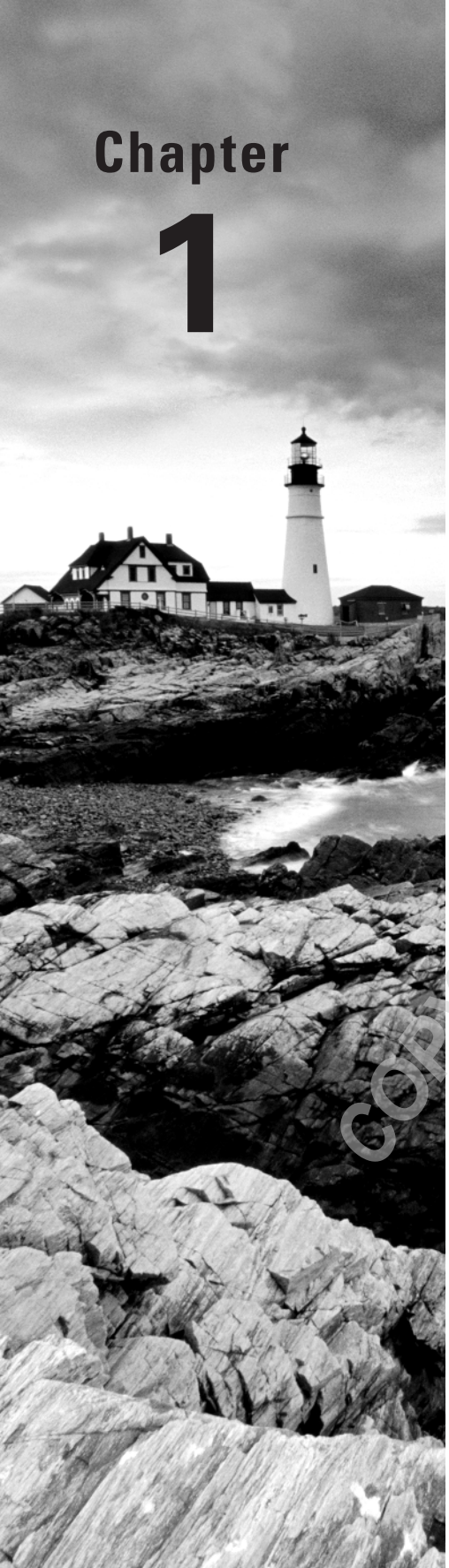


Chapter

1

Introduction to Wireless Local Area Networking

THE FOLLOWING CWTS EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **Identify deployment scenarios for common WLAN network types**
  - Small office/home office (SOHO)
  - Extension of existing networks into remote locations
  - Building-to-building connectivity
  - Public wireless hotspots
  - Mobile office, classroom, industrial, and healthcare
  - Municipal and law-enforcement connectivity
  - Corporate data access and end-user mobility
  - Last-mile data delivery: wireless ISP
  - Transportation networks (trains, planes, automobiles)
- ✓ **Define the roles of the following organizations in providing direction and accountability within the wireless networking industry**
  - IEEE
  - Wi-Fi Alliance
  - Regulatory Domain Governing Bodies

- ✓ **Summarize the basic attributes and advantages of the WLAN standards, amendments, and product certifications**
  - Wi-Fi certification
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11n
  - Wi-Fi Multimedia (WMM) certification
  - WMM Power Save (WMM-PS) certification
  - Wi-Fi Protected Setup (WPS) certification
  - Push-button
  - PIN-based
  - Wi-Fi Protected Access (WPA/WPA2) certification
  - Enterprise
  - Personal

Wireless computer networks have taken computer communication to a new level. This communication technology is the combination of computer local area networking (LAN) and radio frequency (RF) technology. By combining these two technologies, computer users have the opportunity to access and share information in ways that would seem unattainable a few years ago.

This chapter will look at various ways in which wireless local networks are used and deployed. We will also cover organizations responsible for managing and creating wireless LAN standards. Details of the 802.11 standard and amendments will be discussed illustrating the communications and functional aspects. Finally, we will discuss interoperability certifications available for communications, quality of service, and security of IEEE 802.11 wireless networks.

Common WLAN Deployment Scenarios

The availability of wireless LAN technology has increased while the cost continues to decrease, making wireless LANs a viable solution for many business models, including small offices, home offices, and personal use. This chapter will look at scenarios in which wireless networking is used, and provide an overview of standards-based solutions and interoperability certifications. The following are some common applications utilizing wireless local area networks (WLANs):

- Small office/home office (SOHO)
- Enterprise: corporate data access and end-user mobility
- Extension to remote locations
- Mobile office
- Public wireless hotspots
- Classroom
- Healthcare
- Last-mile data delivery: wireless Internet service provider (ISP)
- Industrial
- Municipal and law-enforcement connectivity
- Transportation networks
- Building-to-building connectivity

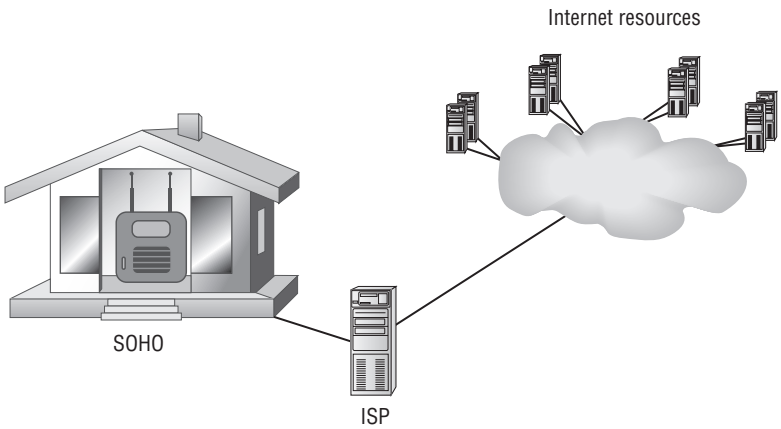
Small Office/Home Office (SOHO)

Many small office/home office (SOHO) businesses have the same needs as those of larger businesses with regard to technology, computer networking, and communication. Computer networking technology is common regardless of the size of the business. Whether there are 1 or 100 employees or even more, many are categorized as small businesses. Wireless LANs can play a major role in small businesses. Many of these locations will have a high speed Internet connection such as DSL (digital subscriber line) or cable modem for access outside the local network.

With the number of work-at-home professionals continuing to grow at a very high rate, the need for wireless networking in this environment is also continuing to grow. The same goes for the small office environment. Deployments such as these typically involve a small number of users. Therefore, the equipment used may be consumer brands sold in consumer electronics and department stores.

Figure 1.1 shows a SOHO configuration with a wireless LAN router connected to an Internet service provider allowing access to the necessary network/Internet resources.

FIGURE 1.1 Example of a SOHO wireless LAN configuration



Enterprise Deployments: Corporate Data Access and End-User Mobility

Enterprise organizations have used wired local area networks for many years. With the increased need for mobility, wireless LANs within enterprise organizations have also increased in popularity. In earlier years, due to lack of interoperability and security features, many enterprise organizations limited wireless LAN deployments to extensions of networks where wired connectivity was either not feasible or too costly. Because of advancements in wireless LAN technology over the recent years, deployments in enterprise organizations are now growing at a rapid pace.

Wireless LANs in the enterprise are used with—but not limited to—client workstation connectivity (desktop and notebook), printers, barcode scanners, voice handsets, and location services. The cost of this technology has decreased while capabilities, performance, and security have increased, making wireless a very attractive solution for many enterprise organizations. The cost savings over hard-wired solutions are enormous, adding to the attractiveness. Finally, wireless connectivity is the only option in some cases, such as mobile Voice over Wi-Fi handsets for voice communications.

Extending Existing Networks with Wireless LAN

Early wireless networking technology was typically deployed to allow an extension of an existing wired network infrastructure. For example, some users who required access to the computer network exceeded the distance the IEEE 802.3 Ethernet standard allowed for a copper-wired connection, therefore other solutions were needed to provide connectivity. Other wired technology, such as fiber optics and leased lines, were sometimes cost prohibitive or not logistically feasible. Wireless local area networks were an excellent alternative.

Mobile Office and Public Wireless Hotspots

Mobility is one of the major benefits of wireless networking. Mobility allows users to access information from a variety of locations, either public or private. One example is wireless hotspots. These days, it is rare to visit any public location, be it a restaurant, hotel, coffee shop, or airport, and not be able to find a public wireless hotspot.

A *wireless hotspot* is defined as a location that offers 802.11 wireless connectivity for devices (computers, PDAs, phones, etc.) to connect to and access the Internet. Many users work from remote locations and require Internet access as part of their job.

A typical wireless hotspot will be configured with at least one wireless LAN router connected to an Internet service provider (ISP). In some cases, this setup could be as simple as a location offering free Wi-Fi Internet access for its customers. More sophisticated hotspots will have several wireless routers or a complete wireless infrastructure and will be connected to a remote billing server that is responsible for collecting revenue from the potential user. In many cases, when a user connects to the hotspot router, they will be prompted with a web page for authentication. At this point they might be asked to enter information such as an account number, username and password, or a credit card number to allow usage for a limited period of time. In the case of a free hotspot, typically this web page lists terms and conditions the user agrees to prior to accessing the Internet. This type of web page configuration is known as a *captive portal*.

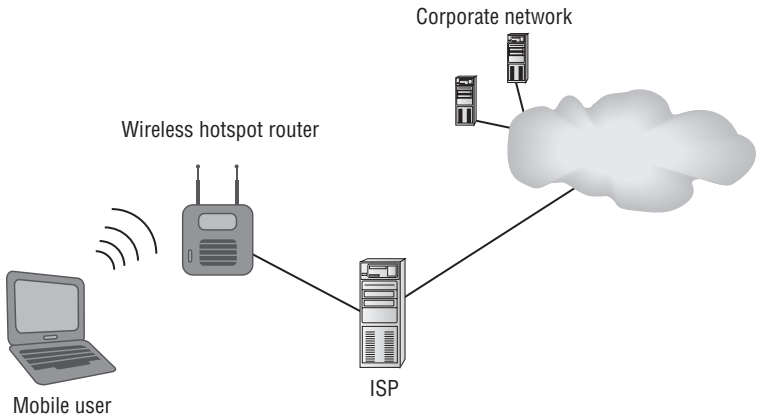
Wireless hotspots can raise security concerns for the user. Without a secure connection, all information is passed in clear text through the air via radio frequency, allowing an intruder to capture usernames and passwords, credit card numbers, or other information that could lead to identity theft. Most hotspots do not have the capability to provide a secure connection for the user from their computer or wireless device to the wireless router or network. The secure connection then becomes the responsibility of the user. Many corporations

allow employees to work remotely from wireless hotspot connections. In this case, usually a *virtual private network* (VPN) is used to ensure security. A VPN creates a secure tunnel between the user and the corporate network, allowing for a secure encrypted connection for the user from the wireless hotspot to their corporate network over the Internet or public network.

For users who connect to wireless hotspots, it is very important for their wireless devices to be secured with the appropriate antivirus software, firewall software, and up-to-date operating system patches or service packs. Following these guidelines will help protect the user from attacks when they are connected to and using a wireless hotspot.

Figure 1.2 shows a simple wireless hotspot implementation.

FIGURE 1.2 Wireless hotspot allows users to connect to the Internet from remote locations.



Educational Institutions: Classroom Deployments

Educational institutions can benefit from wireless networking in many ways. Wireless LAN deployments are common in elementary and high schools. Universities have deployed campus-wide wireless LANs amounting to thousands of access points servicing tens of thousands of users on a single campus.

Wireless LAN technology allows for increased mobility in the educational environment, providing huge cost savings on technology refresh. Mobile carts with notebook computers are one example. A high school can deploy infrastructure devices such as access points in classrooms and purchase several mobile carts with notebook or tablet computers to be used when and where needed. This is beneficial since it will save on supplying many classrooms with computers where continual utilization may be low. Some school buildings may be older or historic buildings and installing cabling is not possible or cost prohibitive. Wireless provides the solution.

Healthcare

The growth of wireless LAN deployments in the healthcare industry is quite impressive. Healthcare installations have many challenges when it comes to design, deployment, and support of wireless networking.

Hospitals in many cases run $7 \times 24 \times 365$ days a year. Wireless LANs have numerous applications in hospitals, including:

- Patient registration
- Patient charting
- Prescription automation
- Treatment verification
- Inventory tracking

One of the obstacles to take into consideration is interference. Hospitals use many devices that operate in the unlicensed industrial, scientific, and medical (ISM) RF band. This can create challenges for design and reliability of the wireless network.

Legislative compliance such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) also needs to be taken into consideration when designing wireless installations for healthcare.

Last-Mile Data Delivery: Wireless ISP

Last-mile data delivery is a common term used in telecommunications to describe the connection from a provider to an endpoint such as home or business. (Last-mile is not necessarily a mile in distance.) This can be a costly solution in many applications since each endpoint needs a separate physical connection. Wireless provides a more cost-effective solution for last-mile data delivery.

Some communication technology, such as DSL, has physical limitations that prohibit connections in some cases. It may not be cost effective for telecommunication service providers to supply connections in rural or semi-rural areas due to return on investment. Wireless LANs can service areas that may not be part of a last-mile run. Providing Internet access from a wireless ISP is one application. Things to consider for feasibility are line of site, obstacles, and interference.

Industrial, Municipal, Law Enforcement, and Transportation Networks

Wireless LANs are valuable technology in the industrial, municipal, and law enforcement fields, and in transportation networks.

Some industrial deployments have been using wireless LAN technology for many years, even prior to the development of standards-based solutions. Examples include barcode and scanning solutions for manufacturing, inventory and retail.

Federal and local law enforcement agencies frequently maintain state-of-the-art technology utilizing computer forensics and wireless LAN technology. Technologies that use 19.2 Kbps connectivity are becoming obsolete due to slower data transfer rates. Municipal deployments that include police, fire, utilities, and city or town services are often all connected to a common wireless LAN.

Transportation networks are no exception. Wireless LAN installations are becoming more common in places like commuter buses, trains, and airplanes. Users can connect for free or by paying a nominal fee. This type of connectivity now allows a user to better employ idle time. This is especially helpful to the mobile user or "road warrior" who needs to make the best use of available time.

Building-to-Building Connectivity

Connecting two or more wired LANs together over some distance is often necessary in computer networking. Depending on the topology, this can be an expensive and time-consuming task. Wireless LAN technology is often used as an alternative to copper cable, fiber optics, or leased line connectivity between buildings. Whether connecting two or multiple locations together, point-to-point or point-to-multipoint links can be a quick and cost-effective solution for building-to-building connectivity.

Antenna selection plays an important role in this type of connectivity and will be discussed further in Chapter 6, "WLAN Antennas and Accessories." Other factors to consider in either point-to-point or point-to-multipoint connections are radio frequency and distance, both of which will determine if a link is feasible.

Point-to-Point Link

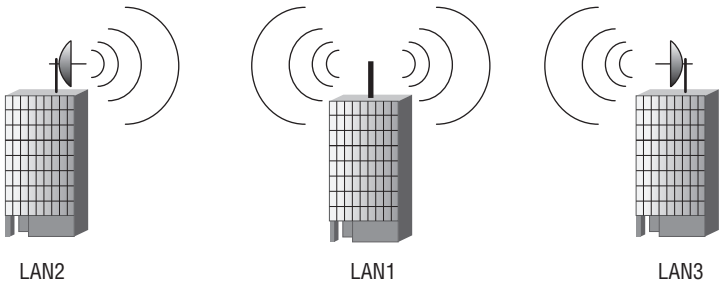
Connecting at least two wired LANs together is known as a *point-to-point link* (see Figure 1.3). Some WLAN equipment manufacturers claim the distance of point-to-point links can be up to 25 miles—sometimes further depending on terrain and other local conditions. These links can serve both wired and wireless users on the connected local area networks. Point-to-point links typically call for semidirectional or highly directional antennas. When an omnidirectional antenna is used in this configuration, it is considered a special case, called a *point-to-multipoint link*. This will be discussed in Chapter 6.

FIGURE 1.3 A point-to-point link using directional antennas

Point-to-Multipoint Link

A network connecting more then two LANs together is known as a *point-to-multipoint link* (see Figure 1.4). This configuration usually consists of one omnidirectional antenna and multiple semi- or highly directional antennas. Point-to-multipoint links are often used in campus-style deployments where connections to multiple buildings or locations may be required.

FIGURE 1.4 A typical point-to-multipoint link using an omnidirectional antenna



Radio Frequency Regulatory Domain Governing Bodies

Wireless networks use radio frequency (RF) to communicate. The RF spectrum needs to be regulated in order to ensure correct use of the allocated frequency bands. The International Telecommunication Union–Radiocommunication Sector (ITU-R) is responsible for global management of RF spectrum, in addition to satellite orbits. This organization currently comprises 191 member states and over 700 sector members. It manages five regions, one of which is Region A, North and South America, Inter-American Telecommunication Commission (CITEL).

Figure 1.5 shows all five regions and the geographic area they encompass.

FIGURE 1.5 ITU-R region map

For additional information, visit www.itu.int/ITU-R.

Table 1.1 shows the five regions, the geographic areas they cover, and the website uniform resource locator (URL) address for each region.

TABLE 1.1 ITU-R Regions, Geographic Locations and Website URLs

Region	Location	URL
Region A	America	www.citel.oas.org
Region B	Western Europe	www.cept.org
Region C	Eastern Europe and Northern Asia	www.rcc.org
Region D	Africa	www.atu-uat.org
Region E	Asia and Australia	www.aptsec.org

United States: Federal Communications Commission (FCC)

The regulatory body that manages RF spectrum for the United States is the *Federal Communications Commission (FCC)*. The FCC, founded in 1934, is responsible for regulating licensed and unlicensed radio frequency spectrum. IEEE 802.11 wireless networks may use licensed or unlicensed RF spectrum for communication. A benefit of using unlicensed radio spectrum is no cost to the end user. The IEEE uses two of three unlicensed RF bands allowed by the FCC:

- 2.4 GHz industrial, scientific, and medical (ISM) band
- 5 GHz Unlicensed National Information Infrastructure (UNII) band

This will be illustrated further in looking at details of standards-based wireless communications.

For additional information, visit www.fcc.gov.

Europe: European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) is a European standards organization responsible for producing standards for information and communications technologies, including fixed, mobile, radio, converged, broadcast, and Internet technologies. ETSI was created by the European Conference of Postal and Telecommunications Administrations (CEPT) in 1988.

In Europe, radio frequency use is managed by CEPT. CEPT develops guidelines and provides national administrations with tools for coordinated European radio frequency spectrum management.

IEEE and Wireless LAN Standards

The *IEEE* (originally known as the *Institute of Electrical and Electronics Engineers*) is a nonprofit organization responsible for generating a variety of technology standards, including those related to information technology. Since 1997 the IEEE has released a series of standards related to WLAN networking.

The IEEE wireless networking standards are described in the order in which they were released. They define communication: range, power, and speed. Some of these standards will be explained more thoroughly later in this book.

For additional information, visit `www.ieee.org`.

802.11

The 802.11 standard, released in 1997, is what defined the wireless LAN communication standards. The data rates used in this standard (1 and 2 Mbps) are considered slow by today's standards and technology.

The IEEE Standard 802.11-2007 (previously known as 802.11ma) is the most current standard. This standard rolled up the 802.11 standard and various amendments such as 802.11a/b/e/g/h/I, and others into one document. However, many in the industry still refer to the original names: 802.11b, 802.11a, 802.11g, and so on.

User and application requirements for 802.11 are discussed in Chapter 4, "Radio Frequency (RF) Fundamentals for Wireless LAN Technology."

The following list provides details such as frequency range, spread spectrum technology, and data rates for the 802.11 standard.

- 2.4 GHz ISM band
- Frequency-hopping spread spectrum (FHSS)
- Direct-sequence spread spectrum (DSSS)
- Infrared (IR)
- 1 and 2 Mbps

Frequency-hopping spread spectrum is considered legacy technology. However, some companies still manufacture a limited line of equipment to support legacy implementations.

802.11b

The 802.11b amendment to the 802.11 standard works in the 2.4–2.5 GHz ISM band. This amendment, released in 1999, specifies high rate DSSS (HR/DSSS)

The 802.11b amendment was released before the 802.11a amendment.

The following list provides details such as frequency range, spread spectrum technology, and data rates for the 802.11b amendment.

- 2.4 GHz ISM band
- Direct-sequence spread spectrum (DSSS)
- High rate–direct-sequence spread spectrum (HR/DSSS)
- 5.5 and 11 Mbps
- Backward compatible to 802.11 DSSS for 1 and 2 Mbps

With the release of the 802.11b amendment, wireless LAN technology became more affordable and mainstream. This amendment introduced two higher rate data speeds of 5.5 and 11 Mbps, making the technology more desirable.

802.11a

This amendment to the 802.11 standard operates in the 5 GHz UNII band. Released in 1999, this standard operates over four frequency ranges in three bands—UNII-1, UNII-2, and UNII-3. UNII-1 is for indoor use only, UNII-2 is for indoor or outdoor use, and UNII-3 may be used indoors or outdoors but is typically used outdoors. The data rates for 802.11a are up to 54 Mbps using orthogonal frequency division multiplexing (OFDM).

The following list provides details such as frequency range, spread spectrum technology, and data rates for the 802.11a amendment.

- 5GHz UNII band
  - 5.150–5.250 GHz UNII-1
  - 5.250–5.350 GHz UNII-2
  - 5.725–5.825 GHz UNII-3
- Orthogonal frequency division multiplexing (OFDM)
- 6, 12, 24 Mbps OFDM required data rates
- 9, 18, 36, 48, and 54 Mbps OFDM data rates are supported but not required.

A benefit to using the 5 GHz UNII band is less interference. Currently, many fewer devices use 5 GHz UNII license-free band than those using the 2.4 GHz ISM band. Less interference means increased performance and reliability.

In late 2003, the FCC made changes regarding the 5 GHz unlicensed band. Additional frequencies above those described in the IEEE 802.11a amendment can now be used for IEEE 802.11 wireless networking. These changes will be discussed further in Chapter 6.

802.11g

This amendment to the 802.11 standard was released in 2003. It operates in the 2.4 GHz ISM band as do 802.11 and 802.11b. This amendment addresses extended data rates with OFDM and is backward compatible to 802.11 and 802.11b.

The following list provides details such as frequency range, spread spectrum technology, and data rates for the 802.11g amendment:

- 2.4 GHz ISM band
- Direct-sequence spread spectrum (DSSS)
- High rate–direct-sequence spread spectrum (HR/DSSS)
- Extended rate physical–orthogonal frequency division multiplexing (ERP-OFDM)
- Packet binary convolutional code (PBCC; optional)
- 1 and 2 Mbps (compatible with DSSS)
- 5.5 and 11 Mbps complementary code keying (CCK; compatible with HR/DSSS)
- 6, 12, 24 Mbps OFDM required data rates
- 9, 18, 36, 48, and 54 Mbps OFDM data rates are supported but not required.

802.11g is backward compatible to 802.11 and 802.11b because it operates in the same 2.4 GHz ISM band and supports the same access methods. One benefit of 802.11g compatibility is many established infrastructures and devices have used 802.11 and 802.11b for years. This allows them to continue to operate as normal with upgrades or replacement as appropriate.

In order to allow the slower DSSS data rates of 1, 2, 5.5, and 11 Mbps to operate in an 802.11g network, the amendment addresses the use of protection mechanisms. These protection mechanisms will degrade the performance of 802.11g clients to some degree when 802.11b radios are present.

Table 1.2 provides a summary and comparison of details regarding the currently released 802.11 communication standards.

TABLE 1.2 Summary of 802.11 Communications Standards and Amendments

Details	802.11	802.11a	802.11b	802.11g
2.4 GHz ISM band	x		x	x
5 GHz UNII bands		x		
FHSS	x			
DSSS	x		x	x
HR/DSSS			x	x
ERP-OFDM				x
OFDM		x		
1 and 2 Mbps	x		x	x
5.5 and 11 Mbps			x	x
6, 9, 12, 18, 24, 36, 48, 54 Mbps		x		x

802.11n

The 802.11n amendment is currently in draft and has not yet been ratified. As of this writing, the 802.11n amendment is expected to be ratified in Q4 2009. However, the 802.11n draft 2.0 is available, and products for both SOHO and enterprise are Wi-Fi certified and available to the market under draft 2.0.

Real World Scenario

How to Maximize the Throughput in an 802.11g Network

In certain cases the only way to maximize the throughput of an 802.11g network is to set the data rates of the access points to support 802.11g data rates only. The tradeoff is that 802.11b devices will not be able to connect to the network because the access point will not recognize the 802.11b data rates. This would work well where backward compatibility to 802.11b is not required and all equipment in use supports 802.11g. An analogy would be a group of individuals all speaking one language. They all understand the same language so they have no need to accommodate a second language.

Due to protection mechanisms defined in the 802.11g amendment, throughput will degrade in an 802.11b/g mixed mode environment when 802.11b devices are present. This is because the 802.11b devices have a maximum data rate of 11 Mbps (HR/DSSS) and they share the medium with the 802.11g devices that have a maximum data rate of 54 Mbps (OFDM). Think of the language analogy. If a group of individuals are speaking two different languages, a translator may be required. A discussion among the group would take longer because the translator would need to translate the languages. Likewise, protection mechanisms will have an impact on the throughput for the 802.11g devices since the 2.4 GHz medium is shared. If there are no 802.11b devices in the radio range of an access point in an 802.11b/g mixed mode environment, then protection mechanisms should not affect throughput, since the access point will not have to share the medium with the two different technologies

If you do not have any 802.11b devices on your network, you can set your access point to 802.11g only mode by disabling the 802.11b data rates. In this configuration, your 802.11g devices will perform better since protection mechanisms will not be enabled. However, if there are any 802.11b devices not belonging to your network in the "listening" range of the access point, data collisions will increase at the access point. This is because 802.11b and 802.11g operate in the same RF range, and the 802.11g (OFDM) access point does not understand the 802.11b (HR/DSSS) transmissions. (It sees them as RF noise.) In this configuration, overall throughput will still exceed that of an access point set to 802.11b/g mixed mode in the presence of 802.11b devices. The access point will hear the 802.11b transmissions, but they will not be serviced because they are only seen as RF noise. Thus they will have less impact on throughput.

The following list provides details such as frequency range, spread spectrum technology, and data rates for the 802.11n amendment.

- 2.4 GHz ISM band
- 5 GHz UNII bands
- MIMO (multiple input multiple output)
- Up to 600 Mbps
- HT-OFDM

Additional IEEE 802.11 Amendments

In addition to communications, the IEEE creates amendments regarding specific functionality including security and quality of service. The following amendments discuss some of these functions.

802.11e

The original 802.11 standard lacked quality of service (QoS) functionality features. In the original 802.11 standard, Point Coordination Function (PCF) mode provided some level of QoS. PCF mode is a function of the access point and allows for polling of connected client devices. This creates a contention-free period for data transmissions and provides QoS-like functionality. However, few if any vendors implemented this mode of operation.

The 802.11e amendment defines enhancements for QoS in wireless LANs. 802.11e introduced a new coordination function, hybrid coordination function (HCF). HCF defines traffic classes and assigns a priority to the information to be transmitted. For example, voice traffic is given a higher priority than data traffic, such as information being sent to a printer.

802.11i

The 802.11i amendment addresses advanced security solutions for wireless LAN, since the original 802.11 standard was known for several security weaknesses.

Manufacturers of WLAN equipment addressed the following security features:

- Service Set Identifier (SSID) Hiding
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

Each of these had known vulnerabilities, allowing for security weaknesses in 802.11 wireless LANs. The 802.11i amendment addressed these weaknesses by several enhancements, discussed in Chapter 10, "WLAN Security."

Interoperability Certifications

By creating standards, the IEEE is encouraging technology progression. Vendors often implement wireless devices and networks in a proprietary manner, within or outside the standard. This model often leads to a lack of interoperability among devices. In the wireless community, such practices are not widely accepted. Users want all of their devices to function well together. The combination of proprietary implementations and user dissatisfaction fostered the creation of interoperability testing and certification.

This section will discuss vendor interoperability certifications related to IEEE 802.11 standard equipment. These certifications address communications, quality of service, and security.

Wi-Fi Alliance

As mentioned in the previous section, the IEEE is responsible for generating the standards for wireless networking. However, equipment manufacturers are not required to provide proof that their equipment is compliant to the standards. Starting with the release of the 802.11b amendment, several early WLAN equipment manufacturers—including Symbol Systems, Aironet, and Lucent—formed an organization known as Wireless Ethernet Compatibility Alliance (WECA) to promote the technology and to provide interoperability testing of wireless LAN equipment manufactured by these and other companies. In 2000, WECA was renamed the *Wi-Fi Alliance*. The term *Wi-Fi* represents a certification and is often misused by people in the industry. Wi-Fi is a registered trademark, originally registered in 1999 by WECA and now registered to the Wi-Fi Alliance.

For additional information, visit `www.wi-fi.org`.

Figure 1.6 shows an example of a Wi-Fi certified logo.

FIGURE 1.6 Wi-Fi Certified logo for devices that are Wi-Fi certified

Wi-Fi Protected Access (WPA) Certification Overview

The *Wi-Fi Protected Access (WPA)* certification was derived from the fact that security in the original 802.11 standard was weak and had many security vulnerabilities. This certification was designed as an interim solution until an amendment to the 802.11 standard addressing security improvements was released. The 802.11i amendment addressed security for the 802.11 family of standards. The bottom line is that WPA is a pre-802.11i certification introducing more advanced security solutions such as Temporal Key Integrity Protocol (TKIP), passphrase, and 802.1X/EAP.

This pre-802.11i certification addressed two options for wireless LAN security. The two options are personal mode and enterprise mode. Personal mode is intended for the small office/home office (SOHO) and home users. Enterprise mode is intended for larger deployments.

Wi-Fi Protected Access 2 (WPA 2.0) Certification Overview

The WPA certification by the Wi-Fi Alliance worked out so well that it was decided to certify wireless LAN hardware after the 802.11i amendment was released. This new certification, known as *Wi-Fi Protected Access 2 (WPA 2.0),* is a post-802.11i certification. Like WPA, WPA 2.0 addresses two options for wireless LAN security: personal mode and enterprise mode. This certification addresses more advanced security solutions and is backward compatible with WPA. We will take a look at both WPA and WPA 2.0 in more detail in Chapter 10.

- The personal mode security mechanism uses a passphrase for authentication, which is intended for SOHO and personal use. The use of a passphrase to generate a 256-bit preshared key provides strong security.
- The enterprise mode mechanism uses 802.1X/EAP for authentication, which is port-based authentication designed for enterprise implementations. 802.1X/EAP provides strong security using external authentication and Extensible Authentication Protocol (EAP). This works well as a replacement for legacy 802.11 security solutions.

Table 1.3 provides a high-level description of the WPA and WPA 2.0 certifications.

TABLE 1.3 DETAILS OF THE WPA AND WPA 2.0 CERTIFICATIONS

Wi-Fi Alliance Security Mechanism	Authentication Mechanism	Cipher Suite/ Encryption Mechanism
WPA – Personal	Passphrase	TKIP/RC4
WPA – Enterprise	802.1X/EAP	TKIP/RC4
WPA 2.0 – Personal	Passphrase	CCMP/AES or TKIP/RC4
WPA 2.0 – Enterprise	802.1X/EAP	CCMP/AES or TKIP/RC4

Wi-Fi Multimedia (WMM) Certification Overview

The *Wi-Fi Multimedia (WMM)* certification was designed as a proactive certification for the 802.11e amendment to the 802.11 standard. As mentioned earlier in this chapter, the 802.11e amendment addresses quality of service in wireless LANs. The WMM certification verifies the validity of features of the 802.11e amendment and allows for a vendor-neutral approach to quality of service.

Quality of service is needed to ensure delivery of information for time-sensitive, time-bounded applications such as voice and streaming video. If a wireless network user were to send a file to a printer or save a file to a server, it is unlikely they would notice any minor latency. However, in an application that is tuned to the human senses such as hearing or eyesight, latency would more likely be noticeable.

Wi-Fi Multimedia Power Save (WMM-PS) Certification Overview

Wi-Fi Multimedia Power Save (WMM-PS) is designed for mobile devices and specific applications that require advanced power-save mechanisms for extended battery life. Listed are some of these devices and applications that benefit from it:

- Voice over IP (VoIP) phones
- Notebook computers
- PDAs
- Headsets
- Mice
- Keyboards

Power-save mechanisms allow devices to conserve battery power by "dozing" for short periods of time. Depending on the application, performance could suffer to some degree with power-save features enabled. WMM Power Save consumes less power by allowing devices to spend more time in a "dozing" state—an improvement over legacy power save mode that at the same time improves performance by minimizing transmission latency.

Wi-Fi Protected Setup (WPS) Certification Overview

Wi-Fi Protected Setup (WPS) was derived from the fact that small office and home office users wanted a simple way to provide the best security possible for their installations without the need for extensive technical knowledge of wireless networking. Wi-Fi Protected Setup provides strong out-of-the-box setup adequate for many SOHO implementations.

The Wi-Fi Protected Setup certification requires support for two types of authentication that enable users to automatically configure network names and strong WPA2 data encryption and authentication:

- Push-button configuration (PBC)
- PIN-based configuration, based on a personal identification number

Support for both PIN and PBC configurations are required for access points; client devices at a minimum must support PIN. A third, optional method, Near Field Communication (NFC) tokens, is also supported.

Summary

This chapter discussed many applications in which wireless LANs are currently used, from small office/home office to corporate deployments and last-mile connectivity. Standards-based wireless deployments continue to grow at a fast pace, replacing proprietary and legacy-based implementations.

The IEEE is an organization that creates standards and amendments used for 802.11 wireless LANs. This chapter described the released communication standards that address range, power, and speed including:

- 802.11a
- 802.11b
- 802.11g

Also some details regarding 802.11n were discussed which at the time of this writing is in draft 2.0.

Standards that addressed quality of service and security were also discussed. The IEEE creates standards based on radio frequency regulations. We also looked at radio frequency regulatory domain governing bodies and their role in regulation of the RF spectrum used for IEEE 802.11 wireless networking.

As discussed in this chapter, the Wi-Fi Alliance is an organization addressing interoperability testing for equipment manufactured to the IEEE standards. This testing results in a variety of certifications for

- Communication
- Quality of service
- Security

Key Terms

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

captive portal

Federal Communications Commission (FCC)

IEEE (Institute of Electrical and Electronics Engineers)

last-mile data delivery

point-to-multipoint link

point-to-point link

virtual private network
Wi-Fi Alliance
Wi-Fi Multimedia (WMM)
Wi-Fi Multimedia Power Save (WMM-PS)
Wi-Fi Protected Access (WPA)
Wi-Fi Protected Access 2 (WPA 2.0)
Wi-Fi Protected Setup (WPS)
wireless hotspot

Exam Essentials

Understand details of common WLAN applications. These common WLAN applications can include small office/home office (SOHO), corporate data access, end-user mobility, and building-to-building connectivity.

Understand the function and roles of organizations that are responsible for the regulation and development of WLAN technology. The IEEE, FCC, ETSI, ITU-R, and Wi-Fi Alliance play important roles with wireless technology. Know the function and role of each organization.

Remember frequency ranges, data rates, and spread spectrum technologies for IEEE 802.11 communication standards. Understand the details of the 802.11, 802.11b, 802.11a, 802.11g, and 802.11n standard and amendments. It is important to know the supported data rates and operating radio frequency of each.

Know the purpose of IEEE specific function amendments. Be familiar with the details of 802.11e and 802.11i specific function amendments. Know that 802.11e is for quality of service and 802.11i addresses security.

Understand the differences among interoperability certifications by the Wi-Fi Alliance. Know the purpose of the WPA, WPA 2.0, WMM, WMM-PS, and WPS Wi-Fi Alliance certifications. Understand which address security, quality of service, and power-save features.

Review Questions

1. Point-to-point links typically use which antenna types? (Choose 2.)
   - **A.** Semidirectional
   - **B.** Omnidirectional
   - **C.** Highly directional
   - **D.** Long range omnidirectional
2. Typically a point-to-multipoint link consists of ____ connections.
   - **A.** Two
   - **B.** Three
   - **C.** Four
   - **D.** Five
3. True or false? A point-to-point link always uses an omnidirectional antenna.
   - **A.** True
   - **B.** False
4. What organization is responsible for unlicensed frequency band regulation in the United States?
   - **A.** ETSI
   - **B.** Wi-Fi Alliance
   - **C.** IEEE
   - **D.** FCC
   - **E.** WPA
5. 802.11g LANs operate in what frequency range?
   - **A.** 900 MHz
   - **B.** 5.15–5.25 GHz
   - **C.** 5.25–5.35 GHz
   - **D.** 2.4–2.5 GHz
6. Which of the following organizations is responsible for standards compliance?
   - **A.** FCC
   - **B.** ETSI
   - **C.** IEEE
   - **D.** WPA2
   - **E.** Wi-Fi Alliance

7. 802.11a uses which spread spectrum technology?
   - **A.** ERP-OFDM
   - **B.** HR/DSSS
   - **C.** OFDM
   - **D.** FHSS

8. 802.11b is capable of which of the following data rates? (Choose 3.)
   - **A.** 1 Mbps
   - **B.** 6 Mbps
   - **C.** 5.5 Mbps
   - **D.** 11 Mbps
   - **E.** 12 Mbps

9. 802.11g is backward compatible to which of the following IEEE wireless LAN standards? (Choose 2.)
   - **A.** 802.11 DSSS
   - **B.** 802.11a OFDM
   - **C.** 802.11a ERP-OFDM
   - **D.** 802.11b HR/DSSS
   - **E.** 802.3af

10. In the 802.11a amendment, the UNII-3 band can be used for which of the following WLAN applications?
    - **A.** Indoor and outdoor
    - **B.** Outdoor only
    - **C.** Indoor only
    - **D.** The UNII-3 band cannot be used for WLANs.

11. The 802.11i amendment to the standard addresses which of the following technologies?
    - **A.** Quality of service
    - **B.** DSSS
    - **C.** Security
    - **D.** MIMO

12. Which of the following best describes the Wi-Fi Alliance?
    - **A.** U.S.-based standards organization
    - **B.** Interoperability testing organization
    - **C.** Works with the FCC to verify compliance
    - **D.** Local regulatory body for Europe

13. Which of the following is addressed by the Wi-Fi Multimedia (WMM) certification? (Choose 2.)
    - **A.** Security
    - **B.** WPA and WPA2
    - **C.** QoS
    - **D.** Quality of service

14. Wi-Fi Protected Setup was designed for which of the following wireless applications?
    - **A.** Small office/home office (SOHO) organizations
    - **B.** Enterprise organizations
    - **C.** FCC interoperability
    - **D.** Security organizations

15. The 802.11g standard uses which two spread spectrum technologies?
    - **A.** FHSS
    - **B.** OFDM
    - **C.** ERP-OFDM
    - **D.** DSSS
    - **E.** MIMO

16. WPA was developed as an interim solution for which amendment to the 802.11 standard?
    - **A.** 802.11a
    - **B.** 802.11n
    - **C.** 802.11e
    - **D.** 802.11i
    - **E.** 802.11g

17. Which of the following is correct regarding 802.11e?
    - **A.** Only operates in the 5 GHz frequency range
    - **B.** Only operates at 1, 2, 5.5, and 11Mbps
    - **C.** Addresses wireless security
    - **D.** Addresses wireless quality of service

18. According to the 802.11a amendment, which of the following data rates are mandatory?
    - **A.** 1, 2, 5.5, and 11 Mbps
    - **B.** 6, 24, and 54 Mbps
    - **C.** 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
    - **D.** 6, 12, and 24 Mbps
    - **E.** 1, 6, 12, and 24 Mbps

19. You support a wireless network for an office of five employees. The installation consists of one access point, three notebook computers, and two desktop computers. The access point and computers in the office have wireless adapters that are Wi-Fi WPA 2.0 Certified. You want to use the highest level security possible without additional cost or administration. Which of the following solutions would be best for this deployment? (Choose 2.)

A. WEP

B. WPA 2.0 personal

C. WPS

D. WMM

E. WPA 2.0 enterprise

20. Which two of the following options are for Wi-Fi Protected Access 2 (WPA 2.0)?

A. Personal mode

B. Protection mode

C. Professional mode

D. Enterprise mode

E. WPA 2 mode

Answers to Review Questions

1. A, C. Semidirectional and highly directional antennas are used for point-to-point links. Omnidirectional antennas are for point-to-multipoint links. Long range omnidirectional antennas do not exist.
2. B. Point-to-multipoint links typically have three or more connections.
3. B. Point-to-multipoint links use omnidirectional antennas, but point-to-point links do not.
4. D. The FCC is the local regulatory body responsible for frequency regulation in the U.S.
5. D. 802.11g LANs operate in the 2.4–2.5 GHz ISM band. 900 MHz is not used with 802.11 wireless LANs, and 5 GHz is 802.11a.
6. E. The Wi-Fi Alliance performs interoperability testing and verifies standards compliance.
7. C. 802.11a uses OFDM; ERP-OFDM is used in 802.11g.
8. A, C, D. 802.11b can use 1, 2, 5.5 and 11 Mbps. 6 and 12 Mbps are used in 802.11a and 802.11g.
9. A, D. 802.11g is backward compatible to DSSS and HR/DSSS
10. A. The UNII-3 band can be used indoors or outdoors, but typically is used outdoors only.
11. C. 802.11i addresses security. 802.11e addresses quality of service.
12. B. Wi-Fi Alliance performs interoperability testing for IEEE 802.11 wireless LAN standards.
13. C, D. Both C and D are both correct since QoS is an acronym for quality of service. WMM is a proactive Wi-Fi Alliance certification for quality of service. WPA and WPA are certifications that address security.
14. A. Wi-Fi Protected Setup was designed with SOHO users in mind.
15. C, D. 802.11g can use ERP-OFDM and DSSS.
16. D. WPA was designed as a pre-802.11i solution for wireless security.
17. D. 802.11e is a specific function amendment addressing quality of service.
18. D. The IEEE requires 6, 12, and 24 Mbps for 802.11a OFDM.
19. B, C. WPA 2.0 Personal and WPS are both designed with the small business in mind.
20. A, D. WPA 2.0 consists of personal mode using passphrase and enterprise mode using 802.1X/EAP.