Wi-Fi Handbook

Building 802.11b Wireless Networks

Frank Ohrtman
Konrad Roeder

McGraw-Hill
New York Chicago San Francisco Lisbon
London Madrid Mexico City Milan New Delhi
San Juan Seoul Singapore Sydney Toronto

The McGraw-Hill Companies

Library of Congress Cataloging-in-Publication Data

Ohrtman, Frank.
Wi-Fi handbook: building 802.11b wireless networks / Frank Ohrtman, Konrad Roeder.
p. cm.
Includes Index
ISBN 0-07-141251-4 (alk. paper)
1. IEEE 802.11 (Standard) 2. Internet service providers—Standards.
3. Telecommuncation—Technological innovations—United States.
I. Roeder, Konrad. II. Title

TK5105.5668.036 2003
004.67'8—dc21 2003044574

1 2 3 4 5 6 7 8 9 0 DOC/DOC 0 9 8 7 6 5 4 3

ISBN 0-07-141251-4

The sponsoring editor for this book was Stephen S. Chapman and the production supervisor was Sherri Souffrance. It was set in Century Schoolbook by MacAllister Publishing Services, LLC.

Printed and bound by RR Donnelley.

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please write to the Director of Special Sales, Professional Publishing, McGraw-Hill, Two Penn Plaza, New York, NY 10121-2298. Or contact your local bookstore.

This book is printed on recycled, acid-free paper containing a minimum of 50 percent recycled de-inked fiber.

CHAPTER 1

Introduction

In the late 1990s, the telecommunications boom went bust because new market entrants, known as *Competitive Local Exchange Carriers* (CLECs), were forced to compete with *Incumbent Local Exchange Carriers* (ILECs) on the same financial terms of the incumbents. The failure of the CLECs resulted in a net investment loss of approximately $3 trillion, adversely affecting capital markets and severely depressing the overall telecommunications economy as well as saddling subscribers with artificially high rates.

The Telecommunications Act of 1996 aimed to introduce competition in the local loop by legally requiring incumbents to lease space on their switches and provide access to their subscribers to any and all competitors. New market entrants found themselves stonewalled in the courts by the incumbents when attempting to gain legal access to the incumbents' facilities. Once legal access was gained to the incumbents' switching facilities, the incumbents conveniently forgot the orders or otherwise sabotaged the operations of the CLECs in the incumbents' switching facilities.

Given the astronomical expense of deploying a conventional, but alternative network or the legal obstacle of gaining access to the *Public Switched Telephone Network* (PSTN), it is not surprising that seven years after the passage of the Telecommunications Act of 1996, only 9 percent of American residential phone lines are handled by competitive carriers. Given this dismal figure, it is clear that regulatory agencies such as the *Federal Communications Commission* (FCC) and the utilities commissions of the 50 states have failed to adequately enforce either the letter or spirit of the Telecommunications Act in regards to introducing competition in the local loop.

A competitive local loop environment has two apparently insurmountable obstacles: (1) the high cost of Class 4 and Class 5 switches and (2) gaining access to the local loop network. At the time of this writing, despite the guarantees contained in the Telecommunications Act of 1996, it appears obvious that competition will never come *in* the local loop but will have to come *to* the local loop in the form of an alternative network. The only way consumers will enjoy the benefits of competition in the local loop is when alternative technology in switching and access offers a competitor less barriers to entering and exiting the telecommunications market. If telecommunications consumers are supposed to enjoy the benefits of competi-

tion in their local loop, the ability to bypass the switching architecture to gain access (via copper wires from the telephone company) must be offered.

Telecommunications Networks—The Need for an Alternative Form of Access

An understanding of the PSTN is best grasped by examining its three major components: access, switching, and transport (see Figure 1-1). Each element has evolved over the 100-plus-year history of the PSTN. *Access* pertains to how a user accesses the network. *Switching* refers to how a call is switched or routed through the network. *Transport* describes how a call travels or is transported over the network. This network was designed to handle voice. Eventually, data was introduced onto this network. As data traffic on the PSTN grew, high-capacity users found it inadequate. These subscribers then moved their data traffic to data-specific networks. Many data users find themselves limited to an infrastructure that is dependent on wires, whether they are using fiber-optic cable, coaxial cable, or twisted-pair copper wire. Although wireless communication is not new (forms of radio communication have been in use for almost a century), using wireless communication to bypass wired monopolies is now a practical opportunity for subscribers of both voice and data

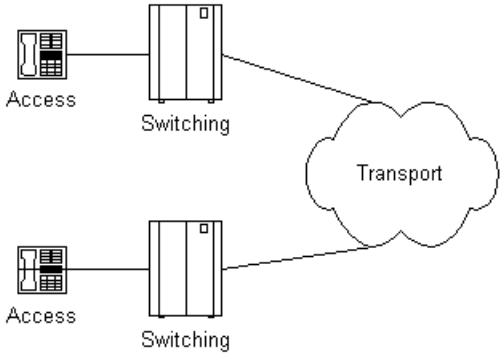

Figure 1-1
The three components of a telephone network: access, switching, and transport

services. The primary form of bypass is the use of cellular phones. The wireless technology 802.11b also holds great promise in delivering broadband data (up to 11 Mbps).

Access

Access refers to how a user accesses the telephone network. For most users, access is gained to the network via a telephone handset. Transmission and reception occurs via diaphragms where the mouthpiece converts the air pressure of voice into an analog electromagnetic wave for transmission to the switch. The earpiece performs this process in reverse. The most sophisticated aspect of the handset is its *Dual-Tone Multifrequency* (DTMF) function, which signals the switch by tones. The handset is usually connected to the central office (where the switch is located) via copper wire known as *twisted pair*, because, in most cases, it consists of a twisted pair of copper wire. The stretch of copper wire connects the telephone handset to the central office. Everything that runs between the subscriber and the central office is known as the *outside plant*. Telephone equipment at the subscriber end is called *customer premise equipment* (CPE). One of the chief reasons the majority of subscribers have no choice in local service providers is the prohibitive expense of deploying any alternative to the copper wire that now connects them to the network. Secondly, gaining right-of-way across properties to reach subscribers borders on the impossible both in legal and economic terms.

Switching

The PSTN is a star network; that is, every subscriber is connected to another via at least one, if not many, hubs known as *offices*. Those offices contain switches. Very simply, local offices are used for local service connections and tandem offices are used for long-distance service. Local offices, better known as *central offices*, use Class 5 switches and tandem offices use Class 4 switches. Figure 1-2 details the relationship between Class 4 and Class 5 switches. A large city might have several central offices. Denver (population 2 million), for example, has approximately 40 central offices. Central offices in a

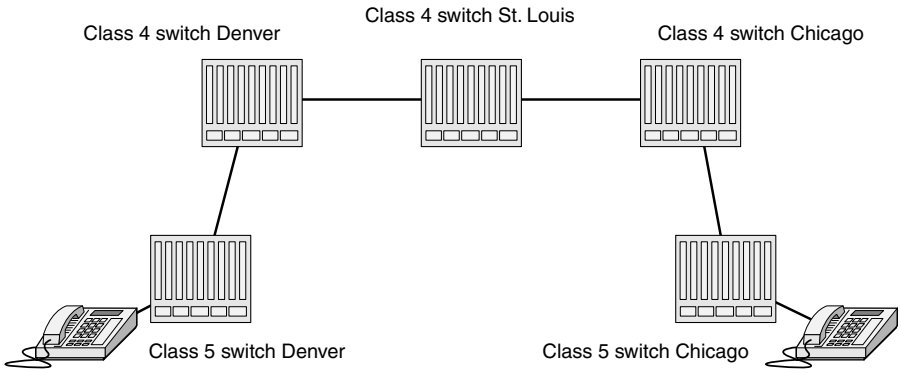

Figure 1-2 The relationship between Class 4 and Class 5 switches.

large city often take up much of a city block and are recognizable as large brick buildings with no windows.

Transport

The PSTN was built at great expense over the course of more than a century. Developers have been obsessed over the years with getting the maximum number of conversations transported at the least cost in infrastructure possible. Imagine an early telephone circuit running from New York to Los Angeles. The copper wire, repeaters, and other mechanisms involved in transporting a conversation this distance were immense for the time. Hence, the early telephone engineers and scientists had to find ways to get the maximum number of conversations transported over this network. Through much research, different means were developed to achieve the maximum efficiency from the copper wire infrastructure. Many of those discoveries translated on technologies that worked equally well when fiber-optic cable came into the market. The primary form of transport in the PSTN has been *time-division multiplexing* (TDM). In the 1990s, long-distance service providers (*interexchange carriers* [IXCs]) and local service providers (*Local Exchange Carriers* [LECs]) migrated those transport networks to *Asynchronous Transfer Mode* (ATM). ATM is a means of transport from switch to switch. The emergence of *Internet Protocol* (IP) backbones is drawing much of the traffic off ATM networks and moving it to IP networks.

Replacing the PSTN One Component at a Time

The three components of the PSTN are being replaced in the free market via substitution by other technologies and changes in the regulatory atmosphere. The *Memorandum of Final Judgement* (MFJ) of 1984 opened the transport aspect of the PSTN to competition. This gave rise to an explosion in the number of long-distance service providers in the United States. The bandwidth glut of 2000 has driven down the cost of long-distance transport.

The Telecommunications Act of 1996 was intended to further the reforms brought on by the MFJ of 1984, but it has failed to do so. The act specified how incumbent telephone companies were to open their switches to competitors. The incumbents stalled this access first by legal maneuvering and then by outright sabotage. The same tactics were employed in blocking competitive access to the access side of their networks. A technology known as *softswitch* offers a technology bypass of the PSTN switches. This still leaves the *last mile* (also known as the *first mile*) under the control of the incumbent service providers.

A new technology known as 802.11b and its associated variants offer the possibility for service providers to bypass the incumbents' local loop to deliver service to the last mile. The applications for 802.11b began with enterprise and government networks and have migrated to home networks. In the year prior to this writing, the industry experienced an explosion in the sales of wireless network products. As this technology becomes more popular, subscribers will gain confidence in wireless technologies and their related services, and will increasingly "cut the wire" to incumbent wired service providers.

This book provides a roadmap for cutting those wires. It provides an introduction to 802.11b and its related protocols (802.16, 802.11a, 802.11g, 802.11i, and so on). It offers extensive evidence of the myriad applications of 802.11b currently in operation with guidelines for implementing 802.11b. A series of case studies offer evidence of the viability of 802.11b and related wireless technologies.

802.11 Works—An Overview of the Installation and Operation of Wireless Networks

The evidence of successful deployments of wireless networks for both data and voice applications raises questions as to whether this technology could be deployed as an alternative to the PSTN. If it carries data and voice competently, why should a business or residence continue to subscribe to expensive (and often monopolistic) wireline services? The emergence of *voice over Internet Protocol* (VoIP) and its associated infrastructure technologies (for example, softswitch) reduces the transmission of voice to the simple routing and transportation of data packets. Hence, it is no longer necessary for a subscriber to contract with a telephone company for local or long-distance voice services.

Despite the popularity of the Internet and its myriad services, incumbent service providers, telephone companies, and cable TV companies have failed to offer a ubiquitous broadband Internet service. If broadband Internet access were as ubiquitous as telephone service was at the time of this writing, the American economy, for example, would reap a $500 billion annual benefit.[1] This book explores wireless architectures that will potentially compete with the PSTN for the delivery of voice and data services.

Objections to Wireless Networks

The position that wireless technologies will replace the PSTN is met with a number of objections. Primarily, these objections are focused on *quality of service* (QoS) issues, the security of the wireless

[1]Robert Crandall and Charles Jackson, "The $500 Billion Opportunity: The Potential Economic Benefit of Widespread Diffusion of Broadband Internet Access," *Criterion Economics* (July 2001): 69.

network, limitations in the range of the delivery of the service, and the availability of bandwidth. This book overcomes these objections.

Quality of Service (QoS)

One of the primary concerns about wireless data delivery is that, like the Internet over wired services, QoS is inadequate. Contention with other wireless services, lost packets, and atmospheric interference are recurring problems for 802.11b and its associated wireless protocols as alternatives to the PSTN. QoS is also related to the ability of a *wireless Internet service provider* (WISP) to accommodate voice on its network. The PSTN cannot be replaced until an alternative, competent replacement for voice over copper wire is available (see Figure 1-3).

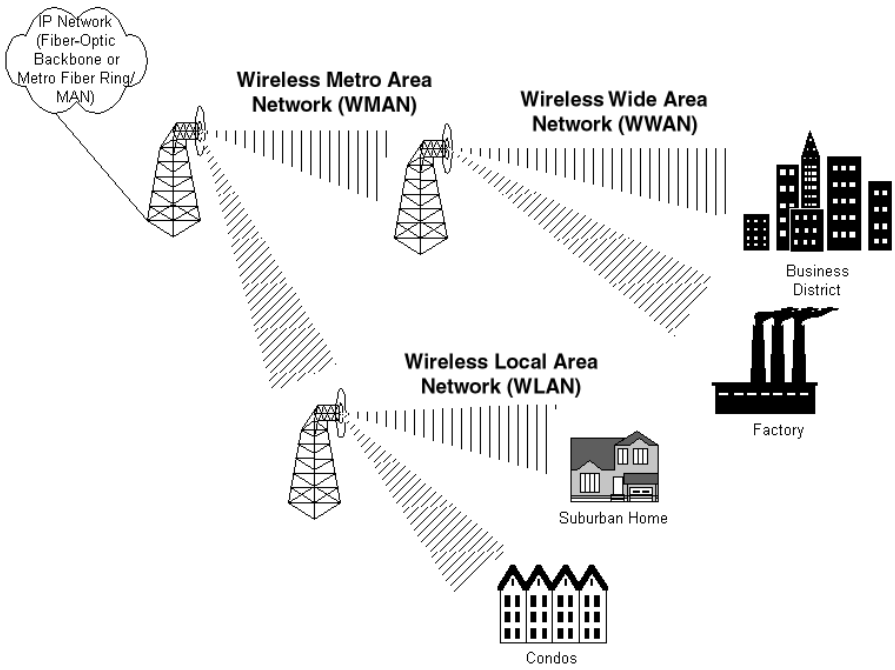

Figure 1-3
An overview of a broadband wireless alternative to the PSTN

Security

The press has been quick to report on weaknesses found in wireless networks. 802.11b has two built-in basic network security mechanisms: the *service set identifier* (SSID) and *Wireless Equivalency Privacy* (WEP). These measures may be adequate for residences and small businesses, but they are inadequate for entities that require stronger security. A number of measures that will provide the necessary level of security for the subscriber can be added to those wireless networks. This book provides suggestions for deploying industrial-grade security.

Range

In most applications, 802.11b offers a range of about 100 meters. So how, you might ask, will that technology offer the range to compete with the PSTN? Range is a function of antenna design and power, but mostly antenna design. With the right antenna, the range of 802.11 is extended to tens of miles.

The Economic Advantage of 802.11

Every *information technology* (IT) manager and manager of any alternative service provider must carefully weigh both the *return on investment* (ROI) and the *net present value* (NPV) of a new technology when deciding on investing in new platforms. Is a wireless network less expensive to purchase and operate than a wired network? What about the convergence of voice and data on one network? What about apparent intangibles such as worker productivity on wired versus wireless networks? This book offers practical examples of ROI and NPV problems to help solve these dilemmas.

For service providers, wireless technologies pose a potential cost-effective solution in that they do not require right-of-way across private or public property to deliver service to the customer. Many businesses cannot receive broadband data services as no fiber-optic cable runs to their building(s). The cost of securing permission to dig

a trench through another property and running the requisite cable is prohibitive. With 802.11b and its associated technologies, it is possible to merely beam the data flow to that building. This solution carries over to the *small office/home office* (SOHO) market in that the data flow can be beamed to homes and small businesses in places where no fiber-optic or other high-bandwidth service exists.

The Regulatory Aspects of Wireless Networks

What are the regulatory concerns for a WISP when deploying a wireless enterprise network? The FCC addresses wireless services in what is popularly known as *Part 15*. Wireless data requires spectrum on which to transmit over the airwaves at a given frequency. 802.11 and most of its associated protocols operate on what is known as *unlicensed spectrum*. Unlicensed spectrum does not require the operator to obtain an exclusive license to transmit on a given frequency in a given region. Unlike the operators of radio stations or cellular telephone companies, a WISP, public or private, is transmitting for free. Assuming WISPs ultimately compete with cell phone companies for subscribers, a WISP that utilizes 802.11 technologies may find itself at a strong advantage over *third-generation* (3G) networks. 802.11 delivers wireless data up to 11 Mbps on cost-free unlicensed spectrum, whereas 3G delivers bandwidth at approximately 128 Kbps over very expensive licensed spectrum. Will the unlicensed spectrum remain free of charge? How should conflicts on the airwaves be settled? How is the public best served in the commons of the frequency spectrum?

Improved Quality of Life with Wireless Networks

When deployed as a broadband IP network solution, 802.11b will enable an improved standard of living in the form of telecommuting,

lower real-estate prices, and improved quality of life. A wave of opportunity for wireless applications is in the making. Most of it lies in the form of broadband deployment. The potential for better living through telecommunications lies largely with the ubiquitous availability of broadband.

Only approximately 9 percent of American households have access to broadband Internet. Incumbent service providers have failed to expand that figure given the cost of their wired infrastructure and right-of-way legal barriers. Given the relative low cost of delivering wireless data to a business or residence, 802.11b technologies offer a very convenient alternative to conventional technologies in deploying broadband Internet to businesses and residences around the world.

Disruptive Technology

In the business book *The Innovator's Dilemma* (2000), Clayton Christensen describes how disruptive technologies have precipitated the failure of leading products as well as their associated and well-managed firms. Christensen defines criteria to identify disruptive technologies regardless of their market. Such technologies have the potential to replace mainstream technologies as well as their associated products and principal vendors. Disruptive technologies, abstractly defined by Christensen, are "typically cheaper, simpler, smaller, and, frequently, more convenient" than their mainstream counterparts.

Wireless technology, compared to incumbent wired networks, is a disruptive technology. For the competitive service provider, 802.11b is "cheaper, simpler, smaller, and, frequently, more convenient" than copper wire and its associated infrastructure. In order for a technology to be truly disruptive, it must disrupt an incumbent vendor or service provider. Some entity must go out of business before a technology can be considered disruptive. Although it is too early to point out the incumbent service providers driven out of business by 802.11b, its technologies could be potentially disruptive to incumbent telephone companies. The migration of wireline telephone traffic from ILEC to cellular is a powerful example of this trend.

Conclusion

This book describes how wireless technologies meet or exceed the performance parameters of wired last-mile networks and pose a potentially disruptive scenario for telephone service providers. In a market economy, it is inevitable that if competition cannot come in the local loop, it will surely come to the local loop. Given that wireless technologies could potentially match the last mile in terms of QoS, security, range, bandwidth, and economics, 802.11b provides the crucial avenue for competitive service providers to enter telecommunications markets worldwide. Delivering broadband Internet to homes and small businesses has many societal benefits. As a result of the sloth of incumbent service providers in deploying broadband Internet access to the last mile, wireless applications present what is probably the fastest avenue in delivering a huge economic surplus to society.

Why did 802.11b come before 802.11a? The â€˜aâ€™ amendment to the standard was released at the same time as 802.11b. But it introduced a more complex technique, known as OFDM (orthogonal frequency division multiplexing) for generating the wireless signal. In other words, 802.11a offered a few advantages over 802.11b: It operated in the less crowded 5 GHz frequency band, making it less prone to interference. Its bandwidth was much higher than 802.11b, with a theoretical max of 54 Mbps. You probably havenâ€™t encountered many 802.11a devices or routers. This is because 802.11b devices were cheaper and PDF | 802.11b networks can not be relied upon as part of the critical infrastructure of organisational networks. Recently released tools and exploits | Find, read and cite all the research you need on ResearchGate.Â 802.11b wireless card. When the build requirements were met the driver was installed on the machine. Linux uses. configuration files in /etc/pcmcia to control PCMCIA devices, how they are recognised and, which drivers to load for these devices. The pcmcia.config and hermes.conf files had to be. altered so that the newly built driver would be loaded instead of the standard driver for the. network card. Restarting the card-services in Linux with the networking card inserted showed. IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands. They are the world's most widely used wireless computer networking standards, used in most home and office networks to allow laptops, printers, and