前标准小组正在进行的一项主要工作，就是将现有的VLAN扩展至无线网络。针对这一点，不同厂商采取不同的做法。评估这些做法时有一些基本的考虑因素。

802.11是以所谓的“服务集”(service set)为基础，但并未明确定义何谓服务集。此外，在802.11中有两种“服务集标识符”(SSID)。“扩展式服务集标识符”(ESSID)就是“网络名称”(注3)。几个接入点可以被设定为一组连接。当工作站打算连接至无线网络，就会发出探查信息找寻ESSID，属于该SSID的接入点就会加以响应。ESSID可以附着在Beacon帧中，但并非必要（隐藏ESSID是通过隐瞒而达到安全性的做法。参考第九章，便可发现Probe Response帧中包含未经加密的SSID）。“基本服务集标识符”

注3：这种说法有点简化。ESSID只是基础结构型网络的网络名称。本书假定各位使用的是基础结构型网络，而非独立型网络。

(BSSID) 是第二种服务集标识符，亦即接入点的MAC地址。它被用来作为传送于无线与有线网络间的帧的传送端或接收端地址。

一般而言，每个ESSID均具有独立的BSSID。接入点在单一Beacon帧中传递多组ESSID或是响应非Beacon帧中所记载的ESSID，这种做法将导致许多问题，但却无从防范。例如，Windows Zero Configuration 软件通常不接受配置设定中出现的第二个隐藏式ESSID。它会试着连接到 Beacon 中所记载的 ESSID，而非试图搜寻隐藏式ESSID。

当接入点首度使用户能连接至不同的VLAN，提供配置设定给用户的一般做法，就是将VLAN命名成一个SSID，然后让用户自行选择。虽然这种做法十分有灵活性，允许用户自行选择如何连接至VLAN并且允许用户考虑环境情况切换VLAN，但这种灵活性却如剑之双刃，当用户选择了错误的配置设定时，容易造成用户的混淆。为其他额外的SSID传送 Beacon 帧不可避免地要牺牲稀少的网络资源。在许多环境中，根据用户配置文件 (user profile database) 动态为用户指定 VLAN 是比较好的做法。

IP 寻址

IP地址通常反映了物理网络的拓扑结构，无线网络也不例外。IP地址的指派是附属于选择网络拓扑结构的一项决定。有些网络设计要求指派新的地址与路由配置，有些则不要。试图以分级的方式分配地址空间的机构（或许是基于路由表大小的考虑）将会发现难以使“逻辑地址的指派”与“底层的物理拓扑结构”相符，而使用物理 IP 地址空间的机构将发现这种做法较具优势。

网络服务

理想情况下，新的网络设备只要接到现有的基础设施并稍做设定，应该就可以运作。用户经验对有些网络服务而言十分重要，应该仔细考虑。

DHCP

用户的期待通常是只要连接到网络就可以开始使用。无线网络也不例外，但却会让问题变得更糟。用户希望只要连接到任何无线网络就可以开始使用。但实际上，要让无线接口的 IP 堆栈自动取得适当的 IP，唯一的方式就是通过 DHCP。

有些接入点本身内置DHCP服务器。只有一两个接入点的小型网络可以选择使用内置的DHCP服务，不过大型网络应该只使用 DHCP 寻址信息的单一来源。接入点的DHCP服务器或许无法承担大量的负载，有些接入点在连接结束后随即会将地址收回。

任何DHCP服务都应该掌握所有可用的地址空间，这件事最好不要在接入点中进行。接

入点的功能就像桥接器，将DHCP请求从无线网络传至有线网络，再由DHCP服务器予以回复。灵活运用DHCP代理（DHCP helper），只需要一部服务器就可以服务好几个IP网络，不论其被实现为VLAN还是多个无线子网络。

注意： 用户通常会假定DHCP存在，因此最好加以使用。为了达到最好的效果，应该尽量减少DHCP服务器的数目。

操作系统登录

无线网络所面临的挑战之一，就是验证用户身份时通常必须将网络连接至身份验证服务器。例如，Windows登录即是通过域控制器（domain controller）来验证。这在有线网络并不困难，因为只要插上网线即可达到目的。不过在无线网络中，就会面临“鸡生蛋，蛋生鸡”的问题。验证网络连接时必须用到身份证明，但要验证用户身份却得先有网络连接。并非所有操作系统厂商都会考虑这个问题。如果刚好碰上这个问题，就必须使用特别的登录功能或是其他客户端软件来填补这个空隙。

客户端集成

不同的逻辑架构需要不同的客户端软件的支持。构建网络时很容易将安全性抛诸脑后，所谓客户端集成，不过是安装新的驱动程序。不过对任何网络而言，安全性都是不可或缺的。

使用静态WEP密钥可以提供最起码的安全性。有些旧设备只支持静态WEP，如果无法升级则别无选择。静态WEP的配置设定通常内置于驱动程序或客户端设定工具，不需要其他集成操作。不过为了安全性，可能的话最好采用静态WEP以外的解决方案。

基于802.1X的链路层在安全性解决方案方面已有显著的进展，不过需要相当的客户端集成操作。客户端系统必须安装802.1X申请者软件且必须正确设定。近来许多操作系统（Windows 2000、Windows XP与Mac OS X 10.3）已经集成了申请者软件。旧式系统可能需要另外安装客户端软件包方能支持802.1X。

VPN的解决方案各有不同，这取决于厂商与所采用的VPN技术。基于SSL的VPN是将客户端的访问导向某个安全的网站，以之作为应用的入口。由于这种技术是以安全的网站为基础，因此除了可能已经安装在操作系统上的Web浏览器，并不需要安装其他软件。不过，SSL VPN的缺点是需要额外的处理方能保护非Web式应用，用户也需要经过训练。IPSec VPN需要安装额外的软件，但能够处理任何以IP为基础的应用。VPN客户端软件之所以越来越复杂，原因之一是大多数厂商希望在VPN客户端软件中塞进更多的功能。

有些机构也许没有足够的能力为用户安装客户端软件。例如，大学里的用户通常必须开启VPN隧道方能访问外部的网站，在职进修的学生通常需要从教室连接到公司访问资源。一般而言，在IPSec隧道中另辟IPSec隧道（IPsec tunnels inside IPsec tunnels）来运行多个客户端程序，如果有人这么做的话，这并不是一个好的做法。

网络拓扑范例

重点确立之后，就可以勾勒出无线局域网络的面貌。大致上，无线局域网络的部署主要有两种方式，至于采用何种方式，则取决于是否在链路层使用安全防护。本节将说明并分析无线局域网络的四种不同架构。本节所提到的四种范例在某种程度上可说是相当严谨。等到无线局域网络硬件市场成熟，设备将会整合这些拓扑的所有功能，让用户得以自行挑选符合各自需求的功能。

拓扑类型1：单一子网络

起初只有一种拓扑类型。接入点本身就是简单的桥接器，只能够将无线工作站附接至其所连接的有线网络。接入点本身并没有什么智能，因此设计无线网络时必须以接入点当中的桥接引擎为核心。网络只支持简单的移动性。当接入点只是简单的桥接器，无法处理复杂的VLAN或路由操作时，就必须附接在相同的IP子网络。只要工作站位于相同的IP子网络，便不需要重新启动网络堆栈，而且能够维持本身的TCP连接。

设备本身的限制会影响到最终的网络架构。每个接入点均连接至单一网络。虽然这种网络提供移动性，但通常很难设置，特别是在大型园区里。除了更改骨干网络配置，管理人员还必须指派新的IP地址范围以及适当地加以路由。这种架构的开发，是在较牢靠的安全协议问世之前用来使有线网络免遭无线网络的波及。如今，打造两套平行网络的管理负担与成本使得这种架构已经被大型网络排除在外，除非网络中只有少数几个接入点。

早期典型的无线局域网络部署拓扑如图21-2所示。此网络由单一链路层网域所构成，而且每个连接至网络的工作站均被赋予隶属该子网络的IP地址。因此，这种单一架构也被称为单一子网络的无线局域网络（*single-subnet wireless LAN*）、围墙花园架构（walled garden architecture）或VPN架构（此外，必须注意的是，大多数家用网络均采用这种单一子网络的做法，虽然通常只有一个接入点）（注4）。图21-2的指导原则是，接入点无法提供链路层移动性以外的服务，因此必须连接至相同的逻辑链路层。其他设计上的

注4：极大型的归属网络也许需要用到好几个接入点。通常，一个接入点应该能够覆盖3000至5000平方英尺，对大多数归属网络而言，这应该已经足够了。

决定有助于进行无线设备的访问控制，并可借助现有的服务来减轻管理上的负担。以下将逐一说明。

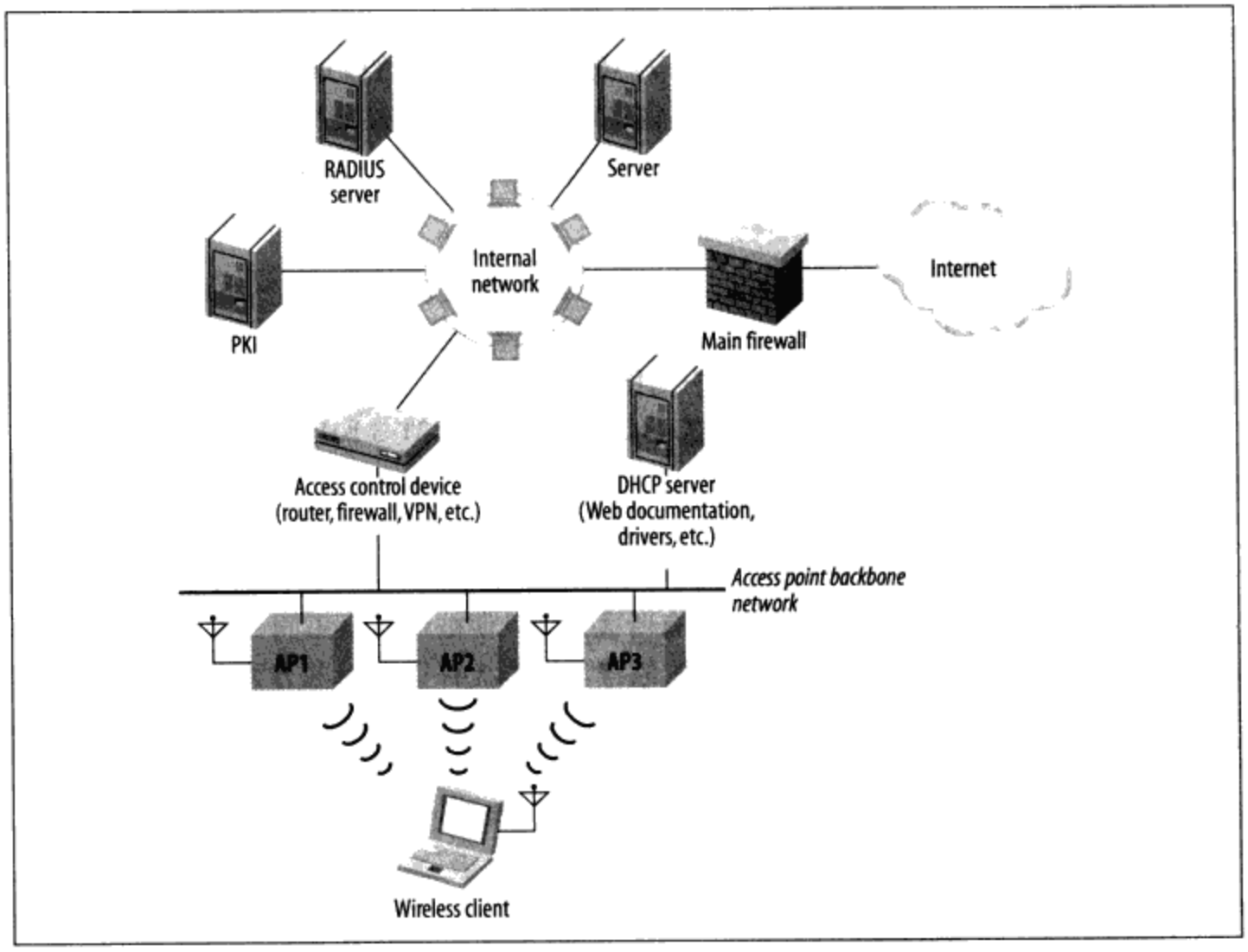


图 21-2：单一子网络拓扑

移动性

图 21-2 中，串联所有接入点的网络乃是单一 IP 网络，通常称为接入点骨干。为了让用户能够在接入点间漫游，网络必须是单一 IP 子网络，就算它跨越好几个地区，因为 IP 不允许网络层漫游（Mobile IP 显然是此项规则的例外，参见本章的附文）。网络层的移动性是由交换式基础设施所提供，以此基础设施将所有接入点连接在一块，使用IP寻址机制，除了链路层的移动性，并不需要其他。

图21-2的骨干网络实际的规模可以很大，不过并非毫无限制，亦即所有接入点都必须以链路层直接连接到骨干路由器（以及其他接入点）。802.11 工作站可以在网络中自由移动。不过，目前的 IP 设置并无法跨网段（子网络）。对于外部的 IP 工作站而言，图 21-2 的 VPN/ 访问控制设备，乃是“最后一跳”（last-hop）路由器。要连接位于此无线

网络的工作站，必须通过此IP路由器。无线工作站究竟连接至第一还是第三个接入点并不重要，因为均可通过最后一跳路由器来连接。从外部来看，无线工作站无异于连接至Ethernet的工作站。

不过，如果工作站离开子网络，就必须取得新的IP地址，然后重新建立连接。图21-2中，这种设计的目的是为了将单一IP子网络指派给无线工作站使用，并允许它们在接入点间自由移动。在此并未禁用多个子网络，不过一旦使用多个子网络，就无法在子网络间提供无间隙的移动性。

相互合作提供移动性的接入点必须在layer 2相连。方式之一如图21-3 a)所示，就是在现有的有线网络基础设施外，另行构建一套如图21-2所示的无线网络基础设施。接入点额外获得了一组交换器以及网络电缆的支持并且上行链路（uplink）至核心网络。如要尽量缩减硬件，可以采用VLAN（虚拟局域网络），如图21-3 b)所示。在图21-3 b)中，交换器不仅扮演layer-2中继器（repeater）的角色，在逻辑上亦同时会将所有的连接端口划分为多组layer-2网络。接入点可被置于其中一个VLAN中，这个wireless VLAN（无线虚拟局域网络）可以拥有自己的IP子网络。从交换器流向网络核心的帧会标记VLAN代号，这样它们在逻辑上便能够有所区别，以便被传送至不同目的地。多重子网络可以使用相同的上行链路，因为VLAN的标记功能允许以逻辑的方式区别帧。来自有线网络的帧会通过同一个VLAN代号加以标记，来自无线虚拟局域网络的帧则以不同的VLAN代号标记。帧只会被传送至交换器中相同VLAN的连接端口，因此来自无线VLAN的帧只会送给接入点。

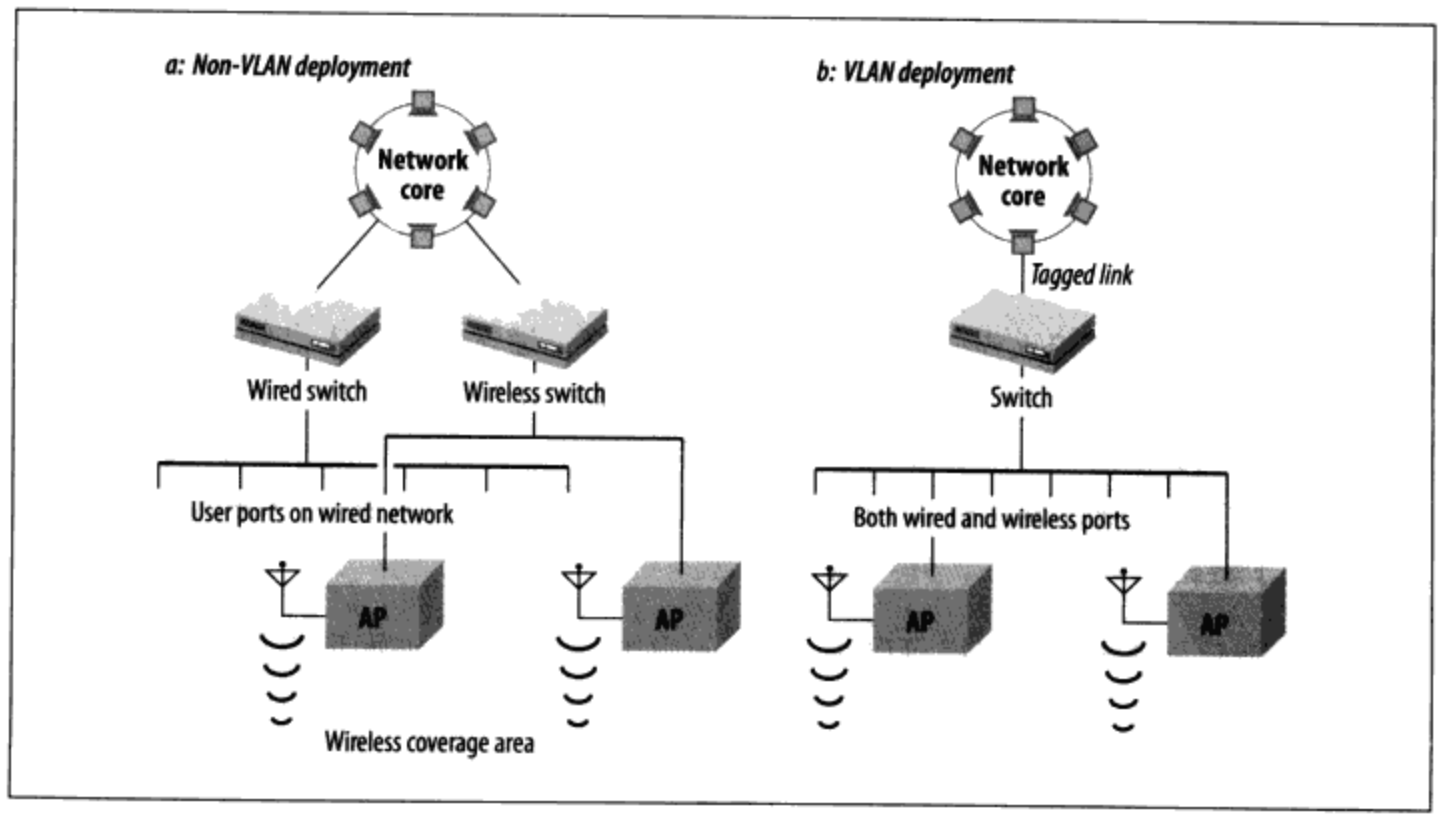


图21-3：802.11网络部署的物理拓扑

让骨干接入点成为VLAN，可以扩展相当长的距离。具备VLAN能力的交换器可以彼此串联，而这些经过标记的链路（tagged link）可以串联不同的地理区域而形成单一逻辑网络。在图 21-4 中，两部交换器是以标记链路相连，四个接入点均被指派给相同的VLAN。这四个接入点可被置于相同的IP子网络，有如连接至同一部集线器（hub）。标记链路让两部交换器隔开，实际的有效距离则取决于所使用的技术。如果采用光纤链路，则可以在好几栋建筑物间构建 VLAN，因此单一 IP 子网络可以覆盖好几栋建筑物。

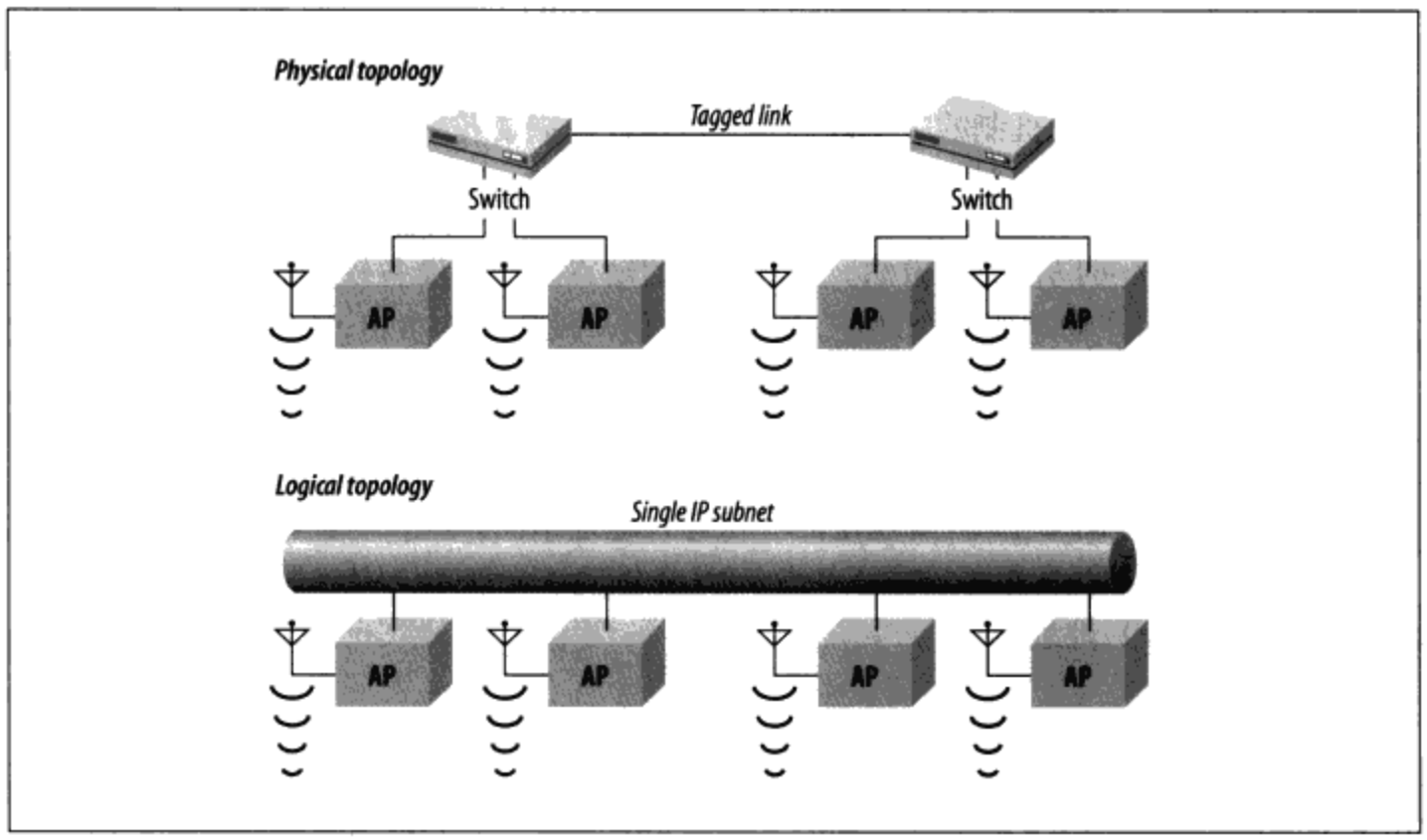


图 21-4：利用 VLAN 来连接多部交换器

标记链路（tagged link）在成本与复杂度上程度不一。要连接同一栋建筑物的不同区域，可以使用传统的Ethernet电缆；要在两栋建筑物间建立连接，则必须使用光纤。建筑物之间的电压不尽相同。以铜线之类的导体连接两栋建筑物，有可能在两部Ethernet交换器之间产生电流，从而导致严重的损坏。光纤电缆不会导电，在户外也不会受到电磁噪声的干扰，在顾虑到电磁风暴的环境中，必须将此纳入考虑。另外，光纤的优点是可以进行远距离高速传输。如果有多部Fast Ethernet设备被连接到只配备单一Fast Ethernet接口的交换器，那么上行链路时就会遇到瓶颈。为了在大型网络中提供较佳的传输质量，上行链路通常会使用 Gigabit Ethernet。

预算较为宽裕的大型机构所使用的上行链路不必局限于Ethernet。过去我所服务的一家公司就采用了都会型（metro-area）ATM，用链路层连接市内的几栋建筑物。只要在Ethernet与ATM之间加上适当的转换机制，类似的服务即可作为交换器间的骨干。

以 DHCP 来指定地址

就图21-2而言，有两个位置适合摆放DHCP服务器。一个是在接入点骨干子网络上，由一部独立的DHCP服务器负责为无线子网络上的工作站提供可用地址。这种做法需要为每个子网络提供一部DHCP服务器。另外，有能力进行路由转送的设备通常包含DHCP中继机制（relay）。如图21-2所示的安全设备（防火墙与VPN）便具备路由转送的能力并且提供DHCP中继机制。利用DHCP中继机制，来自无线网络的请求就会被接入点桥接至接入点骨干，然后通过访问控制设备转送至公司的主要DHCP服务器。如果机构以DHCP集中管理地址分配事宜，那么最好通过DHCP中继机制，利用现成、可靠的DHCP服务。使用DHCP中继机制的唯一缺点是，转送过程需要花费额外的时间。并非所有工作站均会耐心等候，此时就不该将DHCP中继机制纳入考虑。

当然，静态寻址是可以接受的做法。静态寻址的缺点是需要准备较多的地址，因为不论使用与否，每个用户均需要一个地址。为了减少用户设定上的负担，可以考虑使用DHCP针对各个MAC地址指派固定的IP地址。

最后，地址指派与安全性之间有可能存在某种交互关系。如果采用VPN解决方案，可以在基础设施中使用RFC 1918所规定的（私有）地址空间。DHCP服务器所配发的私有地址可以让节点与VPN服务器联系，当VPN身份确认无误后，VPN服务器即会配发可路由的（routable）地址。

安全性

在本章所提出的架构中，这是最古老的架构，早在过去几年链路层安全性出现之前就已经存在。它通常用于链路层安全性并非作为考虑重点的场合，如所提供的服务优先于安全性（例如ISP）或是以上层VPN技术提供安全性的场合。无线网络设计时的安全性取舍将于第二十二章详细探讨。

骨干工程

取决于现有的骨干，使用这种拓扑类型也许需要大幅修改，也许只要稍作变动。为了达到最大的移动性，每个接入点均需连接至横跨整个园区的无线VLAN。如果网络原本就构建在交换式核心之上，要创建一个横跨好几个配线柜与多部交换器的VLAN就相对比较简单。如果建筑物之间以路由器串接，就无法构建扩展至整个园区的单一VLAN，不相邻建筑物间的移动性就必须另行处置。更糟的是，有些旧式网络并非以交换器为核心，因此无法轻易扩展VLAN的范围。

此外，VLAN的网络半径实际上有限制。802.1D（桥接标准）建议VLAN最好不要超出7部交换器的服务半径。实际的拓扑类型或许无法将整个覆盖区域纳入单一VLAN，就算可以，也必须大幅修改整个网络核心。

性能

这种设计的性能可能变动极大，因为当中包含一个瓶颈（choke point）。这种设计若要得到良好的表现，最重要的是避免将所有流量导向单一逻辑路径。所有骨干设备必须有足够的能力处理来自整个无线网络的负载。

相较于使用冲突探测协议的有线局域网络，基于冲突避免原则的无线局域网络协议能够应付更高的负载。我们可以假定无线链路达到饱和，不过这取决于关联至特定接入点的用户数。可使用的最大传输率依产品而异，6 Mbps 对 802.11b 而言应该算合理，至于 802.11a 与 802.11g 则可达到 27~30 Mbps。

低速的802.11b比较容易避免壅塞。既然每个接入点的潜在负载只有6 Mbps，接入点骨干所配备的全双工 Fast Ethernet 链路应该能够处理 30 个以上的接入点。虽然 30 个接入点还称不上大型网络，但足以提供相当大的覆盖范围，能够在相当大的开放空间提供低带宽的应用。如果将瓶颈设备升级为Gigabit Ethernet，便能大幅提升可连接的接入点数量。由上行与下行流量决定，或许可以连接 200 至 300 个接入点，而不必担心造成骨干网络的壅塞。当然，gigabit 设备的成本远高于 Fast Ethernet 设备。

802.11a与802.11g可以达到更高的速度，因此可能衍生更多的问题。既然速度快了好几倍，因此Fast Ethernet设备只能服务几个接入点。以最大的上行与下行传输而言，全双工 Fast Ethernet 可以连接6个接入点，就算只是要覆盖中型的办公室都略嫌不足。同时具备 802.11a 与 802.11g 功能的双频接入点更是雪上加霜，因为这两种无线电接口均会造成高度负载。

表 21-3 列出了骨干技术的讨论以及会让链路达到饱和的接入点数目。这只是粗略的估计。每一种骨干技术除以接入点的负载，可估算出链路达到饱和状态将需要多少个接入点。此表并未将协议所造成的负担或者上行与下行流量的区别纳入考虑，这只是让各位在为无线子网络选择适当的上行链路技术时有个粗略的参考。

表21-3：让骨干饱和所需要的接入点数量

	802.11b (~6 Mbps)	802.11a 或 802.11g (~30 Mbps)	双频 a/b (~36 Mbps)	双频 a/g (~60 Mbps)
半双工 Fast Ethernet (100 Mbps)	16	3	2	1
全双工 Fast Ethernet (200 Mbps)	33	6	5	3
全双工 Gigabit Ethernet (2000 Mbps)	333	66	55	33

客户端集成

从客户端集成的观点来看，这种架构算是最多样化的。以服务供应商为例，客户端很少或几乎不需要任何调整。既然未进行任何安全防护，也就无需任何配置设定。不过，如果将较上层的安全性应用于此架构，客户端就需要额外的集成操作。

拓扑类型2：E.T. Phone Home或Island Paradise

有些机构规模太大，无法设置单一接入点网络。建筑物分布于方圆数里的大学就是最典型的例子。要让单一接入点网络扩展至整个校园根本不可能，毕竟大型园区是以路由网络为基础。

妥协方案是由网管人员将无线网络分割为几个“孤岛”。以大学为例，一座孤岛相当于一栋建筑物或一个系，使用独立的IP寻址与路由信息。将无线局域网络分割为孤岛还可以满足某种有价值的行政目的。不同系可以设置独立的无线网络，使用自己的安全策略，满足自己的网络服务目标。孤岛型网络在设置上也比较快速，因为无需与其他孤岛协调，而且各个孤岛的网络设置工作可以同时进行。

这种拓扑类型可以在“连接至接入点骨干网络的接入点间”提供无间隙的移动性。在无法以单一VLAN作为接入点骨干的网络中，常见的妥协方案是将移动性限制在某个最有用的特定区域。举例来说，在拥有多栋建筑物的园区，通常是在个别建筑物中提供无间隙移动性，但建筑物间却无法漫游。各栋建筑物均配备如图21-2所示的无线局域网络，所有接入点骨干网络最后串联至园区骨干。

在图21-5a)中，有几个彼此相连的“孤岛”，每个孤岛各自提供本身的移动性。孤岛间的漫游无法由802.11本身来提供，需要类似Mobile IP或特殊的工作站软件。802.11允许ESS跨网段，但不支持无间隙的漫游操作。

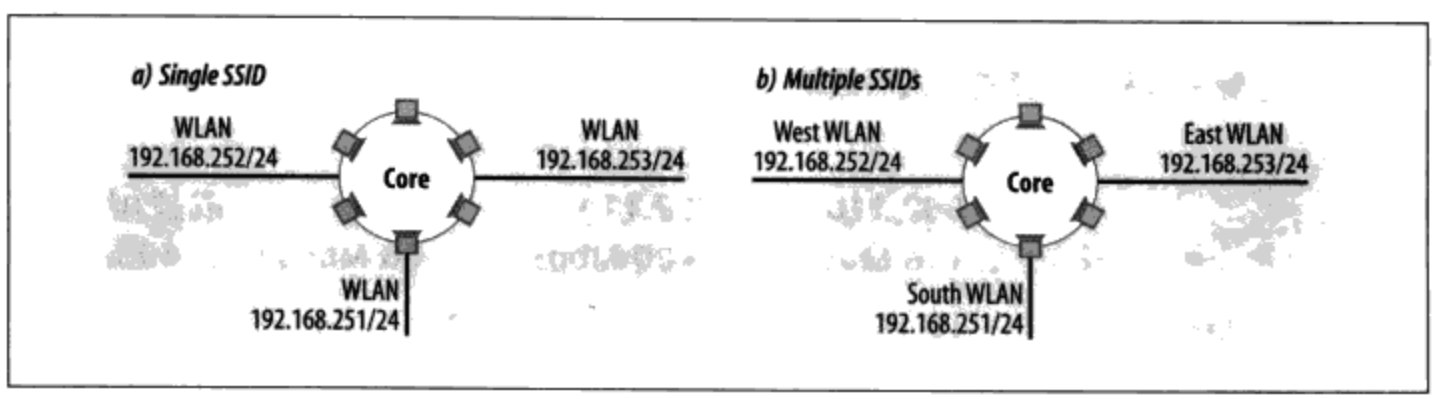


图21-5：非连续空间的位置

如果必须将园区分割成几个不相连的区域，那么务必为你的用户保留最重要的移动性。

大多数情况下，个别建筑物中的移动性是重要的。大多数建筑物是以交换器为核心，可以在整栋大楼中提供连接。

移动性

单一子网络架构是为所有接入点创建单一子网络来提供移动性，并让所有用户位于相同的子网络。这种架构借用了相同的概念，但应用在无法创建单一子网络的网络上。

在最基本的层次，此架构提供了可移植性。用户可以在孤岛间自由移动，丝毫不受限制。不过跨越孤岛时用户必须重新建立连接。重新建立连接有几种方式，有些根本不需要用户的介入。许多大学只提供有条件的可移植性，要求用户在离开之前关闭用到网络资源的应用程序。如果由可移植性的限制造成问题，可以利用客户端软件或点对点隧道协议来达到 IP 网络间的移动性。

这种拓扑类型与第一种拓扑类型非常类似，只是被复制到多个不同的地区。此外，彼此相连的孤岛可以通过防火墙连接至核心网络。孤岛间的移动性可以借助点对点隧道协议达成，确保用户不论身在何处，均能够连接至相同的逻辑位置。

图 21-6 显示了如何将移动性移植到一组分布式网络。图 21-6 a)中，两个工作站分别被赋予了一个 IP 地址，此 IP 地址来自工作站所连接的局域网络（图中标示为“Net X”与“Net Y”者）。连接之后，就会从“指定给 X 与 Y 网络的 IP 空间”配发地址给工作站。不过，工作站同时会连接至“集散中心”（central concentration point）。在逻辑上，工作站所连接的是集线器（concentrator），工作站会被配发一个 IP 地址，此 IP 地址来自集线器逻辑上所连接的网络（图中标示为“Net Z”者）。工作站所发送的封包将使用“集散中心”所配发的地址（Z）作为来源地址，但封包会被置于隧道（tunnel）中进行传送。回复信息会被路由回 Z，不过集线器维护了一组映射关系，可将网络 Z 上的地址映射至各局域网络上的地址。注意，图 21-6 a)中并未指明使用何种点对点隧道方式（tunneling method）。Mobile IP 的做法基本上类似，一些特殊的 IPSec 工作站亦然。

虽然图 21-6 a)的做法在概念上十分简单，但必须修改所有无线设备的软件。除了必须为所有无线设备安装新软件等管理方面的挑战，还得担负网络堆栈可能不稳定的风险。软件厂商也不见得支持所有操作系统平台，就算支持所有主要操作系统，也不见得支持一些嵌入式设备。图 21-6 b)提供了另外一种做法：将点对点隧道移至网络。在图 21-6 b)中，接入点并未直接连至骨干网络。骨干网络只用来将接入点连接至流量集散中心（traffic concentration point）。所有来自工作站的帧或封包均通过此隧道传送至集散设备，由集散中心分送到网络的其他部分。即工作站连接至哪个网络并不重要，因为任何数据均会被路由至流量集散中心。

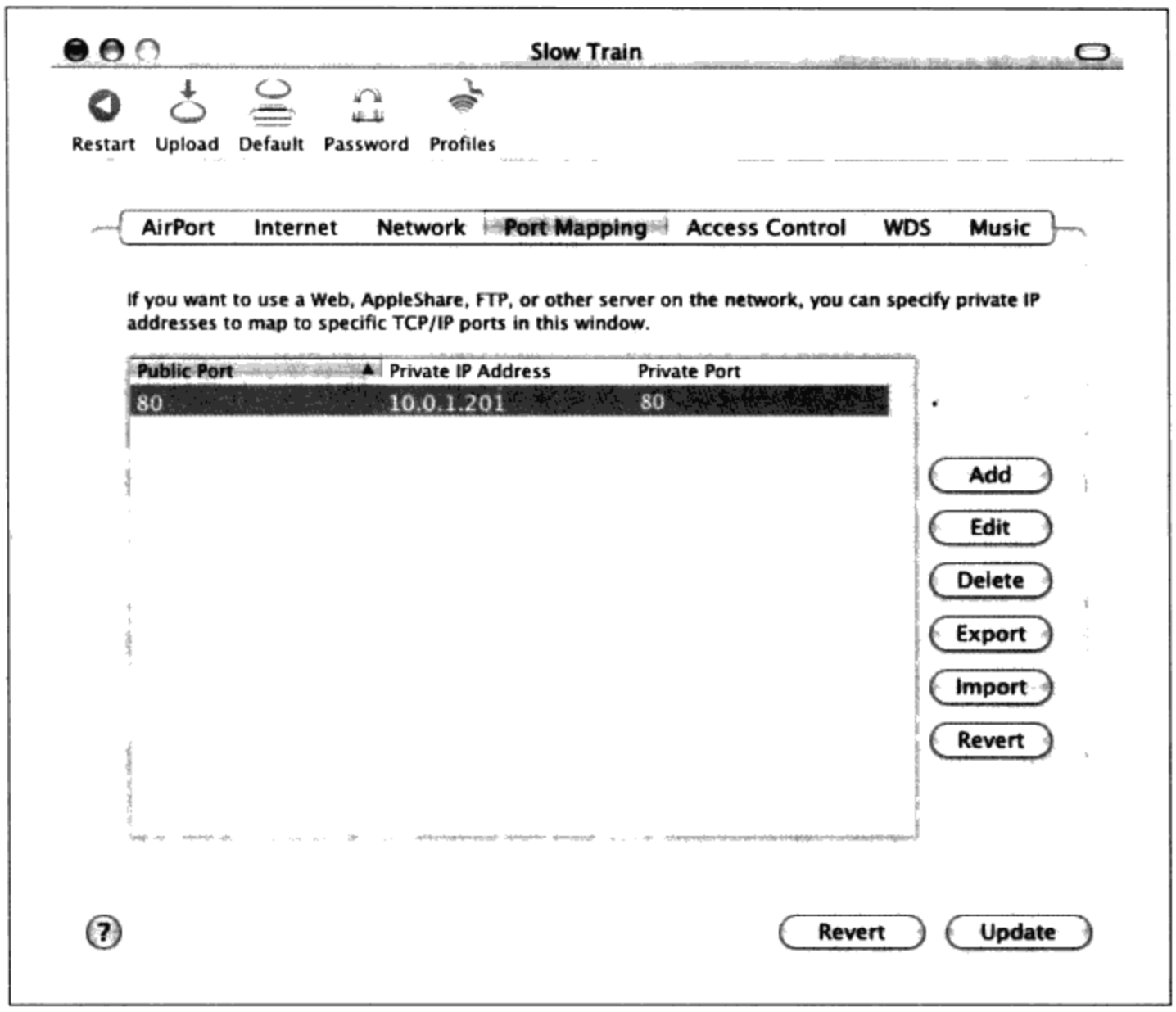


图21-6：以通道提供移动性

图21-6所举的两个例子中，重点在于工作站的IP地址变的与位置无关（location-independent）。局域网络上的IP地址只用于维持连通性，逻辑上的网络连接点则是由集散中心来定义，就像上一个拓扑类型一样。

点对点隧道的做法可以结合两个离散的覆盖区域。第一种拓扑类型中，移动性非有即无。以图21-5的离散覆盖区域为例，网络设计人员受限于局域网络原本的设计，只能针对最重要的区域为用户提供移动性。使用点对点隧道，可以将网络重组为单一的移动性块，但不必重新设计整个网络骨干。不过，点对点隧道的配置设定以及如何解决拓扑类型重叠问题仍有其困难。

安全性

这种架构的一项优点即是容易与IPsec配合使用。IPsec是一组坚固、值得信赖的加密协

议，被广泛运用于不安全的网络环境以及用来保护行经Internet的敏感数据。许多需要保护个人私密信息的机构也都在广泛使用IPsec。

网络层安全性的缺点在于它为恶意的攻击者提供了一个立足点。如果网络连接未经保护，攻击者便可取得网络地址，然后开始攻击其他工作站或者位于防火墙外的网络设施。坚固的防火墙防护绝对不可少，如此方能防范源自不可信赖的网络的任何攻击。主机的安全性也极为重要，因为恶意攻击者也许会试图摧毁工作站的安全防护来劫持VPN隧道，因此个人防火墙也是不可或缺的软件。

IPsec在设计上已经考虑到点对点架构。当用于主要网站间时，基本上是以点对点进行传输。不过，局域网络本身并非点对点网络（只要问问那些曾经使用ATM LAN Emulation的人便会明白！）若未经过修改或重新设定网络配置，使用组播的应用程序可能无法与IPsec配合使用。

性能

相较于第一种拓扑类型，为这些孤岛提供连接使得这种拓扑类型具备前者所欠缺的优势。每个孤岛的网关都必须能够传送该孤岛的流量，而不是由单一网关来处理所有无线局域网络的流量。无线与有线网络间存在比较多的瓶颈（choke point），因此每个瓶颈可以较小，使用较为便宜的设备。

这种架构经常与IPsec配合使用，通常是配合现有的VPN终端设备。可能发生的问题是VPN设备通常是作为远程的用户终端。如果局域网络的用户开始使用IPsec，现有的VPN终端设备也许会不敷使用。集中管理的VPN设备必须能够为所有无线局域网络上的流量负载提供加密。一个802.11b接入点大约会有6 Mbps的流量负载，而802.11a或02.11g接入点的流量负载可能高达30 Mbps。

针对这种拓扑类型，有几种不同的点对点隧道选项可供使用。点对点隧道（tunneling）必然会造成网络的负担，因为它必须用到封装机制。无线局域网络设备所面临的另一项挑战是，必须在点对点隧道协议中进行封包分割。有些用来连接接入点的局域网络骨干并不支持庞大的帧，因此行经Ethenet的任何点对点隧道协议均需进行分割与重组。除了分割所造成的负担，点对点隧道协议也需要额外的标头信息。分割操作可能造成不小的负担，这取决于所选用的协议。

将用户流量引导至网络骨干可能会降低服务质量。大型网络可能无法在接入点与集散设备间提供一致的低延迟转送性能，特别是将点对点隧道机制运用在类似IP这种尽力传递（best-effort）的协议上时。对一般的数据而言，服务质量稍微降低尚可接受。但如果无线网络是用来服务语音协议，点对点隧道机制就会造成实质上的影响。

骨干网络

相较于单一子网络架构，这种拓扑类型较能整合无法支持单一VLAN的分散网络。最糟的情况下，使用这种架构必须构建好几个小型的单一子网络骨干。不过，如果将点对点隧道功能移至网络内部，就可以让网络扩展至更远的地方，而无需更动骨干的任何部分。

客户端

VPN软件通常与这种架构配合使用，无线网络工作站的客户端软件必须经过设定。对某些机构而言，这并不会造成太大的负担，特别是大多数用户均已配备VPN软件时。不过，有些机构会限制具有远程访问权力的用户数目，以避免集成工程过于复杂或是对远程访问设备造成过大的负载。如果在这类机构任职，安装客户端软件以及部署大范围的无线网络将成为沉重的负担。如前所述，要保护个别工作站免于链路层的攻击，个人防火墙是必备的软件。最好内设个人防火墙，同时可以集中控制个人防火墙设定的VPN软件。

拓扑类型3：动态VLAN

“单一子网络”与“孤岛”等拓扑类型在设计上考虑到了市面上第一代接入点的限制。早期的接入点只是将所有用户连接至同一个网络，并未区分用户群，也没有给予差别待遇。“动态VLAN”则是首度使用有线领域VLAN的拓扑类型，让用户群得以使用不同的VLAN。这种拓扑类型是现有网络的扩展，将安全系统与过滤条件带进无线领域，而非另外构建一个平行网络。

802.1X是动态指定VLAN的基础。它完美地结合了无线网络与现有的身份验证基础设施。身份验证服务器具有用户数据与用户权限，可以将此权限信息映射到无线网络。举例来说，图21-7中的RADIUS服务器便是用来为接入点指定VLAN。RADIUS的“access accept”信息中包含了一种属性，可用来为通过身份验证的用户指定VLAN。根据这项信息，接入点可以标记来自该用户的所有帧并将之送至相应的VLAN。

在链路层（而非较上层）进行身份验证的优点是可以将用户置于特定的网络上，并且在一开始就赋予用户访问该网络的权限。当接入点从RADIUS服务器接收到消息，就会送出一个802.1X的“EAP Success”消息给工作站。工作站的网卡驱动程序会将“EAP Success”消息解读为“连上”（link up）并且送出DHCP请求，开始初始化网络堆栈。此时，网络已经根据用户的访问权限自动完成本身的配置设定。

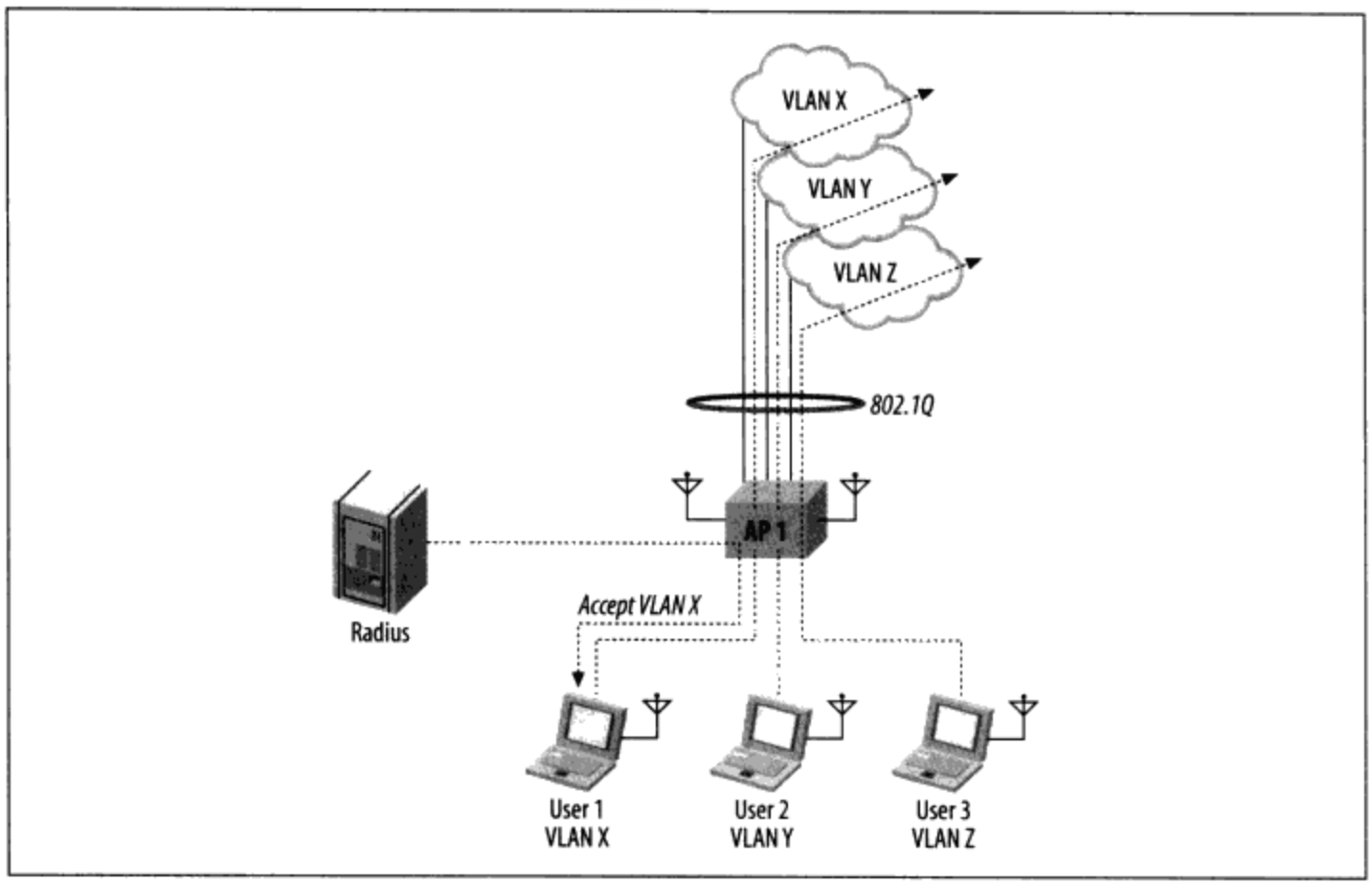


图 21-7：动态 VLAN 拓扑

移动性

在最高层次，此拓扑类型的移动性相当于第一种拓扑类型。用户连接至具有一致性的VLAN，因此不论身在何处，IP地址均维持不变。既然IP地址不变，则任何传输层或应用程序的状态在连接过程中仍然有效。

不过，这种拓扑类型底层所实现的移动性比单一子网络架构具备更多优点。第一个优点与使用身份验证服务器有关。RADIUS服务器所提供的属性可以确保用户连接至同样的VLAN，因此用户总是可以连接至网络上相同的逻辑点。

除了有助于实现移动性，一致的VLAN联机可以让其他服务运作得更加顺畅。在链路层提供移动性可以减轻上层协议的负担以及额外的操作。IPsec隧道可以维持一致性，因为IP地址并未改变；同样地，因为IP地址维不便，Mobile IP也没有必要更新位置。

安全性

由于VLAN的指定是通过802.1X与RADIUS，因此这种拓扑类型的安全性是以链路层动态产生的密钥为基础，包括动态WEP、WPA与CCMP。动态产生密钥带来使用认证服务器的第二个好处：一旦辨识出用户身份，便可为他们区分组群，给予不同的安全等级待遇。

为了区别不同用户组群的数据，接入点会使用多组密钥。身份验证后，每个用户均会被赋予一个默认（广播）密钥以及一个映射（单播）密钥。广播域（broadcast domain）的界限是由拥有相同广播密钥的工作站共同定义的。图21-8中，左边的两个用户属于相同的用户组，使用相同的广播密钥。如果其中一个工作站发出ARP请求，另一个将会予以响应。分属不同广播域的用户无法解读与处理此帧，因为他们持有不同的广播密钥。虽然各个用户组必须共享无线带宽，但只要分属不同用户组，在无线网络上就会有所区别。

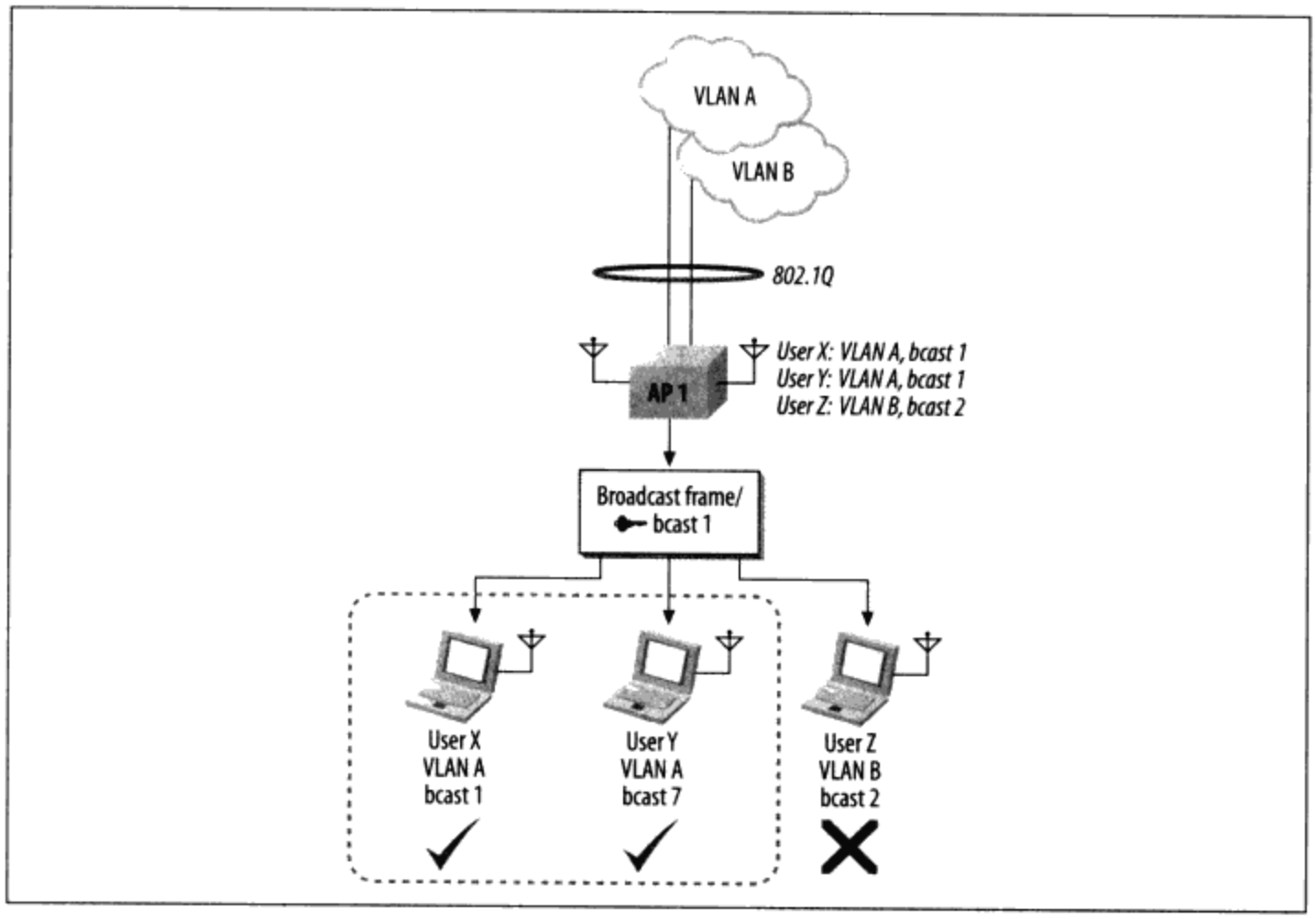


图21-8：以密钥划分广播领域

此外，以VLAN区分用户组，让网络得以提供差别式服务，如图21-9所示。用户识别与差别待遇的做法常被用来提供访客服务。内部用户根据用户数据库进行辨识与验证，然后将它连接至内部网络。访客在用户数据库中并无账号，因此无法通过网络的身份验证。认证失败后，访客就会被连接至不同的逻辑网络。访客网络或许会显示“形象页面”（splash pages）要求访客点选，同意不得滥用网络。有些机构甚至要求访客必须付费方能访问网络。

链路层安全性的另一个优点是可以将组播完美地整合到安全性协议当中。局域网络协议通常会大量使用组播或广播帧，而且用到组播帧的机会只会有增无减。无线网络之所以吸引人，是因为它们具备灵活性且不受空间限制。用来协助自动发现与设定新设备的协议通常十分依赖组播帧。

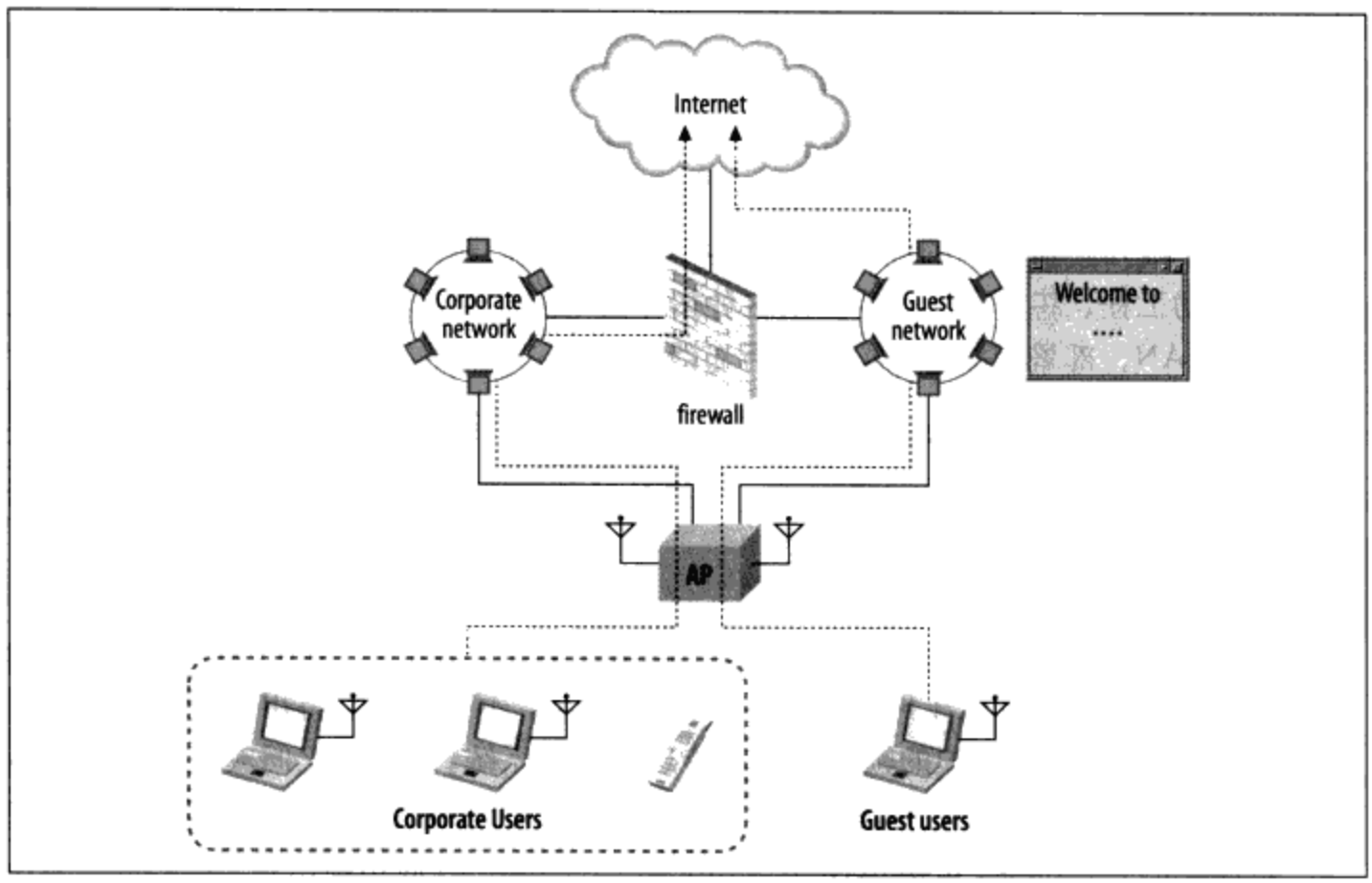


图 21-9：差别式用户服务

这种拓扑类型的一个缺点是跟官方对安全性的要求有关的。写作本书时，链路层安全性尚未符合 FIPS-140 标准（美国联邦政府的网络安全标准），因为 802.11i 的动态密钥衍生算法还有一点瑕疵，虽然CCMP所使用的加密模式已被核准过关。但要符合FIPS-140的要求，802.11i 网络所使用的密钥衍生算法还需要稍作修正。

性能

这种架构不需要架设关卡。在网络边界交换帧可以省去大型封包转送设备的需要。无线局域网络属于访问网络，因此就定义上而言，无线局域网络不应该造成网络核心过多的负载。不过，这种架构的缺点是部署时最好已经有现成的大型高速交换式核心。

骨干网络

要动态使用VLAN信息，通常得重新设计网络骨干。哪些部分需要重新设计，取决于无线局域网络与核心网络的连接方式。当无线局域网络连接至核心以便把用户连接至不同网络时，通常是使用 802.1Q 标记链路（tagged link）。无线局域网络产品的差异在于是否广泛使用标记以及这些标记在网络上的分布情形。大致上，要将VLAN信息传递至接入点主要有两种方式。

直接核心连接

在此情况下，接入点必须直接连接至网络核心，通常是通过 802.11Q 标记链路。

需要注意的是，接入点是以逻辑链路连接至核心网络。使用某些设备时，接入点必须直接与核心网络连接，亦即每个与接入点连接的交换端口（switch port）都必须支持无线用户所使用的任一VLAN。将所有接入点直接与核心连接，需要在骨干网络大动工程，甚至因此破坏使用这种拓扑类型的规则。如果连接AP的插槽并不支持 VLAN，部署网络之前必须先行布线。

直接连接至网络核心也有潜在的安全风险。大多数连接会对用户进行身份验证，不过连接本身却没有经过这道手续。攻击者只要将接入点调包，就可以直通网络核心。

间接（点对点隧道式）核心连接

有些产品允许使用点对点隧道协议，无需将所有接入点直接连接至网络核心，如此可以避免大幅变动骨干网络。用户连接至接入点，不过接入点将用户的帧置于核心网络之前，要先将用户的帧通过隧道传送至远程系统。接入点之间或者接入点与集散设备之间均可建立传输隧道。所使用的点对点隧道协议可以是专属协议，也可以是简单的封装标准，如Generic Routing Encapsulation（通用路由封装，简称GRE）、IP in IP 或者 Point-to-Point Protocol over Ethernet（简称PPPoE）。

图 21-10 a)中，两个接入点分别位于不同的VLAN。用户身份验证完成后，接入点负责将用户连接至适当的VLAN。如果接入点被直接连接至用户必须连接的VLAN，联机就相当简单；否则，必须在两个接入点间建立传输隧道。AP2会先找出用户应该连接的VLAN所在，然后通过其与AP1之间的隧道传送用户的帧。在逻辑上，用户还是连接至AP1，不论其实际所在位置为何，这取决于实现方式。或许有必要避免在距离过远的两端建立传输隧道。如果两个网络跨越州际甚至跨越海洋，终究会引发用户的抱怨。

图 21-10 b)中，连接点集中于网络核心，而非分散于网络边界。接入点所接收到的帧会通过隧道传送至集线器（concentrator），然后送至适当的网络。VLAN信息只有在帧抵达终点时才用得到。抵达集线器之前，帧本身并未包含任何VLAN标记。使用远程点对点隧道系统的好处是允许用户连接至本地以外的VLAN，只要集线器能够访问 VLAN 即可。

比较而言，点对点隧道式连接不需要大幅修改骨干网络，因为标记可以在本地进行处理。如果是直接连接的话，与接入点相连的各个连接端口都必须承载用户所要连接的VLAN的完整信息。其对于骨干网络的影响大致和第一种拓扑类型相去不远。相对而言，间接连接可以跨spanning tree（生成树）领域延伸至较远的地区，而个别交换端口的配置设定也比较简单。

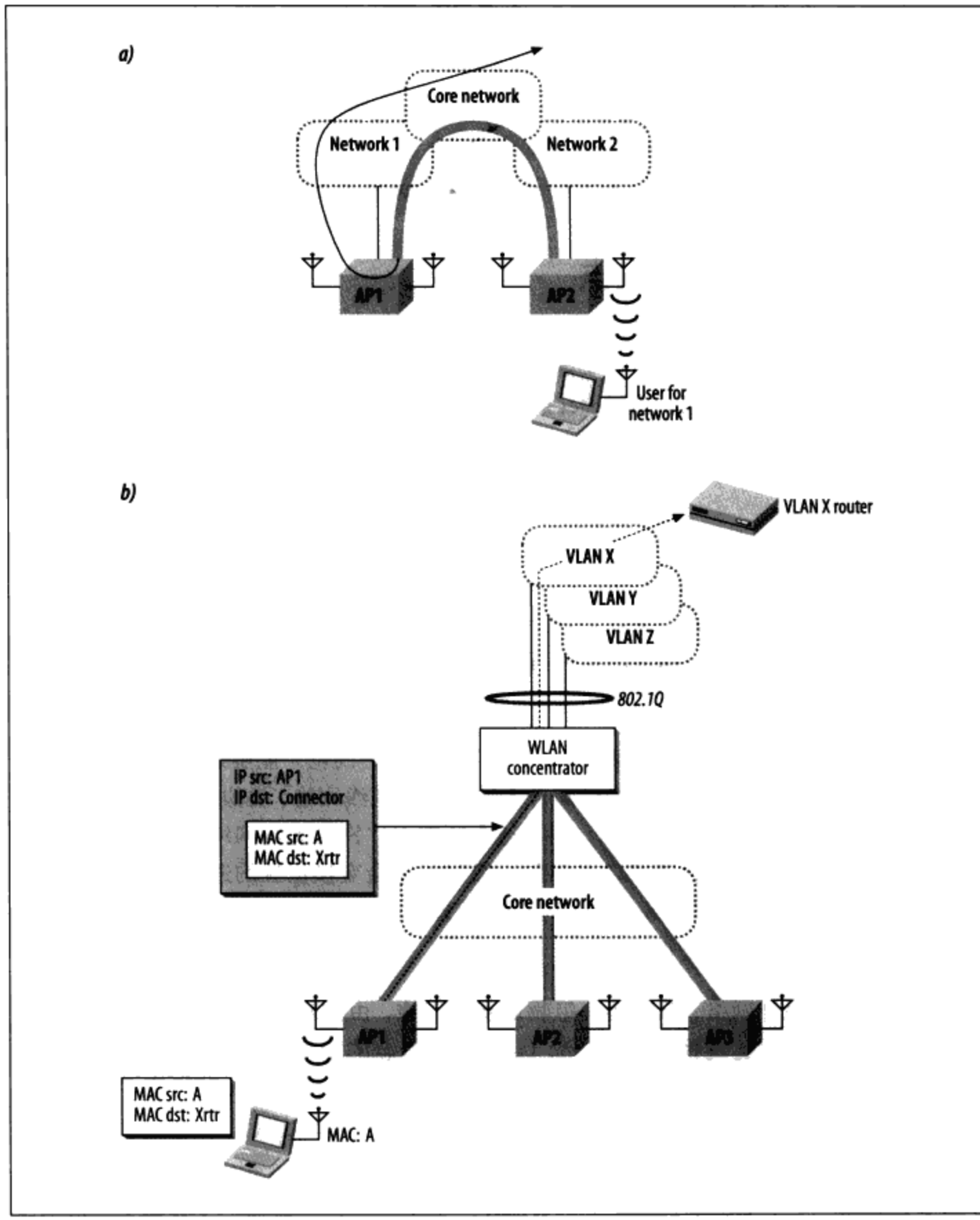


图 21-10：动态 VLAN 产品的核心连接

客户端

常见的操作系统大多已经内置802.1X申请者软件。Windows 2000、Windows XP与Mac OS X 10.3等操作系统均内含802.1X申请者软件。如果打算使用其所支持的身份验证协议，就无需担心软件安装的问题。此外，这些内置的申请者软件通常可以通过大规模的系统管理工具进行配置设定，协助传送所需要的证书或配置设定信息。

拓扑类型4：虚拟接入点

前一种拓扑类型是直接应用802.1X与动态VLAN。不过，只有包含一类用户时这种架构的运作才最顺畅，因此有点不切实际。目前大多数网络在设置时通常是将员工连接至内部网络，同时为访客提供对Internet的访问。支持不同用户的功能已经相当常见，但必须对安全性架构做额外的调整。不同的逻辑网络必须平行运作，而且通常使用不同的安全模型。

构建多重逻辑网络的方法之一，就是构建多重物理网络，然后分别管理。但由于耗费网管人员的时间、接入点的摆放位置、电力、网络连接与无线电波资源等因素，使得构建多组物理网络根本不切实际。替代方案是使用虚拟接入点，只要一套物理基础设施，就可以构建出多重逻辑网络。物理网络拥有者就像电信业者一样，负责维护基础设施以及传递其他网络的数据。

几年前，机场兴起一阵热潮，让商务旅客（以及他们的钱包）能够通过802.11连接至Internet。起初，机场是和特定集成厂商合力打造单一无线网络，类似本章所提到的第一种拓扑类型。它只供商务旅客使用，并不适合所有人。许多无线网络应用根本被忽视。无线网络最适合用来提供需要移动或每隔一段时间就会变换位置的连接，例如零售柜台或是登机口的航空设备。不难理解为何信用卡处理服务或航空公司会认为设计给旅客用的网络无法提供必要的安全性。

以虚拟接入点来设计网络，只需要一组物理基础设施，由实际建设的业主所拥有。实际拥有者负责协调整栋建筑物的频率分配（注5）。从资金的角度来看，单一物理网络就是一种独门生意，拥有者可以对访问网络的动作进行收费。分租办公大楼的业主可以让无线网络的使用更加方便，吸引更多的承租人。

对网络用户而言，虚拟接入点可能更符合所需。既然实体建设是由单一机构负责，就不至于重复投资，也不会产生频谱之争。虚拟接入点可以提供一般接入点的服务，但因为共享基础建设，相较之下就便宜得多。最高级的虚拟接入点相当于好几个独立的接入点。

注5：分租大楼的新式租约通常会写明业主保有电磁频谱的控制权，可以设置整栋建筑物的网络，无需顾及承租户的设备，虽然FCC并不同意此种做法。

可以料想未来虚拟接入点系统将提供管理接口给用户。网络服务的承租户未来将可通过低端的管理接口自行设定所承租的虚拟网络。

以虚拟接入点打造的网络如图 21-11 所示。基本上，它允许网管人员以一组物理设施来设置与控制数个动态 VLAN。图中有三个使用 WLAN 的网络。网络 A 是典型的公司网络。用户要访问此网络，必须在公司的 RADIUS 服务器上具有账号。网络 B 属于一家热点（hot spot）服务供应商。为了不受设备的限制，许多服务供应商会使用基于 Web 的身份验证系统，除非用户已经通过身份验证并且同意付费，否则便无法访问网络。最后，网络 C 被设计用来提供 IP 语音服务并且配备了一个 IP PBX 系统。一组接入点被设置来支持以上这三个网络。网络 A 使用第一个 SSID。此 SSID 的安全性配置要求用户必须通过 802.1X 与 RADIUS 服务器进行身份验证，打算连接至该网络的系统需要安装必要的客户端软件，例如杀毒软件。SSID A 可以支持网络 A 上的几个不同 VLAN，这取决于后端 RADIUS 服务器的设定。在设定上，网络 A 支持坚固的加密方式。网络 B 使用第二个 SSID 并且通过 Web 进行身份验证。只要通过身份验证，用户就可以访问 Internet。网络 B 并未加密，因为服务供应商不希望局限于某种特定平台，或要求用户使用 Web 浏览器以外的特殊软件。SSID C 被设置来支持 IP 语音（voice over IP）应用。SSID C 上的流量比其他两个网络具有优先性，因为语音流量对服务质量的要求较高。如何进行身份验证取决于所使用的设备。有些 VoIP 手机尚未支持 802.1X，网管人员只能依赖 MAC 过滤与静态 WEP 提供安全性。

移动性

这种拓扑类型所提供的移动性基本上和前一种拓扑类型没有两样。VLAN 可以在网络边界动态产生并将用户连接至网络，因此客户端工作站是被动态连接至网络上正确的接入点。和之前的情况一样，可以使用额外的协议让移动性扩展至其他 VLAN 领域。

对虚拟接入点而言，限制移动性相当重要。此架构在设计上侧重于如何提供服务，但有时候并不需要无所不在的服务。如果办公大楼打算为承租户提供连接服务，业主或许会限制承租户的连接范围。连接服务可以限制在某个特定楼层或侧翼，而不是整栋大楼均可随处连接。如果机场打算以虚拟接入点设置网络，公共的热点服务供应商应该被限制在公共范围，而机场的可用网络就不能随便访问了。不同产品会以不同的做法来限制移动性。和其他网络控制功能一样，最好选用可以集中管理的访问控制。

安全性

由于和链路层的关系密切，这种拓扑类型通常配合 802.1X 与 RADIUS 一起使用。802.1X 不见得必要。但每个虚拟接入点都应具备独立的安全性配置，让客户可以自行调整本身的安全性策略。不同的客户有不同的需求，以虚拟接入点打造的网络应该容许任何合理

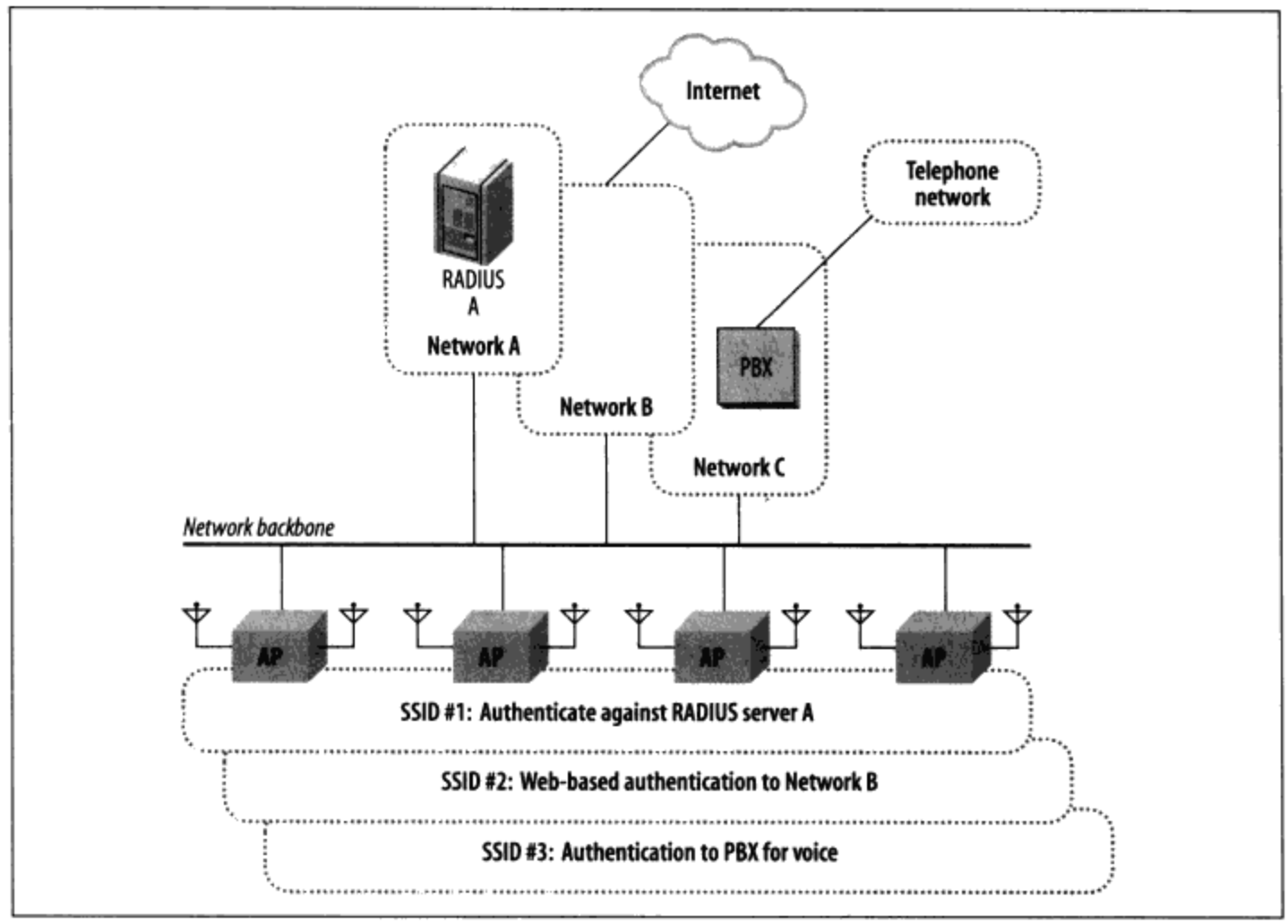


图 21-11：虚拟接入点

的安全性策略。举例而言，大多数热点供应商均采用Web式登录系统。虽然对某些应用而言，Web式登录系统已经够好了，但法律上的规定或许会要求对个人资料的访问采用更严格的做法。虚拟接入点网络必须能够同时容许两种访问方式。

性能

性能不会受到瓶颈（choke point）的限制。由于无线网络直接连接至较大的网络核心，性能上的唯一限制就是核心的壅塞。

多承租户网络所面临的最大问题是业主所打造的网络是否足以应付所有用户的需求。如果网络是私有且用于自身目的的，就可以估计出网络的需求。如果是提供网络服务给别人，借由咨询用户得来的估计或许会十分模糊。

另外值得注意的是，由于以单一接入点扮演多个虚拟接入点的角色，分析软件或许会显示信道负荷过度的情况。如果网络在设计上是以所有用户需求的总吞吐量为考虑重点，在空中多加几个网络是可以接受的。

骨干网络

和其他接入点一样，虚拟接入点用来连接无线与有线网络。以虚拟接入点为例，无线与有线网络两者均可构建于一套共享的物理设施。除了单一有线网络或者一组由同一机构拥有的网络外，也会有将几个客户网络连接至骨干的需求。当所有网络均属于同一机构，或许会有类似的安全需求，因为它可以轻易地连接至无线网络。要将无线网络映射到由不同（或许彼此竞争的）客户所拥有的有线网络，可能需要额外的方式来确保安全性。

客户端

和其他拓扑类型一样，需要安装哪些客户端软件，大部分取决于所使用的安全协议。在简单的一端，网络可以采取最简单的方式，使用Web式身份验证就无需安装任何客户端软件；在最困难的一端，网络可以使用几种安全协议，每一种协议各自有其对客户端软件的需求。虚拟接入点网络的优点之一在于虚拟接入点可以创建好几个网络，每个网络各自有其特殊的安全配置设定。

模糊的界限：Wi-Fi 交换器

过去几年最常被提及的无线网络发展，即新型“Wi-Fi 交换器”架构的出现。广义而言，Wi-Fi交换器是将网络功能自接入点转移到提供控制与管理功能的集成设备。

对无线网络而言，控制与管理功能十分重要。无线网络通常需要相当多的网管支持，因为它们是由一群小型设备组成。通过管理功能的支持，Wi-Fi 交换器可以协助网管人员打造更大型的网络。只要通过几部交换设备，网管人员就可以管理所有接入点，而不必单独管理个别接入点。

既然可以省下控制接入点的时间与精力，则Wi-Fi交换器有助于在无线网络中加入更多接入点。接入点数目更多，意味着每个接入点的覆盖范围缩小但更为密集，这可以降低竞争带宽的机会。

Wi-Fi交换器可用于本章所提到的任何一种拓扑类型，虽然各家厂商的产品在各种拓扑类型上的表现可能不尽相同。不同厂商会采取不同的做法来降低管理上的负担以及提供整个网络的移动性。因此，最好挑选适合于自己网络并且支持所选拓扑类型的产品。

逻辑架构的选择

选择逻辑架构时必须衡量许多不同的因素。其中一些攸关安全性，这将于下一章探讨。不过，大部分是与如何在性能、简单性与功能方面取得平衡有关。

1. 不论选择何种架构，起码应该提供移动性。802.11是在扩展服务集范围内提供移动性，对工作站而言，此ESS必须位于单一IP子网络。本章提到的所有架构均将工作站连接至单一子网络，虽然所使用的机制可能完全不同。

   a. 对只有几个接入点的小规模部署而言，任何一种架构均属可行。如果规模很小，前两种比较容易设立，且如果未来不太可能新增接入点，此类做法比较具有成本意识。

   b. IEEE的接入点内部协议只提供链路层的移动性。若要跨越路由器的界限至新的广播领域，需要在网络层协调无线局域网络访问设备。写作本书时，若要提供子网络移动性，通常还需要挑选同一家厂商的解决方案。Mobile IP虽是开放标准，但并未得到广泛采用。

2. 客户端必须感觉到他们被连接至单一IP子网络，不论连接点的实际位置为何。不过，并非所有工作站都必须连接至相同的子网络。多重子网络可以在空中相互重叠。在空中提供多重子网络可以更精确地控制用户的访问权限以及区分不同的用户组，但需要用到802.1X。

3. 现有的网络会造成何种限制？过去的决策这个包袱或许会限制目前的可能选择。

   a. 由于生成树（spanning tree）的限制，分布甚广的不规则网络可能无法将VLAN扩展至整个网络。在接入点必须连接至核心网络时，或许就无法使用单一无线VLAN或是动态VLAN模型。

   b. 动态VLAN拓扑类型可能必须借助广泛分布于网络上的802.1Q标记。如果尚无法取得VLAN信息，网管人员就必须找出一种方式，可以将它传送至支持无线网络的所有地区。需要直接与核心连接的产品无法兼容于路由式核心网络（routed core network）。

   c. 瓶颈（choke point）可能分布在网络各处。之前已经存在的瓶颈会对可以连接至各处的无线设备数量造成限制。如果有意在架构中设置瓶颈，则它的速度必须够快，才不至于对吞吐量造成限制。

4. 网络拓扑类型的选择部分取决于网络所使用的安全协议。动态VLAN指派只能配合802.1X一起使用，因此对打算使用链路层安全机制的网管人员而言，后两种拓扑类型最适合。前两种拓扑类型比较适合使用IPsec与个人防火墙等网络层安全机制。本章并未直接探究不同安全做法之间的取舍，这些将留待下一章处理。

5. 静态寻址并没有必要。它只会造成不必要的复杂度，却无法带来多少好处。网管人员必须管理地址的分配并且直接参与无线局域网络新系统的安装事宜。

   a. 静态寻址只会带来些许安全性方面的好处。发送端并不会验证来源IP地址，攻击者可能会搜集无线网络上所使用的IP地址，除非设置坚固的链路层防护。

b. 若要追踪用户，比较好的做法是采用802.1X这类以用户为中心的网络。只要在RADIUS服务器设定好通行于全网络的用户名称，用户与IP地址之间就不必存在对应关系，只需对应到用户名称即可。

c. 动态寻址可以减少用户间意外使用相同地址的机会。通过DHCP代理机制，只要一部DHCP服务器就可以服务好几个VLAN；如果已经有现成的DHCP服务器，就没有理由再架设另外一部。

表21-4列出了本章曾探讨过的各种因素。安全性是相当复杂的议题，不可能被浓缩成简单的表格，因此下一章将以整章的篇幅加以探讨。当各位参考此表并思考购买决策时，切记各种产品适合配合的技术不尽相同。

表21-4：拓扑类型比较表

	单一子网络	孤岛型网络	动态 VLAN	虚拟接入点
移动性	VLAN 越大，移动性越高。受限于 802.1D 最大直径	因孤岛大小而异	高	高，但必须予以设限
性能	因瓶颈设备的性能而异	因集线器的性能而异	高，因为采用分布式加密	与动态 VLAN 相同
骨干网络	高，但因现有网络而异	因移动性范围而异[a]	因连接至网络核心的类型而异	与动态 VLAN 相同
客户端	因客户端软件而异[b]	因客户端软件而异[b]	操作系统内置	与动态 VLAN 相同，处理各种客户端安全模型的能力较佳
IP 寻址	高（新的子网络与路由）	高（新的子网络与路由）	不需要	与动态 VLAN 相同

a: 新型产品可用逻辑方式将接入点连接至网络的控制设备以减轻骨干网络的负担。

b: 单一子网络与中心集线器架构通常会配合 VPN 软件来提供额外的安全性。如果使用 VPN 软件，显然就需要规模较大的客户端集成操作。

第二十二章

安全性架构

自从无线局域网络出现，就与安全性（或者说缺乏安全性）脱离不了关系。无线局域网络的部署之所以不简单，是因为要在开放的网络媒介中提供安全性，原本就是莫大的挑战。早期的无线网络简直就像是在停车场开放网络插座供众人使用。

早期限制访问和保护数据的解决方案之所以可笑，部分是因为历史的教训不见得能够立即适用。传统的网络安全性强调物理媒介的防护以降低网络遭受攻击的风险，但无线网络之所以有用，却是因为媒介并非锁在墙壁和门之后。既然无法为建筑物打造一层RF防护罩，那么最好假定对任何有意访问的人而言，物理层的门户都是洞开的。

既然网络媒介无法提供任何物理安全性，就必须通过加密来保护用户的登录操作以及流经网络的数据。加密可以在仅以无线电波相连的设备间建立信任关系。密码系统有助于识别用户的身份并且确保接入点的确不是冒充的。一旦用户通过身份验证，密码系统还可以继续扮演众人所熟悉的角色，将流经网络的数据搅乱以防遭人拦劫。

网络安全性与网络架构之间的关系密不可分。早期的802.11网络在安全性方面的基本瑕疵，导致现有的有线网络与无线网络之间被划分了一道实体与逻辑上的界线，因此牺牲了可用性。经过改良后，安全协议已经能够将无线网络整合到现有的有线网络。但是与物理网络仍然有所区隔，因为无线媒介具备与其极为不同的物理属性。对用户与网管人员而言，它属于整体的一部分。从某些方面来看，它的演化过程和移动电话网络有点类似。蜂窝式移动电话网络在实体上也有所区隔，因为它们需要运用特殊设备与管理系统来处理用户无线链路所带来的挑战。不过，它们也是现有电话网络的逻辑扩展。无需训练，用户即可在移动电话网络里使用相同的（语音）应用，而移动电话网络也被整合到了电话管理系统中。如今无线局域网络已有能力提供适当的安全性，因此两者便开始整合在一起。

安全性的定义与分析

一般而言，数据安全性可用三种属性加以定义，三者兼备方能够确保安全性。此处所提出的只是非正式的定义。本节中，我会试着遵循基本的步骤，说明无线局域网络的安全性何以失败，以及如何采用业界所开发的解决方案来解决部分问题。

完整性（Integrity）

大致而言，如果数据遭未经授权的用户篡改，完整性就已经被破坏。（数据是否遭人不当更改？）

私密性（Secrecy）

这三项属性当中，私密性或许是最容易理解的。每个人都有秘密，也清楚泄密的后果。（数据是否已经被公开？）

可用性（Availability）

能用的数据才算是数据。拒绝服务（denial-of-service）攻击是可用性最常见的威胁。（想要读取数据时是否能够如愿？）

无线局域网络技术在这三个领域均力有未逮。值得注意的是，不论是因为早期加密协议的基本瑕疵致数据易遭窥视，还是缺乏坚固的用户身份验证，问题的焦点都集中在私密性方面。然而，无线局域网络的瑕疵不仅如此。在最近的协议问世之前，无线局域网络一向很难防范所谓的“流量注入”（injecting traffic）攻击，而缺乏帧验证机制也使得拒绝服务攻击变得十分容易。

网络与计算机安全性通常被视为风险管理议题，无线安全性也不例外。有许多方法可以提高无线网络的安全性，市面上许多产品也都能符合各位的需求。在实际动手之前，最好心中先有个蓝图。对你的网络而言，哪些是最重要的网络安全议题？你愿意花费多少代价来降低这些切身议题所造成的风险？本章只是稍微勾勒出必须考虑的议题。较完整的做法可以参考一些重要的政府出版物，如NIST（美国国家标准与技术研究院）所出版的网络安全系列专刊（Special Publication）。Special Publication 800-48 探讨了许多无线局域网络的相关议题，虽然对802.1X着墨不多（注1）。NIST也负责制定联邦信息处理标准（Federal Information Processing Standards，简称FIPS），其中有若干FIPS出版物可作为构建安全网络环境时的参考。

无线局域网络的安全问题

802.11原始标准出炉后，有不少关于安全性的研究与分析陆续进行着。设计之初，并未

注1： NIST SP 800-48 可自 *http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf* 下载。

将安全性纳入原始规范，因此对未经授权的用户而言，网络形同门户洞开，也无法保护行经网络的任何数据。设计上，无线局域网络十分具有灵活性。灵活性通常不是坏事，不过如果一项技术在设计时可以不必考虑适当的安全性，灵活性反倒可能变成一种诅咒。

请出示身份证明：身份验证

授权使用之前，必须先验明正身。为了区分哪些用户有权访问数据，必须通过密码系统来进行身份验证。除非网络能够确认用户身份，否则不该提供机密协议所使用的加密密钥。早期协议的失败原因之一就是只验证用户所使用的硬件，而不验证用户本身。虽然用户与机器之间的关系密切，但两者之间的关联不见得如乍看之下那么一致与可预期。

为了改善最初的802.11身份验证机制，后续开发出了几种不同的做法。比较常见的做法是设置一套透明的代理机制，负责接收来自网页的请求，然后导向自定义的入口页面进行身份验证。通过加密网页，Web身份验证可以有效改善身份验证机制，但无法提供更坚固的加密方式，因为无法以之衍生出链路层加密协议所需要的密钥。

空气中的秘密：加密

保护行经无线链路的数据的私密性，是所有无线网络均需面对的首要挑战。由于没有实体界限，数据就如字面所言“散布于空气中”（in the air），只要持有适当的接收设备，任何人均可随意取得。以802.11无线局域网络为例，各位手上的802.11网络接口即可作为接收器，也可以外接高增益的天线。

要避免数据沦落到“不对的”人手中，必须对数据进行加密控制。攻击者可以被动聆听帧且加以分析，若要防范数据遭受拦劫，势必要借助密码系统。密码系统就像是广谱抗生素（broad-spectrum antibiotic），可以为数据提供机密性，防止数据遭不当人士取得。数据的机密性通常是靠加密协议达成，只允许拥有密钥的经过授权的用户访问数据，以确保数据在传输过程中未遭篡改。

整个网络的私密性与完整性：私设接入点

只要在大多数网络工程师面前提到“无线安全性”，得到的反应通常是强调如何保护无线链路，提供适当的加密操作来维护链路的安全。但私密性也牵涉到如何将未经授权的用户排除在外，不论是有线还是无线网络。

如果未采取适当的安全机制加以保护，无线网络很有可能变成能够随意进出的侧门。安全的内部网络与接入点之间若连接不当，就可能为外人另辟蹊径，绕过原本已经就位的安全防护。此外，有些网管人员担心未经授权（或私设）的接入点会在未经许可的情况下被偷接到网络上。私自架设的接入点通常是消费性电子产品，其安全性与可靠性也就可想而知了。

不过，私设设备终究不是特别令人感兴趣的安全问题。在网络的领域中，每股新的浪潮都会带来不同的风险。不过这些风险终将被解决，私设设备也不例外。关键策略是找出这些私设设备所在的位置并将可能的损害降到最低。

要找出未经授权的私设设备，有几种可行的方式。最原始与最粗暴的方式，就是在膝上型计算机安装Netstumbler，然后四处搜寻接入点。一旦侦测到未授权设备，就可以开始放慢脚步，试着找出实际位置所在。Netstumbler只是个简易的工具，大多数的802.11接口也只能显示概略的信号强度。相较于四处搜寻，比较高级的做法是使用无线协议分析仪。有些分析仪提供额外的功能，可以协助追踪未经授权的接入点，例如外接用于搜寻的定向型天线或者能够实时显示当前信号强度的特殊搜寻模式。就算不用定向型天线，能够实时显示信号强度变动的搜寻模式在定位私设设备上也很有效率。通过AirMagnet分析仪，我曾经在几分钟内就追踪到一个接入点。

四处搜寻私设设备有时会碰上问题，特别是当用户已经认出谁是“接入点猎人”，知道何时该关闭私设设备电源时。除了通过劳功力密集的搜寻方式外，网络工程师已经逐渐采用网络型解决方案。只要战略性地将无线电探测设备遍布在管辖范围，当这些私设设备一开机，网管人员就会立即发现。所使用的探测工具可以是分布式分析仪当中的特殊模式、特殊的无线IDS或者接入点中央控制系统功能。有些网络型系统甚至能够加以反制，以瘫痪或其他手段来拒绝私设设备，不过这些功能在广泛采用之前可能还需要经过一番改良。

网络完整性：流量注入

和有线Ethernet一样，帧欺骗（frame spoofing）在802.11中并不困难。如果没有使用加密协议，恶意的用户只要修改802.11接口的MAC地址，就可以达到目的。和Ethernet不同的是，802.11所使用的物理媒介会在空中四处传播。802.11设备并非连接到物理媒介，而是置身其中。确保空中的帧来自合法授权的网络相当困难，需要用到一整组加密协议。除了改善加密机制外，WPA还提供加密协议来验证每个帧，以防范伪造与流量注入攻击。

如同其他一些问题，流量注入的风险取决于许多因素。在某些企业网络，遭窥视的风险可能高于流量注入。对服务供应商而言，帧欺骗或许是最主要的风险，因为这对营业收入没有半点帮助。

网络可用性：拒绝服务

802.11网络可能遭受两种类型的拒绝服务攻击。在无线电层，噪声会严重干扰数据传输。任何位于802.11频带的电波干扰源都有可能使得数据传输中断。攻击者可以使用已知的能够完全断绝传输的噪声让数据无法传输。由于无法以“法拉第笼”（Faraday cage）防

护整栋建筑物，最好的可行方案就是找出干扰源并予以关闭。大多数情况下干扰源并非恶意造成，只要能找出干扰源，事情就不难解决。有些手持式设备可以显示噪声的准确位置，有助于找出干扰源何在。

就算使用TKIP或CCMP，也只有承载用户有效载荷数据的帧才会验证传送端地址。管理与控制帧并不会经过验证，因此很容易伪造。拒绝服务攻击十分简单，因为攻击者只需要知道接入点的MAC地址，就可以开始传送Disassociation或Deauthentication信息。将来或许重要的控制信息也必须经过802.11协议的验证。在此之前，网管人员必须设计可以侦测伪造控制帧的工具，否则就得承受此种风险。

网络完整性与可用性：私人设备

无线安全协议是设计来对用户进行身份验证与授权，但用户通常会拥有好几部机器。有些用户喜欢携带私人机器到办公室并连上公司网络。私人设备通常不像公司设备装有完整的防护软件与设定。在家里，私人设备通常被直接连到未经过滤的Internet，可能会感染各式各样的病毒或蠕虫。一旦感染病毒的机器连上公司网络，它就可能被当成跨越安全防护的跳板。

论及无线局域网络的安全时往往会提到“病毒载体”（viral vector），虽然这属于一般性的安全问题。任何带进办公室并连上网络的机器均可能夹带恶意软件，不论是连接到有线网络还是无线网络。防范病毒载体主要有两种方法。其一是在网络周边进行病毒扫描，将防毒软件或类似工具整合至网络交换器。长远来看，这是有效的策略；短期而言，得视病毒扫描与恶意软件侦测等截然不同的需求（高CPU负载，较大的内存需求）如何整合到目前的交换器硬件而定，因为交换器通常只包含用来发送封包的特殊芯片组以及运算能力有限的通用型处理器。

另外一种做法才刚出现。许多采用Microsoft技术的网络非得使用Microsoft的机器身份验证（machine authentication）。为了确保用户使用的是经过授权且具备适当安全防护的机器，认证服务器必须将“用户身份验证”与“机器身份验证”加以结合。有些802.1X认证者可以整合两种认证方式，虽然这种做法在密码学上并不完整，因为这两种认证方式并未被牢牢地结合在一起。RADIUS服务器厂商才刚开始采用类似的做法。如果能够成功结合两种认证，新的身份验证协议（或者协议选项）将可为此种组合提供密码学上业已证明的安全性。

网络完整性：分道传输

网络通常用来服务不同的用户组。组间通常没有任何交集且不应共享任何数据。VLAN、封包过滤以及防火墙可用来区分用户组。要在无线链路维持用户组的区分，不同组必须使用不同的加密密钥。此概念在前一章提到虚拟接入点架构时已经说明过了。

在网络边界实施分道传输（traffic separation）效果最好。服务供应商很难要求客户使用特定的软件配置。很少有服务供应商能够指定公共网络必须使用特定厂商的VPN软件，就算有也是少数。相较之下，强制使用操作系统内置的802.1X软件就比较容易。

分道传输在企业的802.11网络中可能没有容身之处，特别是在新公司或者中小企业。不过对于具备灵活性的网络而言，“服务供应商”（service provider）一词有更广的定义。许多学院对802.11十分感兴趣，打算在新建大楼或改建时使用802.11以省下布线成本，并允许其他厂商代售Internet访问服务以增加收入。许多城市也有此想法，特别是那些已经提供Internet访问的单位，例如图书馆。一般大众将被置于只能访问Internet的网络上，市政机关的雇员则使用另外的网络。此外，有时必须根据部门进一步区分权限，特别是那些掌管机密数据（如公众保健信息）的市政机关雇员。灵活性也有助于各城市达到各自的社会目标，如果现有场所（如图书馆）的网络方便雇员使用的话。

身份验证与访问控制

设计之初，无线网络就已经考虑到连接的便利性。事实上，便于连接乃是许多新式无线技术的主要优势。802.11网络会对所有聆听Beacon帧者宣告自身的存在。为了防范网络受到未经授权的访问，可以使用以下四种访问控制：

工作站身份验证

连接至无线局域网络的首要步骤是进行802.11工作站身份验证。工作站身份验证可以是“开放系统身份验证”，只进行简单的认证操作；或者是“共享密钥身份验证”，必须使用WEP密钥（细节见第九章）。有些产品提供MAC地址过滤功能，可以在身份验证阶段过滤掉未经授权的工作站的MAC地址。

关联

身份验证完成后，工作站会试图与接入点关联。通常，此过程并未使用任何安全防护，虽然可以在此步骤使用MAC地址过滤。

链路层

一旦无线工作站与接入点的虚拟网络“连接端口”建立关联，就可以使用基于802.1X的链路层安全协议。授权用户可以连接至经过许可的资源，未授权用户则会被踢出网络。无线网络易受窥视，因此必须选用具备坚固密码系统基础的身份验证协议。

网络层或传输层

IP网络在安全性方面有一段不幸的过去，许多较上层的安全性产品可以布设在网络的关键点。防火墙可以用来隔离不受信任的网络以及验证用户身份。至于VPN终端设备，则能够在不可信赖的网络中提供加密功能。

不同的身份验证协议适用于OSI协议栈的不同层次。起初，链路层安全机制十分脆弱，网管人员被迫使用较上层的安全协议。过去几年，投注在“无线局域网络安全性的工程与设计”上的努力主要侧重于坚固链路层安全机制。目前，在网络安全方面网管人员有几种选择。从最脆弱到最坚固排序，分别是：

WEP共享密钥身份验证

若使用共享密钥身份验证，打算访问网络的系统必须响应接入点的质询信息。共享密钥身份验证的构造十分糟糕，因此已被802.11i拒用（建议不要使用）。

MAC地址过滤

网络上各接入点均拥有一份允许网络访问的MAC地址列表。MAC地址很容易伪造与复制，但一些旧设备无法提供更好的机制。

WPA预共享密钥（WPA-PSK或WPAPersonal）

WPA主要新增了一种预共享密钥模式，允许工作站在只拥有“密码短语”(passphrase)的情况下进行身份验证。虽然它比上述两种方式坚固，但还有更坚固的做法。

802.1X协议

802.1X是设计来在准许用户访问网络前辨识与验证用户。因为它是以EAP为基础前辨识与验证用户，因此“802.1X”通常是指执行于EAP之上的扩展身份验证方式。有些软件称之为“WPA Enterprise”。

网络层身份验证

IP网络不具有安全性并非新鲜事。过去许多产品试图以各种方式解决身份验证的问题，一旦网络（IP）层建立后，就可以使用各种系统或协议。最适合无线网络的方法就是用来保护网络流量的VPN技术。

工作站身份验证与关联

工作站身份验证或关联阶段所能够提供的安全保护十分脆弱。连接初期能够使用的安全机制一点都不坚固。

一种早期的“安全性”功能即所谓的封闭式网络（*closed network*）（注2）。802.11问世之初，工作站必须设定接入点所使用的网络名称（SSID）。当时客户端软件还相当原始，关联之前，会先在空中搜寻具有特定网络名称的Beacon帧。封闭式网络有两个组件。接入点会依标准的规定传送Beacon帧，但不包含SSID信息元素。拿掉Beacon帧的SSID

注2：此功能有几种不同的称谓，包括隐藏式网络（cloaked network）、SSID广播抑制（SSID broadcast suppression）、私有网络名称（private network name）等。

可以稍微提高私密性，因为有些客户端软件不会显示出该网络。要与之关联，工作站必须送出包含SSID的Probe Request帧，因此它的作用类似于一把隐藏的“密钥”。使用隐藏SSID功能的接入点只接受“在Probe Request中指出遭隐藏的SSID”的工作站。不过由于Probe Request并未加密，只要观察联机成功的案例，就可以得知SSID为何并以此作为后续关联时之用。需要立即得知SSID的攻击者甚至可以让已授权工作站解除关联，强迫工作站在重新关联时传送必要的SSID。

MAC地址过滤是相当常见的做法，几乎所有产品均支持。接入点维护一份经过授权的MAC地址列表，不在列表上的工作站的关联请求就会被拒绝。过滤MAC地址只能算是聊胜于无，仍然还有不少改进的空间。和有线Ethernet网卡一样，802.11网卡也可以变更MAC地址，因此以MAC地址作为访问控制根本没有任何效果。只要使用封包捕获软件，攻击者即可监视成功的关联，轻易取得一堆允许关联的MAC地址。

使用MAC地址过滤功能经常导致一堆令人头痛的问题。维护这些地址列表就是管理上莫大的负担，特别是用户倾向于使用多部设备或者经常更换所使用的网卡。有些产品并不适合用于大规模的环境下，必须分别输入相同的信息。可以集中管理地址列表的有些产品需要使用TFTP，但在网络安全上，TFTP根本毫无立足之地。

第二种身份验证方式为WEP共享密钥身份验证。对打算访问网络的设备，接入点会送出一个质询信息。如第五章所述，共享密钥身份验证已遭破解，无法防范任何恶意访问网络的攻击者。就算对WEP密钥一无所知，也可以假造出合法的响应信息，通过WEP质询（不过除非还原出WEP密钥，否则无法传送帧）。

有些产品容许结合地址过滤与共享密钥身份验证。不过，两者都很容易被破解。除非无线工作站无法支持较坚固的协议或者无法升级，否则这两种多此一举的方式根本就不用考虑。这些只能使用原始身份验证机制的设备通常已经十分老旧。应用于后勤工作算是802.11技术的一项早期胜利，其所使用的手持式库存与追踪扫描仪的运算能力通常有限。有些并不支持WEP，有些甚至还在使用MS-DOS！

注意： 地址过滤与共享密钥身份验证是糟糕的安全机制，除非必要，例如设备无法提供更好的机制，否则不要使用。

链路层身份验证

相较于简单的过滤机制，链路层身份验证可说是一大进步，主要形式有802.1X与WPA。验证用户身份有几点好处。典型的链路层身份验证机制在进行身份验证时只容许有限的网络访问，只有在确定用户身份后才会准许完整的网络访问。在无线局域网络领域，能

够在网络连接阶段及早取得用户身份可让网络提供更精确的访问控制，因为可以对用户进行区分并在用户访问网络之前限制访问权限。对网络协议而言，链路层身份验证是通透的，可以配合任何网络协议使用。如今网络逐渐走向同质化，而且大多以IP为基础，虽然有些旧协议仍然使用IPX之类的封包。链路层身份验证协议可用来保护IP与IPX网络。有时候，链路层身份验证的速度也比较快，因为可以在网络接口启动时立即运行。因此，与其使用为广域网络设计的协议，倒不如使用在链路建立时即可启动的链路层身份验证。

WPA Personal（预共享密钥）

WPA有两种模式。比较简单的模式就是传递预共享密钥（WPA-PSK）给所有无线工作站。无线链路所使用的密钥是根据预共享密钥交换的随机数衍生而来。和其他使用预共享密钥的协议一样，WPA也无法抵抗固执的攻击者发起的字典式攻击。基本上，WPAPSK只能当作一种快捷方式。WPA-PSK是以密码短语（passphrase）与SSID衍生出所需要的预共享密钥，而不是根据运算密集的TLS信息交换过程来产生密钥（注3）。

大多数情况下，各SSID中的所有工作站仅会使用单一预共享密钥。在此种网络中，所有工作站共享相同的密钥。使用预共享密钥，攻击者即可监视第七章所提到的四次握手过程，推衍出其他工作站所使用的独立密钥。攻击者也可以伪造信息来强迫其他工作站重新进行身份验证，以便捕捉完整的四次握手过程。

WPA-PSK的安全性绝大部分取决于密码短语（passphrase）的质量。802.11i的附录H提到密码短语的质量并注明密码短语中每个字符通常相当于2.5个位的安全性。密码短语太短会很容易遭受字典式攻击。

防止使用脆弱的密码短语的最佳方式，就是使用二进制预密钥共享模式，然后键入256个位的预共享密钥，或者使用较坚固的密码短语（并非所有产品都允许直接输入预共享密钥）。密码短语最好使用20个以上的字符并且避免使用常见与易遭字典式攻击破解的词汇。有关密码短语的进一步建议以及密码短语质量的讨论详见Passphrase FAQ（注4）。

对没有什么重要数据的小型网络而言，可以使用WPA的预共享密钥模式。安全性基本上就是风险管理，有些网络只需要用到WPA PSK，因为其中并没有什么重要数据。

注3：有一种称为coWPAtty的攻击工具程序可自*http://remote-exploit.org*下载。

注4：Passphrase FAQ可自*http://www.stack.nl/~galactus/remailers/passphrase-faq.html*下载。尽管它是为PGP而写的，但是其中有许多建议也适用于passphrase技术，包括WPA-PSK。

注意： WPA预共享密钥最好只用在小型、风险较低，或者供访客使用、不需要极力防护的网络中；否则，应该改用下列身份验证协议之一。

802.1X EAP 身份验证

802.1X是一种可扩展的架构，其本身并不是一种协议。但有一堆协议可供网管人员挑选，这些协议各有其优缺点。要从中挑选出一组候选方案，得先考虑无线网络的实际需求。由于通过空气传输，无线网络原本就易遭窥视，因此必须采用坚固的加密方式来保护用户数据。除了只传送加密过的用户数据，比较好的做法是提供相互认证。用户必须加以验证自不待言，而在缺乏物理连接的情况下，必须使用加密操作以确保用户是连接到合法、经过核准的无线局域网络。随机产生的密钥比静态密钥安全，尤其是如果定期更新动态密钥的话。符合这些实际需求的协议有三种，不过通常会将第四种协议纳入考虑。

Cisco的“轻量级EAP”（Lightweight EAP，简称LEAP）是比较旧的协议，在标准问世之前，它是Cisco设计来解决无线局域网络的安全性瑕疵的。值得注意的是，它是最早为个别用户提供动态衍生密钥的协议，不过它的设计无法符合其他实际需求。LEAP使用MS-CHAP v1对用户数据进行扰频。虽然MS-CHAP v1并不是以明文来传送用户数据，不过它基本上已遭破解，无法提供真正的保护（注5）（许多嵌入式设备仍然使用MS-CHAP v1，因为它不需要用到太多的CPU资源）。此外，LEAP也提供相互认证，不过只用到两次MS-CHAP交换（每个方向一次）。最后，LEAP是Cisco的专属协议。虽然有其他选项可以代替，但客户端必须使用其他额外的软件或者Cisco网卡，而认证者方面必须使用Cisco接入点。我曾共事的机构大多试图放弃LEAP，因为它是Cisco的专属协议。客户端系统必须使用LEAP软件，它可由Cisco驱动程序提供或者使用其他厂商所开发的客户端软件。经常见到广泛使用LEAP的机构另外购买Cisco网卡来插在已经内置无线网卡的便携式设备上。由于LEAP有弱点，因此才有EAP-FAST协议的开发。撰写本书之际，EAP-FAST尚未得到广泛使用。

而三种被广泛考虑的标准是EAP-TLS（EAP-Transport Layer Security）、PEAP（Protected EAP）以及TTLS（Tunneled Transport Layer Security）。三者均使用TLS对用户身份数据提供坚固的加密防护，并且使用TLS密钥交换过程提供链路层密钥所需要的种子。此外，三者均提供相互认证功能。它们均能与身份验证服务器建立TLS隧道，使用服务器所提供的证书，作为“网络至用户”（network-to-user）的相互认证基础。

注5： 详见 *http://asleap.sourceforge.net/*，一种用来还原LEAP密码的工具。它的做法是强迫用户进行身份验证，然后对密码散列值进行暴力破解。

相互认证时EAP-TLS均使用证书。要建立TLS隧道，网络方面得先提供证书给用户，让用户验证网络的真实性。验证完服务器的证书后，客户端系统就会将用户证书传送给认证服务器进行类似的验证。EAP-TLS相当坚固、安全且易于理解，但并非毫无弱点。客户端认证是通过用户证书，需要存在PKI来产生、签署与传递证书。如果证书系统尚未建立，就不适合使用EAP-TLS了。

其余两种协议（PEAP与TTLS）十分类似。两者均以TLS隧道传递服务器证书，提供第一阶段的“网络至用户”的身份验证，并且使用TLS隧道为第二阶段的“用户至网络”的身份验证所使用的用户身份数据加密。PEAP与TTLS并未完全依赖证书，但无线网络上的认证者都必须拥有证书。选用PEAP还是TTLS，不只是要考虑何种协议适合你的需求。TTLS较具灵活性，除了在隧道中传送“用户至网络”的身份验证数据，几乎可以配合各种类型的第二阶段身份验证机制。PEAP的限制较多，因为它要求必须使用EAP method来进行第二阶段身份验证。实际上，最常见的PEAP supplicant就是Windows XP/2000内置的申请者软件，且只支持一种不需要使用证书的第二阶段协议MS-CHAP版本2。对拥有众多Windows工作站的网络而言PEAP是不错的选择，因为它不需要额外的授权或者安装额外的软件。

注意：应尽量避免使用LEAP，因为它是专属协议，防护也相对较弱。尽可能使用基于TLS的身份验证协议，因为此类协议具备相互认证与密钥分配的功能。

EAP-TLS、PEAP与TTLS这三种协议均以TLS为基础。EAP-TLS要求以客户端证书进行身份验证，但除非拥有PKI，否则无法使用。PEAP与TTLS类似，两者都是不错的选择。前者在只使用Windows的环境中比较有用，后者在使用旧式身份验证系统的环境中比较有用。

网络层身份验证

许多早期的无线网络是跟有线基础设施分隔开的，并且使用现有的身份验证与访问控制机制。举例来说，在前一章中，图21-2所提到的单一子网络拓扑有一个理所当然的瓶颈(choke point)。防火墙通常部署在瓶颈所在处，提供某种程度的访问控制功能。如果此瓶颈设备也具备VPN功能，那么除了加密帧，也可以使用VPN软件来进行身份验证。

防火墙可以提供较严格的认证机制，也的确能够与RSA SecurID之类的单次密码系统整合使用。新型的IPsecVPN设备已逐渐集成了类似的功能，虽然必须使用扩展式身份验证（eXtended Authentication，简称XAUTH）、混合式IKE（Hybrid Mode IKE）或者用于认证控制密钥的质询/响应（Challenge/Reponse for Authenticated Control Keys，简称CRACK）等扩展功能。XAUTH十分普及，但受制于本章所提到的“复合绑定”

(compound binding) 问题。高度安全的网络或许希望能够以协议扩展功能来避免这些问题，以IPsec配合用户证书作为身份验证机制。VPN设备也可以是SSLVPN设备，不见得是IPsec终端机。除了客户端软件，采用SSL的VPN设备实际上比较容易使用，因为它们只需要用到Web浏览器。

有些机构选择使用Web式身份验证系统，而不是采用全功能（且昂贵）的防火墙，无线网络本身采用最低限度的身份验证与加密机制，不对访问做特别的限制。有些网络使用802.11的开放系统身份验证，而且未使用加密（一些较有安全意识的网络已经开始为Web式身份验证系统加上WPA-PSK功能，但这是比较新的做法）。代理机制负责接收来自网页的请求，然后导向安全的登录页面。认证完成之前，Web系统会将来自客户端的封包加以丢弃。一旦认证成功，便允许客户端系统的封包进出。必须注意的是，有些Web式身份验证系统的确对登录程序进行加密处理，但并未提供坚固的链路层加密。

当无线局域网络首度成为重要议题，有些厂商开始销售所谓的“无线访问控制器”(wireless access controller) 设备，其中通常包含封包过滤、“身份验证、授权与计费”(authentication,authorization,and accounting，简称AAA）服务以及DHCP服务器，有些设备甚至包含DNS服务器与VPN终端机以及封包整形（packet shaping）或带宽限制(rate limiting)。AAA功能通常由与现有企业基础架构（如RADIUS）相连的接口所提供，这些架构通常已经做好设定，可供远距离访问之用。有些产品还包含动态DNS，如此一来就可以为个别用户提供动态的网域名称以及通过DHCP提供IP地址。

以RADIUS整合用户身份验证

RADIUS通常被拿来作为身份验证的后端，不论身份验证是在协议堆栈的哪个层次进行。无线设备与VPN均采用外部的RADIUS服务器。大多数机构都会有一个用户账号系统，比较常见的做法是将RADIUS服务器摆在账号系统之前，以便对其他的网络设备进行访问控制。RADIUS服务器也可以用来整合不同的用户账号系统，以便形成单一的用户数据库。

虽然RADIUS服务器能够定义本地用户（local user），但其所提供的用户管理工具通常十分简单。大多数RADIUS服务器在部署时会参照其他用户账号数据来源，扮演协议翻译的角色。一些常见的外部用户数据库包括：

Windows 域

大多数机构多少都有一些使用Windows域或ActiveDirectory的用户。将RADIUS服务器与Windows密码整合在一起对用户而言十分简便，因为Windows密码通常就是主要的用户身份证明。一般用户通常厌恶记忆密码。通过Windows域可以让

用户使用相同的身份进行不同的操作。从大学院校到大型的多国企业网络，Windows受欢迎的程度不同，有些机构只用Windows网络技术。

一般令牌卡（如RSA SecurID、Secure Computing SafeWord）

一般令牌卡通常会使用RADIUS前端，有些RADIUS服务器也可以将身份证明数据（证书）直接传给令牌卡服务器进行审核。如果整合令牌卡服务器，管理人员便可在无线网络中使用较坚固的令牌身份验证。

LDAP目录

目录服务具有相当大的扩展性，希望集中管理用户数据的机构通常给予高度的评价。密码、访问权限、策略以及联络信息都可以存储在同一个目录之下。访问LDAP目录时，RADIUS服务器可以根据LDAP所提供的数据进行认证。举例而言，大学用户不外乎教职员工与学生，学生的网络访问权限就有所限制。

Kerberos领域

有些大学也大举投资Kerberos身份验证。RADIUS会从一般用户处取得身份证明数据，然后以之取得Kerberos通行证（ticket）。如果认证成功，就允许进行访问。目前，Kerberos的整合操作都还很松散。核发给用户的只是假的通行证，并未真正用于身份验证，不过有些大学希望将现有的Kerberos架构应用到新的无线网络。预料未来将会出现一些新的协议使用Kerberos通行证数据来进行身份验证。

Unix密码系统

Unix密码系统包含Pluggable Authentication Modules（可插入的身份验证模块，简称PAM）以及Network Information System（网络信息系统，简称NIS）。大举投资于Unix的机构可以利用现成的身份验证系统来产生单点登录（single-sign-on）。使用这些认证机制的RADIUS服务器安装于Unix系统并通过系统调用来验证用户身份。

RADIUS代理服务器

RADIUS服务器可将认证请求传给其他RADIUS服务器。在分布式环境中，例如大型研究机构，想要建立集中式用户数据库根本不可能。最好的解决方案是接受用户账号原本就是分散的事实，确保RADIUS服务器能够将身份验证请求转交其他RADIUS服务器进行处理。

TACACS

TACACS是另外一种访问控制服务。它广泛使用于网络设备，主要是用来存储网管人员的账号，很少用来存储一般用户的账号数据。

RADIUS身份验证与Microsoft Windows数据库

查询Windows用户账号的方式有两种。操作系统API调用可用来查询位于域控制器

(domain controller)的用户数据。服务器间所使用的网络协议也可以用来查询用户数据。在旧式的以Windows NT4为基础的网络中，域控制器使用了一种服务器间(inter-server)协议，目前这种协议已经被开放源码社群用逆向工程解析了出来。外部的RADIUS服务器可以运行伪装成域控制器的软件，通过网络查询Windows账号数据。事实上，大多数Unix系统上的RADIUS服务器均可借助逆向工程所得出的数据来验证NT域的用户。Windows RADIUS服务器必须安装于用来查询用户数据的域控制器。

以Windows 2000为主体的网络大多使用Active Directory。除了原本的功能外，Active Directory也导入了新的服务器间协议，不过这些都是Microsoft的专属协议。Microsoft的RADIUS服务器被称为Internet Authentication Server（IAS），可以使用Active Directory来查询存储于其他成员服务器（member server）上的用户数据。这些协议尚无人对之进行逆向工程，因此无法用于第三方的RADIUS服务器，必须通过域控制器的系统调用API，方能取得用户信息。访问用户身份证明的请求一旦通过API传给域控制器，域控制器就会使用Active Directory协议来远程查询用户数据（注6）。

安装Active Directory时可以选择原生（native）或者兼容（compatibility）模式。在原生模式中，成员服务器仅使用较新的Active Directory协议；在兼容模式里，可以使用较旧、较不安全的NT Domain协议。目前，大多数的Active Directory均采用原生模式，并未启用兼容选项。

因此，网管人员遂面临一种抉择：到底应该采用Microsoft RADIUS服务器，或者在域控制器上安装第三方的RADIUS服务器，还是采用兼容模式的Active Directory。最后一个选项牵涉到安全问题，通常也无法作用，因为它同时限制了Active Directory的功能。如果需要通过Active Directory来验证用户身份，要不就是采用Microsoft的IAS，要不就是在域控制器上安装第三方的RADIUS服务器（应该注意的是，并非所有第三方的RADIUS服务器均支持Windows，例如大多数第三方的RADIUS程序并无法在Windows上运行）。对许多机构而言，这两种选择都是莫大的挑战，因为通常必须大幅修改由域控制器所构成的大型网络的控制流程。

警告： 大多数RADIUS服务器软件均无法访问Windows用户身份证明数据，除非安装在域控制器上。如果需要验证Windows用户账号，最好安装一部域控制器。

注6：只能间接查询用户身份证明，而且必须安装于域控制器，对Microsoft RADIUS服务器来说这反而是一种优势，因为它原本就是与Windows服务器操作系统配合使用的。第三方所开发的RADIUS服务器则必须另外安装于域控制器。相较于便宜的Microsoft RADIUS服务器，网管人员必须衡量购置第三方的RADIUS服务器是否值得。

以加密确保私密性

用户身份确定无误并赋予其访问权限后，网络必须保护用户所传送的数据不被窥视。无线局域网络能够使用的加密协议如下：

静态 WEP

静态 WEP 使用单一密钥来保护客户端与接接入点间的数据传输。在多数实现中，所有工作站通常会共享一个密钥，因此大幅降低了使用上的安全性。

802.1X 动态 WEP

2001 年底，传统上使用单一密钥的静态 WEP 的瑕疵已经不容忽视。幸运的是，当时 802.1X 规范说明书刚好从标准委员会出炉，它为我们提供了动态传递密钥的方式。定期更新 WEP 密钥可以有效防范许多针对静态密钥的攻击。

临时密钥完整性协议（TKIP）

TKIP 属于 802.11i 的一部分，设计来提供更高的安全性，但无线接口的硬件必须支持 RC4 加密功能。为了确保帧的完整性，TKIP 配合 Michael 完整性校验来侦测帧在传送过程中是否遭到篡改。TKIP 与 Michael 只是用来包扎 WEP 伤口的绷带。它们的确比较安全，但有多安全就很难说了。

CBC-MAC 计数模式协议（CCMP）

CCMP 是 802.11i 的第二个主要部分。CCPM 采用新的加密操作方式，将加密与完整性校验操作结合为单一协议，而非分别使用不同的协议。它与过去链路层所使用的 RC4 安全协议完全决裂。如今芯片组已经集成了 AES 硬件加密功能，AES 是 CCMP 使用的密码。

网络层加密协议

除了在链路层保护无线网络，也可以使用历经考验的网络层加密协议，比如IPsec、SSL 或 SSH。

静态 WEP

静态 WEP 是相当可怕的安全协议，除了聊胜于无外就没什么好说的了。除非无法使用其他方法加密数据，否则最好不要使用静态 WEP。对大多数设备而言，静态 WEP 可说已遭淘汰。只要操作系统支持并且安装了最新的驱动程序，几乎所有网卡均已支持 802.1X 链路层安全机制。唯一考虑使用静态 WEP 的场合只有在特定的应用设备无法支持更好的机制时。

各位手上或许留有一些老旧的设备，由于处理能力有限或者升级代价太高，只能够支持静态 WEP。用来清点库存的 802.11 手持设备与 IP 电话机即属此类。如果别无选择，最

好先检查最明显的安全漏洞。弱IV是静态WEP工具的最大漏洞。当Airsnort经媒体披露，许多厂商随即更新软件以避免使用弱IV。虽然新版软件无法彻底解决WEP的基本瑕疵至少可以大幅降低风险。部署之前，最好确定所使用的静态WEP是否会产生弱IV。如果答案是肯定的，可要求厂商提供补丁程序。如果无法防范此种攻击却又继续供货，只能称之为黑心厂商。

静态WEP聊胜于无，比起丝毫不设防，它至少提供了某种程度的保护。它可以防止无心的用户意外连接到隔壁邻居的网络。不过，静态WEP并无法防范有心攻击的人士。如果非得使用静态WEP，最好确定能否承受WEP网络被攻陷的后果，并确定攻击者无法以此作为攻击发起点来进一步瘫痪整个网络。

注意： 静态WEP是逼不得已才会使用的加密协议。除非别无选择，否则不要使用，同时做好适当的防范措施以免暴露太多弱点。

802.1X 动态 WEP 钥

虽然802.1X是设计来作为身份验证之用，它对WEP的改良也同等重要。802.1X所包含的信息可用来将密钥从接入点传递给工作站。动态产生密钥有助于解决WEP的瑕疵，虽然它并不是完整的解决方案。

动态产生密钥有一项重要的前提。密钥必须近乎随机，亦即必须有来源提供密钥材料（*keying material*）或者密钥随机位（*entropy*）。密钥材料可以来自身份验证方式，例如以TLS为基础的身份验证方式，也可以直接输入预共享密钥。经过一系列操作，所使用的协议就会将密钥材料从一连串的随机位转换成链路层加密密钥。

注意： 链路层的动态密钥必须从主秘钥（master secret）衍生而来。主秘钥可以由用户直接提供，也可以来自身份验证过程。

从系统管理人员的观点来看，最重要的是可以动态地为无线链路产生密钥。网管人员不必凭空杜撰WEP密钥或者负责将密钥传送给用户与网络设备。用户认证过程会产生一堆在密码学上被认定为安全的随机数据来衍生出WEP密钥。工作站仍然使用WEP加密来保护帧，但用来加密帧的密钥是用户所独有且定期更新的。网管人员可以设定密钥的更新时间。用户的密钥是在身份验证过程中产生且定期更换，而非一直使用同一个密钥直到所有设备同时更换它。

密钥生成消息可用来传递用户密钥（映射密钥或单播密钥）以及广播密钥（组或默认密钥）。任何工作站只要离开网络或者经过一段时间，就会立即更新默认密钥。

工作站关联期间，初始向量（IV）会不断循环使用。不过，IV的问题来自于重复使用带有相同密钥的IV。只要将密钥产生定时器的时间调短，就可以避免重复使用相同的“IV+密钥”组合。以24位的IV而言，约有1600万种（2^{24}）不同的IV。与802.11帧速率相比较，就可以计算出最大密钥长度。分析802.11帧速率时，我会把流量负载视为一连串的“交易”，每次交易包含一个TCP segment与相应的TCP ACK（注7）。每次交易消耗两个IV。以1600万来计算，可以计算出耗尽IV空间需要多少时间。表22-1列出了以不同负载系数（load factor）计算出的结果。在许多方面，此表显示出密钥的存活时间相当短。为了安全起见，密钥的使用时间通常设为半小时，如此可以更有效地防范重复使用IV。

表22-1：IV空间的存活时间

	802.11b	802.11a/g，未使用保护机制
每秒交易次数	479	2334
每秒使用IV数	958	4668
IV空间耗尽时间，以小时为单位		
100%负载	4.8小时	1.0小时
75%负载	6.5小时	1.3小时
50%负载	9.7小时	2.0小时
25%负载	19.5小时	2.4小时

最早出现的WEP攻击工具是根据Fluhrer-Mantin-Shamir理论来攻击。*airsnort*与*wepcrack*均先搜集弱IV，还原密钥需要数百万个帧。近来出现的工具结合了Fluhrer-Mantin-Shamir与其他类型的攻击可以更快还原出密钥，所需搜集的帧甚至少于百万个。其中，*aircrack*（注8）是最值得注意的工具。

注7：详见《When Is 54 Not Equal to 54? An Analysis of the Maximum TCP Throughput of 802.11a,b, and g》（*http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html*）一文的分析。必须注意的是，本文假设TCPsegment与ACK信息的比例为1:1，比其他具备更佳TCPsegment/ACK比的模型消耗更多的IV。不过，出于安全性的考虑，以不符实际的压力测试模型来估算安全限制仍有其用处。

注8：可自*http://www.cr0.net:8040/code/network/aircrack/*下载。

WEP仍然无法抵挡帧完整性校验攻击，这和WEP架构有关。事实上，改善完整性校验乃是802.11i的主要任务之一。值得庆幸的是，目前尚未出现针对完整性校验的攻击工具。

注意： 动态WEP充其量只是过渡时期的解决方案，除非设备不支持TKIP，否则不应使用。使用动态WEP时切记将密钥使用时间调短，以防范WEP分析工具的攻击。我建议时间不要长于15分钟。

改良型RC4加密：TKIP

动态WEP是没有更好选择时才用的“创口贴”（Band-Aid），或者作为一种考虑更好替代方案时，在合理的安全范围内部署链路层身份验证架构的方式。802.11i包含了两种新的链路层安全机制。临时密钥完整性协议（Temporal Key Integrity Protocol，简称TKIP）是设计来解决针对WEP的攻击以及维持与现有硬件的向下兼容性。TKIP比WEP安全，但尚未经历完整性的考验。

TKIP的设计目的是在尽可能提供安全性的同时维持向下兼容性。第一波802.11芯片通常是以软件提供安全性，如果有的话。为了解决软件加密所造成的性能问题，第二波芯片开始采用硬件加密，包括RC4加密。TKIP是设计来配合WEP帧的处理操作以及解决WEP所有的一些弱点。

TKIP保留了RC4帧加密并更新了现有的802.11系统。和动态WEP一样，TKIP依赖特定来源提供随机数据作为密钥产生的基础，因此必须配合WPA-PSK或其他802.1X EAP method一起使用。除了基本类似之处，它也为个别帧产生独特的密钥，以中止针对初始向量的攻击，并在遭受重放攻击时暂时停止传送帧。TKIP同时改善了完整性校验机制，确保帧的传送者拥有适当的加密密钥并且使用经过改良的完整性校验。

在大多数硬件中，TKIP与动态WEP可以共存。大多数接入点可以为每个工作站暂存特有的链路层密钥。如果一个工作站使用动态密钥，另一个使用TKIP，就会反映在密钥的存储上。同时使用这两种加密协议的确会降低广播帧的安全性，因为位于相同网络的所有工作站必须共享相同的广播密钥。

注意： 对大多数的部署而言，应该将TKIP视为起码的标准，除非系统不支持。然而，不应该将TKIP视为长期的解决方案。

CCMP：AES 加密

TKIP受制于WEP留下的包袱。802.11i的“CBC-MAC计数模式协议”(Counter Modewith CBC-MAC Protocol，简称CCMP）是全新的设计，一开始就将安全性考虑在内。它的设计目标是提供能够与现有可信赖协议（如IPsec）匹敌的安全性，但没有IPsec加诸无线局域网络的限制。CCMP的设计始于AES密码（cipher），它是大多数新式安全协议的基础。WEP的老旧使得TKIP无法成为合格的安全协议，但CCMP的底层结构已经被美国政府核准，适用于敏感的应用场合。

除了以AES来提升性能，CCMP也针对现有的加密协议进行改良。传统的加密协议可用于加密，以保护行经不可信赖路径的数据或者用于真实性校验，从而确保数据在传输过程未遭篡改。WEP只提供加密功能并且依赖一种有瑕疵的完整性校验算法。TKIP以两种不同方式使用密钥。和WEP一样，密钥被用来加密帧，额外的密钥则用来提供完整性校验算法。而CCMP允许以单一密钥来达成这两种目的，如此可以减轻计算上的负担以及提升性能。

CCMP的主要缺点是客户端软件的实现通常很没有效率。虽然CCMP没有理由不能与使用RC4的加密协议共存，但是大部分的驱动程序并不支持这种做法。CCMP与使用RC4的加密协议并用时，驱动程序必须支持使用CCMP来传递单播帧，以及使用基于RC4的加密协议来传送广播帧。我尚未见过任何厂商支持此种操作模式。使用CCMP的缺点是：由于必须同时支持两种网络，配置设定会变得更加复杂，此外，各位可能必须换掉目前所使用的无线网卡。

注意：长期而言，CCMP是相当吸引人的链路层安全协议，不过由于产品本身的限制，可能必须同时维护好几个无线网络以及进行设备的叉式升级（forklift upgrade）。

较上层的安全协议（IPsec、SSL与SSH）

当无线协议首度被认定存在基本瑕疵时，各方都想要尽快找出解决方案。网络设计人员开始转向业经证明的加密协议以加密流经空中的数据。其中，IPsec是最主要的受惠者，虽然SSL与SSH也经常出现在考虑名单上。以上这些协议均提供识别用户、加密数据以及确保封包在传输过程中未遭篡改的机制。

使用较上层安全协议的缺点是只能对内容提供保护。网络层安全协议可以为网络层以及网络层以上的协议提供安全服务，但无法保护底层协议。安全管理人员通常担心VPN工作站遭到“反转”（turnaround）攻击，亦即攻击者使用现成的隧道访问受保护的网络。

为了解决潜在的漏洞，必须使用标准的主机防护以及个人防火墙与杀毒软件。目前市面上有多种个人防火墙，便宜的必须个别安装，而较贵的功能较多，比较牢靠，也可以集中管理。针对VPN工作站的攻击的确堪虑，因此有些VPN厂商会在安装包中附增个人防火墙软件。

警告：实现于链路层之上的安全协议无法为链路层提供有效的保护。因此，较上层的安全协议必须以额外的主机安全协议加以辅助，例如个人防火墙软件。

实现于较上层协议之上也比较容易支配网络架构。VPN端点通常使用固定的IP地址，且大多数VPN客户端软件并无法应付IP地址改变的情况。虽然802.11支持漫游至不同的网络，但网络可能分别位于不同的IP子网络。一旦IP地址改变，就必须重新建立VPN连接。更重要的是，用户必须接受“只要地址改变，就必须重新建立连接”的情况。

要尽量延长连接时间，网络设计人员必须使工作站跨越网络时保持连接状态。这可以借助链路层识别管理工具完成，可以使用前一章介绍的动态VLAN架构所提到的802.1X协议在接入点间进行切换操作，或者使用前一章介绍的单一子网络架构来针对切换限制设计网络。对网络管理人员而言，前者在配置设定上比较复杂，但在构建上可能比较容易。因为它不需要额外的骨干工程。

许多VPN技术皆是针对点对点加密所做的设计。组播应用可以通过IP，但IPsec并未包含任何方式可以传递组密钥，因此无法支持多对一的传送。在点对点链路分配密钥算是一个“简单”的问题，因为进行对话的只有两方（所谓“简单”，是指问题并非无法处理而且存在解决方案，并不是指很容易就可以达成）。为“单点对多点”连接生成密钥是一个“困难”的问题，因为单一传送者与多个接收者之间必须同意使用一组密钥，而且当接收者加入或离开此组播连接时必须能够更新密钥。组播数据本质上适用于一些场合，最值得注意的是流媒体（streaming media）。大公司可以通过内部的组播会谈（multicast session）召开内部会议，并确保组播数据以无线网络传送时经过加密。组播数据也广泛应用于金融市场，因为它相当适合用来传递市场数据。IPsec组播标准仍在由标准委员会制定中，目前尚未完成。

IPsec得到广泛使用是因为它实现于网络层，因此与使用何种应用程序无关。只要应用程序能够适应IPsec封装与加密所造成的迟延，就可以正常运作。在最常见的IPsec架构中，使用新的程序或新增一部服务器并不需要做任何变动。IPsec被广泛用于远程访问，这意味着网络上通常存在一部可以提供加密的IPsec终端设备。许多移动设备早已安装与设定好客户端程序，用户经过训练后会逐渐习以为常。如果有现成的VPN集线器（concentrator）与闲置的带宽，就可以让现有的IPsec远程访问扩展至内部的无线局域网络。

赋予现有VPN集线器新的任务可能会造成性能问题，特别是如果VPN设备原本是作为远程访问之用。相较于局域网络用户，远程访问用户并不需要很宽的带宽。在定义上，远程访问性能受限于上行链路速度。既然许多机构仍然使用T-1线路或相当于SDSL的连接速度，远程访问连接速度就只有2 Mbps。将VPN扩展至无线局域网络，需要对VPN集线器进行升级或者使用内置IPsec终端机的无线局域网络系统。IPsec也可能导致性能问题。加上IPsec标头，最大尺寸的IP封包将被分割为两个封包片段。其中一个封包将包含标头信息，其封包大小仍然相当于最大尺寸，但被IPsec标头挤到第二个封包的数据将形成小封包片段。在重组与解密封包之前，必须完成两个片段的接收。

虽然网管人员能够控制IPsec解决方案的头端，但无法控制客户端。不论部署规模的大小，安装与设定这些客户端软件都是莫大的挑战。确切地说是，如果有客户端软件可用的话。IPsec客户端软件是在各平台间取“最小公分母”，因此有些解决方案只支持Windows。支持Mac OS与Linux的IPsec软件少得可怜，绝大部分是因为VPN集线器的缘故。X厂商的终端设备需要配合X厂商的客户端软件，才有办法让远程访问更加方便。少数厂商会为自已的终端设备提供Mac OS平台的客户端软件，但Linux的客户端软件就很少见了（FreeS/WAN虽然实现了IPsec，但并不支持部署所需要的特殊客户端功能）。

客户端软件的负担并不会因为使用IPsec而减轻。IPsec可以在网络层阻挡各式各样的攻击，但无力保护链路层的数据。举例而言，IPsec并无法阻止ARP欺骗或ARP毒药攻击，因为它并不会加密或验证ARP帧。IPsec也无法防范一些网络层攻击。因为IPsec要求客户端必须取得IP地址，许多用IPsec防护的无线局域网络遂允许任何系统连接至网络并且通过DHCP取得IP地址。取得立足点后，攻击者就可以对网络基础设施发起IP拒绝服务攻击。个人防火墙可以防范链路层攻击，但又得安装、设定与管理额外的客户端软件。近年来个人防火墙已有长足的进步，有些优秀的解决方案甚至允许进行集中设定与管理。

IPsec用户身份验证也会导致严重的安全风险。site-to-site（站点对站点）VPN使用双方均了解的对等（peer）系统并且位于固定位置上。在取代专线的情况下，一些位于已知位置的系统可能会核发证书，采用坚固的身份验证方式。不过，远程访问完全是另外一回事。IPsec并不是专为用户身份验证而设计的。虽然可以采用数字证书，但通常因为会造成管理上的梦魇而被拒绝。不少规范说明书以IPsec进行旧式的身份验证，但所有方案均不完整。其所使用的主要协议XAUTH（eXtended Authentication）虽然得到广泛使用，但并未完全标准化。XAUTH要求在IPsec握手之初即表明身份，同时必须以安全性递减的“积极”（aggressive）模式来运作。握手与最后用来传递用户身份证明的隧道的安全性取决于使用的共享秘钥。一些XAUTH实现允许（甚至要求）所有用户使用相同的共享秘钥。此外，XAUTH的设计也十分差劲，同样受制于之前所提到的“复合绑

定”（compound binding）问题（一些通过认证的Ipsce产品可以启用FIPS模式来停用XAUTH）。遗憾的是，许多厂商仍旧继续使用XAUTH，因为它广泛实现于许多OEM的客户端程序。XAUTH的主要替代方案是“混合模式”（Hybrid Mode）。混合模式的设计显然较好，但并未得到广泛使用。

IPsec的替代方案是只允许使用内置的有坚固加密系统的应用程序。基于Web的系统可以通过SSL（secure socket layer）加以保护。主机登录可以通过SSH加以保护。SSH也可以用来保护多种TCP网络连接，虽然连接端口转送（port-forwarding）的配置对一般用户而言可能过于复杂。有些环境或许已经部署了Kerberos之类的架构来提供应用层的安全性，在这种情况下，要扩展至无线工作站并不是什么难事。

安全协议的选择

选择安全协议时，首先必须决定你打算保护网络堆栈的哪一层：链路层、网络层、传输层、应用层，还是各层的某种组合？基于802.1X的链路层安全防护与VPN分属不同层次，两者并不互斥。究竟是选择第2层、第3层的安全性还是两者全选，取决于你的目的与需求。两者均提供加密以防范信息遭人窥视，也均提供用户身份验证。在身份验证完成之前，802.1X会拒绝网络的访问以防范可能遭受的攻击，它所使用的身份验证机制也优于IPsec的远程访问身份验证方式。802.1X搭配改良后的Layer 2加密最符合许多机构的安全需求。简单地讲，IPsec隧道的安全性高于WEP“会话”（session），即使WEP会话使用了802.1X防护并且经常更新密钥。

协议堆栈的安全防护

自本书第一版发行以来，802.11的最大改变就是出现了合理的安全性架构。首先以及最重要的是，安全性协议必须维护网络的安全。在无线局域网络中，安全性几乎可说是身份验证与加密的函数。

“复合绑定”漏洞

大多数传统的身份验证方式并不安全。随着时间的累积，身份验证协议日渐能够抵挡外来的攻击，但广泛部署的旧方法仍将使用多年。为了保护这些旧式身份验证协议的安全，常见的做法是提供某种形式的加密信道，在不安全的网络中保护以往不安全的认证方式。TLS（Transport Layer Security）与IPsec（IP Security）这类坚固的点对点隧道技术的发展为保护旧式身份验证协议提供了诱人的方法。使用安全隧道（secure tunnel）来保护较弱的旧式认证方式被称为“复合式身份验证”（compound authentication），因为身份验证过程被区分为两个步骤，首先是建立一个安全的信道，然后是进行用户身份验证。

最值得注意的复合式身份验证，就是无线网络所使用的TLS点对点隧道方式（TTLS与PEAP）以及IPsec常用的XAUTH（eXtended Authentication）。设计安全协议相当不简单，比较简单与安全的做法是使用广泛部署与历经考验的协议，例如TLS或IPsec，来提供必要的加密组件。

不过，在2000年10月经研究发现，大多数复合认证方式的共通设计不足以防范特定类型的“中间人”（man-in-the-middle，简称MITM）攻击。问题出在隧道“内层”认证方式并未与“外层”防护隧道强力结合或“绑定”（bound to）在一起。在隧道内交换敏感的“内层”认证数据之前，这些协议并未校验身份验证是否针对“外层”隧道的双方。之所以会产生复合绑定问题，并不是因为隧道内的协议或内层认证方式，而是因为两者的结合方式。内层的身份验证协议必须证明内层隧道的端点和外层隧道的端点是一致的（注9）。

理论上，目前复合绑定所产生的漏洞颇大。不过要成功利用这些漏洞，攻击者必须主动参与。MITM攻击要能成功，攻击者必须在目标网络上装设无线设备，与合法的认证者完成第一阶段的身份验证，然后针对打算窃取其身份的客户端发动攻击。成功的攻击必须实际访问网络与设备，同时主动传送数个封包。

XAUTH的标准化已经不再继续进行，也不会有后续的补丁来解决复合绑定的漏洞。要解决IPsec的复合绑定问题，可以在所有客户端使用数字证书。无线局域网络协议尚未完成，将会继续修改以解决复合绑定的瑕疵。

加密

相较于任何使用RC4的帧加密方式，IPsec会话或许能够提供更坚固的加密能力。考虑到此标准及其实现已经问世一段时间，IPsec的确相当值得信赖，特别是配合静态地址与数字证书使用时。要说它有什么弱点，大概就是网络层协议无法为MAC层提供安全防护。在受到IPsec保护的无线网络中，攻击者可以轻易取得IP地址并对其他用户或VPN组件发动拒绝服务攻击，因为在启用网络协议之前并不需要经过身份验证。

安全性认证

有时候，产品必须通过安全性认证（security certification），这因所处的环境而异。通常，政府网络必须使用经过评定的产品。在美国，此过程是根据FIPS（联邦信息处理标准）140-2进行的；一些政府机构联合起来，以世界级的Common Criteria（通用标准）

注9：IPsec的Quick Mode（第二阶段）是以signature（签署）信息来达到同样的目的，而signature信息则是IKE（第一阶段）交换过程所得出的结果。XAUTH破坏了此模型。

评定取代拼凑而成的国家标准。这些安全性评定通常比较为人重视，不过值得注意的是，许多通过评定的产品通常移除了一些易用的功能。

目前，链路层无线安全协议尚未通过FIPS 140-2认证。链路层安全系统当中的一些组件必须通过NIST的审核，整个系统方能得到认证。目前已经验证过的组件列表参见*http://csrc.nist.gov/cryptval/*。通过审核之前，必须逐一验证的主要组件有：

“加密”密码

802.11i的CCMP所使用的AES已经通过审核。RC4尚未通过，几乎可以确定未来也无法通过审核，连带使得TKIP也无法通过认证。

密码操作模式

802.11i的CCMP所使用的CCM模式于2004年5月经NIST Special Publication 800-38C审核通过。

Hash算法

将主密钥扩展为密钥层次结构的准随机函数是以HMAC-SHA1为基础，目前已经审核通过。

密钥封装

密钥是敏感的素材，必须加密后再传送至网络。RFC 3394定义了NIST密钥封装函数（key wrap function），目前已通过审核。

密钥衍生

2005年1月，NIST发布了实现指南（*http://csrc.nist.gov/cryptval/140-1/FIPS-1402IG.pdf*）。根据这份文件，NIST打算发布Special Publication 800-56，正式审核通过密钥衍生方法。

虽然很少有商用产品符合安全标准，但有个例外相当有趣。一家大型政府契约商Harris Corporation（正好是802.11 PRISM芯片组的原始开发厂商）销售了一套称为“SecNet11”的802.11系统，使用美国国家安全局认证过的加密机制。买家必须先经过NSA审核。价格当然是天价，每个无线局域网络接口超过3000美元，每个接入点则叫价1600美元。

网络支持

除了安全性本身，决定在哪些网络堆栈层实行安全防护也受到其他因素的影响。最重要的不安全因素与客户端软件有关。配合操作系统内置的组件显然较具优势。既然802.1X申请者已经内置于主要操作系统，因此802.1X系统最具优势。IPsec客户端程序通常因终端设备厂商而异。在上述两种情况中，客户端软件都只要设定一次即可。只要公司所使用的SSID不同于其他网络，802.1X客户端通常比较好把握该于何时开始运行。如果

已经广泛部署IPsec，那么一开始就将无线局域网络视为远程访问网络或许会容易些，因为这样一来就无需对用户进行再教育。不过在选择IPsce之前，最好确定VPN终端设备还有裕余，可以应付新用户的局域网访问速度。

移动性的支持也是重要的考虑因素。为防止IPsec隧道被塞爆，必须安排网络提供IP层的移动性。有人称此种做法为创建一种“移动VPN”。IP层的移动性可以由网络本身提供，只要让所有接入点位于相同的VLAN即可，或者通过每个接入点连至VPN服务器的重叠隧道，甚至是通过802.1X动态指定VLAN。既然802.11i兼容设备能够在接入点间转移安全上下文（security context），对具有许多高度移动性用户的网络而言，它或许稍具优势。

对网络应用程序的支持程度也会造成对特定协议的偏好。IPsec并不支持非IP协议。仍然使用IPX或AppleTalk协议的网络可能没有任何选择。IPsec并不支持IP组播，其他链路层安全方案则是将IP组播视为一系列的组播帧。对一些延迟不能过长的应用（例如语音传输）而言，IPsec的速度或许太慢。我尚未听说有支持IPsec的话机或者任何打算推出IPsec 802.11电话的计划。

应用不同，需要保护的部分也就有所差异。有时候，只需要针对传输过程最弱的一环加以防护即可，对链路层加密即已足够；有时候，则必须使用site-to-site加密，全程提供必要的安全防护。数据需要多长的防护距离取决于电波离开之后所连接网络的安全性。如果两个接入点连接至相同骨干网络，链路层加密或许就已经足够。如果离开电波之后，数据必须跨越不可信赖的网络，就需要某种形式的网络层或更上层的加密保护。

在各层进行身份验证时应该考虑的因素如表22-2所列。

表22-2：决定身份验证层的主要考虑因素

链路层（802.1X）	网络层（VPN）
集成的操作系统组件	可能已经随VPN集线器部署
防范layer2网络遭受攻击	用户较熟悉，不需要太多训练
移动性架构较佳	提供链路层以外的防护
支持IP组播与非IP协议	安全性认证要求使用VPN，例如FIPS
在语音方面支持较快的切换（handoff）操作	

身份验证方式的选择

身份验证技术的选择通常取决于其与现有数据库之间如何连接。首先必须知道账号数据目前存放在哪里。究竟是存放在Windows NT域，还是Active Directory？到底是存放

在LDAP数据库，还是Kerberos realm？一旦知道用户数据存放在何处，该选择何种身份验证系统也就呼之欲出了。

EAP method的选择

实际上，要提供帧加密所需要的强加密密钥，必须使用基于TLS的EAP method。如此一来，就只剩下三种选择：EAP-TLS、PEAP与TTLS。EAP-TLS很难使用，因为每个工作站均需要证书。如果没有现成的PKI，实际上也不可能使用这种方式。PEAP与TTLS十分类似，问题在于应该使用哪一种。虽然这两种协议十分相似，但在加密隧道中却支持不同的身份验证方式。不妨以连接现有用户数据库的接口来决定使用何种身份验证方式。如何访问验证所需要的用户数据决定了应该采用何种EAP method。其中有三种身份验证方式可以访问大多数数据库，少数情况下则必须使用其他可行方式。

Pass word Authentication Protocol（简称PAP）传送用户名称与密码时并未加密。它只是将用户名称与密码传给身份验证服务器，和身份验证服务器中所存放的密码进行比对。既然未经加密，因此在未提供私密防护的网络连接中不该使用PAP（用于无线局域网络时PAP被包在加密信道内，因此是安全的）。PAP并非一种EAP method，因此并未得到PEAP的支持。PAP最常见的是用于使用“单向加密密码”（one-way encrypt password）的用户数据库，例如LDAP目录或Unix的*/etc/password*文件。有些系统只以SHA-1或MD5格式存储密码的单向散列（on-way hash）值，而不是以可还原的格式存储密码或者只存储密码本身。当用户或程序希望证明其身份时，其所输入的密码会先经过单向散列函数的处理，再将所产生的散列值与存储在用户数据库中的散列值进行比对。PAP通常配合令牌卡（token card）一起使用，因为令牌卡所使用的字母数字代码（alphanumeric code）可以和用户名称一并传送。一些支持TTLS/Token Card方式的申请者软件即使使用TTLS/PAP，但并不会高速缓存密码，因为令牌码很快就会逾时。由于几乎所有传统的身份验证数据库均支持密码身份验证，因此均可使用TTLS/PAP。如果不确定的话，不妨试试看TTLS/PAP。

Microsoft CHAP version 2（简称MS-CHAP-V2）会进行一次challenge/response握手。客户端与服务器共享一个秘钥（secret），并且通过相互质询以此秘钥来计算质询值。此秘钥即为用户密码（user password）的MD4散列值。虽然此散列值无法还原，但将被当成秘钥使用，因此“相当于密码”。Microsoft客户端软件广泛支持MS-CHAP-V2且通常配合PEAP一起使用，作为内层的身份验证方式。如果有现成的身份验证数据库存储在Windows域或Active Directory，MS-CHAP-V2就是内层身份验证方式的不二选择。它可以“如是”（as-is）用于TTLS，或者可以配合额外的标头信息（EAP-MSCHAP-V2）来当作EAP method使用。

第三种常见的内层身份验证方式是*EAP-Generic Token Card*（简称EAP-GTC）。EAP-

GTC原本是设计用来记录用户名称与令牌码。它并未提供任何握手或私密防护。既然它传递给服务器的是不会重复使用的令牌码，未提供任何防护是可以理解的。不过，最近它被当成一种EAP method，用来传送用户名称及相应的身份验证数据。没有一种EAP方法允许直接同时传送用户名称与密码，但EAP-GTC仍然可能被当成密码传送协议来用。没有任何方法能够防范EAP-GTC被当成PAP之类的身份验证方式使用，除了在实现方面把关。作为一种EAP method，EAP-GTC可以配合TTLS或PAP一起使用。

此外还有一些内层的身份验证方式可供使用，包括*Challenge Handshake Authentication Protocol*（质询握手身份验证协议，简称CHAP）、*Microsoft CHAP,version1*（简称MS-CHAP）与*EAP-MD5 Challenge*（简称EAP-MD5）。CHAP与Microsoft CHAP只用于旧式的身份验证数据库，除非现有的身份验证数据库不支持较新的认证方式，否则不应该使用这类认证方式。两者均可配合TTLS一起使用，因为它们均非EAP method。EAP-MD5并未提供安全防护，它虽然被用在有线网络的802.1X中，但几乎不会用在无线网络，因为无法防范他人窥视。

表22-3所列的三种内层身份验证方式或许可以配合现有的用户数据库一起使用。根据所选用的内层身份验证方式，可以配合PEAP或TTLS一起使用。此外，也可以根据各位打算使用的TTLS或PEAP实现来选择内层认证方式。标准允许EAP-GTC配合PEAP一起使用，但Windows内置的申请者软件并不支持此种操作。

表22-3：常见的EAP method

内层身份认证方式	外层EAP method	账号或用户数据库类型	附注
PAP	只能使用TTLS	单向散列系统（大部分的LDAP目录、Unix密码格式）、令牌卡	可能是第二常见的内层身份验证方式。是最通用的方式，通常可以配合任何数据库一起使用
MS-CHAP-V2	TTLS或PEAP	Windows用户账号（NT域、ActiveDirectory）或任何存储为MD4散列值的方式	由于Windows的原因，这是目前最常见的内层身份验证方式
EAP-GTC	TTLS或CiscoPEAP	与PAP相同	只有Windows版的Cisco supplicant支持

选定EAP method与内层身份验证协议后，就可以构建所需要的接口。要访问一组Windows用户账号，RADIUS服务器必须访问用户密码的MD4散列值。如果使之成为

域的成员，无需进一步设定，Microsoft的IAS服务器就可以从域系统中取得用户身份证明数据。第三方所开发的RADIUS服务器必须安装于域控制器，方能够访问用户的账号信息。任何受信赖的域也可以通过域协议被访问。

近来LDAP目录服务开始逐渐流行，特别是以扩充性为主要考虑因素的大型网站。LDAP目录有几种访问方式。有些是通过 RADIUS 前端程序。无线局域网络设备可以直接与RADIUS 前端对话，或是通过 RADIUS 代理服务器与 LDAP 目录的RADIUS 服务器对话。有些RADIUS 服务器也能够扮演LDAP 客户端的角色。取得目录证书后，RADIUS服务器就能够绑定至该目录，直接验证用户身份。与目录绑定的好处是可以通过SSL来保护目录的访问，进一步保护后端的身份验证连接。功能较少的RADIUS 服务器也可以与LDAP连接，做法是以客户端所提供的 LDAP 证书与目录绑定并且只查成功的案例。不过，只是进行绑定并查看成功的案例，RADIUS 服务器还是无法访问该目录所存放的用户元数据（user metadata）。如果目录中存放了可供无线局域网络使用的权限信息，RADIUS 服务器最好与之绑定，以便将用户授权信息提供给无线设备。

Kerberos 服务器受到许多学术单位的欢迎，有些 RADIUS 服务器可以通过 Kerberos 验证用户身份。这些RADIUS 服务器会试图从Kerberos 服务器取得通行证（ticket）；如果成功取得通行证，则允许用户进行访问。不过，Kerberos通行证与IP地址绑在一块，所以对“用户授权”而言并无太大用处。

身份验证架构

身份验证系统必须能够与现有的用户数据库连接才有用处。有时候，用户账号系统并不大，网管人员所面临的主要问题在于如何建立无线局域网络与用户数据库之间的接口。有些机构十分庞大，即使经过分割，也必须将维护用户账号的责任分散至各地理或管理区域。而分属不同部门的用户操作时，可能需要跨越地理或管理区域的界限。此时，网络设计的最终目标应该是为用户提供移动性与跨界限的生产力（不介意的话，可以称之为“分布式无线局域网络的Schengen设计原则”）。此种设计常见于大学校园中，由各学院或系所自行构建的网络。

图 22-1 显示了一座虚构的大学校园，其中包含了5个网络：图书馆、负责为一般区域与没有专属网络的院系提供网络的IT服务中心、自行构建独立网络的工程学院、医疗中心以及商学院。各部门自行维护本身的用户数据库，采用各自偏好的格式。为了提供无线局域网络的访问，可以通过一个RADIUS 前端来访问不同的数据库。其中，用户数据库与 RADIUS 前端并未实际标示出来。

设计身份验证架构时，目的是提供一种身份验证机制，让使用单一用户账号得以跨越所有园区网络。举例而言，任何进入图书馆的用户，不论是学生还是教职员工，都应该能

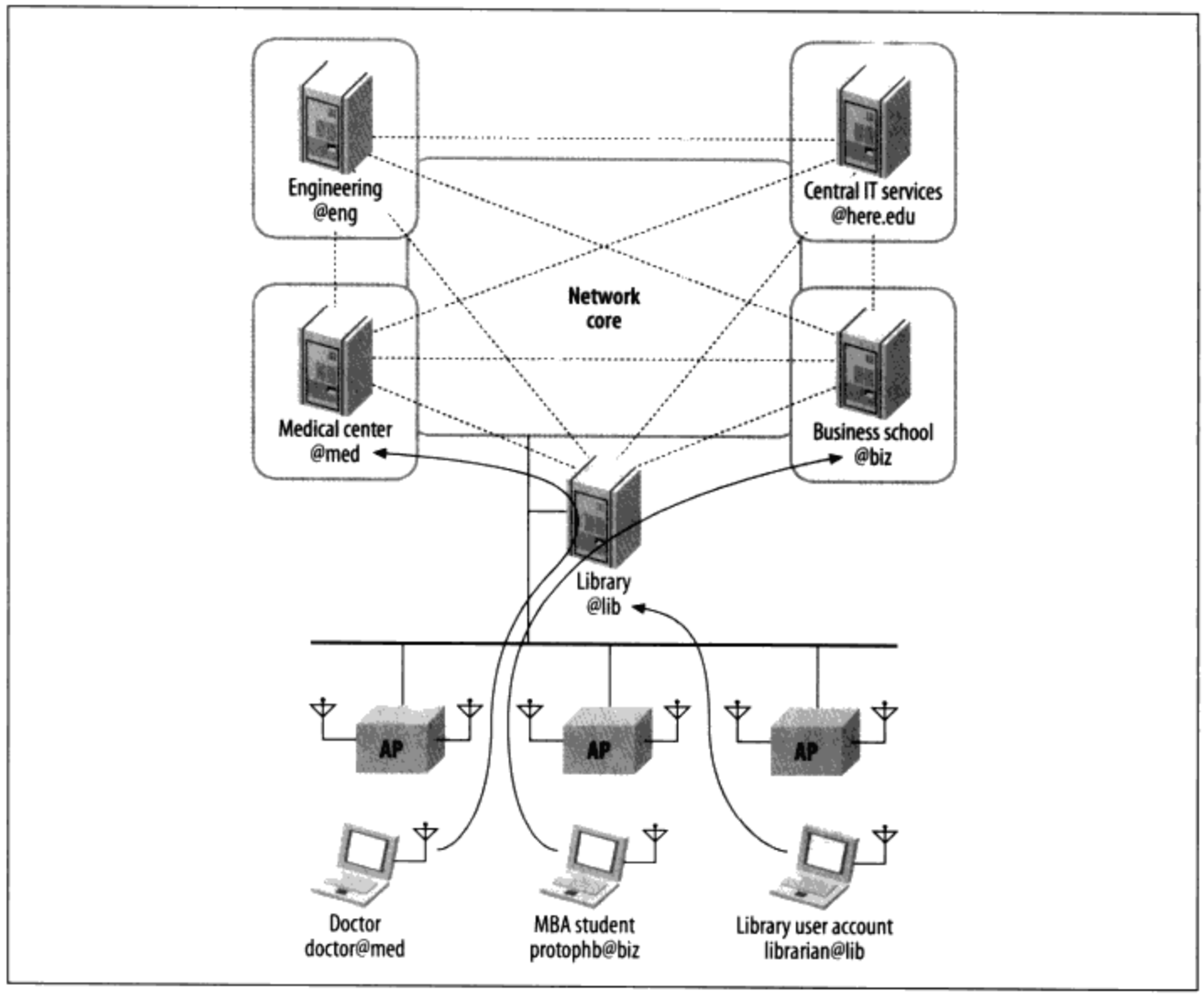


图 22-1：网状身份验证架构

够以归属网络（home network）的身份使用图书馆网络。如果各部门的RADIUS服务器间存在信任关系且能够彼此传递身份验证请求，那么单一账号即已足够。账号是指定给RADIUS领域，其可以将身份验证请求路由至事先定义好的服务器。图书馆的RADIUS服务器知道来自*user@med*的请求必须转送给医疗中心的RADIUS服务器。如果该服务器接受此用户，则允许该用户进行访问。

网络间的信任关系乃是此种架构的关键成分。如同在移动电话领域，要能够随处访问网络，归属网络与访问网络（visit network）之间必须存在一种漫游协议。网管人员必须依赖这种信任关系，因为他们必须开放访问权限给其他单位所验证的用户。在校园环境中，此种漫游协议可能是非正式的。在更大型的网络上，或许需要正式的法律文件来达成协议。一个由欧洲大学所组成的联盟EduRoam构建了一个RADIUS网状网络。加入EduRoam之前必须签署正式的协议文件。

在这类环境中，计费机制也可以派上用场。校园图书馆把预算用于购置教学资源，但不包括构建先进的网络服务。通过计费机制，网络服务供应商（例如图书馆本身）可以为来自其他网络的用户提供服务，以此作为网络支出的经费，而不必面临经费无着落的困境。

授权

在辨识用户与验证身份后，接下来或许需要限制网络的访问权限。限制访问权限有几种不同的方式，比较常见的两种方式是以访问控制列表进行封包过滤以及VLAN的指派。从某些角度而言，后者是比较方便的做法，可以利用VLAN间现有的封包过滤机制为不同用户组指定适合的基本规则。

通常，用户账号当中会包含若干“元数据”（metadata），用来记载该用户适用于何种权限。这些数据通常是针对机构的角色而定。角色必须转换为具体的行动，例如“将来自Group A的所有用户置于VLAN A”，或者“Group B的设备采用Filter B规则”。

“身份”（identity）与“角色”（role）离不开用户账号，这些数据通常会被转换为RADIUS服务器与无线局域网络设备本身所遵循的限制。角色不同，RADIUS服务器就会传回不同的限制属性。RADIUS属性可能触发无线局域网络设备更进一步、更为详细的行动。举例来说，RADIUS服务器可能为来自特定设备的数据指定某种过滤规则，可以确定的是，这些限制的细节将由无线局域网络的硬件来定义。

加密方式的选择

选定身份验证方式后，链路层加密方式的选择就比较简单了，因为必然会挑选大多数硬件所能支持的最坚固协议。这些协议的配置设定方式几乎一样，从用户的角度来看，它们的功能没有什么两样。

关于静态WEP，该说的都已经说了。除非别无选择，否则不要使用静态WEP。几乎所有通用型设备均已支持较佳的协议，但一些特殊应用设备（如802.11电话或条形码扫描器）除外。出于安全上的考虑，或许需要停止部署这类设备，如果这些安全问题无法通过其他方式得到适当的解决或者评估后显示风险极高的话。

使用动态产生密钥的WEP显然较好，因为经常变换的密钥可以防范针对WEP发动的攻击，如第五章所述。对通用型运算设备而言，起码应该使用动态WEP来保护用户数据。有时候，必须更新驱动程序后方能使用动态密钥，不过2002年中以后所发行的驱动程序大多已支持动态密钥。

不过就算搭配动态密钥，WEP还是存在种种瑕疵，因此在写作本书时，大多数网络均采用TKIP来提供起码的安全性。TKIP的硬件需求和WEP一样，因此几乎所有的802.11设备均支持TKIP。TKIP也需要软件的支持，但已经十分普遍。TKIP与WAP已经内置于各式操作系统，如Windows XP与MACOS 10.3。Linux尚未广泛支持WPA，因为驱动程序架构尚无法集成申请者软件，虽然未来可望进一步集成。

注意：计划升级为更安全的协议时，大多数机构应该以TKIP作为升级的目标。至于动态WEP，只能视为最起码的需求。

如果链路层加密要求高度的安全性，CCMP就是不二选择。TKIP要求协议侦测到密钥遭受攻击时，必须提供“反措施”以降低威胁性。需要反措施，无异承认该协议本身的强度存在基本的限制。不过，安全性并非全无代价。在所有链路层加密协议中，CCMP对软硬件的要求最高。它只能用于具备AES硬件加密能力的无线接口。近来的网卡几乎均已支持，但较早的网卡则不支持。如果各位手上有一堆无法支持AES硬件加密的旧式网卡，想要升级为具备AES能力的网卡不仅所费不赀，也是一项不小的挑战。

注意：CCMP可以提供最佳的安全性，不过它对软硬件的要求也最高。有些膝上型计算机厂商只采用最便宜的芯片组，因此除非另外购置网卡，否则根本无法支持CCMP。

支持多重SSID

802.11安全协议架构容许在同一个接入点中同时使用多组加密协议。客户端可以选择使用其中一种协议。单播帧的加密通常会采用接收端所支持的最坚固协议，组帧则是使用所有系统均支持的最坚固协议来加密。如果接入点有一组支持WPA的已关联的工作站，但另外有一个只支持动态WEP，则组密钥必须使用动态WEP。

标准并未限定必须支持哪些协议，不过实现上混用不同类型的加密协议可能会造成问题。其中最常见的限制是，大多数客户端软件并未支持以CCMP密钥加密单播帧的同时，另以非CCMP加密类型（TKIP、动态WEP或静态WEP）来加密组帧。未来或许会有驱动程序支持此种混合模式。目前，通常是以另外一个SSID来支持CCMP。也就是一个网络支持基于RC-4的加密协议，一个网络只支持CCMP。遗憾的是，采用两组SSID的确可能造成用户的混淆，因为连接至哪一个SSID纯粹掌握在用户手里。

注意：客户端软件的限制导致无法对相同的SSID同时使用CCMP与RC4加密。要同时使用两者，802.11接入点必须支持多重SSID。

私设接入点

网管人员所面临的主要风险之一，就是用户私自架设未经授权的802.11网络。所谓的“私设”(rogue)接入点可能造成相当大的威胁。最主要的威胁是，用户私自架设的接入点，不像经授权部署的设备那样具备完整的安全性配置设定。用户或许没有足够的能力与意愿来正确地启用攸关安全性的功能。即使这些设备已经采取适当的防护，未经授权的设备也可能干扰现有网络的运作。

侦测

对付私设设备的首要步骤就是确定它们是否存在。要确认未经授权设备的存在，必须使用某种无线电设备。802.11设备刚问世那几年，接入点还十分昂贵，因此只需要携带一部膝上型封包嗅探器(sniffer)，就可以扫遍所有接入点。当有更多人熟悉802.11，私设设备的侦测便需要转变为持续、自动化的过程。考虑到成本与管理因素，如今侦测过程已经被整合进大多数的无线局域网络主流系统。根据厂商的实现方式，侦测组件可以是一种扫描功能，定期搜寻未经授权的设备，也可以是特定的扫描设备。未授权设备的扫描可以是被动地聆听数据、Beacon或Probe Response帧，也可以主动使用802.11 Probe Request帧，让未经授权的网络自动现形。

为了达到效果，侦测必须涵盖所有可用的802.11信道。起初，企业的部署方案通常采用802.11b，其所使用的无线电接口芯片组并无法操作于802.11a频带，也无法使用802.11a的调制技术。有些私设接入点的人比较聪明，故意采购802.11a设备，理由是比较不容易被网管人员侦测到，况且网管人员所使用的分析工具也只是针对802.11b。

无线局域网络基础设施必须内置侦测能力，否则就需要使用独立设备。网管人员通常必须在提供给用户的服务质量、侦测信息的质量与成本之间作出取舍。专用的侦测设备可以提供最好的侦测结果，但成本最高。以原本为用户提供服务的设备来侦测未经授权的设备虽然比较便宜，但可能会中断或拖累原本的服务。

搜寻未经授权的部署时，主要是针对私设设备所显露的迹象。至少，侦测器必须搜寻是否存在其他Beacon帧。所有接入点与ad hoc网络均会发送Beacon帧。比较完整的802.11系统也会观察工作站的数据，并将电波范围内的工作站列表拿来跟已关联的工作站进行比对。只要出现于前者的工作站并未出现在后者，就是关联至未经授权的接入点了。

物理定位

一旦侦测到私设接入点，在采取任何行动之前，网管人员通常希望能够找出它的物理位

置。有时候，只要知道有私设接入点存在，让网管人员找到用户并予以停用即可。如果需要主动反措施，最好是锁定特定区域的私设设备。目前，有几种主要的定位方式：

1. 计算最近接入点的半径
2. 三角定位
3. RF 指纹辨识
4. 时间差

要找出私设接入点所在，最简单的方式是利用最近接入点的半径，如图 22-2 a)所示。在网络上搜寻 MAC 地址后，就可以根据侦测到该设备的基站位置来粗略判定其位置。开放空间的无线电信号传播是依循已知的数理模型。根据侦测到该设备的接入点所接收到的信号强度，就可以计算出最大半径，只要知道以最大传输功率进行传输的设备的最大半径为多大，再与所接收到的信号强度进行比对即可。在图 22-2 a)中，接入点所接收到信号的强度可用来判定其与最近接入点间的开放空间距离，但无法提供任何足以判定该接入点位于圆周上哪个位置的线索。

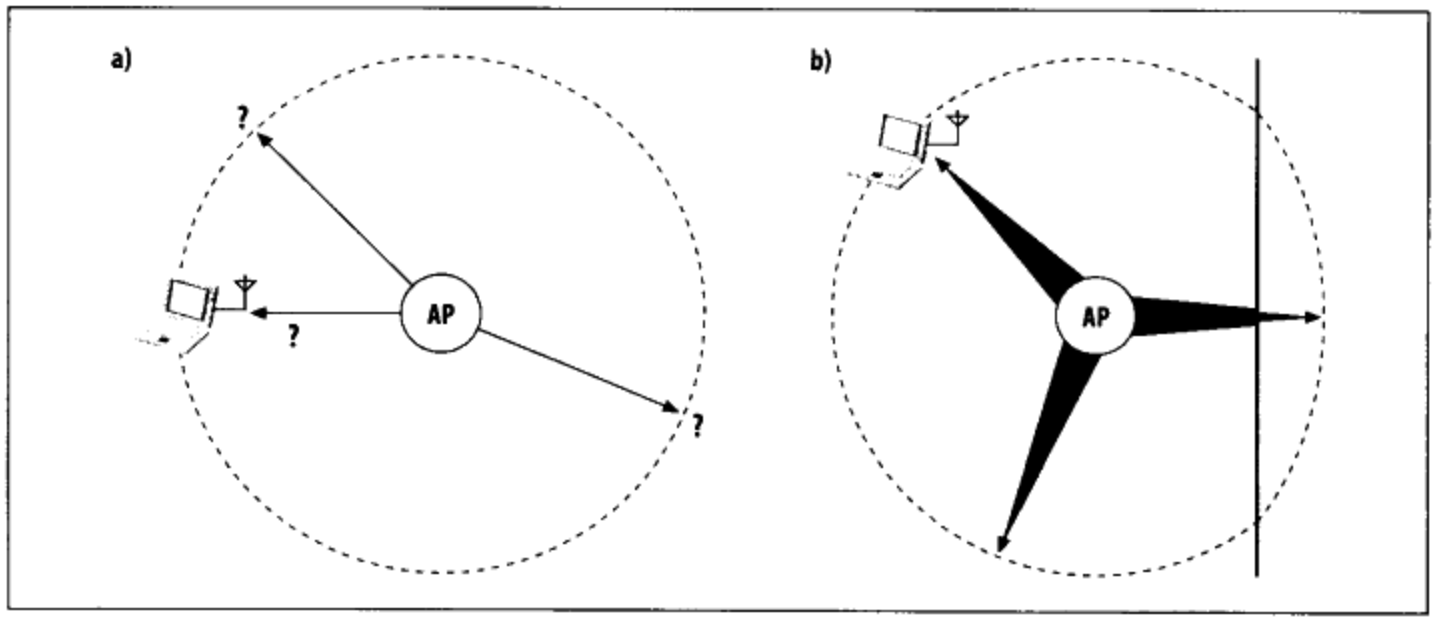


图 22-2：最近接入点的半径

接入点半径计算有几项缺点。首先，以最大功率传输的信号的开放空间半径较实际半径长。开放空间模型所容许的半径高达 100 英尺，所得出的 30000 平方英尺的面积过大，因此没有实际用处。比较好的定位方式，是先以一些定位工具为整个无线电环境建立一个数理模型并将特定路径上的建筑物纳入考虑。在大多数办公大楼中，有效覆盖半径通常在开放空间的一半以下。将覆盖半径从开放空间中的 100 英尺的理论值减少为特定环境中的 50 英尺以下的实际值，就可以将目标缩减至较少的 8000 平方英尺。不过，8000 平方英尺仍然相当于 70 至 100 个隔间（cubicle），这取决于隔间的大小以及办公室的平

面布局。图 22-2 b)的右边有一道墙，它会缩短覆盖半径，因为无线电信号必定会穿透墙面。箭头的厚度表示某个定点的信号强度。当无线电信号行经墙面，信号强度就会降低，覆盖范围因此而变小。如果这类建筑物为数越多，修正覆盖半径的效果就越好。在充满隔间的典型办公室中效果就没那么显著，因为信号可以传送至较远的距离。

计算到最近接入点的半径的做法可以进一步使用三角定位来加以改善，如图22-3所示。三角定位原本是指根据其与三个已知点的距离来进行定位。有些无线局域网络系统所使用的“三角定位”（triangulation）技术采用三个以上的测量点。

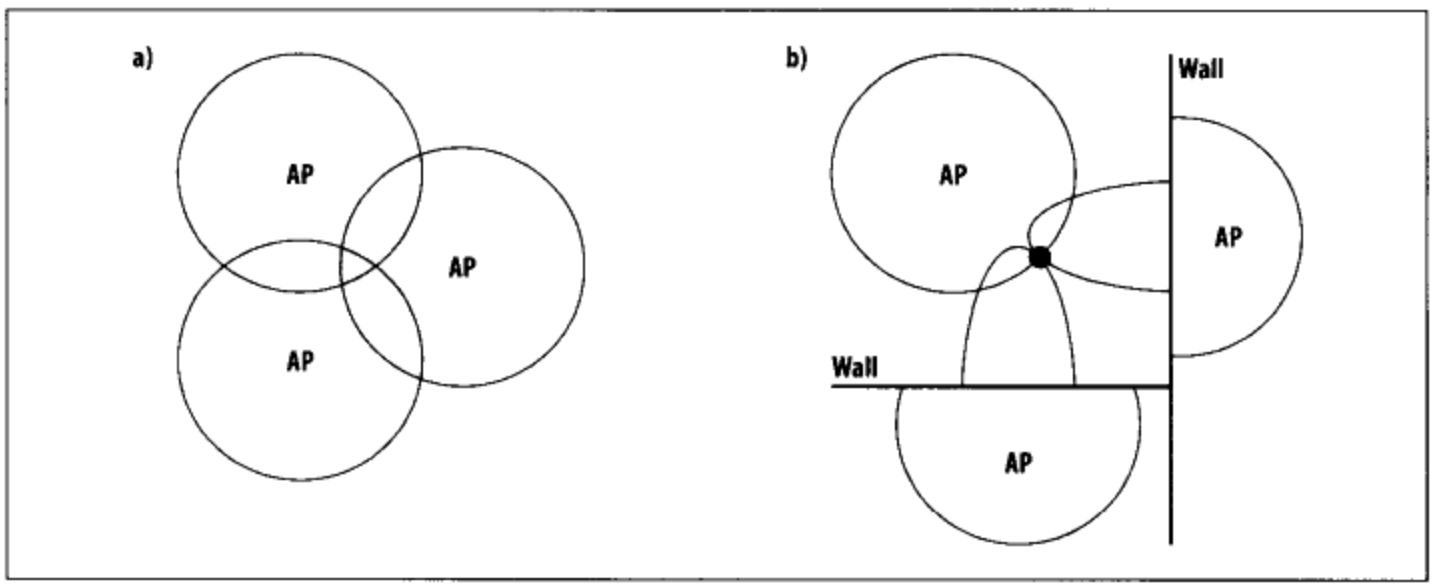


图 22-3：三角定位

重叠的覆盖区域、重叠的半径，有时再加上或然率的模拟，可以用来搜寻设备的可能位置。在图 22-3 a)中，三个接入点的重叠覆盖区域被猜测为设备的所在位置。和计算最近基站半径的做法一样，三角定位算法可以配合对建筑构造的了解来得到比较精确的定位。在图22-3 b)中，若将两面墙所造成的信号阻隔效应也纳入考虑，预测的结果就更为精确。

如果采用RF指纹测量，定位就可以更加精确。取得无线电波与建筑物的互动数据后，就可以根据这些数据来修正数理模型，了解无线电波的实际行为。要建立一套指纹数据库，必须先将设备摆在已知定点然后加以测量。接收信号强度及其他信号特性等数据随后会被当成该位置的“指纹”（fingerprint）被加以存储。指纹包含所有难以计算的信号传播特性，例如墙面的反射以及多径干扰。要定位未知的设备，可以拿它的信号特性与指纹数据库进行比对，便可精确地定位出其所在位置。定位预测的质量取决于已建立的指纹数，这些指纹通常必须通过实地勘探来建立。虽然指纹辨识有助于改善定位信息，但需要搜集大量相关数据并建立够大的指纹数据库，方能达到想要的精确性。

最后一种定位方式就是根据接收信号的时间差。信号强度受到一些因素的影响，包括建筑物构造。不过，无线电波总是以光速行进。可以在不同测量地点以三角定位法计算接

收信号的时间差。虽然这种技术可以精确定位，但由于无线电波的行进速度很快，因此需要使用十分精确的时间同步技术。图22-4中，两个接入点用来测量来源信号的到达时间。经过一段时间，信号到达第一个接入点。定位系统必须十分精确地计算出信号到达两部测量设备的时间差。无线电波每十亿分之一秒行走一英尺，因此定位设备必须能够辨识信号到达两部测量设备的细微时间差。虽然理论上可行，但信号时间差的做法通常需要用到相当特殊的设备与定时设备，它们的精确度是一般接入点所无法比拟的。

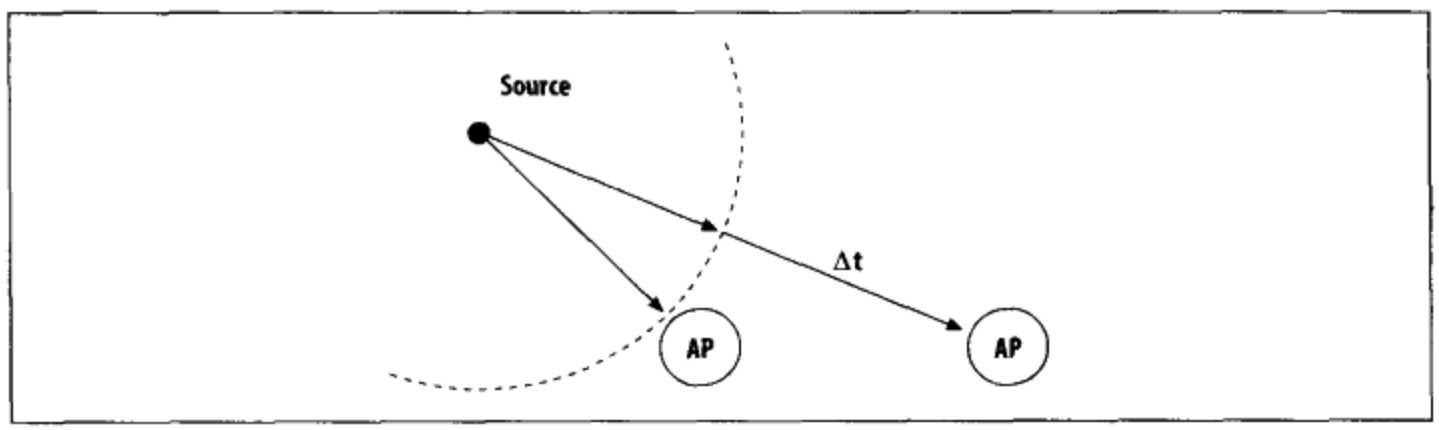


图22-4：时间差分析

关闭私设接入点

有些产品能够自动关闭未经授权的网络，这种功能通常被称为“封锁”（containment）或“抑制”（suppression）。技术上的细节虽然不同，但同样是使用协议上的一些技巧来阻止或中断私设接入点的连接。一般而言，这些做法若不是阻止其他工作站关联至私设接入点，就是设法中断现有的连接。有些技巧是利用无需验证的控制帧，以基础结构型设备来冒充私设接入点。未来802.11协议如果对重要的网络控制信息进行验证，这种做法还会有多少反制效果尚待观察。图22-5显示了两种对私设网络发动拒绝服务攻击的主要技术。

要中断关联过程，可以使用一些设备送出伪造的Beacon或Probe Response帧，如图22-5 a)所示。既然Beacon或Probe Response帧不会经过验证，则授权接入点可以轻易冒充私设接入点。伪造的帧所包含的信息可能和私设接入点所传送的帧彼此冲突，令工作站不知所从。如果发现某个网络既是加密网络（在Beacon帧中设定Protected Frame位），又是未加密网络（清除Protected Frame位），有些工作站就无法与之关联。伪造Probe Response帧也可以达到相同的效果。有些无线局域网络系统会试着捕捉工作站的关联请求，把跟私设接入点关联的工作站加以“俘虏”以避免造成损害。至于已经与私设接入点关联的工作站，可以使用Dissasociation与Deauthentication帧来处置，如图22-5 b)所示。这些信息并未经过签署，因此容许网络系统将工作站踢出私设接入点。

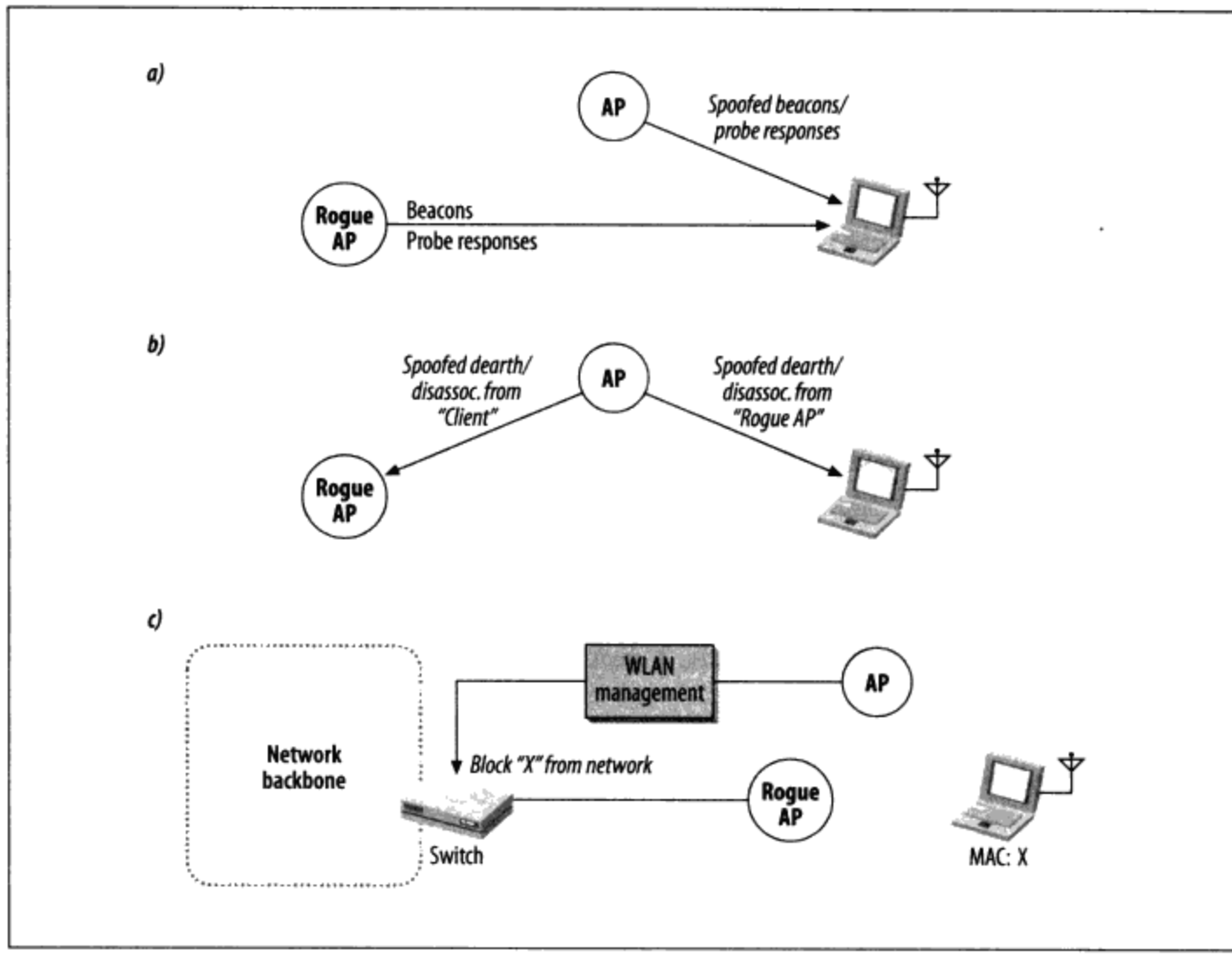


图 22-5：私设接入点的封锁技术

要以伪造信息干扰工作站的操作并不简单。由于多重路径以及基础设施与工作站间的相对位置均会造成影响，因此不见得能够完全拦截所有这些打算联机至私设接入点的工作站。有些设备会以工作站的地址送出伪造的 Deauthentication 给私设接入点，迫使私设接入点解除与这些与其关联的工作站的连接。有些无线局域网络管理系统可以进一步限制私设接入点可能造成的损害。如果可以辨识出与私设接入点关联的工作站，无线局域网络管理系统理论上会在骨干网络采取行动，不让此工作站联机使用骨干网络的服务，如图 22-5 c)所示。

封锁私设接入点怪异与有趣之处在于802.11网络通常是因为用户有移动性的需求。为了确保涵盖范围足以让私设网络停摆，必然得使用相当数目的封锁设备。事实上，封锁所需要的802.11接入点数量相当于用来提供服务的接入点的数量。为了提供必要的封锁能力，通常需要部署足够的接入点，才不会影响正常的网络访问。

之所以逐渐以802.1X supplicant来取代接入点，是因为可以在提供服务之前先与网络进

行身份验证。启用802.1X的有线网络可以在私设接入点造成问题之前即予以回绝，而不是等到它们出现后才进行封锁。

律师的忠告

封锁私设接入点可能会被视为意图干扰无线网络的计算机犯罪(请咨询熟悉当地法规的律师，毕竟这并不是我的专业)。假冒私设接入点而让它们因此停摆的设备，主要是设计来干扰无线网络的操作。如果该网络属于邻居或对街的咖啡馆所有，这种行为可能已经触犯法律或者会导致民事诉讼。

为了避免替律师制造更多就业机会，在发动反制攻击之前，最好确定私设接入点的确连接到自己所防护的网络。举例而言，如果私设接入点属于对街的咖啡馆所有，而有人导致他们的网络停摆，他们大概不会善罢甘休。容纳许多办公室的大型建筑物必定会有许多相邻的无线网络，对这些网络不该采取反制攻击（如果隔壁就是精通计算机领域的律师事务所，对他们的接入点采取反措施无疑是自找麻烦）。

最近FCC管制当局明文禁止业主声称拥有电磁频谱的任何权力。因此，对承租户或邻居发动私设接入点的反制攻击是相当不智的。

第二十三章

网络规划与项目管理

无线局域网络的部署之所以不简单，部分是因为整个过程并不是那么结构井然，特别是相较于有线局域网络的部署而言。如今构建Ethernet网络已经十分容易。几乎每个人都拥有各自的交换式Fast Ethernet（或更快的）连接端口，核心交换设备甚至使用更快（或者经过合并）的链路。至于布线方面，不少厂商已经累积了多年的经验，经过这么长一段时间，对于如何布线基本上已经有相当的共识。

相较之下，无线网络就像是蛮荒的西部。网络至终端用户间的服务质量取决于用户与最近的网络设备之间的距离且随之递减。网络性能（capacity）受到覆盖范围的大小以及建筑物实际格局的影响。从无线电传输的角度而言，每栋建筑物均有其特性，而且到处都有可能出现意外的干扰，例如微波炉、电线或严重的多径干扰。更糟的是，不仅你自己本身，甚至连用户或邻居的所作所为都可能对网络媒介的质量造成影响。

打算部署无线局域网络时，可以先从明显的问题开始："需要多少接入点？""应该摆在哪里？"要回答这些问题，必须进行实地勘探（site survey）。实地勘探通常在无线局域网络计划启动时便开始进行，而且经常是整个网络项目计划相当重要的部分。本章仍从技术的角度说明实地勘探与项目本身密不可分的本质。在规划阶段需要做些什么才能够成功部署？接入点的摆放规划属于无线局域网络推行（roll-out）的一部分，因此本章将协助各位拟定自己的部署计划，包括实际的布局计划。

无线局域网络的规划过程分为几个阶段。需求的搜集，不见得需要花费很长的时间来准备冗长的文件。规划过程结束后，对于网络的覆盖范围与性能需求应该就会了然于胸。为了修正需求并将之落实成为符合需求的设计，可能需要在现场花费不少的时间与精力。

项目规划与需求

一旦确定要构建无线局域网络，最好及早着手规划。无线局域网络技术仍在继续进展当中，网管人员越早参与，结果就越加完美。如果无线局域网络要装设在新建大楼，在建筑物的基本架构图出炉后就可以尽早让网管人员参与，特别是接入点的摆放位置有所限制时。我曾共事的一家机构对空间的美感要求极高，接入点最后只能置于钢筋骨架结构旁边，而且被迫隐藏在隔间镶板（paneling）之后。如果网管人员早点参与规划，不仅能够找出更适合的摆放位置，也不用浪费那么多金钱。

规划有线网络相对比较简单。虽然视网络规模需要不同程度的技艺，但基本上，网管人员都已经相当熟悉整个规划过程。有线网络媒介的行为是可预测的，固定式网络的升级也十分容易。而无线局域网络技术还没有那么成熟，相形之下规划过程就更为重要了。

无线局域网络项目规划通常被视为实地勘探。然而实地勘探只是其中一环，成功的无线局域网络部署需要好几回合的勘探，每次勘探的目的都不尽相同。对预计安装于新建大楼的无线局域网络在施工过程中就可能必须来回勘探好几次。如同以往，在“破土”（breaking cable）进行网络扩充操作之前就应该着手规划。

实地勘探是构建无线局域网络的核心工作。不过，实地勘探要有结果，事前的准备工作就相当重要。在“破土”进行网络扩充操作之前，最好事先搜集技术上的需求，征询必要的信息以便厘清用户心目中有哪些期望是重要的。你可以使用下列检查表来记录用户的需求，各项要点将在后续各节详加说明：

吞吐量

需要多少吞吐量？这个问题部分取决于将用在无线局域网络上的设备类型，如果是可以显示较大与较复杂图片的PC-like设备，自然希望无线局域网络越快越好。大多数情况下，通常会选择采用54 Mbps的物理层的802.11a或802.11g网络。

覆盖范围

需要覆盖哪些地区？需要完全覆盖吗？有些区域比较难以覆盖。电梯井（elevator shaft）通常位于中央大楼的核心，比较难以覆盖。要在电梯里头提供信号不难，但大多数用户或许无此需要。

用户密度

除了用户所在位置，也需要注意用户数的多寡。公共场所的用户通常比较密集，例如会议室、大厅与餐厅。

机动性

无线局域网络已经不再是玩家专属的新奇玩物。几年前，在过渡阶段，人们还可以

接受网络仅提供自动重新设定的服务。不过随着无线局域网络日渐成熟，设计人员在设计网络的时候还必须考虑如何在覆盖区域内提供持续的连接。

用户数目

有多少人会使用无线网络？他们心目中所期待的服务质量如何？记得将未来的成长率计算在内！

实体上的考虑

是否需要为无线局域网络骨干重新铺设网线，还是可以利用现成的架构？如何对这些新增加的接入点供电？接入点与天线能否暴露在外，还是必须隐藏起来？

美观上的考虑

无线局域网络需要隐藏到什么程度？接入点是否允许被用户看到，还是需要隐藏起来？

逻辑网络架构

大多数情况下，逻辑架构必须在整个连续的覆盖范围内支持相同的IP地址段。在逻辑网络架构下，用户或许会取得不同的IP地址。近来随着技术的发展，目前已经不需要再根据IP寻址架构来调整移动性区域。

应用上的特性

是否有任何应用对延迟十分敏感？是否有任何应用必须提供及时(time-critical)的数据？

安全需求

部署之前，各位或许想要设计出一种网络，它既可以解决本书所探讨的安全问题，又可以提供一个足以防范未来的可能攻击的可靠环境。安全议题与架构已经在前两章探讨过了。

网络所在环境的考虑

影响无线电波传播与信号质量的因素很多。建材、结构与楼层规划均会影响无线电波在整栋建筑物中的行径。干扰势不可免，但是每栋建筑物里的干扰程度亦不尽相同，而且温度与湿度也会造成些许的影响。及早进行实地勘探有助于掌握相关因素，而详细的实地勘探可以在实际建设之前发现问题所在。

项目管理

和所有项目一样，预先规划日程与预算是不可或缺的。本章并未提供任何非技术层面的指南，因为每个组织的情况通常不太一样。

网络需求

和其他网络技术一样，部署无线局域网络之前必须先回答三个问题："部署在哪？""速

度有多快？”与“经费有多少？”通常，成本是通过预算过程独立确定的，网络设计人员必须试着在预算的限制下提供最佳的局域网络服务。“部署在哪？”是指无线服务所涵盖的地区集合。一般希望能够涵盖所有地方，但有些项目为了节省成本，会将部署规模缩小至会议室与公共空间。“速度有多快？”是指无线网络的性能（capacity）。无线局域网络客户端的速度取决于其与接入点之间的距离以及接入点与工作站之间障碍物的多寡。要建设一个高吞吐量网络，必须专注于如何缩短工作站与接入点的一般距离。有些物理空间会对无线电波造成相当程度的影响，需要相当数量的接入点方能完整覆盖。

网络设计人员必须在这三项变量中取得平衡，方能够构建合格的网络。在一些环境中，建筑物本身的实体设计很容易阻挡电波的传播，因此必须缩小网络的覆盖范围，其性能也会因此而受到影响。有些网络预算有限，只求能够符合最低性能要求。在比较少见的情况下，或许可以针对整个覆盖范围提供较高的带宽而不必考虑成本问题。设计人员必须持续针对这三项设计因素进行调整与优化。当无线局域网络的用户逐渐成长时，网络本身也必须随之扩充。一开始是特定区域的部署，随后可能必须提供完整的覆盖范围。以覆盖范围为主要考虑且尽量减少接入点数目以节省成本的网络，日后或许会转变为性能较高的网络，可满足用户的额外需求以及日渐增加的用户数。要在这三种需求中取得平衡，纯粹是一种艺术。幸运的是，有一些工具可以协助我们在这些取舍间作出决定。

覆盖范围需求

网络有覆盖范围。有线网络的覆盖范围取决于分布在各地的网络连接端口，要提供网络服务，必须进行布线并提供连接端口。而无线网络提供覆盖范围的方式不同，因为无线网络的传输媒介遍布整个空间并且能够穿透墙壁。掌握无线电波的空间传播型态，乃是了解如何覆盖整个范围的关键。

首先必须回答的问题是要覆盖哪些范围。是涵盖整栋建筑物与园区，还是在特定区域提供无线网络？一般的做法是先在特定区域试行并借此熟悉技术。有时候，试行的范围覆盖整个IT部门，大厅或会议室等公共场所也常涵盖其中。

对提出无线局域网络覆盖范围需求的人而言，“无所不在”（ubiquitous）是个流行的词，不过对必须满足此项需求的人来说，这可能是个恐怖的词。这是否意味着必须涵盖建筑物的每一寸空间呢？例如，真的需要为洗手间提供高质量的服务吗？对公共建筑而言，是否连逃生路线也包含在内？

覆盖室内区域需要多少个接入点取决于许多因素。首先，这与建筑物的构造有关。墙面越多，意味着无线电波将遭受更多物质的阻隔，因此需要更多的接入点。不同材质对射频有不同的影响。以相同材质而言，墙面越厚，信号损耗越大。信号功率最容易受到金属影响，因此电梯井（elevator shaft）与空调风管（air duct）皆会严重妨碍通信质量。

有色或经涂覆的窗户通常会严重干扰无线电信号。有些建筑甚至会使用金属电镀天花板或在地板中镶入大量金属。木材与大多数玻璃窗的影响较小，不过防弹玻璃就不见得了（注 1）。砖块与混凝土的影响介于金属与一般未经处理的玻璃之间。

第二个主要因素是打算提供何种速度。“只是提供无线局域网络访问服务”与“提供特定的数据率”完全是两回事。802.11a 的速度介于 6 Mbps 与 54 Mbps 之间。速度越低，覆盖范围就越大。相较于只是提供 802.11 访问服务的网络，让整个网络支持 54 Mbps 的数据率需要更多的接入点。图 23-1 显示了三种主要 802.11 物理层的比较以及如何在距离 / 数据率间作出取舍。

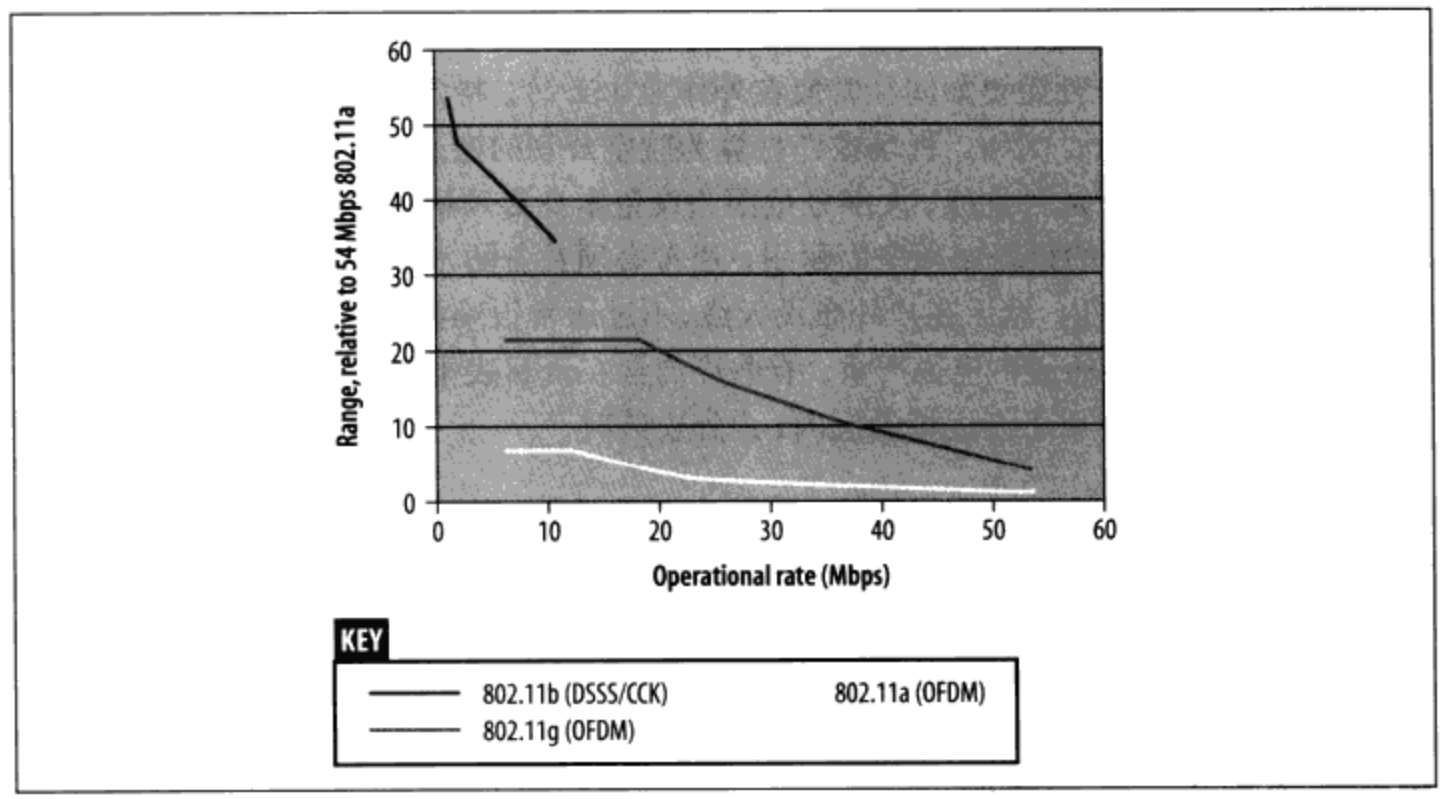


图 23-1：开放空间路径损耗的相对距离比较

图 23-1 是根据开放空间损耗的理论值绘制而成。它显示了 802.11a、802.11b 与 802.11g 于各种速度下的相对传输距离。计算时，我使用了典型的传输功率（802.11b/g 为 20 dBm 或 100 mW，802.11a 为 11 dBm），然后计算每一种速度在何种距离下功率会降至电波灵敏度以下。至于典型的灵敏度，我是以 Cisco a/b/g 无线网卡的规范作为参考。图中所显示的传输距离是相对最小距离的，亦即 802.11a 的最高数据率 54 Mbps 的最小距离。

为了达到性能目标，相邻接入点的覆盖范围必须有相当程度的重叠。如果目的是在特定区域提供高速的传输（例如 36 Mbps），则在较低速的传输时必然会出现更大的重叠区

注 1：　防弹玻璃的普及程度超乎一般人的想象。

域。规划时切记保持某种程度的重叠，方能够确保切换操作（handoff），同时也应尽量减少接入点的数量以维持最佳性能。这些是设计无线局域网络时必须特别注意的取舍问题。

覆盖范围的最后考虑因素是网络本身的目的为何。无线网络有特定的覆盖范围，但传输与接收范围可能并不相同。接收范围通常较广，特别是并未将接入点的传输功率调至最大时。增加接入点密度但调低功率的好处是在接收范围内会有比较多的重叠部分。只要用户私下部署未经授权的接入点，就很难不被网络中的接入点侦测到，而且可以更精确地定位其所在。

相较于室内的覆盖范围，户外有另外一套不同的取舍标准与工程需求，而且通常牵涉到恶劣的天候下用户是否需要如同往常般在外作业（注2）。特定的应用也适合将室内/户外覆盖范围一并考虑，例如，机场或许打算为航空公司的搬运设备提供户外访问服务。将设备置于户外向来是种挑战，大部分是因为设备本身必须耐候，必须符合不少环境或安全法规。置于户外的设备必须坚固耐用，通常必须具备防水或耐候能力。一种解决方案是将接入点装在室内，然后在户外布设天线，不过通常很难找到长度合适的外接天线。就算可以，线材的损耗通常也很严重。有些厂商会在价目表上列出耐候器材，特别是当他们销售的设备主要用于大规模的室内/户外安装时。

耐候机壳可能必须符合其他安全标准。国际电工委员会（International Electrotechnical Commission，简称IEC）60529标准中列有测试流程，可用来评测耐水与耐砂粒的能力。在美国，外部机壳也必须符合国际电气制造业协会（National Electric Manufacturer's Association，简称NEMA）250标准。

覆盖范围与实际安装限制

一般用户的需求中通常包含期盼的信号覆盖范围，不过实际上可能会有所限制。比较常见的限制包括无法提供电源或网络连接。有些机构要求对接入点与天线必须予以隐藏，也许是为了维护网络的实体安全，也许只是为了保持建筑物的美观。

接入点通常是挂得越高越好。就像试图夺取战地制高点的童子军，当接入点位于所有障碍物之上时，运行性能最好。将接入点置于隔断（cubicle）或其他物体之上，通常可以让信号更稳定、传得更远。有些接入点提供安装支架，可以固定在墙壁或倒吊于天花板瓷砖（ceiling tile）的吊杆（suspension bar）上。有些厂商建议将接入点安装于天花板

注2：本章并未论及802.11点对点链路。显然，这种链路只用于户外，而且可以在任何气候下常年使用。

瓷砖之上，再配合穿透天花板瓷砖的外接天线。天花板厂商甚至已经开始进入这个市场，生产整合了天线的天花板材（注 3）。

许多商业建筑使用所谓的“倒吊式”（dropped）天花板，在真正的天花板之下另外悬挂天花板瓷砖。网线与电线置于天花板瓷砖之上，跟空调风管（air duct）放在一块。有些建筑物将整栋建筑物的空调风管系统置于天花板瓷砖与天花板之间的空隙间。安全标准规定，置于空调风管空间（plenums）的物品不得危及建筑物的用户。万一失火，建筑物内部人员所面临的最大危险就是浓厚的黑烟可能会遮蔽视线，阻碍逃生的路线。置于空调风管系统的设备一旦产生烟雾，就会立即弥漫整栋建筑物。因此，为了保护建筑物内部人员，置于天花板之上的设备必须符合一些特定的安全标准。如果打算将无线局域网络设备置于天花板之上，务必确定它们是阻燃的（*plenum-rated*）。除了接入点，这也包含附挂于天花板之上的所有辅助设备。馈电器通常不是阻燃的，因为它们通常可以置于配线柜内。布于天花板之上的线材几乎可确定的是必须是阻燃的。防火安全标准是由 Underwriters Laboratories 所制定的并出版为 UL 的 2043 标准。UL 也负责测试产品是否符合标准，通过校验后才予以认证。

性能需求

覆盖范围并非无线局域网络设计的完结篇。在网络负载范围内，接入点的作用类似集线器。对特定覆盖范围而言，无线带宽是固定的。在覆盖范围内，802.11b 接入点能够传送 6 Mbps 的用户数据。802.11 网络实际上使用的是共享式媒介。除非无人与之竞争媒介，距离接入点甚远的用户才有办法享受 6 Mbps 的速率。当很多用户使用网络时，同样的 6 Mbps 必须由所有用户共享，而协议本身必须公平地（或者不公平地）分配容量给各工作站。

对服务用户的网络而言，必须在覆盖范围与服务质量间作出取舍。只要配合高增益的外接天线，就可以使用较少的接入点，但带宽就必须在较大的范围来共享。基本上，扩大覆盖范围的做法并无对错可言，特别是用户密度较低的时候。有些部署会使用单一接入点配合外接天线来覆盖较广的区域，因为对网络容量的需求并不高。有些用户不多的 K-12 学校即属此类，可说是图 23-2 左边的代表。图 23-2 右边，用户甚多的网络会倾向于使用覆盖范围较小但数目较多的接入点。网络工程师有时会借用移动电话的术语，称此种网络具有许多“微蜂窝”（microcell）。既然覆盖范围较小，接入点就可以服务较少的用户（虽然无法保证）。图 23-2 中，右边的图示将相同的区域划分为三个区域。因此，每个接入点只需要服务较少的工作站，每个工作站的吞吐量也因此提高。

注 3: 例如 Armstrong 的 I-ceilings 天线面板（*http://www.armstrong.com/commceilingsna/article7399.html*）。

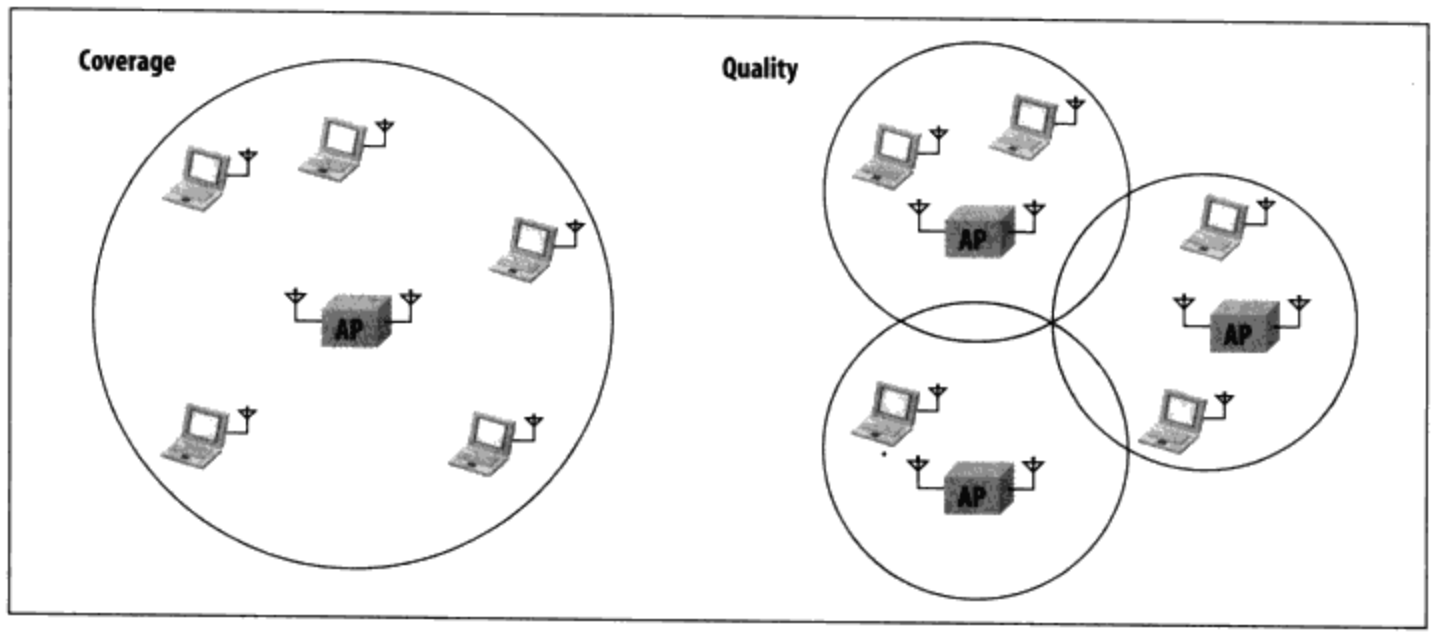


图 23-2：覆盖范围 / 服务质量的取舍

评估需求时，区域总吞吐量（或是单位面积的吞吐量）是相当有用的指标。图 23-2 中，左右两个网络覆盖相同的面积。不过由于具备三个接入点，因此右边的网络可以提供三倍的吞吐量。并非所有网络均需要高区域总吞吐量，至少一开始是如此。当无线局域网络逐渐受到欢迎，图 23-2 中的用户从 5 位变成 10、15 甚至 50 位时，就需要进一步增加区域总吞吐量。

需要为每个用户保留多少容量呢？一种做法是对网络应用与性能需求进行详细研究，然后据以设计网络。不过以实际来看，大多数网络似乎都是以“薛定谔的猫”(Schrodinger's Cat) 理论在运作着：只要有封包在传送，网络就会持续运行；一旦深入探究它的运作方式，它便停止运行。一般而言，大多数无线网络项目均始于“好像有此需要”的模糊概念，而不是“它应该用起来像有线网络”的想法。既然没有任何反对意见，我建议至少为每个用户保留 1 Mbps 的带宽。802.11a 与 802.11g 网络允许为每个用户保留较高的速率，特别是将流量估计得比较高时。

探讨覆盖范围 / 服务质量间的取舍以及区域总吞吐量

正常负载之下，接入点相当于集线器，容量是由覆盖范围内所有用户共享的。使用覆盖范围较广的接入点来构建网络通常花费较少，因为所使用的接入点数量较少；但服务质量可能较差，因为总容量较少。接入点负责的覆盖区域较大，距离较远的工作站就必须使用较低的速率联机。

一种衡量服务质量的方式为计算服务区域内的总吞吐量，它在某种程度上反映了接入点的密度。其他条件不变的情况下，较多的接入点意味着较多的无线通信容量。图 23-3 显

示了三个网络。图左的网络只有一个接入点，最多可提供30 Mbps的用户数据给工作站使用。中间的网络包含三个接入点，使用较低的功率运作。由于将覆盖区域分割为较小的独立无线电区域，因此可以提供更多的吞吐量。粗略而言，将有90 Mbps用来服务工作站。至于图右的网络，虽然只有一个接入点，但却使用分区天线（sectorized antenna），相当于三支定向天线。在某些实现中，每个分区会被指定不同的信道，如此一来也可以减少工作站在传输时发生冲突的机会。在最复杂的情况下，分区天线的每个信道可被当成独立的接入点，工作站可用的总吞吐量亦为90 Mbps。传输质量也可以用“服务区的单位平方英尺（per square foot of service area）可提供多少megabit来衡量，这和服务区的可用吞吐量总和并不冲突。

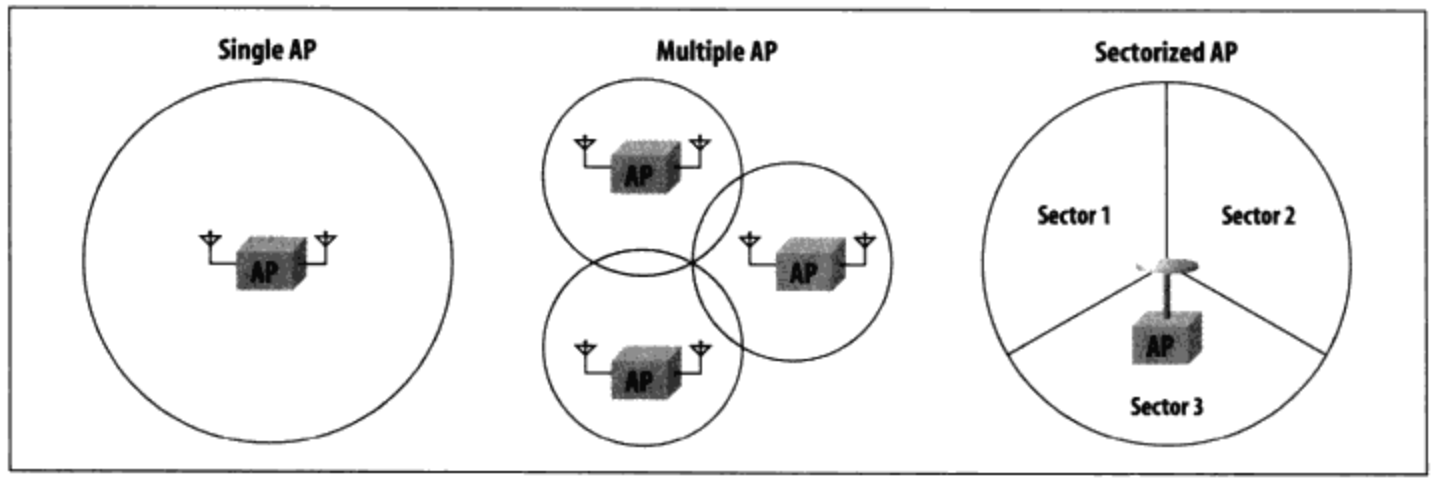


图 23-3：服务区总吞吐量图示

在Ethernet领域，交换器可以通过减少媒介竞争来提高网络的吞吐量。提升无线网络可用容量的做法也采取同样的方式。缩小每个接入点的覆盖范围，就可以在单一服务区域部署更多接入点。虽然关于所谓的“Wi-Fi交换器”的宣传不断，但都是基于同样简单的设计原理。当网络中的组件变多时，网络管理就变得比较困难，为了将复杂度集中于几个定点，最好不要到处使用聚合设备（aggregation device）。

注意： 基本上，无线局域网络必须在覆盖范围与服务质量之间作出取舍。提升质量的同时，也必须缩小每个接入点的覆盖范围。

工作站的限制

业界所面临的一个主要挑战，乃是绝大部分的802.11操作均掌握于工作站及其所使用的软件手中。

几乎所有支持移动性的“重要”协议操作都掌握在工作站手里。由客户端软件决定何时漫游、如何扫描新的接入点以及何时连接至网络。在网络中，不同机器会出现不同的行

为，因为802.11并未规定何时漫游或如何挑选接入点的算法。把这么多协议交给工作站实现，它却又不受任何标准规范，因而导致工作站的行为通常十分神秘。举例来说，可以准备三部膝上型计算机，插上802.11接口卡后置于一台车上四处闲晃。这三部计算机将在不同时间漫游至不同的接入点，而且通常会表现出不同的行为。未来的标准（特别是即将到来的802.11k）应该有助于改善漫游决策的质量。

以“决定关联至网络的工作站”为例。大多数情况下，首度启动时，工作站会进行比较智能的扫描，挑选信号最强的接入点加入。对许多网卡而言，它们的智能就到此为止。它们将持续与第一部接入点连接，即使附近出现更合适的接入点。除非完全丧失信号，否则没有什么可以强迫网卡进行漫游。这种行径通常被称为“捕虫灯效应”(bug light)，因为工作站就像是被灯火所吸引的飞蛾，无法抽身。具有捕虫灯效应的工作站的传输率特别差。就算它们已经远离原本联机的地点，还是会降低速度只求维持联机。

如此一来不仅拖累远距离工作站的联机速度，也大幅减少了其他工作站的可用容量。低速传送时，以OFDM PHY（802.11a或802.11g）封装的最大封包（1500 byte）需要更长的传输时间。在最极端的情况下，以54 Mbps传送最大帧需要用到57个数据符号，相当于248微秒；而以6 Mbps传送时，则需要用到512个数据符号，相当于2068微秒，亦即8倍以上的时间。较慢的传输速率剥夺了其他工作站1800微秒的传输时间。

将这么多攸关整体的协议操作交付工作站处理，限制了网络基础设施在必要时采取最佳手段的可能。举例而言，蜂窝网络能够将移动电话转交给具有较大容量的接入点处理。无线局域网络协议尚无此种能力。有些无线局域网络系统厂商已经提供“接入点负载平衡”（AP load balancing）功能，宣称可以让网管人员合并两个接入点，为所在地区提升整体的网络性能。一种常见的做法是监视每个接入点的关联数或者各接入点的流量，然后将工作站自负载较高的接入点取消关联，鼓励它们转移至负载较轻的接入点。但如果得不到工作站的支持，将很难达到负载均衡的情况，因为大多数工作站还是倾向于关联回原先的接入点。

注意：不论何时何地，漫游均属客户端现象。由于决策掌握于客户端软件，网络设备对于改善用户状况就只能做到这些。

切合期待的吞吐量

当更多用户加入无线局域网络时，网络容量必须平均分配给更多用户，因此吞吐量就会下降。对采用DCF（分布式协调功能）的网络而言，比较实际的经验法则是大约可以达到50%~60%的额定速率，因为必须将帧间间隔、前导码以及帧头等额外的负担纳入考虑。网络协议额外增加了网络层成帧与重传的负担。大多数网络协议所面临的共同难题

是，要提供稳定的传输就必须使用传输层确认机制。每个TCP段均必须得到确认（虽然不见得是个别确认），而TCP确认信号又可能与其他正在传送的段产生冲突（注3）。表23-1依经验法则列出了每种接入点的网络容量。

表23-1：根据经验法则推测各种802.11技术的网络容量

技术	最大容量
802.11直接序列	1.3~1.5 Mbps
802.11b	6 Mbps
802.11g，使用保护机制	15 Mbps
802.11g，未使用保护机制	30 Mbps，虽然比较少见
802.11a	30 Mbps

在设计上，跟“服务质量”（QoS）有关的技术通常是尽量榨出更多的网络容量，但并未得到广泛部署。如果QoS的历史有任何值得借鉴之处，那就是“说之者众，用之者少”。

802.11n及后续标准

超越54 Mbps后802.11将何去何从？当802.11a与802.11g标准出炉，产品开始出现在市面上时，“下一步往何处去”的问题就会开始浮现。

2003年，IEEE 802.11工作组成立了一个高速研究小组，开始探究如何进一步提升无线局域网络的速度。TGn（任务组N）正致力于开发一种标准，希望在扣除其他协议所造成的负担后，能够达到100 Mbps以上的净吞吐量。而任务组的目标是超越100 Mbps，看来似乎不难达成原先设定的目标。目前任务组手中有两份彼此竞争的提案，在第十五章已经有所说明。两者均使用“多进/多出”（multiple-input/multiple-output，简称MIMO）技术来提升速率。粗略而言，其中一种提案致力于提升最高数据率，另外一种则是维持较低的最高数据率而侧重于提升无线链路的性能。

每个接入点的用户数

规划网络时，必须知道每个接入点的用户数的多寡。802.11限制每个接入点最多只能有2016个工作站与之关联。实际上，每个接入点的可关联用户数远低于此。

对802.11b而言，6 Mbps的实际容量算是合理的假设。要为每个用户提供1 Mbps的联机速度，乍看之下，每个802.11b接入点似乎只能服务6个用户。不过，网络流量原本

注3：我曾听过一个估计数字，据说只要在网络层与传输层使用TCP/IP协议组，大概就有10%左右的帧需要重传。

就有高有低（bursty），根据流量模式，自然可以假设能够服务更多的用户。为每个用户提供1 Mbps的联机速度是基于“用户有时会处于闲置状态”的前提。我发现3:1至5:1大概是较合理的比例。依此比例，一个802.11b接入点最多能够服务20至30位用户。

然而，就算升级到802.11a或802.11g，每个接入点所能够服务的用户数也不会因此而更多。在802.11中，速度取决于距离。工作站距离接入点较远，就会转而使用较稳定但速度较慢的编码方式进行传输。只有距离接入点相当近的地方才可能使用较高的速度，因此每个接入点服务20至30位用户仍然算是合理。

如果你的应用对网络特性十分敏感（例如VoIP），每个接入点所能够服务的工作站数量就会更少。无线网络尚无法对复杂的服务质量进行优先级排序，只能依赖媒介本身对工作站的访问进行仲裁。语音与数据的特性有别。当媒介达到饱和且接入点使出浑身解数倾泄出队列中所有数据时，将可达到最高的数据吞吐量。语音帧必须及时传递且队列必须尽量维持为空的，才有办法接收高优先级的帧并立即传送。不论是直接使用802.11链路还是通过IP传送，语音流量对于延迟或剧烈的抖动（jitter）均十分敏感。为了避免不必要的延迟，在更好的QoS技术来临之前，必须进一步限制使每个接入点只能服务8至10个电话听筒。

移动性的需求

无线局域网络已经不再是玩家专属的新奇玩物。几年前，当用户移动到不同位置时网络仅需重新进行自动配置设定，这还可以接受。当无线局域网络日渐成熟时，用户开始期待不论身在何处，网络均能够提供不间断的联机。

连续的覆盖范围与无间隙的漫游应该是园区环境的常态。用户可能以无法预料的方式移动于园区之内，但仍然希望持续使用网络且联机不致中断。一般而言，只要未动用交通工具，用户就会认为无线局域网络仍然可用。为整个园区设计覆盖范围时，必须考虑到用户可能跨越路由器的界限，因此设计时必须考虑如何维持他们所使用的地址，通常是通过某种形式的点对点隧道协议。不同的无线局域网络架构有不同的点对点隧道方式。详细的讨论参见第二十一章。

网络集成的需求

网络规划有两个要素。首先，物理集成（physical integration）纯粹是一步一脚印的工作。除了建筑蓝图，如果可能，最好取得实际的网络架构图。省去昂贵费时的布线工夫，安装无线局域网络硬件变得简单不少。知道现有配线柜的位置与内容是重要的第一步。逻辑集成（logical integration）是第二个步骤，它包含如何将无线局域网络集成至现有的网络。

物理集成

物理集成包括如何将各个元素摆到正确的位置。接入点必须根据事先的规划摆放并正确地布线。如果考虑到美观因素，新增设备时或许需要重新布线；否则，从现有的插槽接线到接入点所在位置即可。根据所选择的产品与架构，网线可能是接到接入点控制器、特殊的 wireless VLAN 或是配线柜中的网络。

除了配线，还得供电给接入点。在接入点所在位置直接供电并无不可，但不建议这么做。许多企业级接入点的设计主要是通过 Ethernet 网线供电，甚至连外接电源都没有提供（有些接入点是另外提供48伏特的外接电源，亦即其电源电路被设计成运作在PoE的电压上）。有些交换器可能具备“Ethernet 供电”（PoE）的能力，但使用前必须检查与确定是否兼容。符合 802.3af 标准是电源兼容的最佳保证，不过各位手上或许有些设备是厂商的专属规格。如果必须由配线柜提供电源，可以购买其他厂商所生产的馈电器（power injector）。

逻辑集成

进行无线局域网络的逻辑集成之前必须先挑选一种架构（参见第二十一章）。不同架构有不同的集成需求。不过，一般而言，无线局域网络至少必须连接到某个网络。若要连接至一个以上的网络，或许必须使用以AAA 为基础的动态网络分配（dynamic network assignment）。这些网络绝大部分属于 IP 网络。不过有时候，无线局域网络也需要支持旧式网络协议。

网络规划的第二个要点是思考逻辑网络的变动。移动式工作站该如何寻址？如果所有无线工作站使用单一 IP 子网络，则必须为之分配 IP 地址空间并确定它能够被正确路由至无线子网络。分配新的地址空间时，切记为所有接入点与其他辅助设备留点额外空间。切勿禁不起诱惑地采用地址转换（address translation）。虽然有些应用程序可以配合 NAT 一起使用，但未来的应用程序如果不认得 NAT，就会造成潜在的问题。在 NAT 普及之前已经写成的应用程序也可能无法使用。

扩充网络时必须新增接入点设备。接入点或许需要 IP 地址。如果接入点的地址是通过 DHCP 取得，那么最好在 DHCP 服务器中为每个接入点指定固定的地址，不要让 DHCP 服务器随机指派。如果接入点通过 IP 隧道（tunnel）连回中央控制器，各位或许必须设定一些过滤规则来让双方得以进行传输，并且分别在接入点与中央控制设备上设定必要的传输隧道。

物理层的选择与设计

802.11物理层的选择通常由用户需求而非物理设计所驱动。大多数情况下，它也会受到“打造最快网络”的需求驱动。物理层的选择关系到工程。物理层本身并无优劣之分，选择物理层时，其实是在一些不同的因素间进行取舍。总而言之，2.4 GHz ISM频带比较不受障碍物的影响，因此802.11 b/g信号的传输距离较远。不过，吞吐量会受到向下兼容性的限制，而且很难只用3个信道来规划网络。此外，使用2.4 GHz ISM频带的设备并不少，很可能受到某些设备，例如Bluetooth、2.4 GHz无绳电话、X10摄影机或其他类似设备的干扰。即使干扰不存在，只能使用3个信道也会限制吞吐量，如果信道与其他网络重叠的话。802.11a比较适合高密度、高容量的网络，除了不受向下兼容性的限制，能够使用的无线电频谱也比较宽。表23-2展示了2.4 GHz与5 GHz 802.11网络的比较。

表23-2：2.4 GHz与5 GHz 802.11网络的比较

	802.1b/g (2.4 GHz)	802.11a (5 GHz)
单一接入点的性能	802.11b较低；802.11g中上	各信道均可提供最大吞吐量
单位面积的潜在性能	低。只有3或4个信道可用，信道重叠与干扰实际上无可避免	高。信道较多，亦即网络元素间较不会造成自身的干扰
距离	较低的频率可以传送较远的距离	较糟。较高的频率有较高的开放空间路径损耗
干扰	不少设备使用相同频带	较少有使用相同频率的设备
	信道有限，导致许多共享信道干扰	信道较多，比较容易规划，特别是在三维空间
与旧硬件的向下兼容性	兼容于802.11直接序列与802.11b硬件	不兼容

要减轻大规模无线局域网络部署的负担，方式之一是尽量自动化。有些产品可以自动规划信道，其中一种做法是根据实际的测量结果来进行信道规划。网管人员可根据用户密度、安装的难易度以及环境的限制来摆放接入点。网络启用后，接入点就会通过有线网络相互通信，以便选择最佳的信道分配。有些产品会持续监控无线电波，依环境的变化来动态调整信道的设定。除了实际测量，另外一种替代方案是为建筑物建立虚拟模型。为建筑物建立虚拟模型时，可以利用数学模型将干扰降至最低并根据计算结果来分配信道。和无线局域网络设计的其他方面一样，有些产品会同时采用这两种技术。

2.4 GHz（802.11 b/g）信道规划

802.11b 与 802.11g 共享相同的频带。两者适用相同的管制要求，也使用相同的信道表（表 23-3）。虽然最多可以有 14 个信道，但每个信道只有 5 MHz 宽。直接序列传输被扩展开时，所跨越的频带会宽于指定的信道（参见图 12-5）。要得到最佳的效果，第一与第二个旁瓣最好不要受到干扰。理想情况下，信道之间最好相隔 33 MHz。

大多数管制区的无线电频谱并不足以分配给 3 个完全不相重叠的信道。大多数用户宁愿容许在第二个旁波瓣稍微重叠，这样起码有相距至少 25 MHz 的 3 个信道可用，不致于只能使用两个完全不相干扰的信道。如此一来，就可以得到 1、6、11 的信道组合。虽然每个信道会稍微受到干扰，不过牺牲一点吞吐量换得第三个信道还是十分值得的。

有时候，四信道的分配（1、4、8 与 11）也有其用途（注 4）。不过代价是信号重叠的部分更多，最高吞吐量也会因此降低。虽然牺牲最高传输速度（peak speed）以换取较高的整体速度（total area speed）在某些情况下是值得的，不过我个人认为并不划算。

表 23-3：不同管制区域所使用的无线信道

信道编号	使用频率（GHz）	美国 / 加拿大[a]	ETSI[b]
1	2.412	✓	✓
2	2.417	✓	✓
3	2.422	✓	✓
4	2.427	✓	✓
5	2.432	✓	✓
6	2.437	✓	✓
7	2.442	✓	✓
8	2.447	✓	✓
9	2.452	✓	✓
10[c]	2.457	✓	✓
11	2.462	✓	✓
12	2.472		✓

a: 802.11 标准允许美国与加拿大使用不同的无线电频谱，不过美国 FCC 与加拿大产业部采用相同的规范。

b: 并非全欧洲均采用 ETSI（European Telecommunications Standards Institute）所建议的规范，例如西班牙（本表并未列出）就只能使用信道 10 与 11。

c: 所有管制当局均允许使用信道 10，因此大多数接入点会将之作为默认信道。

注 4： 欧洲可以使用较宽的信道间隔，例如使用 1、5、9 与 13 的四信道部署。

实地勘探的部分目的是为了在规划覆盖范围时能够尽量避免信道重叠。天线的价值在此浮现，因为它们可以调整覆盖范围，使之符合建筑物或房间的形状。不论选用何种天线，均可采用一种通用的模式。移动电话产业使用“六角模式”（hex pattern）作为信道规划的基础。图23-4显示了规划大型覆盖区域时不可避免的问题。从不相重叠的3个信道中挑选其一作为中心信道，以黑体字表示。本例中，我随意挑选信道1作为中心信道。为避免重叠，中心信道四周必须使用其余两种不相重叠的信道。为四周选定信道后，就可以接着规划其他中心信道。图23-4中，可以看到另外两个以圆圈标示的中心信道。

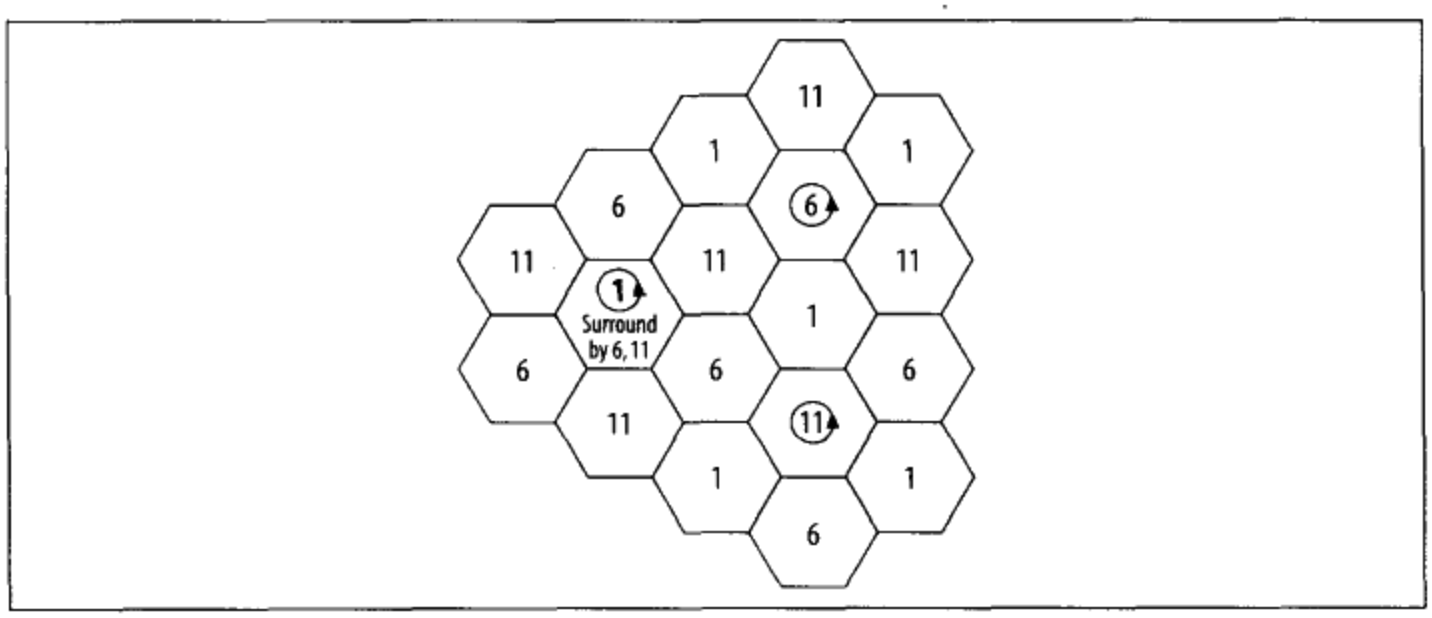


图23-4：频章规划

当然，图23-4所呈现的是理想环境中的信道配置。在建筑物中，无线电的传播不仅受到障碍物的影响，信道重叠的情况也通常无可避免。举例来说，中心信道1外环的信道6与信道11就可能互相干扰。

2.4 GHz信道规划的限制

只有3个信道而无法进行信道规划并不令人惊讶。数学上有所谓的“四色地图定理”（Four-Color Map Theorem）。早在19世纪中期就已经发现，绘制任何二维地图至少需要4种颜色（注5）。遗憾的是，802.11 b/g网络只有3个不相重叠的信道。地图的相邻区域若使用同样的颜色便难以分辨。相邻接入点的覆盖区域若使用同样的信道亦然，而且因为共享信道的干扰，必然会影响双方的吞吐量。

要将信道的重叠程度降至最低，通常必须仔细调整接入点的摆放位置或借助外接天线，

注5：在Cray超级计算机的协助下，经过1200小时的运算，终于在1976年证明了“四色定理”（Four-Color Theorem）。它是最早通过计算机辅助得到证明的定理之一。

不过得付出不少时间与精力。在三维空间里，那就更不容易了。而无线电信号可能穿透地板或天花板，因此规划信道时必须考虑到三维空间。

即使在宽广、开放的平面空间，在各位认为绝无可能的地方还是会出现意外的干扰。2002年，Associated Press在一篇有关干扰问题的报道中提到，Florida附近居然成立了自己的ad-hoc频率分配委员会，以确保左邻右舍不致使用相邻信道！

GHz（802.11a）信道规划

以802.11a规划网络有两项主要优点。首先，802.11a起码有12个信道，因此信道规划不成问题。表23-4显示了各信道的频率。必须注意的是，有些早期的802.11a网卡并不支持最高频带，因此信道149及以上的信道并不适用于所有网卡。如果遇上这种情况，不是换掉旧网卡，就是只能使用其他8个信道。不论是8个还是12个信道，对二维空间的规划而言均绰绰有余。至于三维空间，只要小心规划，大多数情况都不成问题。

表23-4：802.11a信道（附注美国管制规定）

信道编号	使用频率（GHz）	备注
36	5.180	最低的最大功率
40	5.200	最低的最大功率
44	5.220	最低的最大功率
48	5.240	最低的最大功率
52	5.260	稍高的最大功率
56	5.280	稍高的最大功率
60	5.300	稍高的最大功率
64	5.320	稍高的最大功率
149	5.745	并非所有网卡均支持
153	5.765	并非所有网卡均支持
157	5.785	并非所有网卡均支持
161	5.805	并非所有网卡均支持

混合式信道规划（802.11a+b/g网络）

大多数网络通常一并使用802.11 b/g以便兼容旧硬件，而以802.11a作为未来扩充之用。有些厂商推出的双模接入点只比单模的贵上一些。有时候，三模/双频网络的建设成本只比单纯的802.11g网络多出几百或几千美元。除非预算很紧，否则多付一点成本就可以让带宽加倍，其实是十分划算的。

在可预见的未来，大多数802.11设备还是会使用2.4 GHz频带。大多数芯片组厂商还是专注于生产802.11g设备。市面上一些三模芯片组同时支持802.11a与802.11b/g，不过尚未广泛内置于膝上型计算机。当初我所建设的Supercomputing无线网络同时间最多会涌进1300位用户，其中只有100位使用802.11a。随道芯片组与无线网卡的价格持续滑落，802.11a会逐渐为大众所接受，我预计室内将大幅改用802.11a。至于户外环境，传输距离还是主要的考虑因素。频率越低，传输距离越远，因此在户外仍然将由802.11b/g维持目前的领导地位。

接入点摆放位置规划

目前，大多数用户认为有线网络“就是可行”（just work）。在产品的成熟度与可预测性方面，无线网络还是有所不及。无线网络所使用的协议还是有点难以预测，有些较新的协议甚至需要你卷起袖子亲自动手。规划网络时有一堆工作必须优先进行。由于无线网络让用户得以不受空间限制访问资源，因此网络本身必须清楚掌握用户所在位置。

一旦了解用户需求与决定采用何种802.11物理层后，接下来的问题就是应该将接入点置于何处，这取决于需求与预算。决定接入点的摆放位置可能只需要几个小时，也可能需要来回进行好几次，花费大量的时间与金钱。此过程之所以称为实地勘探，是因为有一些工作必须在网络的安置地点进行，不过新一代的工具已经可以通过计算机模拟来取代不少接入点摆放工作。

有几个选项可用来判断应该将接入点置于何处。对同意列名于“使用客户名单”的早期采用者，厂商可能愿意提供实地勘探服务，虽然在本书付印之前，成为早期用户的时机早已消逝。增值经销商或许也有能力进行详细的实地勘探，经销商可将实地勘探当作顾问服务来销售或以之作为成交的筹码。有些专门从事技术教育训练的公司也会提供类似的课程。

建筑物

建筑物的构造乃是限制接入点摆放位置的主要因素之一。墙壁、门窗都会影响无线电信号。取得楼面设计蓝图并及早实地勘探对网络规划有极大的帮助。有时候，各位也许有机会针对施工中的建筑物进行规划。这时候必须把握每一次实地勘察的机会，因为在墙壁砌起之前可以更清楚地掌握建筑物的内部结构。为施工中的建筑物进行规划的主要缺点是，除非等到建筑物完工，否则无法进行各项实验。

一旦取得楼面设计图，就可以评估信号必须涵盖哪些地方。如果建筑蓝图十分完整并且包含布线信息，应该会同时记录就近的电源插座。各位也可以初步观察有哪些结构可能造成问题，例如通风管（ventilation duct）或者以钢筋混凝土砌成的墙面。

不论是否使用电子仪器让规划过程自动化，都应该在现场再次确认。看看是否有蓝图未曾记载的变更之处。确认现场所使用的建材。除非是老建筑或古迹，否则墙壁通常采用轻隔间材质（sheetrock hung from stud），只要敲敲墙面就可以得到验证。问问看是否有防火墙（实际的防火墙，不是网络防火墙），因为防火墙对RF信号会造成相当大的影响。结构或承重墙可能是钢筋混凝土材质，这将对电波形成极大的障碍。如果必须将接入点隐藏在特定地区，就该彻底研究如何隐藏以及对网络操作有哪些潜在的影响。此外，对挑高的天花板或者其他难以安置的地点也必须加以查看。在巡视过程中，可能会有来自四面八方的异样眼光，不要在意，继续前进。完整巡视一遍，可能会得到不少异样的眼光。就将它视为此行的绩效指标吧。

根据第一次实地勘探记录下所有相关的环境因素。最重要的是，各位可以根据结构的变更修正蓝图，毕竟蓝图绘制之后的变动通常不会记录，尤其是老建筑。同时，最好记录下潜在的干扰源。2.4 GHz ISM频带无需使用许可证，因此对于使用该频带的各种设备可能并未统一管制。新型的无绳电话(cordless phone)同样使用2.4 GHz频带，Bluetooth与一些其他无线设备亦然。如果预料到干扰源不少，可以使用频谱分析仪在无线局域网络频带测量辐射量。事实上，除非是特别强的干扰源，否则不必每次都使用频谱分析仪。一种名为Berkeley Varitronics YellowJacket的手持分析仪内置了2.4 GHz ISM频带的频谱分析仪，可用来追踪非802.11信号的干扰。

如果贵单位在进行RF测试，必须为实验室加上屏蔽以免干扰无线局域网络。依经验法则，接入点的摆放至少要远离较强的干扰源25英尺。

接入点摆放位置的限制

实际上，“尽可能将接入点置于高处”意味着最好将它们摆在天花板的高度。许多办公建筑使用“倒吊式”（dropped）或“悬吊式”（suspended）天花板。接入点可以安装在天花板吊杆（ceiling mounting bar）或者置于天花板之上。必要时，可将接入点置于所有办公室隔断（cubicle）之上。不妨跟厂商确认接入点的辐射模式（radiation pattern）。如果接入点原本的设计是从天花板向下传送无线电波，将它们置于办公室隔断之上就无法达到预期的效果。

比较常见的做法是根据实际限制来调整接入点位置。主要限制因素之一在于接入点通常通过Ethernet电缆连接至网络（注6）。离接入点最近的配线柜不能超过100米。由于规范较具灵活性，有时候网线可以比规范限制的稍长，但总不能永远心存侥幸。它取决于

注6：少数产品可以使用第二种无线电构成“网状”回程线路（“mesh” backhaul），预料这项功能将会日渐普及。

插线（patch panel）、支架（riser）与天花板的布线，实际上需要使用较长的网线来连接接入点。

电源通常是接入点摆放的另外一项限制因素。早期的接入点需要用到电源插座，不过机构很少会在天花板上安装电源插座。安装电源插座通常所费不菲。随着802.3af的发展，有些组织开始通过网线为接入点供电。Ethernet供电（Power over Ethernet，简称PoE）的优点不少，不过，要让100米的网线维持48伏特的电压，本身就有工程上的难度且无法在电缆长度方面投机取巧。

为无线网络布设新的网线是值得考虑的，特别是如果现有的网络插座无法轻易支持新的接入点时。现有的网线通常在脚板（baseboard）附近，不适合用来连接高挂式网络设备。铺设新的网线有许多优点。它可以直接拉至接入点所在的天花板，如此就不会露出极丑的网线。旧式布线或许在Category 5线材成为标准前就已经存在。布设新的网线也可以增加某种程度的灵活性。考虑到有时需要移动接入点，有些新式布线会在天花板的网线终端加装网络插座，允许使用跳线（patch cable）让接入点移动至附近。

根据天花板上的组件配置，有时很难沿着通风管布线或将接入点置于通风管附近。通常，只要将接入点稍微挪至下一块天花板的位置即可，这并不会严重影响接入点的覆盖范围。此外，让接入点远离灯具及其电源线也很重要。

最后的考虑因素与实体的安全性有关。有些机构认为必须为接入点加上防盗措施。有时候，将接入点安装于天花板就算防盗措施，毕竟已经将接入点隐藏起来。有些接入点附有防盗锁孔，可将之固定在无法轻易移动的物体上面（注7）。

施工中的建筑物

随着无线局域网络的普及，许多无线网络在建筑施工期间就已经开始着手设计。为施工中的建筑物设计无线局域网络不仅有许多乐趣，也是不小的挑战。

首先碰到的问题是会受到其他工程进度的影响。幸运的是，可以借助模拟工具来估计所需要的接入点数目。施工图通常十分完整，而且通常在实际动工前网络小组就可以取得相关图纸。一开始，可以先评估不同材质可能造成哪些影响并且建立初步的模型。

当建筑物逐渐成型，就可以到各个区域巡视一遍。根据施工进度，实地勘探可以分几个阶段进行或者一次解决。在施工期间进行勘查，通常需要得到承包商的首肯、安全帽外加放弃申诉抗辩的权利（liability waiver）。在建筑物各个区域确认一下模拟阶段所做的

注7：Kensington防盗锁孔（Kensington Security Slot）的相关信息详见*http://www.kensington.com/html/1356.html*。

假设是否正确。例如，赋予各个墙面的电波损耗系数是否正确？当初所构建的模型是否需要修正？完工后，就可以将接入点置于定位进行实际测试，进一步校验“模拟工具”当初所做的预测是否正确。

为施工中的建筑物设计无线局域网络的最大挑战之一就是环境处于持续变动的状况。在比较少见的情况中，可能会因为少料甚至是美观上的考虑而于最后关头更换建材。记得尽量让设计保持灵活性并且预留一些安全空间以防错误发生。

初步规划

决定接入点的数目与初步摆放位置是规划的第一个里程碑。几年前接入点还十分昂贵，当时决定初步摆放位置的最佳方式是估计需要几个接入点，然后将它们集中置于开放空间。如今接入点已经相当便宜，尽量减少接入点数目已经不再是主要的考虑因素。

根据两项经验法则，可以粗略估计出所需要的接入点数量。第一项经验法则是根据区域来计算。在典型的开放式办公室环境，以最大功率传输的接入点可以覆盖3000至5000平方英尺（275至400平方米）的区域。只要知道打算覆盖多大范围，将之除以每个接入点的覆盖范围（footprint）即可。鲜有障碍物的开放空间可以取较大的数目；封闭隔间的办公室或者内部结构复杂的建筑物就要取较小的数目。除了区域大小，也可以根据用户密度来估算所需要的接入点数量。依经验法则，可以将组织中的用户数除以20至50。如果无线网络十分受欢迎且广为使用，就可以除以较小的数目；如果无线网络对用户而言仍属新鲜物且属于实验性质，就可以除以较大的数目。这两个数目取其大者，就可以粗略估计出应该安装多少个接入点。

至此只是粗略知道需要多少接入点，不见得知道应该将它们摆放至何处。要将这些粗略的估计转换为初步计划还需要不少工作。如果经验足够，那么不难判断应该将接入点置于何处。结构墙或防火墙通常会完全阻断信号。多层建筑的主要承重结构通常位于中央核心，而且通常使用钢筋混凝土材质。以每英尺10 dB至20 dB的衰减计算，通常可以将之视为一种RF屏蔽。当信号穿越两至三间一般大小的办公室，大多数接入点仍然能够维持运作在最小速度之上，这取决于中间障碍物的多寡。一般而言，尽可能将接入点摆在障碍物较少的开放空间。要让接入点能够随时提供必要的服务，最好将接入点置于办公室隔断与走廊之上。

到目前为止，制定初步计划通常是依赖人工方式，需要高度的技巧与广泛的经验。过去几年开始出现了一些模拟工具，可将初步规划过程自动化。这些工具将依照建筑物的工程图创建无线电传播的数学模型。当网络设计师变更模型中的接入点摆放位置时，此工具就会立刻重新计算出接入点的覆盖范围。这类电子工具很有价值，它可以合理推测出接入点的摆放位置，减少实际验证的次数。对于尚在施工的建筑物，这些工具更是特别

有价值。有些工具能够直接读取建筑设计图，亦即计算机辅助设计（Computer-Aided Design，简称CAD）文件。有些工具只接受简单的图形文件，例如GIF或JPEG。记得要取得建筑物平面图。建筑物平面图通常是由设备部门负责保管，也可以通过房东或业主取得。如果是新的方案，不妨直接向建筑师索取。

虽然模拟工具十分有用，但切记不要只是纸上谈兵。无线电传播十分复杂，特别是在室内的微波频带。无线电波对不同材质有不同的反应，只要隔个几英寸，覆盖范围就可能截然不同。要使用这些模拟工具，必须具备正确的建筑营造知识，但是网管人员不见得专精于此，故模拟工具并无法完全取代实际的实验。

不论使用何种技术，还是得从实体规划推衍出初步计划。此时尚不需要无线信道的细节规划。如果使用模拟工具，不妨让它提供一份提案，等到实际安装后再做修正。不过，初步规划就是初步规划，不要期待可以就此定案。这个阶段的目的并不是完成所有任务，只是取得一个切入点。表23-5依经验法则推算出了典型的全向型天线在不同空间的最佳覆盖半径。如果打算提供较高的传输率，覆盖半径就不能太大。最好的做法是借助本节所讨论的模拟工具。

表23-5：依经验法则推算不同类型空间可能的覆盖半径

空间类型	最大覆盖半径（2.4 GHz）	最大覆盖半径（5 GHz）
封闭式办公室	最多 50~60 英尺	35~40 英尺
开放式办公室（办公隔间）	最多 90 英尺	60 英尺
走廊与较大的房间	最多 150 英尺	75 英尺
户外（未进行天线工程）	最多 300 英尺	不用说
户外（使用定制天线）	好几英里	不用说

初步报告

初步计划可以作为进一步行动的基础。它可以用来估计在特定区域部署无线局域网络的成本。此外，也可以聘请布线承包商根据初步计划来实际布线。计划本身可能包含：

1. 初期工作所搜集到的需求报告。
2. 根据实地勘探测量评估出的覆盖范围。覆盖范围可以细分为信号接收良好、信号接收普通与信号接收不良三种。根据数字模型所提出的报告可以勾勒出不同传输率的大概轮廓。
3. 描述各个接入点的摆放位置及其相关配置。有些自动规划方面的软件工具能够根据楼面图提供详细的位置与设定信息，例如：

a. 接入点的操作信道。

b. 最大覆盖范围，或许是以“不同速度的覆盖轮廓”来表示。

c. IP配置，如有必要的话。“轻量级接入点”可能没有IP地址。

d. 天线类型与配置，包括定向型天线所指的方向。

e. 产品特有的信息。有些机构会根据MAC地址来追踪设备，因此在报告中附上相关信息就十分有用。

无线电资源管理与信道规划

图23-4容易造成一种错觉，让人误以为信道规划十分简单。打造室内网络时信号的传播其实复杂得多。信道重叠的情况通常发生于室内，因为必须使用较高的功率方能穿透障碍物，因此到处充斥的信号功率均高于要求。

初步计划应该包含基本的信道表（channel map）。可以确定的是，信道规划必然需要进一步调整。进行调整时，可以使用手持式工具以手动方式找出重叠的信道，或者让接入点自动搜寻最空闲的信道。既然2.4 GHz频带只有3个信道可用，任何变动都可能在网络中造成“骨牌效应”（ripple），故需要花费一些时间以得到最终的解决方案。

规划的修正与测试

根据所要求的精确程度以及预算，计划的修正过程可大可小。在小型或预算很紧的项目中，只要有初步规划，启用网络后视后续发展如何即可。比较慎重的部署可能会依初步计划安装部分或全部的接入点，然后进行一连串的测试来验证是否符合需求。如果初步计划十分精确，或许不需要任何修改，测试的主要目的在于找出之前未曾发现的干扰或死角，再据以重新设计。大多数情况下，干扰问题可以通过接入点的重新摆放来解决。接入点的摆放位置通常不需要太大的调整。如果还是无法解决，可能就要更换不同的天线或接入点了。有时候，可能需要经过好几回合的设计与测试阶段，虽然这种情况比较少见。

检查计划时应尽可能复制用户经验。无线局域网络与接入点间的障碍物会使电波强度减弱，因此在实地勘探时应尽量复制原本的使用情况。测试时与完工后应该使用一样的天线。如果办公人员也会用到无线网络，记得确认一下关起门后是否还能够合乎信号接收上的要求。更重要的是记得关上金属百叶窗，因为金属物质最容易影响无线电波。

信号测量应该符合网络用户的期待，只有一项例外。大部分实地勘探工具是以某个定点根据几个特定时点的数据来分析信号质量，因此在实际进行测量时，记得将膝上型计算

机置于定点。务必多测量一些数据，因为用户会带着膝上型计算机四处移动，而且多径衰落效应可能会导致信号质量有相当的落差，即使只是相隔几步的距离。

比较严谨的机构可能会测试不同的客户端设备。无线局域网络会因实现上的差异而有截然不同的表现，就算使用完全相同的软件，工作站也会显现出截然不同的行为。如果需要知道系统的实际表现，就要对软件使用相同的配置设定，在同一时间进行相同的测试以便多搜集几个系统的信息。

最后的测试报告应该包含接入点的最后摆放位置以及确实的覆盖范围。覆盖范围可以用地区来表示，虽然附上各区域能够稳定提供的传输率可能更为有用。有时候，性能特性报告也十分有用，特别是应用程序的组合具备某种特性时。

如果建筑物尚在施工中，验证过程就必须等到完工后进行。如果整栋建筑物同时施工，最好及早进行基本的测量操作，以便判断是否需要大幅修改无线电模型，将费时、校验正确性的验证测试留到最后。

验证与测试工具

过去，要得知接入点的覆盖范围与完成接入点的规划相当费时，因为需要将接入点摆放至不同的位置，反复测量接入点的信号质量。随着自动规划工具的发展，那么不论是基于模拟还是自我调整机制，在验证阶段通常已经不必用到这些工具了。通常只有在发现测试系统遭遇问题时，才需要深入分析无线链路的性能。

最常见的信号质量测量项目就是封包（比较正确的说法是帧）错误率（packet error rate，简称PER）与接收信号强度指示（received signal strength indicator，简称RSSI）。帧错误率越低越好。过去，8%以下的PER就有办法提供可接受的性能。接入点较为密集的网络应该能够轻易达到5%或更低的帧错误率。比较复杂的基础结构型设备通常可以直接测量个别工作站的帧错误率以及RSSI与信噪比。能否达到较高的数据率，RSSI与信噪比是关键因素。必须通过特定的信噪比阈，才有办法以特定的数据率传送可辨识的帧。

少数工具可以报告“多径时间扩展效应”（multipath time dispersion），亦即测量信号经由不同路径的时间因素。延迟扩展（delay spread）越大，信号的相关（correlation）还原作业就越困难。如果延迟扩展较大，设备就必须接受较高的错误率或者减速使用较保守的编码方式。不论如何，吞吐量都会因此下降。延迟扩展越大，吞吐量就越低。测量多径传播没那么重要，不过这种用来搜集多径相关问题数据的工具还是颇有价值。

当802.11b还是无线网络的主流时，市面上有许多针对便携式运算平台（如Compaq的IPAQ）开发的手持式工具。不过随着802.11a与802.11g的普及，手持式设备就逐渐失

宠而为Tablet PC所取代。大多数手持式设备使用较慢的外部接口，无法跟上新标准的数据率。举例来说，IPAQ使用16位的PC Card接口，频率只有8 MHz。虽然这种速度对11 Mbps的802.11b接口而言已经足够，不过较高速的802.11a与802.11g就得使用CardBus接口。Tablet PC在验证阶段还有另外一个优点。它可以执行许多初步规划可能会用到的工具，包括可以执行验证软件来搜集实际的测量信息以及将这些验证测量数据和之前所计算出来的预测值进行比对。

特别难缠的干扰有时候必须动用频谱分析仪，方能找出非802.11网络的干扰源。它是能够扫描大范围的频带以找出信号传输来源的设备，并不便宜。如果不愿花几美元，可以请个咨询顾问，或者使用限定于ISM频带的频谱分析仪来追踪干扰源。不论如何，频谱分析仪都是最后的手段，只有最难缠的问题才需要用到。

RF指纹的搜集

有些无线局域网络系统需要搜集上一章所提到的RF“指纹”(fingerprint)。只有在接入点已经置于最后位置时方能进行指纹的搜集。之后，就可以将测试设备摆在特定位置上，让系统搜集指纹。

准备最后的报告

在规划与测试过程中，应该准备初步文档来记录接入点的摆设位置。测试完成之后，必须以文档加以记录。如果初步计划是以电子文件形式存放，那么除了根据测试结果加以修正，也必须将变动纳入最后的报告。

除了接入点的摆放，有些客户还希望知道，将驱动程序安装至所有受影响的膝上型计算机需要花费多少工夫。影响的大小必须视客户所使用的管理工具的复杂程度而定。有时候，只要在报告的附录中附上一份驱动程序安装说明的副本即可。有些客户端会需要驱动程序的安装细节，以确定驱动程序安装时会自动对Windows Registry进行的任何必要的变更。

使用天线调整覆盖范围

有时候，接入点的覆盖范围必须涵盖某些“不合常理”的特定区域。大多数接入点均会使用全向天线，此种天线在各个方向的辐射范围均等。不过，有时候需要将基本的无线电覆盖模式从圆形调整为其他形状。通常，这牵涉到调整接入点的覆盖范围以符合特定区域的需求，或者提升信号以填满某个区域。随着接入点价格的大幅滑落，已经没有必要以天线调整覆盖范围，虽然这种做法仍有其重要意义。

过去，无线电设备厂商需要提供天线并确保系统符合免许可证频谱的管制规定。2004年7月，FCC放宽了管制规定，允许无线电设备厂商指定最大增益，让用户自行选购具有相同增益特性的天线（注8）。在此之前，无线电与天线必须一并送检，私自更换天线基本上是违法的。新的管制规定出炉后，制造商可以单独验证符合管制规定的系统，而一般用户可以选用任何符合管制规定的天线。举例来说，如果无线电系统制造商是以10 dBi的天线送检，用户就可以自行选购增益较低的同类型天线（例如8 dBi）并且合法使用它。

天线类型

无线网卡均内置天线，不过这些天线只能算是差强人意。如果打算在整个办公室甚至更广的范围内（如公司园区）接收信号，就必然得为接入点加装外接天线。考虑使用特殊的天线时，只需注意若干必要的规范：

天线类型

天线类型决定了本身的辐射模式，天线可以是全向型（omnidirectional）、双向型（bidirectional）或是定向型（unidirectional）。全向型天线适合覆盖较大范围时使用，双向型天线特别适用于走廊，定向型天线则最适合在建筑物或不同网络之间架设点对点链路。

增益

所谓天线增益，是指天线沿所指定的方向增强信号。天线增益的测量单位为dBi，代表相对于各向同性辐射体（isotropic radiator）的分贝数。各向同性辐射体纯粹是理论上的假设，代表任何方向的辐射均相等的物体。我从未见过无线网卡内置天线的增益规格，不过我猜可能为负数（亦即比各向同性辐射体差）。简易型外接天线的增益大约为3至7 dBi。定向型天线的增益有可能高达24 dBi（注9）。

半功率点波束宽

半功率点波束宽（half-power beam width）意指天线辐射模式的宽度，以天线辐射衰减至峰值的一半加以测量。半功率点波束宽是了解天线有效覆盖范围的关键。对高增益天线而言，半功率点波束宽可能只有几度。一旦离开半功率点波束宽的范围，信号通常会迅速衰减，这完全取决于天线的设计。不要以为半功率点波束宽与

注8：参阅文件04-165，其中修改了相关电信法规。网址为*http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-165A1.pdf*。

注9：如果仍觉不够，则顺便告诉各位读者，阿雷西博（Arecibo）射电望远镜的增益超过80 dBi。

全向型天线无关。典型的全向型（垂直）天线只有在水平面具有全向性，只要位于天线上方或下方，信号就会减弱。

就天线而言，我们探讨的重点几乎完全放在传送特性上，主要是因为一般人比较容易理解。值得庆幸的是，天线的接收特性与传送特性相同。不论是接收还是传送信号，天线所起的作用是一致的。这个结果或许在各位意料之中，不过如何证明它就已经超出本书的范围。现在，让我们看看现有的天线类型（图23-5显示了各种类型的天线）：

垂直天线

这是相当普通的全向型天线。大多数厂商均会销售各种类型的垂直天线，主要差别在于增益不同。垂直天线所宣称的增益由10 dBi至3 dBi不等。全向型天线如何产生增益呢？要记得，垂直天线只有在水平面才具备全向性。在三维空间里，其辐射模式类似甜甜圈。较高的增益意味着该甜甜圈经过挤压，也意味着天线较大且较为昂贵，不过802.11服务所使用的天线并不大。

如果打算涵盖特定的户外区域，例如公司园区的几栋建筑物之间的中庭，就不适合使用悬挂在屋顶的垂直天线，特别是在建筑物本身相当高的情况下。由于本身半功率点波束宽的缘故，垂直天线比较适合水平辐射，向下辐射的能力就不是那么好了。如果遇上这种情况，最好将天线置于一楼或二楼的窗户外面。

偶极天线

偶极（dipole）天线具有“8”字型的辐射模式，适合用于走廊或较狭长的地区。实际上，它和垂直天线看起来没有什么两样。事实上，有些垂直天线不过是直立组装的偶极天线。

八木天线

八木天线（Yagi）是常见的高增益指向型天线。它的形状有点类似传统电视天线，支架上悬挂着一排平行的金属片。然而，802.11服务中大概不会见到裸露的八木天线，因为商业用途的八木天线通常会封装在天线罩（radome）里。天线罩本身只是一层塑料外壳，用以保护置于户外的天线主体。802.11服务所使用的八木天线增益约在12至18 dBi之间。校准八木天线并不会比抛物面天线来得困难，不过还是需要一些小技巧。

抛物面天线

这是一种增益相当高的天线。由于抛物面（parabolic）天线具备相当高的增益（商用802.11抛物面增益天线最高可达24 dBi），相对的波束宽也就更为狭窄了。抛物面天线大概只能用来架设建筑物之间的链路。由于波束宽狭窄，因此对一般用户而言并没有太大用处。有些厂商宣称其所销售的抛物面天线传输距离可达20英里。默认情况下，链路两端是使用相同的天线。不要低估校准抛物面天线的困难度。某种

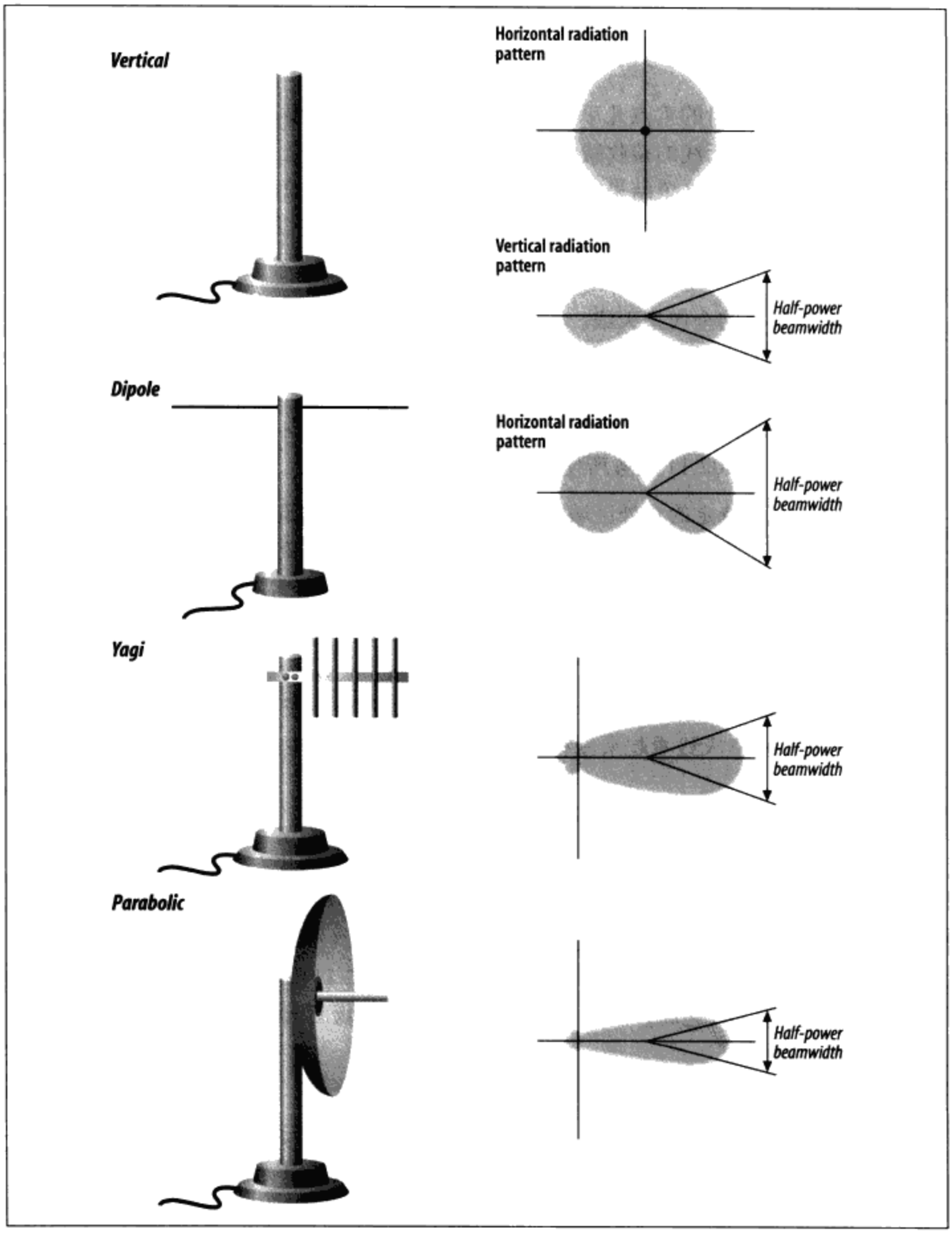


图 23-5：各种类型的天线

商用产品据称只有6.5度的波束宽。安装抛物面天线时，最好将之牢牢固定；否则，只要被暴风雨打偏，联机就可能为之中断。

有些厂商会额外区分网状（天线的反射面有点类似弯曲的烤肉架）与栅格状抛物面天线。对此用户无须担心，只要天线设计得好，就不必担心网状（mesh）与栅格状（grid）反射面的性能差异。不过在强风地带，网状抛物面天线就比较占优势。

抛物面与八木天线主要用于建筑物之间的链路。最大的问题是如何正确校准天线。如果双方距离不超出目视范围，不妨训练一下自己的瞄准能力。其实在这种情况下根本不需要用到如此复杂的天线。如果栋距之间超出视力范围，除了买个较好的指南针，另外最好向美国地质勘探局（U.S. Geological Survey）买份地形图，然后估计彼此如何对准。记得要调整磁北（magnetic north）。如果愿意花一笔费用，或许可以在其中一方安装高增益的垂直天线，如此可以简化整个安装过程，因为只需要校准单边天线。如果信号相当微弱，校准完第一支天线后便可以用抛物面天线取代垂直天线。

高增益天线可能会有管制上的问题，特别是在欧洲地区，因为当地的功率限制较美国严格。在美国，Orinoco品牌销售的高增益抛物面天线不能使用ISM频带的边界信道（即第1、2、10与11信道），因为信号会泄漏到频带之外。

天线接线

花了这么多工夫探讨天线，现在让我们回过头来思考，如何将天线连接至接入点或无线网卡。大部分厂商均销售两种电缆：较便宜的细线（通常直径为0.1英寸）以及较昂贵与较粗的低损耗线（通常直径为0.4英寸）。细线通常不能超过几英尺长，因为细线相当容易造成信号损耗，太长就会吞噬掉所有信号。我曾接触过一个网站，它将接入点隐藏在天花板之上并使用穿越天花板的外接天线。不过，整个组装最后只是白费力气。外接天线的增益为2 dB，但天线与接入点之间的线材也有2 dB的损耗。

细线主要用来连接膝上型计算机的无线网卡与台式机上的便携式天线如此而已。以数字来说明，假设有家厂商标明2米的电缆损耗为2.5 dB。这意味着，在2米长的电缆中信号强度将消失近一半。另外一家厂商所提供的线材标明在2.4 GHz频带，每100英尺的损耗为75 dB。这意味着信号是以2的25次方（大约3300百万）倍数的损耗，这显然不是大家所乐意见的。我知道有家厂商建议使用中度增益的RG58线材。在便携式的使用场合，RG58的确比细线好一点，不过也好不了多少（每100英尺35 dB）。如果采用RG58线材，请尽量将电缆截短。更好的方式是舍弃RG58，看看能否换成LMR-200（一种高质量、损耗只一半的线材）。

如果使用低损耗线材，结果将会如何？情况显然较好，但可能不如各位的预期。有家802.11厂商使用Times Microwave LMR-400线材。LMR-400是相当高级的线材，不过

在2.4 GHz频带，每100英尺仍有6.8 dB的损耗。也就是说，在100英尺长的线材中，超过3/4的信号会消失不见。由此例可知，天线要尽可能靠近接入点，将传输线的长度尽量缩短。如果打算采用屋顶型天线，为在中庭用餐的用户提供网络服务，记得不要将接入点置于地下室的配线柜，然后再拉线至屋顶。如果可能，最好将接入点置于屋顶，再以耐候材料加以包围。如果不行的话，至少将接入点置于阁楼或屋顶的管线间隙中。尽量缩短传输线是最好的做法，没有其他方案可以取代。同时，切记传输线绕经墙壁或导管时有可能变短。我一直搞不懂为什么，不过只要仔细测量，就会发现电缆总是短少个2英尺。重点是，接入点至天线的直线距离或许只有20英尺。如果最后得用上50英尺的电缆才有办法连接彼此，也不用太过惊讶。电缆本身或许会行经转角与导管，何况在到达目的地之前，还存在其他可能影响线长的因素。

最后，天线接头也有关系。所有无线厂商均销售不同长度的电缆并会附上所需要的接头与适配器。我强烈建议采用最便捷的方式，直接购买焊好接头的现成线材。接头损坏是无线系统失灵最常见的原因，尤其是安装RF接头的经验不足时。

天线分集

改善多径衰落（multipath fading）常用的一种方法，就是使用多组天线（天线分集）。与其加大天线，不如使用多组天线，然后选用接收信号较佳的天线。采用天线分集（*antenna diversity*）并不需要用到复杂的数学理论或信号处理技术。

有些无线局域网络厂商在无线网卡中内置多组天线，有些产品甚至允许无线网卡外接多组天线。802.11标准建议使用天线分集，但并未强制要求。如果环境中的干扰十分严重，挑选厂商时不妨将天线分集纳入考虑。

放大器：放大功率

放大器主要用来提升信号的功率。在无线电网络的发射端，放大器可以协助将信号传送至更远以覆盖更大的范围。有些发射放大器也集成了接收端前置放大器，有助于改善信号灵敏度。

在室内部署802.11网络时通常无需使用放大器来提升传输功率。而提升接入点的传输功率可以覆盖更大的范围，能够加入网络的工作站也就越多。为了维持信号质量，设计网络时最好使用较多的低功率小型接入点。如果无线局域网络的部署重点在于覆盖范围而不计信号质量，就可以使用高功率的垂直天线。

一般而言，高传输功率只是说来好听，实际上并不见得较好，除了一些例外的情况。在提高接入点密度之前，小区网络可能希望提供较大的覆盖范围，何况接入点的价格远高于放大零件。以802.11打造的点对点链路也是放大器一项不错的应用。如果距离过长，

天线增益根本就无法将信号拉至本底噪声之上。Ruby Ranch Internet Cooperative (*http://www.rric.net*)(注10)所使用的上行链路算是记录得比较完整的一个户外点对点案例。以802.11打造广域网络（WAN）的远程ISP也会广泛使用放大器。

SSB Electronics（*http://www.ssbusa.com/wireless.html*）与HyperLink Technologies（*http://www.hyperlinktech.com/web/amplifiers_2400.html*）是两家802.11放大器厂商。不过，如果打算使用802.11放大器，要切记：

- 不要超出法定功率限制，绝对功率与ERP两者皆是。
- 802.11无需使用许可证。如果干扰到其他服务，那是你的问题。如果一项有许可证服务干扰到你，那也是你的问题。如果网络的服务范围太广又使用高功率，干扰问题通常无可避免。
- 请使用合乎802.11标准的设备。有些放大器虽然涵盖可使用的频率范围，但是使用上并不合法。

警告： FCC的确强制要求落实相关规范，而且处罚相当惊人。如果你违反相关管制规定，FCC大概会很不高兴，特别是超过功率限制或使用未经核准的设备时。

注10： RRIC本身就是个迷人的网站，我极力推荐。当地的电信公司拒绝在附近提供DSL服务，而一群志愿者却使之付诸实现。

第二十四章

802.11 网络分析

没有痛苦，就无自觉。

——据说出自 C.G. Jung

20 世纪 90 年代，计算机专业人员有如医师一般，必须为人们诊断疑难杂症。如同医生会遇到陌生人所提出的医疗问题，计算机专业人员也必须面对一堆由陌生人所提出的古怪技术问题。每当有陌生人知道我从事网络相关行业时，通常会问："为什么 Internet 经常断线？"越思索这个问题，我越相信真正的问题应该是"为什么 Internet 不会更常断线？"

虽然不敢奢望能够以本章有限的篇幅来回答上述问题，不过看得出来，网络问题显然已经影响到了我们的现实生活。有线网络会停摆，无线网络也不例外。无线局域网络能够提高生产力，而完全瘫痪的风险也相对较高，何况可以确定的是，有限的带宽必然不敷使用。构建无线局域网络后，网络工程师必须准备就绪，随时调查可能发生的问题。

不论针对何种网络，可信赖的网络分析工具在工程师的百宝箱中向来不可或缺。在有线骨干网络方面，不乏一些可以在疑难排除时提高生产力的网络分析工具。同样地，无线网络的疑难排除也可以受惠于适合的网络分析工具。有时候，就得凭借这些工具，才有办法知道空中发生了什么事。本章主要讲解网络工程师所借助的网络分析工具。市面上有许多商用分析软件，Linux 平台上也有一些免费的工具可用。不过在深入研究这些工具之前，我们最好先来探讨为何网络管理人员需要无线网络分析工具。

网络分析工具

虽然有共同的继承，802.11 毕竟不是 Ethernet。它具备了一些额外的协议功能，每个功能都可能是问题的来源。网管人员有时必须深入协议底层的细节，了解空中到底发生了

哪些事，方能解决802.11网络的问题。在有线网络领域，网络分析软件向来被视为网管人员百宝箱里相当好用的工具，因为它们能够提供低层的细节。在无线网络领域，分析软件不仅同样好用，或许更为重要。在802.11网络中，可能出现差错的环节更多，因此要迅速找出疑难排除的着力点，一套优秀的分析工具是不可或缺的。

问题的避免最好始于规划阶段。有些分析软件可以提供RF信号强度的细节统计报告，这在决定接入点摆放位置时相当有帮助。分析软件可以协助网管人员确保BSS之间有充分的重叠以便及时切换，从而避免产生信号接收死角。当无线网络逐渐成长而必然需要服务更多用户时，为了不影响性能，管理人员可能会考虑缩小每个接入点的覆盖范围，以便在既定范围内提供更多合计吞吐量。在缩小覆盖范围的过程中，网管人员或许必须将部署计划重新演练一遍，因而终究还是离不开手边的分析工具。

既然无线网络的带宽有限，迟早还是必须面对性能问题。性能问题有可能是因为有太多用户共享太少接入点，或是与无线层所导致的问题有关。802.11的设计者了解无线传输媒介可能导致哪些问题。实际上，遇到持续干扰时，通常会以较简单（以及较低速）的编码方式重新传送帧并且对帧进行分段处理。

干扰是影响802.11网络性能的主要因素之一。除了直接导致已传送帧失效而必须重传，干扰同时会带来两种间接影响。低劣的传输质量可能导致工作站切换到较低速率，以便保持较可靠的无线链路质量；低速传输通常可以提高传输的成功率，不过也因此牺牲了吞吐量。此外，802.11工作站可能会为了克服干扰转而分段待传帧，因此降低了实际传送的用户数据的比例。相较于其他局域网络协议，802.11的标头并不算小。当传输数据量不变时，帧分段必然会增加传输的标头的数量。

一般网络只会用到少数几种应用程序。到底用户所抱怨的性能问题是指一般性的网络问题，还是某种特殊应用上的问题？只要查看所传送封包大小，网络分析软件即可协助找出问题成因。小封包较多，代表遭遇干扰而过度使用帧分段功能。有些分析软件还可以提供无线网络帧传输率的分配报告。802.11b网络能够以11Mbps的速率传输，不过如果干扰存在，帧极有可能以较低速率（5.5 Mbps、2 Mbps甚至是1 Mbps）传送。如果工作站具备高速的运行能力却以较低的速率传输，很有可能是因为大量干扰所致。性能取决于无线容量（capacity）。降为较低速率的工作站或许不会占用太多吞吐量，却会占用无线媒介相当多的时间。有些分析软件可以针对电波的利用率（radio utilization）提出报告，这在追踪特定性能问题时特别有用。

要解决干扰的问题，可以将接入点或天线换个角度，或是在覆盖不足的区域加装一个接入点。分析软件可以让网管人员在心里有个概念，知道应该进行何种改变有助于解决问题，不必等到用户向你描述有何异常。有些分析工具可以提供所收到帧的RF信号质量报告，以协助网管人员找出较佳的硬件摆放位置。避免将用户当成白老鼠反复试验，可

让你看起来更专业一点，也可以让用户舒服些。缩短疑难排除时间向来就是网络分析工具的强项。

此外，网络分析工具尚可协助网管人员校验802.11 MAC特定功能的运行是否正常。虽然可以在数据流经无线骨干网络时再加以分析，不过问题通常是出现在无线链路上。帧是否得到确认？如果没有，则必须加以重传。DS位的设定是否正确？如果答案是否定的，那么地址字段的诠释必然会出现错误。如果接入点的有线端出现格式不对的封包，可能的损毁点将不止一个。分析工具可以在帧行经空中之际加以查看，协助找出损毁封包的来源。格式不符的帧可能来自工作站，也可能是被接入点损毁的。寻求厂商支持之前先确定问题所在，对问题排除有莫大的帮助。

802.11 网络分析软件

802.11网络分析工具目前十分常见，每个无线局域网络管理人员的工具箱都应该配备。大部分的802.11网络分析软件都只需配合一个802.11网卡即可使用。之所以不需要特殊硬件，是因为一般市售的802.11网卡均已提供捕获封包所需要的RF硬件。唯一需要注意的是，这些软件通常只能搭配市面上的几种网卡使用。

任何无线网络部署的预算都应该将网络分析软件纳入考虑。要直接购置或自行打造悉听尊便，不过我预料大部分机构还是以采购商用产品为主，将开发与调试的工作交由网络分析软件厂商负责，毕竟商业级分析软件的采购、安装以及使用都比自行打造来得快。

AirMagnet（*http://www.airmagnet.com*）与WildPackets的AiroPeek（*http://www.wildpackets.com*）是最著名的两个商用无线分析软件。我在Interop Labs排除各种无线问题时就经常使用它们。

Ethereal

Ethereal是标准的开放源码网络分析软件。和其他专业分析软件一样，它支持一系列通信协议，可以从不同网络接口捕获实时数据。和其他专业分析软件不同的是，Ethereal完全来自一句口号（“Sniffing the glue that holds the Internet together”）。

Ethereal可以在大部分的Unix及Windows平台上运行。这两种平台的源代码均可自由取得，不过修改工作在Unix平台上比较容易，因为Unix平台有许多可以免费取得的程序开发环境。如同许多开放源码项目，Ethereal的发行受到GNU Public License的规范。许多常见的网络协议解码功能均被包含其中。就本节而言，最重要的协议是IEEE 802.11以及LLC，每个802.11帧都会用到它们。当然，TCP/IP协议组也包含在内。

随着802.11逐渐普及与Linux逐渐可提供更好的支持，可供配合的硬件也越来越多。起初只有基于Prism芯片组的网卡支持网络分析。不过，目前大多数接口卡均已提供这项功能。本节所使用的Ethereal为2005年1月底发行的0.10.9版。

Windows 平台上的封包捕获

Ethereal 奠基于 *pcap* 这个封包捕获链接库之上。在 Windows 中可以使用移植到此平台的版本，称为 WinPcap。虽然 Windows 几乎支持所有的 Ethernet 接口，但无线网卡的编程接口还是有所不同。有些网卡使用promiscuous模式时无法捕获任何帧，而即使关闭 promiscuous 模式，有些网卡依然只能捕获往来于该工作站的帧。相较于Linux，在Windows中捕获无线封包与所使用的网卡密切相关，因此我比较倾向于使用 Linux 平台。

编译与安装

要编译Ethereal程序已经不像以前那么困难。一些无线分析所需要的补丁文件均已整合到主要的源代码中，因此可以“开箱即用”（out of the box）。

在编译Ethereal之前，必须先安装libpcap与GTK+链接库。libpcap用来捕获封包，GTK+则是用来显示结果。此外，内核（kernel）必须支持才有办法捕捉封包，因此在设定内核配置时，必须加入 Packet Socket（*CONFIG_PACKET*）支持。

Ethereal 本身使用标准的开放源码编译流程，即从 *http://www.ethereal.com* 下载源代码后，以 *./configure*、*make* 及 *make install* 等命令即可完成编译的工作。

Ethereal 与 Windows

在 Windows 环境中，二进制包的重要性相对较高，因为缺乏高质量且免费的开发环境。虽然在 Windows 环境上并未提供相同等级的 802.11 支持，但 Ethereal 还是值得拥有，特别是在每天都需要用到 Windows 系统的日常工作里。Windows 的 Ethereal 二进制版本可从 *http://www.ethereal.com* 下载。在 Windows 里，Ethereal 需要用到WinPcap链接库以提供类似*libpcap*的支持。WinPcap可自 *http://netgroup-serv.polito.it/winpcap/* 下载。WinPcap 只支持 32-bit Windows 操作系统（95、98、ME、NT以及2000）并且以BSD方式授权使用。值得注意的是，Microsoft Research 对 WinPcap 提供了部分赞助。

将无线接口设定为监听模式

要捕获封包，必须先将无线接口切换为监听模式（monitoring mode），这相当于Ethernet接口的封包捕获模式（promiscuous mode）。启动监听模式的方法因无线驱动程序而异。

Cisco Aironet无线网卡

Cisco Aironet无线网卡有两种监听模式。第一种称为*rfmon*模式，驱动程序会传回当前工作站所在网络的所有帧。第二种简称为*y*模式，驱动程序会捕获当前信道的所有帧。要选取监听模式，可以通过proc文件系统更改驱动程序的运行配置：

```
bloodhound:~# echo "Mode: rfmon" >/proc/driver/aironet/ethX/Config
bloodhound:~# echo "Mode: y" >/proc/driver/aironet/ethX/Config
```

要回到正常的工作站设定，可将模式切换回*ess*：

```
bloodhound:~# echo "Mode: ess" >/proc/driver/aironet/ethX/Config
```

捕获封包时，必须将所使用的网络接口名称提供给Ethereal。2.4.19版以前的系统内核可以使用接口的Ethernet名称（ethX），2.4.20版之后则使用wifiX的。

Prism无线网卡

采用Prism芯片组的网卡有两种驱动程序可供使用：Absolute Value Systems的*linux-wlan-ng*（*http://www.linux-wlan.org*）以及HostAP驱动程序（*http://hostap.epitest.fi*）。*linux-wlan-ng*驱动程序在0.1.15版之后将监听纳为基本功能。它的启用是通过wlanctl-ng命令，而非无线扩展（wireless extensions）命令：

```
bloodhound:~# wlanctl-ng wlan0 lnxreq_wlansniffer enable=true channel=6
```

要关闭监听模式，可以使用如下命令：

```
bloodhound:~# wlanctl-ng wlan0 enable=false
```

采用Prism芯片组的网卡也可以配合HostAP驱动程序进行监听。它使用自定义的（private）系统调用（类似无线扩展功能）来启动监听模式。只要传送监听模式命令（2或3）给网卡，就可以启动监听模式。模式2可以监听所有标头，模式3只用来监听802.11标头。要关闭监听模式，可以将模式指定为0：

```
bloodhound:~# iwpriv eth1 monitor mode
bloodhound:~# iwpriv eth1 monitor 0
```

Orinoco 无线网卡

0.15版以后的orinoco_cs驱动程序不需补丁便已支持监听模式。较早版本的补丁程序可自 *http://airsnort.shmoo.com/orinocoinfo.html* 下载。要查看驱动程序是否安装补丁，可以用 *iwpriv* 命令来查询：

```
bloodhound:~# iwpriv eth1
```

如果驱动程序支持监听功能，也可以通过 *iwpriv* 予以启用。支持监听功能的驱动程序具备两种模式。模式1会在前面附加Prism样式的监听标头，用来报告信号强度及其他物理层参数，模式2则只会附加802.11标头。监听时可以任选一种模式以及信道。例如，要监听第6信道且要求附带完整的Prism标头监听信息，可以使用如下命令：

```
bloodhound:~# iwpriv eth1 monitor 1 6
```

要停止监听，可以将模式指定为0：

```
bloodhound:~# iwpriv eth1 monitor 0
```

采用 Atheros 芯片组的网卡

采用Atheros芯片组的网卡使用第十九章所提到的MADwifi驱动程序。最新版的MADwifi可以用 *iwconfig* 命令将网卡切换为监听模式。如有必要，也可以用 *iwconfig* 指定要监听的信道，例如以下列命令来设定 *ath0* 接口：

```
bloodhound:~# iwconfig ath0 mode monitor
bloodhound:~# iwconfig ath0 channel 6
```

不过我发现某些版本必须事先指定一个IP地址，接口才会出现在封包捕获列表。所指定的IP地址与实际使用的无关。

```
bloodhound:~# ifconfig ath0 1.2.3.4
bloodhound:~# ifconfig ath0 up
```

运行 Ethereal

启动Ethereal后会弹出主窗口，如图24-1所示。任何用户均可启动Ethereal，但是必须具备管理员权限方能够捕获封包（不过任何用户均可加载捕获文件进行分析）。主窗口分为三个部分。最上面的窗格称为封包列表窗格（packet list pane），提供每个封包的高级情况。它会列出每个封包的捕获时间（Time）、来源与目的地址（Source与Destination）、协议（Protocol）以及封包的基本解码（Info）。Protocol字段所填的是用来分析该帧的最终解码协议。在802.11网络上，最终的解码协议可能是IEEE 802.11管理帧或是TCP分析协议（如果该802.11帧包含了一个经过LLC封装的IP封包以及一个

装载HTTP的TCP段）。随着链路层加密的使用频率增加，802.11通常成为最终的解码协议，因为Ethereal的原始封包捕获（raw capture）无法对这些帧进行解密，也无法“看透”受保护的上层协议。

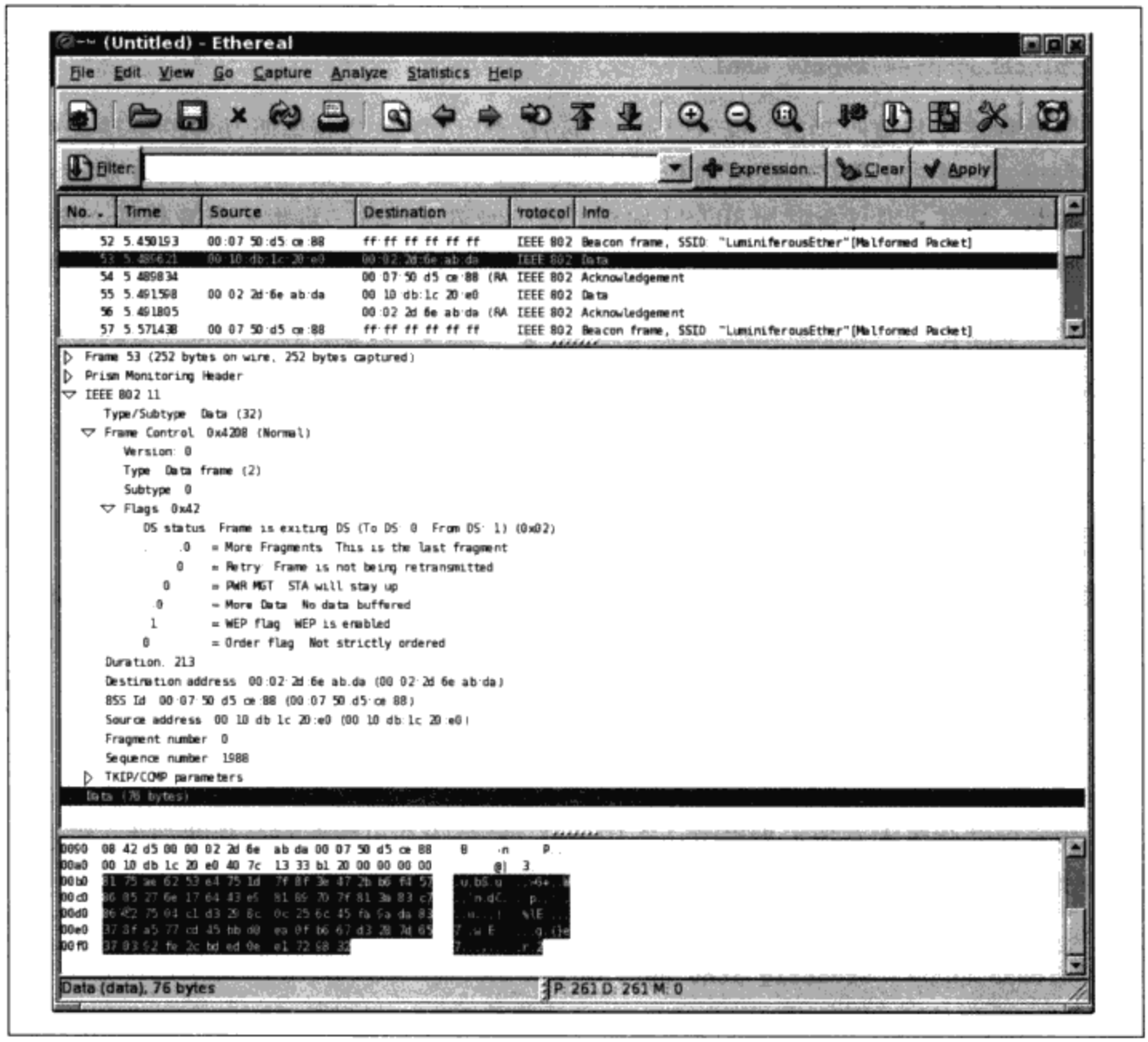


图24-1：Ethereal主窗口

中间的窗格称为树状视图窗格（tree view pane）。封包中所有主标头均会列出，展开后可以得到更多细节。所有封包均有基本的“Frame”树状视图，其中包含到达时间与捕获长度等细节。802.11网络可以加入Prism Monitoring标头，其中包含无线链路数据。Prism标头原本是针对Prism设备所开发的，后来为大多数驱动程序所采用。虽然图24-1来自采用Atheros芯片组的网卡，不过MADwifi驱动程序还是在前面附加了Prism监听标头。有些驱动程序则提供是否启用Prism标头的选项。

最底层的窗格称为数据视图窗格(data view pane)。它用来显示所选封包中的原始二进制数据，同时会高亮度显示在“树状视图窗格”中所选的字段。如果可以的话，就会进一步分析该帧。对于未加密数据，Ethereal 可以解读逻辑链路控制（Logical Link Control，简称LLC）标头。LLC 可以包含 ARP 封包、IP 封包、TCP 段（segment）等数据。Ethereal 包含了许多常用协议的解析器(dissector)，通常可以完整分析802.11帧。不过经过加密的帧就无法解读了，如图 24-1 中高亮度显示的部分。

在树状视图窗格选取任何字段，数据视图窗格中相应的位就会高亮度显示。图24-1 选取了帧的Data 字段，底下的数据视图窗格即以高亮度显示。我个人比较喜欢使用等宽字体(monospace font)，如此一来底下的数据视图窗格所显示的数据就可以按字段对齐。

位于 Ethereal 窗口最上方的信息栏包含四个重要元素。最左边的按钮“Filter:”用来指定过滤条件，只列出感兴趣的封包。其后的“文本框”(text box）允许用户直接输入过滤条件，不必从头开始设定。Ethereal 会将之前使用过的过滤条件留存在“历史列表”(history list)，让过滤条件的切换变得较为简单。最后是一个文本字段，用以显示各种不同的信息，这取决于当时 Ethereal 正在进行何种操作。它可能显示 Ethereal 目前正在捕获封包，也可能显示加载的捕获文件名称或树状视图中目前标示出的字段。

捕获数据

数据的捕获十分直接。找到“Capture”菜单，接着选取“Start”选项，随即会出现Capture Preferences 窗口。Ethereal 可以使用它所侦测到的任何接口，甚至是无线局域网络接口。

第一件事是选取想要监听的接口。对无线网络接口而言，所使用的名称可能是 *eth*、*ath* 甚至 *wlan*。不过在开始捕获封包之前，必须先将接口切换到监听模式。在 Ethereal 中可以使用 *-i* 命令行选项来指定接口。如果想统一使用单一接口处理分析事宜，可以使用脚本将 *ethereal* 映射至 *ethereal -i ath0*。

通常，我会启用“Update list of packets in real time”以及“Automatic scrolling in live capture”这两个选项。如果不选取前者，则只有当捕获停止时方能追踪整个过程；如果不选取后者，整个追踪记录就无法下拉到最后面。对于实时分析而言，速度相当重要。将域名解析（name resolution）停用，可以降低封包捕获的负担，也让工作站避免漏失封包。

减少数据量

原始的捕获文件可能十分庞大，要在一堆无用的封包中去沙捡金可是一件极高难度的挑战。善用网络分析软件的关键在于将封包数目筛减至关键的少数封包。为此，Ethereal

提供了三种方式：捕获过滤（capture filter）、显示过滤（display filter）以及标注封包（marking packet）。

捕获过滤

捕获过滤（capture filter）是降低Ethereal处理的数据量最有效率的方式，因为它们会大量涌入监听封包的接口。如果封包捕获接口丢弃某个封包，该封包就不会送至Ethereal做进一步处理。遗憾的是，捕获过滤对802.11而言并没有多大用处。如果在前面附加Prism监听标头，就无法使用捕获过滤。

Ethereal使用了*libpcap*，因此其所使用的捕获过滤语法和*tcpdump*一样。其中提供了一些基本的语句，可以任意组合为较长的表达式。这些基本语句允许以Ethernet或IP地址、TCP或UDP端口号以及IP或Ethernet协议作为过滤条件。也有一些是以来源或目的地地址作为过滤条件。遗憾的是，大多数适合的协议编号在802.11网络中通常经过加密，因此没有多大用处。

警告：802.11帧在LLC标头中携带有Ethernet协议编号，因此在加密网络上无法轻易予以过滤。

显示过滤

显示过滤（display filter）用在Ethereal能够辨识的任何字段，光是这一点就比捕获过滤强许多。显示过滤可以使用Ethereal内设的所有解码器，因此可以过滤Ethereal能够辨识的协议的所有字段。无线局域网络管理人员可以根据802.11或LLC标头字段来过滤帧。802.11封包过滤的实际范例将于本章稍后提及。

使用Ethereal进行802.11分析

应用到802.11网络时，有些Ethereal功能可以随时使用。本节将会列出一些在无线网络中使用Ethereal的小技巧，排列先后并无特定意义。

显示过滤

Ethereal可以过滤802.11标头中的任何字段。帧字段将依结构层次排列。所有802.11字段的变量名称均会前缀*wlan*字样并以两种次类别分别记载Frame Control（*wlan.fc*）及WEP Information（*wlan.wep*）字段的相关信息。图24-2显示了802.11标头字段的变量名称。图中，每个字段均会被标上数据类型。Boolean字段会被标上B；MAC address

会被标上MA；无符号整数会被标上U，另外加上位数。表24-1列出的是相同信息，只不过删去了无助于Ethereal显示过滤的字段。

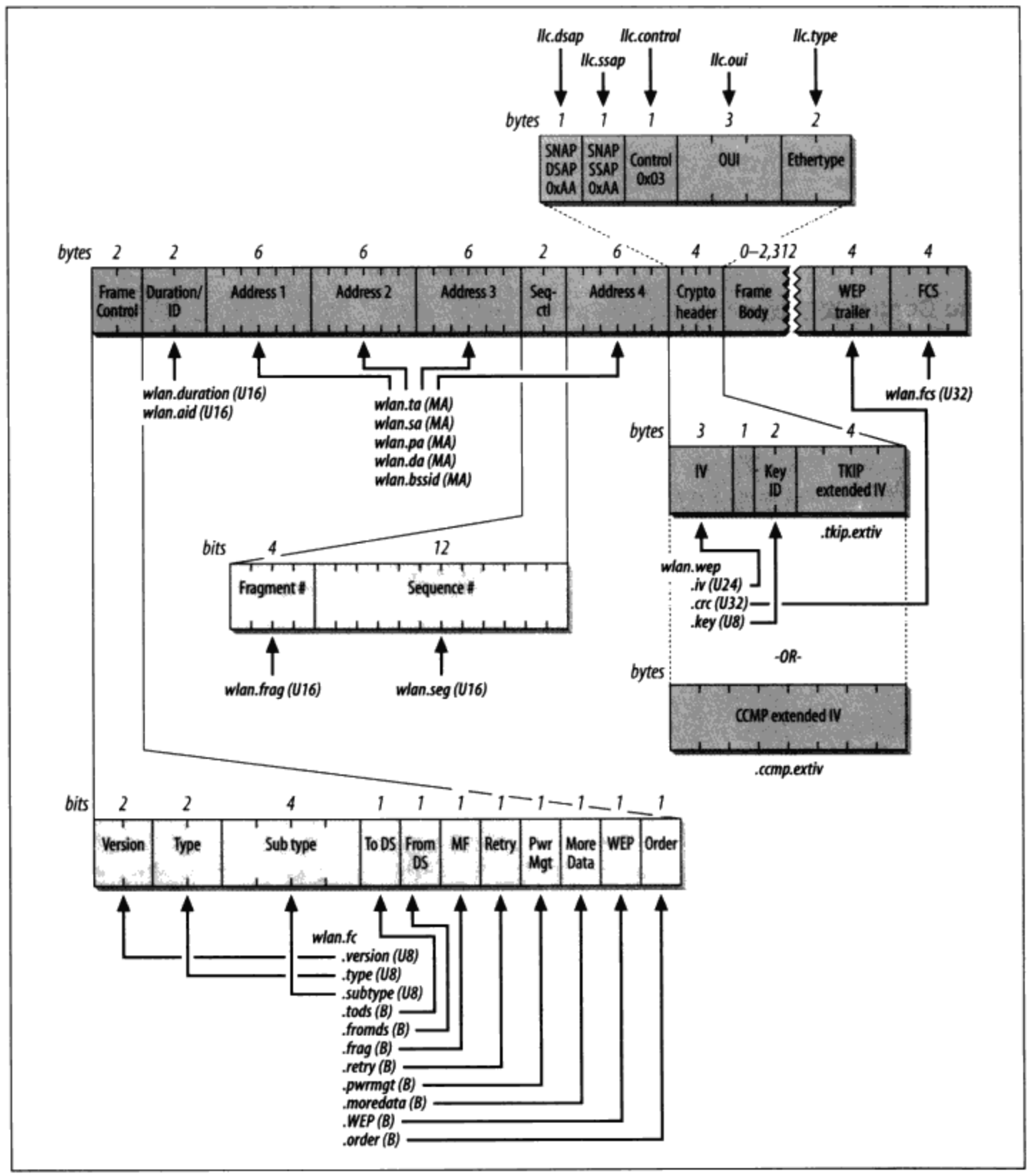


图24-2：标头字段变量

表24-1：Ethereal字段变量与802.11标头字段的对应表

802.11标头字段	Ethereal字段变量
标头字段	
Either source or destination address	*wlan.addr*
Transmitter address	*wlan.ta*
Source address	*wlan.sa*
Receiver address	*wlan.ra*
Destination address	*wlan.da*
BSSID	*wlan.bssid*
Frame Control次字段	
Frame type	*wlan.fc.type*
Frame subtype	*wlan.fc.subtype*
ToDS flag	*wlan.fc.tods*
FromDS flag	*wlan.fc.fromds*
Retry flag	*wlan.fc.retry*
Protected frame (WEP) flag	*wlan.fc.wep*
Protection字段	
WEP Initialization vector	*wlan.wep.iv*
TKIP IV	*wlan.tkip.extiv*
CCMP IV	*wlan.ccmp.extiv*
Key identifier	*wlan.wep.key*

这些字段可以通过运算符（operator）加以组合。Ethereal支持了一组标准的比较运算符：== 代表相等，!= 代表不相等，> 代表大于，>= 代表大于或等于，< 代表小于，而 <= 代表小于或等于。举例来说，显示过滤若为`wlan.fc.type==1`，则代表控制帧。

对于逻辑运算符`and`与`or`均有支持。如同许多程序语言一样，惊叹号（!）代表逻辑上的否定。Boolean类型的字段可用来查看存在与否，因此欲启用WEP的控制帧，可用如下的显示过滤来表示：`wlan.fc.type==1 and wlan.fc.wep`。

图24-3以树状视图（tree view）显示了完整的802.11标头。在树状视图窗格中选取802.11标头，底下的ASCII视图就会将组成802.11标头的位高亮度显示。将802.11标头的树状结构展开，即可解读所有字段。

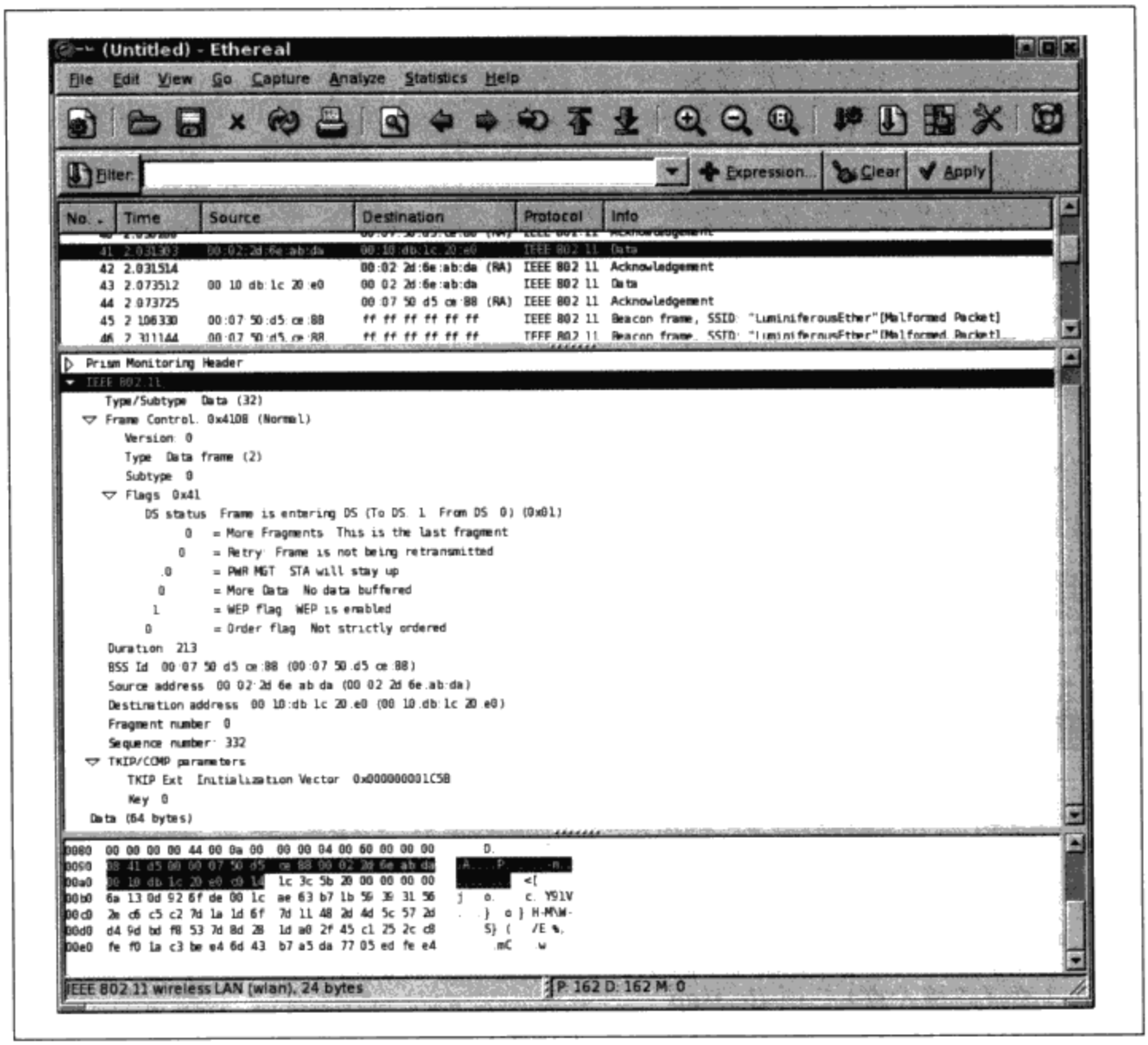


图 24-3：树状图中的 802.11 标头

了解 LLC 标头以筛选协议

为了在无线链路之上以多路传送较高层协议的数据，802.11 采用了 LLC SNAP 封装（SNAP 封装在第三章结尾处已提及）。802.11 并无协议字段，因此接收端无法直接从标头分辨不同类型的网络协议。为了能够支持多种协议，因此加入了长度为 8 个字节的 SNAP 标头。SNAP 标头经过解码后显示于 Ethereal 的树状视图窗格，如图 24-4 所示为 EAPOL 密钥帧。

选中树状视窗中的 LLC 标头，相应的 8-byte 标头即会出现在封包转储（packet dump）处。从数据视图窗格（data view pane）里可以清楚看到 SNAP 标头中的 8 个字节。该标头由 5 个字段构成：

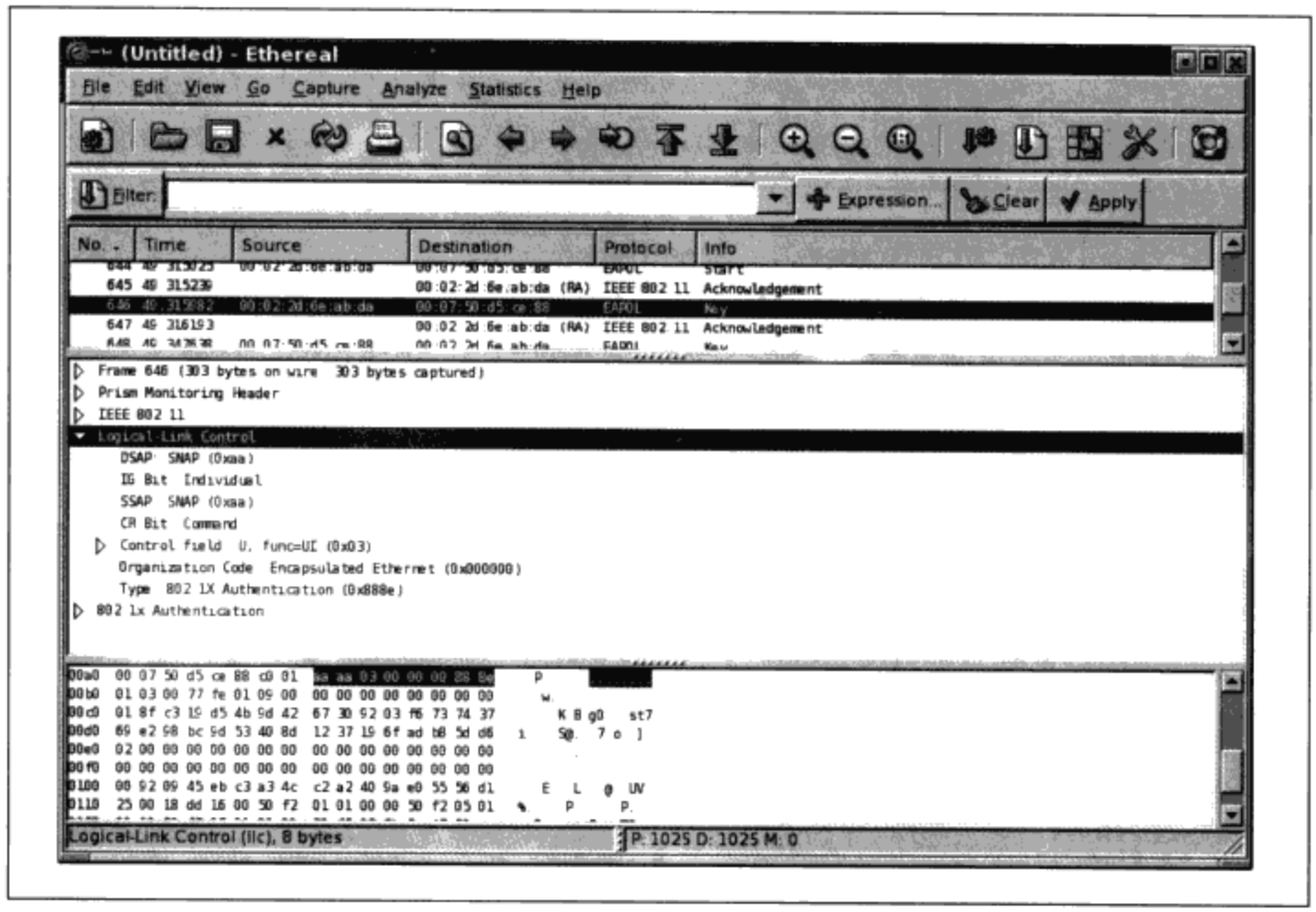


图24-4：LLC SNAP标头

DSAP（目的服务接入点）——llc.dsap

对SNAP封装而言，这个值通常设定为0xAA。

SSAP（源服务接入点）——llc.ssap

对SNAP封装而言，这个值通常设定为0xAA。

Control（控制）——llc.control

此字段源自HDLC。和所有以HDLC传递的数据一样，它被用来将LLC标头之后的数据标示为未编号信息（unnumbered information）。所谓未编号信息是指使用非联机式数据传输（connectionless data transport），而且该数据无需重新排序或给予确认。

OUI（组织唯一标识符）——llc.oui

此字段用来决定如何解释其后的字节。IP以RFC 1042标准封装于LLC，RFC 1042规定使用OUI 0x00-00-00（有些厂商或许会使用特定的OUI作为专属系统传输之用）。

Protocol Type（协议类型）——llc.type

此字段由相应的Ethernet帧复制而来。Type字段对应到Ethernet的类型代码。在IP网络中，其值可能是代表IP的0x0800或代表ARP的0x0806。图24-4中显示为0x88-8e，因为此帧乃是EAPOL（802.1X）帧。

802.11规范将LLC封装列为必要，因为这样一来，802.11帧就无需直接承载协议信息。不过有时LLC标头经过加密，除非事先解码，否则无法得知实际的内容。

802.11 网络分析项目清单

为了说明网络分析软件如何协助网络工程师监察无线局域网络流量，本节列出了排除一般身份验证问题时的项目清单（checklist）。此处所举的例子虽然使用Ethereal，不过也适用于之前所提到的商用软件。

显示过滤初探

显示过滤对802.11而言特别有用，因为它们能够用于解码帧的细节。在进行一般疑难排除过程之前，了解显示过滤的若干要件将有所帮助。

排除 Beacon 帧

追踪原始802.11数据时，Beacon帧可能造成妨碍。大多数产品最多每秒可送出Beacon帧10次，占捕获到的帧的绝大多数。要移除Beacon帧，可以编写相当于Beacon帧的显示过滤条件，然后予以排除。

- 以`wlan.fc.type==0`指出所要筛选的是管理帧。
- 以`wlan.fc.subtype==8`指出所要筛选的是Beacon帧。
- 将两者合并后为其加上惊叹号（逻辑否定运算）：`!(wlan.fc.type==0 and wlan.fc.subtype==8)`。

筛选来自特定工作站的数据

通常，封包捕获是针对某个受测工作站。工作站之间会有不同类型的帧往来，因此筛选的进行方式取决于所要筛选的项目。

第一种方式是在显示过滤中使用 *wlan.addr* 变量，以此代表来源或目的地地址。

- 若要保留来自某个工作站的数据，可以使用“`wlan.addr==00:02:2d:6e:ab:da`”形式的显示过滤，只要在其中填入适当的MAC地址即可。这种方式相当于使用“`wlan.sa==00:02:2d:6e:ab:da or wlan.da==00:02:2d:6e:ab:da`”，只是后者比较冗长。

来源与目的地地址只出现于802.11数据帧。要排除某些问题，可能必须深入查看802.11

管理操作，例如帧的肯定确认。帧的肯定确认是针对接收端地址，而非目的地地址。要查看往来于特定工作站且包含确认信息的帧，可以在显示过滤中指定接收端地址。

- 只要以“`wlan.ra==00:02:2d:6e:ab:da`”形式的显示过滤，将受测工作站的MAC地址指定为接收端地址，就可以显示所有传送给该工作站的确认信息。要查看该工作站所发出的确认信息，必须加入第二个接收端地址，格式为“`wlan.ra==00:02:2d:6e:ab:da or wlan.ra==00:0b:0e:84:32:91`”，其中第二个地址代表提供服务的接入点。

筛选特定的协议

如果可以取得数据帧的内容，则可以把LLC标头设定为显示过滤的对象目标。要查看特定的协议内容，可以使用 *llc.type* 变量。输入协议编号时必须使用不带破折号的十六进制数值。

- 使用“`llc.type==0x888e`”形式的显示过滤，可以查看特定的Ethernet协议。

此外尚可利用LLC标头来搜寻以802.1H封装的帧，其OUI为00-00-F8。*llc.oui* 是6位的十六进制数值。在加密网络上，LLC标头只出现于802.1X帧，因此如果此过滤条件没有显示较上层的协议，也无需感到惊讶。

- 以RFC 1042进行封装的帧可用`llc.oui==0x000000`予以显示。
- 以802.1H进行封装的帧可用`llc.oui==0x0000F8`予以显示。

一般疑难排除任务

对如何以“显示过滤”筛选出感兴趣的帧有了初步了解后，就可以进一步探讨疑难排除任务。本节主要探讨如何筛选出感兴趣的帧并予以描述，并不打算使用一堆截屏图（screenshot）来详细举例说明。

身份验证疑难排除

- 显示过滤：筛选出往来于某个工作站的EAPOL帧，同时查看其确认信息。

  `llc.type==0x888e and wlan.addr==`*`supplicant-MAC`* **and** (`wlan.ra==`*`supplicant-MAC`* or `wlan.ra==`*`AP-MAC`*)

每个EAPOL帧均有一个以序号的形式出现的标识符。每个EAP封包均用来确认之前所接收到的信息。查看802.1X会话（session），确定每个EAPOL帧均有相应的802.11确

认信息，而且EAP标识符会逐渐增加。有些申请者无法应付重传的情况并会导致死机（因此，接入点必须对这些中止的802.1X会话解除身份验证，要求其重新开始）。

只要查看EAP封包的内容，就可以发现身份验证于何处失败。如果是在TLS隧道建立后才发生错误，有可能是因为申请者无法验证服务器的证书；如果数据已经通过TLS隧道，便有可能是其他因素造成，此时可以查看RADIUS服务器的日志文件来寻找线索。

密钥传递的疑难排除

- 显示过滤：筛选出往来于某个工作站的EAPOL密钥帧。

  `llc.type==0x888e and eapol.type==3 and wlan.addr==` *`supplicant-MAC`*

正确传递密钥必须经过6个步骤。部分握手过程如图24-5所示。首先，必须完成四次握手。作为一开始的完整性校验，必须确定每个帧均得到肯定确认。最快的方法是查看Ethereal中的帧编号。如果帧编号每次增加2，有可能跳过的即为802.11确认帧。

密钥传递失败最常见的原因之一，就是申请者（supplicant）与认证者（authenticator）的安全参数不符。Ethereal内设解析器（dissector）可以解读密钥帧中所包含的信息元素。图24-5的树状视图窗格底下显示了被解读的信息元素的开头。其中，组密钥被解读为动态WEP。之后只有一组单播密码组（unicast cipher suite）。WPA规定只能有一组单播密码组，不过大多数产品并未遵循此规定。有些申请者并未遵循一般做法，因此无法顺利通过身份验证。如果Association Request与密钥握手所使用的信息元素不符，认证者将会判定此交换过程失败。

性能的疑难排除

排除性能问题通常比辨识性能问题来得简单。一般而言，性能议题可以分为下列几种：

- 显示过滤1：筛选出往来于某个工作站的帧，同时查看确认信息。

  `wlan.addr==`*`client-MAC`* `and (wlan.ra==`*`supplicant-MAC`* `or wlan.ra==`*`AP-MAC`*`)`

此过滤条件可以显示往来于特定工作站的所有数据以及确认信息。查看记录下来的所有数据并查看是否有重复传送的帧。如果没有接收到确认信息，则必须重传完整的帧。如果重传数次之后仍然没有得到确认，网卡就会降低传输速率以改善联机的可靠度。较低速率所要求的“信噪比”较低。解决这类性能问题的方法之一，是在该区增加接入点密度以提升信号质量。改善接入点或工作站所使用的天线也会有所帮助。

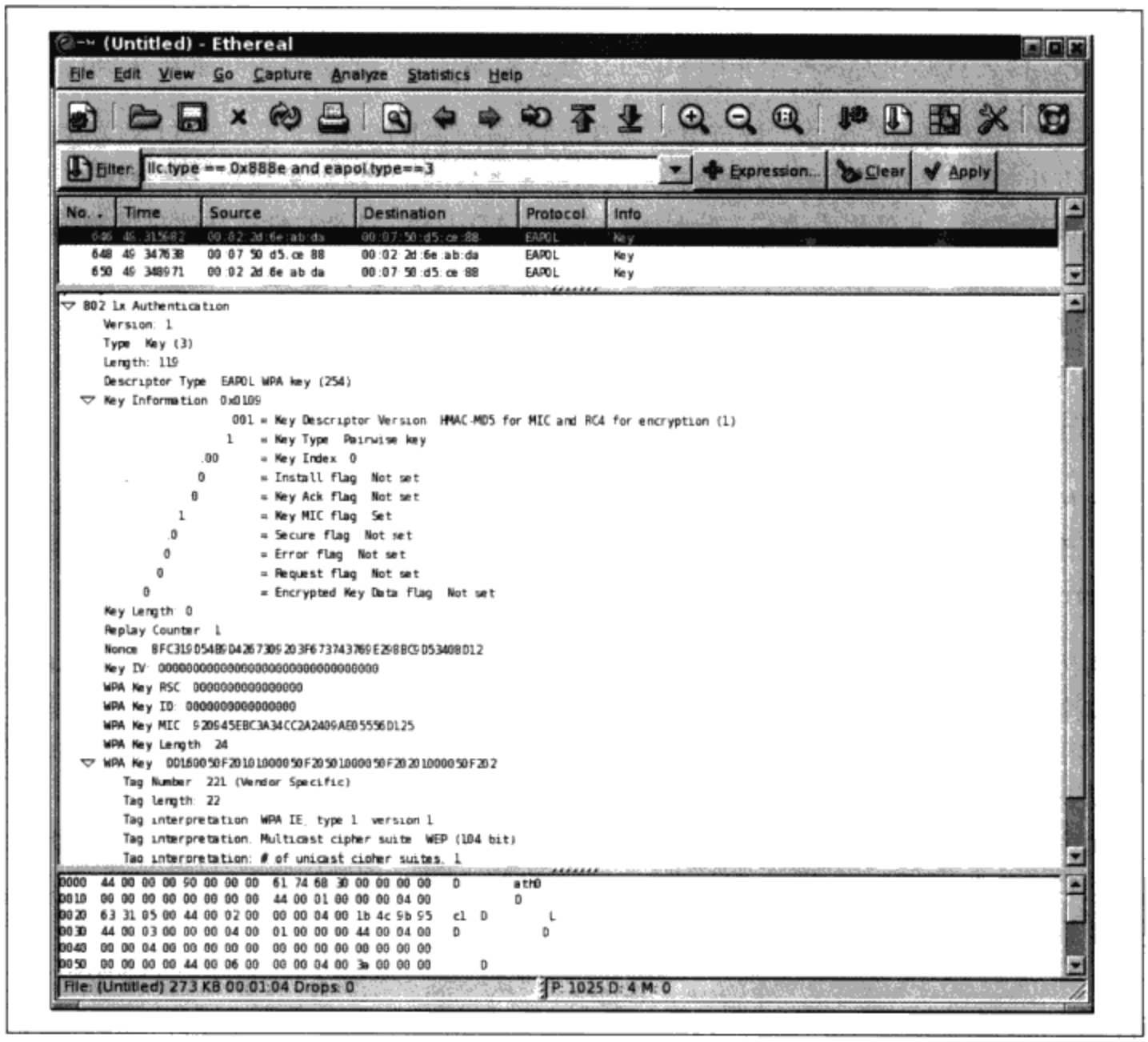


图24-5：密钥握手过程

- 显示过滤2：筛选出低于某种速度的数据。

  `prism.rate.data <  (speed tag)`

配合上一个过滤条件，可以只显示高于或低于特定速度的帧。Prism监听标头中是以一个整数代表帧的速度。由于它是以500 kbps为单位，因此以megabits表示时必须将它乘以2。例如，要显示所有低于2 Mbps的帧，必须指定`prism.rate.data < 4`。

数据视图窗格下面的状态栏用来显示封包数目以及已显示的封包数目。图24-1中，被捕获到的帧数为261（注记为P），而这261个帧均已显示（注记为D）。以计算器配合显示过滤2，可以让你对何种速率传送多少帧有大致的概念。有些商用软件是以“精灵”（wizard）实时显示分析结果。

- 显示过滤3：筛选出来自重叠网络的数据。

  `wlan.bssid != AP-MAC`

用户或许会抱怨因网络重叠所造成的性能问题。802.11 b/g 网络的性能特别容易受到重叠网络的影响，因为实际上只有三个（非重叠）信道可用。要评估网络重叠的程度，可以在捕获封包后使用“显示过滤3”保留来自其他网络的帧。如果帧为数不少，试着找出那些接入点的位置所在，然后予以关闭。

WEP 数据解密

有些分析软件可以解读WEP加密帧，只要在其中提供密钥即可。举例来说，在Ethereal的“Edit”菜单中点选“Preferences”选项，然后选择“IEEE 802.11 protocol”，就会出现如图 24-6 所示的 WEP 选项。只要输入密钥，Ethereal 就会以这些密钥解读经加密的帧。手动WEP密钥比较容易取得，动态WEP密钥就必须依赖申请者或者接入点方面提供。*iwconfig* 命令可显示出 Linux 申请者所使用的加密密钥。有些接入点以特定的方式提供密钥表的内容，网管人员可利用它找出工作站所产生的密钥。

RADIUS 分析

虽然不见得与无线局域网络攸关，但Ethereal事实上也可以解读RADIUS帧。在RADIUS协议的参数选择（Preferences）配置中，可以输入RADIUS所使用的共享秘钥。输入之后，所有被保护的字段均会被自动还原。如此一来，或许可以自动还原动态密钥，不过我尚未听说有任何 Ethereal 外挂模块可以达到此目的。

其他工具

其他工具通常用于网络分析。虽然不限于作为疑难排除工具，不过它们通常被用来评估覆盖范围。

搜寻、测量与映射网络

搜寻802.11网络是与之连接的首要步骤。有些分析工具可以找寻或评估现有网络的覆盖范围。极端的网络搜寻方式称为“扫基站”（wardriving），即用户以网络搜寻软件记录下所有接入点的位置。NetStumbler（*http://www.netstumbler.com*）与 Kismet（*http://www.kismetwireless.net*）是其中最著名的两种工具。

网络侦测是一种被动的过程。Beacon帧可以通过802.11接收器被搜集，根本无从防范。假定你的网络必然会被发现是最好的对策。与其依赖晦涩的网络名称或者隐蔽的网络

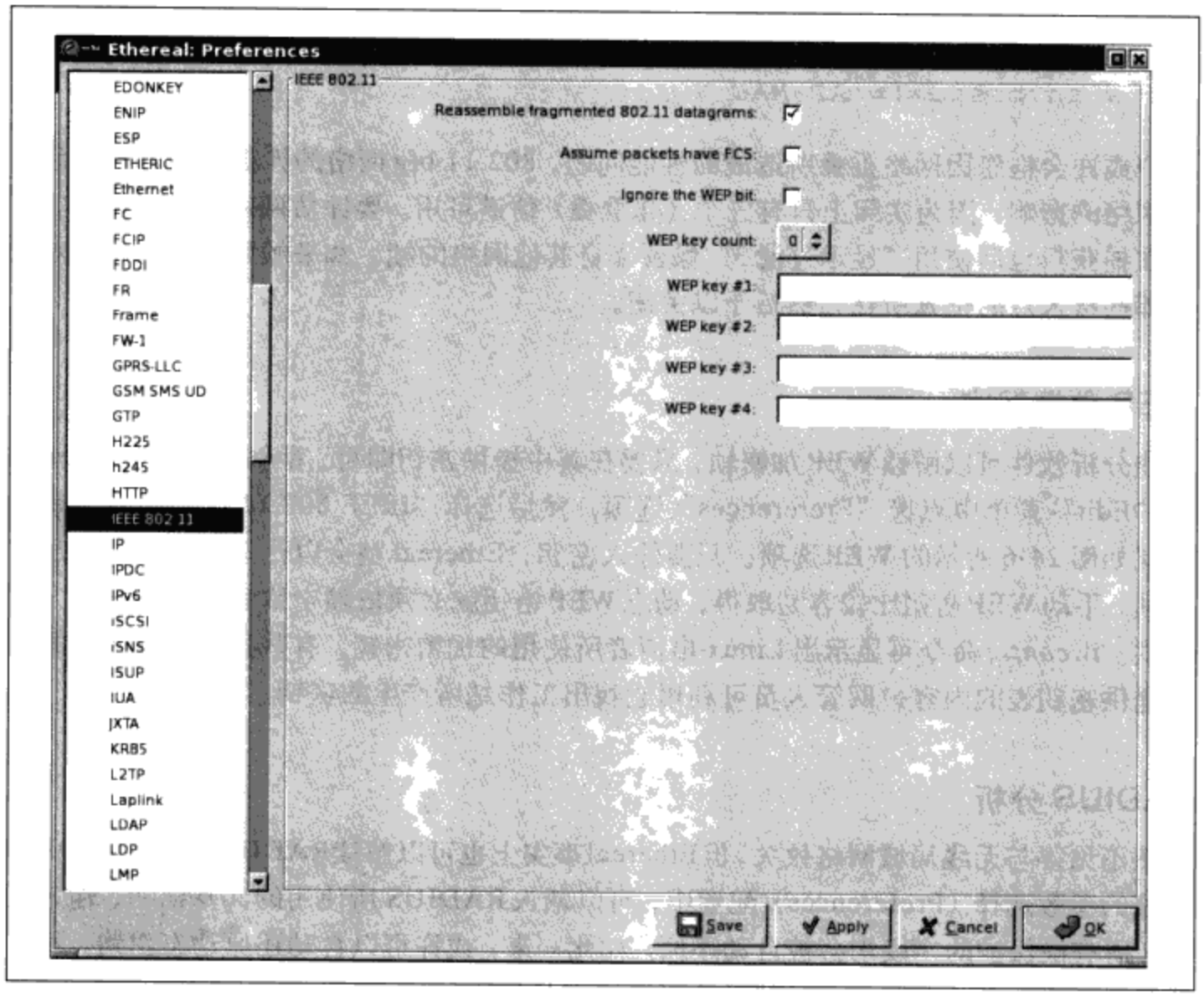


图 24-6：键入 WEP 密钥

位置，甚至使用较低的传输功率，倒不如使用正确的安全工具，例如使用第六章与第七章所提到的身份验证与加密方式来保护网络。就算网络被发现，其中的数据也无碍。

WEP 密钥恢复

目前有些开放源码工具可以用来攻击 WEP 弱密钥。其中最著名的就是 AirSnort，它于 2001 年 8 月首度问世，最新的程序代码可自 *http://airsnort.shmoo.com/* 下载。AirSnort 是第五章所提到的“Fluhrer-Mantin-Shamir WEP 攻击”最早与最著名的公开实现，不过并非目前唯一的破解工具（注 1）。

注 1： 实际的范例参见 WEPcrack（*http://wepcrack.sourceforge.net/*）与 Aircrack（*http://www.cr0.net:8040/code/network/aircrack/*）。

WEP密钥恢复工具主要是针对某些特定的“弱”初始向量（IV）。Ethereal借用AirSnort的分类码，目前已经可以显示出弱IV，而商用软件很早以前就具备这项功能。

要防范WEP密钥恢复攻击，网管人员可以将密钥的使用时间缩短为5～15分钟。有些厂商已经修改程序代码，避免使用弱IV。2002年初，Interop Labs发现许多厂商以惊人的速度立即作出响应，从此不再使用弱IV。到了2004年，虽然已有两年的时间可以进行修正，列在已修正名单上的几乎还是同一批厂商。

估计密钥恢复时间

密钥恢复有两个要件。首先，必须搜集到足够多带有弱IV的帧方能进行攻击，我称之为搜集时间（*gathering time*）。其次，成功的攻击必须处理保存下来的帧，我称之为分析时间（*analysis time*）（注 2）。

以我自己的经验而言，要搜集到足够的资料远比实际进行攻击要耗费更多的CPU时间。只要有足够的样本，分析只不过需要几秒的时间。分析时间是以线性成长，因此较长的密钥只能多提供几秒钟的保护。如果将密钥长度加倍，攻击所需要的CPU时间也会倍增，不过将几秒钟加倍仍然是几秒钟。

身份验证

大多数无线网络的802.1X身份验证协议是以TLS隧道提供安全防护。*ssldump*工具（*http://www.rtfm.com/ssldump/*）可用来解读TLS握手过程以及经由隧道传输的任何数据。不过解密时需要证书所使用的私钥的副本。

注 2：　有关分析时间的探讨参见*http://securityfocus.com/infocus/1814*。

第二十五章

802.11 性能与调整

过去一段时间，无线网络管理人员已经搭了一阵子顺风车。无线网络不仅新鲜，而且够酷。用户对它们可以提供什么样的服务大多没有什么概念。只要可以运行，用户就已经心满意足，告诉他们不要期待无线网络会提供类似 100BaseT Ethernet 的性能，就可以轻松交代过去。大部分无线设备的用户并不多，因此不会有好几十甚至上百个工作站同时关联到由少数接入点构成的服务区域。此外，大部分无线网络在逻辑上从属于现有的有线网络。在设计上，802.11 是为了弥补现有局域网络的不足，而不是打算取而代之。如果使用上偏重有线局域网络，就算没有无线网络，用户还是可以完成手上的工作，因此无线网络似乎没那么重要。比较可能发生的问题是，你不知道要如何摆放接入点，使它能够覆盖所需要的范围以及如何安装驱动程序，然后随时更新你的安全配置设定。

不过，随着时间增长，用户的要求也会越来越高。网络性能或许相当差劲，即使只有你注意到这件事。改变外在环境（例如调整接入点的摆放位置、使用外接式天线等）或许可以解决某些问题，不过有些问题最好通过调整管理参数来解决。本章所要讨论的主题即是加以微调便可改善整个无线网络性能的管理参数。

802.11 性能评估

和其他网络技术一样，802.11的速率也有两种。一种是名义上的“宣称”（headline）速率，另一种才是网络上的实际传输速率。大多数情况下，实际的有效载荷吞吐量一定低于宣称的数字。在 802.11 领域，有效载荷（payload）的吞吐量更是低于其所宣称的数字，主要是因为协议本身的负担就已经很大了。将名义（或额定）速率除以一半大概就是实际的数字。这算是不错的经验法则。

为了有助于与实际结果两相比较，通常可以事先计算出理论上的最大吞吐量。802.11的

数据传输由一系列原子操作（atomic operation）组成，如图 25-1 所示。图中所显示的是最简单的帧交换，由一个 802.11 Data 帧及其相应确认帧所构成。至于原子操作的要件，后续会加以说明。当然，如果牵涉到帧或是必须用到第十四章所提到的 802.11g 保护机制，整个交换过程就会比较复杂。

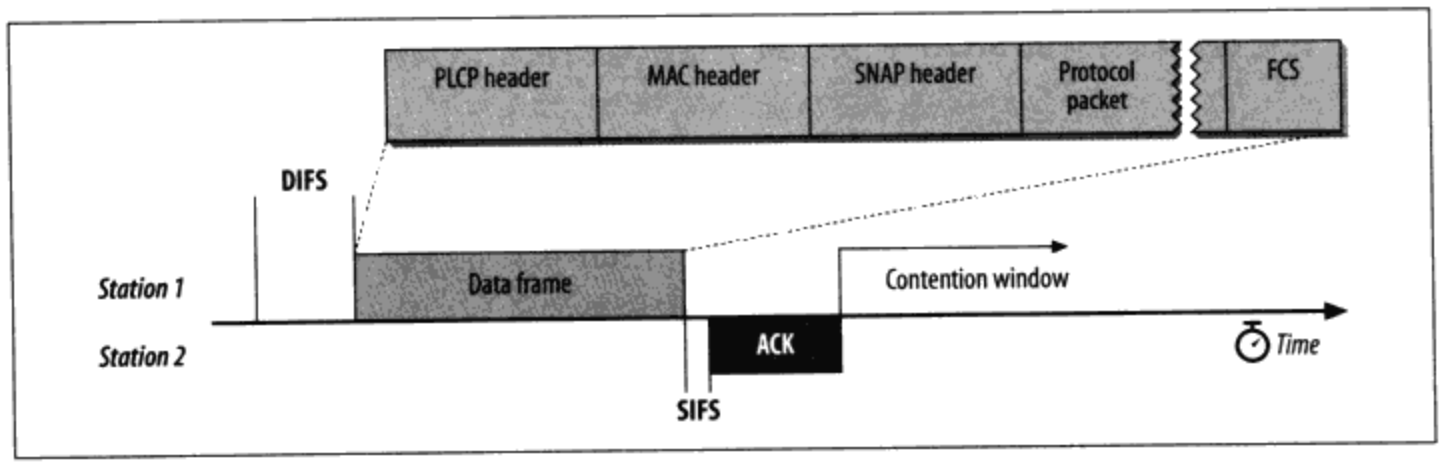


图 25-1：原子操作

每个原子操作均由几个帧组成，帧之间以“帧间间隔”（interframe spacing）加以区分。访问媒介时，通常以分布式帧间间隔（Distributed Inter-frame Space，简称 DIFS）开始整个帧交换序列，之后的帧则以短帧间间隔（Short Inter-frame Space，简称 SIFS）加以区分。DIFS 与 SIFS 的实际值取决于使用的物理层，详见相关章节。

帧必须通过物理层传送至空中，因此每个帧均具有物理层标头，由前导码以及其他协助解读帧的字段所组成。一般而言，前导码乃是物理层标头传输时间的关键组件。物理层帧本身就包含 MAC 帧，占用 28 个字节。MAC 帧中包含了长度为 8 个字节的 SNAP 标头，因此封装一个数据帧，就会增加36个字节的额外负担。如果再加上加密标头，MAC 标头的长度就不止如此了。

较上层协议封包本身是根据所使用的特定物理层规则加以传送的。不同物理层有其最小块（block）或符号（symbol），大小以“位”（bit）为单位。速率为 11 Mbps 的 802.11b 网络使用长度为 8 个位的符号。802.11a 与 802.11g 所使用的符号可以承载更多的数据，至于符号的大小，则取决于所使用的速率。以54 Mbps为例，其所使用的符号长度为216 个位（未来802.11n甚至将采用更大的块）。数据块的传送需要固定的时间。各种速率之间的差异主要是各个数据块所封装的数据位数不同，和块传送的快慢无关。例如，对物理层帧而言，1536 个字节的有效载荷（payload）包含了 12288 个位。对 802.11a 物理层来讲，此帧需要 57 个符号来传递。

要计算一次原子交换操作（atomic exchange）需要多少时间，可以先将它拆分成几个步骤，然后计算每个步骤所需时间的总和。首先，我们从帧间间隔的总和开始。虽然目前

的趋势倾向于采用较复杂的帧结构，不过对于有些原子交换操作，帧间只包含一个DIFS以及一个SIFS。计算出用掉多少帧间间隔后，接下来就可以根据所使用的物理层，开始分析帧的基本组成。每个帧的分析方法通常都一样，只有保护机制是比较明显的例外，因为此时必须用到较老的传输类型。每个帧均具有一个物理层标头（physical header）以及之后的物理层有效载荷（physical payload）。物理层有效载荷就是MAC帧（由MAC帧头、任何数据帧特有的SNAP标头、较上层协议的封包以及帧尾所组成）。

计算示范

举例而言，假设我们打算在802.11a网络上传送1500个字节的单一数据帧。此分析的目的纯粹是为了示范如何分析帧的组成，并不代表完整的模型，因此对于较上层协议可能造成的影响均忽略不计。

在802.11a网络中，每个SIFS需耗时16微秒，每个DIFS需耗时34微秒。交换一个数据帧，工作站需要等候一个DIFS时间，接着传递它的数据帧，然后等候确认帧。802.11确认帧会在经过一个SIFS时间后传出。因此帧间间隔总共用掉了50微秒。

接下来，分析数据帧。802.11a的preamble与signal字段需耗时20微秒。1500个字节的数据封包被封装于MAC帧，加上SNAP标头，总长度为1536个字节。如果此帧受到CCMP的保护，进行封装时就会附加上16个字节的标头与完整性校验值，如此一来，物理层帧的有效载荷总长度即为1552个字节，相当于12416位。以54 Mbps的速率来传输，物理层帧的有效载荷会以每个符号216位的方式进行分割，因此传递此帧会用到58个符号（12416/216）。每个符号需耗时4微秒（216/(54*10^6)），所以传递此数据帧共费时232微秒（58*4）。

802.11确认帧的长度只有14个字节（112个位），因此只需要一个54 Mbps符号即可传送完毕。有些芯片组使用较低的数据率。36 Mbps以上的数据率只需用到一个符号，至于再低的数据率就需要不止一个符号。18与24 Mbps需要2个符号，12 Mbps需要3个符号，9 Mbps需要4个符号，而6 Mbps需要用到5个符号。考虑到在传输时间和稳定性之间取得合理的平衡，假设确认信息以12 Mbps传送。3个符号需耗时12微秒，加上标头（20微秒）总计需耗时32微秒。

加起来，长度为1500个字节的有效载荷需要用到50微秒的帧间间隔、232微秒的传送时间以及32微秒的确认时间，总共是314微秒。如果没有竞争的情况发生，每秒可进行3184次原子交换操作（1/(314*10^-6)）。每次交换可以传递1500个字节的数据，因此总数据率为38 Mbps（3184*1500*8）。在接近理想的状况下，协议数据大约耗费理论速率的30%（(54-38)/54）。

性能模型的其他组件

上述讨论隐含了许多过于宽松的假定。大多数实际运行的802.11网络能够达到理论值的55%到60%就算不错了。重要的网络通常会用到上层协议，因此会造成封装上的额外负担。例如，TCP/IP标头就用掉了40个字节，同时还会要求对方予以确认。吞吐量是否进一步下滑，取决于TCP/IP如何被整合到此性能模型。

此外，上述范例也隐含假定没有媒介竞争的情况发生，然而这并不符实际。虽然802.11 MAC会尽量避免冲突情况发生，但是冲突终究不可避免。有些工程师认为TCP/IP甚至会使得冲突的情况更加恶化，因为当传送端继续传送数据时，TCP/IP却已经试图传送会话层（session-layer）的确认信息给传送端。

其他一些来源，例如协议堆栈所造成的负担，也会影响网络的性能。上述计算尚未剔除Beacon帧所造成的负担，也未考虑帧漏失对吞吐量所造成的影响。

块确认

有了上述范例，就比较容易了解“块确认”（block acknowledgment）这个概念的威力何在。帧间间隔与802.11确认信息用掉了原子交换操作10%以上的传输时间。只要调整数据帧与确认之间的比例，就可以大幅降低这些负担所耗费的时间。

改善性能

由于带宽有限，无线网络通常背负着性能不彰的罪名。如果有人这样抱怨，在研拟出改善性能的策略之前，当务之急就是找出客观评估性能的方法。

有些商用的网络分析软件会提供“信道利用率”（channel utilization）报告。报告的内容不外乎花费在传送与接收帧的时间比例或每秒传输多少兆位。比较起来，前者应该比较有用，因为它将“因距离接入点的远近而可能产生的速度变动”也纳入考虑。如果所有已关联的工作站均相距甚远，或许只能以1 Mbps的速率进行操作。假设信道完全以1 Mbps的速率进行传输，根据上例所描述的理想状况，以100%的信道利用率而言，可以达到0.94 Mbps的吞吐量。有些分析软件只会提供位传输率报告，但并不会提到利用率有多高。

如果有竞争无线电资源的情况发生，就应该加以调整来减少竞争的次数。提升性能的最好方法就是降低接入点的功率。只要缩小覆盖范围，工作站和接入点的距离就必然较近，如此将（有希望）可以较高的速率进行操作。

覆盖范围较小还有助于避免同信道（co-channel）的干扰问题。接入点必须在覆盖范围

内共享带宽。如果有两个高传输功率的接入点使用相同信道，就有可能相互干扰。虽然通信协议在设计时已经将此问题纳入考虑范围，不过两部设备同时进行传输还是会严重拖垮性能。另外指定不同的信道也有助于避免干扰，不过带宽还是受限于当前技术所容许的信道数。对802.11b与802.11g而言，完全独立的信道只有3个，还是可能受到邻近接入点相当程度的干扰。802.11a可以使用较多的信道，因此较适合应用在接入点密度较高且覆盖区域彼此重叠之处。

改换更好的物理层也是个办法。802.11b网络必须将已经不敷使用的6 Mbps带宽分配给所有已关联的工作站。802.11a与802.11g可以提供较高的吞吐量，一般约有30 Mbps左右。如果可能的话，升级所有工作站也有助于性能的提升，不过要特别注意802.11g保护机制。保护机制会大幅降低吞吐量。虽然无法提供精确数据，根据还算不错的经验法则推算，它大概会降低一半以上的吞吐量。

如果保护机制真的拖垮了整个吞吐量，当务之急就是予以停用，不过“说”通常比“做”简单。只要有任何802.11b信号，保护机制就会启动，不论工作站是否已经关联。既然802.11b设备的设备量不容小觑，802.11g网络大多被迫启动保护机制，因此大幅降低了整体的性能（注1）。

注意：至于高带宽、高密度的网络，最好采用802.11a。它的信道不仅比较多，也不必背负向下兼容的包袱。

有时候，性能其实受限于网络架构本身。如果在无线局域网络与其他网络之间建立一道防护墙，所有流量就会受限于单一瓶颈。如果该瓶颈无法负荷所有流量，性能就会因此大打折扣。安全协议也会对性能造成负面影响，例如IPSec允许上层协议传送最大封包(maximum-size packet)，不过一旦加上Ipsec标头，反而必须进行封包分割。分割之后，两者（最大封包与零星封包）均必须竞争媒介使用权才能进行数据帧的传输，因而会导致传输的延迟。

性能也有可能因为应用不同而被认为差劲。一般而言，数据传输相当具有灵活性，对于网络延迟问题比较宽容。数据帧迟到的情况并不构成问题，因为这不过意味着网页加载得较慢。数据传输的流量通常起伏不定，就算瞬间涌进大量封包，也是可以接受的。如

注1：由此看来，一般用户该选择802.11b/g还是802.11a就再清楚不过了。协助布设Supercomputing 2004会场的无线局域网络时，我发现80个接入点中塞满了1300位802.11b/g用户，而802.11a用户只有100人。用我的802.11a网卡，不仅无需和他人竞争无线媒介，也可以全速上网。

果网络需要支持实时传递，工程就变得比较复杂。语音传输必须要能够及时送达，次序不能错乱，流量也不能起伏不定。就算网络带宽可以支持数兆位流量的服务，但如果所提供的语音质量低于一般，还是令人无法接受。802.11 网络的服务质量（Quality of Service）依据刚开始形成的规范。虽然接入点承受得住少许的语音通话，但一旦网络负载增加或者语音数据无法及时传送，服务质量就会大打折扣。就算网络未达饱和状态，语音性能还是有可能十分差。

若要榨干每一滴网络性能，最后的手段就是微调802.11规范书所列的各种参数，下一节将针对这些参数做进一步的探讨。不过就我本身经验所及，调整802.11参数并无法大幅提升性能，因此不值得投注太多时间。接入点已经十分便宜，不如多添购几个，反而比较符合经济效益。

802.11 可调参数

802.11 有一些可供调整之处，可以在比较严峻的情况下尽可能挤出额外的性能。不过，如要找出最佳数值，不免要经过一番试验。

无线电管理

和其他类型的无线网络一样，802.11 网络最珍贵的资源即是无线带宽。无线频谱受限于管制当局，无法轻易增加。可喜的是，有些参数可以优化网络无线资源的使用状态。

信标间隔（Beacon Interval）

Beacon 帧在“基础结构型网络”（infrastructure network）里扮演着许多基本角色。基本上，Beacon 帧定义了整个“基本服务集”（basic service set，简称BSS）的覆盖范围。在基础结构型网络里，所有通信都必须通过接入点，就算在同一个BSS当中有两个工作站要传递帧亦然。接入点通常会固定在一点，如此一来，Beacon 帧的传送距离便不会因时间而改变（注 2）。工作站通过 Beacon 帧，可以判断出目前所处范围有哪些“扩展服务集”（Extended Service Set，简称ESS）可提供服务，同时利用所收到的信号强度来监视信号质量。

注 2：多径干扰（multipath interference）会在特定时刻产生特定的干扰模式（interference pattern）。某些特定地点有时位于接入点的覆盖范围，有时受到多径衰落的影响。不过，类似地点已在覆盖范围的边界地带，因此不该将之视为基本服务区域的一部分。此外，802.16(WiMax)极有希望能够在移动时提供连接与数据传输。

不过，传送 Beacon 帧会耗费无线带宽资源。如果缩短 Beacon 发送间隔，被动式扫描（passive scanning）就会比较稳定，也较为快速，因为Beacon帧会较频繁地将网络的存在公布给无线链路。Beacon间隔较短有助于提升漫游的效率，因为漫游中的节点收到覆盖信息的频繁度会因此增加。Beacon帧发送得越频繁，对移动较快的节点而言就越有好处，因为更新信号强度的相关信息的速度相对变快（注 3）。延长 Beacon 发送间隔间接提高了连接节点的省电能力，因为聆听间隔（listen interval）以及 DTIM 间隔都会因此改变，这些在“电源管理调整”一节都会加以探讨。延长 Beacon 发送间隔也可以让吞吐量有所提升，因为媒介的竞争会因而减少。Beacon帧所占用的时间是无法用来传送数据的。如果各位使用虚拟接入点网络，由于每个网络均需要有自己的Beacon参数集，负担就会急剧倍增。

RTS 阈值

802.11 包含 RTS/CTS 清空过程（clearing procedure），主要辅助较大帧的传送。任何大于 RTS 阈值的帧都必须经过清空过程，方能够通过 RTS 由天线加以传送，而且必须收到来自传送对象的 CTS 信号。RTS/CTS 主要对抗来自隐藏节点的干扰。通过通知邻近地区所有工作站即将进行帧交换，RTS/CTS 交换机制可将来自隐藏节点的干扰降至最低。802.11 标准规定，RTS 阈值应该设定为 2347 个字节。如果网络吞吐量相当低或重传帧比例偏高，可以降低 RTS 阈值以启动 RTS 清空机制。

第三章曾经提到，所谓的隐藏节点是指网络上存在工作站看不到的节点。在什么情况下会遇到隐藏节点？老实说其实不少。网络上总是有些角落，虽然节点能够与接入点直接通信，但节点之间却无法彼此对话。想象一个最简单的网络：一个接入点位于广场中央，没有其他事物可以反射或阻挡信号。一个移动式工作站从接入点所在位置向东移动，直到信号微弱到几乎无法通信。另外一个工作站往西移动。两个工作站都可以和接入点通信，不过彼此都无法得知对方的存在。

以上的模拟状况应该可以说服各位，隐藏节点其实不可避免，但并不常见。工作站与最近的接入点之间如果相去甚远，在恶劣的环境下，就有可能导致隐藏节点。不过，既然无线网络已经十分普及，四处林立的接入点实际上已经足以避免大多数的隐藏节点问题。

分段阈值

MAC 层的帧分段，是由分段阈值（fragmentation threshold）这个变量所控制。任何大

注 3： 不过，802.11 原本就不是针对高速移动而设计的。蜂窝（cellular-based）广域技术在这方面较占上风。

于分段阈值的帧都会被分割为较小的单位，再加以传送。分段阈值的默认值是2346，或物理层所容许的MAC帧最大长度。不过，RF物理层所使用的MAC帧长度通常是4096个字节，因此这个参数通常默认为2346。这个值立即会让人联想到其与RTS/CTS清空过程经常一并运行。

在干扰十分严重的环境中，调降此阈值可以提升整体有效吞吐量。一旦漏失某个帧片段，需要重传的部分也只有该片段。从定义可知，漏失的帧片段必然小于整个帧，因此重传所需花费的时间较短。设定这个参数必须特别小心。设得太低，有效吞吐量反而会下降，因为确认每个片段必须用掉额外的时间；同样地，设得太高也会降低有效吞吐量，因为较大帧一旦损毁，便会增加无线信道重传的负担。

重传限制

网络中每个工作站都具备两种重传限制（retry limit）。其中之一是丢弃帧之前可以重传的次数限制。长帧重传限制（long retry limit）适合大于RTS阈值的帧，默认值为4。需要用到RTS/CTS清空机制的帧有4次重传机会，如果该帧遭丢弃，就会通知较上层的协议。短帧重传限制（short retry limit）适合小于RTS阈值的帧，默认值为7。

降低重传限制可减少每个系统所必须准备的暂存空间。帧越快逾时，丢弃这些逾时帧的速度就越快，因此内存更新速度也越快。提高重传限制可能会降低吞吐量，因为与上层协议间的交互会更加频繁。当TCP遗失封包时，较好的解决方式是放慢速度。较大的重传限制值也可能增加宣告封包遗失所需要的时间。

电源管理调整

从一开始，802.11就是为移动设备而设计的。移动设备之所以有用，就是因为它不受电源线的限制，因此大多配备电池。802.11包含了一些参数，可让工作站节省电力，然而代价是牺牲整体吞吐量或造成工作站的延迟。

聆听间隔

当工作站与接入点关联时，所指定的参数之一即是聆听间隔（listen interval）。所谓聆听间隔，是指工作站两次苏醒之间历经多少个Beacon间隔数。较长的聆听间隔可让工作站关闭传送器较长的时间。关闭电源较久，意味着可以省下更多电力，因此显著延长了电池的使用时间。每个工作站都可以设定自己的聆听间隔。

延长聆听间隔有两个缺点。接入点必须为休眠中的工作站暂存帧，因此较长的聆听间隔对接入点而言，意味着必须准备更多暂存空间（缓冲区）。如果聆听间隔较长的工作站为数甚多，就可能超出基站暂存空间的负荷。其次，增加聆听间隔会延迟帧的传递。如

果接入点准备转送数据给工作站时工作站正处于休眠状态，该帧只好等到工作站苏醒之后再加以传送。苏醒之后，工作站必须从所收到的Beacon帧中，判断接入点上是否有暂存帧，然后送出PS-Poll帧以获取暂存数据。整个暂存与获取过程会增加帧的传送时间。这种情况是否可以接受，完全取决于对流量的需求。就电子邮件之类的异步传输而言，延长聆听间隔不会造成太大的问题；不过对于实时性、时间敏感度要求较高的应用程序（例如，证券市场实时信息或未来通过802.11接口的IP phone）而言，就无法接受较长的聆听间隔。延迟时间增加对某些特定的应用程序而言有可能产生问题。数据库应用程序特别容易受到延迟时间的影响。目前已经有一个任务组着手MAC的改良工作，以便在802.11网络中确保传输的服务质量，不过标准目前尚未形成。

DTIM周期

DTIM周期仅限基础结构型网络使用，所有与接入点关联的节点均会共享此一参数。这个参数由接入点管理人员设定并且在Beacon帧中加以广播。所有Beacon帧均包含一个“传输指示映射”（traffic indication map，简称TIM），用以告知工作站是否有暂存帧待传。为个别工作站暂存的单播帧只有在工作站轮询时才会加以传送。这种轮询的方式并不适合于组播或广播帧，因为这样一来必然耗费不少带宽，而且传递组播帧与广播帧要花费一番工夫。基本上，广播与组播帧是在每次DTIM（Delivery TIM）周期过后传送的，而不是使用轮询的方式。

改变DTIM与改变聆听间隔有相同的效果（这并不值得惊讶，因为DTIM如同组播与广播帧的聆听间隔）。增加DTIM可让移动式工作站节省较多的电力，不过代价同样是必须耗费接入点更多的暂存空间以及响应时间的延迟。增加DTIM之前，最好确定一下所有应用程序均容许延迟时间的增加以及广播与组播并不是用来同时传递数据给所有工作站。如果应用程序使用广播与组播帧来确保所有工作站同时收到相同数据，例如实时跑马灯，增加DTIM反而会造成反效果。

ATIM窗口

在基础结构型网络里，大部分的省电功能是接入点所提供。在独立型（或特设）网络中，部分省电功能则移交给网络接口的驱动程序处理。在特设（ad hoc）网络中，工作站必须随时保持清醒以便传送或接收Beacon信号，而且在ATIM（Announcement TIM）窗口的持续时间中也必须处于清醒状态。ATIM窗口是以时间单位（TU）来度量。

减少ATIM窗口可以节省较多的电力，因为移动式的工作站所需要的开机时间会因此减少。在两个Beacon间，工作站可以关闭电源，这段期间不必有任何动作。增加ATIM窗口也同时提高了工作站苏醒的几率，如果其他工作站也有帧待传的话。服务质量也会因此而提升，所需要的暂存空间也相对较小。

对同步或实时应用而言，减少或不用ATIM窗口的效果，相当于在基础结构型网络里延长DTIM周期。换句话说，对于要求实时传递数据的应用，这可能会引起问题或导致不稳定。联机游戏是“对等式”（ad hoc）网络最显著的实时应用，不过“对等式联机游戏”（ad hoc gaming）的网络在调整上通常侧重于低延迟与高吞吐量，而非省电功能。

定时操作

定时操作是802.11网络中一项要件。许多管理操作都牵涉到好几个步骤，每一项操作都会用到自身的定时器。

扫描定时

为了决定要加入哪一个网络，一开始工作站必须先扫描现有网络。有些产品允许用户设定扫描时间。在这些产品中，可能会同时开放主动扫描定时器（*active scan timer*）与被动扫描定时器（*passive scan timer*）供用户设定。所谓主动定时器，是指工作站送出Probe Request帧之后预计花费多少时间等候响应信息，以TU为单位。所谓被动式扫描，是指工作站聆听各个无线信道的Beacon帧；而被动式扫描定时器，是指工作站切换到下一个信道前在每个信道所停留的时间。

与加入网络有关的定时器

当工作站发现所要加入的基础结构型网络，就会与接入点进行身份验证并与之关联。每个步骤都有相应的逾时定时器。认证逾时（authentication timeout）在认证过程的每个阶段都会重新设定，如果有哪个步骤逾时，认证就算失败。在较忙碌的网络中，可能必须提高逾时值。关联逾时（association timeout）在关联过程中扮演着类似的角色。

驻留时间（只见于跳频网络）

FH PHY停留在单一信道上的时间称为驻留时间（dwell time）。它通常是由当地管制当局（local regulatory authority）所规定，因此无法设定，除非通过网卡驱动程序变更到不同的管制区（regulatory domain）。

可调参数一览表

为了便于查询，表25-1列出了本章所有内容的一览表，包括每个可调参数可能造成的效果。

表25-1：可调参数一览表

参数	参数的意义及其单位	调低参数所造成的效果	调高参数所造成的效果
Beacon（信标）	Beacon 帧之间所历经的时间，以 TU 为单位	被动扫描较快完成，移动式工作站移动较快时仍能保持连接	无线容量与吞吐量微幅增加，同时可以延长电池使用时间
RTS Threshold（RTS 阈值）	大于此阈值的帧以 RTS/CTS 过程来处理	在隐藏节点十分常见的情况下可大幅提高吞吐量	理论上的最大吞吐量增加，但只有在毫无干扰的情况下方能真正获得改善
Fragmentation Threshold（分段阈值）	大于此阈值的帧以分段来处理	干扰果应只及于帧片段，而非整个帧，因此可以提升有效吞吐量	降低帧片段确认信息所造成的负担，有助于提升无噪声地带的吞吐量
Long Retry Limit（长帧重传限制）	大于 RTS 阈值的帧的重传次数限制	帧较快被丢弃，因此所需要的暂存缓冲区较少	到达重传限制的时间拉长，TCP有可能因此降低所使用的数据率
Short Retry Limit（短帧重传限制）	小于 RTS 阈值的帧的重传次数限制	与 Long Retry Limit 同	与 Long Retry Limit 同
Listen Interval（聆听间隔）	处于省电模式的工作站两次醒来之间所历经的 Beacon interval 数	可以减少传送给工作站的多播帧迟延时间。同时有助于减轻接入点缓冲区的负载	由于收发器关闭时间较长，因此可以节省电力
DTIM Period（DTIM 周期）	两次 DTIM 之间所历经的 Beacon interval 数（只适用于 infrastructure 网络）	传递数据给处于省电模式的工作站时可以减少组播与广播帧的迟延时间。同时有助于减轻接入点缓冲区的负载	由于收发器关闭时间较长，因此可以节省电力
ATIM Window（ATIM 窗口）	在 independent 网络中，Beacon 帧发送后工作站必须保持清醒的时间	允许移动式作站在 Beacon 帧发送后较快关闭收发器，可以节省电力	可以改善处于省电模式工作站的延迟状况，有助于减轻网络上其他工作站的缓冲区负载
Active Scan Timer（主动扫描定时器）	工作站送出 Probe Request 帧后，预计花费多少时间等候响应信息	进行扫描时工作站会快速切换信道	扫描费时较久，但成功几率较高

表25-1：可调参数一览表（续）

参数	参数的意义及其单位	调低参数所造成的效果	调高参数所造成的效果
Assive Scan Timer（被动扫描定时器）	工作站监测个别信道是否有信号存在所花费的时间	如果扫描时间过短，工作站有可能找不到网络	扫描费时较久，但成功几率较高
Authentication Timeout（身份验证逾时）	身份验证过程中，每个帧之间最长不得超过多少时间	身份验证过程加快。如果此逾时值甚小，可能必须重试相当多次	没有显著影响
Association Timeout（关联逾时）	关联过程中，每个帧之间最长不得超过多少时间	关联过程必然加快。如果此逾时值甚小，可能必须重试相当多次	没有显著影响

第二十六章

结论与展望

预测并不容易，尤其是预测未来。

——Yogi Berra

我们终于可以一窥当前 802.11 网络发展状况的全貌。本章里，我们打算取出水晶球，看看事情将如何发展。首先，我们关注的是目前正在进行且即将完成的标准。之后，我们将采取较长远的视角，试着勾勒出无线局域网络的发展方向。

标准化工作

802.11标准的出版只不过是整个无线局域网络标准化过程的开端。为了让标准可以出炉，事实上一些公司做了不少妥协，有些工作只是留待未来解决。802.11 工作组的业务完全对外公开，任何人均可访问该小组的网站 *http://grouper.ieee.org/groups/802/11/*，以得知802.11 修订工作的最新进展。在标准发展的过程中，任务组会在网站上发布更详尽的报告，包括各种提案的票选结果。

标准的修订由任务组（Task Group）负责。任务组以英文字母来划分，任何标准修订的结果则沿用相应任务组的英文字母代号。例如，OFDM PHY 标准是由任务组 A（TGa）负责，其所修订的标准就称为 802.11a。

本书第一版问世之后，陆续有几份标准的修订通过审核。54 这个数字随着802.11g产品营销到世界各地。802.11h 修改了 802.11a 所使用的底层技术，使之适用于欧洲，同时说服美国政府在全球协调频带(worldwide harmonized band)开放新的频谱。目前，802.11i 已经大幅平息了用户对于安全性的疑虑并且用 AES 加密技术取而代之。

新的标准

目前有几份标准特别值得注意。802.11依然是新技术开发的沃土。未来，任务组必须以两个英文字母来命名，由此即可看出802.11技术已臻成熟。

任务组E：服务质量

比起有线网络，无线网络的带宽相对有限。任务组E正着手通过多组队列操作与保留媒介使用权等方式来提供服务质量（quality of service，简称QoS）的相关标准。为了进一步提升服务质量，802.11e将会定义一种新的协调功能，称为混合协调功能（hybrid coordination function，简称HCF），以及新的网络访问方式。此外，任务组E也定义出所谓的块确认协议（block acknowledgment protocol），以减少容易造成网络负担的零散操作。

802.11e已经耗费了很长的开发时间（原本802.11e同时涵盖QoS与安全性，后来安全性转由任务组I负责，如今802.11i已完成）。由于标准久久无法定案，于是业界从目前的草案中挑选出部分功能，让实现上有个过渡性的依据，即所谓的Wi-Fi多媒体标准（Wi-Fi Multi-Media，简称WMM，请参考*http://www.wi-fi.org/OpenSection/wmm.asp*）。WMM对于802.11e，就好比WPA对于802.11i，两者均属于标准制定过程中的阶段性成果（snapshot）。

任务组K：无线电资源

移动电话网络广泛使用无线电测量技术，让无线电的容量得以优化。有些802.11产品已经开始尝试监控信号质量，不过目前并没有所谓的标准做法。任务组K正着手开发一项供802.11使用的标准，让接入点能够搜集信号的相关统计数据，以此决策出较明智的操作方式。其所定义的测量方式允许802.11工作站搜集诸如噪声分布（noise distribution）、隐藏工作站（节点）数目以及特定操作信道负载等相关信息。

任务组N：高速（100+ Mbps）MIMO物理层

TGn原本收到四份完整的提案。不过剔除其中两份后，只剩下本书第十五章所提到的两项提案。经标准委员会投票表决，TgnSync的支持度稍微领先于WwiSE。由于两者差异颇大，可见在最后标准制定之前，尚会面临一番激战。

根据TGn提案所开发的产品其实不能宣称该产品符合802.11n草案（draft 802.11n），因为所谓的官方标准草案根本尚未出炉。更何况在本书付印之际，还不知道会采用哪份提案。号称“pre-N”的产品必须冒着被撤销Wi-Fi认证的风险。因此，有些根据特定提案所开发的产品遂自称为“MIMO”。

未来标准

任务组P正着手开发车用802.11标准，称为车用环境无线访问（Wireless Access in Vehicular Environments，简称WAVE）。汽车的移动速度较快，需要补充强切换（necessitating handoff）方面的功能。其中还包含对等（peer-to-peer）功能，可以在车辆间构建网状（mesh）网络。和其他形式的802.11网络不同，未来它可能会需要使用得到许可的频谱。802.11p原本是设计来作为搜集与下载安全信息的一种标准方式，不过有人认为它最终会取代蜂窝式通信（cellular communications）。

任务组R正着手开发漫游协议（roaming protocol）。802.11i的事先认证（preauthentication）有其限制，因为它无法减轻漫游的运算负荷。TGr所定义的协议主要是通过网络传递密钥材料来避免上述缺点。在2005年1月所举行的会议中已经剔除了一些提案，这是通往最后标准的路途中迈出的重要一步。

任务组S负责开发网状网络（mesh networking）标准，主要用于多跳（multi-hop）环境，目前尚处于起步阶段。

任务组U负责修改802.11，使之能与其他网络技术互通。它的目标与802.21工作组类似。TGu针对802.11做了必要的修改，以便与第三代移动电话等网络技术互通，至于802.21则负责开发一种可以兼容所有网络技术的独立框架。

相关标准

802.1X原本是针对有线网络设计的，而应用在无线网络时，一直受限于某些临时性的标准。本质上，这些过渡性的标准只能算是实现上的协议，如何将访问控制整合到无线网络实际上还是一团糟。802.1X-2004制定出了新版的EAPOL，同时厘清了两种状态机器（state machine）的操作方式。目前它并未被广泛采用，不过可以确定的是，市场上应该很快就会推出相关产品。

随着更多用户采用不同的无线技术，且由于这些技术拥有各自的覆盖范围和距离，于是这些网络之间的切换问题（inter-network handoff）开始浮现。例如，有些移动玩家在热点（hot spot）使用802.11网络，在车上则使用移动电话网络传递数据。如何在两种截然不同的网络间实时切换是802.21工作组的焦点所在。

无线网络的当前趋势

长远来看，无线网络的发展将会呈现何种面貌？在家用市场，802.11几乎已经逐退其他对手（例如HomeRF），巩固了它在短距离数据访问上的地位。不过就长期而言，移动性与安全性方面的议题还是比较重要，虽然两者尚有一些不易解决的问题。然而，就安全

性议题而言，目前已经从纯粹防御性的封闭模型转为较灵活的无线网络，而且可以快速导入应用。

安全性

安全性向来是无线局域网络的主要议题，不过近来所提出的协议已经平息了许多针对无线网络的抱怨。网络与用户之间的交互认证如今可以通过802.1X与EAP完成。802.11i为无线局域网络提供了网络管理人员所期盼的坚固、可信赖的加密方案。WPA则为网络提供了实用上足够的安全性，而业界也允诺设计出符合严格安全标准的协议。

目前网络设计的新趋势是将无线网络与既有网络整合在一起，而不是将无线网络置于孤立的环境中，导致它未能发挥应有的功能。无线网络让用户摆脱空间的限制，进而提高生产力。早期的无线网络在有线与无线网络间设置了访问控制，迫使用户学习新的数据访问方式，而这会白白浪费许多应有的生产力。较坚固的安全协议让用户得以将网络视为单一整体。用户访问数据时可将之视为局域网络，而不需要通过麻烦的远程访问过程。

改变无线局域网络的安全性模型非常依赖于用户身份验证功能。在用户账号与网络活动间建立密切的关联性，才有所谓的“责任”(accountability)，足以消除各种形式的网络误用。同时，身份验证也让无线局域网络安全性不再是着眼于一般的防堵机制，而是将重点放在类似局域网络所使用的安全模型上。

身份验证协议

如今，RADIUS几乎已经成为身份验证的代名词。无线局域网络赋予了RADIUS新的生命，不过事实上，RADIUS是Internet真空管时期的产物。大多数用户已经不再使用调制解调器拨号，不过这个原本为拨号用户设计的协议如今却成为了局域网络媒介（LAN medium）的基础。RADIUS之所以不适合应用于局域网络的访问（LAN access），是因为加诸其上的种种复杂性。用过市面上的RADIUS服务器的人都知道，晦涩难解的配置文件可说是复杂无比。

认证协议本身需要与时俱进，方能跟得上IP传输商品化的脚步。无线网络已经驱使大部分组织在某种程度开放网络访问供访客使用。当IP传输越来越便宜，供给越来越容易，用户就会开始期待能够在更多地方访问更多数据。认证协议需要适应更加开放的环境，使用户能够在任何地方访问网络。特定的服务供应商，如iPass，已经开始提供类似的服务，打造Internet2的研究大学（research universities）（译注1）也开始进行类似的项目。

译注1：研究大学（research universities）是指提供完整学士课程并且能够授予硕士及博士学位的大学，“研究”为学校的发展重心。

要建立所谓的“联邦网络”(federated network)，先决条件是身份验证系统必须具备扩展代理能力(extensive proxy capability)，这样网络系统才有办法确认来自不同组织的访客的身份。如果未来Internet身份验证系统演变成带有类似DNS的功能，可以让组织找到能够验证访客的服务器而不必预先建立信任关系，我也不会因此感到惊讶。

权限控制

当网络更加开放且允许访客访问，网络安全就具备了一种崭新的含义。确保组织的设备安全是项艰巨的任务，但并非没有现成的解决方案。通过平台标准化、随时注意是否需要进行安全性修补、为网络部署防火墙以及随时更新防病毒与入侵侦测程序，即可确保一定程度的安全。不过，如果危险因素来自外部的机器，这种“随时保持更新”的安全模型就有可能失灵。虽然公司可以为内部设备提供安全防护软件，然而访客的机器却只能自求多福。有些新的软件解决方案将网络授权(network authorization)的概念加以延伸，亦将访客机器的使用状态涵盖在内。只有被验证为“干净”的机器才可以访问网络。权限控制(admission control)是延伸授权的一种方式，不仅考虑到用户的权限，还包含了用户计算平台的安全状态。

私设设备监控

如何通过防范未经授权的无线局域网络部署以控制无线频谱，向来是无线局域网络安全课题的一个主轴。虽然其中牵涉到一堆工程任务，但理论上还是和过去没有什么两样。基本做法除了监控无线频谱以检测是否出现不该有的AP，如有必要，还可以采取适当的步骤予以关闭。近年来，这项工作进一步扩及监控内部网络是否遭人盗用，有时也用于客户端设备。

如果发现身份不明的设备，首先必须加以分析以决定威胁的程度。连接到其他骨干的无线网络不致构成威胁，不太可能成为攻击的目标。如果和其他公司共享办公室，信号必然会泄露到邻近区域。攻击别人的网络不仅会破坏彼此的关系，也有可能触犯计算机犯罪法(computer crime laws)。为了提供网络安全，必须将各种威胁加以分级。没有连接至贵公司网络的免许可证无线设备且不在你的监督与安全控制范围内，则必须将其排除在外。对于访客或其他人所使用的ad-hoc网络也不该予以干涉。只要受到适当保护，连接到贵公司网络的接入点也可以被排除在外。

和其他领域没什么两样，巩固网络安全是每日的基本功课。检测与评估私设接入点的功能已经逐渐内置到无线基础设施中。虽然有些公司开始使用额外的设备来提供监控与安全服务，但大多数网络部署实际上已经整合进了所需要的基本功能。

网络部署与管理

无线局域网络一直依循之前两种创新的典范。个人计算机与局域网络的发展一开始都不在IT人员的雷达检测范围（under-the-radar）内。不过，这两种技术最后都演变成通过中央管理的服务，给网管人员提供了不少信息。无线局域网络已经脱离这段远离雷达检测范围的阶段，迅速成为标准的连接方式。

如今，网络部署的主要挑战在于如何超越简单的覆盖模型（coverage model）。早期的无线网络在设计上只是为了涵盖特定区域。不过随着用量的增加，定点覆盖已经不够使用。如何确保较高的容量乃是协议开发与部署的首要课题，特别是在那些用户已经习惯宽带有线网络的地区。

网络规划

传统的802.11网络规划是件吃力不讨好的事，不但要到处游走，还得手动测量一堆数据。和其他技术创新一样，当人们更了解底层机制，就会开发出一些工具来改善规划流程。这些工具相当于将无线电专门技术外包出去（outsourcing），毕竟大多数网管人员都不是无线电专家。

其中一类工具会借助平面图（floor plan）以及建筑知识（architectural knowledge）计算出需要多少接入点及其摆放位置，另外一些工具则是使用动态无线电校正，好让网络适用于该环境。有些产品同时采用这两者。不论如何，过去昂贵费时的实地勘探（site survey）已经没有必要。实地勘探不仅是劳动量大，价格也过于昂贵。

就像以往设计师必须学习如何将网络布线整合到建筑规划中一样，他们也得学习如何将802.11整合到设计过程中。如同以往，尽早确定需求绝对有帮助。对于需求有了初步的概念后，就可借助工具计算出初步的AP摆放位置。将取得的信息反馈给建筑师与室内设计师后，建筑的规划就可以提升网络性能，同时也将麻烦减至最少。如果AP摆放位置纯粹迁就美感或容易安装，网络的覆盖范围就会受影响。

不过并非经过规划之后整个过程就此结束。由于计算出来的模型不见得完美，可以预见后续还得变更原始设计。构建无线局域网络时，通常必须经过好几个回合的反复测试与优化。幸好，随着接入点价格的下降，如今已经不必斤斤计较可以省掉几个接入点。

规划出实体结构后，接着必须厘清打算采用何种网络逻辑结构。随着无线网络逐渐普及，无间隙移动性就成为了众所期盼的重点。无间隙移动性的需求通常与机构大小无关。如果建筑物相当庞大，规划起来可是饶富趣味的挑战。

回程线路

互用性实验室（Interop Labs）有一则流传已久的笑话，内容是说，有些无线局域网络新手需要大量的Ethernet网线与电源线，以便供电以及连接所有接入点。事实上，无线网络所使用的电电缆比起其他技术的丝毫不逊色。到目前为止，无线网络还是依靠后端的布线来提供网络连接与供电。

一般而言，布置网线要比电源线简单，理由有多个。为了简便，接入点通常只用一条线同时联网与供电。不过，有时候情况并不允许。例如在较大的会场里，天花板里布有供照明用的电源线，却没有网线。因此有些公司着手研究如何以无线网络为骨干，不必为了无线局域网络再去安装网线。双模接入点（dual-radio access point）可以使用其中一种信号提供服务，以另一种信号作为上行链路（uplink），电源线仅用来供电。网状骨干技术在一些布线困难的环境中特别有用。在超过100公尺的Ethernet网线派不上用场的情况下，这可能是唯一的解决方案。

迷你“管制者”与仲裁者

使用802.11很容易引发频谱方面的争议，特别是802.11b与802.11g所使用的2.4 GHz频带已经拥堵不堪。频谱免许可证意味着所有人均可使用，没有所谓先占先赢的事情。2002年年末，T-Mobile在Portland的个人电信公司（Personal Telco）（译注2）的地盘上装设新的接入点。由于两家的接入点使用相同的操作信道，因而造成彼此的相互干扰。既然技术上无法解决干扰问题，于是双方互相提出要求。

虽然Portland事件是最早曝光的频谱之争，但可以预见往后还会陆续发生更具争议的问题。有些机构试图以特定方式控制无线频谱。小型办公室林立的建筑物可能会使用单一无线局域网络配合多个虚拟无线网络。有些机场只允许单一实体无线网络，然后将网络容量出租给旅客、航空公司与商店。由于不少的协议内容已经侵犯到电磁频谱的管辖权，因此FCC宣告这些协议均属无效，除了某些少数的特例（注1）。

译注2：这是无线网络的自愿型或小区型应用。拥有宽带上网线路的计算机用户利用某种系统来建立无线网络，让一定范围内有上网需求的任何人都可通过他们的宽带网络上网，而不必向宽带商家申请宽带上网。这种宽带上网服务是免费提供或以比个人宽带费用低很多的价格来提供的。在美国提供此类服务的有Bay Area Wireless Group、Seattle Wireless、Portland's Personal Telco Project、NYCWireless.Net以及Boston's GuerillaNet。

注1：详见FCC于2004年6月所发布的文档DA-04-1844A1（网址位于*http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-04-1844A1.pdf*）的这段文字“重申（reaffirm）……不论立场为何，唯独FCC有权裁决免许可证设备的射频干扰（RFI）争议……消费者安装与操作自制天线时必须遵循FCC法规……这些规定适用于免许可证器材的使用，例如Wi-Fi接入点。”

自动无线电调谐技术（automatic radio tuning technology）只能算是部分的解决方案。既然信道有限，有时候就不可能将干扰排除至最佳状况（打造远距802.11网络的热潮使得问题更加严重，如此一来就有更多802.11信号会被传至拥堵地区）。有时候，技术高手（technically competent individual）可以协助解决用户间的争端。有些高科技小区已经出现类似问题，亦即左邻右舍均使用相同信道。有些自愿者已经在邻居间成立频率分配委员会（frequency allocation committee），协调四周的邻居所使用的信道以便改善性能（注2）。既然不具法律权威，这些仲裁者或管制者其实并没有法律强制权，所依靠的只是技术上的权威。

访客访问

不过更重要的是，未来需要各种不同的访问管理方式。许多早期的无线局域网络只是附属于公司网络。现有的身份验证概念是针对已知、静态的用户组（如公司员工）而设计的。为员工提供网络访问服务是项重大的任务，不过这只是冰山一角。就像移动电话一样，无线网络当初的承诺是不论多么偏远，不论用户身在何处，均能够随时联机。

公共空间（如机场或车站）的802.11网络设计必须将允许谁使用网络以及这些人享有何种权力等相关问题纳入考虑。网络服务必须经过身份验证，同时必须保护用户相互间的安全。要提供牢靠的服务给不同的用户组，同时组间必须彼此独立，需要在网络结构上加以思考。

高等教育机构不断在测试访客访问的底线。研究小组通常跨越多个研究机构，学者也常常在不同地方进行访问。有个项目计划构建一个“联盟”（federation），让加入联盟的机构用户也可以使用其他成员的网络，而不必在各个机构分别申请账号。这项计划的挑战涵盖了纯技术性的议题、技术与过程的具体细节交集以及纯策略上的议题。在技术层面上，各成员间必须建立某种形式的可信赖身份验证链路（trusted authentication link）（注3）。虽然有其限制，但这些联盟仍习于使用RADIUS。

然而，就算用户由自家的机构进行身份验证，还是必须将此用户与访问网络的内部人员区分开来。为了提供可说明性，该用户的身份数据必须传给被访问机构。被访问网络的管理人员所要求的可能不只是用户姓名而已。如果某个访客染上蠕虫或其他病毒，就必须将该访客的计算机隔离并通知该用户手动加以清除。不过如果访客来自远方，可能无法联系该访客的在藉机构以取得联系。举例来说，在身份验证过程中，主动提供移动电

注2：详见Associated Press的相关报道（*http://community.bouldernews.com/business/02bwire.html*）。

注3：EduRoam（*http://www.eduroam.org*）即属此类项目。其他地区也有类似项目正在进行。

话号码就可以协助管理人员。不过，主动提供特定信息的同时得兼顾隐私，这本来就是当前的身份验证协议所面临的主要技术挑战（注 4）。

应用

无线网络的首要应用乃是自由——免于有线的自由以及免于没有网络可用的自由。用户可以四处移动，但网络插座可不是。第一代的应用采用虚拟的 Ethernet，这让许多应用程序无需改变即可使用。当应用程序开发人员逐渐累积经验后，就会开始在应用程序中缓存一些数据，因为他们知道网络连接可能转瞬即逝。

无线网络在促进公用运算（utility computing）方面也扮演着重要的角色。既然各种应用在网络上，就需要更普遍的网络访问方式。通过身份验证方式以及运算设备的无线局域网络接口的改良，网络本身就成为这些应用的中介。较佳的身份验证系统也有助于驱使各式应用实行单点登录机制（single-sign-on）。

定位

早期无线网络的应用通常只是移植自有线网络，新式应用则是运用了比较多的位置信息。会议通常是在较大型的建筑物中进行，为了引导与会人员，通常会花费不少资金在标示牌上。目前，有些会场已经开始以无线网络来提供位置信息，可以让与会人员自定义路径，同时也提供“最近场所”（what's near me）的导览应用。IBM Research 开发出一套办公室系统，可以追踪人员以及更新所在位置信息（注 5）（还好，未来定位的相关发明可以比较不那么“老大哥”）。

语音

期待多年之后，网络语音（voice over IP）的时代终于来临。有些服务供应商现在已经能够在DSL上提供比移动电话更好的语音质量。经过多年的抗拒，如今消费者已经开始接受这种科技，虽然通话质量不能说是顶尖，但是较有灵活性。

802.11 是下一代无绳电话（cordless phone）通信协议的强势竞争者。目前，打算同时使用无绳电话与802.11 网络的用户请注意，无绳电话必须使用不同的频带（有时候可以

注 4：正因为缺乏适合的商业解决方案，因此Internet2 联盟着手开发了一套称为 Shibboleth（*http://shibboleth.internet2.edu*）的软件系统。

注 5：这就是与办公家具制造商 Steelcase 合作开发的 cubicle 项目，详见 *http://www.research.ibm.com/bluespace/*。

趁清仓大甩卖或者到 eBay 上看看还有没有旧式的 900 MHz 无绳电话），不然就得祈盼买来的无绳电话能与 802.11 和平共存。利用 VoIP，无绳电话可以分享相同网络，如此一来就可不需担心上述问题。未来消费性电子产品如果配合 802.11，会进一步降低芯片成本，进入良性循环。

在我看来，802.11 VoIP 手机缺少身份验证功能的缺点很快就可以得到解决。到目前为止，大多数手机除了过滤 MAC 外，还没有什么安全功能。802.1X 身份验证配合 EAP 加密模式是最起码的安全性要求。如果话机采用会谈开始协议（Session Initiation Protocol，简称 SIP），就可以在有 802.1X 能力的 hot spot 上使用。电信商可以在通话密集的区域构建较便宜的802.11网络来分担移动电话的话务，不用另外购置昂贵的移动电话设备。不过，要在两种截然不同的基础设施之间切换话务显然没有那么简单。

数据广播

无线网络本质上属于广播媒介。和Ethernet一样，工作站会接收到往来于802.11 网络的所有帧，帧过滤规则在此同样适用。Ethernet 与 802.11 的主要差异在于无线电（radio）很难与交换（switching）类比。802.11 帧会传递到四面八方，无法像雷射一样聚焦以将数据传递给特定接收对象。组播帧可以用来构建提供数据广播给多个接收者的应用程序。只要有适当的可靠协议，就可以赋予无线局域网络小规模的广播能力。就像有些电视台利用数字电视的闲置带宽来传送数据，无线局域网络也可以成为短距离的视频广播机构。有些消费性电子厂商已经开始参与 802.11 标准的制定，因此通过 802.11 进行影像传输并非完全遥不可及。

协议架构

客户端拥有太多权限是 802.11 常见的议题。在 802.11 中，所有工作站可说是生而平等。假设有 19 个用户关联到接入点，而接入点却只负责 5% 的协议处理事宜。基本上，要求网络基础设施负责50%的协议处理事宜并不为过。后续成立的任务组已经朝这个方向前进，使控制权更加集中，希望在漫游、切换与服务质量方面能有所改善。

联盟与移动性

从协议架构的角度来看，联盟（federation）与移动性（mobility）密不可分，因为两者攸关网络共享或设备在管辖权不同的网络之间的可移植性。借用移动电话的术语，这些概念开始导致数据层面（负责传递数据）与控制层面（负责提供身份验证与权限管理以及为数据层面设定网络）之间的分工。

当欧洲电信专家撰写第二代蜂窝式移动网络（cellular network）的相关标准时，显然没

有任何一家电信商拥有足够的资源，可以构建一整个泛欧蜂窝式移动网络（pan-European cellular network）。无绳电话的发展起初受限于缺乏一种可以涵盖欧洲所有区域的共通标准。这些专家了解，移动电话的价值与其可使用的范围成正比。因此，当GSM标准最后被采用时就特别强调漫游功能，允许用户使用不同的网络，而由单一电信商收费。

当802.11的使用率逐渐增长，身份验证与跨网络漫游标准就越加重要。3G许可证惊人的成本已经迫使一些电信业者面临破产边缘。为了找寻出路，有些电信商已经计划共同分担基础建设，以便分摊昂贵的3G网络构建成本与风险。许多802.11热点服务供应商同样面临类似的处境，共组联盟之后，就可以让用户访问其他商家的网络。

当类似情况变得更为普遍，结盟的效果就会超越服务供应商的层面，进而涵盖策略联盟公司以及研究机构。由于RADIUS不够使用（does not scale）或是无法提供必要的功能，因此必须另外开发用来识别与管理访客的相关协议。

随着802.11逐渐普及，熟悉其他网络技术的组织所具备的优势就更加明显。受到便宜、频谱免许可证的吸引，许多电话公司已经开始筹建自己的供应商体系以提供802.11服务。现有的电话公司则是利用802.11网络来推销WAN宽带业务。移动电话厂商也开始利用802.11作为扩展移动通信网络的便宜的替代方案。目前这项服务已经推出，也发布了几款802.11/3G双模手机。802.11与广域技术的结合其实很自然，毕竟它可以在通话密集之地提供充足便宜的容量，将长途网络留给更适合的技术服务。

允许快速移动的同时又能降低网络负担是许多标准制定小组的目标。虽然802.11i预先身份验证协议可以大幅缩减切换接入点所需要的时间，但是并不能减轻网络处理所必须面临的负担。要产生成对主密钥（pairwise master key），还需要进行完整的802.1X身份验证。因此，对RADIUS服务器而言负担并没有改变，何况跨广域网络（WAN）的预先身份验证可能必须得到千里之外的响应。要提供因特网规模（Internet-scale）的移动性，能够在网络间传递（而不是等到每次接入点进行切换时才取得）密钥就变得十分重要，这些协议是由任务组R负责开发的。

未来的协议

虽然无线网络具有相当大的灵活性，却也因此造成管理上不小的负担。要能自动搜寻网络具备何种能力，就不能局限于低端的无线参数，这样网络方能宣布身份验证的方式。

以往，接入点的功能受限于底层的硬件。新式的无线电产品比较侧重软件功能，甚至连接入点本身也更加面向软件。当接入点功能逐渐倾向于完全由软件定义时，市场就进一步区分为高端与低端两个等级。低端产品大概就是将公版（reference design）稍作修改随即大量生产；至于高端产品，则是可以在其公版上运行高度自定义的软件。

为了让AP成为执行802.11程序代码的平台，IETF已经成立一个工作组来负责开发无线接入点控制与服务配置（Control and Provisioning of Wireless Access Points，简称CAPWAP）协议（注6）。CAPWAP已经在RFC 3990提出问题陈述（problem statement），目前处于网络架构与目标定义阶段，主要是针对使用轻量级接入点（lightweight access points）的网络。接入点控制协议可望在2006年1月出炉。当接入点逐渐商品化，或许基于Linux的接入点只要通过固件更新，就可以使用标准的隧道协议（tunneling protocol）。此外，若是有人为了让开放源码接入点能够使用新的控制芯片而着手开发新的固件，我也不会感到惊讶。

结语

如今，Wi-Fi的蔓延已经势不可挡。自从本书第一版发行以来，无线网络已经从一种有趣的玩意变成不可或缺的技术。许多公司用它来提高生产力以及吸引员工，就像有些大学利用它来吸引学生一样。随着芯片与网卡成本的下降，用户均负担得起使用无线网络的笔记型计算机。

网线依然会继续留在最适当的工作岗位。无法移动的固定运算资源以及带宽需求较高的网络依然受制于网线。不过，无线网络似乎泰然自若地往网络连接的标准方式（standard method of network connection）的目标迈进。未来，“你们有Wi-Fi吗？”将会取代“网线插座在哪？”而成为联网时的标准问题。

注6： 此工作组的首页是 *http://www.ietf.org/html.charters/capwap-charter.html*。

名词解释

AAA（身份验证、授权与计费）

身份验证、授权与计费（Authentication, Authorization, and Accounting，简称AAA）。供用户证明身份、访问资源以及搜集使用状况统计的一种协议或系统。RADIUS是802.11网络中最常见的AAA协议。

access point（接入点）

见“AP”。

ACK（确认）

确认（Acknowledgment，简称ACK）。ACK机制被广泛使用于802.11，让802.11得以在不可靠的无线媒介上提供可靠的数据传输。相关细节见“基于竞争的数据服务”。

Acknowledgment（确认）

见“ACK”。

ad hoc（临时性网络；对等式网络；独立型网络）

一种临时性网络，此网络中的节点（即工作站）之间只维持着短暂的关联关系。另见“IBSS”。

AES（高级加密标准）

高级加密标准（Advanced Encryption Standard，简称AES）。NIST经过五年的评估最后于2001年所选用的cipher（密码；加密算法；加密器），以取代旧的数据加密标准（Data Encryption Standard，简称DES）。AES为128位的块密码（block cipher）具有128、192或256位的密钥，被广泛用于许多需要使用块密码的协议中，包括802.11i的CCMP，不过CCMP只使用128位的密钥。AES的规范说明书参见FIPS第197号出版物（*http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf*）。

AID（关联标识符）

关联标识符（Association Identifier，简称AID）。接入点内部分配的数据结构编号，用来辨识个别的移动式节点（mobile node，即工作站）。

AKM（身份验证与密钥管理）

身份验证与密钥管理（Authentication and Key Management，简称AKM）。一组用来确定用户身份与密钥的协议。无线网络目前规范了两种协议：802.1X与pre-shared key（预共享密钥）。

AP（接入点）

接入点（Access Point，简称AP）。功能类似网桥（Bridge），用来连接802.11无线工作站与有线骨干网络。相关细节见第二十章。

AS（身份验证服务器）

身份验证服务器（Authentication Server，简称AS）。用来验证用户身份的网络服务。802.11网络通常会使用RADIUS。

ASN（抽象语法标记）

抽象语法标记（Abstract Syntax Notation，简称ASN）。用来撰写管理信息库（Management Information Base，简称MIB）文件的形式描述。

association identifier（关联标识符）

见“AID”。

ATIM（通知传输指示消息）

通知传输指示消息（Announcement Traffic Indication Message，简称ATIM）。ATIM是ad hoc（独立式）802.11网络中用来宣告尚有帧暂存待传的指示信息。相关细节见第八章。

basic service set（基本服务集）

见“BSS”。

BER（位错误率）

位错误率（Bit Error Rate，简称BER）。所收到的错误位数。此数字通常不会太高，一般以科学记数法表示。10^{-2}代表所收到的100个位当中有1个位出现错误。

BPSK（二进制相移键控）

二进制相移键控（Binary Phase Shift Keying，简称BPSK）。这是以相位偏移进行位编码的调制方式。此机制是以两种相位分别代表单一位值的0与1（译注1）。

BSS（基本服务集）

基本服务集（Basic Service Set，简称BSS）。802.11网络的基本组件（building block），每个BSS包含了一组逻辑上彼此关联的工作站。

BSSID（基本服务集标识符）

基本服务集标识符（Basic Service Set Identifier，简称BSSID）。这是同一个“基本服务集”中所有工作站于帧头（frame header）共享的标识符，长度为48位。

CCITT（国际电报电话咨询委员会）

国际电报电话咨询委员会（Comite Consultatif International Telephonique et Telegraphique，简称CCITT）。是联合国的附属机构，负责制定电信的相关标准。目前改组之后称为国际电信联盟－电信标准化部门（International Telecommunication Union-Telecommunication Standardization Sector，简称ITU-T）。

CCK（补码键控）

补码键控（Complementary Code Keying，简称CCK）。这是将数据块（data block）转换为复合码（complex code）的调制机制，同时编码每个块的数个位。

CCM

CCM是“Counter Mode with CBC-MAC”的缩写；CBC-MAC是“Cipher-Block-Chaining Message-

译注1：0度与180度两种载波相位分别代表0与1。

Authentication-Code”的缩写。这是一种经认证的块密码模式（authenticated block cipher mode），定义于RFC 3610，可以搭配任何一种128位的块密码，不过通常与AES搭配使用。

CCMP

“Counter Mode with CBC-MAC Protocol”的缩写。802.11i将CCMP定义为AES搭配CCM的操作模式。这是目前无线局域网络中，最为坚固（strongest）的加密协议。

CF（无竞争）

不以竞争作为访问媒介的方式的服务，称为无竞争（Contention Free，简称CF）服务。CF是点协调者（Point Coordinator，简称PC）通过点协调功能（Point Coordination Function，简称PCF）所提供的服务。无竞争服务在实际中并不常见。

CFP（无竞争周期）

无竞争周期（Contention-Free Period，简称CFP）。提供无竞争服务的同时，802.11还允许某些竞争式媒介访问。由中央机制（central authority）控制的周期称为无竞争周期。

CRC（循环冗余校验）

循环冗余校验（Cyclic Redundancy Check，简称CRC）。这是一种数学校验运算（checksum），用来侦测所传输的帧数据是否损毁。CRC属于一种线性散列函数，不适合用来确保数据的安全性。

CSMA（载波监听多路访问）

载波监听多路访问（Carrier Sense Multiple Access，简称CSMA）。这是一种“先听后说”机制，作为传输资源的访问的媒介。所有工作站均可访问传输媒介（即多路访问），不过在传输之前必须确定当时无人使用该媒介（即载波侦测）。

CSMA/CA（载波监听多路访问/冲突避免）

载波监听多路访问/冲突避免（Carrier Sense Multiple Access with Collision Avoidance，简称CSMA/CA）。这是一种CSMA方式，通过延迟访问时间来避免多方同时访问传输媒介。802.11与AppleTalk的LocalTalk协议均使用CSMA/CA。

CTS（清除发送）

清除发送（Clear to Send，简称CTS）。这是通知对方已收到请求发送（Request to Send，简称RTS）信息，可以开始传送数据的确认。在避免隐藏节点干扰的RTS-CTS清空交换过程（clearing exchange）中，CTS是第二个组件。

DA（目的地地址）

目的地地址（Destination Address，简称DA）。这是负责处理帧的工作站的MAC地址。通常目的地地址即为接收端地址。不过在基础结构型网络（infrastructure network）里，由无线端桥接至有线端的帧的目的地地址必然位于有线网络，而接收端地址则位于接入点的无线接口上。

DBPSK（差分二进制相移键控）

差分二进制相移键控（Differential Binary Phase Shift Keying，简称DBPSK）。这是以相邻符号（successive symbol）间的相位偏移进行位编码的调制方式。两种不同的相位偏移可使符号

(symbol) 与数据位 (data bit) 之间形成一对一的编码率 (译注 2)。

DCF (分布式协调功能)

分布式协调功能 (Distributed Coordination Function, 简称DCF)。这是802.11竞争式服务中无线媒介的访问规则。面临竞争情况时, DCF将会使用指数退避 (exponentially increasing backoff)、延迟访问 (deferring access)、帧确认 (frame acknowledg nent)以及何时交换特定帧或何时需要分割帧等规则, 作为媒介访问的判断依据。

DFS (动态频率选择; 动态选频)

动态频率选择 (Dynamic Frequency Selection, 简称DFS)。这是欧洲无线电管制局所要求的频谱管理服务 (spectrum management service), 主要是为了避免干扰5 GHz的雷达系统以及将功率扩展至所有可用信道。DFS是FCC决定在美国开放谐波频带 (harmonized frequency band) 的关键因素。

DHCP (动态主机配置协议)

动态主机配置协议 (Dynamic Host Configuration Protocol, 简称DHCP)。这是由IETF制定, 用来自动设定主机配置的一套标准。需要设定配置的主机会以广播方式提出请求, 由DHCP服务器予以响应。DHCP的出现无异于说明Internet成长之快, 使得网管人员再也无法全盘掌控整个网络。

DIFS (分布式帧间间隔)

分布式帧间间隔 (Distributed Inter-Frame Space, 简称DIFS)。在基于竞争的服务中用来分隔原子交换帧的 (时间) 间隔。另见"DCF"。

distributed coordination function (分布式协调功能)

见"DCF"。

distributed inter-frame space(分布式帧间间隔)

见"DIFS"。

DQPSK (差分正交相移键控)

差分正交相移键控 (Differential Quadrature Phase Shift Keying, 简称DQPSK)。这是以相邻符号 (successive symbol) 间的相位差进行位编码的调制方式。有四种不同的相位, 可使符号 (symbol) 与数据位 (data bit) 之间形成一对二的编码率 (译注 3)。

DS (分布式系统)

分布式系统 (Distribution System, 简称DS)。这是用来串联接入点的一组服务。逻辑上包含有线骨干网络, 加上常见于大部分商用接入点的桥接功能。见图 2-6。

DSSS (直接序列扩频)

直接序列扩频 (Direct-Sequence Spread Spectrum, 简称DSSS)。这是在宽带中将信号展开而后传送的传输技术。在接收端, 经展开的信号会收敛为较强的信号, 所有窄带噪声亦经扩频处理。从端口数来看, 基于2Mbps与11Mbps的802.11设备大多属于直接序列接口。

DTIM (延迟传输指示映射)

延迟传输指示映射 (Delivery Traffic

译注 2: 0度与180度两种相位差分别代表0与1。

译注 3: 0度、90度、180度与270度四种相位差分别代表00、01、11与10。

Indication Map，简称DTIM）。信标帧中如果包含DTIM，表示接入点即将传送其暂存的广播与组播帧。

EAP（可扩展身份验证协议）

可扩展身份验证协议（Extensible Authentication Protocol，简称EAP）。这是802.1X所使用的“框架身份验证协议”（framework authentication protocol），用来提供网络身份验证。实际的认证操作授权给称为“认证方式”（method）的子协议负责。

EIFS（扩展帧间间隔）

扩展帧间间隔（Extended Inter-Frame Space，简称EIFS）。EIFS在四种帧间间隔中延迟最久，主要用于传输过程出现错误时。

EIRP（有效等向辐射功率）

有效等向辐射功率（Effective Isotropic Radiated Power，简称EIRP）。任何天线系统均会形成无线电波的传送轨迹，该轨迹中的功率即为有效等向辐射功率。

ERP（有效辐射功率）

有效辐射功率（Effective Radiated Power，简称ERP）。用来描述天线所传送的无线电波强度。

ESS（扩展服务集）

扩展服务集（Extended Service Set，简称ESS）。逻辑上由一群接入点串联而成的组合。只要所有工作站被设定成认得彼此，即可在ESS链路层漫游（link-layer roaming）。

ETSI（欧洲电信标准协会）

欧洲电信标准协会（European Telecommunications Standards Institute，简称ETSI）。ETSI是由多国共同组成的标准制定机构，有权管理与制定欧洲大部分地区的电信标准。GSM标准的制定即是ETSI主导的。以ETSI为首所制定的无线局域网络技术称为高性能无线局域网络（High Performance Radio LAN，简称HIPERLAN），与802.11相互竞争。

extended inter-frame space（扩展帧间间隔）

见“EIFS”。

FCC（联邦通信委员会）

联邦通信委员会（Federal Communications Commission，简称FCC）。美国的电信主管机关。联邦法规第47篇（Title 47 of the Code of Federal Regulations）所公布的联邦通信委员会规定（FCC Rules）为美国主要的电信管理法规。无线局域网络必须符合FCC Rules第15节（Part 15）有关RF设备的相关规定。

FCS（帧校验序列）

帧校验序列（Frame Check Sequence，简称FCS）。这是附加于IEEE 802网络上的帧中，用来侦测数据是否损毁的校验码（checksum）。如果接收端所计算出的FCS与帧中所记载的不同，便可推论出该帧已经损毁并将其丢弃。

FH（跳频）

跳频（Frequency Hopping，简称FH）。见“FHSS”。

FHSS（跳频扩频）

跳频扩频（Frequency Hopping Spread Spectrum，简称FHSS）。利用时间长短不一的窄带信号，将RF能量扩展于宽带中的技术。

FIPS（联邦信息处理标准）

联邦信息处理标准（Federal

Information Processing Standard，简称FIPS）。美国联邦政府及其契约商等非军事机构所使用的公开标准。

four-way handshake（四次握手）

这是802.11i所定义的将成对主密钥（pairwise master key）展开为完整的密钥层次结构（key hierarchy）的密钥交换过程。四次握手让申请者（supplicant）与认证者（authenticator）借此协调出动态产生的加密密钥。

GFSK（高斯频移键控）

高斯频移键控（Gaussian Frequency Shift Keying，简称GFSK）。这是以符号周期（symbol period）载波信号的频率进行数据编码的调制技术。相对而言，GFSK较能抗拒模拟噪声，因为大部分模拟噪声由调幅方式产生。

GMK（组主密钥）

组主密钥（Group Master Key，简称GMK）。认证者（authenticator）用来产生组临时密钥（Group Transient Key，简称GTK）的密钥。

GTK（组临时密钥）

组临时密钥（Group Transient Key，简称GTK）。由组主密钥（GMK）结合组随机号码（group random number）所衍生出来的密钥。GTK用来产生组密钥层次结构（group key hierarchy），其中包含用来保护广播与组播数据的密钥。

HR/DSSS（高速直接序列扩频）

高速直接序列扩频（High-Rate Direct-Sequence Spread Spectrum，简称HR/DSSS），意指802.11b设备所传输的信号。虽然在许多方面类似先前的2-Mbps传输方式，但由于采用较为先进的编码技术，因此能够提供较高的数据率。

IAPP（接入点内部协议）

接入点内部协议（Inter-Access Point Protocol，简称IAPP）。接入点彼此间所使用的通信协议，用来提供漫游服务。802.11F制定了一份IAPP标准，不过并未被广泛采用。

IBSS（独立基本服务集）

独立基本服务集（Independent Basic Service Set，简称IBSS）。没有接入点参与其中的802.11网络。有些厂商将IBSS称为临时性或对等式网络（ad hoc network）。另见“ad hoc”。

ICV（完整性校验值）

完整性校验值（Integrity Check Value，简称ICV）。在WEP加密之前，针对个别帧所计算出的校验码（checksum）。ICV的设计，是为了让接收端可以侦测出帧是否有异样，以避免帧遭他人篡改。不过WEP用来产生ICV的算法本身就有瑕疵，因此大幅削弱了WEP防止篡改的功用。

IEEE（电气和电子工程师协会）

电气和电子工程师协会（Institute of Electrical and Electronics Engineers，简称IEEE）。制定IEEE 802网络标准的专业机构。

IR（红外线）

红外线（Infrared Light，简称IR）。相较于可见红光，波长较长且频率较低的光线。可见红光的波长大约不超过700 nm（纳米；埃）。

ISI（符号间干扰）

符号间干扰（Inter-Symbol Interference，简称ISI）。由于多重路径

的延迟效应，所传送的符号可能因相互干扰而毁损。如何避免符号间干扰是无线局域网络的重要课题之一，特别是采用OFDM的无线局域网络。

ISM（工业、科学与医疗）

工业、科学与医药（Industrial, Scientific, and Medical，简称ISM）。FCC规定（FCC Rules）第15节（Part 15）中特别为工业、科学与医疗用途保留了无须取得许可证即可使用的频带。2.4-GHz ISM频带原本保留给微波炉使用，以免只是为了加热一点食物，就得大费周章地通过FCC的层层关卡。不过既然无须取得授权，使用本频带的设备也就不在少数，其中包括802.11无线局域网络。

ITU（国际电信联盟）

国际电信联盟（International Telecommunications Union，简称ITU）。前身为CCITT。严格来说，ITU只提供建议（recommendation）而非强制规定（regulation）或电信标准（standard）。不过许多国家赋予ITU提案与法律同等的效力。

IV（初始向量）

初始向量（Initialization Vector，简称IV）。通常是指加密标头（cryptographic header）中公开的密钥材料（keying material），主要用于块密码（block cipher）。WEP虽然采用流密码（stream cipher），不过还是在帧头中公开了秘钥（secret key）的24位初始向量。

LLC（逻辑链路控制）

逻辑链路控制（Logical Link Control，简称LLC）。IEEE所制定的规范，在Ethernet上可以借由LLC达到协议多路复用。802.11帧所携带的数据即是经过LLC所封装的数据单元。

KCK

EAPOL密钥确认密钥（EAPOL Key Confirmation Key）。在四次握手过程中用来产生“消息完整性校验值”（message integrity check value）的密钥，衍生为成对层次结构的一部分。亦称为“key MIC key”。

KEK

EAPOL密钥加密密钥（EAPOL Key Encryption Key）。在四次握手过程中用来加密密钥的密钥，衍生为成对层次结构的一部分。它也可以作为成对密钥。

MAC（媒介访问控制）

媒介访问控制（Medium Access Control，简称MAC）。IEEE网络中，用来仲裁带宽用量及判定传输媒介使用权属的功能。

MIB（管理信息库）

管理信息库（Management Information Base，简称MIB）。一个用来指定每部设备的功能与配置参数的ASN（抽象语法标记）规范。通常与SNMP或其他网络管理系统搭配使用。

MIC（消息完整性校验码）

消息完整性校验码（Message Integrity Code，简称MIC）。针对一组欲保护数据计算出来的散列值，用以防止数据遭人篡改。在大多数密码系统中，这类散列值称为消息认证码（Message Authentication Code，简称MAC）。为避免与媒介访问控制（Medium Access Control）的缩写MAC混淆，802.11采用“MIC”的写法。

Michael

消息完整性校验算法，由TKIP规范。

MIMO（多进/多出）

多进/多出（Multiple-Input/Multiple-Output，简称MIMO）。一种天线配置，使用多组传输与接收天线来同时传输多组数据流。MIMO天线的配置通常简写为YxZ，其中Y与Z为整数，分别代表传输天线与接收天线的数量。

MPDU（MAC协议数据单元）

MAC协议数据单元（MAC Protocol Data Unit，简称MPDU）。帧的代名词。不过MPDU并未包含PLCP标头。

MSDU（MAC服务数据单元）

MAC服务数据单元（MAC Service Data Unit，简称MSDU）。由MAC接收之后传送给（网络上）其他MAC的数据。MSDU只由较高层的（协议）数据组成。举例来说，802.11管理帧(management frame)就不包含MSDU。

NAV（网络分配向量）

网络分配向量（Network Allocation Vector，简称NAV）。NAV主要用于实现虚拟载波监听功能（virtual carrier sensing function）。如果传输媒介处于忙碌状态，工作站就会延迟访问。为了确保稳定性，802.11提供了两种载波监听功能。第一种是物理（physical）载波监听功能，判断工作站是否正在解读合法的802.11信号？”以及类似情况，是以物理监听到的信号是否超过能量阈值(energy threshold)作为判断准则。第二种是虚拟（virtual）载波监听功能，判断传输媒介是否处于忙碌状态，是以NAV作为判断依据。大多数帧会在NAV字段中指定一段时间，礼貌性要求其他工作站在这段期间暂时停止访问传输媒介，直到该帧被传送出去为止。接收到NAV的其他工作站得知此一信息之后，便会暂缓访问传输媒介以避免冲突发生。相关细节见第三章关于“基于竞争的数据服务”的部分。

NIST（美国国家标准与技术研究院）

美国国家标准与技术研究院（National Institute of Standards and Technology，简称NIST）。这是一个美国政府机构，负责为联邦政府制定技术标准。NIST标准被大多数非政府机构与各级政府机关采用。

OFDM（正交频分复用）

正交频分复用（Orthogonal Frequency Division Multiplexing，简称OFDM）。将宽频带分割后，通过这些较窄的子频带，以多路传送与还原数据技术传送。802.11a与802.11g均采用OFDM技术。而802.11n使用MIMO来传送多重OFDM数据流。

OSI（开放式系统互联参考模型）

开放式系统互联参考模型（Open Systems Interconnection，简称OSI）。由一系列网络标准所组成的模型。鉴于IP网络已然存在，这些带有巴洛克风格（规模宏大且式样复杂）的网络标准也就乏人问津了，从来没有用于实际中。

PBCC（分组二进制卷积码）

分组二进制卷积码（Packet Binary Convolution Coding，简称PBCC）。802.11b网络中所使用的一种数据编码方式，实际上并未被广泛采用。曾经有人提议在20+ Mbps网络中采用PBCC，不过这项提议已被拒绝。

PC（点协调者）

点协调者（Point Coordinator，简称PC）。接入点所具备的功能之一，负责

在无竞争服务期间，居中协调各方对无线电波媒介的访问。

PCF（点协调功能）

点协调功能（Point Coordination Function，简称PCF）。这是接入点所提供的一组规则，用来居中协调各方对传输媒介的访问。

PCMCIA（国际个人计算机存储卡协会）

国际个人计算机存储卡协会（Personal Computer Memory Card International Association，简称PCMCIA）。这是制定PCMCIA标准，让各种不同接口设备得以跟笔记型计算机彼此互联的产业团体。802.11接口绝大部分属于PCMCIA形式。因为名称又长又难念，有人戏称PCMCIA为“无法招架计算机产业术语的家伙”（People Who Can't Manage Computer Industry Acronyms）。

PDU（协议数据单元）

见“protocol data unit”。

PER（封包错误率）

封包错误率（Packet Error Rate，简称PER）。类似位错误率，主要用来测量封包的错误比例。

PHY（物理层）

IEEE物理层（physical layer）的常见缩写。

physical-layer convergence procedure（物理层会聚过程）

802.11网络中，PHY（物理层）的上层组件。每种物理层协议各自拥有特定的物理层会聚过程，主要是辅助MAC（媒介访问控制）层进行成帧。

PIFS（PCF帧间间隔）

PCF帧间间隔（PCF Inter-Frame space，简称PIFS）。在无竞争服务中，只要媒介闲置超过一个PCF帧间间隔的时间，工作站即可传送数据。

PLCP（物理层会聚过程）

见“physical-layer convergence procedure”。

PMD（物理媒介相关）

物理媒介相关（Physical Medium Dependent，简称PMD）。PHY（物理层）的底层组件，负责传送RF信号给其他802.11工作站。

PMK

成对主密钥（Pairwise Master Key）。这是申请者与认证者之间所有密钥数据的最终来源。它可以衍生自身份验证过程中的EAP method，或者由预共享密钥（pre-shared key）直接提供。

PPDU（PLCP协议数据单元）

PLCP协议数据单元（PLCP Protocol Data Unit，简称PPDU）。完整的PLCP帧包含PLCP标头、MAC标头、MAC数据字段以及MAC与PLCP标尾。

PRF（伪随机函数）

伪随机函数（Pseudo-Random Function，简称PRF）。一种802.11i函数，会将一小部分数据展开为较大量的数据。PRF最常用来将主密钥展开成密钥层次结构。

protocol data unit（协议数据单元）

协议层之间彼此沟通时所使用的数据单元。例如，IP层的协议数据单元即为IP封包。各个IP实现之间可相互利用IP封包通信。另见“service data unit”。

PS（省电操作）

省电操作（Power Save，简称PS）。在802.11中冠有“PS”前缀的操作。

PSDU（PLCP服务数据单元）

PLCP服务数据单元（PLCP Service Data Unit，简称PSDU）。PLCP负责传送的数据，亦即附加PLCP标头的MAC帧。

PSK - Phase Shift Keying（相移键控）

相移键控（Phase Shift Keying，简称PSK）。以载波相位偏移传送数据的调制方式。

PSK - Pre-shared Key（预共享密钥）

一种802.11i身份验证方式，以预先设定好的静态密钥进行身份验证。此密钥必须手动传递。亦称为WPA-PSK。

PTK（成对临时密钥）

成对临时密钥（Pairwise Transient Key，简称PTK）。从成对主密钥产生的密钥，其中包括加密与完整性协议所使用的密钥以及传递动态密钥所需要的密钥。

QPSK（正交相移键控）

"Quadrature Phase Shift Keying"的缩写。这是以不同的相位（相位偏移）进行位编码的调制方式。有4种相位，分别代表2个位的所有可能组合方式（译注4）。

RA（接收端地址）

接收端地址（Receiver Address，简称RA）。帧接收工作站的MAC地址。RA可能是帧的目的地地址，但不尽然。例如，在基础结构型网络（infrastructure network）里，目的地为分布式系统（distribution system）的帧，它是由接入点所接收的。

译注4：0度、90度、180度与270度4种相位分别代表00、01、11与10。

RADIUS（远程认证拨号用户服务）

远程认证拨号用户服务（Remote Authenticated Dial-In User Service，简称RADIUS）。这是用来确认拨号用户身份的协议，因802.1X而被广泛使用，是802.1X系统中最常见的身份验证服务。

RC4（RC4加密算法）

WEP所使用的加密算法，由RSA Data Security公司开发，授权费用十分高昂。由于RSA可能提起法律诉讼，因此没有人愿意冒险以开放源码实现WEP。

RLAN（无线电局域网）

无线电局域网（Radio LAN，简称RLAN）。欧洲无线电管制当局所使用的名词，意指任何一种使用无线电波技术的无线网络。虽然802.11最为普及，不过还存在其他的无线网络。比较著名的还有ETSI的HIPERLAN。

RF（射频）

射频（Radio Frequency、简称RF）。用来形容与无线接口有关的事物（例如"RF调制器"、"RF能量"等）。

RSN（强健安全网络）

"Robust Security Network"的缩写。这是一种采用802.11i安全规则且不支持WEP的网络。

RTS（请求传送）

请求传送（Request to Send，简称RTS）。用来启始RTS-CTS清空过程的帧。当所要传送的帧大于RTS限制阈值（threshold）时就会用到RTS帧。

SA（来源地址）

来源地址（SourceAddress，简称SA）。不同于TA，SA是产生帧的工作站的地址。当帧由分布式系统（distrib ution

system）流向无线网段时，来源地址便会有所改变，不再是无线工作站的地址。

SDU（服务数据单元）

见“service data unit”。

Service Data Unit（服务数据单元）

某个协议层从上一层接收而来的数据即属服务数据单元。例如，IP服务数据单元由TCP层数据加上TCP标头组合而成。当协议层收到服务数据单元后，会加上适当的标头，再将它传递给下一层。另见“protocol data unit”。

SFD（起始帧定界符）

起始帧定界符（Start of Frame Delimiter，简称SFD）。在帧头中，SFD用来示意同步已经结束，之后即属实际帧内容。

SIFS（短帧间间隔）

短帧间间隔（Short Inter-Frame Space，简称SIFS）。在4种帧间间隔中延时最短。此为原子帧交换过程（atomic frame exchange）中帧与帧之间的间隔。

SSID（服务集标识符）

服务集标识符（Service Set Identity，简称SSID）。通常，SSID是用户容易辨识的一组字符串。

SYNC（同步）

同步（Synchronize，简称SYNC）是由PLCP传送，让传送与接收双方的位定时器得以同步的一连串位。

TA（传送端地址）

传送端地址（Transmitter Address，简称TA）。实际传送帧的工作站。通常是基础结构型网络的接入点地址。

TIM（传输指示映射）

传输指示映射（Traffic Indication Map，简称TIM）。信标（Beacon）帧的组成字段之一，用来通知已关联的工作站，接入点中有暂存的单播（unicast）与组播（multicast）数据待传。

TK（临时密钥）

临时密钥（Temporal Key，简称TK）。由802.11i密钥层次结构（key hierarchies）产生，用于认证协议的临时性密钥。临时密钥是链路层加密协议（如TKIP或CCMP）的主要输入项。

TKIP（临时密钥完整性协议）

临时密钥完整性协议（Temporal Key Integrity Protocol，简称TKIP）。802.11i中一种改良过的加密协议。TKIP保留WEP的基本操作方式，但使用新的密钥生成（keying）与完整性校验机制来提供更多安全性。

TPC（传输功率控制）

“Transmit Power Control”的缩写。欧洲管制当局所要求的频谱管理服务，可确保所使用的5 GHz电波不致干扰卫星服务。

WEP（有线等效加密）

有线等效加密（Wired Equivalent Privacy，简称WEP）。批评者戏称此为“窃听同义协议”（Wiretap Equivalence Protocol）。WEP是一种加密个别数据帧的标准，原本仅只打算提供起码的安全保护。就此而言，WEP的表现倒是恰如其分。2001年8月间，WEP的安全性遭到彻底瓦解，用来攻击的源代码也随之公开。

Wi-Fi（无线保真）

"Wireless Fidelity"的缩写。这是Wi-Fi联盟（前身为Wireless Ethernet Compatibility Alliance）所推行的认证方式，目的在于测试802.11产品的互用性。原本，Wi-Fi适用于符合802.11b（11-Mbps HR/DSSS）标准的设备。如今，它也涵盖802.11g与802.11a的互用性以及WPA的安全认证。

WPA and WPA2（WPA与WPA2）

WPA代表Wi-Fi Protected Access（Wi-Fi保护访问）。这是基于802.11i draft 3所提出的安全标准。Wi-Fi联盟采用802.11i draft 3以尽早对初期的TKIP产品进行兼容性认证，从而让各方尽快实行802.11安全协议。WPA2是基于最后核准的802.11i标准的。