Creating and Administering Wireless Networks



802.11® Wireless Networks

The Definitive Guide



O'REILLY®

Matthew S. Gast

IPR2024-01049
Apple EX1021 Page 1

802.11® Wireless Networks

The Definitive Guide

IPR2024-01049
Apple EX1021 Page 2

802.11® Wireless Networks

The Definitive Guide

Matthew S. Gast

O'REILLY®

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

IPR2024-01049
Apple EX1021 Page 3

802.11® Wireless Networks: The Definitive Guide
by Matthew S. Gast

Copyright © 2002 O'Reilly & Associates, Inc. All rights reserved.
Printed in the United States of America.

Published by O'Reilly & Associates, Inc., 1005 Gravenstein Highway North,
Sebastopol, CA 95472.

O'Reilly & Associates books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*safari.oreilly.com*). For more information contact our corporate/institutional sales department: (800) 998-9938 or *corporate@oreilly.com*.

Editor: Mike Loukides

Production Editor: Matt Hutchinson

Cover Designer: Ellie Volckhausen

Printing History:

April 2002: First Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O'Reilly logo are registered trademarks of O'Reilly & Associates, Inc. Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly & Associates, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps. The association between the image of a horseshoe bat and 802.11 wireless networks is a trademark of O'Reilly & Associates, Inc.

802.11® and all 802.11-based trademarks and logos are trademarks or registered trademarks of IEEE, Inc. in the United States and other countries. O'Reilly & Associates, Inc. is independent of IEEE.

While every precaution has been taken in the preparation of this book, the author and publisher assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

ISBN: 0-596-00183-5
[M]

Table of Contents

Preface ix

1. Introduction to Wireless Networks 1
   - Why Wireless? 1
   - A Network by Any Other Name... 5

2. Overview of 802.11 Networks 7
   - IEEE 802 Network Technology Family Tree 8
   - 802.11 Nomenclature and Design 9
   - 802.11 Network Operations 16
   - Mobility Support 20

3. The 802.11 MAC 23
   - Challenges for the MAC 25
   - MAC Access Modes and Timing 27
   - Contention-Based Access Using the DCF 31
   - Fragmentation and Reassembly 34
   - Frame Format 35
   - Encapsulation of Higher-Layer Protocols Within 802.11 43
   - Contention-Based Data Service 44

4. 802.11 Framing in Detail 51
   - Data Frames 51
   - Control Frames 60
   - Management Frames 66
   - Frame Transmission and Association and Authentication States 83

IPR2024-01049
Apple EX1021 Page 5

5. Wired Equivalent Privacy (WEP) 86
Cryptographic Background to WEP 86
WEP Cryptographic Operations 89
Problems with WEP 93
Conclusions and Recommendations 96

6. Security, Take 2: 802.1x 99
The Extensible Authentication Protocol 100
802.1x: Network Port Authentication 105
802.1x on Wireless LANs 110

7. Management Operations 114
Management Architecture 114
Scanning 115
Authentication 120
Association 124
Power Conservation 128
Timer Synchronization 137

8. Contention-Free Service with the PCF 140
Contention-Free Access Using the PCF 140
Detailed PCF Framing 144
Power Management and the PCF 149

9. Physical Layer Overview 151
Physical-Layer Architecture 151
The Radio Link 152
RF and 802.11 158

10. The ISM PHYs: FH, DS, and HR/DS 164
802.11 FH PHY 164
802.11 DS PHY 176
802.11b: HR/DSSS PHY 189

11. 802.11a: 5-GHz OFDM PHY 198
Orthogonal Frequency Division Multiplexing (OFDM) 199
OFDM as Applied by 802.11a 205
OFDM PLCP 208
OFDM PMD 211
Characteristics of the OFDM PHY 212

IPR2024-01049
Apple EX1021 Page 6

12. Using 802.11 on Windows **214**
Nokia C110/C111 215
Lucent ORiNOCO 229

13. Using 802.11 on Linux **236**
A Few Words on 802.11 Hardware 237
PCMCIA Support on Linux 238
linux-wlan-ng for Intersil-Based Cards 244
Agere (Lucent) Orinoco 254

14. Using 802.11 Access Points **262**
General Functions of an Access Point 262
ORiNOCO (Lucent) AP-1000 Access Point 269
Nokia A032 Access Point 279

15. 802.11 Network Deployment **293**
The Topology Archetype 294
Project Planning 307
The Site Survey 314
Installation and the Final Rollout 325

16. 802.11 Network Analysis **329**
Why Use a Network Analyzer? 329
802.11 Network Analyzers 331
Commercial Network Analyzers 332
Ethereal 332
802.11 Network Analysis Examples 348
AirSnort 363

17. 802.11 Performance Tuning **368**
Tuning Radio Management 368
Tuning Power Management 371
Timing Operations 373
Physical Operations 373
Summary of Tunable Parameters 374

18. The Future, at Least for 802.11 ..... **376**
Current Standards Work 376
The Longer Term 378
The End 382

IPR2024-01049
Apple EX1021 Page 7

A. 802.11 MIB 383
B. 802.11 on the Macintosh 396
Glossary 411
Index 419

IPR2024-01049
Apple EX1021 Page 8

CHAPTER 1

Introduction to Wireless Networks

Over the past five years, the world has become increasingly mobile. As a result, traditional ways of networking the world have proven inadequate to meet the challenges posed by our new collective lifestyle. If users must be connected to a network by physical cables, their movement is dramatically reduced. Wireless connectivity, however, poses no such restriction and allows a great deal more free movement on the part of the network user. As a result, wireless technologies are encroaching on the traditional realm of "fixed" or "wired" networks. This change is obvious to anybody who drives on a regular basis. One of the "life and death" challenges to those of us who drive on a regular basis is the daily gauntlet of erratically driven cars containing mobile phone users in the driver's seat.

We are on the cusp of an equally profound change in computer networking. Wireless telephony has been successful because it enables people to connect with each other regardless of location. New technologies targeted at computer networks promise to do the same for Internet connectivity. The most successful wireless networking technology this far has been 802.11.

Why Wireless?

To dive into a specific technology at this point is getting a bit ahead of the story, though. Wireless networks share several important advantages, no matter how the protocols are designed, or even what type of data they carry.

The most obvious advantage of wireless networking is *mobility*. Wireless network users can connect to existing networks and are then allowed to roam freely. A mobile telephone user can drive miles in the course of a single conversation because the phone connects the user through cell towers. Initially, mobile telephony was expensive. Costs restricted its use to highly mobile professionals such as sales managers and important executive decision makers who might need to be reached at a moment's notice regardless of their location. Mobile telephony has proven to be a

IPR2024-01049
Apple EX1021 Page 9

accommodate as many users as needed. Although wireless LANs have somewhat limited bandwidth, the limiting factor in networking a small hot spot is likely to be the cost of WAN bandwidth to the supporting infrastructure.

Flexibility may be particularly important in older buildings because it reduces the need for constructions. Once a building is declared historical, remodeling can be particularly difficult. In addition to meeting owner requirements, historical preservation agencies must be satisfied that new construction is not desecrating the past. Wireless networks can be deployed extremely rapidly in such environments because there is only a small wired network to install.

Flexibility has also led to the development of grassroots community networks. With the rapid price erosion of 802.11 equipment, bands of volunteers are setting up shared wireless networks open to visitors. Community networks are also extending the range of Internet access past the limitations for DSL into communities where high-speed Internet access has been only a dream. Community networks have been particularly successful in out-of-the way places that are too rugged for traditional wireline approaches.

Like all networks, wireless networks transmit data over a network medium. The medium is a form of electromagnetic radiation.* To be well-suited for use on mobile networks, the medium must be able to cover a wide area so clients can move throughout a coverage area. The two media that have seen the widest use in local-area applications are infrared light and radio waves. Most portable PCs sold now have infrared ports that can make quick connections to printers and other peripherals. However, infrared light has limitations; it is easily blocked by walls, partitions, and other office construction. Radio waves can penetrate most office obstructions and offer a wider coverage range. It is no surprise that most, if not all, 802.11 products on the market use the radio wave physical layer.

Radio Spectrum: The Key Resource

Wireless devices are constrained to operate in a certain frequency band. Each band has an associated *bandwidth*, which is simply the amount of frequency space in the band. Bandwidth has acquired a connotation of being a measure of the data capacity of a link. A great deal of mathematics, information theory, and signal processing can be used to show that higher-bandwidth slices can be used to transmit more information. As an example, an analog mobile telephony channel requires a 20-kHz bandwidth. TV signals are vastly more complex and have a correspondingly larger bandwidth of 6 MHz.

* Laser light is also used by some wireless networking applications, but the extreme focus of a laser beam makes it suited only for applications in which the ends are stationary. "Fixed wireless" applications, in which lasers replace other access technology such as leased telephone circuits, are a common application.

IPR2024-01049
Apple EX1021 Page 10

that have proven to be quite valuable to DSL and cable modem customers. In spite of the hype and press from 3G equipment vendors, the rollout of commercial 3G services has been continually pushed back.

In contrast to Bluetooth and 3G, equipment based on the IEEE 802.11 standard has been an astounding success. While Bluetooth and 3G may be successful in the future, 802.11 is a success *now*. Apple initiated the pricing moves that caused the market for 802.11 equipment to explode in 1999. Price erosion made the equipment affordable and started the growth that continues today.

This is a book about 802.11 networks. 802.11 goes by a variety of names, depending on who is talking about it. Some people call 802.11 *wireless Ethernet*, to emphasize its shared lineage with the traditional wired Ethernet (802.3). More recently, the Wireless Ethernet Compatibility Alliance (WECA) has been pushing its *Wi-Fi* ("wireless fidelity") certification program.* Any 802.11 vendor can have its products tested for interoperability. Equipment that passes the test suite can use the Wi-Fi mark. For newer products based on the 802.11a standard, WECA will allow use of the *Wi-Fi5* mark. The "5" reflects the fact that 802.11a products use a different frequency band of around 5 GHz.

Table 1-2 is a basic comparison of the different 802.11 standards. Products based on 802.11 were initially released in 1997. 802.11 included an infrared (IR) layer that was never widely deployed, as well as two spread-spectrum radio layers: frequency hopping (FH) and direct sequence (DS). (The differences between these two radio layers is described in Chapter 10.) Initial 802.11 products were limited to 2 Mbps, which is quite slow by modern network standards. The IEEE 802.11 working group quickly began working on faster radio layers and standardized both 802.11a and 802.11b in 1999. Products based on 802.11b were released in 1999 and can operate at speeds of up to 11 Mbps. 802.11a uses a third radio technique called orthogonal frequency division multiplexing (OFDM). 802.11a operates in a different frequency band entirely and currently has regulatory approval only in the United States. As you can see from the table, 802.11 already provides speeds faster than 10BASE-T Ethernet and is reasonably competitive with Fast Ethernet.

Table 1-2. Comparison of 802.11 standards

IEEE standard	Speed	Frequency band	Notes
802.11	1 Mbps 2 Mbps	2.4 GHz	First standard (1997). Featured both frequency-hopping and direct-sequence modulation techniques.
802.11a	up to 54 Mbps	5 GHz	Second standard (1999), but products not released until late 2000.
802.11b	5.5 Mbps 11 Mbps	2.4 GHz	Third standard, but second wave of products. The most common 802.11 equipment as this book was written.
802.11g	up to 54 Mbps	2.4 GHz	Not yet standardized.

* More details on WECA and the Wi-Fi certification can be found at *http://www.wi-fi.org/*.

IPR2024-01049
Apple EX1021 Page 11

Network Administration

O'REILLY®

802.11 Wireless Networks: The Definitive Guide



Using a wireless network is a liberating experience. But underneath the experience lies a complex protocol, and even more complex issues arise when your data isn't limited to traveling on physical wires. How do you structure your network so mobile users can move around effectively? How do you extend wireless coverage so it's available everywhere you need it? What kinds of security issues do wireless networks raise? How do you tune your network for optimal performance? How do you provide enough capacity to support the users you expect initially, and how do you deal with the problems that arise as more users join the network?

802.11 Wireless Networks: The Definitive Guide discusses all these issues, and more. This book is for the serious system or network administrator who is responsible for deploying or maintaining a wireless network. It discusses how the 802.11 protocols work, with a view towards understanding which options are available and troubleshooting problems that arise. It contains an extensive discussion of wireless security issues, including the problems with the WEP standard and a look at the 802.1x security standard. Since network monitoring is essential to any serious network administrator, and commercial packet sniffers for wireless applications are scarce and expensive, this book shows how to create a wireless packet sniffer from a Linux system and open source software.

In addition to the current 802.11b standard, *802.11 Wireless Networks: The Definitive Guide* also looks forward to the newest developments in wireless networking, including the two new 54-Mbps standards: 802.11a and 802.11g. It also surveys other efforts moving through the standards track, including work to facilitate mobility between access points, quality of service, spectrum management, and power control.

Finally, *802.11 Wireless Networks: The Definitive Guide* shows you how to configure wireless cards and Linux, Windows, and OS X systems, and how to work with access points. Few books in any field combine the theory you need to know with the practical experience and advice you need to get things working. *802.11 Wireless Networks: The Definitive Guide* is one of those books. If you are responsible for a wireless network, you need this book.

ISBN 0-596-00183-5
US $44.95
CAN $69.95
90000
9 780596 001834
6 36920 00183 6

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

IPR2024-01049
Apple EX1021 Page 12