

Le présent fichier PDF **Sommaire** reproduit des extraits du document

802.11 (Wi-Fi) Networking Handbook

Les auteurs de cet ouvrage sont : Neil Reid, et Ron Seide
Il a été édité par McGraw-Hill en 2003

Cet ouvrage est disponible sous le numéro **AC 26785** dans l'inventaire de la collection de l'ACONIT, Association pour un conservatoire de l'informatique et de la télématique, Grenoble.

Il comprend 364 pages, structurées en 5 parties, avec de nombreux schémas, et des descriptions de normes. Depuis la date d'édition de cet ouvrage ces normes ont évolué, afin d'inclure de nouvelles situations.

Cet ouvrage montre comment les dispositifs Wi-Fi peuvent être utilisés.

Les extraits fournis dans le présent PDF donnent en copie :

- Les pages de couverture, dont la 4^{ème} page de couverture indiquant les orientations du texte et qui sont les auteurs
- La page de copyright,
- Un complément sur les auteurs,
- La table des Matières (5 pages),
- L'Avant-Propos (2 pages),
- La préface (2 pages),
- La partie histoire du chapitre-1 (10 pages),
- L'introduction à l'utilité des standards (normes) du chapitre-2 (3 pages),

Pour utiliser ce document, mentionnez les auteurs et McGraw-Hill, ainsi que la Base de Données ACONIT n° 26785.

Il est rappelé que la loi sur les droits d'auteur n'autorise que les reproductions partielles de documents à titre individuel et pour des motifs de recherche.

• design • implementation • administration



OSBORNE

802.11 (Wi-Fi)

Networking Handbook

- ❖ Maximize Wi-Fi performance and reliability, and tailor a Wi-Fi LAN to your current and future needs
- ❖ Make your wireless network as secure as your wired LAN
- ❖ Manage even the largest Wi-Fi networks, and get detailed outline of all current and future 802.11 standards
- ❖ Compare common WLAN standards, including HomeRF, BlueTooth, and 802.11, and learn why you should deploy 802.11

Neil Reid and Ron Seide

Technical Editor: Bruce Alexander

Your One-Stop 802.11 Wireless LAN Resource

802.11 (Wi-Fi) Networking Handbook

Get briefed on the intricacies of wireless LANs, and learn why 802.11 is best-suited among the WLAN technologies for most wireless applications. With a comprehensive approach that's easy to understand, this resource covers the entire integration of wireless LANs into an overall network architecture, from equipment and component

selection, through design and deployment. Learn site survey techniques, performance tips, architecture requirements, and best practices by reviewing the secrets of successful deployments. The authors' front-line experience with Cisco® Systems gives them the unique ability to bring Wi-Fi into the comfort zone of IS professionals at any level.

- ❖ Leverage your existing hardware, including switches and routers
- ❖ Utilize tools like SNMP-compliant network management software and AAA servers
- ❖ Get pertinent, up-to-date information on the public access of wireless LANs
- ❖ Understand radio frequency fundamentals
- ❖ Select the right equipment for various indoor and outdoor deployments, including access points, client adapters, and bridges
- ❖ Learn why 802.11 technology must be viewed as a fully integrated component to existing networks
- ❖ Navigate the regulatory environment summarized—including international considerations
- ❖ Secure your wireless network with propriety or IEEE standards-based security products and architectures
- ❖ Deliver robust and interoperable Quality of Service

Neil Reid is a business development manager for 802.11 and fixed wireless systems at Cisco Systems, Inc. He has worldwide responsibilities for 802.11 and fixed wireless product requirements, tactics, and strategies for systems engineers engaged in Cisco network solutions.

Ron Seide is a product line manager in Cisco's Wireless Networking Business Unit, where he works with development engineers and industry analysts as well as major enterprises and organizations in various stages of wireless LAN deployment.

The McGraw-Hill Companies



OSBORNE
www.osborne.com

OSBORNE DELIVERS RESULTS!

802.11 / WIRELESS LANs



7 83254 04087 8

ISBN 0-07-222623-4



9 780072 226232

\$50.00 USA

\$74.95 CDN

McGraw-Hill/Osborne
2600 Tenth Street
Berkeley, California 94710
U.S.A.

To arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact **McGraw-Hill/Osborne** at the above address. For information on translations or book distributors outside the U.S.A., please see the International Contact Information page immediately following the index of this book.

802.11 (Wi-Fi) Networking Handbook

Copyright © 2003 by The McGraw-Hill Companies. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

567890 CUS CUS 01987654

ISBN 0-07-222623-4

Publisher

Brandon A. Nordin

Vice President & Associate Publisher

Scott Rogers

Editorial Director

Tracy Dunkelberger

Acquisitions Editors

Tracy Dunkelberger,

Lisa McClain

Project Editor

Lisa Wolters-Broder

Acquisitions Coordinator

Martin Przybyla

Technical Editor

Bruce Alexander

Copy Editor

Bill McManus

Proofreaders

Susan Carlson Greene,

Lisa Wolters-Broder

Indexer

Valerie Robbins

Computer Designers

Tabitha M. Cagan, Lucie Ericksen

Illustrators

Michael Mueller, Lyssa Wald

Series Design

Lyssa Wald, Peter F. Hancik

Cover Series Design

Jeff Weeks

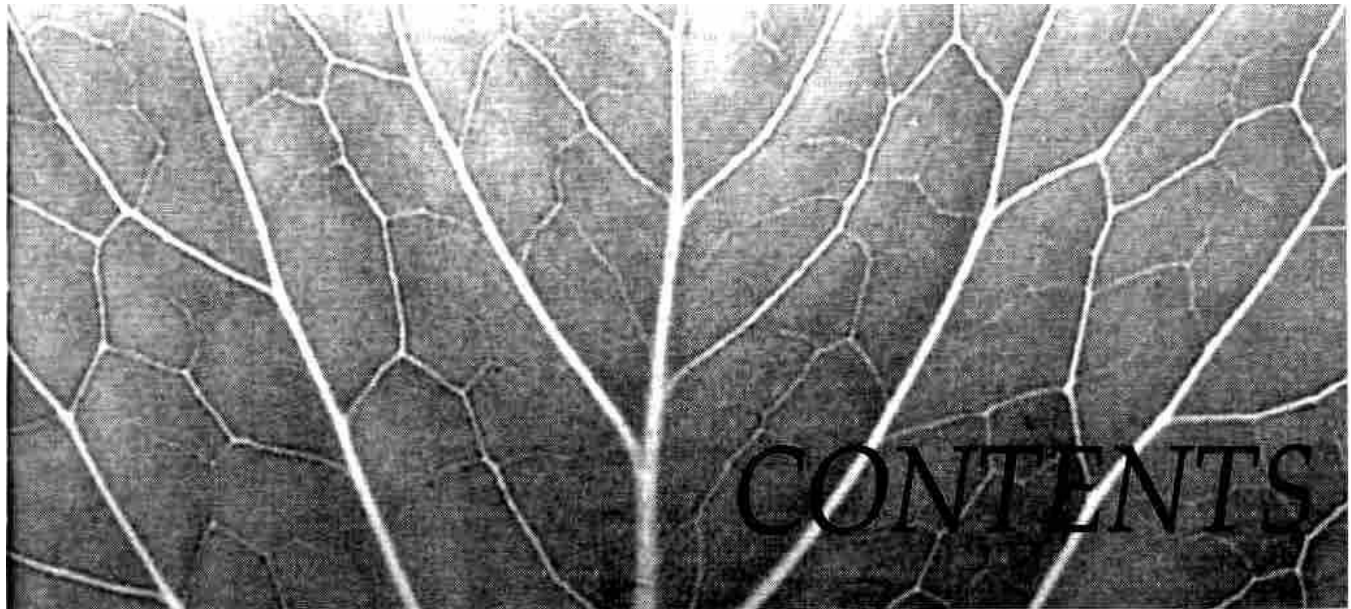
This book was composed with Corel VENTURA™ Publisher.

Information has been obtained by **McGraw-Hill/Osborne** from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, **McGraw-Hill/Osborne**, or others, **McGraw-Hill/Osborne** does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

ABOUT THE AUTHORS

Neil Reid is a business development manager for 802.11 and fixed wireless systems at Cisco Systems, Inc. He has worldwide field responsibilities for 802.11 and fixed wireless product requirements, tactics, and strategies for systems engineers engaged in network solutions for Cisco.

Ron Seide has more than a decade of experience in data communications. He's served in marketing and management capacities at various technology companies and is currently a product line manager at Cisco Systems. There, he plays a part in shaping the near- and long-term direction for Cisco's industry-leading line of Wi-Fi equipment. Ron interacts regularly with high-profile customers, industry analysts, and the trade media both to communicate product and industry trends and to understand first hand the needs of the marketplace. He has an undergraduate degree in economics and a master's degree in business administration, is an avid amateur winemaker, and is a former Jeopardy! champion. Ron, his wife Vicky, and their four children reside in their native northeastern Ohio.



Acknowledgments	xiii
Foreword	xvii
Preface	xix

Part I Moving from Wired to Wireless Networks

❖ 1 A Brief History of Wireless LANs	3
Radio, the Foundation of the Wireless LAN	4
A Founding Mother of Wireless LANs	5
Wireless Data Acquisition Systems: The Precursors of the Wireless LAN	7
The First Wireless LANs	9
802.11: The First Wireless LAN Standard	11
❖ 2 A Summary of Common WLAN Standards	13
Globalization of Standards	14
Early Technology Adopters vs. Standards	16
Technological Maturity	17
Stability of Basic Design	17
Interoperability	17
How 802.11 and Other Standards Are Developed	18
Introduction of New Technology	18
Relatively High Interest by Developers	19
Deployment of Technology to Early Adopters	19
Standards Definition by One or More Technology Providers	20
Establishment of Standard by Standards Body	20

Ratification of Standard by Technology Providers	21
Institute of Electrical and Electronics Engineers	22
Wireless Ethernet Compatibility Alliance and Wi-Fi	27
Competing WLAN Standards	28
The 802.11 Standard	30
The HomeRF Standard	34
The Bluetooth Standard	35
❖ 3 Understanding Radio Frequency Fundamentals	37
Frequency Basics	40
Power Transmission	41
Frequency Bands	44
Modulation	44
Spreading Techniques	50
Duplexing Techniques	60
Error Control	61
Earth Curvature Calculation for 802.11 Bridges	64
❖ 4 The RF Physical Layer	65
The RF Physical Layer—Layer 1	66
The Fundamental Radio Elements	66
The Radio	67
The 802.11 Radio	67
The Primary MAC Layer Functions	74
Antennas	78

Part II Designing Your Enterprise Wireless LAN

❖ 5 Performance, Architectural, and Interoperability Considerations . . .	91
Wi-Fi Performance	93
The Data Rates Supported by Wi-Fi	93
What Really Matters: Throughput	97
Going the Distance: Range	110
Interoperability	115
Checklist	117
❖ 6 802.11a and 802.11g: High Performance Wireless LAN Standards	119
Orthogonal Frequency Division Multiplexing	121
Different Bands, Different Benefits	123
Checklist	135

❖ 7	Understanding the Regulatory Environment	137
	They're Here to Help: The Regulatory Agencies	
	Applicable to Wi-Fi	138
	Regulatory Domains	138
	The FCC Regulatory Domain	140
	The ETSI Domain	148
	The Japanese Regulatory Domain	152
	Other Regulatory Domains	153
	Checklist	153

Part III WLAN Equipment and Component Selection

❖ 8	Selecting the Right Wireless LAN Equipment Components	157
	Defining the WLAN Requirements	158
	Migrations of the Technology	159
	Defining Your Technology Requirements	161
	Selecting Necessary WLAN Services	164
	Hardware Selection of the Access Point	166
	Single or Dual Radio Architecture	168
	Selecting the Client Product	171
	Summary	172

Part IV Integrating WLAN into Your Network Infrastructure

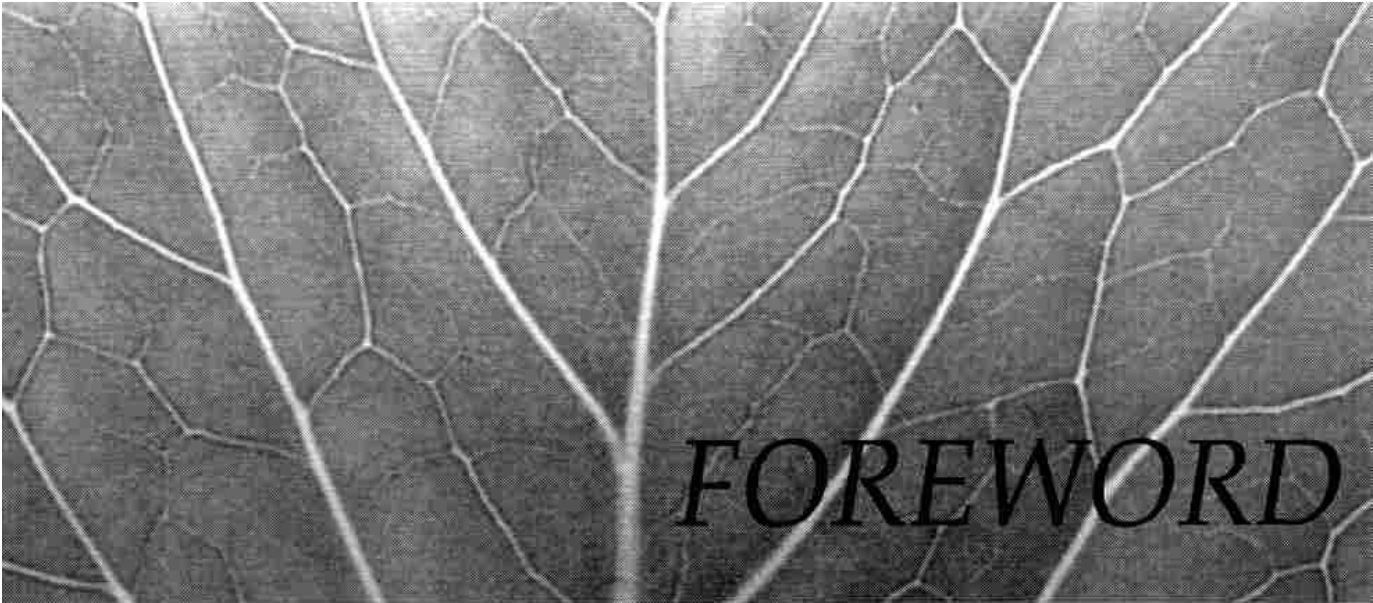
❖ 9	Wireless LANs in the Enterprise	175
	What Is the Enterprise?	176
	Wi-Fi Deployment in the Enterprise	178
	Designating Areas	178
	Capacity Planning	183
	Coverage Planning: The Site Survey	186
	Wi-Fi Management in the Enterprise	199
	Maintaining the Infrastructure	200
	Monitoring the Infrastructure	202
	Checklist	202
❖ 10	Wireless LANs in Small, Branch, and Home Offices	205
	The Primary Issues to Consider When	
	Selecting 802.11 Equipment	206
	How Will the WLAN Be Used?	207
	Which Protocol—11b, 11a, or 11g?	208

How Many Access Points?	209
Which Vendor to Select for Access Points and Client Adapters?	209
Which Antennas to Select for the Access Points and Client Adapters?	213
What Security Protocol to Use?	214
Self-Installation or Professional Installation?	215
Who to Call If the Network Goes Down?	215
Where to Acquire Training for the Devices for Deployment and Use?	215
Summary	216
❖ 11 Wi-Fi Security Best Practices	217
Authentication and Encryption	218
Authentication	218
Encryption	222
WEP: When Equivalency Isn't Equal	224
802.1X Authentication	229
Dynamic Encryption Keys	231
The 802.11i Standard	233
Different Types of Security for Different Applications	239
Checklist	242
❖ 12 QoS in Wireless LANs	243
Identifying Time-Sensitive Traffic	246
Prioritizing Traffic	247
The 802.11e Standard and WME	247
Enhanced Distributed Control Function	249
Hybrid Control Function	251
Checklist	253

Part V 802.11 and the Last Mile

❖ 13 Hotspots: Public Access of Wireless LANs	257
Where's the Wi-Fi?	258
Business Models for Hotspots	260
Settlements and Billing	261
Regulatory Issues	263
Early Wi-Fi Service Providers	264
Checklist	265

❖ 14 802.11 In the Service Provider Market	267
U-NII, 802.11a and the Last Mile	268
802.11 As Final Mile for Fiber Lateral Bypass	280
802.11 for Extension of DSL and Cable	281
Practical Considerations for Using 802.11b for Final Mile	281
Two Notes of Advice for Final Mile and Service Providers	285
Venture Capital Aspects of Unlicensed vs. Licensed Spectrum	287
❖ A Audio, Video, Voice, and Data to a PDA over 802.11 at a Nuclear Power Plant	291
General Site and Industry Considerations	292
Site Survey Considerations	295
Hardware	305
Software	306
Security	307
802.11 Network Uses	309
❖ B Glossary	311
❖ Index	345



FOREWORD

When I installed one of the original NCR WaveLAN network cards almost ten years ago, I knew the wireless LAN market would be big. But I'd be fibbing a bit if I said I knew it would be *this* big. In less than a decade, an exotic technology that was both bulky and expensive has been transformed into one of the hottest networking technologies available, used by millions of people every day for work and play.

Despite the technology's success, we've only scratched the surface of possibilities. To reach full market potential, technical obstacles must be overcome. Higher performance. Better security. Quality of Service. The list goes on. Just as important, there is a compelling need for technical information on WLAN system design, implementation, and management. Too much of the information currently available is either too technical or too business-oriented.

In the meantime, many organizations have struggled with WLAN integration issues, stubbing their toes on pilot projects that cause as many problems as they solve. Not only is the world of analog microwave radio alien to most data networking experts, it is complex enough that I have often deflected questions about how it all works, referring to it as the magic of physics.

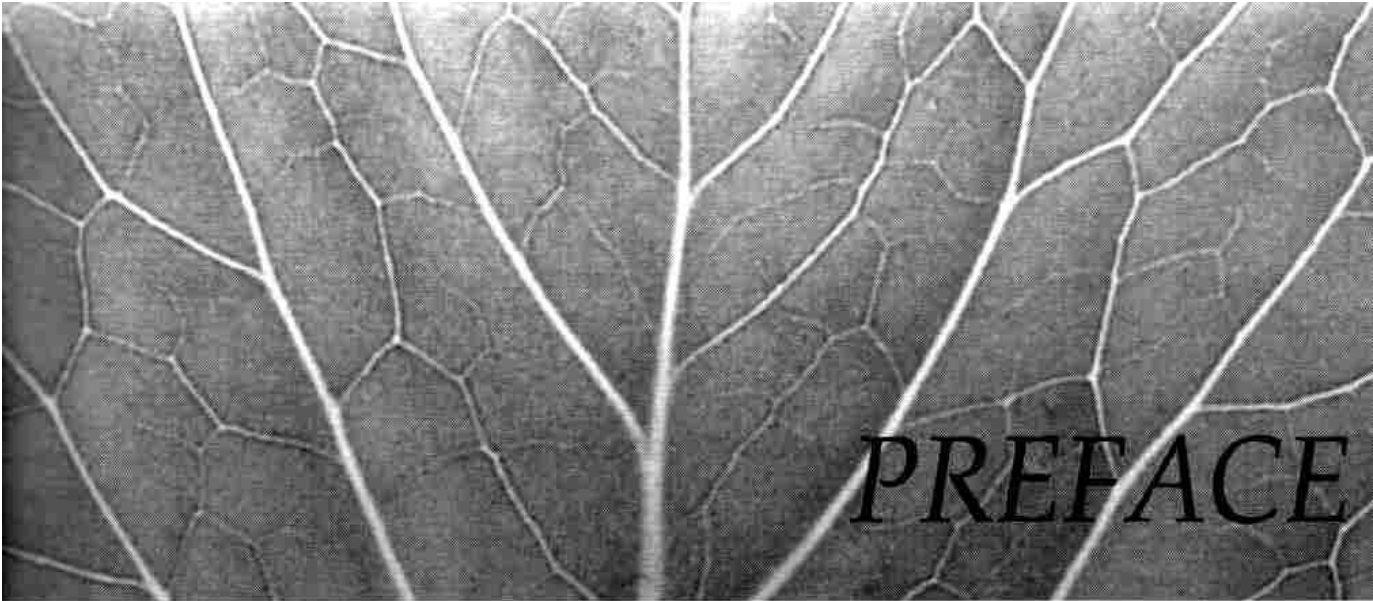
But magic is not really what wireless networking is all about. Instead, modern wireless LANs merge the complexities of two technologies that first appeared in the 1960s: digital microwave radio and packet-switched data communications. Each one is complex. Together, they are much more so.

Neil Reid and Ron Seide fill an important void by presenting an authoritative and readable treatise on today's most popular WLAN technology: IEEE 802.11, also known as Wi-Fi. They cover all key points, from technical protocol details to security and regulatory issues. The information they provide is technically comprehensive and accurate (thanks in part to the contributions of technical editor Bruce Alexander, a respected industry veteran), but it is also presented in a down-to-earth manner, with attention focused on real-world applications. Whether you're a beginner or an expert with WLANs, you'll likely come away from this book with some new insights.

Dave Molta

Director, Syracuse University Center for Emerging Network Technologies (CENT)

Senior Technology Editor, Network Computing Magazine



PREFACE

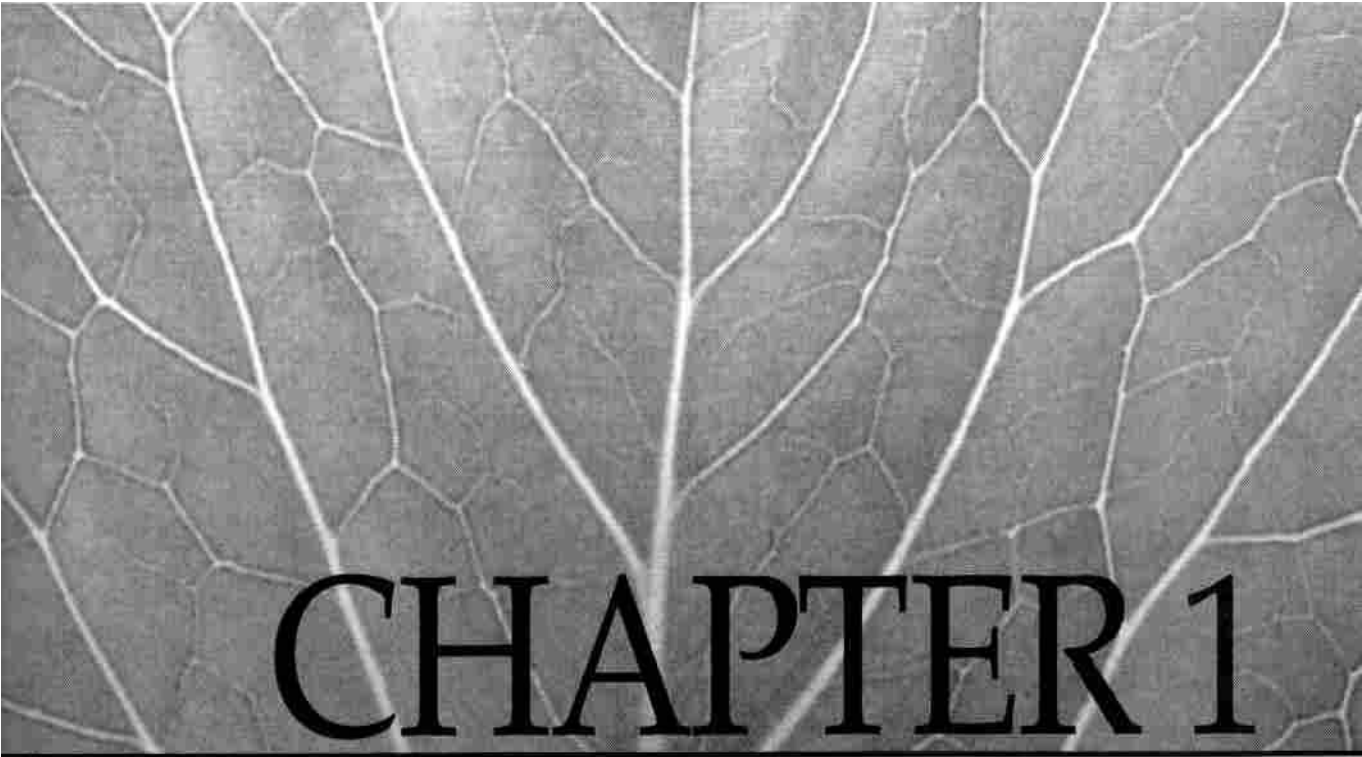
One of the hottest Internet technologies today is the wireless local area network (WLAN). The preeminence of this technology can be measured in part by the fact that it is one of, if not the only, technology that has remained “recession proof” during the last two years. Another suitable metric would be that of the billions of dollars in annual sales that this technology generates on a worldwide basis. The predominant standard for this technology was, and continues to be, assembled by the IEEE with an array of workgroups under the general heading of 802.11. These workgroups cover a multitude of challenging issues, such as carrier frequency, modulations, security, quality of service, interoperability, and many others.

Technical literacy on this subject, the practical application thereof, and a contextual understanding of the wide array of issues are every bit as important today as is understanding Ethernet. Whereas the bulk of discussions between network administrators, technology vendors, and CxOs used to center on how a radio performed, the discussions are much more centered now on security and mobility in general. The scope of this technology is now way beyond that of radio technology fundamentals. The authors of this work along with the technical editor are part of the team at the very forefront of this technology, given their respective positions at Cisco Systems, which designs and ships more 802.11 technology for enterprise networks than any other company. This book is essentially a

detailed response to the most commonly asked questions from network managers and end users around the world.

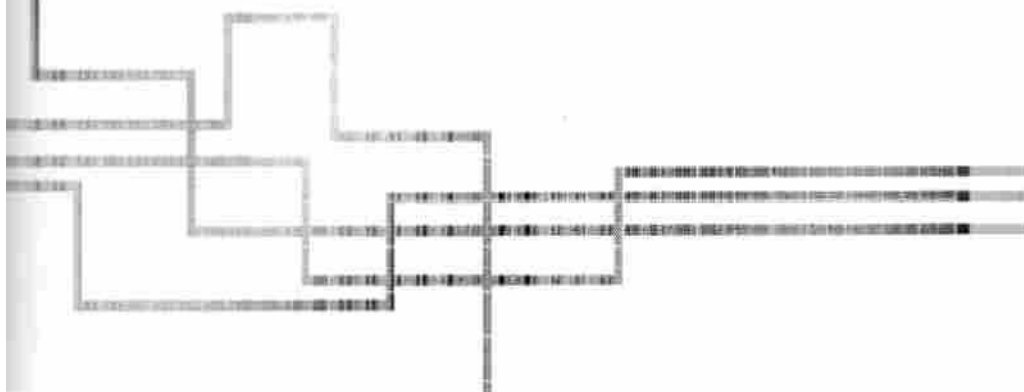
It is our hope that, through this book, you'll not only gain an understanding of this wonderful and important technology, but also be part of a technology revolution that has no equal in human history in terms of adoption rate—the Internet.

*Best Regards,
Neil Reid and Ron Seide*



CHAPTER 1

A Brief History of Wireless LANs



Although the technology is referred to as wireless local area networking (wireless LAN), at its core, it's radio. And so, while the history of Wi-Fi or 802.11 only goes back to the mid-1980s, the history of the technology began over 100 years earlier. In this chapter, we provide a brief history of the technology that forms the foundation of wireless LANs. We do this both because the development and deployment of radio and data communications are among the most fascinating technology stories of the twentieth century and because having at least a passing acquaintance with what came before today's wireless LANs helps you to understand the evolution to today's standards and, more importantly, where they're likely to go.

RADIO, THE FOUNDATION OF THE WIRELESS LAN

As radio technology is the foundation of the wireless LAN, the early work in electromagnetics is in turn the foundation of radio. The Scottish theoretician James Clerk Maxwell first put forth the notion of electromagnetic waves in 1864, postulating that they arose as an electronic current changed direction. A device designed to produce electromagnetic waves by changing the direction of an electrical current, a process known as oscillation, is in essence a transmitter. The German Heinrich Hertz built upon this, developing equipment in the 1880s that actually sent and then received electromagnetic waves over the air. This equipment was capable of increasing the number of waves produced in a given period of time, their frequency, and their rate of change or oscillation. His name, of course, became a common unit of measure for frequency, where 1 hertz (Hz) means one complete oscillation or cycle per second. In radio, the more common kilohertz (KHz) means thousands of these waves per second, megahertz (MHz) means millions of waves per second, and so on through gigahertz (GHz). In this way, the increasingly shorter electromagnetic waves may be quantified and placed in increasing order of frequency or descending order of wavelength—it's the same idea since the more frequent the cycle, the shorter the wave will be. This linear quantification is today known as the radio frequency or electromagnetic spectrum.

It was Guglielmo Marconi who took this pioneering work to the next step and then on to practical application. While his name is forever linked with what we today colloquially refer to as radio, the transmission of sound, his first application was actually an early form of data communications. In the decade following the work of Hertz, Marconi synthesized his developments with those of Samuel Morse. Marconi reasoned that if it were possible to transmit binary signals (dots or dashes) across a wire, it should be possible to send these same signals across an electromagnetic wave and use them as a means of communication.

In 1895, when he was just 21 years old, Marconi sent and received his first radio transmissions across the attic of his parent's villa in the Italian countryside. The following year, he was achieving transmissions of over a mile. With improvements to his transmitters and antennas, distances increased quickly and dramatically, moving radio from the realm of science into that of technology. Marconi realized the commercial potential for his radio telegraphy equipment, obtaining his first patent in 1896 and

forming a company, the Wireless Telegraph and Signal Company Limited, in England the following year. By 1898, Marconi's wireless telegraphy equipment was being used for ship-to-shore communications as well as terrestrial applications in lieu of wired systems—an early example of wireless supplanting more traditional wired infrastructure. The next year, a wireless link between England and France was established, and in 1901, a message was sent from England to Newfoundland across the Atlantic ocean.

Thomas Edison was the driving force behind the first commercially deployed wireless systems in the United States, which became the foundation of General Electric, one of the largest and most successful companies in the world. Edison's work was based on that of Marconi and one of Edison's own former employees, Nicola Tesla, a recently arrived immigrant from Europe. Interestingly, after many years of controversy, in 1998 Tesla was given formal recognition by the U.S. Patent Office as an inventor of radio, a distinction formerly held solely by Marconi.

The world of wireless technology has come a very long way from the days of Tesla, Marconi, and others. From the crude but brilliant devices built in their labs, differing types of wireless technologies have proliferated on every continent and are deemed mission-critical business tools for efficiency as well as important items for personal safety and convenience.

It is interesting to compare the early days of radio with those of the personal computer industry. In our time, the development of the PC is held up as the standard for rapid development from theory and concept to practical application. The early PC industry was driven by energetic and brilliant young people like Bill Gates and Steve Jobs. The development of radio is no less astounding. From theory to application in a decade, from proof of concept to commercialization (in the form of a multinational company!) in two years. All driven by a man in his early twenties. Marconi and others like David Sarnoff, Alexander Popov, Lee DeForest, and Reginald Fessenden made additional advancements and refinements, ushering in the "golden age" of radio in the 1920s with commercial broadcasting and the societal change it fostered. In 1923, the United States government first began the process of dividing up the radio frequency spectrum into allocations for specific uses and users. Eleven years later, the Federal Communications Commission (FCC) was chartered. Today, Marconi Corporation, while being a worldwide communications technology provider, is one that, ironically, plays little role in radio and wireless LANs.

A FOUNDING MOTHER OF WIRELESS LANs

Innovation often comes from unlikely sources, and few are more unlikely than a glamorous actress and a noted composer sitting together at a piano at a 1940s Hollywood cocktail party. Hedy Lamarr was a well known movie star and widely held to be one of the most beautiful women in the business. What was unknown to the general public and even her adoring fans was that she possessed a sharp intellect and, as a native of Austria, a hatred for the growing Nazi régime in Germany.

George Antheil was a noted composer, one of his compositions in which airplane propellers were used as drumsticks having been performed at Carnegie Hall. The story goes that when Hedy was married to an arms dealer in her native country, she picked up fragments of ideas for radio innovation in Europe. George, of course, was well versed in music theory, in particular the patterns of the 88-key piano keyboard. At that party, these two areas of knowledge came together to aid in the Allied war effort.

A system of spreading narrowband radio communications across a broad band of the frequency spectrum was devised by Lamarr and Antheil as a means of guiding torpedoes to their targets in a manner that was less susceptible to frequency jamming techniques or eavesdropping. This was accomplished by having the frequency that the controller and the torpedo used to communicate move or “hop” from one channel to the next with a predetermined and coordinated pattern. Their resulting patent, awarded August 11, 1942, was the first spread spectrum system. Not surprisingly, the number of hops in these patterns was 88, matching the number of keys on the piano keyboard. Player piano rolls were envisioned as a means of controlling these hopping patterns.

To jam a signal that is spread across a wide portion of the frequency spectrum, all of the spectrum that the signal is spread across would have to be jammed. By having the signal hop from one frequency to another, in a pattern predetermined by and known only to the sender and receiver, the pattern would have to be “hacked”—the code would have to be broken—by the intercepting party. While this general concept invented in front of a piano at a party may today seem intuitive, it was unique and unobvious enough to warrant a patent.

Spread spectrum radio communications was well before its time and was never actually used during the Second World War. It was, however, considered to be important enough by the U.S. military to have been classified and kept secret until the 1960s. Given the secrecy shrouding the patent and the development stemming from it, it's impossible to estimate the degree to which the patent was employed in future developments. What is known is that by the 1960s, when data processing technology advanced to the point that a computer (not a piano roll) could control hopping patterns, spread spectrum frequency hopping indeed did become the foundation for secure, robust, and nonjammable military communications. The value of this approach for commercial purposes is clear: private radio users often require secure communications in the same way that the military does. Although it's relatively uncommon for private communications to be intentionally jammed, unintentional jamming, and resulting performance loss or complete breakdown of the system, is inevitable if many users are sending radio communications in the same frequency band.

In 1981, the U.S. government declassified Lamarr and Antheil's now-expired patent for a “Secret Communications System.” The timing of this release into the public domain wasn't a coincidence: in 1985, the FCC first allocated portions of the radio frequency spectrum for use without license by “industrial, scientific, and medical” (ISM) parties. The operation in these ISM bands was, and today still is, covered under FCC Part 15 rules, which stipulate the types of radio communications permitted. One of the schemes allowed for use in the ISM bands is spread spectrum technology. Prior

to this, spread spectrum had been used on only a limited commercial basis for communications with multiple satellites. With spread spectrum, a greater number of users, with no specific knowledge of or coordination among each other, can operate in the band without unintentionally jamming each other's communications. While spread spectrum transmission was ideal for the military for one set of reasons, it was additionally ideal for unlicensed private use for other reasons—a most useful and extensible technology!

WIRELESS DATA ACQUISITION SYSTEMS: THE PRECURSORS OF THE WIRELESS LAN

The first systems that bear any real resemblance to today's wireless LANs began to appear in 1985. A thread that runs through the history of this technology is that if an application is so ideal for wireless connectivity, users will accept a suboptimal solution. Retail is just this sort of application. Indeed, in retail and associated warehousing and distribution center environments, there is an obvious need for a retail associate or inventory manager to roam freely throughout the facility with a data acquisition terminal like a bar code scanner. This "wirelessness" can of course be accomplished by batching the collected data and then uploading it at the end of a session, but this doesn't provide for the real-time, up-to-the-minute information that is so critical to making just-in-time (JIT) inventory systems work. A far better solution is for the data collection device to be in continual, real-time contact with the inventory system. Communication via radio waves is the natural way to do this as dragging a cord through store aisles is impractical to the point of comical.

It's something of a stretch to refer to these wireless systems as being local area networks. Rather, these first wireless data acquisition systems were simply a collection of devices that were modified in some very clever ways that were not envisioned by their original designers. Unlike a LAN, these systems were actually point-to-multipoint polling systems where user devices don't contend for or simultaneously share the transmission medium but rather use it in turn. The design for these early data acquisition systems was actually based on a far-flung wide area system, ALOHANET, a wireless system that connected the Hawaiian Islands. Operating at 9600 bits per second (bps), ALOHANET was the first system for sending data packets over radio and represents not only a precursor to wireless LANs but also the foundation for the predominant *wired* local area technology—Ethernet.

Telxon Corporation of Akron, Ohio, then a leading manufacturer of batch-processing data acquisition terminals, developed one of the first wireless systems by bolting a 1200bps modem to a batch-processing terminal via the asynchronous serial interface that typically was used for uploading data at the end of a session. In *addition* to the cable that ran from this terminal to the handheld scanning gun, a cable was run to what is essentially an off-the-shelf walkie-talkie onto which a cable connector had been soldered. This three-piece system—radio, terminal, and scanner—was inelegant to say

the least; the user with a system of three heavy pieces would often literally drag the radio across the floor as they moved down an aisle (suboptimal, but not nearly as bad as dragging a cable through the entire facility!). On the receiving side, an off-the-shelf walkie-talkie was similarly modified and attached to a modem to demodulate the data coming in over the air from the remote units. This device then interfaced into a modified batch-processing collection terminal. The fact that this system sold at all indicates just how well wireless fits in a retail environment. In addition to the user, the inelegance of this system impacted those who managed these systems. This system was based on serial interfaces with no real networking protocols involved, putting it beyond the reach of most information technology departments. Even though the traffic on the system was unidirectional, was time sliced such that two terminals never transmitted simultaneously, and was typically just bar code scans, the low bit rate of the modem coupled with the radio described below limited the number of users per base station to ten.

But it was on the radio side where most of the inconvenience was concentrated. The rugged, commercial-grade walkie-talkies used were not the toys found under Christmas trees but rather licensed devices used commonly on construction sites, by security firms, and by municipal workers. Although the FCC had declassified the spread spectrum patents in 1981, and, at the request of the FCC, the Institute of Electrical and Electronics Engineers (IEEE) began to study the commercial applicability of spread spectrum communications, the radios pressed into service in wireless data acquisition systems were narrowband devices and not based on spread spectrum technology. Indeed, it wasn't until 1985 that regulations were in place to allow for the regulated use of spread spectrum technology by the public.

Operating in the ultrahigh frequency (UHF) portion of the frequency spectrum in the 450- to 470MHz range, these narrowband crystal-controlled radios were set at the factory to a particular 25KHz-wide narrowband channel that could only be retuned to a different channel by changing the crystal at the factory. To operate on any of these 25KHz-wide channels, a geographic operation license from the FCC is required. The implications here are numerous. First, it is of course desirable for a geographically distributed organization like a retailer to have interchangeable devices. It is, however, unlikely that a single channel is available for licensing in all geographies where that retailer operates. The upshot is that licensed radios that are incapable of being tuned to a different channel are specific to their location, which adds administrative, support, and inventory burdens. Worse still, if all 25KHz-wide channels are already licensed in a particular location (a likely scenario in heavily populated areas), wireless operation is simply not possible. Finally, in retail, it's common for periodic physical inventories to be done by contracted firms that move from location to location, performing full inventory over a single night with a large team. Here, the requirement for a geographic license is either a major inconvenience or a motivator for noncompliance. Additionally, the ten-user limit, which is also driven by the narrow license band, makes for a less efficient operation.

By 1988, incremental improvements to these early data acquisition systems were being made. By integrating the radio into the data acquisition terminal, the user's system went from being a three-piece unit back to the same two pieces found in batch-processing units. By migrating from the first 1200bps modems to what were then state-of-the-art 9600bps modems, the user count per base station increased from 10 to 30 users. It's interesting to note that this increase in system performance, and corresponding increase in user count, was achieved not by increasing the available bandwidth (it was still limited to the narrow 25KHz-wide band) but rather by using a higher-order modulation system found in the 9600bps modem. This same means of improving performance through better data modulation algorithms (not increases in bandwidth) is today driving performance increases in contemporary wireless LANs.

These improvements contributed to wireless data acquisition systems breaking out of their first retail markets. Most any business traveler has some familiarity with the next market to adopt these real-time wireless systems. Airport-based car rental agencies, Avis in particular, were the next set of customers to embrace these systems. Here again, the need to rapidly acquire data about the returning cars and process the transaction in real time was so great that these companies were willing to take the risks and bear the inconvenience that are inherent in being an early adopter of a technology. In addition to the multipart user system, the licensed radio negatively impacted the use of the system for car rental companies in much the same way as it did retailers. In outdoor airport environments, this effect was even more pronounced, as signals from nearby licensees had greater potential for interference when outdoors. Additionally, airports are in general "noisier" environments for radio frequencies, creating a general interference impact on these narrowband systems set to static channels. Clearly, improvements to these early systems needed to take place to address their limitations.

THE FIRST WIRELESS LANs

With the 1985 changes to FCC Part 15 regulations that allowed for the use of spread spectrum radio in commercial applications, the door was opened to commercialize the technology. A little more than a year after the FCC regulation change, a company, Telesystems SLW, was formed in Toronto to exploit this development.

It's interesting to note that while the system designed by Telesystems was indeed spread spectrum, it used a variation on this theme that is different than the frequency-hopping system put forth in the original spread spectrum patent. Rather than having a narrowband signal hop from one frequency to the next over a given wide band, Telesystems employed a system referred to as *direct sequence*, whereby a narrowband signal is spread over the given wide band by multiplying the width of the signal across a greater set of frequencies. The result of this system is similar to that of frequency hopping; that is, the narrowband signal that is spread out over a wider band is less

susceptible to interference because only some portion of the multiplied signal needs to reach its intended receiver for the transmission to be successful. Additionally, and much like with frequency hopping, the direct sequence signal at that time provided some level of security insofar as the decreased power per unit of bandwidth made the signal less discernible from the surrounding noise when using contemporary eavesdropping equipment.

In 1988, the first commercial systems based on Direct Sequence Spread Spectrum (DSSS) technology were released to the market. In addition to incorporating DSSS, these systems operated not in a licensed band, but rather in the unlicensed band newly established by the FCC between 902- and 928MHz. Because this band was located close to the licensed band allocated for analog cellular telephone use in North America, it provided manufacturers with the advantage of being able to build their unlicensed devices with repurposed components originally intended for use in cell phones. With license-free operation, the administrative burden and lack of commonality across geographies that was so troublesome to early adopters of wireless data acquisition systems was addressed. With DSSS, cohabitation with other unlicensed users in the same band was possible, allowing users to sort out interference problems by themselves. In general, license-free operation using DSSS was an ideal solution for retailers, car rental agencies, and similar vertical market applications. Naturally, these first unlicensed DSSS systems were targeted at a completely different application.

The first products from Telesystems were designed as cable replacements, either to connect multiple desktop computers to a central base station in much the same way as an Ethernet network would, or to connect the networks in separate buildings together in much the same way as a bridge. Running Novell NetWare, the predominant network operating system at the time and providing a data rate of about 200,000bps (200Kbps), these very first wireless LANs for office environments carried a retail price of \$1,500 per node. Although the product found critical favor, it was ultimately well ahead of its time and provided an insufficient price-to-performance ratio to gain the sort of mainstream acceptance needed to sustain a company. Indeed, today the proliferation of wireless LANs into typical office environments is only just beginning.

Rather, it was the vertical market applications then being served by the licensed narrowband radios where spread spectrum technology first gained a commercial foothold. Recognizing the scalability and geographic consistency advantages of unlicensed spread spectrum operation, Telxon began to offer the Telesystems unlicensed radios in its data acquisition terminals as an alternative to the licensed narrowband radios that were then provided in large part by Motorola. Ironically, to gain a foothold in the marketplace, the Telesystems radios were designed to match the physical specifications of the Motorola radio such that they could be swapped into the same data acquisition terminals. Telxon quickly became the largest customer of Telesystems.

Customers quickly realized the advantages of the new unlicensed offering and a migration began to take place, with the watershed event occurring in early 1991. Wal-Mart, now the world's largest company in terms of revenues, was then, as now, a company and one that aggressively leveraged new technology to further their

leadership. Realizing how the unlicensed radios would enable it to have a common wireless infrastructure across all of its North American operations, Wal-Mart placed a staggering 30,000-piece order with Telxon, to be fulfilled by Telesystems. The order was to be fulfilled in six months' time and at a very low price.

Telxon quickly realized that the only way to meet the delivery and price terms was to make dedicated its supplier, and thus in early 1991, Telxon completed the acquisition of Telesystems SLW and completed the order. In 1999, Telxon spun off its radio group as Aironet Wireless Communications, which months later was acquired by networking giant, Cisco Systems.

While operation in the 900MHz band provided for a common infrastructure across the United States, Canada, and Australia, this band was limited in that it was not allocated for unlicensed operation in other parts of the world. To address markets outside these areas, manufacturers began producing radios that operated in the 2.4GHz portion of the frequency spectrum that was available for unlicensed operation across most of Europe and Japan—as well as in the United States, Canada, and Australia. In similar fashion to the 900MHz band, the 2.4GHz band presented vendors with the advantage of being able to repurpose components originally intended for use in European cellular phones that operated in a nearby licensed band. While 900MHz remained the most commonly used band in North America throughout the first half of the 1990s, 2.4GHz radios began to proliferate as license-free operation began to gain acceptance in Europe and Japan.

Operation in the 2.4GHz band had key advantages over the 900MHz band. By operating in an open band that was essentially common (there are some subtle differences in the frequency range from one country to the next), a manufacturer can build a single radio that, with some minor tuning, can be sold around the world, thereby providing for better economies of scale. Moreover, as license-free operation in North America became more popular, the airwaves at 900MHz became crowded with not just wireless LAN equipment but with the far more common cordless telephones as well. The 900MHz band began to be referred to as a “garbage band” due to all the interference that impacted wireless LAN performance and reliability. But, finally, it was the move toward standardization that sealed the fate of wireless LAN operation in the 900MHz band.

802.11: THE FIRST WIRELESS LAN STANDARD

Realizing the mutual benefit of defining industry standards for wireless LANs, in 1991 individuals representing a number of interested parties, including competing vendors like Telxon, NCR, Proxim Technology, and Symbol Technologies, first submitted a Project Authorization Request (PAR) to the IEEE to establish an interoperable standard for wireless LANs. As an international organization, the IEEE as a general rule drives toward standards that have worldwide applicability. This drove the newly formed group toward the 2.4GHz band and away from 900MHz.

By 1993, the foundation for a standard was in place, and in June of 1997, the IEEE 802.11 standard, more than six years in the making, was ratified. This first 802.11 standard provided for data rates of 1 and 2 megabits per second (Mbps), a rudimentary form of data encryption with the arguably misleading name Wired Equivalent Privacy (WEP), and transmission via both direct sequence and frequency-hopping technologies in the 2.4GHz band as well as over infrared light. The infrared aspects of this standard found little commercial favor and today represent little more than an historical footnote.

While WEP is still deployed, it has been roundly discredited as a viable means of securing traffic on a wireless LAN. As a compromise to satisfy the competing vendors represented in the committee, both frequency hopping and direct sequence spread spectrum were ratified as standards-compliant means of radio transmission. Operation in these two competing manners were, of course, not interoperable and indeed had the effect of interfering with each other and driving down performance when physically collocated. The effects of this compromise were wide ranging, resulted in substantial confusion, and are still being felt today, particularly as early adopters migrate to today's higher speed standards. Nonetheless, the first 802.11 standard marked the beginning of a whole new era and set the foundation for the next standard, 802.11b, which was ratified in 1999 and provides for an 11 Mbps data rate, approximately the same as standard Ethernet.

The details of 802.11b and associated standards, and what they mean to the networking professional, will be covered thoroughly throughout the rest of this book. By either 802.11 or Wi-Fi, the trade name now associated with the technology, wireless LANs are changing what it means to be well connected.

The issue of standards is one that many of us don't think about very often, yet it has been important to humankind for as long as people have been communicating with each other. Standards exist primarily to ensure a common basis and agreement for the form and function of the devices and services by which we are surrounded. Additionally, in modern times, standards are also used to help protect those who use products and services.

Standards also reduce the number of challenges with interoperability and information exchange. The more broadly adopted a standard is, the wider the market for a group of technology providers, with the most preferred standard being one that has been ratified on a global basis. It then follows that the more widely adopted a standard becomes, the greater the amount of synergy between technology providers and the marketplace they service. International standards, however, are far more difficult in practice than in theory.

Standards also define by law what certain values are, such as the foot, the meter, time, a gallon or liter of gasoline, and so on. Standards define what a specific device or service is or is not, and enable both technology and service providers to legitimately claim, use, and adhere to well-defined standards.

GLOBALIZATION OF STANDARDS

One of the earliest examples of a standard was the *cubit*, which was considered to be the length of a man's arm from his elbow to the tips of his fingers. In 8 B.C., this distance was widely agreed to be 17½ inches (although only nine years later it was generally agreed to be 21½ inches). By this standard, according to the Bible, Noah's ark (commonly believed to rest on Mt. Ararat in Turkey) was a relatively large vessel at 437.5 feet long by 72.9 feet wide by 43.75 feet high. Many other ancient records of measurements provide information regarding the size of buildings and the weights and measures used for commodities such as grain and currency.

The measurement of time is a very important standard, and the progress of technology has been directly linked to how well this resource is measured. Consider how the ancient traders and merchants of the Mediterranean engaged the owners of ships and caravans to coordinate the transfer of goods and money. It was common for either the ship's crew or the traders to wait for weeks or even months at a specified site to make their exchanges, because the standard of time used during that period was generally measured by the phases of the month or season. Predating this, navigation on the open ocean from the ancient Mediterranean world to the West could not occur until it was possible to measure time with an appropriate degree of accuracy and consistency.

Standards today have a tremendous impact on how we select and use products. In the United States, we are very familiar with the inch, the pound, the ounce, and the dollar, while most of the rest of the world is more familiar with the metric system and their native forms of currency. As the world continues to become a truly global community, many people have had to become fluent in the standards used in places far from where they work or reside.

Associated with this issue, the United Nations has been struggling with various countries for years in terms of which standard to use for mobile wireless communications, and it is only relatively recently that a world traveler could take their cellular phone from London, England, and travel to Singapore through the United States while using the same phone. This has far less to do with the use of a single standard than it has to do with manufacturers providing cellular phones that automatically switch between as many as three or four different modulation schemes and frequencies, and many people around the world own “dual mode” or even “tri-mode” phones for this specific reason. Standardization of these mobile wireless modulations makes it possible to build a cell phone in Norway that will function properly on three or more continents.

The definition of a standard can be entirely nontrivial. The even larger issue of *when* a standard is adopted is as important as the actual standard itself, as we live in a world where technology is conceptualized, developed, and deployed with rapidly decreasing amounts of time.

In the world of WLANs, we are fortunate to have certain fundamental standards that have been ratified at the global level, such as frequency, power, and time. A WLAN link that operates at 2.4GHz is equally understood and accepted in Japan, England, Canada, and the United States.

The 2.4GHz frequency is, in most nations, set aside for the purpose of having an unlicensed radio frequency system, and is probably the only frequency so well adopted, deployed, and characterized.

Further, since the idea of standardization for broadband, two-way WLAN usage is still somewhat new, regulatory groups, international bodies, and developing standards groups are struggling for control and authority to allocate and/or dedicate specific frequencies for particular uses in numerous countries.

Another issue not widely agreed upon on a global basis is that of *channelization*, which is how radios break up the amount of spectrum available into usable subsets for communication. Further, except for 2.4GHz, spectrum allocations vary widely from country to country in many cases, which makes it difficult for radio manufacturers and service providers to provide truly globally usable products, because they are commonly unwilling to design, test, and submit radios for local federal approval for every country that has a substantial market.

The lack of frequency and output power standards at the international level has forced some hardware vendors to adopt multiple products, designing specific RF units to work in allocated frequency bands for specific countries. This approach raises the cost of goods and inventories. Without this approach, countries with frequency bands different from the key revenue-generating superpowers, such as the United States, England, Germany, France, and Japan, are left without alternatives for broadband wireless.

This is one of the major reasons some companies have adopted architectures that allow indoor equipment, such as the routers and switches at each end of the radio links, to be independent of the carrier frequency, channelization, power requirements, and other settings that reside in the actual radios that operate the outdoor portion of

the network. This approach still requires multiple outdoor units from one or more technology providers, depending on the specific country.

At this point, the technology does not exist, primarily for technical as well as financial reasons, that would enable *ultrawideband* microwave products that would cover multiple radio bands. Until the countries of the world and the governing bodies and regulators get together on frequency standards, there will be limited global acceptance of broadband wireless technology. The outlook for this general ratification is deemed unlikely as countries tend to rightly view spectrum as a national asset, which therefore should not be mandated by foreign countries. This is in part why the generally global adoption of 2.4GHz is a unique situation; and one that is being capitalized upon by radio manufacturers in order to increase the total addressable market.

EARLY TECHNOLOGY ADOPTERS VS. STANDARDS

In the open commercial market, the *early technology adopters*, commonly referred to as *early adopters*, are the first ones to adopt cutting-edge technology. They constitute the portion of the market that is willing to exchange the risk of using an unproven technology for a prospective gain on their competitors. The objective for them in some cases is to acquire as much market share as possible at the earliest date possible. In other cases, early adopters deploy cutting-edge technology on a bet that the overall cost of doing so will more than offset a particular problem. By accepting higher risk, new technologies can enable a competitive edge in both established and emerging markets.

Early adopters are generally very tolerant of the teething problems common to cutting-edge technology and are often selected as the first sites for equipment and technology trials. They also generally possess a higher level of technical savvy and experience and quite often employ unique enhancements to resolve some of the bugs that necessarily accompany relatively unproven technologies and solutions.

The early adopter market does not typically comprise the bulk of the market and is generally comprised of the smaller customers that want to give their larger or more adept competitors a run for their money and are willing to do so in part by adopting higher risk with their selected technologies. The bulk of a market opportunity for technology providers occurs later, after the early adopters have seeded the market with the latest technology and endured the significant growing pains and learning curves of leveraging an emerging technology.

These growing pains are usually fed back to the manufacturers to revise/improve/revisit their products to evolve better solutions that are (hopefully) made available to the risk takers first, who can (once again hopefully) enhance/extend the new providers a technology lead in the emerging market. If successful, or even apparently promising, larger companies will then follow suit in using the technology, which by then has generally been suitably debugged.

It is generally the larger companies that tend to require standards-based products, because this ensures several key issues for them: