The Wireless Spectrum

All wireless signals are carried through the air by electromagnetic waves. The **wireless spectrum** is a continuum of the electromagnetic waves used for data and voice communication. On the spectrum, waves are arranged according to their frequencies, from lowest to highest. The wireless spectrum (as defined by the FCC, which controls its use) spans frequencies between 9 KHz and 300 GHz. Each type of wireless service can be associated with one area of the wireless spectrum. AM broadcasting, for example, sits near the low-frequency end of the wireless communications spectrum, using frequencies between 535 and 1605 KHz. Infrared waves belong to a wide band of frequencies at the high-frequency end of the spectrum, between 300 GHz and 300,000 GHz. Most cordless telephones and many wireless LANs use frequencies around 2.4 GHz. Other wireless LANs use a range of frequencies near 5 GHz. Figure 8-1 shows the wireless spectrum and identifies the major wireless services associated with each range of frequencies.

In the United States, the collection of frequencies available for communication—also known as "the airwaves"—is a natural resource available for public use. The FCC grants organizations in different locations exclusive rights to use each frequency. It also determines what frequency ranges can be used for what purposes. Of course, signals propagating through the air do not necessarily remain within one nation. Therefore, it is important for countries across the world to agree on wireless communications standards. ITU is the governing body that sets standards for international wireless services, including frequency allocation, signaling and protocols used by wireless devices, wireless transmission and reception equipment, satellite orbits, and so on. If governments and companies did not adhere to ITU standards, chances are that a wireless device could not be used outside the country in which it was manufactured.

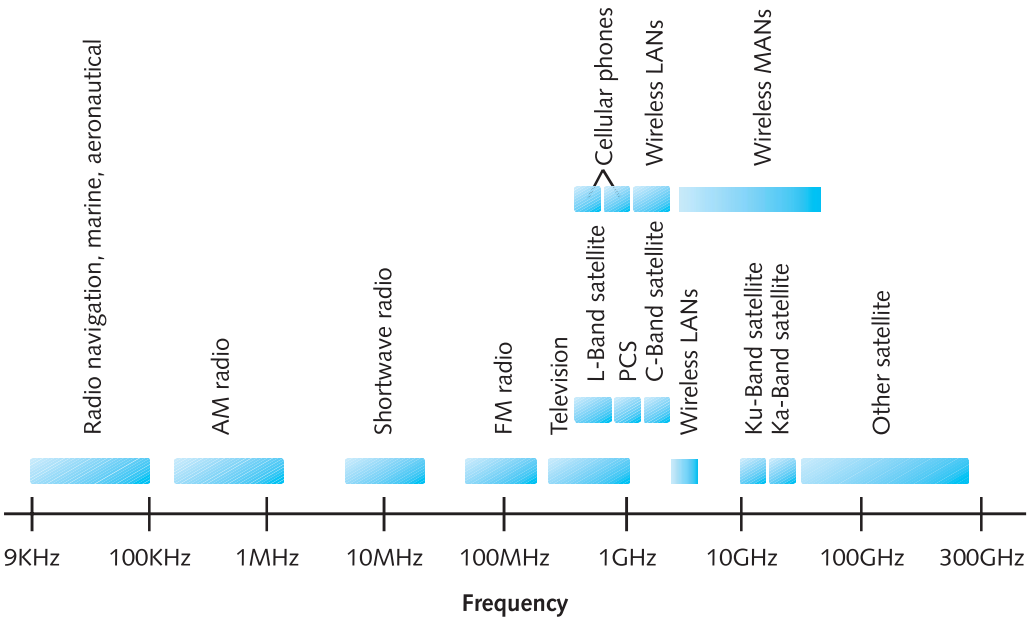

Figure 8-1 The wireless spectrum

Characteristics of Wireless Transmission

In previous chapters you learned about signals that travel over a physical medium, such as a copper or fiber-optic cable. Wired and wireless signals share many similarities, including use of the same Layer 3 and higher protocols, for example. However, the nature of the atmosphere makes wireless transmission vastly different from wired transmission. Because the air provides no fixed path for signals to follow, signals travel without guidance. Contrast this to guided media, such as UTP or fiber-optic cable, which do provide a fixed signal path. The lack of a fixed path requires wireless signals to be transmitted, received, controlled, and corrected differently from wired signals.

Just as with wired signals, wireless signals originate from electrical current traveling along a conductor. The electrical signal travels from the transmitter to an antenna, which then emits the signal, as a series of electromagnetic waves, to the atmosphere. The signal propagates through the air until it reaches its destination. At the destination, another antenna accepts the signal, and a receiver converts it back to current. Figure 8-2 illustrates this process.

Notice that antennas are used for both the transmission and reception of wireless signals. As you would expect, to exchange information, two antennas must be tuned to the same frequency. In communications terminology, this means they share the same channel. Next, you will learn about some fundamental types of antennas and their properties.

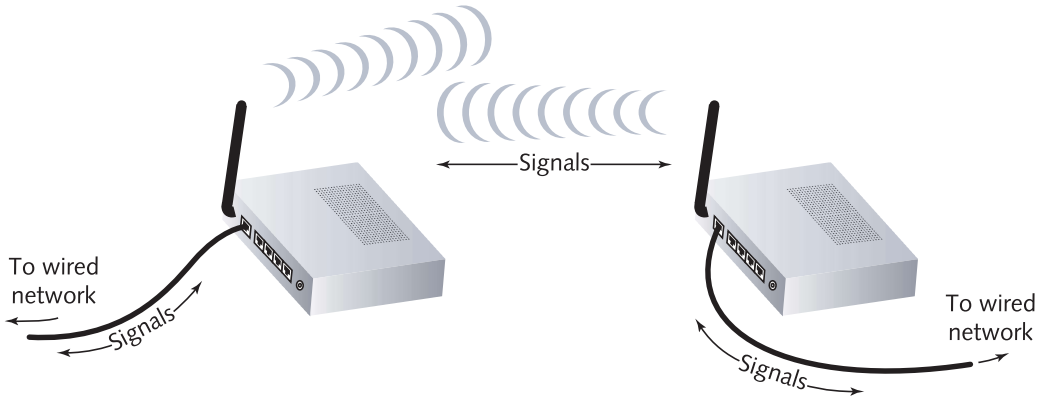

Figure 8-2 Wireless transmission and reception

Antennas

Each type of wireless service requires an antenna specifically designed for that service. The service's specifications determine the antenna's power output, frequency, and radiation pattern. An antenna's **radiation pattern** describes the relative strength over a three-dimensional area of all the electromagnetic energy the antenna sends or receives.

A **directional antenna** issues wireless signals along a single direction. This type of antenna is used when the source needs to communicate with one destination, as in a point-to-point link. A satellite downlink (for example, the kind used to receive digital TV signals) uses directional antennas. In contrast, an **omnidirectional antenna** issues and receives wireless signals with

equal strength and clarity in all directions. This type of antenna is used when many different receivers must be able to pick up the signal, or when the receiver's location is highly mobile. TV and radio stations use omnidirectional antennas, as do most towers that transmit cellular telephone signals.

The geographical area that an antenna or wireless system can reach is known as its **range**. Receivers must be within the range to receive accurate signals consistently. Even within an antenna's range, however, signals may be hampered by obstacles and rendered unintelligible.

Signal Propagation

Ideally, a wireless signal would travel directly in a straight line from its transmitter to its intended receiver. This type of propagation, known as **LOS (line-of-sight)**, uses the least amount of energy and results in the reception of the clearest possible signal. However, because the atmosphere is an unguided medium and the path between a transmitter and a receiver is not always clear, wireless signals do not usually follow a straight line. When an obstacle stands in a signal's way, the signal may pass through the object or be absorbed by the object, or it may be subject to any of the following phenomena: reflection, diffraction, or scattering. The object's geometry governs which of these three phenomena occurs.



Reflection in wireless signaling is no different from reflection of other electromagnetic waves, such as light. The wave encounters an obstacle and reflects—or bounces back—toward its source. A wireless signal will bounce off objects whose dimensions are large compared to the signal's average wavelength. In the context of a wireless LAN, which may use signals with wavelengths between one and 10 meters, such objects include walls, floors, ceilings, and the Earth. In addition, signals reflect more readily off conductive materials, like metal, than insulators, like concrete.

In **diffraction**, a wireless signal splits into secondary waves when it encounters an obstruction. The secondary waves continue to propagate in the direction in which they were split. If you could see wireless signals being diffracted, they would appear to be bending around the obstacle. Objects with sharp edges—including the corners of walls and desks—cause diffraction.

Scattering is the diffusion, or the reflection in multiple different directions, of a signal. Scattering occurs when a wireless signal encounters an object that has small dimensions compared to the signal's wavelength. Scattering is also related to the roughness of the surface a wireless signal encounters. The rougher the surface, the more likely a signal is to scatter when it hits that surface. In an office building, objects such as chairs, books, and computers cause scattering of wireless LAN signals. For signals traveling outdoors, rain, mist, hail, and snow may all cause scattering.

Because of reflection, diffraction, and scattering, wireless signals follow a number of different paths to their destination. Such signals are known as **multipath** signals. Figure 8-3 illustrates multipath signals caused by these three phenomena.

The multipath nature of wireless signals is both a blessing and a curse. On one hand, because signals bounce off obstacles, they have a better chance of reaching their destination. In environments such as an office building, wireless services depend on signals bouncing off walls, ceilings, floors, and furniture so that they may eventually reach their destination. Imagine

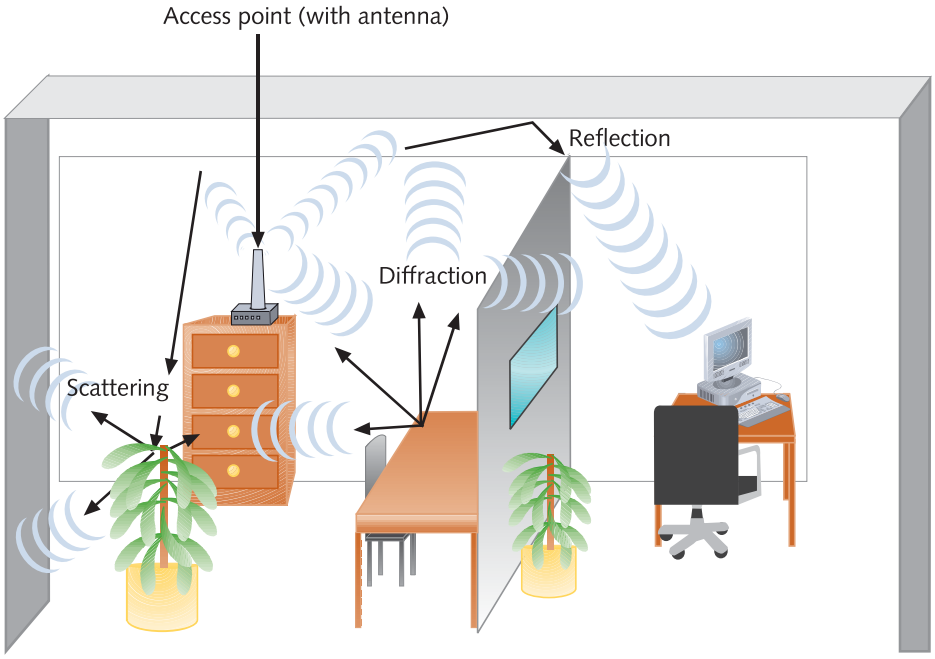

Figure 8-3 Multipath signal propagation

how inconvenient and inefficient it would be, for example, to make sure you were standing within clear view of a transmitter to receive a paging signal.

The downside to multipath signaling is that, because of their various paths, multipath signals travel different distances between their transmitter and a receiver. Thus, multiple instances of the same signal can arrive at a receiver at different times, causing signal delay.

Net+ Signal Degradation

4.7

No matter what paths wireless signals take, they are bound to run into obstacles. When they do, the original signal issued by the transmitter will experience **fading**, or a change in signal strength as a result of some of the electromagnetic energy being scattered, reflected, or diffracted after being issued by the transmitter. Because of fading, the strength of the signal that reaches the receiver is lower than the transmitted signal's strength. This makes sense because as more waves are reflected, diffracted, or scattered by obstacles, fewer are likely to reach their destination.

As with wired signals, wireless signals also experience attenuation. After a signal is transmitted, the farther it moves away from the transmission antenna the more it weakens. Just as with wired transmission, wireless signals are amplified (if analog) or repeated (if digital) to strengthen the signal so that it can be clearly received. The difference is that the intermediate points through which wireless signals are amplified or repeated are transceivers connected to antennas.

However, attenuation is not the most severe flaw affecting wireless signals. Wireless signals are also susceptible to noise (more often called electromagnetic interference or simply, interference, in the context of wireless communications). Interference is a significant problem for wireless

Net+ 4.7

communications because the atmosphere is saturated with electromagnetic waves. For example, wireless LANs may be affected by cellular phones, mobile phones, or overhead lights.

Interference can distort and weaken a wireless signal in the same way that noise distorts and weakens a wired signal. However, because wireless signals cannot depend on a conduit or shielding to protect them from extraneous EMI, they are more vulnerable to noise. The extent of interference that a wireless signal experiences depends partly on the density of signals within a geographical area. Signals traveling through areas in which many wireless communications systems are in use—for example, the center of a metropolitan area—are the most apt to suffer interference.

Frequency Ranges

Net+ 1.7

For many years WLANs have relied on frequencies in the range of 2.4–2.4835 GHz, more commonly known as the **2.4-GHz band**, to send and receive signals. This band offers 11 communications channels that are unlicensed in the United States. An unlicensed frequency is one for which the FCC does not require users to register their service and reserve it for their sole use. Because the 2.4 GHz band also carries cordless telephone and other types of signals, it is highly susceptible to interference. For example, on your home wireless network, your laptop might lose connectivity when your cordless telephone rings. One way to guard against this type of interference is to make sure your access point and cordless telephone use different channels within the 2.4-GHz band.



The **5-GHz band** is used by newer types of WLANs. The 5-GHz band actually comprises four frequency bands: 5.1 GHz, 5.3 GHz, 5.4 GHz, and 5.8 GHz. It consists of 24 unlicensed bands, each 20 MHz wide. Because the 5-GHz band is also used by weather and military radar communications in the United States, WLAN equipment using this range of frequencies must be able to monitor and detect radar signals and, if one is detected, switch to a different channel automatically.

Narrowband, Broadband, and Spread Spectrum Signals

Transmission technologies differ according to how much of the wireless spectrum their signals use. An important distinction is whether a wireless service uses narrowband or broadband signaling. In **narrowband**, a transmitter concentrates the signal energy at a single frequency or in a very small range of frequencies. In contrast to narrowband, broadband uses a relatively wide band of the wireless spectrum. Broadband technologies, as a result of their wider frequency bands, offer higher throughputs than narrowband technologies.

The use of multiple frequencies to transmit a signal is known as **spread-spectrum** technology (because the signal is spread out over the wireless spectrum). In other words, a signal never stays continuously within one frequency range during its transmission. One result of spreading a signal over a wide frequency band is that it requires less power per frequency than narrowband signaling. This distribution of signal strength makes spread-spectrum signals less likely to interfere with narrowband signals traveling in the same frequency band.

Spread-spectrum signaling, originally used with military wireless transmissions in World War II, remains a popular way of making wireless transmissions more secure. Because signals are split across several frequencies according to a sequence known only to the authorized transmitter and receiver, it is much more difficult for unauthorized receivers to capture and

decode spread-spectrum signals. To generic receivers, signals issued via spread-spectrum technology appear as unintelligible noise.

One specific implementation of spread spectrum is **FHSS** (**frequency hopping spread spectrum**). In FHSS transmission, a signal jumps between several different frequencies within a band in a synchronization pattern known only to the channel's receiver and transmitter. Another type of spread-spectrum signaling is called **DSSS** (**direct-sequence spread spectrum**). In DSSS, a signal's bits are distributed over an entire frequency band at once. Each bit is coded so that the receiver can reassemble the original signal upon receiving the bits.

Fixed versus Mobile

Each type of wireless communication falls into one of two categories: fixed or mobile. In **fixed** wireless systems, the locations of the transmitter and receiver do not move. The transmitting antenna focuses its energy directly toward the receiving antenna. This results in a point-to-point link. One advantage of fixed wireless is that because the receiver's location is predictable, energy need not be wasted issuing signals across a large geographical area. Thus, more energy can be used for the signal. Fixed wireless links are used in some data and voice applications. For example, a service provider may obtain data services through a fixed link with a satellite. In cases in which a long distance or difficult terrain must be traversed, fixed wireless links are more economical than cabling.

Many types of communications are unsuited to fixed wireless, however. For example, a waiter who uses a wireless handheld computer to transmit orders to the restaurant's kitchen could not use a service that requires him to remain in one spot to send and receive signals. Instead, wireless LANs, along with cellular telephone, paging, and many other services use mobile wireless systems. In **mobile** wireless, the receiver can be located anywhere within the transmitter's range. This allows the receiver to roam from one place to another while continuing to pick up its signal.

Now that you understand some characteristics of wireless transmission, you are ready to learn about the way most wireless LANs are structured. Later, you'll learn about their access methods and how to install wireless connectivity devices.

WLAN (Wireless LAN) Architecture

Net+ 3.1 3.4

Because they are not bound by cabling paths between nodes and connectivity devices, wireless networks are not laid out using the same topologies as wired networks. They have their own, different layouts. Smaller wireless networks, in which a small number of nodes closely positioned need to exchange data, can be arranged in an ad hoc fashion. In an **ad hoc** WLAN, wireless nodes, or **stations**, transmit directly to each other via wireless NICs without an intervening connectivity device, as shown in Figure 8-4.

However, an ad hoc arrangement would not work well for a WLAN with many users or whose users are spread out over a wide area, or where obstacles could stand in the way of signals between stations. Instead of communicating directly with each other in ad hoc mode, nearly all WLANs use the infrastructure mode, which depends on an intervening connectivity device called an access point. An **access point** (**AP**) is a device that accepts wireless signals from multiple

Net+
3.1
3.4

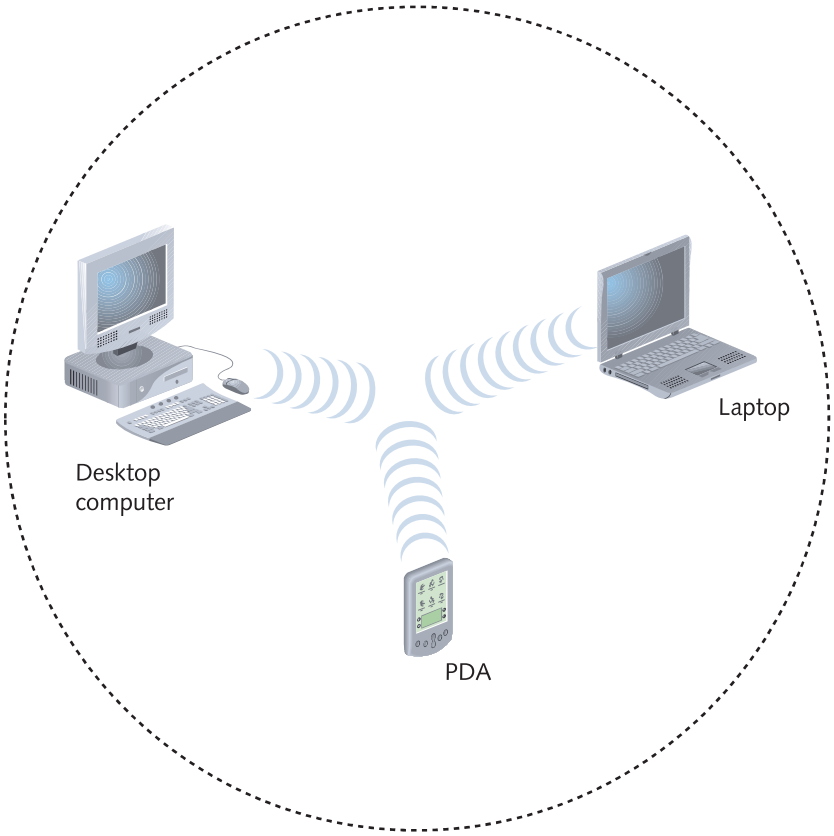

Figure 8-4 An ad hoc WLAN

nodes and retransmits them to the rest of the network. Access points may also be known as **base stations**. Access points for use on small office or home networks often include routing functions. As such, they may also be called **wireless routers** or **wireless gateways**.

To cover its intended range, an access point must have sufficient power and be strategically placed so that stations can communicate with it. For instance, if an access point serves a group of workstations in several offices on one floor in a building, it should probably be located in an open area near the center of that floor. And like other wireless devices, access points contain an antenna connected to their transceivers. An **infrastructure WLAN** is shown in Figure 8-5.

It's common for a WLAN to include several access points. The number of access points depends on the number of stations a WLAN connects. The maximum number of stations each access point can serve varies from 10 to 100, depending on the wireless technology used. Exceeding the recommended maximum leads to a greater incidence of errors and slower overall transmission.

Mobile networking allows wireless nodes to roam from one location to another within a certain range of their access point. This range depends on the wireless access method, the equipment manufacturer, and the office environment. As with other wireless technologies, WLAN signals

Net+
3.1
3.4

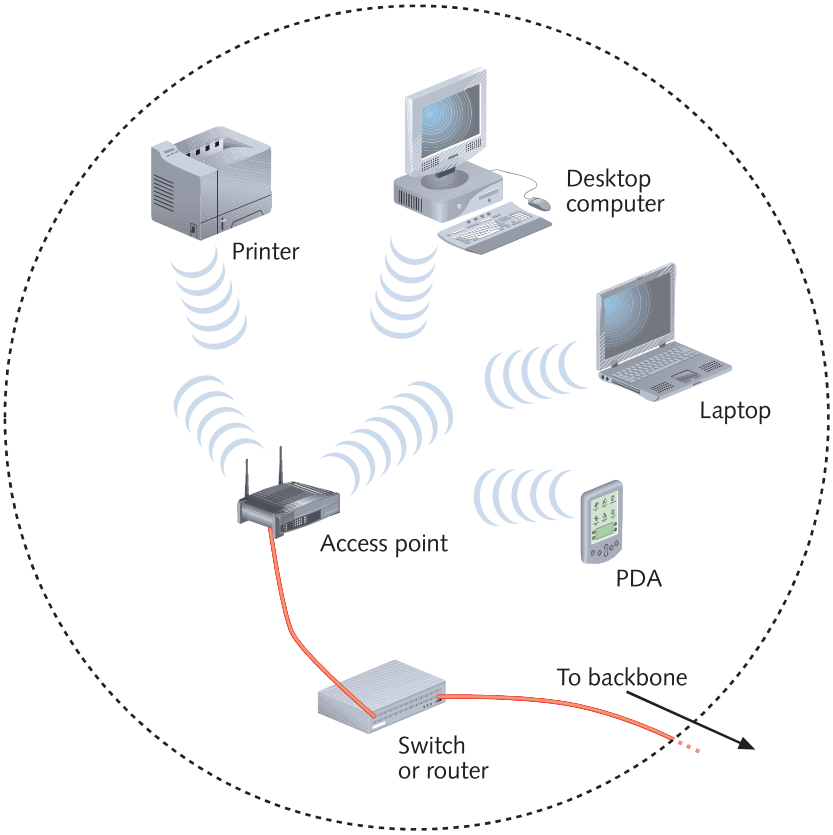

Figure 8-5 An infrastructure WLAN

are subject to interference and obstruction that cause multipath signaling. Therefore, a building with many thick, concrete walls, for example, will limit the effective range of a WLAN more severely than an open area divided into cubicles. In most WLAN scenarios, stations must remain within 300 feet of an access point to maintain optimal transmission speeds.

In addition to connecting multiple nodes within a LAN, wireless technology can be used to connect two different parts of a LAN or two separate LANs. Such connections typically use a fixed link with directional antennas between two access points, as shown in Figure 8-6. Because point-to-point links only have to transmit in one direction, they can apply more energy to signal propagation than mobile wireless links. As a result of applying more energy to the signal, their maximum transmission distance is greater. In the case of connecting two WLANs, access points could be as far as 1000 feet apart.

WLANs support the same protocols (for example, TCP/IP) and operating systems (for example, UNIX, Linux, or Windows) as wired LANs. This compatibility ensures that wireless and wired transmission methods can be integrated on the same network. Only the signaling techniques differ between wireless and wired portions of a LAN. However, techniques for generating and encoding wireless signals vary from one WLAN standard to another. The following section describes the most popular WLAN Physical and Data Link layer standards.

Net+ 3.1 3.4

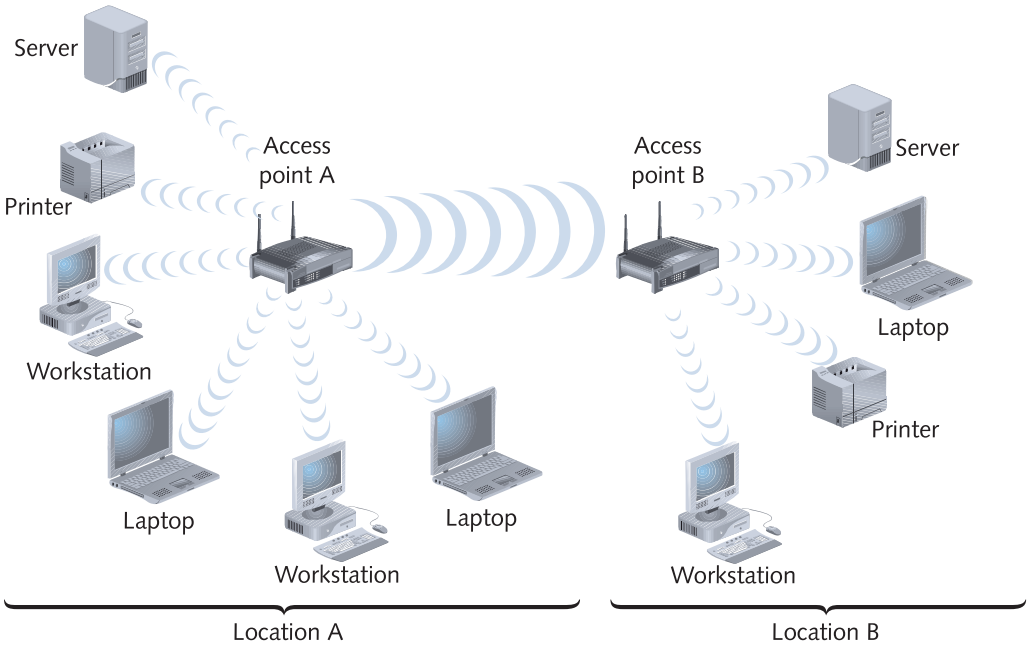

Figure 8-6 Wireless LAN interconnection

8

802.11 WLANs

Net+ 1.7

Similar to the development of wired network access technologies, the evolution of wireless access methods did not follow one direct and cooperative path, but grew from the efforts of multiple vendors and organizations. Now, the industry accepts a handful of different wireless technologies. Each wireless technology is defined by a standard that describes unique functions at both the Physical and the Data Link layers of the OSI model. These standards differ in their specified signaling methods, geographic ranges, and frequency usages, among other things. Such differences make certain technologies better suited to home networks and others better suited to networks at large organizations. The most popular wireless standards used on contemporary LANs are those developed by IEEE's 802.11 committee.

IEEE released its first wireless network standard in 1997. Since then, its WLAN standards committee, also known as the 802.11 committee, has published several distinct standards related to wireless networking. Each IEEE wireless network access standard is named after the 802.11 task group (or subcommittee) that developed it. The three IEEE 802.11 task groups that have generated notable wireless standards are 802.11b, 802.11a, and 802.11g. In addition, a fourth standard, 802.11n, in draft form at the time this was written, will be ratified in 2009. These four 802.11 standards (also known as **Wi-Fi**, for wireless fidelity) share many characteristics. For example, although some of their Physical layer services vary, all three use half-duplex signaling. In other words, a wireless station using one of the 802.11 techniques can either transmit or receive, but cannot do both simultaneously (assuming the station has only one transceiver installed, as is usually the case). In addition, all 802.11 networks follow the same access method, as described in the following section.

Access Method

Net+ 1.7

In Chapter 2 you learned that the MAC sublayer of the Data Link layer is responsible for appending physical addresses to a data frame and for governing multiple nodes' access to a single medium. As with 802.3 (Ethernet), the 802.11 MAC services append 48-bit (or 6-byte) physical addresses to a frame to identify its source and destination. The use of the same physical addressing scheme allows 802.11 networks to be easily combined with other IEEE 802 networks, including Ethernet networks. However, because wireless devices are not designed to transmit and receive simultaneously (and, therefore, cannot quickly detect collisions), 802.11 networks use a different access method than Ethernet networks.

802.11 standards specify the use of **CSMA/CA** (**Carrier Sense Multiple Access with Collision Avoidance**) to access a shared medium. Using CSMA/CA, before a station begins to send data on an 802.11 network, it checks for existing wireless transmissions. If the source node detects no transmission activity on the network, it waits a brief, random amount of time, and then sends its transmission. If the source does detect activity, it waits a brief period of time before checking the channel again. The destination node receives the transmission and, after verifying its accuracy, issues an acknowledgment (ACK) packet to the source. If the source receives this acknowledgment, it assumes the transmission was properly completed. However, interference or other transmissions on the network could impede this exchange. If, after transmitting a message, the source node fails to receive acknowledgment from the destination node, it assumes its transmission did not arrive properly, and it begins the CSMA/CA process anew. Compared to CSMA/CD (Carrier Sense Multiple Access with Collision Detection), CSMA/CA minimizes, but does not eliminate, the potential for collisions.

The use of ACK packets to verify every transmission means that 802.11 networks require more overhead than 802.3 networks. Therefore, a wireless network with a theoretical maximum throughput of 10 Mbps will, in fact, transmit less data per second than a wired Ethernet network with the same theoretical maximum throughput. In reality, most wireless networks tend to achieve between one-third and one-half of their theoretical maximum throughput. For example, one type of 802.11 network, 802.11g, is rated for a maximum of 54 Mbps; most 802.11g networks achieve between 20 and 25 Mbps. As described later in this chapter, however, the new 802.11n standard includes several techniques for reducing overhead and making the technology's actual throughput match its theoretical throughput.

One way to ensure that packets are not inhibited by other transmissions is to reserve the medium for one station's use. In 802.11, this can be accomplished through the optional **RTS/CTS** (**Request to Send/Clear to Send**) protocol. RTS/CTS enables a source node to issue an RTS signal to an access point requesting the exclusive opportunity to transmit. If the access point agrees by responding with a CTS signal, the access point temporarily suspends communication with all stations in its range and waits for the source node to complete its transmission. RTS/CTS is not routinely used by wireless stations, but for transmissions involving large packets (those more subject to damage by interference), RTS/CTS can prove more efficient. On the other hand, using RTS/CTS further decreases the overall efficiency of the 802.11 network.

Association

Suppose you have just purchased a new laptop with a wireless NIC that supports one of the 802.11 wireless standards. When you bring your laptop to a local Internet café and turn it on, your laptop soon prompts you to log on to the café's wireless network to gain access to the Internet. This seemingly simple process, known as **association**, involves a number of

Net+ 1.7

packet exchanges between the café's access point and your computer. Association is another function of the MAC sublayer described in the 802.11 standard.

As long as a station is on and has its wireless protocols running, it periodically surveys its surroundings for evidence of an access point, a task known as **scanning**. A station can use either active scanning or passive scanning. In **active scanning**, the station transmits a special frame, known as a **probe**, on all available channels within its frequency range. When an access point finds the probe frame, it issues a probe response. This response contains all the information a station needs to associate with the access point, including a status code and station ID number for that station. After receiving the probe response, a station can agree to associate with that access point. The two nodes begin communicating over the frequency channel specified by the access point.

In **passive scanning**, a wireless station listens on all channels within its frequency range for a special signal, known as a **beacon frame**, issued from an access point. The beacon frame contains information that a wireless node requires to associate itself with the access point. For example, the frame indicates the network's transmission rate and the **SSID (service set identifier)**, a unique character string used to identify an access point. After detecting a beacon frame, the station can choose to associate with that access point. The two nodes agree on a frequency channel and begin communicating.



When setting up a WLAN, most network administrators use the access point's configuration utility to assign a unique SSID (rather than the default SSID provided by the manufacturer). This can contribute to better security and easier network management. For example, the access point used by employees in the customer service department of a company could be assigned the SSID "CustSvc". In IEEE terminology, a group of stations that share an access point are said to be part of one **BSS (basic service set)**. The identifier for this group of stations is known as a **BSSID (basic service set identifier)**.

Some WLANs are large enough to require multiple access points. A group of access points connected to the same LAN are known collectively as an **ESS (extended service set)**. BSSs that belong to the same ESS share a special identifier, called an **ESSID (extended service set identifier)**. (In practice, many networking professionals don't distinguish between the terms *SSID* and *ESSID*. They simply configure every access point in a group or LAN with the same SSID.)

Within an ESS, a client can associate with any one of many access points that use the same ESSID. That allows users to roam about an office without losing wireless network service. In fact, **roaming** is the term applied to a station moving from one BSS to another without losing connectivity.

Figure 8-7 illustrates a network with only one BSS; Figure 8-8 shows a network encompassing multiple BSSs that form an ESS.

Net+ 1.7 6.6

If a station detects the presence of several access points, it will choose the one with the strongest signal and the lowest error rate compared to other access points. Note that a station does not necessarily choose the *closest* access point. For example, in the case of an Internet café, if another user brought his own access point to the café and his access point had a signal twice as strong as the café's access point, even if the new access point were farther away, your laptop would associate with it instead. Other users' laptops would also associate with his access point. (This assumes that the laptops are not configured to connect to only one specific access point, identified by its SSID in the station's wireless connection properties). This situation can present a security risk for any station within range of this powerful, rogue access point.

Net+ 1.7

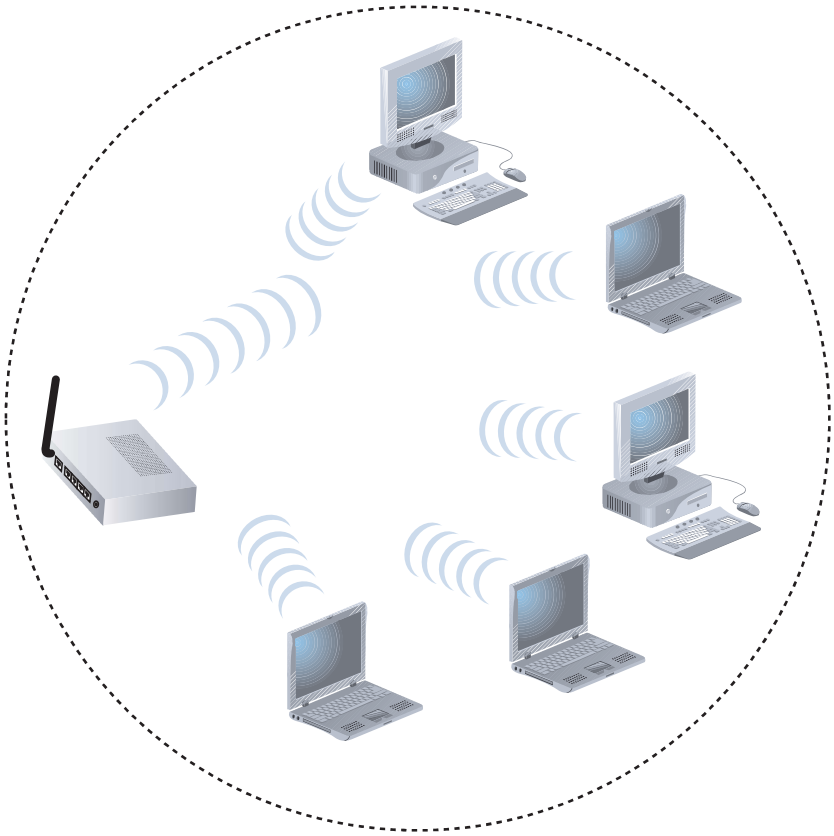

Figure 8-7 A network with a single BSS

On a network with several authorized access points in an ESS, however, a station must be able to associate with any access point while maintaining network connectivity. Suppose that when you begin work in the morning at your desk, your laptop associates with an access point located in a telco room down the hall. Later, you need to give a presentation in the company's main conference room on another floor of your building. Without your intervention, your laptop will choose a different access point as you travel to the conference room (perhaps more than one, depending on the size of your company's building and network).

Connecting to a different access point requires reassociation. **Reassociation** occurs when a mobile user moves out of one access point's range and into the range of another, as described in the previous example. It might also happen if the initial access point is experiencing a high rate of errors. On a network with multiple access points, network managers can take advantage of the stations' scanning feature to automatically balance transmission loads between those access points.



The IEEE 802.11 standard specifies communication between two wireless nodes, or stations, and between a station and an access point. However, it does not specify how two access points should communicate. Therefore, when designing an 802.11 network, it is best to use access points manufactured by the same company, to ensure full compatibility.

Net+
1.7

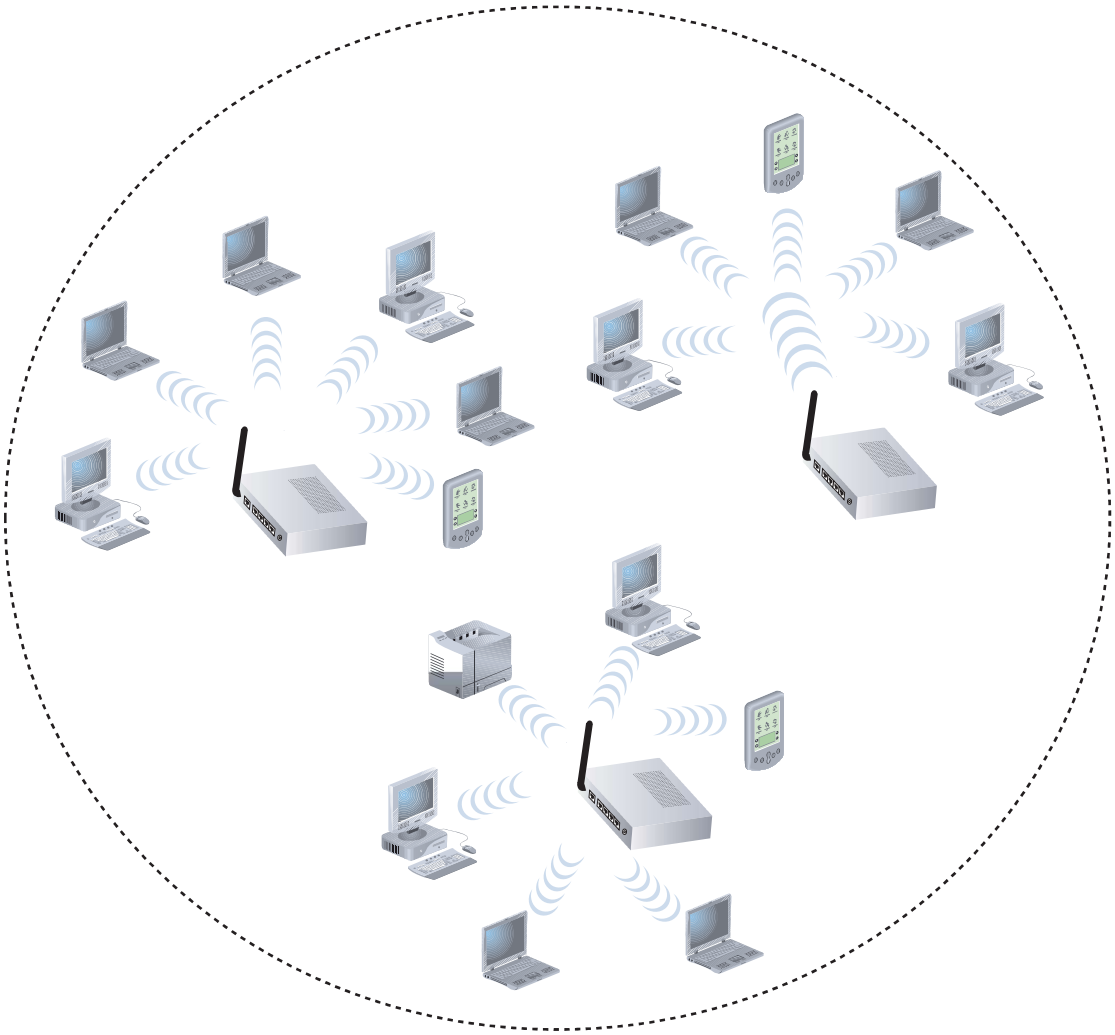

Figure 8-8 A network with multiple BSSs forming an ESS

Frames

You have learned about some types of overhead required to manage access to the 802.11 wireless networks—for example, ACKs, probes, and beacons. For each function, the 802.11 standard specifies a frame type at the MAC sublayer. These multiple frame types are divided into three groups: control, management, and data. Management frames are those involved in association and reassociation, such as the probe and beacon frames. Control frames are those related to medium access and data delivery, such as the ACK and RTS/CTS frames. Data frames are those that carry the data sent between stations. An 802.11 data frame is illustrated in Figure 8-9. (Details of control and management frames are beyond the scope of this book.) Glancing at the 802.11 data frame, its significant overhead—that is, the large quantity of fields added to the data field—becomes apparent. These fields are explained next.

Net+ 1.7

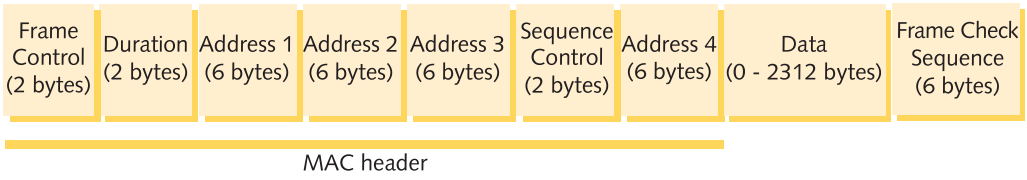

Figure 8-9 Basic 802.11 data frame

Compare the 802.11 data frame with the Ethernet II data frame pictured earlier in Figure 5-15. Notice that the wireless data frame contains four address fields, rather than two. These four addresses are the source address, transmitter address, receiver address, and destination address. The transmitter and receiver addresses refer to the access point or another intermediary device (if used) on the wireless network. The source and destination addresses have the same meaning as they do in the Ethernet II frame.

Another unique characteristic of the 802.11 data frame is its Sequence Control field. This field is used to indicate how a large packet is fragmented—that is, subdivided into smaller packets for more reliable delivery. Recall that on wired TCP/IP networks, error checking occurs at the Transport layer of the OSI model and packet fragmentation, if necessary, occurs at the Network layer. However, in 802.11 networks, error checking and packet fragmentation is handled at the MAC sublayer of the Data Link layer. By handling fragmentation at a lower layer, 802.11 makes its transmission—which is less efficient and more error prone—transparent to higher layers. This means 802.11 nodes are more easily integrated with 802.3 networks and prevent the 802.11 segments of an integrated network from slowing down the 802.3 segments.

The Frame Control field in an 802.11 data frame holds information about the protocol in use, the type of frame being transmitted, whether the frame is part of a larger, fragmented packet, whether the frame is one that was reissued after an unverified delivery attempt, what type of security the frame uses, and so on. Security is a significant concern with WLANs, because access points are typically more vulnerable than devices on a wired network. Wireless security is discussed in detail along with other network security topics in Chapter 12.

Although 802.11b, 802.11a, 802.11g, and 802.11n share all of the MAC sublayer characteristics described in the previous sections, they differ in their modulation methods, frequency usage, and ranges. In other words, each varies at the Physical layer. In addition, 802.11n modifies the way frames are used at the MAC sublayer. The following sections summarize those differences.

802.11b

In 1999, the IEEE released its **802.11b** standard, which is unique among 802.11 standards in its use of DSSS (direct-sequence spread spectrum) signaling. Recall that in DSSS, a signal is distributed over the entire bandwidth of the allocated spectrum. 802.11b uses the 2.4–2.4835-GHz frequency range (better known as the 2.4-GHz band) and separates it into 22-MHz channels. 802.11b provides a theoretical maximum of 11-Mbps throughput; actual throughput is typically around 5 Mbps. To ensure this throughput, wireless nodes must stay within 100 meters (or approximately 330 feet) of an access point or each other, in the case of an ad hoc network. Among all the 802.11 standards, 802.11b was the first to take hold. It is also the least expensive

Net+ 1.7

of all the 802.11 WLAN technologies. In recent years, network administrators have replaced 802.11b with the much faster (and backward compatible) 802.11g standard.

802.11a

Although the 802.11a task group began its standards work before the 802.11b group, 802.11a was released after 802.11b. The **802.11a** standard differs from 802.11b and 802.11g in that it uses channels in the 5-GHz band and provides a maximum theoretical throughput of 54 Mbps, though its effective throughput falls generally between 11 and 18 Mbps. 802.11a's high throughput is attributable to its use of higher frequencies, its unique method of modulating data, and more available bandwidth. Perhaps most significant is that the 5-GHz band is not as congested as the 2.4-GHz band. Thus, 802.11a signals are less likely to suffer interference from microwave ovens, cordless phones, motors, and other (incompatible) wireless LAN signals. However, higher-frequency signals require more power to transmit, and they travel shorter distances than lower-frequency signals. The average geographic range for an 802.11a antenna is 20 meters, or approximately 66 feet. As a result, 802.11a networks require a greater density of access points between the wired LAN and wireless clients to cover the same distance that 802.11b networks cover. The additional access points, as well as the nature of 802.11a equipment, make this standard more expensive than either 802.11b or 802.11g. Of the three currently ratified 802.11 standards, 802.11a is the least popular.



802.11g

IEEE's **802.11g** WLAN standard is designed to be just as affordable as 802.11b while increasing its maximum theoretical throughput from 11 Mbps to 54 Mbps through different data modulation techniques. The effective throughput of 802.11g ranges generally from 20 to 25 Mbps. An 802.11g antenna has a geographic range of 100 meters (or approximately 330 feet).

802.11g, like 802.11b, uses the 2.4-GHz frequency band. In addition to its high throughput, 802.11g benefits from being compatible with 802.11b networks. Thus, if a network administrator installed 802.11b access points on her LAN three years ago, this year she could add 802.11g access points and laptops, and the laptops could roam between the ranges of the 802.11b and 802.11g access points without an interruption in service. 802.11g's compatibility with the more established 802.11b has caused many network managers to choose it over 802.11a, despite 802.11a's comparative advantages.

802.11n

The newest 802.11 standard drafted by IEEE is **802.11n**. At the time this was written, the standard was expected to be ratified in late 2009. However, it has been in development for years, and as early as mid-2007, manufacturers were selling 802.11n-compatible transceivers in their networking equipment. The primary goal of IEEE's 802.11n committee was to create a wireless standard that provided much higher effective throughput than the other 802.11 standards. By all accounts, they succeeded. 802.11n boasts a maximum throughput of 600 Mbps, making it a threat to Fast Ethernet and a realistic platform for telephone and video signals. IEEE also specified that the 802.11n standard must be backward compatible with the 802.11a, b, and g standards.

802.11n may use either the 2.4-GHz or 5-GHz frequency range. It employs the same data modulation techniques used by 802.11a and 802.11g. However, it differs dramatically from

Net+ 1.7

the other three 802.11 standards in how it manages frames, channels, and encoding. These differences, which allow 802.11n to achieve its high throughput, include the following innovations:

- **MIMO (multiple input-multiple output)**—In 802.11n, multiple antennas on an access point may issue a signal to one or more receivers. As you learned earlier, signals issued by an omnidirectional antenna will propagate in a multipath fashion. Therefore, multiple signals cannot be expected to arrive at the same receiver in concert. To account for this, in MIMO the phases of these signals are adjusted when they reach a receiving station, and the strength of the multiple signals are summed. To properly adjust phases, MIMO requires stations to update access points with information about their location. Among 802.11 equipment, this function is only available with 802.11n-capable transceivers. In addition to increasing the network's throughput, MIMO can increase an access point's range. Figure 8-10 shows an 802.11n access point with three antennas.
- **Channel bonding**—In 802.11n, two adjacent 20-MHz channels can be combined, or bonded, to make a 40-MHz channel. In fact, bonding two 20-MHz channels more than doubles the bandwidth available in a single 20-MHz channel. That's because the small amount of bandwidth normally reserved as buffers against interference at the top



Figure 8-10 802.11n access point with three antennas

Net+ 1.7

and bottom of the 20-MHz channels can be assigned to carry data instead. Channel bonding is not recommended for use in the 2.4-GHz band, however. In that range, the probability of interference is too high to make channel bonding practical. Because the 5-GHz band contains more channels and is less crowded (at least, for now), it's better suited to channel bonding.

- Higher modulation rates—As mentioned earlier, 802.11n uses the same type of data modulation used by 802.11a and 802.11g. This modulation technique allows for a single channel to be subdivided into multiple, smaller channels. Simply put, 802.11n makes more efficient use of these smaller channels and is capable of choosing from different encoding methods. 802.11n also allows for shortening the period of time transceivers wait between issuing each bit of data (which is necessary to prevent interference).
- Frame aggregation—802.11n networks can use one of two techniques for combining multiple frames (of the type shown in Figure 8-9) into one larger frame. Combining multiple frames reduces overhead. Suppose four small data frames are combined into one larger frame. Each larger frame will have only one copy of the same addressing information that would appear in the smaller frames. Proportionally, the data field takes up more of the aggregated frame's space. In addition, replacing four small frames with one large frame means an access point and station will have to exchange one quarter the number of statements to negotiate media access and error control. To take advantage of frame aggregation, the maximum frame size for 802.11n is 64 KB, compared to the maximum 802.11a, b, and g frame size of 4 KB. The potential disadvantage with using larger frames is the increased probability of errors when transmitting larger blocks of data. Figure 8-11 illustrates the relatively low overhead of an aggregated 802.11n frame.



Note that not all of the techniques listed here will be used in every 802.11n implementation. Further, reaching maximum throughput depends on the number and type of these strategies used. It also depends on whether the network uses the 2.4-GHz or 5-GHz band. Considering these factors, an 802.11n network's actual throughputs will vary between 65 to 600 Mbps.

As mentioned earlier, 802.11n is compatible with all three earlier versions of the 802.11 standard. However, in mixed environments, some of the new standard's techniques for improving throughput will not be possible. To ensure the fastest data rates on your 802.11n LAN, it's optimal to use only 802.11n-compatible devices.

To qualify for Network+ certification, you need to understand the differences between the 802.11 wireless standards. The next section describes the Bluetooth wireless standard, which, though less common and not included on the Network+ exam, is still used on some networks.

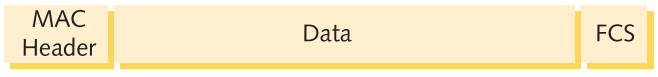

Figure 8-11 Aggregated 802.11n frame

Bluetooth Networks

In the early 1990s, Ericsson began developing a wireless networking technology for use between multiple devices, including cordless telephones, PDAs, computers, printers, keyboards, telephone headsets, and pagers, in a home. It was designed to carry voice, video, and data signals over the same communications channels. Besides being compatible with a variety of devices, this technology was also meant to require little power and cover short ranges. In 1998, Intel, Nokia, Toshiba, and IBM joined Sony Ericsson to form the **Bluetooth Special Interest Group (SIG)** (its members currently number over 9000 companies), whose aim was to refine and standardize this technology. The resulting standard was named **Bluetooth**. Bluetooth is a mobile wireless networking standard that uses FHSS (frequency hopping spread spectrum) RF signaling in the 2.4-GHz band. Recall that in FHSS, a signal hops between multiple frequencies within a band in a synchronization pattern known only to the channel's receiver and transmitter.

Bluetooth was named after King Harald I of Denmark, who ruled in the 10th century. One legend has it that he was so fond of eating blueberries that his teeth were discolored, earning him the nickname "Bluetooth." This king was also famous for unifying hostile tribes from Denmark, Norway, and Sweden, just as Bluetooth can unify disparate network nodes.

The original Bluetooth standard, version 1.1, was designed to achieve a maximum theoretical throughput of 1 Mbps. However, its effective throughput is 723 Kbps, with error correction and control data consuming the remaining bandwidth. The latest version of the standard, version 2.0, was released in 2004. This version uses different encoding schemes that allow Bluetooth to achieve up to 2.1-Mbps throughput. (The newer version of Bluetooth is backward compatible, meaning that devices running version 2.0 can communicate with devices running earlier versions of Bluetooth.) The Bluetooth 1.1 and 1.2 standards recommend that communicating nodes be spaced no farther than 10 meters (or approximately 33 feet) apart. When using Bluetooth version 2.0, communicating nodes can be as far as 30 meters (or approximately 100 feet) apart.

Bluetooth was designed to be used on small networks composed of personal communications devices, also known as **PANs (personal area networks)**. However, due to Bluetooth's relatively low throughput and short range it proved impractical for business LANs. Nevertheless, it has become a popular wireless technology for communicating among cellular telephones, phone headsets, computer peripherals (such as mice and keyboards), and PDAs.

Summary of WLAN Standards

Net+ 1.7

To summarize what you have learned about wireless network standards, Table 8-1 offers comparisons of the common wireless networking standards, their ranges, and throughputs.



The actual geographic range of any wireless technology depends on several factors, including the power of the antenna, physical barriers or obstacles between sending and receiving nodes, and interference in the environment. Therefore, although a technology is rated for a certain average geographic range, it may actually transmit signals in a shorter or longer range.

Net+ 1.7

Table 8-1 Wireless standards

Standard	Frequency range	Theoretical maximum throughput	Effective throughput (approximate)	Average geographic range
802.11b	2.4 GHz	11 Mbps	5 Mbps	100 meters (or approximately 330 feet)
802.11a	5 GHz	54 Mbps	11–18 Mbps	20 meters (or approximately 66 feet)
802.11g	2.4 GHz	54 Mbps	20–25 Mbps	100 meters (or approximately 330 feet)
802.11n	2.4 GHz or 5 GHz	65 to 600 Mbps	65 to 600 Mbps	Up to 400 meters (or approximately 1310 feet) if MIMO used
Bluetooth ver. 1.x	2.4 GHz	1 Mbps	723 Kbps	10 meters (or approximately 33 feet)
Bluetooth ver. 2.0	2.4 GHz	2.1 Mbps	1.5 Mbps	30 meters (or approximately 100 feet)



Net+ 3.4

Implementing a WLAN

Now that you understand how wireless signals are exchanged, what can hinder them, and which Physical and Data Link layer standards they may follow, you are ready to put these ideas into practice. This section first describes how to design small WLANs, the types you might use at home or in a small office. It also describes how larger, enterprise-wide WANs are formed. Next it walks you through installing and configuring access points and clients. Finally, it details the pitfalls of implementing WLANs and how to avoid them. Generally speaking, the material in this section applies to the most popular WLAN standards, 802.11b and 802.11g. However, some aspects of WLAN implementation hold true no matter which standard you follow.

Determining the Design

You have learned that WLANs may be arranged as ad hoc or infrastructure networks. You also know that infrastructure WLANs are far more common. This section assumes your WLAN follows the infrastructure model, and as such, will include access points.

A home or small office network might call for only one access point. In this case the access point, often combined with switching and routing functions, connects wireless clients to the LAN and acts as their gateway to the Internet. Note that the access point functions independently from the Internet access technology. In other words, configuring your home or small office WLAN follows the same principles no matter whether you connect to the Internet using broadband cable or DSL.

Figure 8-12 illustrates the typical arrangement of a home or small office WLAN. Notice that the access point (or wireless router) is connected to the cable or DSL modem using an RJ-45 cable. The cable is inserted into the access point's WAN port, which is set apart from the other data ports (and might be labeled "Internet" or remain unlabeled). The additional ports on the access point allow for wired access to the router. An access point that does not include routing or switching functions would lack these extra ports and act much like a wireless hub.