INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Wireless and Mobile Device Security

SECOND EDITION

Jim Doherty

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Wireless and Mobile Device Security

SECOND EDITION

Jim Doherty

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
5 Wall Street
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Wireless and Mobile Device Security, 2nd Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious, but are used for instructional purposes only.

Production Credits
Director of Product Management: Laura Pagluica
Product Manager: Edward Hinman
Content Strategist: Melissa Duffy
Content Coordinator: Paula-Yuan Gregory
Manager, Project Management: Jessica deMartin
Project Specialist: Allie Koo
Senior Digital Project Specialist: Angela Dooley
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Michael Sullivan
Product Fulfillment Manager: Wendy Kilborn
Composition: S4Carlisle Publishing Services
Project Management: S4Carlisle Publishing Services
Cover Design: Briana Yates
Text Design: Briana Yates
Media Development Editor: Faith Brosnan
Rights Specialist: James Fortney
Cover Image (Title Page, Part Opener, Chapter Opener): © Cherezoff/Shutterstock
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data
Names: Doherty, Jim, 1968- author.
Title: Wireless and mobile device security / Jim Doherty, Professor, University of the Cumberlands Williamsburg, KY.
Description: Second edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2022] | Series: Issa | Includes bibliographical references and index.
Identifiers: LCCN 2020043841 | ISBN 9781284211726 (paperback)
Subjects: LCSH: Wireless communication systems--Security measures. | Mobile communication systems--Security measures. | Wireless LANs--Security measures. | Mobile computing--Security measures.
Classification: LCC TK5105.78 .D64 2022 | DDC 005.8--dc23
LC record available at https://lccn.loc.gov/2020043841

6048

Printed in the United States of America
25 24 23 22 21 10 9 8 7 6 5 4 3 2 1

To Katie, Samantha, and Conor

Contents

© Cherezoff/Shutterstock

Preface

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (www.jblearning.com). Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information security principles packed with real-world applications and examples. Authored by professionals experienced in information systems security, they deliver comprehensive information on all aspects of the topic. Reviewed word for word by leading technical experts in the field, these books are not just current but forward-thinking—putting you in the position to solve current cybersecurity challenges and future ones, as well.

Part I of the text reviews the history of wireless and mobile networks and the evolution of wired and wireless networking—from Alexander Graham Bell to the present bring-your-own-device (BYOD) phenomenon. You'll read about the mobile revolution that took users from clunky analog phones to "smart" devices people can't live without and about the implications of the always on, ever-present aspect of these devices. Although most people view the resulting changes as a net positive, both wireless and mobile networking have introduced significant security vulnerabilities to networking in general. You'll get an overview of network security threats and considerations, with a particular emphasis on wireless and mobile devices.

Part II focuses on wireless local area network (WLAN) security. You'll read about WLAN design and the operation and behavior of wireless in general, particularly on 802.11 WLANs. You'll review the threats and vulnerabilities directly associated with 802.11 wireless networks, their various topologies, and devices. The text will discuss basic security measures that satisfy the needs of small office/home office (SOHO) networks, as well as more advanced concepts in wireless security unique to the needs of larger organizations. You'll learn about the need to audit and monitor a WLAN and the tools available for doing so. Finally, you'll review risk assessment procedures as applied to WLAN and Internet Protocol mobility.

Part III discusses security solutions to the risks and vulnerabilities of wireless networks and mobile devices. You'll read about the three major mobile operating systems and the vulnerabilities of each. Then you'll review the security models of these operating systems and explore how IT organizations manage the security and control of smart devices on a large scale. The text will look at the risks mobile clients present to corporate networks, as well as the tools and techniques used to mitigate these risks. You'll also learn about the

© Cherezoff/Shutterstock

issues surrounding fingerprinting of mobile devices. Finally, you'll review the mobile malware landscape and mitigation strategies to prevent malware from finding its way into an organization's information security resources.

Learning Features

The writing style of this book is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with notes, tips, FYIs, warnings, and sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter assessments appear at the end of each chapter with solutions provided in the back of the book. Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a 2-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

Cloud Labs

This text is accompanied by Cybersecurity Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this textbook. For more information or to purchase the labs, visit go.jblearning.com/doherty2e

New to this Edition

Quite a lot has changed in the 5 years between the 1st and 2nd edition. We've dedicated an entire chapter to the "Always On, Ever Present" phenomenon and put a significant focus on the Internet of Things (IOT), which has resulted in both an explosion of devices on the wireless and mobile networks and in a secondary explosion of vulnerabilities. To make room for these new topics the two chapters dedicated to the evolution of data and mobile networks have been consolidated into a single chapter.

Additionally, this second edition includes the latest Wi-Fi standards (renamed since the original version of this text) and updated version descriptions for both the Android OS and Apple iOS. We've dropped all but passing mentions of the Windows phone operating system and have added up-to-date information on 5G. Finally, we've revised this version to include the latest wireless and mobile security vulnerabilities and remediations. As with any book on network and mobile security, we do our best to keep up with this never-ending game of cat and mouse.

Acknowledgments

I may be the fortunate one with my name on the cover, but there are several people who were instrumental in the creation of this book. Without them I would not have been able to take on, much less finish, this project.

- First and foremost on this list is Alasdair Gilchrist, my researcher, writing assistant, and technical bodyguard. His knowledge skill, effort, and technical expertise were indispensable in all aspects of creating both the manuscript for this book and the associated labs. One of the best things about all of this new technology is its ability to connect people from across the world. In this case, two guys who never met in person—one in North Carolina and one in Bangkok—were able to collaborate while both going about work and life using many of the tools and technologies discussed in this book (in a very secure way, of course). Alasdair is a true professional, and I'm very fortunate to have him on my team.
- Justin Hensley, my technical reviewer/editor and the director of Information Security and Infrastructure at the University of Cumberlands. Justin kept us sharp and did his level best not only to ensure the information in this book was accurate but also that it was accessible to the reader. This book is better and more readable than it would have otherwise been without his keen eye.
- My content strategist Melissa Duffy kept this project moving with unwavering attention and good cheer. Through multiple revisions, technical and editorial reviews, and a couple of nearly missed deadlines, Melissa competently moved the project forward. Writing a book is easy in comparison to getting a book published. Melissa did the heavy lifting.
- The production team at JB Learning included production specialist Allie Koo; media development editor Faith Brosnan; rights specialist James Fortney; and project manager (as S4Carlisle) Manjusha Chandrasekaran who had to fix all my grammatical, punctuation, and formatting errors—no small task! Thanks to this entire team and to all the many others who provided production assistance.

Thank you all. I am truly grateful.
Jim Doherty

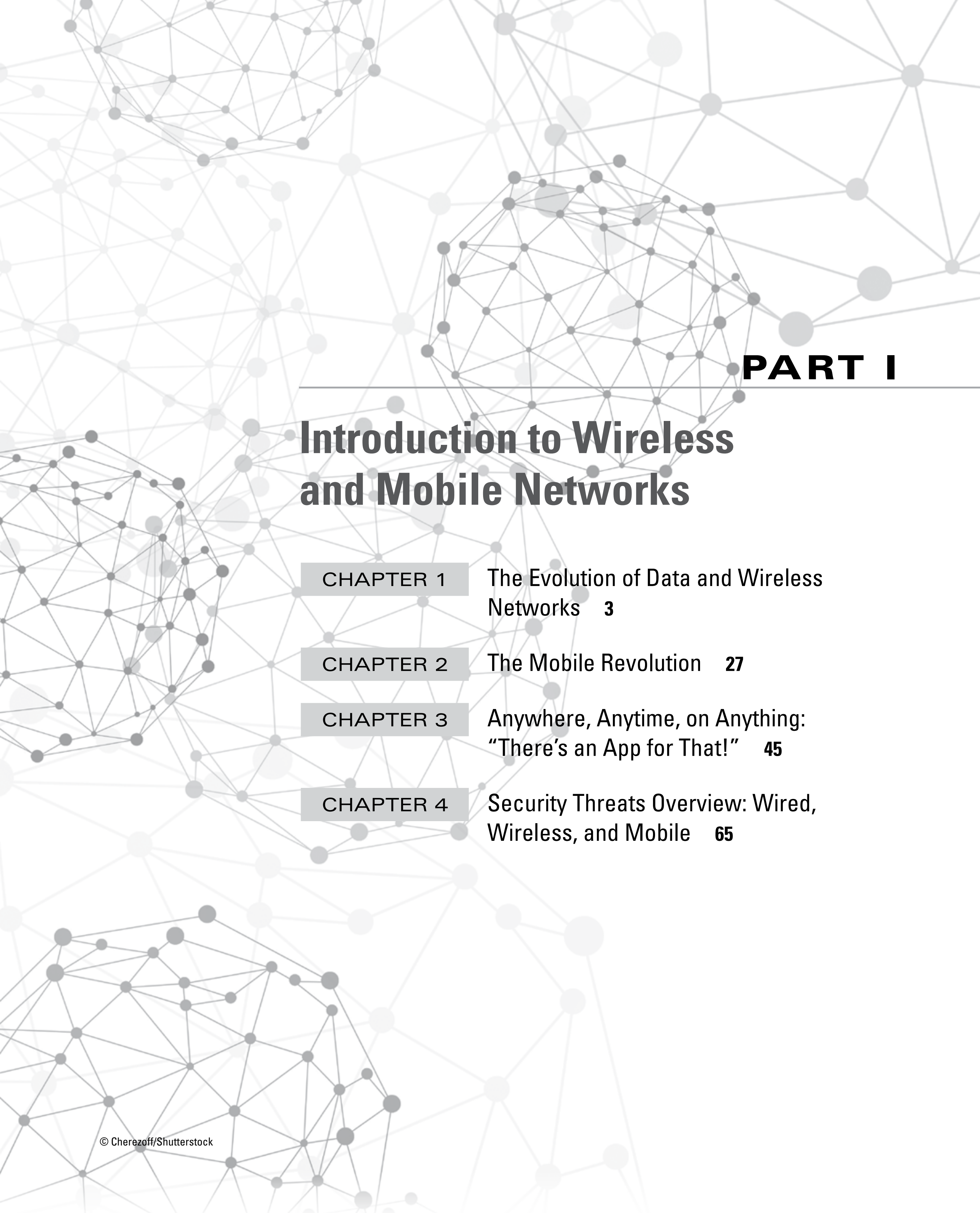
© Cherezoff/Shutterstock

About the Author

Jim Doherty, has more than 20 years of engineering, marketing, and sales experience across a broad range of networking, security, and technology companies. Focusing on technology strategy, product positioning, and marketing execution, he has held leadership positions for CommScope, Cisco Systems, Certes Networks, Ixia, and Ericsson Mobile.

Doherty is also the coauthor of the Networking Simplified series of books, which includes *Cisco Networking Simplified*, *Home Networking Simplified*, and several other titles. He is a former U.S. Marine Corps sergeant and holds a bachelor's degree in electrical engineering from North Carolina State University and a Master of Business Administration degree from Duke University.

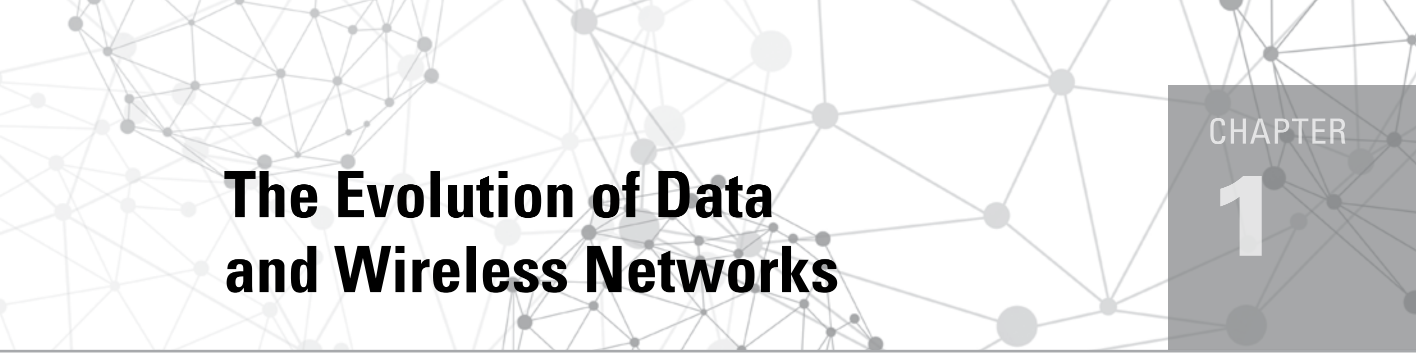
© Cherezoff/Shutterstock



PART I

Introduction to Wireless and Mobile Networks

© Cherezoff/Shutterstock



CHAPTER 1

The Evolution of Data and Wireless Networks

IN THE SPACE OF JUST 25 YEARS, network security, which had already gone through several evolutions, has once again been turned on its head due to the confluence of two phenomena: the untethering of network connectivity and the proliferation of devices that are always on, always connected, and often moving. The ability to log on to both the Internet and corporate networks without having to physically connect a computer to the network via an Ethernet cable has radically altered the culture and has greatly blurred the line between work life and personal life. Further, the willingness (or obsessive need, perhaps) to be connected to all things directly (via computers and smartphones) or indirectly (via smart devices) has redefined privacy and the security of personal data.

Although most people view the resulting changes as a net positive, both wireless and mobile networking have introduced significant security vulnerabilities to networking in general and company and personal information in particular. These vulnerabilities, along with prevention and detection methods, are the focus of this text. However, before jumping into the details of wireless and mobile network security, let's take a look at how these profound changes came about.

Chapter 1 Topics

This chapter covers the following concepts and topics:

- How early forms of data communication worked
- How computers went mobile
- How mobile and data networks converged
- What the origin, purpose, and function of the OSI Reference Model are
- What the origins of wireless technology are
- What the economic impact of wireless networking is
- How wireless networking has changed the way people work

© Cherezoff/Shutterstock

Chapter 1 Goals

When you complete this chapter, you will be able to:

- Describe the evolutionary history of networking
- Describe the function of the OSI Reference Model
- Understand and describe the functions of each layer in the OSI Reference Model
- Describe IP addressing and the key differences between IPv4 and IPv6
- Describe MAC addresses and how they differ from IP addresses
- Provide examples of how wireless networking is used in health care, warehousing, and retail

The Dawn of Data Communication

Data communication and networking have a long history going back to 1837, when Samuel Morse developed the first practical telegraph system. In 1844, Morse sent his first long-distance message, “What hath God wrought!” encoded in Morse code, from Washington, D.C. to Baltimore, Maryland. By 1850, more than 12,000 miles of telegraph lines traversed the country, run by more than 20 different commercial operators. **Telegraphy**, as it was known, used start and stop signals of dots and dashes transmitted over copper wires. It was a one-way message protocol that evolved to support two, and then four, channels. Telegraphy monopolized electronic communication until 1877, when the first telephone networks started to appear.

Despite reservations that telephones would be too technical for the common man, **telephony** was quickly adopted. Indeed, the telephone system quickly usurped telegraphy in terms of traffic carried, revenue generated, and network coverage. Telephony, however, was initially limited to voice. Therefore, despite telegraphy losing out to the telephone as the popular means for interpersonal communications, it remained an effective medium for carrying digital data traffic.

In 1923, the first teletypewriter services came into being, serving the need for true and accurate communications. By 1935, the introduction of rotary dial telex services emerged.

By the 1950s, the **public switched telephone network (PSTN)** had become ubiquitous and affordable, in large part due to broad interconnectivity, creating a network effect. The PSTN could interconnect telephones from anywhere in the community, the country, or even internationally over its network of exchanges. To accomplish this, a hierarchy of networks connected local exchange carriers (LECs) with regional, national, and international carriers via interexchange carriers (IXCs). It was this national and international reach that made the PSTN such an inviting medium when it became necessary to network large business computer mainframes.

NOTE

The **network effect** is a phenomenon in which a technology becomes more valuable as the number of users or units increases. A common example is the fax machine. The first fax machine was useless, but the second fax machine made the first one useful. As more were added, all fax machines had greater utility.

Early Data Networks

By the late 1950s, there was a demand to network the growing number of business computers being deployed by large companies. These computers were large standalone machines that operated independently. IBM accomplished the first successful interface between two digital devices over the analog PSTN using acoustic couplers and telephone sets. These couplers operated over the PSTN at 300 bits per second (bps). At this point, voice networks and the burgeoning data network began to merge.

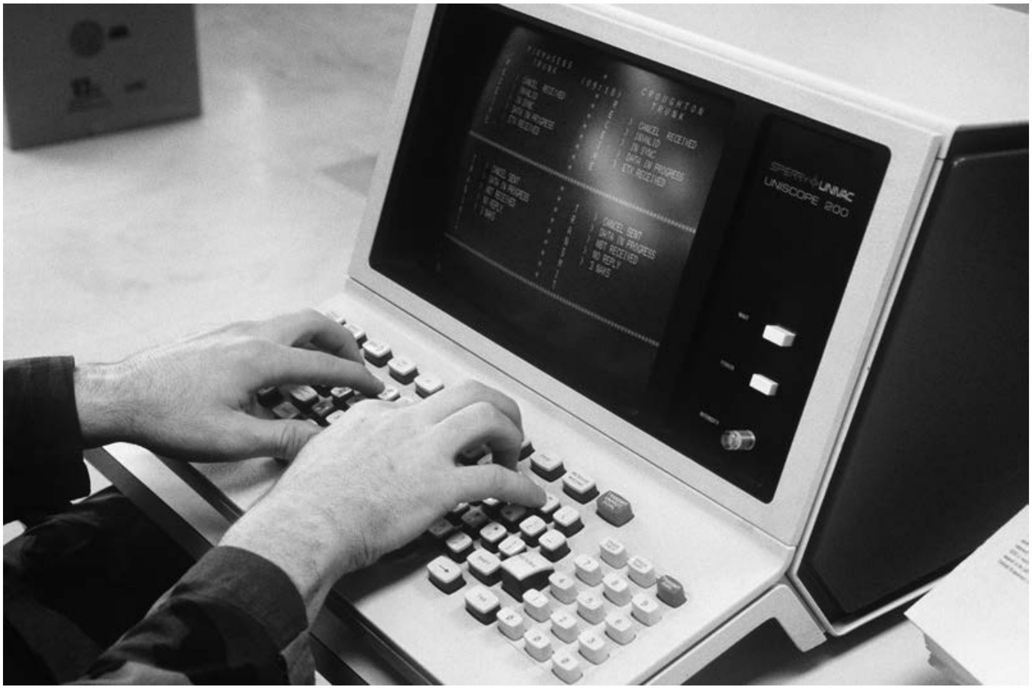
FYI

Until the appearance of the personal computer (PC), computers were huge mainframes that often occupied an entire room. Access to these computers was achieved through a "dumb terminal," which offered a simple text display (often called a *green screen* due to the green color of the font on the black screen), as shown in **FIGURE 1-1**. These displays had no computing power; rather, they were simple readout displays.

FIGURE 1-1

A dumb terminal or green screen.

Courtesy of U.S. Department of Defense.



Another significant point in the history of data communications was the transmission of the first fax over the standard PSTN in 1962. This was possible due to the modulation of data into sound by devices called *modems*, which were attached to either end of the analog telephone lines. A **modem**, short for modulator/demodulator, was required to transfer digital communications over the analog PSTN for the several decades that followed. Modems convert digital data into an analog signal for transport over the wire. At the other end, the analog signal is demodulated to recover the original digital signal. By using modems, computers that had access to a telephone line could communicate over the analog PSTN.

Soon, however, telephone companies saw the obvious benefits of digital technology and began upgrading their networks. Digital communication was accepted as technically superior to analog. Furthermore, digital technology had become both cheaper and more reliable, which made it suitable for transmitting voice communications.

Digital communications have the following advantages over analog:

- More efficient use of bandwidth
- Greater utilization
- Improved error rates (that is, fewer errors)
- Less susceptibility to noise and interference
- Increased throughput
- Support for additional services (such as caller ID, auto-forwarding, and call waiting)

As telecom providers rolled out new digital networks, high-speed digital communication became a widely available service.

The innovation that enabled the technological leap in long-distance digital communication was **packet switching**, used in lieu of **circuit switching**. In circuit switching, a physical connection was made between two phones using a series of telephony switches, creating an electric circuit. While the circuit was in use, no other phones could use the wires connecting the two phones. This was very inefficient because conversations—even among chatty people—are in fact about 50 percent silence when you account for the pauses between words and between speakers. It was also very expensive, especially on long-distance calls, because the callers had to “rent” the exclusive use of a circuit that was almost always in demand.

There were also concerns with circuit switching regarding the resilience of the message path. Circuit switching restricted communications to a preprovisioned point-to-point circuit for the duration of the call. Should any intermediary exchange along the message path fail, the circuit was lost and had to be reprovisioned. Ideally, the call would be automatically rerouted over a different path. However, that required multiple paths to any given destination and an awareness of alternative routes to the destination, which greatly increased the user cost.

In packet switching, the voice signal is first digitized and then chopped up into a series of packets. These packets contain the voice information along with the source and destination. The packets are then forwarded from the source to the destination. Taking advantage of the silent gaps, packets from multiple conversations can share the same circuit, making packet switching much more efficient. Additional efficiencies were created through the development of digital compression techniques so that many of today’s conversations exist on the same wires.

Packet switching is also much more resilient to circuit switching. Packets can take multiple paths from source to destination, so there is no dependence on a single circuit. Also, because each single packet is such a small fragment of the speech signal, many packets can be lost or dropped without noticeably affecting the quality of the call. With packet switching, if any one circuit or exchange fails, the packets are rerouted. Any dropped packets are simply ignored. As it turned out, packet switching was also key to modern data communication.

Not surprisingly, the military was very much involved in developing packet switching. Its interests lay in the possibilities of high-speed failover and resilient data communications under battlefield conditions.

The Internet Revolution

This interest led to the U.S. government's creation of the Advanced Research Projects Agency (ARPA) to research and develop computer networks. The results of the ARPA project were the design, creation, and development of the ARPANET, the first computer network based on packet switching.

The ARPANET project was the predecessor of the modern Internet. However, during the 1970s and 1980s, it was a noncommercial network developed and used by universities and research institutions. During this period, despite being little known and seldom used, the ARPANET project developed several key protocols—one of the most important being the **Transmission Control Protocol/Internet Protocol (TCP/IP)**. TCP/IP would become the protocol of the Internet in the early 1990s.

During that same period, many **local area network (LAN)** technologies vied for supremacy. Several proprietary networking protocols were prevalent and vied for market dominance. The problem was that the proprietary protocols were not compatible. That is, LANs using different protocols could not be connected to each other. The challenge was to connect all these different operating systems and protocols into one heterogeneous network. By the early 1990s, a clear winner had emerged in the LAN technology war: the Ethernet protocol. It became the ubiquitous LAN network standard protocol across the globe. Thirty years later, Ethernet is still the dominant LAN protocol.

APRA was more than LANs

ARPA also went on to create what would become the standard methods of connecting business computers and networks over long distances. These wide area networks (WANs), as they are known, were point-to-point or point-to-multipoint topologies, which enabled companies to connect networks and computers in cities and countries across the globe at high speeds and high throughput.

Advances in Personal Computers

Digital communications were not the only technology growing by leaps and bounds. Within businesses themselves, a revolution was occurring that spelled the end of the road for the huge mainframes and their dumb terminals.

The IBM PC was launched in the early 1980s. It immediately caught the attention of businesses and became popular for running standalone word processing and accounting packages. But because most of the business data resided on the mainframe, both a PC and a mainframe terminal (the "dumb" screen connected to the mainframe) were required on the desktop. Not only was that inconvenient but there was also no easy way to transfer information from the mainframe to the PC applications for local processing. The solution was to connect each PC to the mainframe by networking them over a LAN and harnessing the growing processing power of PCs by just connecting them directly to each other over the LAN. This made the dumb terminal redundant as PC sales skyrocketed and the computer networking industry exploded. Up to this point, however, if you wanted to connect a device to a network or to the Internet, you had to physically connect the device via an Ethernet connection or via a modem connected to the PSTN. However, all of this was about to change with the advent of wireless networking.

Networking and the Open Systems Interconnection Reference Model

Before examining how wired networks evolved into wireless networks, it's important to have a fundamental grasp of basic networking. The logical place to start is the **Open Systems Interconnection (OSI) Reference Model**. Initially proposed in 1984, the OSI Reference Model was the industry's response to the issues created by proprietary data networking and equipment development at the dawn of the networking era. Before this, most equipment manufacturers had developed their own proprietary methods for data networking. These included unique communication protocols, connection interfaces, and procedures for data storage and retrieval, to name a few. In some cases, vendors did this because much of the development in this area was new. But many insisted on going their own way in an attempt to gain a competitive advantage.

This may have seemed like a good idea for the companies breaking into this newly developing market. But it was bad for customers because it locked them into a single vendor solution. Concerns over the limited scope of solutions and clients' natural hesitance to remain locked into a single vendor ultimately stalled the market. This, of course, was not only bad for customers, but it was also bad for vendors because it put an artificial limitation on opportunities.

The answer was to develop a model that defined standards for communication protocols as well as for the physical and logical interfaces between machines and subsystems.

FYI

In many cases, the term *stack* is used in reference to a particular protocol, such as IP. However, you will often see cases in which the phrase "moving up or down the stack" refers to the OSI layers. For example, firewalls were originally Layer 3/4 (IP) devices; however, application firewall vendors are now said to have gone "up the stack" to Layer 7. In cases such as this, the context of how and where the term is used helps identify which meaning of the term applies.

Published by the International Organization for Standardization, the OSI Reference Model defines seven layers (referred to as a **stack**) that describe standards from the physical wire all the way up to the application interfaces on computers. Further, the standard was written such that each layer has a specific function, common among all devices, and a specific way of communicating with the layer above and the layer below in the stack.

As a result of this standardization, different companies were able to specialize in specific solutions or products, confident that their products would be compatible with products from other manufacturers, even if there were no up-front collaboration. This led to a great deal of innovation. It also greatly improved the number of available solutions, because the barriers to entering the market were reduced. It's much easier to start a company based on a niche product than to create an entire end-to-end solution.

More importantly, the OSI Reference Model proved to be an enormous benefit to consumers—businesses, universities, and governments—who enjoyed greater choice and the opportunity to choose "best in breed" products rather than be forced to standardize around a single vendor for their entire network. Most economists and network historians agree that it was this willingness to adopt the OSI Reference Model that helped propel the networking industry into the economic power that it has become.

The Seven Layers of the OSI Reference Model

As noted, the OSI Reference Model has seven layers, each with a specific function and a standard way of communicating with the adjacent layers. From the bottom up, the layers are as follows:

- **Layer 1 (Physical Layer)**—The **Physical Layer** is the signal path over which data is transmitted. This can include copper wires; optical fibers; radio signals such as **Wi-Fi, Worldwide Interoperability for Microwave Access (WiMAX)**, and **Bluetooth**; and any other transmission path. The units of information at this layer are bits or bytes.
- **Layer 2 (Data Link Layer)**—The **Data Link Layer** helps establish the communication path by specifying the **Media Access Control (MAC) address** of each device. Layer 2 is viewed as the "switching" layer because it is the layer where switching paths are determined in LANs. Ethernet is a Layer 2 protocol. The unit of information at Layer 2 is the data frame.
- **Layer 3 (Network Layer)**—The **Network Layer** is typically viewed as the routing or IP layer, although over the years, the line between routing and switching has blurred. This layer handles communication paths between LANs. The IP exists at Layer 3. As such, communication paths are defined in terms of their IP addresses. The unit of information at Layer 3 is the packet.
- **Layer 4 (Transport Layer)**—Known as the **Transport Layer**, Layer 4 is the bridge between the network and the application-processing software on devices. This is where data from applications is broken down into small chunks, or packets, that are suitable for transport from the sending device, and then reassembled on the receiving device.
- **Layer 5 (Session Layer)**—The **Session Layer** defines and manages communications between applications on separate devices.
- **Layer 6 (Presentation Layer)**—Known as the **Presentation Layer**, Layer 6 formats information sent to and from applications.

NOTE

An easy way to remember the layer names in order is to use a mnemonic. There are dozens of them, ranging from funny, to topical, to outrageous. A good top-to-bottom one that is suitable in the workplace is *All People Seem To Need Data Processing*.

- **Layer 7 (Application Layer)**—At the top of the stack is the **Application Layer**, which provides appropriate protocols for Internet applications (e.g., HTTP, SMTP).

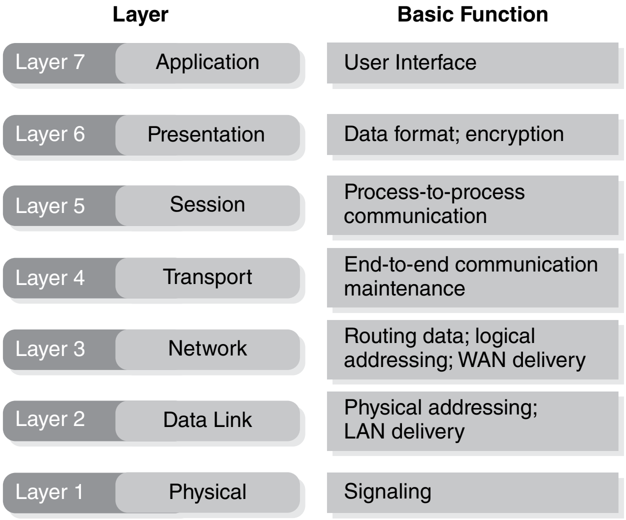
Inter-stack communication is accomplished through the use of headers. As data is created (at the Application Layer) and sent down the stack and across the network to another device, each layer adds its own set of instructions for the corresponding layer on the other machine and for the layer below or above the stack on the same machine.

Although the OSI Reference Model does provide a clear framework, the lines have begun to blur over the years. For example, many people will now reference a new condensed framework called the TCP Model, which lumps Layers 5 through 7 together, referring to them as the "Application Layers." In addition, Layer 3 and Layer 4 are closely associated due the use of TCP/IP, the de facto standard for communication over the Internet. Finally, as previously mentioned, the functional lines between switches and routers have been greatly blurred as innovation and processing power have continued to accelerate, allowing for greater efficiency in multitasking devices. As a result, Layer 2 and Layer 3 are no longer the sole domains of switching and routing, respectively.

An OSI layer can communicate only with the layers immediately above and below it on the stack and with its peer layer on another device. This process of passing instructions to the layer above or below must be used so that information (including data and stack instructions) can be passed down the stack, across the network, and back up the stack on the peer device. **FIGURE 1-2** shows the seven layers in relation to each other along with their basic functions.

FIGURE 1-2

The OSI Reference Model describes how devices communicate with each other over networks.



Layer		Basic Function
Layer 7	Application	User Interface
Layer 6	Presentation	Data format; encryption
Layer 5	Session	Process-to-process communication
Layer 4	Transport	End-to-end communication maintenance
Layer 3	Network	Routing data; logical addressing; WAN delivery
Layer 2	Data Link	Physical addressing; LAN delivery
Layer 1	Physical	Signaling

Communicating over a Network

While a detailed look at the fundamentals of data communication is beyond the scope of this text, a brief overview of a few key aspects of network communication is necessary. In particular, we will look at those aspects of networking that weigh heavily in understanding wireless security. At the simplest level, the two main keys to communication over a network are conditioning the data for transport and ensuring that the data reaches the correct destination.

In the context of this simplified definition, the role of the Application Layers is to condition data for transport over the network or to reassemble data for use by the application on the receiving end. While there are many security considerations at these layers, they are largely independent of the method of transport (either wired or wireless), and are beyond the scope of this text. With the advent of network-connected mobile devices, all known issues that exist in fixed settings become moving targets.

Communication at the Network Layer is achieved through a logical addressing scheme that enables routers to move packets across the network to the correct destination. (In this case, "logical" means that the addresses are assigned and can be changed if needed.) This addressing scheme, called *IP addressing*, allows for data communication between (switched) LANs via routed WANs.

IP Addressing

IP addressing enables a network to correctly route packets across a network. For most of the last 30 years, an IP addressing scheme called **Internet Protocol version 4 (IPv4)** was used. This scheme used a format called **dotted decimal**, which consists of four *octets* (groups of eight in binary code) that define the location of a source or destination LAN—much in the same way a home or business address includes the street number, street, town, state or province, zip code, and country. A typical IP address has the format 198.10.249.168, where one or more of the first octets defines the network segment and the remaining octets define the computers or devices (referred to as *hosts*) on that network. Again, using the analogy of a street address, you can think of the network as being like the street (for example, 5th St.) and the hosts as being like houses on that street (for example, 121 5th St., 122 5th St.). Each octet ranges from a minimum of 1 to a maximum of 255. The maximum number is 255 because it is the largest eight-digit binary number (11111111). Certain numbers, such as 0 and 255, are reserved for certain types of communication.

When IPv4 was first developed, it was thought to be sufficient enough to allow for future expansion. After all, the total number of combinations is more than 4 trillion—although, due to disallowed combinations, as noted, the actual number of usable addresses is in the billions. Even so, that seemed like a lot of addresses. But this was before the Internet exploded and every business office, nearly every home in the developed world, and every **smartphone** needed an IP address. As a result, address space quickly became scarce. Technologies such as **network address translation (NAT)**, a method to mask the address of devices on a network from the outside world, and **Dynamic Host Configuration Protocol (DHCP)**, used to automatically assign IP addresses to devices as needed, work to mitigate the address shortage but both proved to be only stopgap measures given the quick adoption of IP-enabled devices. The real answer to the problem was IPv6.

IPv6

Unlike IPv4, whose 32-bit addresses yielded about 4 billion usable addresses, **Internet Protocol version 6 (IPv6)**, a 128-bit address scheme, allows more than 3.5 undecillion addresses. That's a number with 38 zeroes after it. Given this very large number, it's a good bet that address space will no longer be an issue no matter how many network-connected smart **Internet of Things (IoT)** devices come along. There are also other benefits to IPv6, including the following:

- Auto-configuration
- Improved address management
- Built-in security/encryption capability
- Optimized routing

An IPv6 address contains eight fields of four-digit hexadecimal (base 16) numbers (0 to 9 and a to f) as follows:

    2051:0011:13A2:0000:0000:03b2:000a:19aa

The notation also allows for a shorthand method that eliminates leading zeroes, with an all-zero field represented by a single zero:

    2051:11:13a2:0:0:3b2:a:19aa

Further, successive fields of all zeroes can be shortened with a double colon (::) as follows:

    2051:11:13a2::3b2:a:19aa

The changeover to IPv6 has been discussed for many years. Initial predictions in the late 1990s suggested the conversion would need to occur around 2002. However, as of this writing, the changeover is not yet complete, despite an explosion in the use of devices that has far exceeded any predictions in the early part of the century. IPv4 remains in wide use because converting to IPv6 requires massive upgrades that will cost millions and perhaps billions of dollars and because, so far, the workarounds seem to work. The conversion does seem to be slowly taking shape, however, as most new devices are IPv6 enabled. The tipping point of the conversion will likely be when most networking devices have gone through the natural refresh process over a 7 to 10-year period and are replaced with devices that can accommodate the new addressing scheme.

Data Link Layer

Layer 2, the Data Link Layer, has been dominated by the Ethernet protocol for the better part of 30 years. Used primarily in LANs, Ethernet is how switches move data between machines. Over the years, Ethernet has been expanded. It is used in massive data centers and large metro area networks, furthering its hold on Layer 2 just as IP has dominated Layer 3.

The Dominance of Switching

Switches have always been a critical part of networks. Recently, however, switching has claimed a dominant position in networking. Why? One reason is that switch vendors have added functionality to switches, including features such as Power over Ethernet (PoE). This enabled Voice of Internet Protocol (VoIP) phones to work without an additional power cord (they still needed an Ethernet cable, of course), and gave them Layer 3 and even Layer 4 forwarding capabilities. Improved performance drove ever-increasing speeds, from 1 gigabit (Gb) to 10 Gb to 40 Gb and even 100 Gb and 400 Gb Ethernet. These improvements weighed heavily as dedicated data centers came into prominence in enterprise networks. They have greatly accelerated with the advent of virtualization, where fast switching within massive virtualized data centers is a primary design criterion.

Unlike IP, which was meant to connect LANs with each other, Ethernet connects data between machines that are all on the same network. As such, one of the key components of Ethernet deals with preventing data collisions that occur when multiple computers transmit data at the same time on the same segment of the network.

Much in the way that routers are associated with Layer 3, switches rule Layer 2. A switch connects different network segments together via switch ports, each of which can have multiple machines (or other switches in a hierarchical network). When a data frame (the Layer 2 version of a packet) arrives on a switch port, the switch looks up the source and destination MAC address (a unique identifier assigned by manufacturers to any network-connected device) and makes a forwarding decision based on the rule set associated with the destination MAC address.

Unlike IP addresses, MAC addresses are physically assigned to every individual device that can connect to a network by the manufacturer as it rolls off the factory assembly line. MAC addresses are intended to be both unique and permanent. However, it is possible to spoof a MAC address, which—not surprisingly—has significant security implications.

Physical Layer

At the bottom of the stack, the OSI Reference Model specifies standards for the medium over which data is transmitted. While not often discussed in the same way as Layer 2 or Layer 3, the standards specified at Layer 1 are quite complex. This text will emphasize their importance because **wireless local area network (WLAN)** communication standards are specified here.

Layer 1 defines how the actual bits are transmitted between devices, including specifications on the following:

- **Transmission**—Bit-by-bit procedures
- **Electrical**—Signal levels, amplification, and attenuation
- **Mechanical**—Specifications for cables (type, length) and connectors

- **Procedural**—Modulation schemes, synchronization, signaling, and multiplexing
- **Wireless transmissions**—Frequencies, signal strength, and bandwidth
- **Throughput**—Bit rates
- **Topologies**—Bus, ring, mesh, point-to-point, and point-to-multipoint

Protocols defined at Layer 1 include the following:

- Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH)
- Digital subscriber line (DSL)
- T1/E1
- Integrated Services for Digital Networks (ISDN)
- Ethernet Physical Layer
- Bluetooth
- 802.11 (WLAN)

From Wired to Wireless

The networking industry began to grow in the 1980s and exploded in the 1990s, with the culmination of affordable PCs and the growing popularity of the Internet and the World Wide Web. Already on an incredible trajectory in the late 1990s, the industry benefited from another boost in the form of wireless networking—and there was another even bigger boost to come.

This "second wave" of networking was initially made possible as a result of a groundbreaking decision by the U.S. regulatory body in charge of telecommunication rules, the **Federal Communications Commission (FCC)**—the opening of several bands (contiguous ranges of radio frequencies) of the radio spectrum for unlicensed use in 1985. This was a big change, given that apart from ham radio, which was valued as a nationwide emergency communication system, the radio spectrum was a tightly controlled government asset that required licensed approval for use. This visionary decision (not a phrase often associated with a government regulatory body) had a profound effect on networking as well as on several other industries.

The frequency bands in question—900 MHz, 2.4 GHz, and 5.8 GHz—had previously been reserved for things such as microwave ovens, among others. The FCC's decision allowed anyone to use these bands (or any company to build a product that used these bands) as long as they managed interference with other devices. This made products such as cordless phones and remote-controlled ceiling fans—and, later, wireless networks—possible.

At first glance, it's hard to see exactly why wireless had such a huge impact. At the time, wireless performance was not that great. In fact, compared to a hard-wired Ethernet connection, it was pretty lousy. As it turned out, though, users were far more interested in convenience than performance—at least initially. Before the advent of WLAN, if you wanted to connect to a network, you had to go to where the computer was tethered to an Ethernet port. Or, if you had a laptop (these were also becoming cheaper), you had to go to where the connection port was. This may not seem like a big deal, but "going to the computer" meant leaving where you were and dropping what you were doing.

Wireless networking changed all that. With WLAN, you brought your computer to where you wanted to be and connected to the network from there. The ability to connect in a meeting room or on your couch far outweighed the slower connection speed, especially since there were very few high-speed network applications at the time. (Streaming media meant waiting 5 or 10 minutes to download a single song, for example.) This convenience factor created a massive surge in WLAN usage. In response, manufacturers poured millions into research and development (R&D), which improved performance, which in turn attracted more users.

The first generation of WLAN operated at about 500 kilobits per second (Kbps) on an unlicensed frequency band. In this case, "unlicensed" meant that anyone could use it. It was not restricted or reserved for commercial or government use as long as the transmission power was kept low. The second-generation boosted performance to 2 megabits per second (Mbps), a 400-percent improvement. (Note that the term "generation" is used here in the generic sense rather than as a name, as it is when describing mobile network technology.)

In 1990, the IEEE established a working group to create a standard for WLANs. In 1997, the IEEE 802.11 standard was ratified, specifying the use of the 2.4 GHz band with data rates of up to 2 Gbps. Different versions of the 802.11 standard were developed in subsequent years and were noted via extensions such as a, b, g, and n. Notationally, this would appear as "802.11b," for example.

Outside the enterprise workplace, mobile data communication was becoming commonplace. The combination of affordable powerful laptop computers combined with the availability of affordable, easy-to-configure WLAN routers conditioned Internet users to expect wireless connectivity. This was reinforced when local hotspots sprang up in shopping malls, cafés, restaurants, bars, airports, and even sports stadiums. Home users rushed to buy WLAN access points and routers, as this enabled them to create a WLAN for all devices to connect throughout the household. The fact that one could easily build a WLAN that covered the entire home without having to run or hide cables was a huge selling point to a world that had begun to expect Internet access. Despite lower data rates as compared to wired access, people were willing to trade data rate for broader connectivity options.

In addition to performance issues, WLANs presented new security risks. It was perhaps not surprising then, that when WLAN vendors tried to push into enterprise markets, information technology (IT) security and network managers were less than excited at the prospect of using them. In fact, most were very much against it. The problem was, users were beginning to demand access from anywhere in the office, especially in conference rooms. When IT managers said they would not support wireless connections, many people simply connected their own WLAN routers to an Ethernet port in conference rooms and other locations creating their own rogue access points. This was a huge problem for IT, which rightly set harsh rules against it.

In the end, however, it was too much to fight. User demand simply overwhelmed IT departments' resolve. Consequently, after 2005, businesses gradually started to roll out WLANs in areas where temporary network connections were a convenience rather than a necessity. These areas—reception areas, meeting rooms, cafeterias, and recreational facilities—could be supplied by wireless access points. From a purely functional perspective, this proved to be an ideal use of the technology, as people using their portable devices in those areas would typically not require high throughput, anyway. Rather, they would more likely than not just be checking email or using an instant message application.

On the horizon, though, an even more disruptive technology was rolling in: 3G Mobile IP broadband. This new technology promised to have an even larger footprint—one that could truly be described as "ubiquitous mobile data access."

Business Challenges Addressed by Wireless Networking

Wireless networking addresses several challenges thanks to its inherent ability to allow network access without the hindrance of cables. The most obvious benefit is that areas considered for WLAN deployment do not require a cable run to each desk or print station. This offered major savings in time and effort. Moving cables and activating the Ethernet ports is a considerable burden in any installation, office move, or reshuffle. With WLAN being predominantly wireless, there is a greatly reduced burden on cabling devices because only the backhaul from the access point to the network may need to be cabled. As a result, you can put desks and network printers wherever you want. There is also significant cost savings, particularly in new installations where fewer Ethernet cables are being run to each desk or work space.

NOTE

A Wi-Fi device is generally any device based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. But the term is often used to describe any WLAN-capable device (most of which are 802.11 compatible). The terms Wi-Fi and WLAN are often used interchangeably. The IEEE develops global standards for a wide range of technologies. The 802 standard pertains to LANs and the ".11" extensions define standards for WLAN.

The Economic Impact of Wireless Networking

To understand how wireless became available almost everywhere, you must understand the desire for mobility. It is no longer acceptable to be located at a fixed network point of access. Nowadays, consumers demand the right to move around—to be mobile—so much so that for the average person, it's getting harder to find a networking device that will physically connect at all.

The first wave of the wireless revolution included early adopters who provided fixed-line PC-based Internet services at cafés and shopping malls. Their fee-based services, which were fraught with security issues—typically keyboard sniffers to capture passwords and banking details—soon succumbed to free public wireless broadband offerings.

Soon, it became common to have high-speed ADSL (asymmetric digital subscriber line) and broadband fixed-line networks in residential properties. To reduce churn, Internet service providers (ISPs) often supplied Wi-Fi–enabled gateways to consumers. *Churn* is the movement of a subscriber from one network to another and is one of the **key performance indicators (KPIs)** most relevant to overall performance. These measures helped Wi-Fi gain traction in homes and small businesses, but they alone cannot account for the fact that in 2005, wireless broadband accounted for productivity gains of $28 billion and the trend has continued.

Wireless Networking and the Way People Work

It's somewhat difficult to separate the business impact of Wi-Fi from its economic impact because they are intrinsically tied together. However, this section will focus on one key point: the way in which wireless has changed how companies work. As previously mentioned, wireless networking has changed how people work in the office—particularly **knowledge workers** (that is, professionals whose jobs involve the use and manipulation of data). These were the first wave of employees to use computers and, later, laptops. These workers found it very useful to be able to connect to the network from anywhere in the office, such as meeting rooms, particularly given the collaborative nature of their work.

This was an important change, of course. But there were some industries for which wireless fundamentally changed the way they did business. A few of them are discussed here.

Health Care

One of the first industries to adopt wireless technology was health care, and it has profoundly changed how hospitals work and how doctors and nurses interact with patients. In 2005, productivity improvements from the use of mobile wireless broadband solutions across the U.S. health care industry were valued at almost $6.9 billion. Today, wireless technology productivity is almost impossible to carve out because it's woven into the very fabric of modern health care.

Health care is one of the most labor-intensive industries, as well as one of the most sensitive to keeping personal data private. Nonetheless, health care has managed to use wireless technology to improve communication, as well as provide instant access to information portals for diagnosis and general health information such as diets and lifestyle plans. However, these improvements in efficiency alone don't explain the savings in health care. Over $1 billion of inventory loss avoidance is achieved through the use of wireless tagging or radio-frequency identification (RFID).

One of the obvious improvements that wireless brings to the health care industry is that it allows modern medical devices and monitors to be moved with patients as they travel to different places in the hospital—from their room to a lab, to pre- and post-op, to recovery, and back to their room. Before the availability of wireless, there was a constant need to disconnect, move, and reconnect these devices and monitors, which presented numerous opportunities for errors or breakdowns. Cables, connectors, and ports break down with extended use—and this is compounded when they are used next to hospital beds because of the frequent need to adjust the bed's height and position (from sitting to prone, for example). The result was often pinched or severed cables, many of which went unnoticed for some time, leaving patients unmonitored.

Another benefit to patients, health care professionals, and insurance companies is that wireless technology allows for real-time data at the point of care. This has a couple of significant implications. First, it means the patient can always be monitored, which improves staff reaction time to alerts—a potential lifesaver. Second, it allows for real-time access to patients' files. This is profound. Prior to wireless technology, patients often had a paper chart at the foot of their bed, which a doctor or nurse would look at prior to administering care or running a test. These charts were highly prone to errors—from lost or missing pages, to misinterpreted handwriting, to out-of-date or incomplete information. With wireless, caregivers now have real-time access to patients' digital records, where information is backed up and complete. This also allows for features such as auto-alerts, which help eliminate errors with treatment, incompatible prescriptions, or incorrect dosages. These are lifesaving improvements. Of course, many important security considerations go along with using wireless technology in this manner.

A less dramatic use of wireless in health care—but nonetheless an important one—is that most hospitals offer free Wi-Fi to patients and visitors. In this way, hospitals have greatly improved the satisfaction of patients and visitors alike. For all the drama of a medical emergency, the reality is that the vast majority of the time in a hospital for both visitors and patients is spent sitting around waiting. Offering free access to the Internet provides the perfect distraction.

Warehousing and Logistics

Seemingly at the opposite end of the technology spectrum from health care is the warehousing and logistics industry. Nevertheless, wireless networking has also made a significant impact here.

Prior to the advent of wireless networking, warehouse personnel logged storage locations on paper and used written notes to retrieve them. This method was fraught with errors and inefficiencies, especially in bigger warehouses, which can be as large as 1 million square feet.

Wireless networking allows for much greater efficiency throughout the entire process, from receiving, to shelving, to picking (retrieval), to outbound distribution. Specifically, wireless networking helps with the following:

- **Asset tracking**—With wireless networking, companies can automatically track assets in real time, providing a major productivity gain over manual, semiannual inventory checks.
- **Picking efficiency**—Retrieving inventory for distribution (picking the item off the warehouse floor) used to be a long process. Often, workers walked (or rode) several hundred yards through a warehouse, only to arrive and not find the item. The worker would then have to walk (or ride) all the way back, try to find the error, and repeat the process. With wireless technology, location accuracy is much improved, as is the picking process. This saves a great deal of time and money.
- **Loss control**—Another Wi-Fi automation success has been the savings gained by reducing inventory loss. In the first edition of this text, the authors were able to cite industry studies on the estimated savings through the use of wireless. Since then, “smart inventory” systems (all based on wireless technologies) have become so prevalent that it’s difficult to parse out specific benefits of wireless as a standalone aspect any more than one could have estimated the economic impact of Ethernet cables.

Retail

The retail industry has also taken great advantage of wireless technology. As with the back end of the business, discussed in the preceding section, the front end of the business has also changed as a result of wireless networking. Specifically, wireless has resulted in the following key changes:

- **Inventory counts**—Retailers always want the most popular products on hand, but they must carefully manage their inventory to avoid overstocking. Accurate inventory counts and direct front-of-store and point-of-customer interaction can put warehouse orders into motion in real time.
- **Customer satisfaction**—Retailers spend a great deal of money getting shoppers into their stores. Once shoppers are there, retailers must do their best to convert them into

buyers. This can be difficult, however, in an industry with a transient workforce, especially during those critical shopping seasons when a retail business can be made (or ruined). Arming sales staff with wireless devices turns even brand-new employees into product experts by allowing them to verify back-of-store inventory, suggest popular merchandise tie-ins or up-sells, or check with other local outlets for popular items.

General Business and Knowledge Workers

While it's true that specific industries have taken advantage of wireless networking, the biggest impact of wireless networking has been the way it has fundamentally changed how, where, and when people work. Before the wide adoption of wireless networking, people tended to work mostly in the office. When workers did work outside the office, either after hours or while traveling, they were often limited to offline work. Alternatively, if they went through emails, for example, they submitted work in batches.

With wireless, of course, there is greater flexibility with regard to where you can work—whether it's on the deck of a beach house, at a coffee shop, in an airport terminal, or on an airplane traveling 500 miles per hour, 30,000 feet in the air. As a result, worker productivity has gone up, and continues to rise.

This is great for many, but it does come at a cost. Perhaps most significant is the fact that the line between "work" and "not work" has blurred to the point that it's hard to distinguish where work ends and one's personal life begins. More and more, it seems that businesses expect their employees to be available and checking emails late at night, on weekends, and on vacations. More on topic for this discussion is that using a portable work device to access a network via a public Wi-Fi connection opens a vast array of potential security vulnerabilities that must be accounted for.

Nevertheless, Wi-Fi has brought about considerable increases in savings and overall efficiency. Its impact on the economy was considerable—even in its fledgling state, back in the early 2000s, before the advent of high-speed devices and mobile web applications. Even then, those who embraced the technology found that it delivered major benefits to their businesses.

The Wi-Fi Market

In 2017, the worldwide WLAN market was estimated to be $5.9 billion per year and is projected to be as much as $15 billion per year in 2022. About half of that was attributed to growth in the enterprise space, as fewer and fewer office spaces even bother installing Ethernet ports for users because most are connecting to the network over wireless most, if not all, of the time. However, this annual spending on WLAN equipment is only part of the story. As noted, Wi-Fi technology has changed the way many organizations do business. Indeed, it has created whole new business models.

Coffee shops, bookstores, and cafés have embraced wireless connectivity in two waves. The first wave involved providing wireless access to a private LAN that charged for a one-time use or for a subscription. Many such businesses felt that this was a nice add-on feature and an opportunity for revenue. What's interesting, however, is that due to the reduction in price of Wi-Fi equipment, many businesses have converted to providing free Wi-Fi access, choosing to forego the additional revenue in favor of attracting more customers, whom they welcome to come in and stay. In other words, they encourage clients to actually use their stores as an office, for three reasons:

- Those customers tend to buy other goods and services while there
- It creates a regular and loyal customer base
- Customers simply expect it to be available

Hotels have also been transformed. Not surprisingly, providing Internet access to guests has become essential. Perhaps the biggest impact of wireless technology on the hotel industry is that it has drastically lowered the cost of providing Internet access. This is particularly important in situations where retrofitting an older hotel to offer a wired network would be prohibitively expensive. If not for wireless technology, many hotels would have to choose between a very expensive upgrade and the potential loss of revenue. With wireless technology, Internet access can be provided at a much lower cost. This also has an enormous impact on hosting conferences and events, which is a major component of hotel revenues.

Much like cafés, some hotels offer free network access, especially in the lobby, where they encourage users—especially business travelers—to meet. Interestingly, however, some hotels still charge for "high-speed" or "premium" access in rooms but nearly all offer some level of free Wi-Fi to their guests. Wireless connectivity is simply an expectation as much as running water is.

IP Mobility

The number of mobile wireless devices now far exceeds the number of fixed devices. The growth and adoption rates of smartphones and tablets have created a huge demand on mobile operator data networks, with data traffic rates growing upward of 115 percent compounded per year since 2011. The public's and business's adoption of smartphones and tablets has been so fast that manufacturers of fixed PCs and desktop computers have either shifted to laptops, tablets, or servers, or are out of the market entirely.

The shift toward wireless mobile devices has presented businesses with many opportunities and challenges—most notably, the challenge of how to make best use of new mobile wireless technologies. After all, networks have been designed and secured with static devices in mind. When LANs were designed, it was assumed that employees would be at a desk within a department. The network was segmented accordingly via **subnets** to accommodate physically present numbers of employees and allow for future growth. The emergence of WLAN technology was used to address any unexpected growth. However, the growth in the number of IP-capable wireless devices means that employees are now far more mobile and can work from anywhere in the network or even from outside the network—at home or at a client's site.

This has proved to be very productive for business and has created tremendous improvements in employee efficiencies and communications. Laptops, smartphones, and tablets can be used in any location where there is a WLAN or 4G/5G network connection. These devices can also roam around the workplace LAN, connecting to the WLAN wherever there is a signal. If the WLAN is one single subnet, users can maintain application and web browser sessions.

The ability to roam and maintain an IP session is fundamental to true IP mobility. Ideally, the wireless device must not only be usable in any location, but it should also be usable when in transit between locations and even between IP and mobile networks. This presents a significant problem—when moving from one network or subnet to another, the device will require a change of IP address. However, if the IP address of the mobile device changes, all its current sessions will be lost, and applications will hang and crash.

What is required is a method to allow the seamless transfer of an IP address from one network to another without losing IP sessions. Only then will there be true mobility with roaming using IP wireless devices. This is termed *IP mobility*. The International Engineering Task Force (IETF) uses the term **Mobile IP** to describe its standard communications protocol for addressing this problem. It does so by preserving existing sessions as a device moves to a network with a different IP address space. Because this function is performed at the Network Layer of the OSI Reference Model rather than at the Physical Layer, a device can span different types of wireless and wired networks while maintaining connections and application sessions.

Another goal for the Mobile IP standard is for a device to be able to cross not just network boundaries but technologies as well. Ideally, the device should transparently connect to any technology it can support including wired, wireless, and 4G/WiMAX networks.

In a nutshell, with IP mobility, any compatible device that communicates at the Network Layer can roam from a fixed Ethernet to a wireless Ethernet to a mobile (cell) network without any loss of session and only a noticeable change in the access speeds, if that. There is no need to restart or reboot the operating system (OS) because the Network Layer handles it all seamlessly.

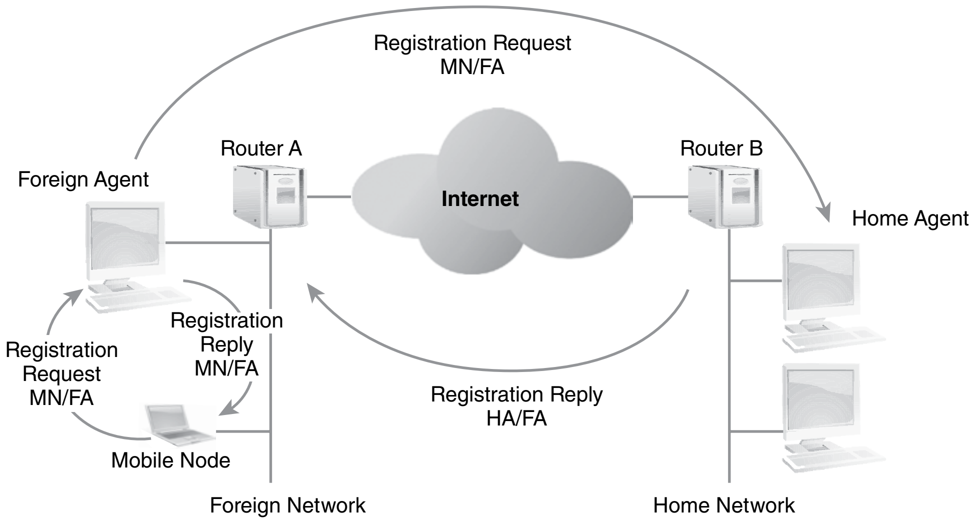
Mobile IP handles the change of IP address and maintains current sessions by using certain Mobile IP client stack specific components. These are as follows:

- **Mobile node (MN)**—This is a device (it could be anything) that changes its point of attachment from one subnet or network to another. It does its own move detection and must determine not just the change in access type, if any, but also the change in the subnet.
- **Home address**—This refers to the mobile node's home IP address, which is where it is registered with the home agent. The address can be static or dynamically assigned when registering with the home agent.
- **Home agent (HA)**—This is a router capable of processing and tracking mobile routing IP updates, tracking mobile node registrations, and forwarding traffic to mobile nodes on visited networks through IP tunnels.
- **Care-of-address (CoA)**—This is the new IP address the mobile node has been assigned by the visited network. The mobile node informs the HA of the CoA when registering its movement.
- **Foreign agent (FA)**—This stores all information about mobile nodes that are visiting its network. It advertises CoAs and routing services to the MN while it is visiting its network. If there is no FA present on a network, then the MN itself must handle getting a local address and advertising it.

Mobile IP enables a wireless device to traverse different network types—fixed, wireless, and cellular—while maintaining session and application status. It provides for transparent

FIGURE 1-3

How Mobile IP sessions are maintained as the user moves around.



handover and supports different access types and IP subnets through the use of IP tunnels from the home network to visited networks. This not only enables wireless devices to work on different networks but it allows them to be seamlessly accommodated without any drop in service. This is true IP mobility. It facilitates real roaming of wireless devices in which the device reconfigures itself automatically and registers with another network type and IP address while the user works without any interruption. **FIGURE 1-3** shows how Mobile IP sessions are maintained as the user moves around.

The Internet of Things

In 2005, having wireless access in the workplace or home was still something of a novelty. Today, wireless networking is so prevalent that one can obtain wireless access on a transcontinental flight. Indeed, passengers will even complain to the flight attendant if the connection is slow or unstable.

One of the biggest technology trends of today is connecting all manner of the Internet and each other. Known as the Internet of Things (IoT), it is the interconnection of virtually any electronic device that can be controlled and optimized via automation or remotely via an Internet connection. With IoT, most people's interactions will be via smart homes and electronics, allowing energy-saving programming, automated lighting, safety programming, and home entertainment. Unlike obtaining broadband access on a plane, which is likely a novel but infrequent experience for most, IoT is dramatically shaping the way people live and interact with their home environment and electronic devices. IoT will also extend to enterprise and industrial settings, and even into implanted medical devices such as heart monitors.

IoT has long been available through wired networks, but adoption among the general public has been slow and limited to those in high-end homes due to the costs associated with wiring and, in older homes, retrofitting. This key barrier has been removed in recent years due to the reduction in the size and cost of wireless technology.

As IoT continues to ramp over the next several years, people will truly live in a wireless world, where everything is connected and remotely controllable. And although this will have a great many benefits with regard to safety, energy efficiency, and convenience, it will also open a whole new world of security threats and vulnerabilities. It's one thing to have your computer files destroyed due to a virus or other malware, or to have your credit card run up by a cyber thief. It's another thing altogether to have a hacker lock you out of your own home, ransom control of your heating system in the dead of winter, or take control of a moving vehicle (while you are in it). For those in the information security business, this will be another front in the cybersecurity war that sees no end in sight.

CHAPTER SUMMARY

Data communication and networking have a long rich history—the advancements from telegraphy to the near universal use of the PSTN seemed to happen at a steady and measured pace over the course of 60 years or so. However, with the advent of packet switching, which enabled multiple transmissions to share a single circuit and the creation of ARPANET and the Internet, the pace of networking and communication innovation accelerated even beyond the wildest expectations of the most enthusiastic futurist of the 1980s.

Initially, networks were wired; but with advancements in mobile telephony came the development of the WLAN, which could be accessed by mobile users.

Wireless networking has changed the world in many ways. It has altered entire industries and brought productivity gains even to sectors that had seemingly squeezed out as much productivity as possible. More than that, wireless networking has changed not only how and where people work but also the very relationship between employees and employers. Wireless technology has brought work into people's homes in a way that previously did not exist.

In a macro sense, wireless technology has made it easier to bring Internet access to people and places that for too long have been on the wrong side of the digital divide. This extended access improves not only the lives of those directly affected but also the surrounding community and, to some degree, the world at large. As they say, a rising tide lifts all boats.

The rise in the use of mobile devices, such as smartphones and tablets, has fueled demand for wireless networks. It has likewise presented businesses with many opportunities and challenges. Mobility has become a way of life, with smartphones and tablets part of the fabric of modern society. For the generation born in the Internet era, to be denied this mobility is unthinkable.

But all of this easy and near constant access, for all the good it has done, has also exposed and even introduced many security vulnerabilities. Vulnerabilities that impact individuals, companies (both large and small), and even nation states. Fortunately, there are many people like you who are interested in mitigating those vulnerabilities so that the benefits can be fully felt by all.

KEY CONCEPTS AND TERMS

Application Layer
Bluetooth
Circuit switching
Data Link Layer
Dotted decimal
Dynamic Host Configuration Protocol (DHCP)
Federal Communications Commission (FCC)
Internet of Things (IoT)
Internet Protocol version 4 (IPv4)
Internet Protocol version 6 (IPv6)
IP addressing
Key performance indicators (KPIs)
Knowledge workers
Local area network (LAN)
Media Access Control (MAC) address
Mobile IP
Modem
Network address translation (NAT)
Network effect
Network Layer
Open Systems Interconnection (OSI) Reference Model
Packet switching
Physical Layer
Presentation Layer
Public switched telephone network (PSTN)
Session Layer
Smartphone
Stack
subnets
Telegraphy
Telephony
Transmission Control Protocol/Internet Protocol (TCP/IP)
Transport Layer
Wi-Fi
Wireless local area network (WLAN)
Worldwide Interoperability for Microwave Access (WiMAX)

CHAPTER 1 ASSESSMENT

1. Digital communication offers which of the following advantages?

A. More efficient use of bandwidth
B. Greater utilization
C. Improved error rates
D. Less susceptibility to noise and interference
E. All of the above

2. ARPANET was the predecessor of the modern Internet.

A. True
B. False

3. Wireless networking was initially supported by IT departments because of the productivity gains it provided.

A. True
B. False

4. Mobile IP solves which important problem?

A. Battery life
B. Wireless connections to the Internet
C. Access to app stores
D. The ability to maintain an IP session while moving

5. Which of the following is *not* a requirement for successful mobility?

A. Location discovery
B. Movement detection
C. Update signaling
D. Omnidirectional antennas
E. Path establishment

6. Switches primarily operate at which layer of the OSI Reference Model?

A. Physical Layer
B. Data Link Layer
C. Network Layer
D. Transport Layer
E. None of the above

7. Wireless networking standards are defined at the Network Layer.

A. True
B. False

8. Layers 4 to 7 are often grouped together and referred to as the "Application Layers."

A. True
B. False

9. IP addressing is specified in which layer?

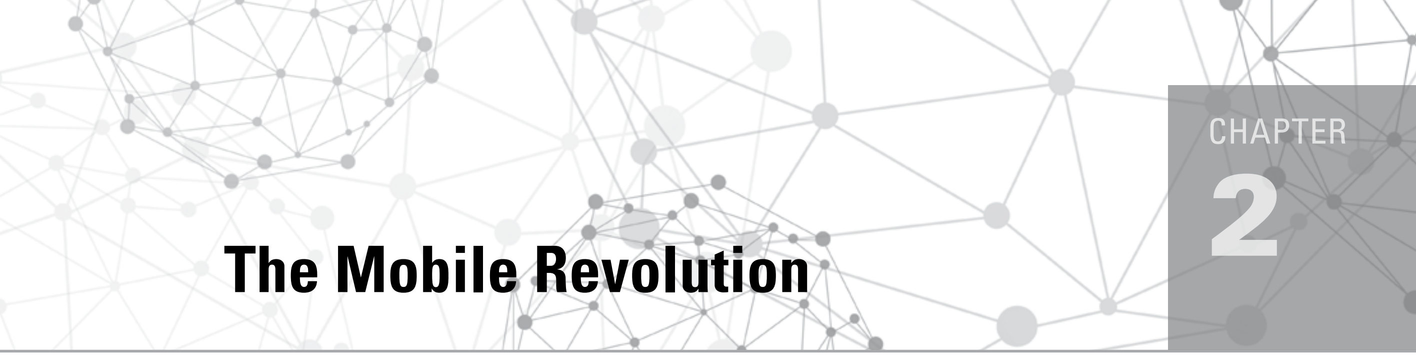
A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4
E. All of the above

10. The Data Link Layer uses a logical addressing scheme to switch data frames.

A. True
B. False

11. Which of the following is *not* a use of Wi-Fi in warehousing?

A. Asset tracking
B. Loss control
C. Forklift automation
D. Picking efficiency



CHAPTER 2

The Mobile Revolution

THIS CHAPTER TAKES A HISTORICAL LOOK AT MOBILE NETWORKS, smartphones, and other mobile devices. With this understanding, you'll be better able to grasp the security issues related or specific to mobile networks and devices.

Over the last 30 years, the advances in mobility have been significant. Evolving from clunky analog phones that were little more than novelty status symbols (and poor communication devices) to business "smart devices" that people can't live without, these devices and the systems that support them have changed how people live, work, and interact. For the security professional, however, mobility represents a new and complex set of challenges.

Chapter 2 Topics

This chapter covers the following concepts and topics:

- How early cellular or mobile devices operated
- How mobile networks evolved
- What the effects of the BlackBerry were
- What the economic impact of mobility has been
- What the business impact of mobility has been
- What some business use cases for mobility are

Chapter 2 Goals

When you complete this chapter, you will be able to:

- Describe basic cellular design
- Provide examples of frequency sharing techniques
- List the main considerations in cellular network design
- Describe the security issues and concerns with both 3G and 4G systems
- Provide examples of business uses for Mobile IP and smart devices

© Cherezoff/Shutterstock

Introduction to Cellular (Mobile Communication)

One of the greatest accomplishments of the 20th century was the rollout of the public switched telephone network (PSTN)—not only because of the technology itself but also because of its ubiquitous reach. With the PSTN, nearly every home in the developed world (and a high percentage of homes even in some undeveloped areas) had a wired communication channel that connected it to the rest of the world, providing a lifeline in times of trouble. The system even provided its own power, keeping the communication channel open when the lights went out. Just imagine the scope and cost of running and maintaining a wired connection in the United States alone, with approximately 125 million homes and 20 million apartments. (This does not even include every business and office.)

In the early 1990s, telephony was extended beyond the limitations of wired connections with the emergence of the first mobile, or **cellular**, phones. Cellular is a generic term for mobile phone systems or devices. It refers to the portioning of frequency coverage maps, discussed shortly. Initially viewed as a perk for high-powered executives and a status symbol for young professionals, cellular phones caught on fast. As their popularity rose, technology companies poured hundreds of millions of dollars into research and development, and the pace of innovation took off.

The first-generation cellular phones in the 1990s had limited range and coverage, short battery life, and poor voice quality. Even so, people clearly saw the benefit of having a phone that could travel with them—although few considered their mobile phone to be their primary phone. Flash forward just 30 years, and mobile phones are now viewed as an essential part of people's lives. In some cases, they are the predominate means by which people interact with the world.

The expansion has been impressive. In the United States, 90 percent of adults now own a mobile phone. Ownership in the 18–29-year-old group is 98 percent. In addition, more and more teens and even preteens have their own smartphones. More impressive is that these statistics transcend gender, race, and income categories. The most amazing aspect of this phenomenon, however, is the growing number of mobile phone users who have disconnected their landlines—something that was unthinkable even 15 years ago.

Mobile phones use all the principles of two-way radio communication that have been around since the early 20th century. Well-known problems such as range, power, signal-to-noise ratios, and interference all come into play. This keeps a lot of radio frequency (RF) engineers gainfully employed. Mobile telephony, however, presents some unique challenges. Indeed, one was so critical to making mobile telephony feasible that the solution to the problem became the name that now describes the entire system: cellular. The problem stems from the fact that in a mobile telephony system, there are far more users than there are available frequency channels over which to communicate. This is a two-part problem; this discussion will begin with the physical distribution of channels, or frequency bands.

Cellular Coverage Maps

One of the limitations of cellular technology is the transmission power of the phone. Because the phone is battery-powered, and because battery life is a big consideration, transmission power must be kept low. (There are health considerations as well. You don't really want a high-powered transmitter pressed to your head for several hours a day!) However, low-transmission power limits the signal range, which means you need to have a receiver nearby.

The solution was to create a coverage map of small geographic sectors, or *cells*, each with its own antenna tower. Two separate teams of engineers from Bell Labs, 20 years apart, conceived and then perfected the idea of using hexagonal (six-sided) cells. This mapping provides the best coverage, leaving no gaps in the coverage plan. This was referred to as a *cellular design* and was so critical to the design of the system that term *cell phone* came into being.

In each cell, there is an antenna array called a **base transceiver station (BTS)**, which communicates directly with the subscriber phones within its coverage area. Usually perched on a tall metal structure, these antenna arrays came to be known as **cell towers**, or simply *towers*. In some places, local ordinances require towers to be camouflaged. As a result, many look like tall trees and are easy to miss if you are not looking closely (which is exactly the point). A mobile phone communicates with the tower. The tower, in turn, communicates over a backhaul circuit either originally on fixed-line **T1/E1** trunks (T1/E1 are the standard digital carrier signals that transmit both voice and data) or on point-to-point microwave links to a **base controller station (BCS)**, which connects to the core network. Today, with 4G/5G networks, the backhaul is typically over high-speed fiber backhaul in urban areas and microwave links in remote locations. Typically, multiple towers will connect to a single BCS. The core network links all BCSs so that calls can be established over the local cellular network. It also has connections via gateways to the PSTN and, more recently, to the Internet.

Bell Labs

For most of its existence in the 20th century, the PSTN was a monopoly service delivered primarily by the Bell Telephone System (which became AT&T), often referred to as "Ma Bell" because it eventually spawned many smaller regional providers called "Baby Bells." One common criticism of monopolies is that they stall innovation due to the lack of competition. However, this did not seem to be the case with Bell; its engineering division, Bell Labs, had a remarkable 70-plus-year run of technology breakthroughs and innovations. These include, among other things, the first operational transistor, the first binary digital computer, the first transatlantic phone call, the development of UNIX operating system, and the development of both the C and C++ programming languages.

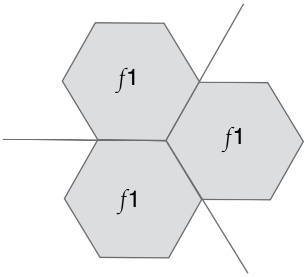
Cellular design fixed the phone transmission power problem. However, this created a frequency interference problem. As shown in **FIGURE 2-1**, if each cell uses the same sets of frequencies, then users in two different cells on the same channel interfere with each other.

The solution to the interference problem was to split up the frequencies to prevent interference from adjacent cells. With this pattern, interference is greatly reduced (see **FIGURE 2-2**).

Taking a step back and looking at the repeating pattern, you can see the genius behind the concept of cellular and **frequency reuse** patterns (that is, the practice of assigning multiple users to the same frequency channel, achieved by the physical separation and power

FIGURE 2-1

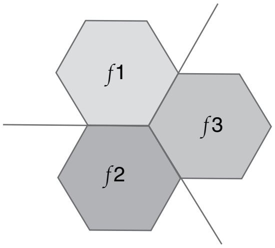
Adjacent cells using the same frequency will interfere with each other, especially near the cell borders.



Frequency Reuse 1

FIGURE 2-2

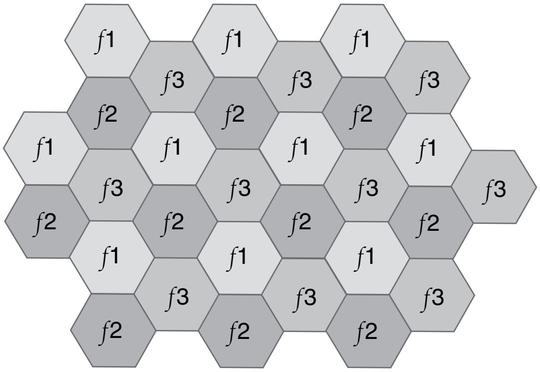
By segmenting frequency use, interference can be greatly reduced or avoided.



Frequency Reuse 3

FIGURE 2-3

A basic frequency reuse pattern on a large scale. Note that no cell is adjacent to another that uses the same sets of frequencies.



management of the transmission streams). This is a simplified view, however. Radio-frequency planning requires more than just creating areas that roughly correspond to the hexagonal cell pattern, because the distribution and density of potential subscribers is not likely to be uniform. Therefore, large cells called **macrocells** (that is, cells within a mobile system for large coverage areas) are needed for rural areas. **Microcells** (cells within a mobile system for small coverage areas) are needed for urban areas. **Picocells** (small hotspot cells offering Wi-Fi connectivity via a mobile carrier) are needed for dense urban areas. This ensures sufficient capacity per cell or area (see **FIGURE 2-3**). Picocells are now often being used inside buildings and large venues as most cellular communication happens inside of buildings where signals from external cell towers are often attenuated. However, picocells are alternatively deployed at the other end of the scale in remote rural areas when a home or office is out of range of the cellular network.

Frequency Sharing

Another challenge with cellular phones is the limitation of frequency channels. For example, the first cellular system rolled out in the United States had only 830 usable channels—not many at all. This limitation was compounded by the fact that frequency reuse patterns reduced the number of channels in any one cell to about 280 channels per cell. Even in the early days of cellular telephony, this small number of channels was not nearly enough to meet demand. There were solutions to this problem, but all of them were based on the concept of allowing multiple access—either through frequencies, time, or code division.

Frequency Division Multiple Access

Frequency Division Multiple Access (FDMA) is the foundation of cellular coverage maps, but in this case, each channel is split up further so that multiple users can share a common channel without interference. FDMA does not require a great deal of timing synchronization, but it does require very precise transmission and receiving filters. FDMA frequencies are assigned for the length of the communication, the downside being that unused channels sit idle. FDMA is a 1G technology, and is still common in satellite communications (see **FIGURE 2-4**).

Time Division Multiple Access

Time Division Multiple Access (TDMA) allows multiple users on the same frequency channel, each with its own sliver of time. This works well in a voice conversation because a phone conversation between two people is mostly silence. That means there's a lot of "empty space" on a channel even when it's in use.

Channel efficiency was greatly improved through the use of voice-compression techniques. These employed intelligent algorithms that could turn speech into mathematical points on a graph. This allowed speech to be replicated with high fidelity (that is, it sounded like the real person on the receiving end) without ever sending the speech signal. As a result, a lot of conversations could be stuffed on to one frequency channel.

TDMA does not require high-performance filtering as FDMA does, but it does require very tight timing synchronization. TDMA helped bridge 1G technology to 2G and allowed for rapid subscriber expansion from the original analog cell systems to digital without expensive upgrades to the system itself (see **FIGURE 2-5**).

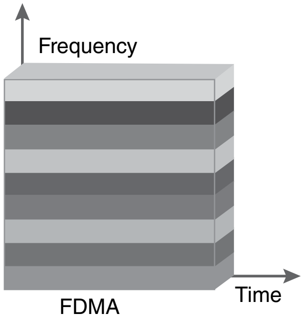


FIGURE 2-4

With FDMA, the frequency spectrum is divided among users.

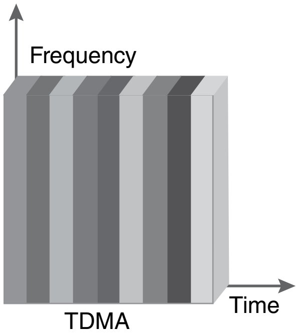
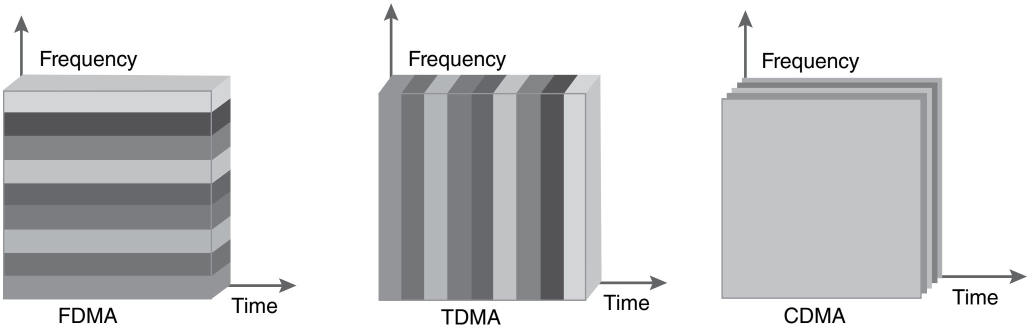


FIGURE 2-5

With TDMA, each user is assigned a time slot so that packets from different communication sessions can occupy a shared frequency without interference.

FIGURE 2-6

With CDMA, communication is spread over multiple frequencies at the same time. Coding algorithms are used to spread and then reassemble the transmissions.



Code Division Multiple Access

Code Division Multiple Access (CDMA) makes it possible for several users to share multiple frequency bands at the same time by spreading the signal out over the frequencies. This spread-spectrum technique uses codes to distinguish between connections. The wide bandwidths and improved power usage greatly reduce interference, and the coding allows multiple users to occupy the same channel at the same time (see **FIGURE 2-6**).

CDMA is a 3G technology that improved the capacity of 1G systems by a factor of 18 and 2G systems by a factor of 6. However, because it relies on lower-powered signals, CDMA suffers from what is known as the *near–far problem*. This is when a receiver locks onto a strong signal from a nearby source, preventing it from detecting a wanted signal from a source that is farther away (and therefore weaker). Because CDMA has multiple signals on the same frequency, the near–far problem creates a frequency jam. This is a potential security issue from an availability standpoint, as would-be **hackers** could prevent communication via jamming. **FIGURE 2-7** shows all three types of basic cellular modulation—FDMA, TDMA, and CDMA—together.

Cellular Handoff

Because mobile phones are—obviously—mobile, cellular networks must be able to accommodate subscribers as they pass out of the range of one transmitter and into the area of