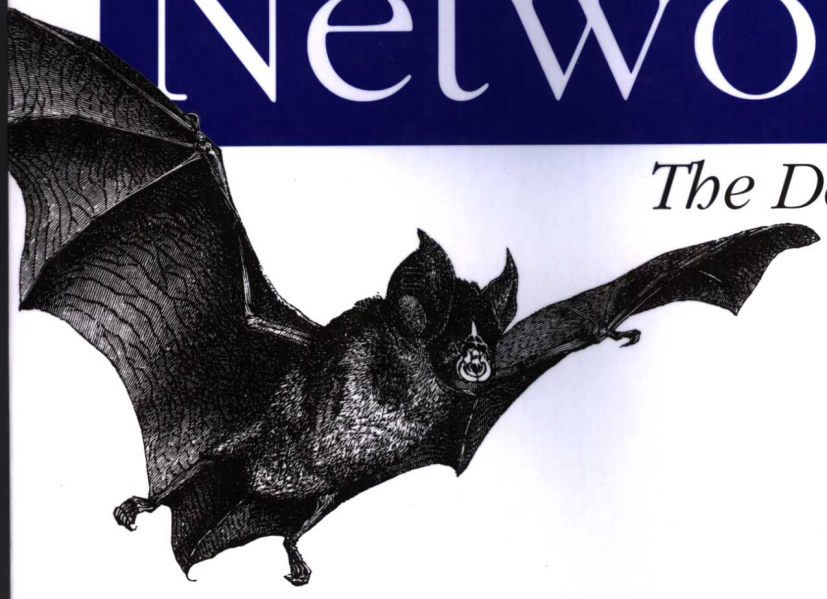
802.11® 无线网络权威指南（影印版）

2nd Edition

Covers 802.11a, g, n & i

802.11® Wireless Networks

The Definitive Guide



O'REILLY®

東南大學出版社

Matthew S. Gast 著

O'REILLY®

802.11无线网络权威指南（影印版）

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希望的用户？怎样处理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视都是一项必须的工作，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排错。

《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和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和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。

ISBN 7-5641-0316-7

9 787564 103163 >

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

ISBN 7-5641-0316-7

定价：82.00元

O'Reilly Media, Inc. 授权东南大学出版社出版

802.11® 无线网络权威指南（影印版）

802.11® Wireless Networks:

The Definitive Guide

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, S. M.）著 . — 影印本 . — 南京：东南大学出版社，2006.4

书名原文：802.11® Wireless Networks: The Definitive Guide, Second Edition

ISBN 7-5641-0316-7

Ⅰ.8... Ⅱ.加... Ⅲ.无线电通信－通信网－英文 Ⅳ.TN92

中国版本图书馆 CIP 数据核字（2006）第 021830 号

江苏省版权局著作权合同登记

图字：10-2006-42 号

书　　名 / 802.11® 无线网络权威指南 第二版（影印版）
书　　号 / ISBN 7-5641-0316-7
责任编辑 / 张烨
封面设计 / Ellie Volckhausen，马冬燕
出版发行 / 东南大学出版社（press.seu.edu.cn）
地　　址 / 南京四牌楼 2 号（邮政编码 210096）
印　　刷 / 扬中市印刷有限公司
开　　本 / 787 毫米 × 980 毫米　16 开本　41.25 印张
版　　次 / 2006 年 4 月第 1 版　2006 年 4 月第 1 次印刷
印　　数 / 0001-2500 册
定　　价 / 82.00 元（册）

第二版

802.11® 无线网络权威指南（影印版）

802.11® Wireless Networks:

The Definitive Guide

Matthew S. Gast

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

东南大学出版社

O'Reilly Media, Inc. 介绍

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。

出版说明

随着计算机技术的成熟和广泛应用，人类正在步入一个技术迅猛发展的新时期。计算机技术的发展给人们的工业生产、商业活动和日常生活都带来了巨大的影响。然而，计算机领域的技术更新速度之快也是众所周知的，为了帮助国内技术人员在第一时间了解国外最新的技术，东南大学出版社和美国 O'Reilly Meida, Inc.达成协议，将陆续引进该公司的代表前沿技术或者在某专项领域享有盛名的著作，以影印版或者简体中文版的形式呈献给读者。其中，影印版书籍力求与国外图书“同步”出版，并且“原汁原味”展现给读者。

我们真诚地希望，所引进的书籍能对国内相关行业的技术人员、科研机构的研究人员和高校师生的学习和工作有所帮助，对国内计算机技术的发展有所促进。也衷心期望读者提出宝贵的意见和建议。

最新出版的一批影印版图书，包括：

- 《深入理解 Linux 内核 第三版》（影印版）
- 《Perl 最佳实践》（影印版）
- 《高级 Perl 编程 第二版》（影印版）
- 《Perl 语言入门 第四版》（影印版）
- 《深入浅出 HTML 与 CSS、XHTML》（影印版）
- 《UML 2.0 技术手册》（影印版）
- 《802.11 无线网络权威指南 第二版》（影印版）
- 《项目管理艺术》（影印版）
- 《.NET 组件开发 第二版》（影印版）
- 《ASP.NET 编程 第三版》（影印版）

Foreword

Matthew Gast was my mentor long before I met him. I began reporting on wireless data networking in October 2000 when I discovered that Apple's claims for its 802.11b-based AirPort Base Station were actually true.

I'd been burned with another form of wireless networking that used infrared, and had spent many fruitless hours using other "interesting" networking technologies that led to dead ends. I figured 802.11b was just another one. Was I glad I was wrong!

This discovery took me down a path that led, inexorably, to the first edition of *802.11 Wireless Networks*. How did this stuff actually work as advertised? I knew plenty about the ISO model, TCP/IP, and Ethernet frames, but I couldn't reconcile a medium in which all parties talked in the same space with what I knew about Ethernet's methods of coping with shared contention.

Matthew taught me through words and figures that I didn't originally understand, but returned to again and again as I descended further into technical detail in my attempts to explain Wi-Fi to a broader and broader audience through articles in *The New York Times*, *The Seattle Times*, *PC World*, and my own Wi-Fi Networking News (*http://www.wifinetnews.com*) site over the last five years.

I starting learning acronyms from *802.11 Wireless Networks* and used Matthew's book to go beyond expanding WDS into Wireless Distribution System into understanding precisely how two access points could exchange data with each other through a built-in 802.11 mechanism that allowed four parties to a packet's transit.

Now as time went by and the 802.11 family grew and became baroque, the first edition of this title started feeling a little out of date—although it remained surprising how many "new" innovations were firmly rooted in developments of the early to mid-1990s. The alphabet soup of the first edition was gruel compared to the mulligatawny of 2005.

Matthew filled the gap between the book and contemporary wireless reality through his ongoing writing at O'Reilly's Wireless DevCenter, which I read avidly. And somewhere in there I was introduced to Matthew at a Wi-Fi Planet conference. We

hit it off immediately: I started pestering him for details about 802.1X, if I remember correctly, and he wanted to talk about books and business. (I wound up writing two editions of a general market Wi-Fi book, neither of which did nearly as well as Matthew's extraordinarily technical one.)

Since then, I have been in the rare and privileged position to be the recipient of Matthew's generosity with his knowledge and humble insight. Matthew isn't one who assumes; he researches. His natural curiosity compels him to dig until he gets an answer that's technically and logically consistent.

Take, for instance, the incredibly political and complicated evolution of the 802.1X standard. (I know, from Matthew, that it's properly capitalized since it's a freestanding standard not reliant on other specifications. Even the IEEE makes this mistake, and it's their rule for capitalization that we're both following.)

802.1X is simple enough in its use of the Extensible Authentication Protocol, a generic method of passing messages among parties to authentication. But the ways in which EAP is secured are, quite frankly, insane—reflecting Microsoft and Cisco's parallel but conflicting attempts to control support of legacy protocols in a way that only damages easy access to its higher level of security.

Matthew eschewed the religious debate and spelled out the various methods, difficulties, and interoperability issues in an O'Reilly Network article that's the nugget of the expanded coverage in this book. I defy any reader to find as cogent and exhaustive an explanation before this book was published. There's nothing as clear, comprehensive, and unaffected by market politics.

At times, Matthew bemoaned the delays that led to the gap between editions of this book, due partly to his joining a startup wireless LAN switch company, but I think readers are better served through his very hard-won, late-night, long-hours knowledge.

Matthew's relationship with 802.11 might have previously been considered that of a handy man who knew his way around the infrastructure of his house. If a toilet was running, he could replace a valve. If the living room needed new outlets, he could research the process and wire them in.

But Matthew's new job took him allegorically from a weekend household warrior to a jack-of-all-tradesman. Matthew can tear out those inner walls, reframe, plumb, and wire them, all the while bitching about the local building code.

It's been a pleasure knowing Matthew, and it's even more a pleasure to introduce you to his book, and let you all in on what I and others have been more private recipients of for the last few years.

—Glenn Fleishman
Seattle, Washington
February 2005

Preface

People move. Networks don't.

More than anything else, these two statements can explain the explosion of wireless LAN hardware. In just a few years, wireless LANs have grown from a high-priced, alpha-geek curiosity to mainstream technology.

By removing the network port from the equation, wireless networks separate user connectivity from a direct physical location at the end of a cord. To abstract the user location from the network, however, requires a great deal of protocol engineering. For users to have location-independent services, the network must become much more aware of their location.

This book has been written on more airplanes, in more airports, and on more trains than I care to count. Much of the research involved in distilling evolving network technology into a book depends on Internet access. It is safe to say that without ubiquitous network access, the arrival of this book would have been much delayed.

The advantages of wireless networks has made them a fast-growing multibillion dollar equipment market. Wireless LANs are now a fixture on the networking landscape, which means you need to learn to deal with them.

Prometheus Untethered: The Possibilities of Wireless LANs

Wireless networks offer several advantages over fixed (or "wired") networks:

Mobility

Users move, but data is usually stored centrally, enabling users to access data while they are in motion can lead to large productivity gains. Networks are built because they offer valuable services to users. In the past, network designers have focused on working with network ports because that is what typically maps to a user. With wireless, there are no ports, and the network can be designed around user identity.

Ease and speed of deployment

Many areas are difficult to wire for traditional wired LANs. Older buildings are often a problem; running cable through the walls of an older stone building to which the blueprints have been lost can be a challenge. In many places, historic preservation laws make it difficult to carry out new LAN installations in older buildings. Even in modern facilities, contracting for cable installation can be expensive and time-consuming.

Flexibility

No cables means no recabling. Wireless networks allow users to quickly form amorphous, small group networks for a meeting, and wireless networking makes moving between cubicles and offices a snap. Expansion with wireless networks is easy because the network medium is already everywhere. There are no cables to pull, connect, or trip over. Flexibility is the big selling point for the "hot spot" market, composed mainly of hotels, airports, train stations (and even trains themselves!), libraries, and cafes.

Cost

In some cases, costs can be reduced by using wireless technology. As an example, 802.11® equipment can be used to create a wireless bridge between two buildings. Setting up a wireless bridge requires some initial capital cost in terms of outdoor equipment, access points, and wireless interfaces. After the initial capital expenditure, however, an 802.11-based, line-of-sight network will have only a negligible recurring monthly operating cost. Over time, point-to-point wireless links are far cheaper than leasing capacity from the telephone company.

Until the completion of the 802.11 standard in 1997, however, users wanting to take advantage of these attributes were forced to adopt single-vendor solutions with all of the risk that entailed. Once 802.11 started the ball rolling, speeds quickly increased from 2 Mbps to 11 Mbps to 54 Mbps. Standardized wireless interfaces and antennas have made it much easier to build wireless networks. Several service providers have jumped at the idea, and enthusiastic bands of volunteers in most major cities have started to build public wireless networks based on 802.11.

802.11 has become something of a universally assumed connectivity method as well. Rather than wiring public access ports up with Ethernet, a collection of access points can provide connectivity to guests. In the years since 802.11 was standardized, so-called "hot spots" have gone from an exotic curiosity in venues that do not move, to technology that is providing connectivity even while in transit. By coupling 802.11 access with a satellite uplink, it is possible to provide Internet access even while moving quickly. Several commuter rail systems provide mobile hot-spots, and Boeing's Connexion service can do the same for an airplane, even at a cruising speed of 550 miles per hour.

Audience

This book is intended for readers who need to learn more about the technical aspects of wireless LANs, from operations to deployment to monitoring:

- Network architects contemplating rolling out 802.11 equipment onto networks or building networks based on 802.11
- Network administrators responsible for building and maintaining 802.11 networks
- Security professionals concerned about the exposure from deployment of 802.11 equipment and interested in measures to reduce the security headaches

The book assumes that you have a solid background in computer networks. You should have a basic understanding of IEEE 802 networks (particularly Ethernet), the OSI reference model, and the TCP/IP protocols, in addition to any other protocols on your network. Wireless LANs are not totally new ground for most network administrators, but there will be new concepts, particularly involving radio transmissions.

Overture for Book in Black and White, Opus 2

Part of the difficulty in writing a book on a technology that is evolving quickly is that you are never quite sure what to include. The years between the first and second edition were filled with many developments in security, and updating the security-related information was one of the major parts of this revision. This book has two main purposes: it is meant to teach the reader about the 802.11 standard itself, and it offers practical advice on building wireless LANs with 802.11 equipment. These two purposes are meant to be independent of each other so you can easily find what interests you. To help you decide what to read first and to give you a better idea of the layout, the following are brief summaries of all the chapters.

Chapter 1, *Introduction to Wireless Networking*, lists ways in which wireless networks are different from traditional wired networks and discusses the challenges faced when adapting to fuzzy boundaries and unreliable media. Wireless LANs are perhaps the most interesting illustration of Christian Huitema's assertion that the Internet has no center, just an ever-expanding edge. With wireless LAN technology becoming commonplace, that edge is now blurring.

Chapter 2, *Overview of 802.11 Networks*, describes the overall architecture of 802.11 wireless LANs. 802.11 is somewhat like Ethernet but with a number of new network components and a lot of new acronyms. This chapter introduces you to the network components that you'll work with. Broadly speaking, these components are stations (mobile devices with wireless cards), access points (glorified bridges between the stations and the distribution system), and the distribution system itself (the wired backbone network). Stations are grouped logically into Basic Service Sets (BSSs). When no access point is present, the network is a loose, ad-hoc confederation called an

independent BSS (IBSS). Access points allow more structure by connecting disparate physical BSSs into a further logical grouping called an Extended Service Set (ESS).

Chapter 3, *802.11 MAC Fundamentals*, describes the Media Access Control (MAC) layer of the 802.11 standard in detail. 802.11, like all IEEE 802 networks, splits the MAC-layer functionality from the physical medium access. Several physical layers exist for 802.11, but the MAC is the same across all of them. The main mode for accessing the network medium is a traditional contention-based access method, though it employs collision avoidance (CSMA/CA) rather than collision detection (CSMA/CD). The chapter also discusses data encapsulation in 802.11 frames and helps network administrators understand the frame sequences used to transfer data.

Chapter 4, *802.11 Framing in Detail*, builds on the end of Chapter 3 by describing the various frame types and where they are used. This chapter is intended more as a reference than actual reading material. It describes the three major frame classes. Data frames are the workhorse of 802.11. Control frames serve supervisory purposes. Management frames assist in performing the extended operations of the 802.11 MAC. Beacons announce the existence of an 802.11 network, assist in the association process, and are used for authenticating stations.

Chapter 5, *Wired Equivalent Privacy (WEP)*, describes the Wired Equivalent Privacy protocol. In spite of its flaws, WEP is the basis for much of the following work in wireless LAN security. This chapter discusses what WEP is, how it works, and why you can't rely on it for any meaningful privacy or security.

Chapter 6, *User Authentication with 802.1X*, describes the 802.1X authentication framework. In conjunction with the Extensible Authentication Protocol, 802.1X provides strong authentication solutions and improved encryption on Wireless LANs.

Chapter 7, *802.11i: Robust Security Networks, TKIP, and CCMP*, describes the 802.11i standard for wireless LAN security. In recognition of the fundamental flaws of WEP, two new link-layer encryption protocols were designed, complete with new mechanisms to derive and distribute keys.

Chapter 8, *Management Operations*, describes the management operations on 802.11 networks. To find networks to join, stations scan for active networks announced by access points or the IBSS creator. Before sending data, stations must associate with an access point. This chapter also discusses the power-management features incorporated into the MAC that allow battery-powered stations to sleep and pick up buffered traffic at periodic intervals.

Chapter 9, *Contention-Free Service with the PCF*, describes the point coordination function. The PCF is not widely implemented, so this chapter can be skipped for most purposes. The PCF is the basis for contention-free access to the wireless medium. Contention-free access is like a centrally controlled, token-based medium, where access points provide the "token" function.

Chapter 10, *Physical Layer Overview*, describes the general architecture of the physical layer (PHY) in the 802.11 model. The PHY itself is broken down into two "sublayers." The Physical Layer Convergence Procedure (PLCP) adds a preamble to form the complete frame and its own header, while the Physical Medium Dependent (PMD) sublayer includes modulation details. The most common PHYs use radio frequency (RF) as the wireless medium, so the chapter closes with a short discussion on RF systems and technology that can be applied to any PHY discussed in the book.

Chapter 11, *The Frequency-Hopping (FH) PHY*, describes the oldest physical layer with 802.11. Products based on the FH PHY are no longer widely sold, but a great deal of early 802.11 equipment was based on them. Organizations with a long history of involvement with 802.11 technology may need to be familiar with this PHY.

Chapter 12, *The Direct Sequence PHYs: DSSS and HR/DSSS (802.11b)*, describes two physical layers based on direct sequence spread spectrum technology. The initial 802.11 standard included a layer which offered speeds of 1 Mbps and 2 Mbps. While interesting, it was not until 802.11b added 5.5 Mbps and 11 Mbps data rates that the technology really took off. This chapter describes the two closely-related PHYs as a single package.

Chapter 13, *802.11a and 802.11j: 5-GHz OFDM PHY*, describes the 5-GHz PHY standardized with 802.11a, which operates at 54 Mbps. This physical layer uses another modulation technique known as orthogonal frequency division multiplexing (OFDM). Slight modifications were required to use this PHY in Japan, which were made by the 802.11j standard.

Chapter 14, *802.11g: The Extended-Rate PHY (ERP)*, describes a PHY which uses OFDM technology, but in the 2.4 GHz frequency band shared by 802.11b. It has largely supplanted 802.11b, and is a common option for built-in connectivity with new notebook computers. The PHY itself is almost identical to the 802.11a PHY. The differences are in allowing for backwards compatibility with older equipment sharing the same frequency band.

Chapter 15, *A Peek Ahead at 802.11n: MIMO-OFDM*, describes the PHY currently in development. 802.11n uses a PHY based on multiple-input/multiple-output (MIMO) technology for much higher speed. At the time this book went to press, two proposed standards were dueling in the committee. This chapter describes both.

Chapter 16, *802.11 Hardware*, begins the transition from theoretical matters based on the standards to how the standards are implemented. 802.11 is a relatively loose standard, and allows a large number of implementation choices. Cards may differ in their specified performance, or in the manner in which certain protocols are implemented. Many of these variations are based on how they are built.

Chapter 17, *Using 802.11 on Windows*, describes the basic driver installation procedure in Windows, and how to configure security settings.

Chapter 18, *802.11 on the Macintosh*, describes how to use the AirPort card on MacOS X to connect to 802.11 networks. It focuses on Mac OS X 10.3, which was the first software version to include 802.1X support.

Chapter 19, *Using 802.11 on Linux*, discusses how to install 802.11 support on a Linux system. After discussing how to add PC Card support to the operating system, it shows how to use the wireless extensions API. It discusses two common drivers, one for the older Orinoco 802.11b card, and the MADwifi driver for newer cards based on chipsets from Atheros Communications. Finally, it shows how to configure 802.1X security using xsupplicant.

Chapter 20, *Using 802.11 Access Points*, describes the equipment used on the infrastructure end of 802.11 networks. Commercial access point products have varying features. This chapter describes the common features of access points, offers buying advice, and presents two practical configuration examples.

Chapter 21, *Logical Wireless Network Architecture*, marks the third transition in the book, from the implementation of 802.11 on the scale of an individual device, to how to build 802.11 networks on a larger scale. There are several major styles that can be used to build the network, each with its advantages and disadvantages. This chapter sorts through the common types of network topologies and offers advice on selecting one.

Chapter 22, *Security Architecture*, should be read in tandem with the previous chapter. Maintaining network security while offering network access on an open medium is a major challenge. Security choices and architecture choices are mutually influential. This chapter addresses the major choices to be made in designing a network: what type of authentication will be used and how it integrates with existing user databases, how to encrypt traffic to keep it safe, and how to deal with unauthorized access point deployment.

Chapter 23, *Site Planning and Project Management*, is the final component of the book for network administrators. Designing a large-scale wireless network is difficult because there is great user demand for access. Ensuring that the network has sufficient capacity to satisfy user demands in all the locations where it will be used requires some planning. Choosing locations for access points depends a great deal on the radio environment, and has traditionally been one of the most time-consuming tasks in building a network.

Chapter 24, *802.11 Network Analysis*, teaches administrators how to recognize what's going on with their wireless LANs. Network analyzers have proven their worth time and time again on wired networks. Wireless network analyzers are just as valuable a tool for 802.11 networks. This chapter discusses how to use wireless network analyzers and what certain symptoms may indicate. It also describes how to build an analyzer using Ethereal, and what to look for to troubleshoot common problems.

Chapter 25, *802.11 Performance Tuning*, describes how network administrators can increase throughput. It begins by describing how to calculate overall throughput for payload data, and common ways of increasing performance. In rare cases, it may make sense to change commonly exposed 802.11 parameters.

Chapter 26, *Conclusions and Predictions*, summarizes current standards work in the 802.11 working group. After summarizing the work in progress, I get to prognosticate and hope that I don't have to revise this too extensively in future editions.

Major Changes from the First Edition

The three years between 2002 and 2005 saw a great deal of change in wireless LANs. The standards themselves continued to evolve to provide greater security and interoperability. Following the typical technology path of "faster, better, and cheaper," the data rate of most 802.11 interfaces has shot from 2 or 11 Mbps with 802.11b to 54 Mbps with 802.11a and 802.11g. Increased speed with backwards compatibility has proved to be a commercially successful formula for 802.11g, even if it has limitations when used for large-scale networks. The coming standardization of 802.11n is set to boost speeds even farther. New developments in PHY technology are anxiously awaited by users, as shown by the popular releases of pre-standard technology. Two entirely new chapters are devoted to 802.11g and 802.11n. European adoption of 802.11a was contingent on the development of spectrum management in 802.11h, which resulted in extensive revisions to the management chapter.

When the first edition was released in 2002, the perception of insecurity dominated discussions of the technology. WEP was clearly insufficient, but there was no good alternative. Most network administrators were making do with remote access systems turned inward, rather than their natural outward orientation. The development of 802.11i was done a great deal to simplify network security. Security is now built in to the specification, rather than something which must be added on after getting the network right. Security improvements permeate the book, from new chapters showing how the new protocols work, to showing how they can be used on the client side, to how to sort through different options when building a network. Sorting through security options is much more complex now than it was three years ago, and made it necessary to expand a section of the deployment discussion in the first edition into its own chapter.

Three years ago, most access points were expensive devices that did not work well in large numbers. Network deployment was often an exercise in working around the limitations of the devices of the time. Three years later, vastly more capable devices allow much more flexible deployment models. Rather than just a "one size fits all" deployment model, there are now multiple options to sort through. Security protocols have improved enough that discussions of deploying technology are based on

what it can do for the organization, not on fear and how to keep it controlled. As a result, the original chapter on network deployment has grown into three, each tackling a major part of the deployment process.

Conventions Used in This Book

Italic is used for:

- Pathnames, filenames, class names, and directories
- New terms where they are defined
- Internet addresses, such as domain names and URLs

Bold is used for:

- GUI components

`Constant Width` is used for:

- Command lines and options that should be typed verbatim on the screen
- All code listings

`Constant Width Italic` is used for:

- General placeholders that indicate that an item should be replaced by some actual value in your own program

`Constant Width Bold` is used for:

- Text that is typed in code examples by the user

Indicates a tip, suggestion, or general note

Indicates a warning or caution

How to Contact Us

Please address comments and questions concerning this book to the publisher:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
(800) 998-9938 (in the U.S. or Canada)
(707) 829-0515 (international/local)
(707) 829-0104 (fax)