CHAPTER TWO

WIRELESS LAN DEVICES AND STANDARDS

After completing this chapter you should be able to do the following:

- List WLAN devices and describe their basic functions
- Explain the different types of communications standards and why standards are important
- List the three major wireless standards and regulatory agencies and their functions
- Describe the different IEEE WLAN standards

Real-Life Wireless

Wireless hotspots are sprouting up everywhere, and nowhere more rapidly than in fast food restaurants and coffeehouses. There is good reason for this: wireless access entices customers to eat and drink more and to stay longer. One national chain found that customers who used wireless access on average stayed 30 minutes longer and ate seven dollars more in food.

McDonald's Corporation decided to add wireless access to over 6,000 of their fast-food restaurants by late 2005, allowing customers to surf the Internet and read their e-mail while munching on a Big Mac. McDonald's plans to charge an hourly or monthly fee for this service. Because so many of its competitors offer free wireless access, industry analysts believe that McDonald's must differentiate itself from free services by the quality of the connection or the applications that they offer.

McDonald's plans to offer much more than basic wireless Internet access. In metropolitan areas customers will be able to download digital issues of current newspapers and magazines and store them on their computers to take home. Also, MP3 music files will be available for download. And in perhaps the most unusual move, the wireless network may be used to distribute movie trailers as a tie-in to McDonald's movie-based meal promotions.

In addition to providing customer wireless access, McDonald's plans to use its wireless network to help manage the restaurant's daily operations. Cashless payment systems, which support credit card transactions and cash register sales at counters and drive-up windows, will be connected to the wireless network. The firm also will use the network to distribute employee training videos.

In this chapter you look at wireless devices and the standards that help create and regulate them. The chapter begins by exploring the different types of unique wireless hardware that go into a wireless local area network (WLAN). Next, it describes the organizations that create WLAN standards as well as those bodies that regulate the standards. And finally, you learn about the wireless LAN standards themselves.

WLAN Devices

Devices that are part of a WLAN are not entirely unique. Each wireless device has a counterpart found in a wired network. The uniqueness of the wireless device is that it uses an antenna or other means to send and receive signals instead of a cable. WLAN devices include wireless client network interface cards, access points, bridges, and gateways.

Wireless Network Interface Card

The hardware that allows a client computer to be part of a wired network is called a **network interface card (NIC)**, sometimes called a **client network adapter**. A NIC is the device that connects the computer to the network so that it can send and receive data. In a wired network, one end (or edge) of the NIC is connected to the computer while the other end has a port for a cable connection, as seen in Figure 2-1. The cable connects the NIC to the network, thus establishing the link between the computer and the network.

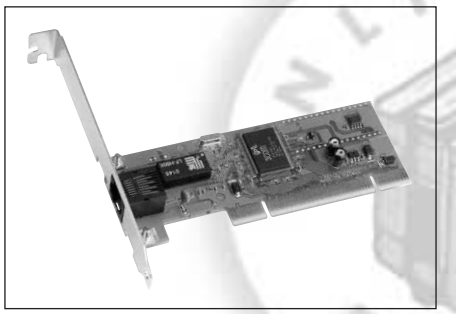

Figure 2-1 Network interface card for a wired network

A wireless network interface card (or wireless client network adapter) performs the same functions as a wired NIC with one major exception: there is no port for a wire connection to the network. In its place is an antenna to send and receive signals. Specifically, when wireless NICs transmit, they:

1. Change the computer's internal data from parallel to serial transmission.
2. Divide the data into packets (smaller blocks of data) and attach the sending and receiving computer's address.
3. Determine when to send the packet.
4. Transmit the packet.

Unlike their wired counterparts, wireless NICs are available in a variety of shapes and styles. For desktop computers, wireless NICs are available for a Peripheral Component Interface (PCI) expansion slot inside the computer, as seen in Figure 2-2a. There are also external wireless NICs that plug into the Universal Serial Bus (USB) port, as either a standalone device (Figure 2-2b) or a key fob (Figure 2-2c).

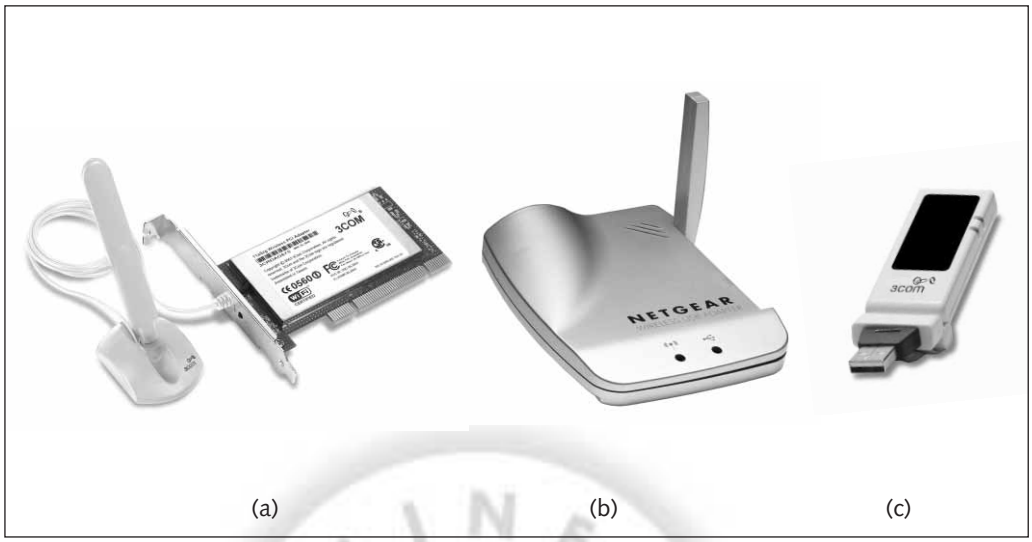

Figure 2-2 Wireless NICs for desktop computers: (a) PCI network interface card, (b) standalone USB device, (c) USB key fob

NOTE

A standalone USB device has an advantage over a key fob because the standalone device can be repositioned to improve reception.

For laptop computers, wireless NICs are also available in different types. One type is the standard PC Card that a user can install. PC Card adapters are typically found on laptop computers and come in different configurations, such as CardBus, PC Card Type II, or PC Card Type III, as seen in Figure 2-3. Another type is the **Mini PCI**. A Mini PCI is a small card that is functionally equivalent to a standard PCI expansion card. It was specifically developed for integrating communications peripherals such as modems and NICs onto a laptop computer. Most laptop computers now come standard with a wireless Mini PCI card installed. Some vendors have enhanced the Mini PCI slot by embedding an antenna in the case of the laptop that surrounds the screen. When a wireless NIC Mini PCI card is used, it automatically activates the antenna to improve the reception of the wireless signal.

NOTE

A CardBus card improves input/output speed over a PC Card by increasing the bus width to 32 bits yet still supports lower-voltage PC Cards.

For smaller devices like personal digital assistants (PDAs), there are several options for wireless NICs, depending on the manufacturer. Some PDAs will accept a standard CardBus or Type II PC Card wireless NIC like those used in a laptop computer. However, sometimes an external attachment known as a **sled** must be purchased and connected to the PDA. The

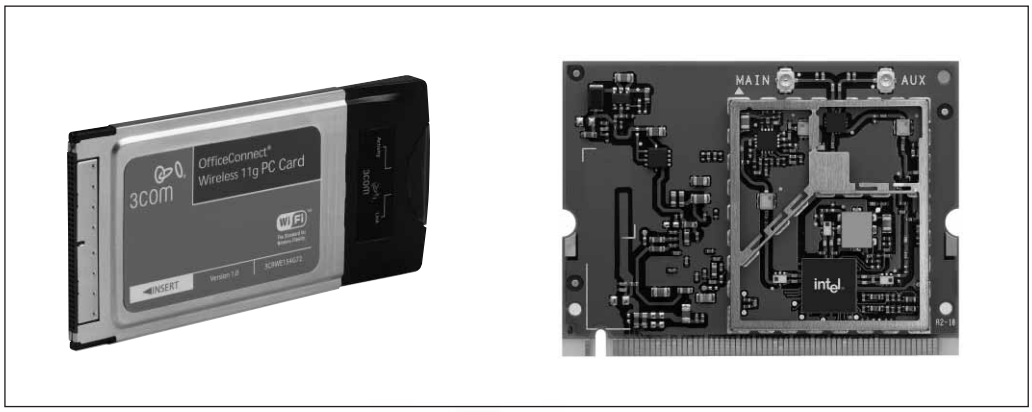

Figure 2-3 Wireless NICs for laptop computers: (a) CardBus card; (b) Mini PCI card

sled contains a slot for a wireless NIC or similar device. Another option is a **CompactFlash (CF) card**, as seen in Figure 2-4. **Flash memory** is a type of solid-state (microchip) technology in which there are no moving parts. CF cards consist of a small circuit board that contains flash memory chips and a dedicated controller chip. There are two advantages of CF wireless NICs over PC Cards: they are smaller and they consume less power. Another option is to use a **SDIO (Secure Digital I/O)** or **SDIO NOW!** card. SDIO cards provide high-speed data input/output with low power consumption for mobile electronic devices.

Figure 2-4 Wireless CompactFlash card

Due to the tremendous popularity of WLANs, separate wireless NICs could soon be a thing of the past. Some vendors plan to integrate a wireless NIC onto a single chip that could be included on the motherboard, eliminating the need for a separate card. Not all vendors agree with this solution, however. Some manufacturers want to keep radio signals farther from the motherboard, to reduce the likelihood of interference with the audio system. Instead of

integrating the components of a wireless NIC on the motherboard of the computer, they integrate a wireless NIC behind the LCD display, thus keeping radio waves away from the motherboard.

The software that interfaces between the wireless NIC and the computer can be part of the operating system or a separate program (driver) that is loaded onto the computer. Beginning with Windows XP, all Microsoft desktop operating systems recognize a wireless NIC without the need for any external software drivers; previous versions of Windows require these external drivers. Incorporating them into the operating system eases installation and also provides additional features such as the ability to connect automatically to different WLANs as the user roams, instead of manually configuring those settings. Some wireless NIC vendors include software drivers for operating systems such as MS-DOS, Windows 3.x, and Linux. Current operating systems for PDAs likewise will recognize a wireless NIC.

Access Point

An access point (AP), seen in Figure 2-5, consists of three major parts. First, it contains an antenna and a radio transmitter/receiver to send and receive signals. Second, it has an RJ-45 wired network interface that allows it to connect by cable to a standard wired network. Finally, it has special bridging software installed to interface wireless devices to other devices.

Figure 2-5 Access point

It is possible to use a standard PC as an access point. Installing a wireless NIC (which functions as the transmitter/receiver), a standard NIC (which serves as the wired network interface), and special AP control software will allow a PC to serve as an AP.

An access point has two basic functions. First, the access point acts as the base station for the wireless network. All of the devices that have a wireless NIC can transmit to the AP, which

in turn redirects the signal to the other wireless devices. The second function of an AP is to act as a bridge between wireless and wired networks. The AP can be connected to the standard network by a cable, allowing the wireless devices to access the data network through it, as seen in Figure 2-6.

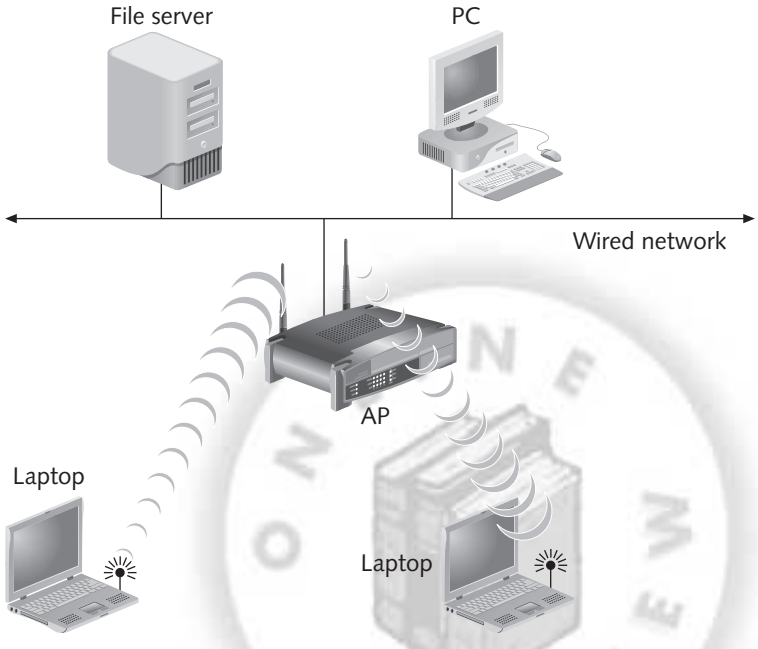

Figure 2-6 An access point acts as a bridge between the wireless network and a wired network

The range of an access point acting as the base station depends on several different factors. One factor is the type of wireless network that is supported. Some wireless networks can transmit up to 115 meters (375 feet) while other types can send and receive signals at only half of that distance. In addition, walls, doors, and other solid objects can reduce the distance the signal may travel.

The number of wireless clients that a single access point can support varies as well. In theory some types of access points can support over 100 wireless clients. However, because the radio signal is shared among users, most industry experts recommend one access point for no more than 50 users if they are performing basic e-mail, light Web surfing, and occasionally transferring medium-sized files. If the users are performing constant network access and transferring large files, a preferred ratio is 20 users per AP.

Access points are typically mounted on a ceiling or a similar area high off the ground to reduce interference from surrounding objects. However, electrical power outlets are generally not found in these locations. In these cases **Power over Ethernet (PoE)** has solved the problem. Instead of receiving power directly from an alternating current (AC) electrical

outlet, direct current (DC) power is delivered to the AP through the unused wires in a standard unshielded twisted pair (UTP) Ethernet cable that connects the AP to the wired network. This eliminates the need for expensive electrical wiring and makes mounting APs more flexible.

Power over Ethernet is now an IEEE standard known as 802.3af.

Remote Wireless Bridge

A **bridge** is a device that is used to connect two network segments together, even if those segments use different types of physical media, such as wired and wireless connections. A **remote wireless bridge** is a wireless device designed to connect two or more wired or wireless networks together. Remote wireless bridges have the same essential characteristics as a wireless LAN AP with two major exceptions. First, remote wireless bridges transmit at higher power than WLAN APs. This enables them to transmit over longer distances than a WLAN. Second, whereas a WLAN AP's radio signal transmits in all directions, remote wireless bridges use directional antennas to focus transmission in a single direction.

Most APs cannot be used in place of a remote wireless bridge. However, some enterprise-level APs, such as the Cisco Aironet 1200, can also perform as a remote wireless bridge.

A remote wireless bridge, seen in Figure 2-7, looks similar to a WLAN AP. Remote wireless bridges typically have the same connections as an AP, which include a wired network connection to connect it to a standard wired Ethernet network. The bridge also contains special software for transmitting and receiving signals. Most bridges have what is known as **delay spread** that minimizes the spread of the signal so that it can reach farther distances. Bridges also have software that enables them to select the clearest transmission channel and avoid noise and interference.

Remote wireless bridges support two types of connections. The first is a **point-to-point** configuration. This configuration is used to connect two LAN segments, as seen in Figure 2-8. The LAN segments can be either wired or wireless. The second configuration is a **point-to-multipoint** configuration. This is used to connect multiple LAN segments together, as seen in Figure 2-9.

Figure 2-7 Remote wireless bridge

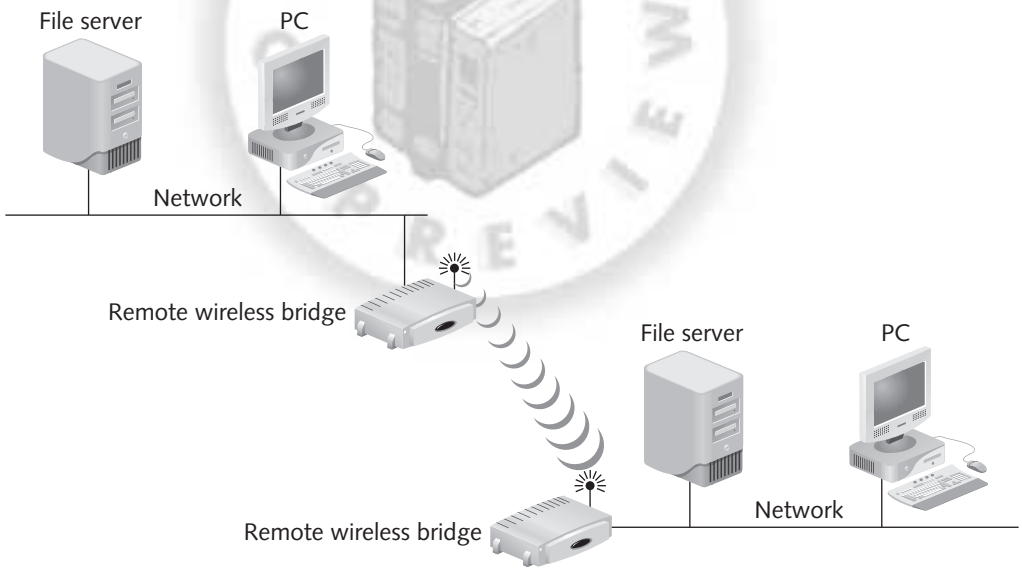

Figure 2-8 Point-to-point remote wireless bridge

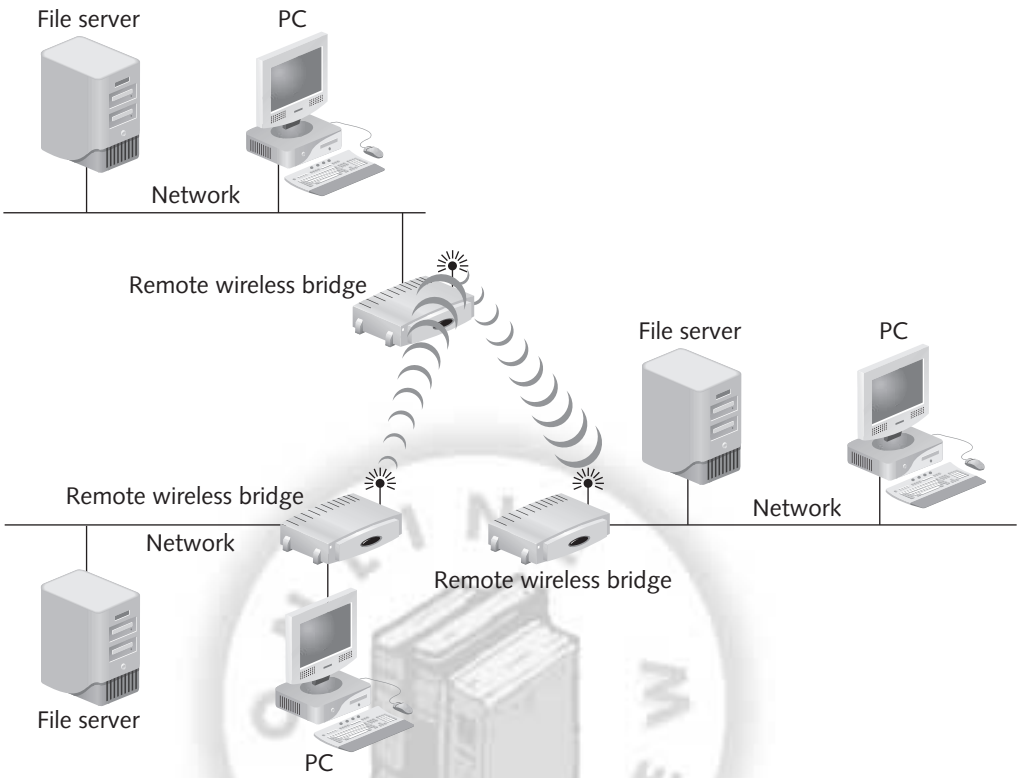

Figure 2-9 Point-to-multipoint remote wireless bridge

A remote wireless bridge can function in one of four different modes:

- If a remote wireless bridge is in **access point mode** it functions as a standard AP only and does not communicate with other remote wireless bridges.
- In **root mode** the bridge, called the **root bridge,** can only communicate with other bridges that are not in root mode. A root bridge cannot communicate with another root bridge or any wireless clients.
- If a remote wireless bridge is set to **non-root mode**, it can only transmit to another bridge in root mode. Some bridge manufacturers enable a remote wireless bridge also to be configured as an access point. This allows the bridge to communicate with a remote wireless root bridge while simultaneously sending and receiving signals with the wireless clients. This is illustrated in Figure 2-10.
- In order to extend the distance between LAN segments, another remote wireless bridge may be positioned between two other bridges. This bridge is then in **repeater mode**, as illustrated in Figure 2-11.

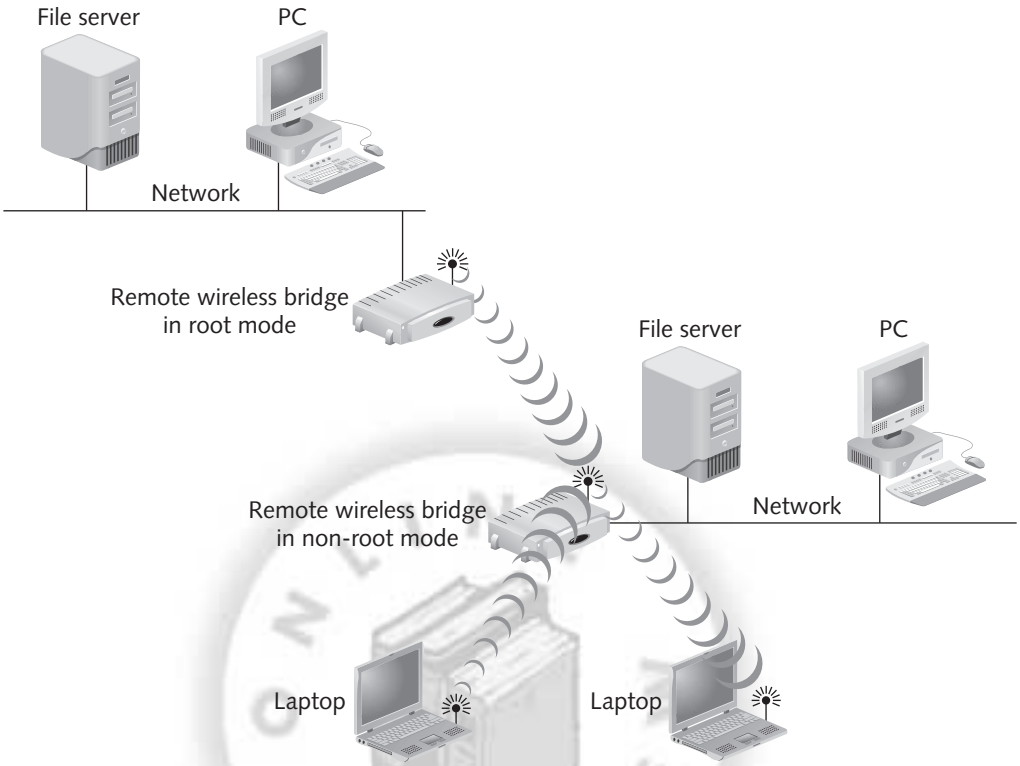

Figure 2-10 Root and non-root modes

Remote wireless bridges are an excellent alternative to expensive leased wired options for connecting remote buildings. Remote wireless bridges are ideal solutions for connecting sites such as satellite offices, remote campus settings, or temporary office locations when the sites are separated by obstacles such as bodies of water, freeways, or railroads that make using a wired connection impractical or very expensive. The distance between buildings using a remote wireless bridge can be up to 29 kilometers (18 miles) transmitting at 11 Mbps or up to 40 km (25 miles) transmitting at 2 Mbps. Even at 11 Mbps, remote wireless bridges are still seven times faster than a traditional T1 connection.

Wireless Gateway

A **wireless gateway** is a device that combines wireless management and security in a single appliance. A wireless gateway performs the following functions:

- *Authentication*—Instead of using the network operating system's username/password scheme to authenticate wireless users, a wireless gateway ensures that all wireless users are authenticated before allowing them to connect to the network. This provides an additional level of security because unauthorized wireless users will not be able to access the network. Wireless gateway authentication usually supports such advanced authentication features.

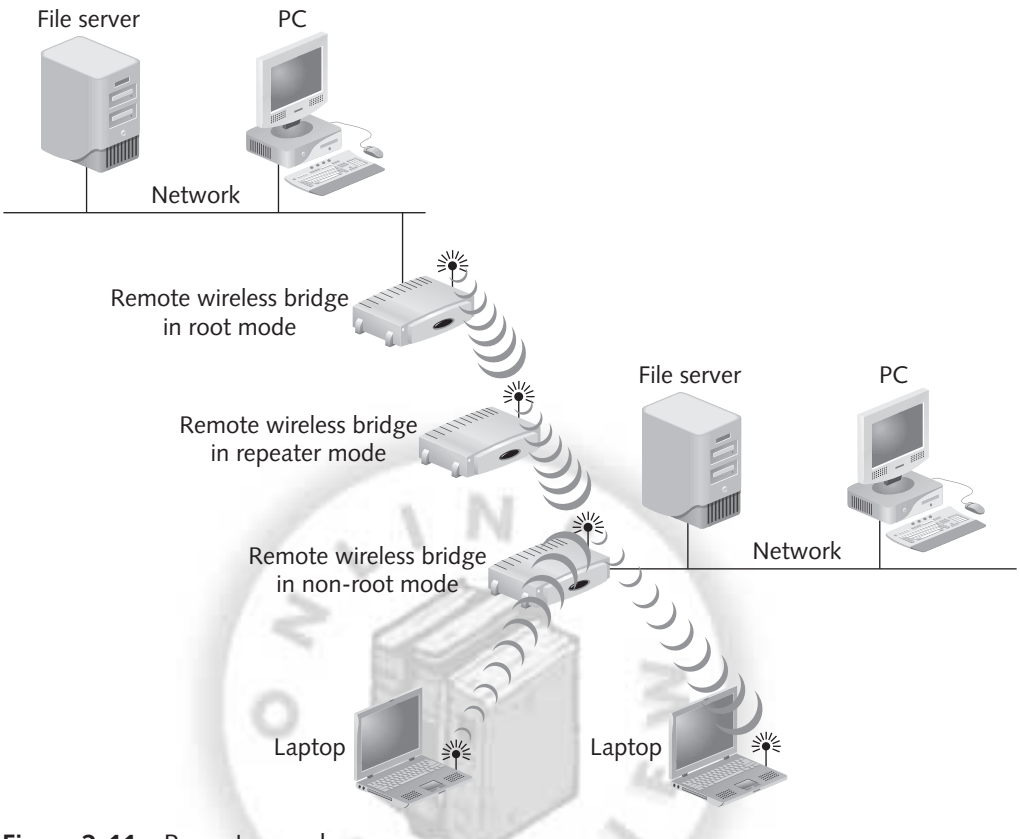

Figure 2-11 Repeater mode

- *Encryption*—A wireless gateway can encrypt all transmissions so that unauthorized eavesdroppers cannot intercept and interpret the wireless signal. This encryption is generally performed using virtual private network (VPN) technology, which is covered in detail in Chapter 9.
- *Intrusion detection and malicious program protection*—Most wireless gateways include real-time monitoring of wireless network traffic in order to detect malicious attacks from wireless users. A wireless gateway enables the wireless network administrator to block intruders and worm penetrations.
- *Bandwidth management*—Because WLAN bandwidth, or the maximum amount of data that can be sent and received, is shared among all users, a few users can monopolize the bandwidth. A wireless gateway allows network traffic to be monitored so that bandwidth can be more evenly allocated among users.
- *Centralized network management*—A wireless gateway can consolidate the management of a WLAN into one device instead of managing each AP individually.

Wireless gateways provide a single mechanism for managing and monitoring the wireless network. They have proven to be very effective in large enterprises that use WLANs extensively.

Understanding Standards

We live in a world of standards. The gearshift lever in your car, the shape of an electrical outlet in your house or apartment, and the size of a CD-ROM disc are all based on standards. And the standards are very important. Imagine what it would be like for someone to try to drive your car if they did not know where Reverse was located, or if you wanted to plug in an appliance but the electrical outlet was the wrong shape, or if there were different sizes of CD-ROMs and your CD-ROM drive would only accept a certain size CD. Standards simply make it easier for us to purchase and use a wide variety of products.

Wireless technology likewise is based on standards. In fact, one of the reasons why wireless LANs have been so tremendously successful since their introduction in late 1999 is because from the outset WLANs have been based on standards. Unlike some computer technologies in which different vendors proposed different standards and the battle had to be fought in the marketplace to see which technology would win the hearts and minds of consumers, wireless technology started with standards and the vendors manufactured products that followed these standards. The standards helped ensure that different products from different vendors all functioned in the same capacity.

In the following sections you explore why standards are necessary, their advantages and disadvantages, different types of standards, and the regulatory bodies responsible for creating and maintaining standards for wireless LANs.

The Need for Standards

The role that standards play in a particular industry varies. Standards for telecommunications have been essential since the very beginning. This is because of the very nature of the industry: telecommunications involves equipment interacting with other equipment. Without standards telecommunications would essentially be impossible.

Yet some professionals in information technology (IT) believe that standards have stifled growth in this fast-paced field. They maintain that waiting for standards to catch up to the rapid changes in IT slows down the process of change and development. The IT industry was founded on cutting edge technology without standards, the thinking goes, so to add standards stymies growth.

Despite this negative perception, in reality standards have proven to be more beneficial than harmful. By examining the advantages and disadvantages of standards, this should become evident.

Advantages and Disadvantages of Standards

Standards have many advantages. For example:

- Standards ensure that devices from one vendor will interoperate with those from other vendors. Devices that are not based on standards may not be able to connect and interoperate with similar devices from other vendors.
- Standards create competition. If a vendor creates a new device apart from standards it is called a **proprietary** device. The vendor owns the specifications and perhaps even a patent on the device. This makes it almost impossible for another manufacturer to produce a similar device. On the other hand, because standards apply to everyone, any vendor can create a device based on a standard.
- Competition results in lower costs for consumers and manufacturers. When several vendors make similar products based on the same standards, it is likely that they will also compete on prices. Competition also results in lower costs for manufacturers. Because standards have been established, manufacturers do not have to invest large amounts of capital in research and development. This reduces startup costs as well as the amount of time needed to bring a product to the market. Also, manufacturing to standards encourages manufacturers to deploy mass production techniques and economies of scale to keep production costs low, savings that in turn are passed on to consumers.
- Standards help protect the user's investment in equipment. It is not uncommon for a proprietary vendor to phase out a product line, leaving a business that purchased the equipment with two choices: continue to use the now-obsolete system with escalating costs for supplies and technical support, or discard the legacy system and buy an up-to-date system. Both choices are very expensive. Standards, however, can help create a migration path for equipment upgrades. Newer standards are generally backward compatible or at least provide a means of migrating to equipment based on the newer standards at a minimal cost.

Standards also have some disadvantages. For example:

- International standards can open domestic markets in larger countries to overseas competition. Manufacturers in other nations may have lower overhead and be able to produce a device cheaper, undercutting domestic manufacturers. However, this also means that standards can benefit industries in the countries with lower overhead.
- Standards can create or reflect political conflict. Although standards are intended to create unity, they can sometimes have the opposite effect. Sometimes one nation will create a standard and offer it as a global standard. However, due to opposing political interests or technologies, other nations may reject that standard and attempt to promote or create their own. This can result in each nation creating its own standards and decreasing the ease of global communications.

Most experts agree that the advantages of standards outweigh the disadvantages, especially in industries such as IT. Table 2-1 summarizes the advantages and disadvantages of standards.

Table 2-1 Advantages and disadvantages of standards

Advantages	Disadvantages
Ensure that telecommunications devices from one vendor will interoperate with those from other vendors	Can threaten industries in large countries
Create competition between vendors, which lowers costs for vendors and consumers	Different countries may create competing or conflicting standards
Help protect the investment in equipment	

Types of Standards

There are two major types of standards in the telecommunications industry, de facto and de jure. A third emerging type of standard, by consortium, is increasingly influencing how standards are set.

De Facto

De facto standards are not actually standards at all. Rather, they are *common practices* that the industry follows for various reasons, ranging from ease of use to tradition to what the majority of the users do. For the most part, de facto standards are established by success in the marketplace. For example, Microsoft Windows has become the de facto standard operating system today for personal desktop computers and network servers. This is because the majority of users have elected to install and run Windows on their computers. There was no standards body that proclaimed Windows as the standard operating system; the widespread use of the industry has created what amounts to be a standard.


NOTE

The word *de facto* comes from Latin and means "from the fact." The word *de jure* is also from Latin and means "from the law."

De Jure

The second type of standard is known as **de jure standards**, which are official standards. De jure standards are those that are controlled by an organization or body that has been entrusted with that task. The process for creating these standards can be very involved. Generally the organization will develop subcommittees responsible for a specific technology. Within each subcommittee there are working groups, which are teams of industry experts who are given the task to create the initial draft. The draft will then be published and requests for comments will be solicited from other organization members (these members may be developers, potential users, and other people having general interest in the field). The comments are then reviewed by the original committee and may be incorporated into the final draft. This is then reviewed by the entire organization before the final standards are officially published.


NOTE

De facto standards sometimes become de jure standards by being later approved by a committee. Ethernet is one example of a de facto standard that later became a de jure standard.

Consortia

One of the complaints against de jure standards is the amount of time it takes for a standard to be completed. For example, the initial standard for wireless LANs took seven years to complete. In the IT economy, this represents an extremely long period of time before products can be brought to the market.

In reaction to this, consortia are often used today to create standards. **Consortia** are usually industry-sponsored organizations that want to promote a specific technology. The goal of a consortium is to develop a standard that promotes their specific technology in a short period of time. Unlike de jure standards bodies, membership in consortia is not always open to everyone, although it might be. Sometimes specific high-profile companies both create a consortium as well as serve on it.


NOTE

One of the most famous consortia is the World Wide Web Consortium (W3C), which is composed of industry giants such as Microsoft, Sun Microsystems, and IBM. The W3C is responsible for creating the standards that are widely used on the Internet today, including Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), and the Document Object Model (DOM).

Enforcing Standards

Although setting standards is essential for IT, enforcing them is equally important. After all, standards would be useless if no one followed them. How are the standards to be enforced? The marketplace itself enforces some standards. That is, a vendor who refuses to abide by standards for cellular telephone transmissions will find that nobody will buy its products. Standards created by consortia often are regulated by the marketplace.

De jure standards, however, must often be enforced by an outside regulatory agency. The role of a regulatory agency is to ensure that all participants adhere to the prescribed standards. The agency must have the power to enforce the standards and effectively punish those who refuse to abide by them. There are a number of international regulatory agencies as well as national agencies whose job is to ensure that standards are strictly adhered to.

Wireless Standards Organizations and Regulatory Agencies

There are three primary standard-setting and regulatory bodies that play a major role in wireless LAN technology. These include the Institute of Electrical and Electronics Engineers (IEEE), the Wi-Fi Alliance, and the U.S. Federal Communications Commission (FCC).

Institute of Electrical and Electronics Engineers (IEEE)

For computer networking and wireless communications the most widely known and influential organization is the **Institute of Electrical and Electronics Engineers (IEEE)**. The IEEE and its predecessor organizations date back to 1884. The IEEE establishes standards for telecommunications. However, the IEEE also covers a wide range of IT standards.


NOTE

You can find out more about the IEEE and its standards on its Web site, *www.ieee.org*.

IEEE is the world's largest technical professional society with members around the globe. Serving the computing, electrical engineering, and electronics professions, the IEEE engages in technical, educational, and professional activities that advance the theory and practice of what they call "electrotechnology." The 37 Societies and Councils of the IEEE routinely publish technically focused journals, magazines, and proceedings, as well as work on over 800 standards. Some of these standards apply to circuits and devices, communication and information technology, control and automation, electromagnetics, geoscience, ocean technology and remote sensing, instrumentation and measurement and testing, optics, power and energy, and signal processing.


NOTE

The IEEE is currently developing standards for rechargeable batteries for laptop computers and electronic voting equipment data exchange.

Although the IEEE is one of the leading developers of global standards in a broad range of industries such as energy, biomedical and healthcare, and transportation, it is best known for its work in establishing standards for computer networks. In the early 1980s, the IEEE began work on developing computer network architecture standards. Its work was called **Project 802**. Project 802 quickly expanded into several different categories of network technology, known as 802.1, 802.2, all the way to 802.16. IEEE Project 802.3 set specifications for Ethernet local area network technology.


NOTE

Project 802 received its name from the fact that the work was begun in 1980 (80) during February, the second month (2).

As older network technologies have been replaced with new technologies, the IEEE 802 committees have likewise reflected the changes in technology. Several committees have been retired, while new committees have been formed to address emerging technologies. Table 2-2 lists the current IEEE 802 network committees.

Table 2-2 Current IEEE 802 committees

IEEE 802 Committee	Description
802.3	Ethernet local area networks
802.11	Wireless networks
802.15	Wireless personal area networks
802.16	Wireless wide area networks

IEEE is also responsible for setting standards for computer technologies besides networking. For example, IEEE 1394 is the standard for FireWire.

Wi-Fi Alliance

Shortly after the IEEE released its revised wireless network standards in 1999, there was concern about how this new wireless technology would be accepted in the marketplace. A consortium of wireless equipment manufacturers and software providers was formed to promote wireless network technology. This group was known as the **Wireless Ethernet Compatibility Alliance (WECA)**. The WECA had three goals:

- To encourage wireless manufacturers to use the IEEE 802.11 technologies in their wireless networking products
- To promote and market these technologies to consumers in the home, in **small office/home office (SOHO)** settings, and in large enterprise businesses and organizations
- To test and certify that wireless products adhere to the IEEE 802.11 standards to ensure product interoperability

SOHO settings have been particularly eager to embrace wireless LAN technology. The sales of wireless LAN equipment to SOHO settings grew by 73% from 2003 to 2004, according to the Dell'Oro Group.

In October 2002 the WECA organization changed its name to **Wi-Fi (Wireless Fidelity) Alliance**, which reflected the name of the certification that it uses (Wi-Fi) to verify that a product follows IEEE standards. While all wireless devices are sometimes called Wi-Fi, only products that have passed the Wi-Fi Alliance testing are allowed to refer to their products as Wi-Fi Certified, which is a registered trademark shown in Figure 2-12.

In addition to product testing and certification, the Wi-Fi Alliance is branching out into new areas. Businesses can apply to be registered as a **Wi-Fi ZONE**. This qualifies them to be placed in an online database of wireless hotspot locations, which can be accessed through the Alliance's Web site. In addition, these businesses can display a Wi-Fi ZONE logo at the physical business location and in product literature.

Figure 2-12 Wi-Fi Certified seal

The Wi-Fi Alliance Web site is *www.wi-fi.org*.

Federal Communications Commission (FCC)

In the United States, the organization that controls and regulates wireless transmissions is the Federal Communications Commission (FCC). In this section you will explore what its role is and how it regulates the radio frequency spectrum on which wireless transmissions take place.

Responsibilities

The **Federal Communications Commission (FCC)** serves as the primary regulatory agency for wireless communications in the United States and its territorial possessions. The FCC is an independent government agency that is directly responsible to Congress, established by the Communications Act of 1934 and charged with regulating interstate and international communications by radio, television, wire, satellite, and cable.

In order to preserve its independence, the FCC is directed by five commissioners who are appointed by the President and confirmed by the Senate for 5-year terms. Only three commissioners may be members of the same political party, and none of them can have a financial interest in any FCC-related business.

The Commerce Department's National Telecommunications and Information Administration (NTIA) serves as the principal adviser to the President on domestic and international communications and information issues. It also represents the views of the Executive Branch before the Congress, the Federal Communications Commission, foreign governments, and international organizations.

The FCC's responsibilities are very broad. In addition to developing and implementing regulatory programs, they also process applications for licenses and other filings, analyze complaints, conduct investigations, and take part in congressional hearings. They also represent the United States in negotiations with other nations about telecommunications issues.

The Web site of the FCC is *www.fcc.gov*.

Regulating the Radio Frequency Spectrum

The FCC plays an important role in wireless communications. It regulates radio and television broadcast stations as well as cable and satellite stations. It oversees cellular telephones, pagers, and two-way radios. The FCC regulates the use of radio frequencies to fulfill the communications needs of businesses, local and state governments, public safety service providers, aircraft and ship operators, and individuals.

The FCC is charged with regulating the radio frequency spectrum. The **radio frequency spectrum** is the entire range of all radio frequencies. The spectrum is divided into 450 different sections or **bands**. Table 2-3 illustrates some of the more common bands. The U.S. is obligated to comply with the international spectrum allocations established by international governing bodies. However, the U.S. domestic spectrum uses may differ from international allocations if these domestic uses do not conflict with international regulations or agreements.

Table 2-3 Common radio frequency bands

Band	Frequency	Common Uses
Very Low Frequency (VLF)	10 KHz to 30 KHz	Maritime ship-to-shore
Low Frequency (LF)	30 KHz to 300 KHz	Cordless telephones
Medium Frequency (MF)	300 KHz to 3 MHz	AM radio
High Frequency (HF)	3 MHz to 30 MHz	Short wave radio, CB radio
Very High Frequency (VHF)	30 MHz to 144 MHz 144 MHz to 174 MHz 174 MHz to 328.6 MHz	TV stations 2-6, FM radio Taxi radios TV stations 7-13
Ultra High Frequency (UHF)	328.6 MHz to 806 MHz 806 MHz to 960 MHz 960 MHz to 2.3 GHz 2.3 GHz to 2.9 GHz	Public safety Cellular telephones Air traffic control radar Wireless LANs
Super High Frequency (SHF)	2.9 GHz to 30 GHz	Wireless LANs
Extremely High Frequency (EHF)	30 GHz and above	Radio astronomy

Radio frequencies of common devices include:

- Garage door openers, alarm systems: 40 MHz
- Baby monitors: 49 MHz
- Radio controlled airplanes: 72 MHz
- Radio controlled cars: 75 MHz
- Wildlife tracking collars: 215 MHz-220 MHz
- Global positioning systems (GPS): 1.227 GHz and 1.575 GHz

Although a license is normally required from the FCC to send and receive on a specific frequency, there is a notable exception. This is known as the **license-exempt spectrum** or **unregulated bands**. Unregulated bands are in effect bands of the radio spectrum that are available nationwide to all users, without requiring a license. Devices that use these bands can be either fixed or mobile. The FCC says that it created the unregulated bands to "foster the development of a broad range of new devices, stimulate the growth of new industries, and promote the ability of U.S. manufacturers to compete globally by enabling them to develop unlicensed digital products for the world market."

The FCC does impose power limits on devices using the unregulated bands, which in effect reduces their range. This prevents manufacturers of devices such as long-range walkie-talkies from using these frequencies instead of the regulated frequencies intended for these products.

All of the FCC unregulated bands are summarized in Table 2-4. Two of the bands are used for WLANs. One of these bands is the **Industrial, Scientific, and Medical (ISM)** band, which was approved by the FCC in 1985. Another unlicensed band used for WLANs is the **Unlicensed National Information Infrastructure (U-NII)** band, approved in 1996. The U-NII band is intended for devices that provide short-range, high-speed wireless digital communications. U-NII devices may provide a means for educational institutions, libraries, and health care providers to connect to basic and advanced telecommunications services. Educational institutions, for example, could form inexpensive wireless computer networks between classrooms. U-NII unlicensed wireless networks could help improve the quality and reduce the cost of medical care by allowing medical staff to obtain on-the-spot patient data, X-rays, and medical charts, and by giving health care workers in remote areas access to telecommunications services. Depending on the type of wireless LAN, it will use either the ISM or the U-NII band.

Table 2-4 Unlicensed bands

Unlicensed Band	Frequency	Total Bandwidth	Common Uses
Industrial, Scientific, and Medical (ISM)	902-928 MHz 2.4-2.4835 GHz 5.725-5.85 GHz	234.5 MHz	Cordless phones, WLANs, wireless Public Branch Exchanges

Table 2-4 Unlicensed bands (continued)

Unlicensed Band	Frequency	Total Bandwidth	Common Uses
Unlicensed Personal Communications Systems	1910-1930 MHz 2390-2400 MHz	30 MHz	Wireless Public Branch Exchanges
Unlicensed National Information Infrastructure (U-NII)	5.15-5.25 GHz 5.25-5.35 GHz 5.725-5.825 GHz	300 MHz	WLANs, wireless Public Branch Exchanges, campus applications, long outdoor links
Millimeter Wave	59-64 GHz	5 GHz	Home networking applications

There are some negative features of the unregulated bands. Because they are not regulated and licensed, devices from different vendors may attempt to use the same frequency. This conflict can cause the signals from different devices to interfere with each other and prevent the devices from functioning properly. Thus the performance of devices using unregulated bands can be unpredictable.

Types of Wireless LANs

Since the late 1990s, the IEEE has approved four standards for wireless LANs: IEEE 802.11, 802.11b, 802.11a, and 802.11g. A new standard, 802.11n, is expected to be approved by 2006. Each of the standards will now be examined in detail.

IEEE 802.11

In 1990 the IEEE formed a committee to develop a standard for wireless local area networks (WLANs) operating at 1 and 2 Mbps. Several different proposals were initially recommended before a draft was developed. This draft went through seven different revisions that took almost seven years to complete. On June 26, 1997 the IEEE approved the final draft.

The IEEE 802.11 standard specified that wireless transmissions could take place in one of two ways. The first is through infrared light, and the other is by sending radio signals.

Infrared Transmissions

All the different types of light that travel from the sun to the earth make up what is called the **light spectrum**. Visible light is just a small part of that entire spectrum. Some of the other energies of the spectrum such as x-rays, ultraviolet rays, and microwaves are invisible to the human eye. **Infrared light**, which is also invisible, can actually be used for wireless transmissions.


NOTE

Infrared light is next to visible light on the light spectrum and shares many of the same characteristics.

Infrared transmissions can send data by the intensity of the infrared light wave instead of "on-off" signals of, for example, a flashlight. To transmit a "1" an **emitter** (a device that transmits a signal) increases the intensity of the current and sends a "pulse" using infrared light. On the receiving end a **detector** (a device that receives a signal) senses the higher intensity pulse of light and produces a proportional electrical current.


NOTE

Emitters and detectors are sometimes combined into a single device.

Infrared transmissions can be either directed or diffused. A **directed transmission** requires that the emitter and detector be directly aimed at one another (called **line of sight**), as seen in Figure 2-13. The emitter sends a narrowly focused beam of infrared light. The detector has a small receiving or viewing area. A television remote control device uses a directed transmission.

Figure 2-13 Directed transmission

A **diffused transmission** relies on reflected light. The emitters on diffused transmissions have a wide-focused beam instead of a narrow beam. The emitter is pointed at the ceiling of a room and uses it as the reflection point. When the emitter transmits an infrared signal it bounces off the ceiling and fills the room with the signal. The detectors are also pointed at the same reflection point and can detect the reflected signal, as seen in Figure 2-14.

Infrared wireless systems have several advantages. Infrared light neither interferes with other communications signals nor is it affected by other signals. Also, because infrared light does not penetrate walls, the signals are kept inside a room. This makes it impossible for someone elsewhere to "listen in" on the transmitted signal. The IEEE 802.11 standard outlines the use of diffused infrared transmissions for WLANs.

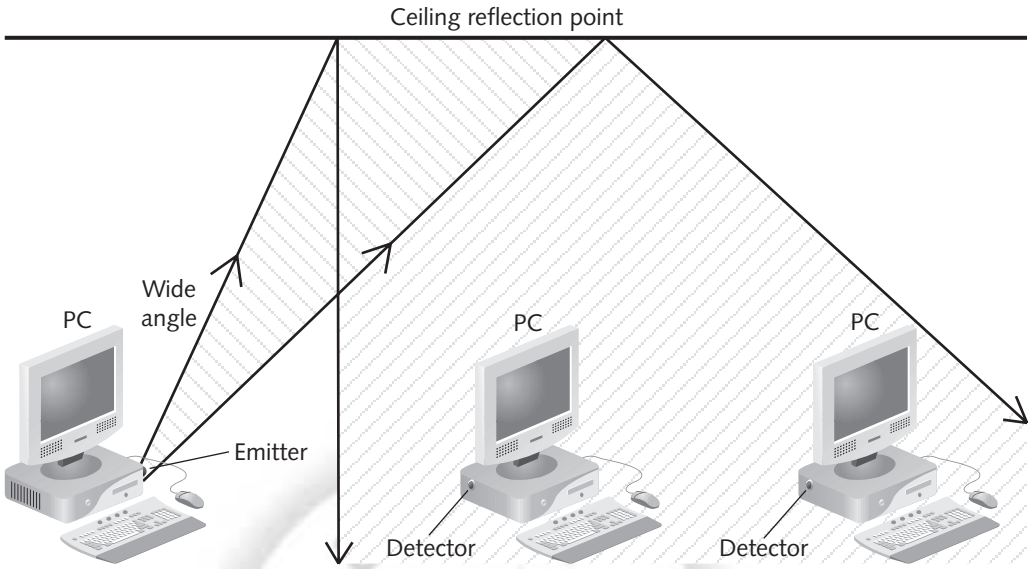

Figure 2-14 Diffused transmission

However, there are significant limitations to infrared wireless LAN systems:

- *Lack of mobility*—Directed infrared wireless systems use a **line of sight** principle, which makes it impossible for mobile users to use it since the alignment between the emitter and the detector would have to be continuously adjusted.
- *Limited range*—Directed infrared systems, which require a clear line of sight, cannot be placed in an environment where there is the possibility that anything could get in the way of the infrared beam. This means devices using infrared transmission must be placed close enough to one another to eliminate the possibility of something moving between them (imagine someone standing in front of your remote while you are trying to change TV channels). And due to the angle of deflection, diffused infrared can only cover a range of about 15 meters (50 feet).
- *Confined to indoor use*—Because diffused infrared requires a reflection point and because transmission is poor in bright sunlight, wireless infrared LANs cannot be reliably used outdoors.
- *Slow transmission speed*—Diffused infrared can send data at only up to 4 Mbps. This is because the wide angle of the beam loses energy as it reflects. The loss of energy results in a weakened signal. The weak signal cannot be transmitted over long distances nor does it have sufficient energy to maintain a high transmission speed. This results in lower data throughput.

Because of these limitations, 802.11 infrared WLAN systems were never widely adopted. Today infrared transmissions are generally used in specialized applications, such as data transfers between laptop computers, digital cameras, handheld data collection devices, PDAs, electronic books, and other similar mobile devices.

WLANs that use infrared transmissions are used in specialized situations where radio signals would interfere with other equipment, such as in hospital operating rooms, or when security is a concern, such as in secure government buildings.

Radio Wave Transmissions

Another approach to wireless LAN transmissions is using radio waves. Unlike infrared transmissions, radio waves can penetrate through objects like walls and thus allow the wireless user to be truly mobile. In addition, radio waves travel longer distances and can be used indoors as well as outdoors. And, radio waves can travel at much higher speeds than infrared transmissions. The IEEE 802.11 standard outlining the use of radio waves in transmissions has become the preferred method for wireless LANs.

How radio waves actually carry data signals is covered in detail in Chapter 3.

IEEE 802.11b

The bandwidth of 2 Mbps for the 802.11 standard introduced in 1997 was not sufficient for most network applications. The IEEE body revisited the 802.11 standard shortly after it was released to determine what changes could be made to increase the speed. In September 1999 a new **802.11b** amendment was added to the standard, which added two higher speeds (5.5 Mbps and 11 Mbps) to the original 802.11 standard (1 Mbps and 2 Mbps). Like the 802.11 standard, 802.11b uses the ISM band.

The 802.11b standard can support wireless devices that are up to 115 meters (375 feet) apart. However, devices that are that far apart might not be transmitting at 11 Mbps. Radio waves decrease in power over distance, much like the sound of your voice: a person standing 1 meter away from you might hear you very clearly, whereas a person 60 meters away would have difficulty hearing you. Instead of completely dropping the signal if it falls out of range to transmit at 11 Mbps, the 802.11b standard specifies that the devices should drop their transmission speed to the next lower level (5.5, 2, or 1 Mbps). This allows devices to transmit farther apart but at slower speeds.

IEEE 802.11a

At the same time the IEEE created the 802.11b standard, it also issued another standard with even higher speeds. The **802.11a** standard specifies a maximum rated speed of 54 Mbps and also supports 48, 36, 24, 18, 12, 9, and 6 Mbps transmissions using the U-NII band. Although the 802.11a and 802.11b specifications were published at the same time by IEEE, 802.11b products started to appear almost immediately, while 802.11a products did not arrive until late 2001. 802.11a products came to the market later because of technical issues along with

the high cost of developing products for the standard. Devices based on the 802.11a standard cannot use complementary metal oxide semiconductors (CMOS) (the semiconductor used in 802.11b WLANs). Instead, they must use a compound such as gallium arsenide (GaAs) or silicon germanium (SiGe). These semiconductors are more expensive and require more capital investment and time to develop and manufacture.

Although the 802.11a standard achieves higher speed, the tradeoff is that devices cannot be as far apart as with the 802.11b standard. A wireless network that follows the 802.11a standard may generally have devices that are no more than 30 meters (100 feet) apart.

IEEE 802.11g

The tremendous success of the IEEE 802.11b standard shortly after its release prompted the IEEE to re-examine the 802.11b and 802.11a standards to determine if a third intermediate standard could be developed. This "best of both worlds" approach would preserve the stable and widely accepted features of 802.11b but increase the data transfer rates to 54 Mbps, similar to those of 802.11a. The IEEE formed an initial task group to explore this possibility. By late 2001 a draft standard was proposed known as **IEEE 802.11g**. The standard was formally ratified in 2003.

The IEEE 802.11g draft was a compromise based on input from several different chip (microprocessor) manufacturers, who had a major stake in the outcome. Although most major commercial wireless networking product vendors will build and sell products based upon whatever standard is approved, the same is not true for the chip manufacturers. These businesses must make huge monetary investments in designing, sampling, and manufacturing the silicon chips used in the wireless network products. They must then try to sell their chips to product vendors that design and build commercial products based on those chips.

The 802.11g standard specifies that devices operate entirely in the ISM frequency and not the U-NII band used by 802.11a. This gives the 802.11g standard the ability to support devices that are farther apart with higher speeds, but it uses the crowded ISM band. Like 802.11b, 802.11g can support devices that are up to 115 meters (375 feet) apart.

Projected IEEE 802.11n

In September of 2004 the IEEE started working on a new standard to significantly increase the bandwidth of today's WLANs. Known as **802.11n**, it will set standards for transmissions exceeding 100 Mbps. The 802.11n committee is evaluating over 60 different proposals regarding how to accomplish this. The top speed of the 802.11n standard will be anywhere from 100 Mbps to 500 Mbps, depending on which proposal is approved.

Although the final proposal might not be ratified until the year 2006, devices that follow one of the proposed options will appear much earlier than that. This is because there is a significant time lag between the time the final proposal is published and when it is ultimately ratified by the IEEE. This occurred with the 802.11g standard: devices were marketed and sold months before the standard was finally ratified. A WLAN based on one of the 802.11n proposals appeared in mid-2004 under the name "802.11 pre-N".

The Wi-Fi Alliance refuses to sanction and certify devices prior to the final release of the standard.

Chapter Summary

- Wireless LAN devices are in many respects similar to those found in a wired network. The difference is that wireless devices use an antenna or other means to send and receive signals instead of a wired connection. A wireless network interface card performs the same function as a wired NIC in that it receives signals from the network. There are a variety of different types of wireless NICs: PCI expansion cards; USB stand alone or key fob devices generally for desktop computers; CardBus, PC Card Type II or Type III, or Mini PCI cards for laptops; and CompactFlash and SDIO cards for PDAs.
- An access point (AP) serves as both the base station for the wireless network and a bridge to connect the wireless network with the wired network. The range of an access point and the number of wireless clients that it can support vary. Power over Ethernet (IEEE 802.3af) technology allows an AP to be positioned in almost any location because electrical current is supplied through the Ethernet cable.
- A remote wireless bridge is a wireless device designed to connect two or more wired or wireless networks together. Remote wireless bridges can use a point-to-point or a point-to-multipoint configuration. Remote wireless bridges can function in four different modes: access point mode, root mode, non-root mode, and repeater mode. A wireless gateway is a device that combines wireless management and security management in a single appliance.
- There are several advantages of standards for the IT industry. Standards ensure that devices from one vendor will interoperate with those from other vendors. Standards also create competition between vendors, which results in lower costs for consumers and often results in lower costs of manufacturing as well. However, there are disadvantages to standards, particularly in international markets. There are three types of telecommunications standards: de facto, de jure, and by consortia.
- There are three regulatory bodies that play a major role in wireless LAN technology. The IEEE has developed network standards since 1980. The Wi-Fi Alliance is a consortium of wireless equipment manufacturers and software providers involved in promoting and certifying wireless technology. The Federal Communications Commission (FCC) is responsible for controlling and regulating wireless transmissions in the United States.
- There currently are three standards or types of wireless LANs. IEEE 802.11b networks transmit at 11 Mbps over a distance of up to 115 meters (375 feet). The 802.11a standard devices transmit at up to 54 Mbps but only up to 30 meters (100 feet). A compromise between the two, the 802.11g, can transmit at 54 Mbps up to 115 meters (375 feet).

KEY TERMS

access point mode — A mode of a remote wireless bridge that causes it to function only as a standard access point.

bands — Different sections of the radio frequency spectrum.

bridge — A device used to connect two network segments together.

client network adapter — A device it connects a computer to a wired network.

CompactFlash (CF) card — A small circuit board the contains flash memory chips and a dedicated controller chip.

consortia — Industry sponsored organizations that promote a specific technology.

de facto standard — Common practice that the industry follows.

de jure standard — Official standard set and controlled by an organization or body.

delay spread — Technology that minimizes the spread of the signal so that it can reach farther distances.

detector — A device that receives the signal in an infrared wireless network.

diffused transmission — An infrared wireless transmission that relies on reflected light.

directed transmission — An infrared wireless transmission that requires the emitter and detector to be directly aligned.

emitter — A device that transmits a signal in an infrared wireless network.

Federal Communications Commission (FCC) — The primary regulatory agency for wireless communications in United States.

flash memory — A type of solid-state technology in which there are no moving parts.

IEEE 802.11 — A wireless local area network with a bandwidth of 2 Mbps.

IEEE 802.11a — A wireless local area network with a bandwidth of 54 Mbps that uses the U-NII band.

IEEE 802.11b — A wireless local area network with a bandwidth of 11 Mbps that uses the ISM band.

IEEE 802.11g — And wireless local area network with the bandwidth of 54 Mbps that uses the ISM band.

IEEE 802.11n — A proposed new wireless LAN standard.

Industrial, Scientific, and Medical (ISM) — An unregulated band used for WLAN transmissions.

infrared light — Invisible light that can be used for wireless transmissions.

Institute of Electrical and Electronics Engineers (IEEE) — An organization that establishes standards for networks.

license exempt spectrum — Radio spectrum available to any users without a license.

light spectrum — All the different types of light that travel from the sun to the earth.

line of sight — Direct alignment of an emitter and transmitter in an infrared wireless network.

Mini PCI — A small card that is functionally equivalent to a standard PCI expansion card.

network interface card — A device that connects a computer to a wired network.

non-root mode — A mode of a remote wireless bridge that only transmits to another bridge that is in root mode.

point-to-multipoint — A configuration used to connect multiple LAN segments.
point-to-point — A configuration used to connect two LAN segments.
Power over Ethernet (PoE) — A technology that sends an electrical current through unused wires of an Ethernet cable.
Project 802 — The original effort by the IEEE to establish network standards.
proprietary — A device created by a vendor.
radio frequency spectrum — The entire range of all radio frequencies.
remote wireless bridge — A wireless device designed to connect two or more wired or wireless networks.
repeater mode — A mode of a remote wireless bridge that is used to extend the distance between LAN segments.
root mode — A mode of a remote wireless bridge that only communicates with other bridges that are not in root mode.
SDIO NOW! — A card that provides high-speed data input and output with low power consumption for mobile electronic devices.
Secure Digital I/O (SDIO) — A card that provides high-speed data input and output with low power consumption for mobile electronic devices.
sled — An external attachment for a PDA that allows CardBus and other cards to be used with it.
small office/home office (SOHO) — Small businesses or businesses run from a home office.
Unlicensed National Information Infrastructure (U-NII) — And unregulated band used for WLAN transmissions.
unregulated bands — Radio spectrum available to any users without a license.
Wi-Fi (Wireless Fidelity) Alliance — A consortium of wireless equipment manufacturers and software providers to promote wireless network technology.
Wi-Fi ZONE — An effort by the Wi-Fi Alliance to promote wireless hotspots.
Wireless Ethernet Compatibility Alliance (WECA) — A consortium of wireless equipment manufacturers and software providers to promote wireless network technology.
wireless gateway — A device that combines wireless management and security in a single appliance.

Review Questions

1. Each of the following is a wireless LAN device except
   a. wireless client network interface card
   b. wireless gateway
   c. access portal
   d. remote wireless bridge

2. A wireless client network interface card performs each of the following tasks except
   a. transmitting the packet over radio waves
   b. determining when to send the packet
   c. dividing data into packets
   d. sending packets to a wired network through a root remote wireless bridge
3. The type of wireless network interface card that would not be found in a laptop computer is a(n)
   a. Mini PCI card
   b. PCI card
   c. CardBus
   d. PC Card Type III
4. A SDIO card would be used in which type of device?
   a. Laptop computer
   b. Desktop computer
   c. Personal digital assistant (PDA)
   d. Access point
5. An access point has a(n) _____ interface that allows it to connect to a wired network.
   a. RJ-45
   b. SDDIO
   c. CF
   d. RJ-111
6. One of the functions of an access point is to serve as a base station for the wireless network. True or False?
7. Although the transmission range of an access point can vary, the number of wireless clients that it can support does not vary. True or False?
8. Power over Ethernet allows wireless client network adapter cards to be placed in locations even though there is not an electrical outlet nearby. True or False?
9. A remote wireless bridge can only connect wireless networks together. True or False?
10. Both point-to-point and point-to-multipoint configurations can be supported by a remote wireless bridge. True or False?
11. A(n) _____ is a device that combines wireless management and security in a single appliance.

12. _____ standards are not formal standards but are common practices that the industry follows.
13. Industry-sponsored organizations that want to promote a specific technology are known as _____ .
14. The _____ organization has been establishing network standards for almost 25 years.
15. The _____ is a consortium that tests and certifies wireless products.
16. List and describe the four different modes in which a remote wireless bridge can function.
17. What are the features of a wireless gateway?
18. What are unregulated bands and how are they used in wireless LANs?
19. What are some limitations to infrared wireless LAN systems?
20. Give a brief summary of the characteristics of IEEE 802.11b, 802.11a, and 802.11g wireless networks.

Hands-On Projects

Project 2-1: Install a Wireless NIC

Although a wireless network interface card is standard on most laptop computers, there may be an occasion for you to install one on an older laptop. In this exercise you install a Cisco Aironet wireless client adapter into a laptop computer. Note that a Cisco card is not required for this exercise, but any standard wireless client adapter card will work. However, the installation steps may be slightly different.

1. If your laptop computer already has a wireless card you should temporarily disable it. Click **Start** and **Control Panel**.
2. Click **Network and Internet Connections** and click **Network Connections** to display your wireless connections, as seen in Figure 2-15.
3. Click **Wireless Network Connection** and then click **Disable this network device**. Minimize this window.
4. Insert the Cisco wireless client adapter. The Found New Hardware dialog box should open. In answer to the question **Can Windows connect to Windows Update to search for software?** click **Cancel**. You will manually install the drivers from the Cisco installation CD.
5. Insert the installation CD into the drive and browse its contents. Double-click the **Win-Client-802.11a-b-c-Ins-Wizard-V1.exe** program. Note that depending on the type of Cisco adapter you are using the installation program may have a slightly different name.

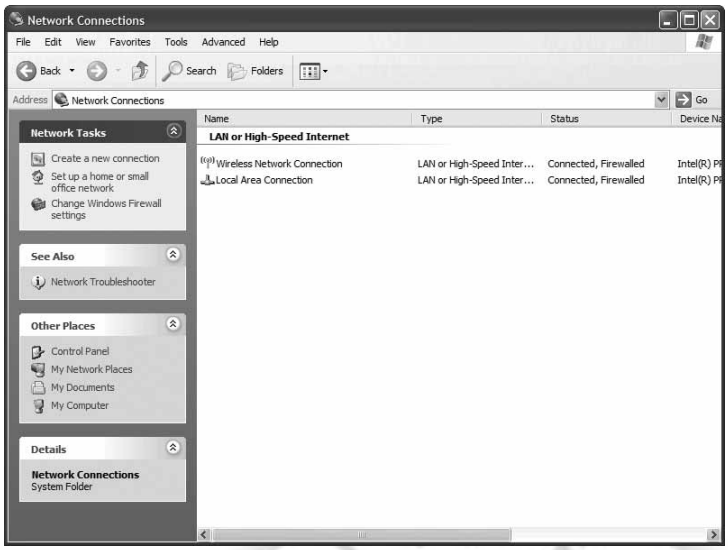

Figure 2-15 Wireless connections

6. When the **Cisco Aironet Installation Program** appears, click **Next**.
7. Click **Install Client Utilities and Driver (Recommended)**. Click **Next**.
8. When asked if you want to continue, click **Yes**.
9. Select the default destination folder, then click **Next**.
10. Accept the default program folder, then click **Next**.
11. A screen information about the Aironet Desktop Utility appears. Click **Next**.
12. Select **Cisco Aironet Desktop Utility**, then click **Next**.
13. Be sure the wireless adapter is installed, then click **OK**.
14. Click **OK** to reboot your computer.
15. The Status light should slowly blink green and the Activity light should rapidly blink amber.
16. Maximize the Network Connections window.
17. Click **Wireless Network Connection**.
18. Click **View available wireless networks** in the left pane to see a list of all the wireless networks that your computer can detect, as seen in Figure 2-16.
19. Close the Wireless Network Connections window.
20. If your laptop already had a wireless card that you disabled, click the **Safely Remove Hardware** icon in the system tray. Click **Safely remove your network card**.
21. Click **Start** and **Control Panel**.

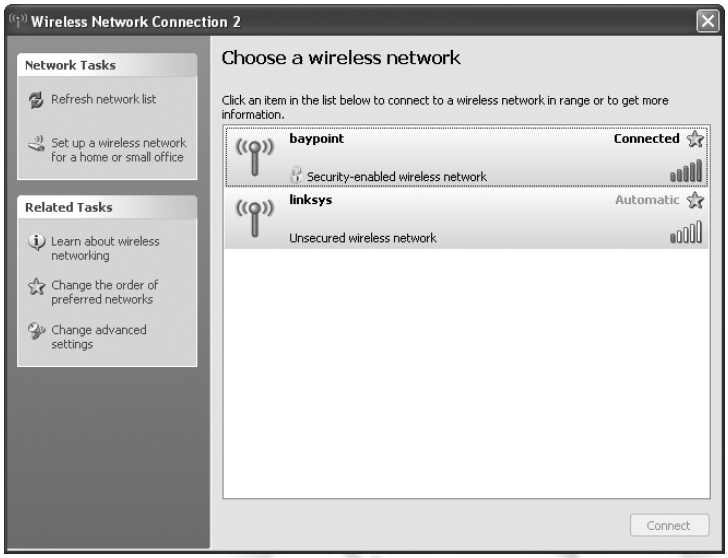

Figure 2-16 Available wireless networks

22. Click **Network and Internet Connections** and click **Network Connections**.
23. Click **Wireless Network Connection** with the right mouse button.
24. Click **Enable**.
25. Close all windows.

HANDS-ON PROJECTS

Project 2-2: Connect to a Cisco Aironet 1200 that Receives an IP Address from a DHCP Server

There are several different ways to connect to the Cisco Aironet 1200 series access point in order to manage it. Because you may not always find yourself in the same setting it is important to explore each of the different ways so you are aware of the different options. In this project you connect to the AP that is receiving an IP number from a DHCP server.

Note that the screen images shown here for these projects may look slightly different from yours depending upon which IEEE standard your Cisco Aironet 1200 is using: 802.11b, 802.11a, or 802.11g.

1. Be sure that the Cisco Aironet 1200 AP is on and functioning properly. If the AP is where you can observe it the look at the three light emitting diodes (LEDs) on the top, as seen in Figure 2-17. The three LEDs report Ethernet activity, association status, and radio activity:

- The Ethernet LED signals Ethernet traffic. This LED is normally green when an Ethernet cable is connected and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected. Be sure that this LED is green.
- The status LED signals operational status. Green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices. This LED should be blinking green.
- The radio LED signals wireless traffic over the radio interface. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point radio.

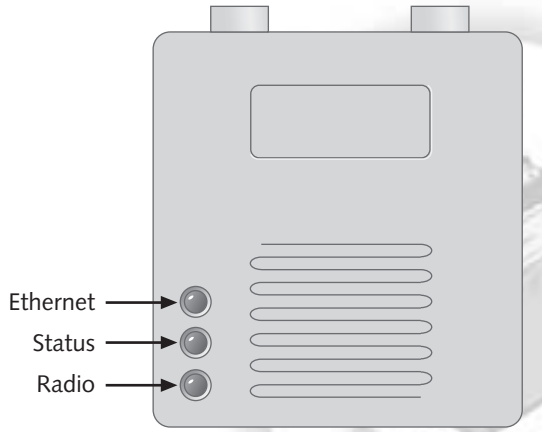

Figure 2-17 Cisco Aironet 1200 AP LEDs

2. Look on the underside of the Aironet to locate the MAC address. It will be preceded by *MAC:*.
3. If you have access to the DHCP server, look up the MAC address and find the corresponding IP address assigned to the AP. If you do not have access you may need to give this MAC address to your network manager or instructor.

Unlike consumer products that combine a DHCP server with an AP, the Cisco 1200 does not have this function.

4. Open a Web browser and enter the IP address like *http://192.168.2.30.*
5. A login screen appears. The default username is *Cisco* and the default password is also *Cisco.* Enter these and click **OK**, or enter the username and password given by your instructor.

6. A screen like Figure 2-18 appears, although your settings may look slightly different.

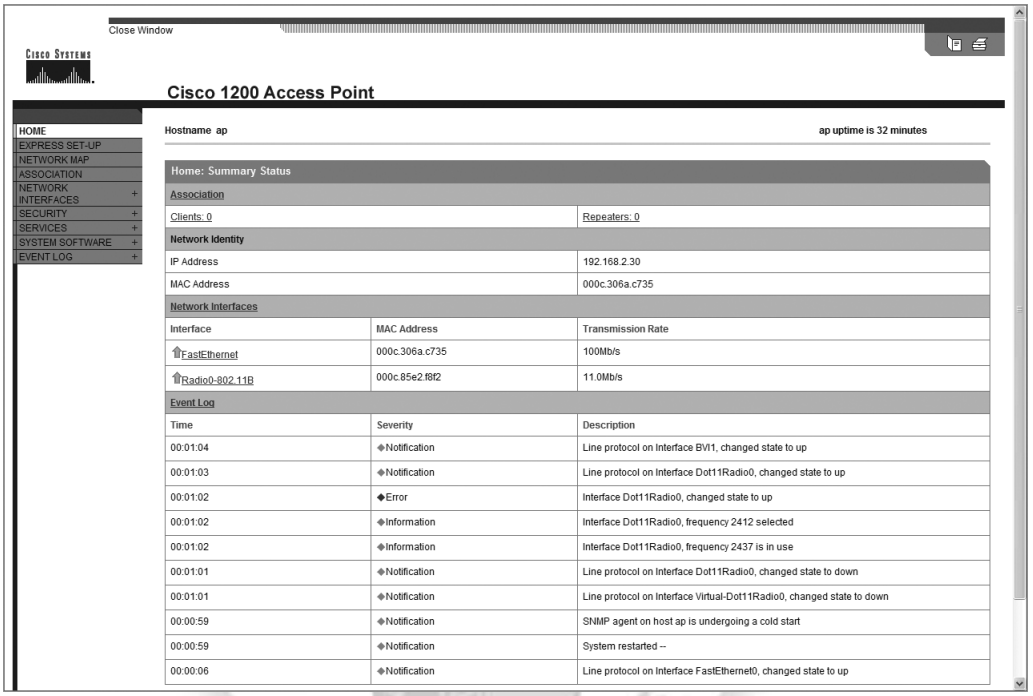

Figure 2-18 Cisco Aironet 1200 Home screen

7. Click on each of the menu options on the left side (**Express Set-Up**, **Network Map**, etc.) and view the different settings. However, do not change any settings unless instructed to do so.
8. Click **Close Window**.
9. Click **Yes** in response to the question **Do you want to close this window?** In order to use this utility you must be using a Windows XP computer.

Project 2-3: Connect to a Cisco Aironet AP Using IPSU

Not all APs receive an IP number from a DHCP server, or you may not be able to find the IP address assigned to it by DHCP. Another way in which to find the IP number assigned to the AP or to assign a number is to use the Cisco IP Setup Utility (IPSU). In this project you download, install, and use the IPSU program. In order to use this utility you must be using a Windows XP computer.

1. Open a Web browser and go to **http://www.houndware.com/website/support/downloads.html**.
2. Click **Cisco IPSU.EXE**.

3. When asked **Do you want to run or save this file?** click **Save**. Select a location to uncompress (Unzip) this file.
4. Select a location on your computer to store the file.
5. When the download is complete click **Run**. Select a location to uncompress (Unzip) this file.
6. Follow the instructions to install the program.
7. Click **Start** and **All Programs** and **Cisco Systems, Inc.** and **IPSU** to start the IPSU program, as shown in Figure 2-19.

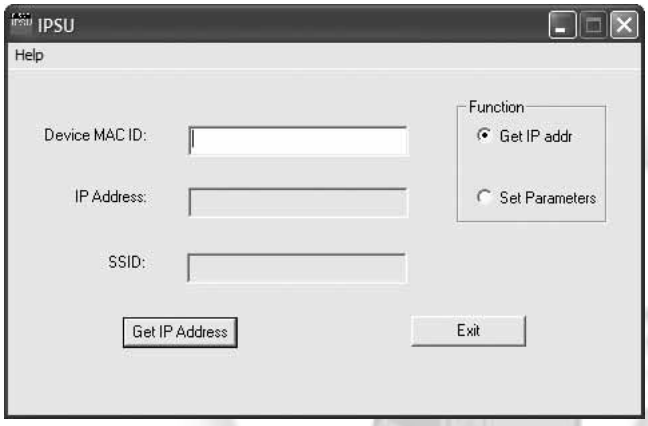

Figure 2-19 Cisco IPSU

8. If the AP has received an IP number from a DHCP server, under **Function** be sure that **Get IP addr** is selected.
9. Enter the MAC address of the AP and click **Get IP Address**. The IP address of the AP will be displayed.
10. To give the AP an IP address under **Function** click **Set parameters**. Enter the IP address to give to the AP. Note that the IP address must be in the same network segment.
11. Click the **Set Parameters** button.
12. Close all windows.
13. To reset the AP to its original factory-default settings, unplug the power cord from the AP. Press and hold the reset button labeled Mode and then plug the power cord back in. Hold the button for three seconds and then release. The AP will reset itself.

Project 2-4: Connect to a Cisco AP Using Telnet

On rare occasion you may not be able to connect to the AP using a Web browser. In this project you connect to the Cisco AP using the Windows Telnet client.

1. Click **Start** and **Run**.
2. Enter **Telnet** and click **OK** to see the Telnet window, as seen in Figure 2-20.

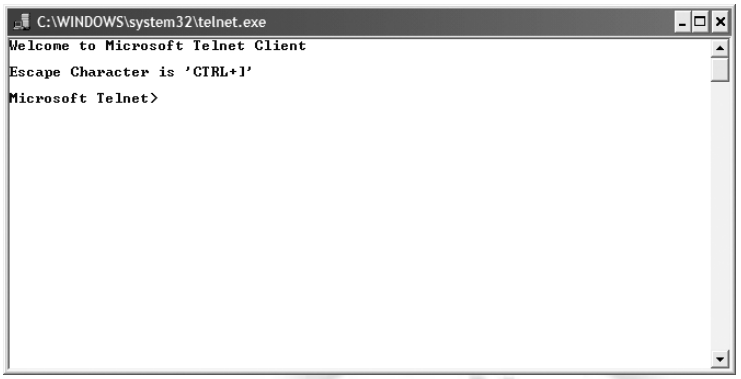

Figure 2-20 Telnet window

3. Enter **Open** and then the IP address of the AP, such as *Open 192.168.2.30.*
4. When prompted, enter the username and password. When the prompt **ap>** appears you are connected to the AP using Cisco's Command Line Interface (CLI) in User mode.
5. Enter **?** to see a list of commands. Enter several of the commands to see what information you receive.
6. Enter **enable** to go to Privileged mode. When prompted enter the AP password. The prompt will change to **ap#**.
7. Enter **show history** to see the commands you have entered.
8. Enter **disable** to return to User mode.
9. Enter **quit**.
10. Close all windows.

Project 2-5: Set up a Linksys AP

In this project you set up a Linksys AP.

1. Plug an RJ-45 patch cable into one of the ports on the Linksys AP and the other end into a network card on a computer.
2. Connect an RJ-45 patch cable from the DSL/cable modem to the port labeled **Internet**.
3. Be sure that your computer is set to receive an IP address automatically by DHCP.
4. Open a Web browser and enter **http://192.168.1.1**.
5. At the login prompt leave the username blank. Enter **admin** for the password.

6. The Linksys setup screen will appear, as seen in Figure 2-21.

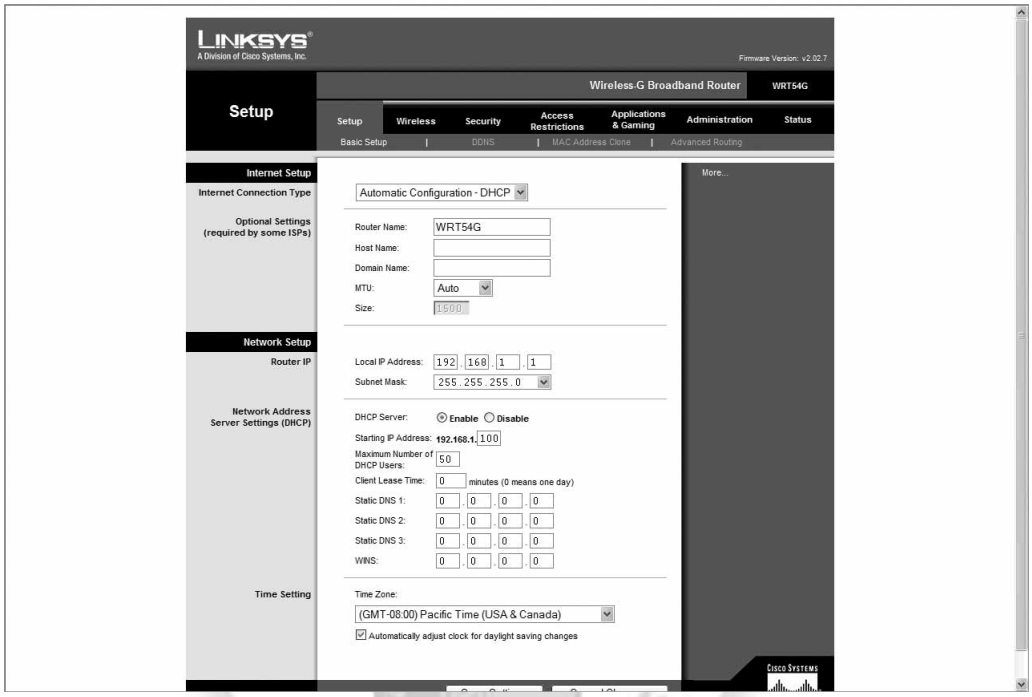

Figure 2-21 Linksys setup screen

7. Leave the **Host name** and **Domain name** fields blank unless instructed by your Internet Service Provider (ISP).
8. Under **Internet Connection Type** check with your ISP to determine if it should be changed to Static Ip or PPPoE.
9. Click **Save Settings**.
10. Click the **Wireless** tab to display the wireless screen, as seen in Figure 2-22.
11. Under **Wireless Network Mode** select **Mixed** in order to accommodate both 802.11b and 802.11g wireless clients.
12. Under **Wireless Network Name (SSID)** enter a name that is less than 32 characters in length (it is also case-sensitive). You can use spaces and special characters.
13. Click **Save Settings**.
14. Close all windows.

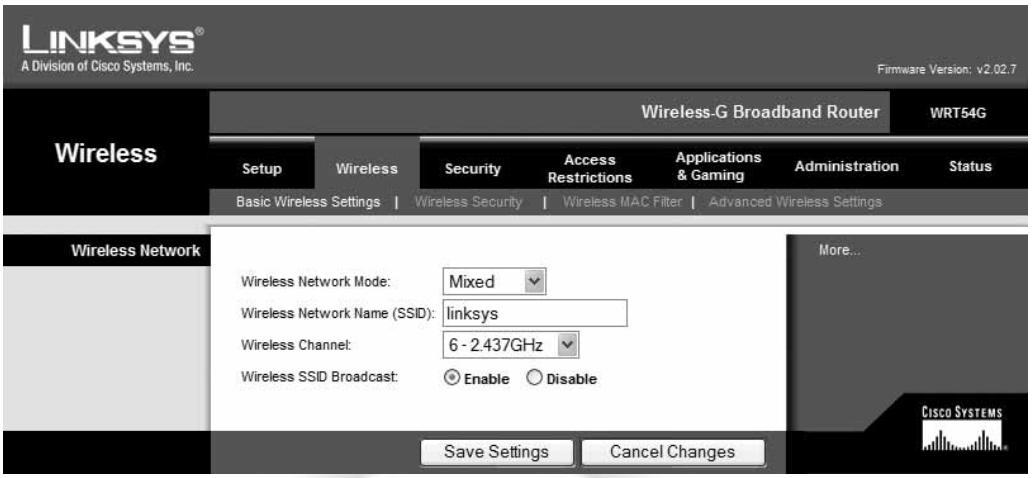

Figure 2-22 Linksys wireless screen

Case Projects

Case Project 2-1: Free or Fee Hotspots?

A debate continues today regarding wireless hotspots in public places and the fees associated with them. Some businesses look at this as a revenue stream, while others offer it as a free service to entice customers. What is your opinion? Do you visit a particular restaurant more frequently because it has a free wireless hotspot? Do you tend to spend more money at those establishments that have free hotspots as compared to those that do not? Perform a brief survey of your friends and acquaintances to see what they say. Write a one-paragraph summary of your findings.

Case Project 2-2: Pricing Wireless NICs for Laptops

Suppose that you inherit a laptop that does not have a Mini PCI wireless client adapter. Which type of wireless network adapter would you want to purchase for your laptop? Using the Internet and print sources, research different types of wireless client adapters for laptop computers. Create a table or chart that shows the advantages and disadvantages of each type along with the cost from at least three different stores or online vendors. Which would you choose?

Case Project 2-3: Comparing Access Points

Using the Internet and print media, identify APs from seven different vendors. Create a table or chart that lists each AP, its features, and costs. Which would you choose for home use? Which would you choose for a SOHO of 25 employees? Why?

Case Project 2-4: Standards and IT

Do standards stifle IT or promote it? Identify three IT professionals and ask their opinions of standards. Be prepared to discuss with them the other side of the argument they take. Write a one-page paper on your findings.

Northridge Consulting Group

Coldstone Lighting is opening another store across town and needs to install a new network. Northridge Consulting has asked you to come up with a presentation for Coldstone outlining the advantages of a wireless network for their retail store. Because the managers at Coldstone do not have a technical background, your presentation should be at a general level and not a technical level. Create a PowerPoint presentation of at least 10 slides that covers what a wireless LAN is, the equipment needed for a wireless LAN, and the advantages and disadvantages of wireless LANs.