Chapter 1: Wireless Standards, Organizations, and Applications

Overview

Define the roles of the following organizations:

- Regulatory Domain Governing Bodies
- IEEE
- Wi−Fi Alliance

Identify some of the uses for spread spectrum technologies:

- Wireless LANs, PANs, MANs, and WANs
- Identify technology roles for WLAN technologies

Wireless local area networks (WLANs) are being used very heavily in government and private sector networks today.

The technology needs no introduction from the perspective of awareness, but there is still much to do in the areas of understanding and effective utilization.

Various branches of government have come to see WLAN technology as a value−added solution instead of a threat that is to be avoided.

However, they have also seen the need to implement security, which has led to both good and bad security policies, as reflected in government regulations and memos.

The good policies are born from a proper understanding of the functionality of WLANs, and the bad policies have evolved from errors in the understanding of foundational principles of wireless networks.

The goal of this chapter—and this book—is to take you on a journey that will lead you to a solid foundational knowledge of WLANs. My hope is that fewer mistakes will be made in the areas of security and technology investment as more engineers and administrators are trained in WLAN technology.

When you extend the analysis to health care, private sector organizations, and home environments, the impact of wireless networking technologies greatly increases. There are very few homes remaining in Sweden that do not have at least one wireless device—even if it is a cordless telephone.

There are even fewer businesses that are not taking advantage of the benefits of wireless equipment. In business, this equipment list includes the following items, as well as others that are not listed:

- Cordless phones
- Wireless Voice over IP phones
- Wireless print servers
- Wireless access points, routers, and bridges
- Radio Frequency Identification devices
- Wireless presentation gateways
- Wireless conferencing systems
- Laptop computers, PDAs, and other mobile wireless client devices

Since this list is only partial and represents some of the more common devices implemented, you can see that wireless technology is being used in many beneficial ways.

In this chapter, you will learn about the organizations that guide the WLAN industry and also briefly consider the standards that are used within WLANs.

Next, the four main uses of wireless spread spectrum technology are discussed, leading to an understanding of the applications available.

Finally, you investigate many of the specific ways in which wireless technology is being implemented today.

Roles Organizations Play Within the WLAN Industry

There are three primary categories of organizations that guide the wireless industry. These categories include regulation, standardization, and compatibility.

- The *Federal communications Commission (FCC)* and the European Telecommunications Standards Institute (ETSI) are examples of regulatory bodies.
- The *Institute of Electrical and Electronics Engineers (IEEE)* is an example of a standards development organization, and the *Wi−Fi Alliance* is a compatibility testing and certification group.

It is important to understand what these organizations do, but it is equally important to understand how they work together. As an example, consider the interdependency between the FCC and the IEEE or the relationship between the Wi−Fi Alliance and the IEEE.

The FCC sets the boundaries within which the IEEE may develop standards. The Wi−Fi Alliance tests equipment to certify it as being reasonably interoperable.
These three organizations provide regulation, standardization, and compatibility services for WLAN technologies within the United States.

The benefits to the consumer are clear. When there are regulations in place, such as power output limits, it is easier to implement localized wireless networks with less interference from surrounding networks.

When there are standards in place, such as the IEEE 802.11 standard, it is easier to purchase devices from different vendors that are interoperable.
When there are certifications in place that validate interoperability, consumers can buy products with confidence that those similarly certified devices should be interoperable at some level and fewer man hours are required for compatibility testing.

In the ideal world, we would get all these benefits with exact perfection. In the real world, Interference is reduced, but not eliminated; hardware is interoperable, but not necessarily fully compatible; testing time is reduced, but not completely eliminated.
If you are installing a wireless network in an office, which shares space with other offices, you may still encounter interference, even with the lower output power.

If you are working with devices from different vendors, you may encounter specific compatibility issues outside the standards upon which the devices are based. If you are implementing hardware that has been certified by the Wi−Fi Alliance, you should still test it with your hardware to ensure there are no compatibility issues.
Even with these realities, the benefits that the regulatory, standards, and compatibility organizations have brought to the wireless industry are immeasurable.

Regulatory Domain Governing Bodies

A *regulatory domain* can be defined as a bounded area that is controlled by a set of laws or policies. Currently, there are governing bodies at the city, county, state, and country levels within the United States.

In other countries, governments exist with similar hierarchies or with a single level of authority at the top level of the country. In many cases, these governments have assigned the responsibility of managing communications to a specific organization that is responsible to the government.

In the United States, this organization is the FCC.
In the UK, it is the Office of Communications (OfCom).
In Australia, it is the Australian Communications and Media Authority.

The following sections outline just four of these governing bodies and the roles they play in the wireless networking industry of their respective regulatory domains.

FCC

The Federal Communications Commission (FCC) was born out of the Communications Act of 1934. Charged with the regulation of interstate and international communications by radio, television, cable, satellite, and wire, the FCC has a large body of responsibility.

The regulatory domain covered by the FCC includes all 50 states of the United States as well as the District of Columbia and other U.S. possessions like the Virgin Islands and Guam. Because WLAN devices use radio wave communications, they fall under the regulatory control of the FCC. The factors regulated by the FCC include:

- Radio frequencies available
- Output power levels
- Indoor and outdoor usage

Radio Frequencies Available You will learn more about radio frequencies in Chapters 2 and 3. For now, it is enough to know that a radio frequency is measured in hertz (Hz).

Hertz is the measurement of wave cycles per second; therefore, a radio frequency of 2.412 gigahertz (GHz) cycles 2,412,000 times per second.

The FCC regulates which frequencies may be used within the regulatory domain it manages. For example, the FCC provides two types of license free bands for radio communications: the Industrial Scientific Medical (ISM) bands and the Unlicensed National Information Infrastructure (U–NII—usually pronounced *you knee*) bands.

Currently, there are 11 ISM bands in various frequencies throughout the radio frequency spectrum, but only the one starting at 2.4 GHz is used by IEEE 802.11, and it is the frequency band most familiar to WLAN users.

The four U–NII bands exist in the 5 GHz frequency range, and are all used by IEEE 802.11.

Frequency Band Total Bandwidth License–Free Band

Frequency	BW	Band	Frequency	BW	Band
2400–2500 MHz	100 MHz	ISM	5.15–5.25 GHz	100 MHz	U–NII
5.25–5.35 GHz	100 MHz	U–NII	5.470–5.725 GHz	255 MHz	U–NII
5.725–5.825 GHz	100 MHz	U–NII			

These license free bands provide both a benefit and a disadvantage. The benefit comes from the fact that you are not required to obtain a license to communicate within these license free bands.

This means that you can buy FCC authorized equipment and install it in your environment without any required permits or fees. However, the disadvantage of using license free bands is that others can also use them.

This means you will have to deal with contention and interference issues and ensure that you have the bandwidth available for your intended purpose in the environment where you will be implementing the WLAN.

It would be nice if we could even say that the use of the license free bands is on a "first come, first serve" basis, but it is not.

You may have a WLAN installed for years only to have a nearby organization install a WLAN on the same frequencies you've been using, which can cause major contention on your network.

The reality is that, as long as this neighbouring network is within FCC regulations, there is very little that can be done aside from some careful negotiations on wireless device placement and channel usage. I will provide more information about this in Chapter 6.

Output Power Levels The FCC also regulates the output power levels of radio frequency devices within these license−free bands. The list below gives a brief summary of the output power limits imposed by the FCC.

There are more complex scenarios that apply to the use of the ISM band that will be covered in chapter 2.

Band	Power	Output Limits Area Usage
U−NII 5.15−5.25 GHz	40 mW	Restricted to indoor operations
U−NII 5.25−5.35 GHz	200 mW	Indoor/outdoor
U−NII 5.470−5.725 GHz	200 mW	Indoor/outdoor
U−NII 5.725−5.825 GHz	800 mW	Higher output power assumes outdoor operations

Indoor and Outdoor Usage Finally, the FCC limits the 5.15−5.25 U−NII band to indoor only usage. The other U−NII bands can be used indoors or outdoors; however, the 5.725−5.825 band is especially well suited for outdoor operations. The area usage of the U−NII bands is summarized in the list above.

The 2.4 GHz ISM band may be used indoors or outdoors, and the output power at the intentional radiator cannot exceed 1 watt. For indoor devices, the output power is usually well under 1 watt and generally resides in a range from 30 to 300 milliwatts [mW].

I'll cover output power concepts and regulations in more detail in Chapter 2. For now, you will want to remember that in the United States, the FCC regulates the frequencies used, the output power levels, and the indoor/outdoor usage limitations.

OfCom and ETSI

The Office of Communications (OfCom) is charged with ensuring optimal use of the electromagnetic spectrum, for radio communications, within the UK. OfCom provides documentation of and forums for discussion of valid frequency usage in radio communications. (Sweden is ETSI region).

The regulations put forth by the OfCom are based on standards developed by the European Telecommunications Standards Institute (ETSI). These two organizations work together in much the same way the FCC and IEEE do in the United States.

MIC and ARIB

In Japan, the Ministry of Internal Affairs and Communications (MIC) is the governing body over radio communications. However, the Association of Radio Industries and Businesses (ARIB) was appointed to manage the efficient utilization of the radio spectrum by the MIC. In the end, ARIB is responsible for regulating which frequencies can be used and such factors as power output levels.

ACMA

The Australian Communications and Media Authority (ACMA) replaced the Australian Communications Authority in July 2005 as the governing body over the regulatory domain of Australia for radio communications management. Like the FCC in the United States, the ACMA is charged with managing the electromagnetic spectrum in order to minimize interference. This is done by limiting output power in license free frequencies and by requiring licenses in some frequencies.

ITU−R

The International Telecommunications Union Radiocommunication Sector (ITU−R) is a sector of the International Telecommunications Union (ITU). The ITU, after an evolving history, was designated as a United Nations specialized agency on October 15, 1947.

The constitution of the ITU declares its purposes as:

- To maintain and extend international cooperation between all its Member States for the improvement and rational use of telecommunications of all kinds
- To promote and enhance participation of entities and organizations in the activities of theUnion, and to foster fruitful cooperation and partnership between them and Member States for the fulfillment of the overall objectives embodied in the purposes of the Union
- To promote and offer technical assistance to developing countries in the field of telecommunications, and also to promote the mobilization of the material, human, and financial resources needed to improve access to telecommunications services in such countries
- To promote the development of technical facilities and their most efficient operation, with a view to improving the efficiency of telecommunication services, increasing their usefulness and making them, so far as possible, generally available to the public
- To promote the extension of the benefits of new telecommunication technologies to all the world's inhabitants
- To promote the use of telecommunication services with the objective of facilitating peaceful relations
- To harmonize the actions of Member States and promote fruitful and constructive cooperation and partnership between Member States and Sector Members in the attainment of those ends
- To promote, at the international level, the adoption of a broader approach to the issues of telecommunications in the global information economy and society, by cooperating with other world and regional intergovernmental organizations and those nongovernmental organizations concerned with telecommunications.

The ITU−R, specifically, maintains a database of the frequency assignments worldwide and helps coordinate electromagnetic spectrum management through five administrative regions.

These five regions are:

- Region A: The Americas
- Region B: Western Europe
- Region C: Eastern Europe
- Region D: Africa
- Region E: Asia and Australia

Each region has one or more local regulatory groups such as the FCC in Region A for the United States or the ACMA in Region E for Australia. Ultimately, the ITU−R provides the service of maintaining the Master International Frequency Register of 1,265,000 terrestrial frequency assignments.

IEEE

The Institute of Electrical and Electronics Engineers (IEEE) states their mission as being the world's leading professional association for the advancement of technology. This means, of course, that they provide standards and technical guidance for more than just the wireless industry. In this section, I focus on the specific standards developed by the IEEE that impact and benefit wireless networking. These standards include wireless specific standards as well as standards that have been implemented in the wired networking domain, which are now being utilized in the wireless networking domain. First, I provide you with a more detailed overview of the IEEE organization.

Overview of the IEEE Organization

The IEEE is a global professional society with more than 350,000 members. The constitution of the IEEE defines the purpose of the organization as scientific and educational, directed toward the advancement of the theory and practice of electrical, electronics, communications, and computer engineering, as well as computer science, the allied branches of engineering, and the related arts and sciences.

Their mission is stated as promoting "the engineering process of creating, developing, integrating, sharing, and applying knowledge about electronics and information technologies and sciences for the benefit of humanity and the profession".

Ultimately, the IEEE created many standards for many niche disciplines within electronics and communications. In this book, the focus is on computer data networks and specifically wireless computer data networks.

In this area, the IEEE has given us the 802 project and, specific to wireless, the IEEE 802.11 standard.

Overview of IEEE WLAN Standards

IEEE projects, such as the IEEE 802 project, are divided into working groups.
The Ethernet standard comes from the IEEE 802.3 working group, and the WLAN standard comes from the IEEE 802.11 working group.

The IEEE 802.11 working group was the eleventh group formed under the IEEE 802 project.

Other working groups of interest to wireless professionals include the IEEE 802.16 working group, which focuses on broadband wireless access, commonly known as WiMAX, and the IEEE 802.20 working group, which focuses on mobile broadband wireless access.

It is interesting to note that the majority of the newly developed working groups, since IEEE 802.11, are wireless specific. This is evidence of the importance of wireless technology in the digital future.

The original IEEE 802.11 standard was ratified in 1997 and is embodied in a document called IEEE 802.11−1997.

The standard was amended in 1999; the base document was altered slightly and replaced by a new base document called IEEE 802.11−1999, and several amendment documents were ratified.

This base document was reaffirmed in 2003 when yet another amendment document was ratified, and renamed IEEE 802.11−1999 Edition (R2003). Several more amendment documents have been ratified since

In addition to the IEEE 802.11−1999 Edition (R2003) document, it is expected that a new base document will be released in the year 2007. This document is likely to be called IEEE 802.11−2007, but at the time of this writing, this document is not yet finalized.

The original IEEE 802.11−1997 standard specified three ways of implementing a physical communication layer (PHY). Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) both use the 2.4 GHz ISM band. The third PHY used infrared but never saw the light of day and is not covered by the CWNA certification for this reason.

Each of these PHYs operates at a mandatory nominal data rate of 1 megabit per second (Mbps) and optionally at 2 Mbps. You will learn more about the detailed specifications of the IEEE 802.11 standards in Chapter 3.

It is interesting to note the massive growth in wireless LAN technology since the release of the IEEE802.11 standard. Before that time, wireless LAN devices used proprietary technologies for communications, and this meant that one vendor's hardware could not communicate with another vendor's hardware.

With the introduction of the IEEE 802.11 standard, a communications structure was defined that vendors could adopt and that would allow for interoperability between the various vendors’ hardware solutions.

The next step was the release of the high rate DSSS (HR/DSSS) PHY, which provided data rates up to 11 Mbps. Once we passed this milestone, the wireless LAN market exploded with growth, revealing a tremendous benefit of standardization: compatibility.

In addition to the working groups, the standards they create are often updated by task groups, and these updates are released as amendments. Amendments can be either ratified or in draft.

When in draft mode, the amendment may still be modified and hardware or software development against the draft amendment is not usually recommended.

When the amendment is ratified, it has been stabilized and development of hardware and software is usually forthcoming.

However, in the real world, many vendors do leap onto amendments that are in the draft mode, as we have seen with IEEE P802.11n—the newer multiple input, multiple output (MIMO)−based amendment to IEEE802.11, in the months leading up to the first quarter of 2007.

Additionally, task groups may be active on a task with no draft yet provided, List below provides a brief description of the amendments to the IEEE 802.11 standard.

IEEE 802.11 Amendment (status as of January 2007)	Description
IEEE 802.11a–1999	Uses Orthogonal Frequency Division Multiplexing (OFDM) instead of DSSS. Provides data rates up to 54 Mbps. Uses the 5 GHz U–NII bands. Not compatible with PHYs that use the 2.4 GHz ISM band such as DSSS and HR/DSSS.
IEEE 802.11b–1999 (amended slightly in 2001)	Uses high–rate direct–sequence spread spectrum (HR/DSSS) instead of the original DSSS. Provides data (HR/DSSS) instead of the original DSSS. Provides data rates up to 11 Mbps. Uses the 2.4 GHz ISM band. Backward compatible with DSSS.
IEEE 802.11c–1998 (incorporated into the IEEE 802.1D–2004 standard, Section 6.5.4)	Updates the IEEE 802.1D bridging standard for 802.11 operations.
IEEE 802.11d–2001	Provides specifications for the use of IEEE 802.11 in more regulatory domains (countries) than were originally specified.
IEEE 802.11e–2005	Defines the layer 2 MAC controls used to meet the Quality of Service (QoS) requirements of multimedia and voice applications over IEEE 802.11 networks.
IEEE 802.11F–2003 Recommended Practice, withdrawn on Feb 3, 2006	An attempt at standardizing how reassociation should occur from access point to access point in a WLAN. Recommended the use of the Inter–Access Point Protocol (IAPP). Supports DSSS and HR/DSSS and adapts OFDM modulation to 2.4 GHz band. Provides data rates up to 54 Mbps. Not compatible with the 5 GHz OFDM PHY due to the use of the 2.4 GHz band.
IEEE 802.11h–2003	Enhances the IEEE 802.11 MAC and OFDM PHY with network management and control. Provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) mechanisms.
IEEE 802.11i–2004	One of the most important enhancements to the IEEE 802.11 standard. Specifies the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is reliant on the Advanced Encryption Standard (AES) and allows for the use of the Temporal Key Integrity Protocol (TKIP). Requires the use of either IEEE 802.1X or preshared key (PSK) for authentication.
IEEE 802.11j–2004	Extends the 802.11 MAC and OFDM PHY to operate in the newly available 4.9–5 GHz band in Japan (and the United States).

IEEE P802.11k (ratification is expected in 2007)	Specifies the use of TPC in frequencies other than 5 GHz band, reporting of client statistics such as signal–to–noise ratio and frame transmissions, and channel statistics of channel management. General purpose is to provide radio resource measurements.
IEEE P802.11n (ratification is expected in 2008)	Defines modifications to the IEEE 802.11 physical and media access control layers that will allow will allow for much higher throughputs and a maximum throughput of at least 100 Mbps. This is currently being accomplished with the use of MIMO (multiple–input–multiple–output) technology in conjunction with OFDM technology.
IEEE P802.11p (ratification is expected in 2009)	Specifies support for the licensed Intelligent Transportation Systems (ITS) band of 5.9 GHz and other 5 GHz bands, specifically 5.850 GHz to 5.925 GHz in North America, for data exchanges between High-speed vehicles. Data communications occur at speeds up to 200 km/h and distances up to 1000 meters.
IEEE P802.11r (ratification is expected in 2008)	Enhancements to the IEEE 802.11 MAC to improve basic service set transitions within extended service sets (ESSs). Sometimes called the fast roaming amendment.
IEEE P802.11s (ratification is expected in 2008)	Specifies the interoperable formation and operation of an ESS Mesh network.
IEEE P802.11T (recommended practice—ratification is expected in 2009)	Provides a set of performance metrics, measurement methodologies, and test conditions to enable measuring and predicting performance of 802.11 WLAN devices and networks as a recommended practice.
IEEE P802.11u (ratification is expected in 2009)	Provides amendments to the IEEE 802.11 PHY and MAC layers that enable interworking with other networks. May provide for handoffs between WiMAX and WLANs or between WLANs and cellular networks.
IEEE P802.11v (ratification is expected in 2009)	Enhancements to provide wireless network management to the IEEE 802.11 MAC, and PHY, to extend prior work in radio measurement that results in a complete and coherent upper–layer interface for managing 802.11 devices in wireless networks. Defines SNMP Management Information Bases that will allow for the configuration of a WLAN client device from a WLAN infrastructure device.
IEEE P802.11w (ratification is expected in 2008)	Improves security of IEEE 802.11 management frames like deauthentication and deassociation frames. Provides data integrity, nonrepudiation,

	confidentiality, and replay protection to these management frames.
IEEE P802.11–REVma (ratification is expected in early 2007)	A rollup project intended to roll the 802.11–1999 (R2003) base document and all its ratified amendments into a new expanded IEEE 802.11 standard base document. Also to be included are some specific definitions of behavior only hinted at in the original standard. Expected to be called IEEE 802.11–2007.

IEEE Standards Impacting WLANs

Other than the specific IEEE 802.11 standard and amendments, there are at least two other project 802 standards that have a tremendous impact on IEEE 802.11. These are IEEE 802.1X and IEEE 802.3–2005, Clause 33. Additional IEEE standards of note are the IEEE 802.1D and 802.1Q standards.

IEEE 802.1X As list above reveals, IEEE 802.1X is a mentioned portion of the IEEE 802.11i amendment. IEEE 802.1X provides port–based authentication and control for your wireless networks in a similar way that it provides the same to wired networks. I will cover IEEE 802.1X in more detail in Chapter 10. **It is a standard for authentication of wireless users and wired users.**

IEEE 802.3–2005, Clause 33 Formerly known as the IEEE 802.3af amendment, this is the standard that defines PoE (Power over Ethernet). Many wireless access points and bridges have support for PoE so that you can install them in locations where Ethernet cables exist but power connections do not. This is particularly useful in closets, on towers, and on rooftops. PoE is covered in more detail in Chapter 7. **This is a standard howto power network devices.**

IEEE 802.1D and IEEE 802.1Q IEEE 802.1D is a standard that defines bridging and priority handling, whereas IEEE 802.1Q focuses on priority tagging and virtual LAN (VLAN) handling for Quality of Service (QoS). IEEE 802.1D includes specifications for bridging, a spanning tree protocol, and specifications for handling IEEE 802.11 MACs in the bridging process (Section 6.5.4). The IEEE 802.1Q standard specifies the operation of bridges that support VLANs. **This is a standard for quality of service.**

IETF

The Internet Engineering Task Force (IETF) is another standards development organization that has impacted the wireless networking industry. You can learn more about the IETF as an organization by visiting their web site at http://www.ietf.org. The primary IETF standards impacting WLANs directly include request for comments (RFC) 3748 and RFC 2865.

IETF RFC 3748

The IETF RFC 3748 details the functionality of the Extensible Authentication Protocol (EAP). EAP is used when IEEE 802.1X port–based authentication is implemented and is, therefore, an integral part of WLAN security. EAP will be discussed more in Chapter 10.

IETF RFC 2865

While EAP provides the authentication flow and specifications, RADIUS provides the highway on which EAP passes. In most implementations of IEEE 802.1X, EAP messages are passed to a RADIUS server where authentication is either approved or rejected. RADIUS will also be covered briefly in Chapter 10.

WiFi Alliance

The WiFi Alliance is a certification organization that provides testing and interoperability analysis for the wireless industry. While the FCC makes the rules and the IEEE determines how to live within those rules, the WiFi Alliance ensures that devices are compatible with the IEEE's way of implementing WLAN technology.

Originally, the WiFi Alliance was known as the Wireless Ethernet Compatibility Alliance (WECA).

In October 2002, the organization was rebranded as the WiFi Alliance. This was done as a measure to improve brand awareness and make the name a more memorable and associative one (a fancy way of saying: to make the name more marketable).

Only products of Alliance members that have been tested successfully by the WiFi Alliance are actually allowed to claim that they are WiFi Certified. This is a subtle distinction as many vendors say their equipment is WiFi equipment and this equipment may or may not be WiFi Certified.

The result has been confusion for some consumers. Ultimately, consumers should look for logos like the ones in below. If a logo like this is on the packaging, the product has been certified by the WiFi Alliance.

Wi Fi
CERTIFIED

Spread Spectrum Technology Uses

Spread spectrum technology is used in multiple ways within modern organizations; however, these different ways can be organized within four primary categories: wireless LANs, *wireless PANs (WPANs)*, *wireless MANs (WMANs)* and *wireless WANs*. The list below summarizes these uses and the following sections provide more detailed information.

Use	Examples	Range	Speeds
WLAN/Backhaul	IEEE 802.11	112 meters/375 feet to several miles	2 Mbps and higher
WPAN	Bluetooth	1–3 meters	723 Kbps to 3 Mbps
WMAN/Backhaul	WiMAX and EDGE	10 kilometers	40 Mbps estimated
Wireless WAN/Backhaul	AT&T microwave, Free Space Optics	Variable	75–135Kbps estimated

Wireless LANs

Wireless LANs (local area networks) are the primary focus of the CWNA certification. The most popular WLAN technology employed today is the IEEE 802.11 standard as amended.

These wireless LANs provide mobility, nomadic ability, and unwired fixed connectivity. Mobility is provided because the user can move around within the coverage area of the access point or even multiple access points, while still maintaining connectivity.

Nomadic ability, the ability to move from place to place and use the network although you may not be using it while moving, is provided because you can power on a wireless client device from any location within a coverage area and use it for a temporary period of time as a fixed location device. Of course, unwired fixed connectivity must exist if nomadic ability is provided.

There are three primary roles that wireless LANs play in today's enterprise organizations:

- Access role
- Distribution role
- Core role

In the *access role*, the wireless network is used to provide wireless clients with access to wired resources. The access point remains fixed while the clients may move. The access point is usually connected to an Ethernet network where other resources, such as file servers, printers, and remote network connections, reside. In this role, the access point provides access to the wireless medium first and then, when necessary, provides bridging to the wired medium or other wireless networks (such as in a mesh network implementation).

In the *distribution role*, wireless bridges provide a backhaul connection between disconnected wired networks. In this case, each network is connected to the Ethernet port of a wireless bridge and the wireless bridges communicate with each other using the IEEE 802.11 standard and amendments. Once these connections are made, network traffic can be passed across the bridge link so that the two previously disconnected networks may act as one.

The final role is the *core role.* In the core role, the wireless LAN is the network. This may be suitable for small networks built on the fly, such as those built at construction sites or in disaster areas; however, the limited data throughput will prohibit the wireless LAN from being the core of the network in a large enterprise installation. Future technologies may change this, but for now, wireless LAN technologies play the access and distribution roles most often.

Wireless PANs

A wireless PAN (personal area network) provides hands free connectivity and communications within a confined range and limited throughput capacity.

Smallscale mesh type wireless networks like those implemented with Zigbee technology are also classed as PANs. Zigbee is an industrial self organized wireless network for sensors/actors/instruments in process industry or similar.

In addition, RFID systems are frequently categorized as wireless PAN technologies, since they have a short communications range. Bluetooth is also a perfect example of a wireless PAN technology that is both beneficial and in widespread use.

Everything from Bluetooth mice to headsets are being used on a daily basis throughout the world. I travel frequently, and the proliferation of Bluetooth headsets in just the past year or two has been really amazing.

Operating in the 2.4 GHz ISM band, Bluetooth technologies can cause interference with wireless LAN technologies like DSSS, HR/DSSS, and ERP. However, the newer adaptive frequency hopping technology helps to reduce this interference if not completely remove it. Adaptive frequency hopping is a new feature found in Bluetooth 1.2 devices and higher.

Wireless MANs

Wireless MANs (metropolitan area networks) differ from wireless LANs and wireless PANs in that they are not usually implemented by the organization that wishes to use the network. Instead, they are generally implemented by a service provider, and then access to the network is leased by each subscribing organization.

However, unlike with wireless WANs, this does not have to be the case. For example, 802.16 ompliant hardware could be purchased and frequency licenses could be acquired in order to implement a private wireless MAN, but the expense is usually prohibitive.

WiMAX is the most commonly referenced wireless MAN technology. Now, in 2008 WiMAX solutions are just beginning to see production and installation. In fact, the first WiMAX Professional Certification training class was held in Hawaii, in January and February 2007. WiMAX is based on the IEEE 802.16 standard and provides expected throughput of approximately 40 Mbps for fixed, line of sight connections and approximately 15 Mbps for mobile, non−line of sight connections.

In addition to the throughput speeds, WiMAX incorporates QoS mechanisms that help to provide greater throughput for all users and important applications using the network.

Wireless WANs

Wide area networks (WANs) are usually used to connect LANs together. If the LANs are separated by a large distance, WAN technologies may be employed to connect them. These technologies include Frame Relay, analog dial−up lines, Digital Subscriber Line (DSL), ISDN, and others.

What they have traditionally had in common is a physical wire connected to something that is connected to something that is eventually connected to the remote LAN. The wireless WAN is completely different because no wire is needed from your local LAN to the backbone network or from the backbone network to your remote LAN. Wireless connections are made from each of your LANs to the backbone network.

Examples of wireless WAN technologies include Free Space Optics, Licensed and Unlicensed Radio, and hybrids of the two. For WAN links that span hundreds of miles, you may need a service provider such as AT&T microwave, but for shorter links of a few miles, you may be able to license frequency bands or use unlicensed technology to create the links.

The key differentiator of wireless WAN technologies from WLAN, WPAN, and WMAN is that the wireless WAN link aggregates multiple communications channels together (multiplexing) and passes them across the single WAN link.

Wireless LAN Technology Roles

The roles played by wireless technology include data networking, voice communications, and video transfer, among others. In addition to the three primary roles discussed earlier in this chapter, there are dozens of specific uses of wireless LAN technologies. This last chapter section will provide an overview of these varied uses as well as a few case studies along the way.

Building−to−Building Connectivity: Bridging

There are many ways to connect another building to your network. You can dig a trench and bury a line that you own. You can place poles and hang a line that you own. You can lease a line from the telephone company. However, the first two have a high initial cost in both money and time, and the last one has an ongoing cost of monthly service fees. Another problem with running your own line is the common scenario where the remote building is actually on the other side of someone else's property. Very few people are kind enough to let you dig a ditch across their property; however, you could run an invisible line—an IEEE 802.11−based connection. By installing a wireless bridge at each building, you overcome these problems. At first, it may seem that a license free link is unlikely, since so many people use IEEE 802.11−based wirelesshardware. With a little thought and a lot of planning, however, you can usually get the job done.

Remember that you can use ERP (formerly known as IEEE 802.11g or Clause 19) devices on both ends, and there are multiple channels from which you can choose. You can also use OFDM (formerly known as IEEE 802.11a or Clause 17) devices, and there are even more channels from which you can choose.
We will cover all the channels that are available to you in Chapter 3, but for now, just remember that you have many channels from which you can choose. It is actually very likely that you can find one, for a short distance building to building link, that is available.

When creating building to building links, you can create point to point (PtP) and point to multipoint (PtMP) links. PtP links are created when one wireless bridge talks to another wireless bridge and both use directional antennas. PtMP links are created when one wireless bridge acts as the center or hub of communications for multiple other wireless bridges. ‘

Due to the large amounts of traffic that can flow through the center bridge in a PtMP configuration, you must be careful when configuring these types of building−to−building links. If the throughput is insufficient for business demands, you might consider creating multiple PtP links instead.

Last−Mile Data Delivery: Wireless ISP

A wireless Internet service provider (WISP) is an Internet service provider (ISP) that is accessed using wireless technologies. WISPs often fulfill the need at the last mile. *Last mile* refers to the last section that must be spanned to reach remote customers. It can be very expensive and, without wireless, sometimes impractical.

Sometimes these WISPs will also lease bandwidth to businesses that require Internet access but are too far from DSL stations and have no other options. WISPs may use IEEE 802.11 technologies for the entire delivery, or they may use other wireless technologies, like WiMAX (IEEE 802.16), from the operations center to the delivery area and then use IEEE 802.11 technologies within the delivery area.

Some WISPs will use WiMAX all the way to the end destination, and it will be up to the subscriber whether to use IEEE 802.11 technologies within their house or business. Since WiMAX and IEEE 802.11 use different frequencies (if the 802.11 devices use the 2.4 GHz spectrum), there should be no conflicts or interference.

Small Office/Home Office (SOHO) Use

In Small Office/Home Office (SOHO) environments, it is very common to have fewer than 25 or even fewer than 10 computers in the entire company. In these scenarios, a wireless LAN can often be your core network. A simple wireless LAN router may be all that is needed.

A SOHO installation can also take advantage of wireless LAN technology at the same time that it utilizes wired technology. For example, using the uplink port found in many switches, you could connect a larger switch to a basic Cisco or Linksys WRT54G router or another vendor such as D−Link, Mikrotik, or Netgear.

The wireless LAN router can provide both wireless access to the network and routing out to the Internet all in one device. The ISP may be using dial up, DSL, or Cable TV modems to provide the Internet connectivity.

Today, Cable TV modems regularly provide between 1 and 100 Mbps, as does DSL. Of course, dialup Internet is still much slower; however, dialup is also still commonly used in rural areas. Thankfully, many brave entrepreneurs have been installing last mile service in these rural areas using licensed and unlicensed wireless solutions.

Mobile Office Networking

Similar to the SOHO installation is the mobile office installation. Mobile offices are used during construction, in disaster zones, fairs, sports activities, and in other such scenarios where you need to have network access with little installation time or complexity.

Interesting devices are on the market that can assist in these mobile office installations. One example is the SonicWALL TZ190, which supports wireless WAN PC cards so that you can route a local network out to the wireless WAN Internet connection. The card protruding from the left side of the device in is the wireless WAN card. Other interesting products have support for 3G technology providing LAN to Wireless solutions.

Industrial: Warehousing and Manufacturing

Warehouses and manufacturing environments are excellent applications of wireless LAN solutions. These environments have often existed for many years and lack the proper cabling to reach even the speeds that wireless LANs can currently provide. At the same time, motors and equipment used in these environments can cause interference problems, so an effective site survey is essential. Storage racks and other materials in and around these types of environments can also be problematic.

Health Care: Hospitals and Offices

Hospitals can benefit from wireless LAN technology in order to have roaming access to patient records as well as pharmacy information. Medical prescriptions can be sent to the hospital pharmacy directly from the patient's rooms, and nurses can give instant digital feedback using PDAs as they make their rounds throughout the hospital. Of course, security will be a top priority in health care installations, so newer equipment supporting the more recent security provisions will be a requirement.

Hotspots: Public Network Access

A WiFi *hotspot* provides wireless Internet access in public areas. Some hotspots are free and wide open, while others are free and secured. Yet other hotspots are subscription based, pay–as–you–go, or a mixture of these.

PDAs and laptops are usually the devices used to connect to hotspots. These hotspots are found everywhere, from coffee shops to libraries to public parks.
It is important to remember that a hotspot is defined as a wireless network that is *intended to give* wireless Internet access either free or for a fee.

There are many locations where you can connect to a wireless network, but many, if not most, of these are *inadvertently giving* wireless Internet access. Examples of these inadvertent networks include homes, businesses, and even government installations that are not properly secured.

Specialty devices have been created that can print receipts, authenticate users, and even disconnect users after time limits expire. These devices are often called hotspot gateways. There are many business models associated with the implementation of a hotspot. Following are a few examples:

- **Traffic Generation** This model profits from the sales of items like coffee, books, music, and other items to the individual who come to the hotspot location for Internet access.

- **Mixed** This model profits from both the fee for access and the sale of items in the area where access is provided. In the United States, Starbucks is probably the most well−known enterprise using this model.

- **Walled Garden Model** This is currently being implemented by many hotels and retail outlets. The concept is to allow connected devices to browse a select group of Internet sites. These sites will pay a fee in order to be in the walled garden. The fees are distributed among the participating hotspots according to the amount of traffic the various hotspots generate.

- **Philanthropist Model** This model assumes that people will love you for giving them free Internet access and that love is reward enough. I know I love this model when I encounter it in my travels. NOTE: I am not referring to stealing network access. I am actually referring to those providers (libraries, municipalities, airports, etc.) that really intend to provide you with network access. If you access a network that is open but not intended for your use, you may be breaching local or regional laws, and you should, therefore, be very cautious and ethical.

Summary

In this chapter, you learned about the different wireless organizations that exist. You learned that there are three primary types of organizations: regulatory, standardization, and compatibility. The FCC falls into the first category, the IEEE into the second, and the Wi−Fi Alliance into the third.

You also learned about the IEEE 802.11 standard that has been developed and the amendments that have been made to it since 1997. Finally, you considered some of the many possible uses of wireless LAN, MAN, PAN, and WAN technologies. Next, review the key terms present here and be sure you can define them all. Then, go through the review questions and answers to be sure that you've grasped the key elements from this chapter.

Key Terms

- ♦ access role
- ♦ core role
- ♦ distribution role
- ♦ FCC
- ♦ IEEE
- ♦ hotspots
- ♦ last mile
- ♦ Wi−Fi Alliance
- ♦ Wireless WAN
- ♦ WLAN
- ♦ WMAN
- ♦ WPAN

Review Questions

1. Which of the following organizations is responsible for compatibility testing of 802.11 hardware?

A. IEEE
B. ETSI
C. Wi−Fi Alliance
D. FCC

2. You want to read the 802.11 standard so that you can better understand the details of the MAC and PHY layer functionality in wireless LANs. Which organization's web site should you visit?

A. IEEE
B. ETSI
C. Wi−Fi Alliance
D. FCC

3. ABC company has contracted with you to install a wireless LAN in their facilities. They inform you that there is a warehouse approximately 400 feet from the main building and that there are no Ethernet wires run to that building. Which of the following technologies will you most likely use to provide wireless network access in the remote warehouse?

A. Wireless PAN
B. Wireless LAN
C. Wireless MAN
D. Wireless WAN

4. What are the two types of wireless bridge links that can be created? (Choose two.)

A. Point−to−point
B. Building−to−building
C. Point−to−multipoint
D. Remote−to−local

5. Which of the following technologies are not wireless WAN solutions? (Choose all that apply.)

A. Zigbee
B. Free Space Optics
C. Wi−Fi Access Points
D. Bluetooth

Answers

1. C. The correct answer is the Wi−Fi Alliance. The IEEE creates standards based on FCC regulations. The ETSI is a European standards body.

2. A. The correct answer is IEEE. The IEEE web site, at http://www.ieee.org, will contain the full text of the IEEE 802.11 standard documents 6 months after each new document is

published. In fact, it can be found at this URL:
http://www.standards.ieee.org/getieee802/802.11.html.

3. **B.** The correct answer is wireless LAN. Since the building is 400 feet away, it is certainly too far for wireless PAN technologies and too close for wireless MAN technologies. Wireless WAN technologies would not likely be used, as you would have to route data from the warehouse to the Internet and then to the main facility and vice versa. In the end, wireless LAN technologies are the only logical solution.

4. **A, C.** The correct answers are point−to−point and point−to−multipoint. Building−to−building is a common phrase used, but it is not the technical term for these wireless bridge links. Remote−to−local is unused terminology.

5. **A, C, D.** The correct answers are Zigbee, Wi−Fi Access Points, and Bluetooth. Free Space Optics (FSO) is the only wireless WAN solution in this list. Zigbee and Bluetooth are wireless PAN solutions, and Wi−Fi Access Points are WLAN solutions.