Chapter 1

Overview of Wireless Standards, Organizations, and Fundamentals

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **History of WLAN**
- ✓ **Standards organizations**
  - Federal Communications Commission
  - International Telecommunication Union Radiocommunication Sector
  - Institute of Electrical and Electronics Engineers
  - Wi-Fi Alliance
  - International Organization for Standardization
- ✓ **Core, distribution, and access**
- ✓ **Communications fundamentals**

Wireless local area network (WLAN) technology has a long history that dates back to the 1970s with roots as far back as the 19th century. In this chapter, you will learn a brief history of WLAN technology. Learning a new technology can seem like a daunting task. There are so many new acronyms, abbreviations, terms, and ideas to become familiar with. One of the keys to learning any subject is to learn the basics. Whether you are learning to drive a car, fly an airplane, or install a wireless computer network, there are basic rules, principles, and concepts that, once learned, provide the building blocks for the rest of your education.

IEEE 802.11 technology, more commonly referred to as Wi-Fi, is a standard technology for providing local area network (LAN) communications using radio frequencies (RFs). The IEEE designated the 802.11-2007 standard as a guideline to provide operational parameters for WLANs. There are numerous standards organizations and regulatory bodies that help govern and direct wireless technologies and the related industry. Having some knowledge of these different organizations can provide you with insight as to how IEEE 802.11 functions, and sometimes even how and why the standards have evolved the way they have.

As you become more knowledgeable about wireless networking, you may want or need to read some of the standards that are created by the different organizations. Along with the information about the standards bodies, this chapter includes a brief overview of their documents.

In addition to reviewing the different standards organizations that guide and regulate Wi-Fi, this chapter discusses where WLAN technology fits in with basic networking design fundamentals. Finally, this chapter reviews some fundamentals of communications and data keying that are not part of the CWNA exam but that may help you better understand wireless communications.

History of WLAN

In the 19th century, numerous inventors and scientists, including Michael Faraday, James Clerk Maxwell, Heinrich Rudolf Hertz, Nikola Tesla, David Edward Hughes, Thomas Edison, and Guglielmo Marconi, began to experiment with wireless communications. These innovators discovered and created many theories about the concepts of electrical magnetic *radio frequency (RF)*.

Wireless networking technology was first used by the U.S. military during World War II to transmit data over an RF medium using classified encryption technology, to send battle plans across enemy lines. The *spread spectrum* radio technologies often used in today's WLANs were also originally patented during the era of World War II, although they were not implemented until almost two decades later.

In 1970, the University of Hawaii developed the first wireless network, called ALOHAnet, to wirelessly communicate data between the Hawaiian Islands. The network used a LAN communication Open Systems Interconnection layer 2 protocol called ALOHA on a wireless shared medium in the 400 MHz frequency range. The technology used in ALOHAnet is often credited as a building block for the Medium Access Control technologies of Carrier Sense Multiple Access with Collision Detection (CSMA/CD) used in Ethernet and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) used in 802.11 radios. You will learn more about CSMA/CA in Chapter 8, "802.11 Medium Access."

In the 1990s, commercial networking vendors began to produce low-speed wireless data networking products, most of which operated in the 900 MHz frequency band. The Institute of Electrical and Electronics Engineers (IEEE) began to discuss standardizing WLAN technologies in 1991. In 1997, the IEEE ratified the original 802.11 standard that is the foundation of the WLAN technologies that you will be learning about in this book.

Legacy 802.11 technology was deployed between 1997 and 1999 mostly in warehousing and manufacturing environments for the use of low-speed data collection with wireless barcode scanners. In 1999, the IEEE defined higher data speeds with the 802.11b amendment. The introduction of data rates as high as 11 Mbps, along with price decreases, ignited the sales of wireless home networking routers in the small office, home office (SOHO) marketplace. Home users soon became accustomed to wireless networking in their homes and began to demand that their employers also provide wireless networking capabilities in the workplace. After initial resistance to 802.11 technology, small companies, medium-sized businesses, and corporations began to realize the value of deploying 802.11 wireless technology in their enterprises.

If you ask the average user about their 802.11 wireless network, they will probably give you a very strange look. The name that most people recognize for the technology is *Wi-Fi*. Wi-Fi is a marketing term, recognized worldwide by millions of people as referring to 802.11 wireless networking.

What Does the Term *Wi-Fi* Mean?

Many people mistakenly assume that *Wi-Fi* is an acronym for the phrase *wireless fidelity* (much like *hi-fi* is short for *high fidelity*), but Wi-Fi is simply a brand name used to market 802.11 WLAN technology. Ambiguity in IEEE framework standards for wireless communications allowed manufacturers to interpret the 802.11 standard in different ways. As a result, multiple vendors could have IEEE 802.11–compliant devices that did not interoperate with each other. The group Wireless Ethernet Compatibility Alliance (WECA) was created to further define the IEEE standard in such a way as to force interoperability between vendors. WECA, now the Wi-Fi Alliance, chose the term *Wi-Fi* as a marketing brand. The Wi-Fi Alliance champions enforcing interoperability among wireless devices. To be Wi-Fi compliant, vendors must send their products to a Wi-Fi Alliance test lab that thoroughly tests compliance to the Wi-Fi certification. More information about the origins of the term Wi-Fi can be found online at Wi-Fi Net News: `www.wifinetnews.com/archives/006029.html`.

Wi-Fi radios are used for numerous enterprise applications and can also be found in laptops, cellular phones, cameras, televisions, printers, and many other consumer devices. More than 300 million Wi-Fi chipsets were shipped in 2007, with current estimates of annual sales of over one billion Wi-Fi chipsets by the year 2011.

According to the Wi-Fi Alliance, there are currently more than 450 million Wi-Fi users worldwide. In a survey that they conducted, 68 percent of those users would rather give up chocolate than do without Wi-Fi. Since the original standard was created in 1997, 802.11 technology has grown to enormous proportions; Wi-Fi has now become part of our worldwide culture.

Standards Organizations

Each of the standards organizations discussed in this chapter help to guide a different aspect of the wireless networking industry.

The International Telecommunication Union Radiocommunication Sector (ITU-R) and local entities such as the Federal Communications Commission (FCC) set the rules for what the user can do with a radio transmitter. These organizations manage and regulate frequencies, power levels, and transmission methods. They also work together to help guide the growth and expansion that is being demanded by wireless users.

The Institute of Electrical and Electronics Engineers (IEEE) creates standards for compatibility and coexistence between networking equipment. The IEEE standards must adhere to the rules of the communications organizations, such as the FCC.

The Wi-Fi Alliance performs certification testing to make sure wireless networking equipment conforms to the 802.11 WLAN communication guidelines, similar to the IEEE 802.11-2007 standard.

The International Organization for Standardization (ISO) created the Open Systems Interconnection (OSI) model, which is an architectural model for data communications.

You will look at each of these organizations in the following sections.

Federal Communications Commission (FCC)

To put it simply, the *Federal Communications Commission (FCC)* regulates communications within the United States as well as communications to and from the United States. Established by the Communications Act of 1934, the FCC is responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable. The task of the FCC in wireless networking is to regulate the radio signals that are used for wireless networking. The FCC has jurisdiction over the 50 states, the District of Columbia, and U.S. possessions. Most countries have governing bodies that function similarly to the FCC.

The FCC and the respective controlling agencies in the other countries typically regulate two categories of wireless communications: licensed and unlicensed. The difference is that unlicensed users do not have to go through the license application procedures before they can install a wireless system. Both licensed and unlicensed communications are typically regulated in the following five areas:

- Frequency
- Bandwidth
- Maximum power of the intentional radiator (IR)
- Maximum equivalent isotropically radiated power (EIRP)
- Use (indoor and/or outdoor)

Real World Scenario

What Are the Advantages and Disadvantages of Using an Unlicensed Frequency?

As stated earlier, licensed frequencies require an approved license application, and the financial costs are very high. One main advantage of an unlicensed frequency is that permission to transmit on the frequency is free. Although there are no financial costs, you still must abide by transmission regulations and other restrictions. In other words, transmitting in an unlicensed frequency may be free, but there still are rules.

The main disadvantage to transmitting in an unlicensed frequency band is that anyone else can also transmit in that same frequency space. Unlicensed frequency bands are often very crowded; therefore, transmissions from other individuals can cause interference with your transmissions. If someone else is interfering with your transmissions, you have no legal recourse as long as the other individual is abiding by the rules and regulations of the unlicensed frequency.

Essentially, the FCC and other regulatory bodies set the rules for what the user can do regarding RF transmissions. From there, the standards organizations create the standards to work within these guidelines. These organizations work together to help meet the demands of the fast-growing wireless industry.

The FCC rules are published in the Code of Federal Regulations (CFR). The CFR is divided into 50 titles that are updated yearly. The title that is relevant to wireless networking is Title 47, *Telecommunications*. Title 47 is divided into many parts; Part 15, “Radio Frequency Devices,” is where you will find the rules and regulations regarding wireless networking related to 802.11. Part 15 is further broken down into subparts and sections. A complete reference will look like this example: 47CFR15.3.

NOTE

The FCC transmit power regulations for the 2.4 GHz ISM frequency band and the 5 GHz UNII bands can be found in the appendix of this book. More information can be found at `www.fcc.gov` and `http://wireless.fcc.gov`.

International Telecommunication Union Radiocommunication Sector (ITU-R)

A global hierarchy exists for management of the RF spectrum worldwide. The United Nations has tasked the *International Telecommunication Union Radiocommunication Sector (ITU-R)* with global spectrum management. The ITU-R maintains a database of worldwide frequency assignments and coordinates spectrum management through five administrative regions.

The five regions are broken down as follows:

Region A: North and South America Inter-American Telecommunication Commission (CITEL)

`www.citel.oas.org`

Region B: Western Europe European Conference of Postal and Telecommunications Administrations (CEPT)

`www.cept.org`

Region C: Eastern Europe and Northern Asia Regional Commonwealth in the field of Communications (RCC)

`www.rcc.org.ru/en/`

Region D: Africa African Telecommunications Union (ATU)

`www.atu-uat.org`

Region E: Asia and Australasia Asia-Pacific Telecommunity (APT)

`www.aptsec.org`

Within each region, local government RF regulatory bodies such as the following manage the RF spectrum for their respective countries:

- Australia: Australian Communications and Media Authority (ACMA)
- Japan: Association of Radio Industries and Businesses (ARIB)
- New Zealand: Ministry of Economic Development
- United States: Federal Communications Commission (FCC)

It is important to understand that communications are regulated differently in many regions and countries. For example, European RF regulations are very different from the regulations used in North America. When deploying a WLAN, please take the time to learn about rules and policies of the local *regulatory domain authority*.

NOTE

More information about the ITU-R can be found at `www.itu.int/ITU-R/`.

Institute of Electrical and Electronics Engineers (IEEE)

The *Institute of Electrical and Electronics Engineers*, commonly known as the *IEEE*, is a global professional society with more than 350,000 members. The IEEE's mission is to "foster technological innovation and excellence for the benefit of humanity." To networking professionals, that means creating the standards that we use to communicate.

The IEEE is probably best known for its LAN standards, the IEEE 802 project.

NOTE: The 802 project is one of many IEEE projects; however, it is the only IEEE project addressed in this book.

IEEE projects are subdivided into working groups to develop standards that address specific problems or needs. For instance, the IEEE 802.3 working group was responsible for the creation of a standard for Ethernet, and the IEEE 802.11 working group was responsible for creating the WLAN standard. The numbers are assigned as the groups are formed, so the 11 assigned to the wireless group indicates that it was the 11th working group formed under the IEEE 802 project.

As the need arises to revise existing standards created by the working groups, task groups are formed. These task groups are assigned a sequential single letter (multiple letters are assigned if all single letters have been used) that is added to the end of the standard number (for example, 802.11a, 802.11g, and 802.3af). Some letters are not assigned. For example *o* and *l* are not assigned to prevent confusion with the numbers 0 and 1. Other letters may not be assigned to task groups to prevent confusion with other standards. For example, 802.11x has not been assigned because it can be easily confused with the 802.1X standard and because 802.11*x* has become a common casual reference to the 802.11 family of standards.

NOTE: More information about the IEEE can be found at `www.ieee.org`.

It is important to remember that the IEEE standards, like many other standards, are written documents describing how technical processes and equipment should function. Unfortunately, this often allows for different interpretations when the standard is being implemented, so it is common for early products to be incompatible between vendors, as was the case with the early 802.11 products.

NOTE: The history of the 802.11 standard and amendments is covered extensively in Chapter 5, "IEEE 802.11 Standards." The CWNA exam (PW0-104) is based on the most recently published version of the standard, 802.11-2007. The 802.11-2007 standard can be downloaded from `http://standards.ieee.org/getieee802/802.11.html`.

Wi-Fi Alliance

The *Wi-Fi Alliance* is a global, nonprofit industry association of more than 300 member companies devoted to promoting the growth of WLANs. One of the primary tasks of the Wi-Fi Alliance is to market the Wi-Fi brand and raise consumer awareness of new 802.11 technologies as they become available. Because of the Wi-Fi Alliance's overwhelming marketing success, the majority of the worldwide 450 million Wi-Fi users immediately recognize the Wi-Fi logo seen in Figure 1.1.

FIGURE 1.1 Wi-Fi logo

The Wi-Fi Alliance's main task is to ensure the interoperability of WLAN products by providing certification testing. During the early days of the 802.11 standard, the Wi-Fi Alliance further defined some of the ambiguous standards requirements and provided a set of guidelines to assure compatibility between different vendors. As seen in Figure 1.2, products that pass the Wi-Fi certification process receive a Wi-Fi Interoperability Certificate that provides detailed information about the individual product's Wi-Fi certifications.

FIGURE 1.2 Wi-Fi Interoperability Certificate

Wi-Fi® Interoperability Certificate

Certification ID: WFAxxxx

This certificate indicates the capabilities and features that successfully completed interoperability testing by the Wi-Fi Alliance. You may find detailed descriptions of these features at www.wi-fi.org/certification_programs.php.

Certificate Date: date_of_product_certification
Category: primary_product_category
Company: company_name
Product: product_name
Model/SKU #: model_number/sku

This product has the following Wi-Fi Certifications:

IEEE Standard	Security	Multimedia	Convergence
IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n draft 2.0 IEEE 802.11d IEEE 802.11h	WPA™ - Enterprise, Personal WPA2™ - Enterprise, Personal **EAP Type(s)** EAP-TLS EAP-TTLS/MSCHAPv2 PEAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM **Vendor EAP Type(s)** EAP-TLS EAP-TTLS/MSCHAPv2 PEAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM	WMM ® WMM Power Save **Special Features** Wi-Fi Protected Setup™ PIN PBC NFC	Voice – Personal CWG-RF Profile (contact manufacturer for results)

For more information: www.wi-fi.org/certification_programs.php

The Wi-Fi Alliance, originally named the Wireless Ethernet Compatibility Alliance (WECA), was founded in August 1999. The name was changed to the Wi-Fi Alliance in October 2002.

The Wi-Fi Alliance has certified more than 4,600 Wi-Fi products for interoperability since testing began in April 2000. Multiple Wi-Fi CERTIFIED™ programs exist that cover basic connectivity, security, quality of service (QoS), and more. Testing of vendor Wi-Fi products is performed in 12 independent authorized test laboratories worldwide. The guidelines for interoperability for each Wi-Fi CERTIFIED™ program are usually based on key components and functions that are defined in the IEEE 802.11-2007 standard and various 802.11 amendments. In fact, many of the same engineers who belong to 802.11 task groups are also contributing members of the Wi-Fi Alliance. However, it is important to understand that the IEEE and the Wi-Fi Alliance are two separate organizations. The IEEE 802.11 task group defines the WLAN standards, and the Wi-Fi Alliance defines interoperability certification programs. The Wi-Fi CERTIFIED™ programs include the following:

802.11a, b, or g—IEEE 802.11 baseline The baseline program certifies 802.11a, b, and/or g interoperability to ensure that the essential wireless data transmission works as expected. 802.11b and g utilize spectrum in the 2.4 GHz band. 802.11g has a higher data rate (54 Mbps) than 802.11b (11 Mbps). 802.11a utilizes frequencies in the 5 GHz band and has a maximum data rate of 54 Mbps. Each certified product is required to support one frequency band as a minimum, but it can support both. The CWNA exam will not use the terms 802.11 a/b/g; however, the a/b/g terminology is commonplace within the industry because of the Wi-Fi Alliance baseline certifications.

Wi-Fi Protected Access 2 (WPA2)—security WPA2 is based on the security mechanisms that were originally defined in the IEEE 802.11i amendment that defines a *robust security network (RSN)*. Two versions of WPA2 exist: WPA2-Personal defines security for a SOHO environment, and WPA2-Enterprise defines stronger security for enterprise corporate networks. Each certified product is required to support WPA2-Personal or WPA2-Enterprise. More-detailed discussion of WPA2 security can be found in Chapter 13, "802.11 Network Security Architecture."

802.11n draft 2.0—IEEE 802.11 baseline This certification program is based on the 802.11n draft amendment that defines a High Throughput (HT) wireless network utilizing multiple-input multiple-output (MIMO) technology. *High Throughput (HT)* provides PHY and MAC enhancements to support throughput of 100 Mbps and greater. This technology is discussed in detail in Chapter 18, "High Throughput (HT) and 802.11n." Please note that Wi-Fi Multimedia (WMM) certification is required for the 802.11n draft 2.0 certification.

Wi-Fi Multimedia (WMM)—multimedia WMM is based on the QoS mechanisms that were originally defined in the IEEE 802.11e amendment. WMM enables Wi-Fi networks to prioritize traffic generated by different applications. In a network where WMM is supported by both the access point and the client device, traffic generated by time-sensitive applications such as voice or video can be prioritized for transmission on the half-duplex RF medium. WMM mechanisms are discussed in greater detail in Chapter 9, "802.11 MAC Architecture."

WMM Power Save (WMM-PS)—multimedia WMM-PS helps conserve battery power for devices using Wi-Fi radios by managing the time the client device spends in sleep mode.

Conserving battery life is critical for handheld devices such as barcode scanners and VoWiFi phones. To take advantage of power-saving capabilities, both the device and the access point must support WMM Power Save. WMM-PS and legacy power-saving mechanisms are discussed in greater detail in Chapter 9.

Wi-Fi Protected Setup—security Wi-Fi Protected Setup defines simplified and automatic WPA and WPA2 security configurations for home and small-business users. Users can easily configure a network with security protection by using a personal identification number (PIN) or a button located on the access point and the client device.

CWG-RF—multimedia Converged Wireless Group-RF Profile (CWG-RF) was developed jointly by the Wi-Fi Alliance and the Cellular Telecommunications and Internet Association (CTIA), now known as The Wireless Association. CWG-RF defines performance metrics for Wi-Fi and cellular radios in a converged handset to help ensure that both technologies perform well in the presence of the other. All CTIA-certified handsets now include this certification.

Voice Personal—application Voice Personal offers enhanced support for voice applications in residential and small-business Wi-Fi networks. These networks include one access point, mixed voice and data traffic from multiple devices (such as phones, PCs, printers, and other consumer electronic devices), and support for up to four concurrent phone calls. Both the access point and the client device must be certified to achieve performance matching the certification metrics.

As 802.11 technologies evolve, new Wi-Fi CERTIFIED™ programs will be detailed by the Wi-Fi Alliance. The next certification will probably be Voice Enterprise, which will define enhanced support for voice applications in the enterprise environment. Some aspects of the 802.11r (secure roaming) and 802.11k (resource management) amendments will probably be tested in Voice Enterprise.

Wi-Fi Alliance and Wi-Fi CERTIFIED

More information about the Wi-Fi Alliance can be found at `www.wi-fi.org`. The following five white papers from the Wi-Fi Alliance are also included on the CD that accompanies this book:

- *Wi-Fi CERTIFIED™ for WMM™: Support for Multimedia Applications with Quality of Service in Wi-Fi Networks*
- *WMM™ Power Save for Mobile and Portable Wi-Fi CERTIFIED Devices*
- *Wi-Fi Protected Access: Strong, Standards-Based, Interoperable Security for Today's Wi-Fi Networks*
- *Wi-Fi CERTIFIED™ 802.11n Draft 2.0: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi Networks*
- *Wi-Fi CERTIFIED™ Voice-Personal: Delivering the Best End-User Experience for Voice over Wi-Fi*

International Organization for Standardization (ISO)

The *International Organization for Standardization*, commonly known as the *ISO*, is a global, nongovernmental organization that identifies business, government, and society needs and develops standards in partnership with the sectors that will put them to use. The ISO is responsible for the creation of the Open Systems Interconnection (OSI) model, which has been a standard reference for data communications between computers since the late 1970s.

Why Is It ISO and Not IOS?

ISO is not a mistyped acronym. It is a word derived from the Greek word *isos*, meaning *equal*. Because acronyms can be different from country to country, based on varying translations, the ISO decided to use a word instead of an acronym for its name. With this in mind, it is easy to see why a standards organization would give itself a name that means *equal.*

The OSI model is the cornerstone of data communications, and learning to understand it is one of the most important and fundamental tasks a person in the networking industry can undertake.

The layers of the OSI model are as follows:

- Layer 7, Application
- Layer 6, Presentation
- Layer 5, Session
- Layer 4, Transport
- Layer 3, Network
- Layer 2, Data-Link
  - LLC sublayer
  - MAC sublayer
- Layer 1, Physical

The IEEE 802.11-2007 standard defines communication mechanisms only at the Physical layer and MAC sublayer of the Data-Link layer of the OSI model. How 802.11 technology is used at these two OSI layers is discussed in detail throughout this book.

NOTE

You should have a working knowledge of the OSI model for both this book and the CWNA exam. Make sure you understand the seven layers of the OSI model and how communications take place at the different layers. If you are not comfortable with the concepts of the OSI model, spend some time reviewing it on the Internet or from a good networking fundamentals book prior to taking the CWNA test.

NOTE

More information about the ISO can be found at `www.iso.org`.

Core, Distribution, and Access

If you have ever taken a networking class or read a book about network design, you have probably heard the terms *core*, *distribution*, and *access* when referring to networking architecture. Proper network design is imperative no matter what type of network topology is used. The core of the network is the high-speed backbone or the superhighway of the network. The goal of the core is to carry large amounts of information between key data centers or distribution areas, just as superhighways connect cities and metropolitan areas.

The core layer does not route traffic nor manipulate packets but rather performs high-speed switching. Redundant solutions are usually designed at the core layer to ensure the fast and reliable delivery of packets. The distribution layer of the network routes or directs traffic toward the smaller clusters of nodes or neighborhoods of the network.

The distribution layer routes traffic between virtual LANs (VLANs) and subnets. The distribution layer is akin to the state and county roads that provide medium travel speeds and distribute the traffic within the city or metropolitan area.

The access layer of the network is responsible for slower delivery of the traffic directly to the end user or end node. The access layer mimics the local roads and neighborhood streets that are used to reach your final address. The access layer ensures the final delivery of packets to the end user. Remember that speed is a relative concept.

Because of traffic load and throughput demands, speed and throughput capabilities increase as data moves from the access layer to the core layer. The additional speed and throughput tends to also mean higher cost.

Just as it would not be practical to build a superhighway so that traffic could travel between your neighborhood and the local school, it would not be practical or efficient to build a two-lane road as the main thoroughfare to connect two large cities such as New York and Boston. These same principles apply to network design. Each of the network layers—core, distribution, and access—are designed to provide a specific function and capability to the network. It is important to understand how wireless networking fits into this network design model.

Wireless networking can be implemented as either point-to-point or point-to-multipoint solutions. Most wireless networks are used to provide network access to the individual client stations and are designed as point-to-multipoint networks. This type of implementation is designed and installed on the access layer, providing connectivity to the end user. 802.11 wireless networking is most often implemented at the access layer. In Chapter 10, "Wireless Devices," you will learn about the difference between *autonomous access points* and the centralized *WLAN controller* solutions that utilize *lightweight access points*. All access points are deployed at the access layer; however, lightweight access points tunnel 802.11 wireless traffic to WLAN controllers that are typically deployed at the distribution or core layer.

Wireless bridge links are typically used to provide connectivity between buildings in the same way that county or state roads provide distribution of traffic between neighborhoods. The purpose of wireless bridging is to connect two separate, wired networks wirelessly. Routing data traffic between networks is usually associated with the distribution layer. Wireless bridge links cannot typically meet the speed or distance requirements of the core layer, but they can be very effective at the distribution layer. An 802.11 bridge link is an example of wireless technology being implemented at the distribution layer.

Although wireless is not typically associated with the core layer, you must remember that speed and distance requirements vary greatly between large and small companies and that one person's distribution layer could be another person's core layer. Very small companies may even implement wireless for all networking, forgoing any wired devices. Higher-bandwidth proprietary wireless bridges and some 802.11 mesh network deployments could be considered an implementation of wireless at the core layer.

Communications Fundamentals

Although the CWNA certification is considered one of the entry-level certifications in the Certified Wireless Network Professional (CWNP) wireless certification program, it is by no means an entry-level certification in the computing industry. Most of the candidates for the CWNA certificate have experience in other areas of information technology. However, the background and experience of these candidates varies greatly.

Unlike professions for which knowledge and expertise is learned through years of structured training, most computer professionals have followed their own path of education and training.

When people are responsible for their own education, they typically will gain the skills and knowledge that are directly related to their interests or their job. The more-fundamental knowledge is often ignored because it is not directly relevant to the tasks at hand. Later, as their knowledge increases and they become more technically proficient, people realize that they need to learn about some of the fundamentals.

Many people in the computer industry understand that in data communications, bits are transmitted across wires or waves. They even understand that some type of voltage change or wave fluctuation is used to distinguish the bits. When pressed, however, many of these same people have no idea what is actually happening with the electrical signals or the waves.

In the following sections, you will review some fundamental communications principles that directly and indirectly relate to wireless communications. Understanding these concepts will help you to better understand what is happening with wireless communications and to more easily recognize and identify the terms used in this profession.

Understanding Carrier Signals

Because data ultimately consists of bits, the transmitter needs a way of sending both 0s and 1s to transmit data from one location to another. An AC or DC signal by itself does not perform this task. However, if a signal fluctuates or is altered, even slightly, the signal can be interpreted so that data can be properly sent and received. This modified signal is now capable of distinguishing between 0s and 1s and is referred to as a *carrier signal*. The method of adjusting the signal to create the carrier signal is called *modulation*.

Three components of a wave that can fluctuate or be modified to create a carrier signal are amplitude, frequency, and phase.

NOTE This chapter reviews the basics of waves as they relate to the principles of data transmission. Chapter 2, "Radio Frequency Fundamentals," covers radio waves in much greater detail.

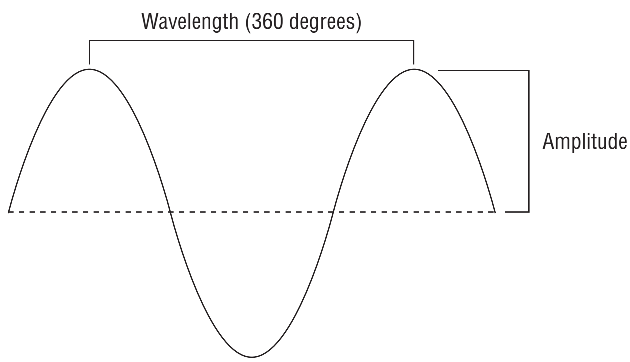
All radio-based communications use some form of modulation to transmit data. To encode the data in a signal sent by AM/FM radios, cellular telephones, and satellite television, some type of modulation is performed on the radio signal that is being transmitted. The average person typically is not concerned with how the signal is modulated, only that the device functions as expected. However, to become a better wireless network administrator, it is useful to have a better understanding of what is actually happening when two stations communicate. The rest of this chapter provides an introduction to waves as a basis for understanding carrier signals and data encoding and introduces you to the fundamentals of encoding data.

Amplitude and Wavelength

RF communication starts when radio waves are generated from an RF transmitter and picked up or "heard" by a receiver at another location. RF waves are similar to the waves that you see in an ocean or lake. Waves are made up of two main components: wavelength and amplitude (see Figure 1.3).

Amplitude is the height, force, or power of the wave. If you were standing in the ocean as the waves came to shore, you would feel the force of a larger wave much more than you would a smaller wave. Transmitters do the same thing, but with radio waves. Smaller waves are not as noticeable as bigger waves. A bigger wave generates a much larger electrical signal picked up by the receiving antenna. The receiver can then distinguish between highs and lows.

FIGURE 1.3 This drawing shows the wavelength and amplitude of a wave.



Wavelength is the distance between similar points on two back-to-back waves. When measuring a wave, the wavelength is typically measured from the peak of a wave to the peak of the next wave. Amplitude and wavelength are both properties of waves.

Frequency

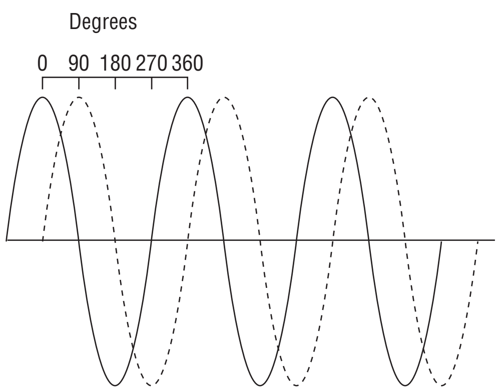
Frequency describes a behavior of waves. Waves travel away from the source that generates them. How fast the waves travel, or more specifically, how many waves are generated over a 1-second period of time, is known as frequency. If you were to sit on a pier and count how often a wave hits it, you could tell someone how frequently the waves were coming to shore. Think of radio waves in the same way; however, radio waves travel much faster than the waves in the ocean. If you were to try to count the radio waves that are used in wireless networking, in the time it would take for one wave of water to hit the pier, several billion radio waves would have also hit the pier.

Phase

Phase is a relative term. It is the relationship between two waves with the same frequency. To determine phase, a wavelength is divided into 360 pieces referred to as *degrees* (see Figure 1.4). If you think of these degrees as starting times, then if one wave begins at the 0 degree point and another wave begins at the 90 degree point, these waves are considered to be 90 degrees out of phase.

In an ideal world, waves are created and transmitted from one station and received perfectly intact at another station. Unfortunately, RF communications do not occur in an ideal world. There are many sources of interference and many obstacles that will affect the wave in its travels to the receiving station. In Chapter 2, we'll introduce you to some of the outside influences that can affect the integrity of a wave and your ability to communicate between two stations.

FIGURE 1.4 This drawing shows two waves that are identical; however, they are 90 degrees out of phase with each other.



Time and Phase

Suppose you have two stopped watches and both are set to noon. At noon you start your first watch, and then you start your second watch 1 hour later. The second watch is 1 hour behind the first watch. As time goes by, your second watch will continue to be 1 hour behind. Both watches will maintain a 24-hour day, but they are out of synch with each other. Waves that are out of phase behave similarly. Two waves that are out of phase are essentially two waves that have been started at two different times. Both waves will complete full 360-degree cycles, but they will do it out of phase, or out of synch with each other.

Understanding Keying Methods

When data is sent, a signal is transmitted from the transceiver. In order for the data to be transmitted, the signal must be manipulated so that the receiving station has a way of distinguishing 0s and 1s. This method of manipulating a signal so that it can represent multiple pieces of data is known as a *keying method*. A keying method is what changes a signal into a carrier signal. It provides the signal with the ability to encode data so that it can be communicated or transported.

There are three types of keying methods that are reviewed in the following sections: amplitude-shift keying (ASK), frequency-shift keying (FSK), and phase-shift keying (PSK). These keying methods are also referred to as *modulation techniques*. Keying methods use two different techniques to represent data:

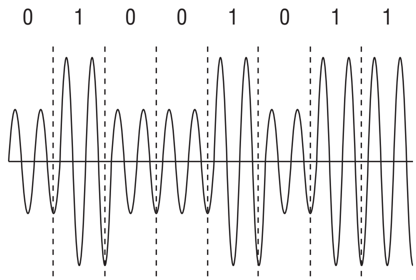
Current state With current state techniques, the current value (the current state) of the signal is used to distinguish between 0s and 1s. The use of the word *current* in this context does not refer to current as in voltage but rather to current as in the present time. Current state techniques will designate a specific or current value to indicate a binary 0, and another value to indicate a binary 1. At a specific point in time, it is the value of the signal that determines the binary value. For example, you can represent 0s and 1s by using an ordinary door. Once a minute you can check to see whether the door is open or closed. If the door is open, it represents a 0, and if the door is closed, it represents a 1. The current state of the door, open or closed, is what determines 0s or 1s.

State transition With state transition techniques, the change (or transition) of the signal is used to distinguish between 0s and 1s. State transition techniques may represent a 0 by a change in a wave's phase at a specific time, whereas a 1 would be represented by no change in wave's phase at a specific time. At a specific point in time, it is the presence of a change or the lack of presence of a change that determines the binary value. The upcoming "phase-shift keying" section provides examples of this in detail, but a door can be used again to provide a simple example. Once a minute you check the door. In this case, if the door is moving (opening or closing), it represents a 0, and if the door is still (either open or closed), it represents a 1. In this example, the state of transition (moving or not moving) is what determines 0s or 1s.

Amplitude-shift keying

Amplitude-shift keying (ASK) varies the amplitude, or height, of a signal to represent the binary data. ASK is a current state technique, where one level of amplitude can represent a 0 bit and another level of amplitude can represent a 1 bit. Figure 1.5 shows how a wave can modulate an ASCII letter *K* by using amplitude-shift keying. The larger amplitude wave is interpreted as a binary 1, and the smaller amplitude wave is interpreted as a binary 0.

FIGURE 1.5 An example of amplitude-shift keying (ASCII code of an uppercase *K*)



This shifting of amplitude determines the data that is being transmitted. The way the receiving station performs this task is to first divide the signal being received into periods of time known as *symbol periods*. The receiving station then samples or examines the wave during this symbol period to determine the amplitude of the wave. Depending on the value of the wave's amplitude, the receiving station can determine the binary value.

As you will learn later in this book, wireless signals can be unpredictable and also subject to interference from many sources. When noise or interference occurs, it usually affects the amplitude of a signal. Because a change in amplitude due to noise could cause the receiving station to misinterpret the value of the data, ASK has to be used cautiously.

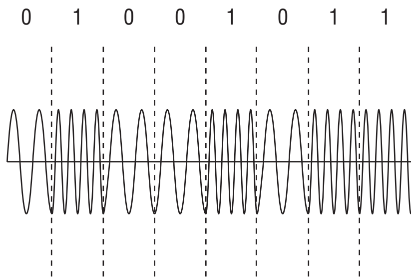
Frequency-shift keying

Frequency-shift keying (FSK) varies the frequency of the signal to represent the binary data. FSK is a current state technique, where one frequency can represent a 0 bit and another frequency can represent a 1 bit (Figure 1.6). This shifting of frequency determines the data that is being transmitted. When the receiving station samples the signal during the symbol period, it determines the frequency of the wave, and depending on the value of the frequency, the station can determine the binary value.

Figure 1.6 shows how a wave can modulate an ASCII letter *K* by using frequency-shift keying. The faster frequency wave is interpreted as a binary 1, and the slower frequency wave is interpreted as a binary 0.

FSK is used in some of the legacy deployments of 802.11 wireless networks. With the demand for faster communications, FSK techniques would require more-expensive technology to support faster speeds, making it less practical.

FIGURE 1.6 An example of frequency-shift keying (ASCII code of an uppercase *K)*



Why Haven't I Heard about Keying Methods Before?

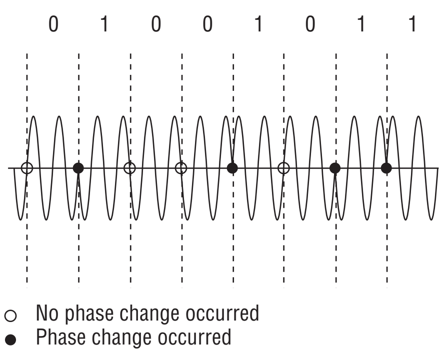
You might not realize it, but you *have* heard about keying methods before. AM/FM radio uses amplitude modulation (AM) and frequency modulation (FM) to transmit the radio stations that you listen to at home or in your automobile. The radio station modulates the voice and music into its transmission signal, and your home or car radio demodulates it.

Phase-shift keying

Phase-shift keying (PSK) varies the phase of the signal to represent the binary data. PSK is a state transition technique, where one phase can represent a 0 bit and another phase can represent a 1 bit. This shifting of phase determines the data that is being transmitted. When the receiving station samples the signal during the symbol period, it determines the phase of the wave and the status of the bit.

Figure 1.7 shows how a wave can modulate an ASCII letter *K* by using phase-shift keying. A phase change at the beginning of the symbol period is interpreted as a binary 1, and the lack of a phase change at the beginning of the symbol period is interpreted as a binary 0.

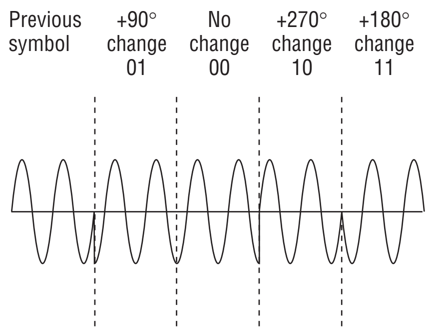
FIGURE 1.7 An example of phase-shift keying (ASCII code of an uppercase *K*)



PSK technology is used extensively for radio transmissions as defined by the 802.11-2007 standard. Typically, the receiving station samples the signal during the symbol period and compares the phase of the current sample with the previous sample and determines the difference. This degree difference, or *differential*, is used to determine the bit value.

More-advanced versions of PSK can encode multiple bits per symbol. Instead of using two phases to represent the binary values, four phases can be used. Each of the four phases is capable of representing two binary values (00, 01, 10, or 11) instead of one (0 or 1), thus shortening the transmission time. When more than two phases are used, this is referred to as *multiple phase-shift keying (MPSK)*. Figure 1.8 shows how a wave can modulate an ASCII letter *K* by using a multiple phase-shift keying method. Four possible phase changes can be monitored, with each phase change now able to be interpreted as 2 bits of data instead of just 1. Notice that there are fewer symbol times in this drawing than there are in the drawing in Figure 1.5.

FIGURE 1.8 An example of multiple phase-shift keying (ASCII code of an uppercase *K*)



Where Else Can I Learn More about 802.11 Technology and the Wi-Fi Industry?

Reading this book from cover to cover is a great way to start understanding Wi-Fi technology. In addition, because of the rapidly changing nature of 802.11 WLAN technologies, the authors of this book would like to recommend these additional resources:

WNN Wi-Fi Net News is a highly respected blog and daily newsletter about all the latest events and happenings in the Wi-Fi industry. Wi-Fi Net News (WNN) has more than 100,000 subscribers and is maintained by blogger Glenn Fleishman. Do yourself a favor and subscribe to Wi-Fi Net News at `www.wifinetnews.com`.

Wi-Fi Alliance As mentioned earlier in this chapter, the Wi-Fi Alliance is the marketing voice of the Wi-Fi industry and maintains all the industry's certifications. The knowledge center section of the Wi-Fi Alliance website, `www.wi-fi.org`, is an excellent resource.

CWNP The Certified Wireless Networking Professional program maintains learning resources such as user forums and a WLAN white paper database. The website `www.cwnp.com` is also the best source of information about all the vendor-neutral CWNP wireless networking certifications.

WLAN vendor websites Although the CWNA exam and this book take a vendor-neutral approach about 802.11 education, the various WLAN vendor websites are often excellent resources for information about specific Wi-Fi networking solutions. Many of the major WLAN vendors are mentioned throughout this book, and a complete listing of most of the major WLAN vendor websites can be found in Chapter 11, "WLAN Deployment and Vertical Markets."

Summary

This chapter explained the history of wireless networking and the roles and responsibilities of the three key organizations involved with the wireless networking industry:

- FCC and other regulatory domain authorities
- IEEE
- Wi-Fi Alliance

To provide a basic understanding of the relationship between networking fundamentals and 802.11 technologies, we discussed these concepts:

- OSI model
- Core, distribution, and access

To provide a basic knowledge of how wireless stations transmit and receive data, we introduced some of the components of waves and modulation:

- Carrier signals
- Amplitude
- Wavelength
- Frequency
- Phase
- Keying methods, including ASK, FSK, and PSK

When troubleshooting RF communications, having a solid knowledge of waves and modulation techniques can help you understand the fundamental issues behind communications problems and hopefully help lead you to a solution.

Exam Essentials

Know the three industry organizations. Understand the roles and responsibilities of the regulatory domain authorities, the IEEE, and the Wi-Fi Alliance.

Understand core, distribution, and access. Know where 802.11 technology is deployed in fundamental network design.

Understand wavelength, frequency, amplitude, and phase. Know the definitions of each RF characteristic.

Understand the concepts of modulation. ASK, FSK, and PSK are three carrier signal modulation techniques.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

access
amplitude
amplitude-shift keying (ASK)
autonomous access points
carrier signal
core
distribution
Federal Communications Commission (FCC)
frequency
frequency-shift keying (FSK)
High Throughput (HT)
Institute of Electrical and Electronics Engineers (IEEE)
International Organization for Standardization (ISO)
International Telecommunication Union Radiocommunication Sector (ITU-R)
keying method
lightweight access points
modulation
phase
phase-shift keying (PSK)
radio frequency (RF)
regulatory domain authority
robust security network (RSN)
spread spectrum
wavelength
Wi-Fi
Wi-Fi Alliance
wireless local area network (WLAN)
WLAN controllers

Review Questions

1. 802.11 technology is typically deployed at which fundamental layer of network architecture?
   A. Core
   B. Distribution
   C. Access
   D. Network

2. Which organization is responsible for enforcing maximum transmit power rules in an unlicensed frequency band?
   A. IEEE
   B. Wi-Fi Alliance
   C. ISO
   D. IETF
   E. None of the above

3. 802.11 wireless bridge links are typically associated with which network architecture layer?
   A. Core
   B. Distribution
   C. Access
   D. Network

4. The 802.11-2007 standard was created by which organization?
   A. IEEE
   B. OSI
   C. ISO
   D. Wi-Fi Alliance
   E. FCC

5. What organization ensures interoperability of WLAN products?
   A. IEEE
   B. ITU-R
   C. ISO
   D. Wi-Fi Alliance
   E. FCC

6. What type of signal is required to carry data?
   - **A.** Communications signal
   - **B.** Data signal
   - **C.** Carrier signal
   - **D.** Binary signal
   - **E.** Digital signal
7. Which keying method is most susceptible to interference from noise?
   - **A.** FSK
   - **B.** ASK
   - **C.** PSK
   - **D.** DSK
8. Which sublayer of the OSI model's Data-Link layer is used for communication between 802.11 radios?
   - **A.** LLC
   - **B.** WPA
   - **C.** MAC
   - **D.** FSK
9. The term *Wi-Fi* is an acronym for which of these phrases?
   - **A.** Wireless fundamentals
   - **B.** Wireless hi-fidelity
   - **C.** Wireless fidelity
   - **D.** Wireless functionality
   - **E.** None of the above
10. The Wi-Fi Alliance is responsible for which of the following certification programs? (Choose all that apply.)
    - **A.** WPA2
    - **B.** WEP
    - **C.** 802.11-2007
    - **D.** WMM
    - **E.** PSK
11. Which wave properties can be modulated to encode data? (Choose all that apply.)
    - **A.** Amplitude
    - **B.** Frequency
    - **C.** Phase
    - **D.** Wavelength

12. The IEEE 802.11-2007 standard defines communication mechanisms at which layers of the OSI model? (Choose all that apply.)

A. Network

B. Physical

C. Transport

D. Application

E. Data-Link

F. Session

13. The height or power of a wave is known as what?

A. Phase

B. Frequency

C. Amplitude

D. Wavelength

14. Global spectrum management is tasked to what organization?

A. FCC

B. Wi-Fi Alliance

C. ITU-R

D. IEEE

15. A modulated signal capable of carrying data is known as what?

A. Data transmission

B. Communications channel

C. Data path

D. Carrier signal

16. Which of the following wireless communications parameters and usage are typically governed by a local regulatory authority? (Choose all that apply.)

A. Frequency

B. Bandwidth

C. Maximum transmit power

D. Maximum EIRP

E. Indoor/outdoor usage

17. The Wi-Fi Alliance is responsible for which of the following certification programs? (Choose all that apply.)

A. WECA

B. Voice Personal

C. 802.11v

D. WAVE

E. WMM-PS

18. A wave is divided into degrees. How many degrees make up a complete wave?

A. 100

B. 180

C. 212

D. 360

19. What are the advantages of using unlicensed frequency bands for RF transmissions? (Choose all that apply.)

A. There are no government regulations.

B. There is no financial cost.

C. Anyone can use the frequency band.

D. There are no rules.

20. The OSI model consists of how many layers?

A. Four

B. Six

C. Seven

D. Nine

Answers to Review Questions

1. C. 802.11 wireless networking is typically used to connect client stations to the network via an access point. Autonomous and lightweight access points are deployed at the access layer, not the core or distribution layer. The Physical layer is a layer of the OSI model, not a network architecture layer.

2. E. RF communications are regulated differently in many regions and countries. The local regulatory domain authorities of individual countries or regions define the spectrum policies and transmit power rules.

3. B. 802.11 wireless bridge links are typically used to perform distribution layer services. Core layer devices are usually much faster than 802.11 wireless devices, and bridges are not used to provide access layer services. The Network layer is a layer of the OSI model, not a network architecture layer.

4. A. The Institute of Electrical and Electronics Engineers (IEEE) is responsible for the creation of all of the 802 standards.

5. D. The Wi-Fi Alliance provides certification testing, and when a product passes the test, it receives a Wi-Fi Interoperability Certificate.

6. C. A carrier signal is a modulated signal that is used to transmit binary data.

7. B. Because of the effects of noise on the amplitude of a signal, amplitude-shift keying (ASK) has to be used cautiously.

8. C. The IEEE 802.11-2007 standard defines communication mechanisms at only the Physical layer and MAC sublayer of the Data-Link layer of the OSI model. The Logical Link Control (LLC) sublayer of the Data-Link layer is not defined by the 802.11-2007 standard. WPA is a security certification. FSK is a modulation method.

9. E. The most common assumption is that that *Wi-Fi* is an acronym for *wireless fidelity*. The problem is that there is no such thing as wireless fidelity, which is in fact a meaningless term that is similar to high fidelity. Wi-Fi is simply a brand marketing name that is used by the Wi-Fi Alliance to promote 802.11 WLAN technology.

10. A, D. 802.11-2007 is the IEEE standard, and WEP (Wired Equivalent Privacy) is defined as part of the IEEE 802.11-2007 standard. PSK is not a standard; it is an encoding technique. Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification program that enables Wi-Fi networks to prioritize traffic generated by different applications. WPA2 is a certification program that defines Wi-Fi security mechanisms.

11. A, B, C. The three keying methods that can be used to encode data are amplitude-shift keying (ASK), frequency-shift keying (FSK), and phase-shift keying (PSK).

12. B, E. The IEEE 802.11-2007 standard defines communication mechanisms at only the Physical layer and MAC sublayer of the Data-Link layer of the OSI model.

13. C. Height or power are two terms that describe the amplitude of a wave. Frequency is how often a wave repeats itself. Wavelength is the actual length of the wave, typically measured from peak to peak. Phase refers to the starting point of a wave in relation to another wave.

14. C. The International Telecommunication Union Radiocommunication Sector (ITU-R) has been tasked with global spectrum management.

15. D. A carrier signal is a signal that has been modulated to carry data.

16. A, B, C, D, E. All of these are typically regulated by the local or regional RF regulatory authority.

17. B, E. The Wi-Fi Alliance maintains certification programs to ensure vendor interoperability. Voice Personal is a certification program that defines enhanced support for voice applications in residential and small-business Wi-Fi networks. WMM-PS is a certification program that defines methods to conserve battery power for devices using Wi-Fi radios by managing the time the client device spends in sleep mode.

18. D. A wave is divided into 360 degrees.

19. B, C. The main advantage of an unlicensed frequency is that permission to transmit on the frequency is free and anyone can use the unlicensed frequency. Although there are no financial costs, you still must abide by transmission regulations and other restrictions. The fact that anyone can use the frequency band is also a disadvantage because of overcrowding.

20. C. The OSI model is sometimes referred to as the seven-layer model.