2

INTRODUCTION TO WIRELESS NETWORKS

Up to a point, it's quite possible to treat your wireless network as a set of black boxes that you can turn on and use without knowing much about the way they work. That's the way most people relate to the technology that surrounds them. You shouldn't have to worry about the technical specifications just to place a long-distance telephone call or heat your lunch in a microwave oven or connect your laptop computer to a network. In an ideal world (ha!), the wireless link would work as soon as you turn on the power switch.

But wireless networking today is about where broadcast radio was in the late 1920s. The technology was out there for everybody, but the people who understood what was happening behind that Bakelite-Dilecto panel (Figure 2-1) often got better performance than the ones who just expected to turn on the power switch and listen.

In order to make the most effective use of wireless networking technology, it's still important to understand what's going on inside the box (or in this case, inside each of the boxes that make up the network). This chapter describes the standards and specifications that control wireless networks and explains how data moves through the network from one computer to another.

Figure 2-1: Every new technology goes through the tweak-and-fiddle stage.

When the network is working properly, you should be able to use it without thinking about all of that internal plumbing—just click a few icons and you're connected. But when you're designing and building a new network, or when you want to improve the performance of an existing network, it can be essential to understand how all that data is supposed to move from one place to another. And when the network does something you aren't expecting it to do, you will need a basic knowledge of the technology to do any kind of useful troubleshooting.

How Wireless Networks Work

Moving data through a wireless network involves three separate elements: the radio signals, the data format, and the network structure. Each of these elements is independent of the other two, so you must define all three when you invent a new network. In terms of the OSI reference model, the radio signal operates at the physical layer, and the data format controls several of the higher layers. The network structure includes the wireless network interface adapters and base stations that send and receive the radio signals. In a wireless network, the network interface adapters in each computer and base station convert digital data to radio signals, which they transmit to other devices on the same network, and they receive and convert incoming radio signals from other network elements back to digital data.

Each of the broadband wireless data services use a different combination of radio signals, data formats, and network structure. We'll describe each type of wireless data network in more detail later in this chapter, but first, it's valuable to understand some general principles.

Radio

The basic physical laws that make radio possible are known as Maxwell's equations, identified by James Clerk Maxwell in 1864. Without going into the math, Maxwell's equations show that a changing magnetic field will produce an electric field, and a changing electric field will produce a magnetic field. When alternating current (AC) moves through a wire or other physical conductor, some of that energy escapes into the surrounding space as an alternating magnetic field. That magnetic field creates an alternating electric field in space, which in turn creates another magnetic field and so forth until the original current is interrupted.

This form of energy in transition between electricity and magnetic energy is called *electromagnetic radiation*, or *radio waves. Radio* is defined as the radiation of electromagnetic energy through space. A device that produces radio waves is called a *transmitter*, and a complementary device that detects radio waves in the air and converts them to some other form of energy is called a *receiver*. Both transmitters and receivers use specially shaped devices called *antennas* to focus the radio signal in a particular direction, or *pattern*, and to increase the amount of effective radiation (from a transmitter) or sensitivity (in a receiver).

By adjusting the rate at which alternating current flows from each transmitter through the antenna and out into space (the *frequency*), and by adjusting a receiver to operate only at that frequency, it's possible to send and receive many different signals, each at a different frequency, that don't interfere with one another. The overall range of frequencies is known as the *radio spectrum*. A smaller segment of the radio spectrum is often called a *band*.

Radio frequencies and other AC signals are expressed as cycles per second, or *hertz (Hz)*, named for Heinrich Hertz, the first experimenter to send and receive radio waves. One cycle is the distance from the peak of an AC signal to the peak of the next signal. Radio signals generally operate at frequencies in thousands, millions, or billions of hertz (kilohertz or KHz, megahertz or MHz, and gigahertz or GHz, respectively).

The simplest type of radio communication uses a continuous signal that the operator of the transmitter interrupts to divide the signal into accepted patterns of long and short signals (dots and dashes) that correspond to individual letters and other characters. The most widely used set of these patterns was Morse code, named for the inventor of the telegraph, Samuel F.B. Morse, where this code was first used.

In order to transmit speech, music, and other sounds via radio, the transmitter alters, or *modulates*, the AC signal (the carrier wave) by either mixing an audio signal with the carrier as shown in Figure 2-2 (this is called *amplitude modulation*, or *AM*) or by modulating the frequency within a narrow range as shown in Figure 2-3 (this is called *frequency modulation*, or *FM*). The AM or FM receiver includes a complementary circuit that separates the carrier from the modulating signal.

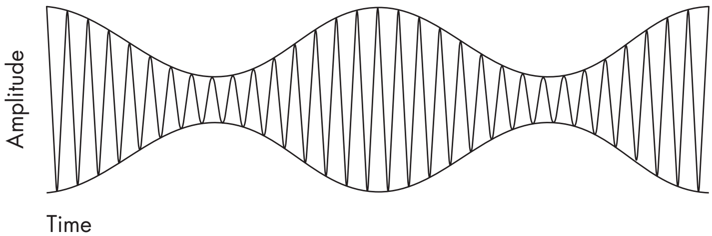

Figure 2-2: In an AM signal, the audio modulates the carrier.

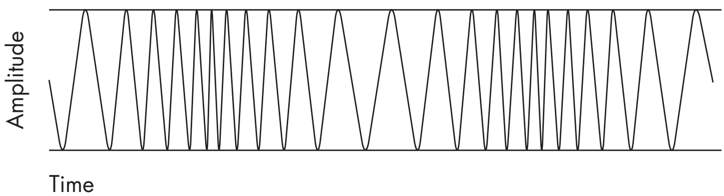

Figure 2-3: In an FM signal, the audio modulates the radio frequency.

Because two or more radio signals using the same frequency can often interfere with one another, government regulators and international agencies, such as the International Telecommunication Union (ITU), have reserved certain frequencies for specific types of modulation, and they issue exclusive licenses to individual users. For example, an FM radio station might be licensed to operate at 92.1 MHz at a certain geographical location. Nobody else is allowed to use that frequency in close enough proximity to interfere with that signal. On the other hand, some radio services don't require a license. Most unlicensed services are either restricted to very short distances, to specific frequency bands, or both.

Both AM and FM are *analog* methods because the signal that comes out of the receiver is a replica of the signal that went into the transmitter. When we send computer data through a radio link, it's *digital* because the content has been converted from text, computer code, sounds, images or other information into ones and zeroes before it is transmitted, and it is converted back to its original form after it is received. Digital radio can use any of several different modulation methods: The ones and zeroes can be two different audio tones, two different radio frequencies, timed interruptions to the carrier, or some combination of those and other techniques.

Wireless Data Networks

Each type of wireless data network operates on a specific set of radio frequencies. For example, most Wi-Fi networks operate in a special band of radio frequencies around 2.4 GHz that have been reserved in most parts of the world for unlicensed point-to-point spread spectrum radio services. Other Wi-Fi systems use a different unlicensed band around 5 GHz.

Unlicensed Radio Services

Unlicensed means that anybody using equipment that complies with the technical requirements can send and receive radio signals on these frequencies without a radio station license. Unlike most radio services (including other broadband wireless services), which require licenses that grant exclusive use of that frequency to a specific type of service and to one or more specific users, an unlicensed service is a free-for-all where everybody has an equal claim to the same airwaves. In theory, the technology of spread spectrum radio makes it possible for many users to co-exist (up to a point) without significant interference.

Point-to-Point

A *point-to-point* radio service operates a communication channel that carries information from a transmitter to a single receiver. The opposite of point-to-point is a *broadcast* service (such as a radio or television station) that sends the same signal to many receivers at the same time.

Spread Spectrum

Spread spectrum is a family of methods for transmitting a single radio signal using a relatively wide segment of the radio spectrum. Wireless Ethernet networks use several different spread spectrum radio transmission systems, which are called frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), and orthogonal frequency division multiplexing (OFDM). Some older data networks use the slower FHSS system, but the first Wi-Fi networks used DSSS, and more recent systems use OFDM. Table 2-1 lists each of the Wi-Fi standards and the type of spread spectrum modulation they use.

Table 2-1: Wi-Fi Standards and Modulation Type

Wi-Fi Type	Frequency	Modulation
802.11a	5 GHz	OFDM
802.11b	2.4 GHz	DSSS
802.11g	2.4 GHz	OFDM

Spread spectrum radio offers some important advantages over other types of radio signals that use a single narrow channel. Spread spectrum is extremely efficient, so the radio transmitters can operate with very low power. Because the signals operate on a relatively wide band of frequencies, they are less sensitive to interference from other radio signals and electrical noise, which means they can often get through in environments where a conventional narrow-band signal would be impossible to receive and understand. And because a frequency-hopping spread spectrum signal shifts among more than one channel, it can be extremely difficult for an unauthorized listener to intercept and decode the contents of a signal.

Spread spectrum technology has an interesting history. It was invented by the actress Hedy Lamarr and the American avant-garde composer George Antheil as a "Secret Communication System" for directing radio-controlled torpedoes that would not be vulnerable to enemy jamming. Before she came to Hollywood, Lamarr had been married to an arms merchant in Austria, where she learned about the problems of torpedo guidance at dinner parties with her husband's customers. Years later, shortly before the United States entered World War II, she came up with the concept of changing radio frequencies to cut through interference. *The New York Times* reported in 1941 that her "red hot" invention (Figure 2-4) was vital to the national defense, but the government would not reveal any details.

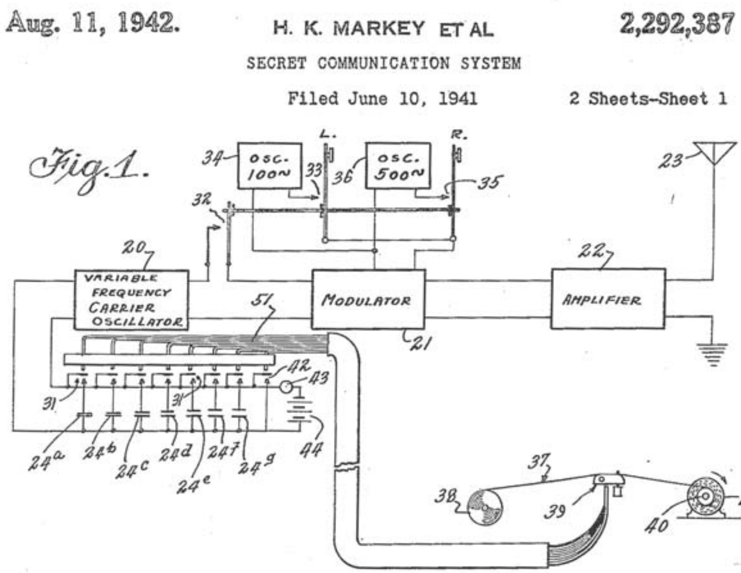

Figure 2-4: Hedy Lamarr and George Antheil received this patent in 1942 for the invention that became the foundation of spread spectrum radio communication. She is credited here under her married name, H.K. Markey. The complete document is accessible at http://uspto.gov.

Antheil turned out to be the ideal person to make this idea work. His most famous composition was an extravaganza called *Ballet Mechanique,* which was scored for sixteen player pianos, two airplane propellers, four xylophones, four bass drums, and a siren. His design used the same kind of mechanism that he had previously used to synchronize the player pianos to change radio frequencies in a spread spectrum transmission. The original slotted paper tape system had 88 different radio channels—one for each of the 88 keys on a piano.

In theory, the same method could be used for voice and data communication as well as guiding torpedoes, but in the days of vacuum tubes, paper tape, and mechanical synchronization, the whole process was too complicated to actually build and use. By 1962, solid-state electronics had replaced the vacuum tubes and piano rolls, and the technology was used aboard US Navy ships for secure communication during the Cuban Missile Crisis. Today, spread spectrum radios are used in the US Air Force Space Command's Milstar Satellite Communications System, in digital cellular telephones, and in wireless data networks.

Frequency-Hopping Spread Spectrum

Lamarr and Antheil's original design for spread spectrum radio used a *frequency-hopping system (FHSS)*. As the name suggests, FHSS technology divides a radio signal into small segments and "hops" from one frequency to another many times per second as it transmits those segments. The transmitter and the receiver establish a synchronized hopping pattern that sets the sequence in which they will use different subchannels.

FHSS systems overcome interference from other users by using a narrow carrier signal that changes frequency many times per second. Additional transmitter and receiver pairs can use different hopping patterns on the same set of subchannels at the same time. At any point in time, each transmission is probably using a different subchannel, so there's no interference between signals. When a conflict does occur, the system resends the same packet until the receiver gets a clean copy and sends a confirmation back to the transmitting station.

For some older 802.11 wireless data services, the unlicensed 2.4 MHz band is split into 75 subchannels, each of them 1 MHz wide. Because each frequency hop adds overhead to the data stream, FHSS transmissions are relatively slow.

Direct-Sequence Spread Spectrum

The *direct-sequence spread spectrum (DSSS)* technology that controls 802.11b networks uses an 11-chip Barker Sequence to spread the radio signal through a single 22 MHz–wide channel without changing frequencies. Each DSSS link uses just one channel without any hopping between frequencies. As Figure 2-5 shows, a DSSS transmission uses more bandwidth, but less power than a conventional signal. The digital signal on the left is a conventional transmission in which the power is concentrated within a tight bandwidth. The DSSS signal on the right uses the same amount of power, but it spreads that power across a wider band of radio frequencies. Obviously, the 22 MHz DSSS channel is a lot wider than the 1 MHz channels used in FHSS systems.

A DSSS transmitter breaks each bit in the original data stream into a series of redundant bit patterns called *chips*, and it transmits them to a receiver that reassembles the chips back into a data stream that is identical to the original. Because most interference is likely to occupy a narrower bandwidth than a DSSS signal, and because each bit is divided into several chips, the receiver can usually identify noise and reject it before it decodes the signal.

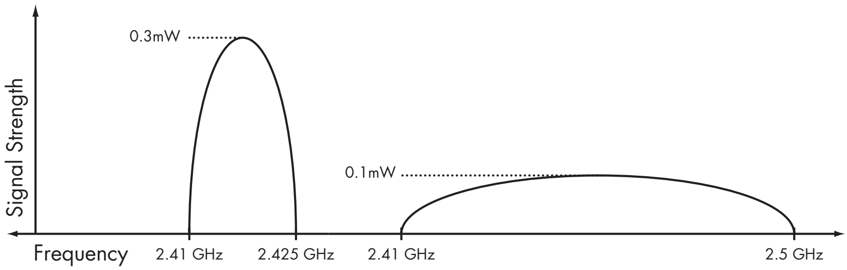

Figure 2-5: A conventional signal (left) uses a narrow radio frequency bandwidth. A DSSS signal (right) uses a wider bandwidth but a less powerful signal.

Like other networking protocols, a DSSS wireless link exchanges handshaking messages within each data packet to confirm that the receiver can understand each packet. For example, the standard data transmission rate in an 802.11b DSSS WI-Fi network is 11Mbps, but when the signal quality won't support that speed, the transmitter and receiver use a process called *dynamic rate shifting* to drop the speed down to 5.5Mbps. The speed might drop because a source of electrical noise near the receiver interferes with the signal or because the transmitter and receiver are too far apart to support full-speed operation. If 5.5Mbps is still too fast for the link to handle, it drops again, down to 2Mbps or even 1Mbps.

Orthogonal Frequency Division Multiplexing

Orthogonal frequency division multiplexing (OFDM) modulation, used in 802.11a Wi-Fi networks, is considerably more complicated than DSSS technology. The physical layer splits the data stream among 52 parallel bit streams that each use a different radio frequency called a *subcarrier*. Four of these subcarriers carry *pilot data* that provides reference information about the remaining 48 subcarriers, in order to reduce signal loss due to radio interference or phase shift. Because the data is divided into 48 separate streams that move through separate subcarriers in parallel, the total transmission speed is much greater than the speed of data through a single channel.

The subcarrier frequencies in an OFDM signal overlap with the peak of each subcarrier's waveform matching the baseline of the overlapping signals as shown in Figure 2-6. This is called *orthogonal frequency division*. The 802.11a standard specifies a total of eight data channels that are 20 MHz wide. Each of these channels is divided into 52 300 kHz subcarriers.

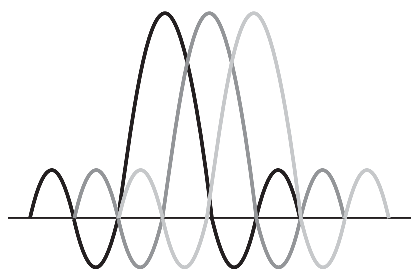

Figure 2-6: In OFDM, the peaks of overlapping frequencies don't interfere with one another.

When a Wi-Fi radio receiver detects an 802.11a signal, it assembles the parallel bit streams back into a single high-speed data stream and uses the pilot data to check its accuracy. Under ideal conditions, an 802.11a network can move data at 54Mbps, but like DSSS modulation, the OFDM transmitter and receiver automatically reduce the data speed when the maximum transmission rate is not possible due to interference, weak signals, or other less-than-perfect atmospheric conditions.

The more recent 802.11g specification was designed to combine the best features of both 802.11b (greater signal range) and 802.11a (higher speed). To accomplish this objective, it uses OFDM modulation on the 2.4 GHz frequency band.

Why This Matters

The great science fiction writer Arthur C. Clarke once observed that "Any sufficiently advanced technology is indistinguishable from magic." For most of us, the technology that controls high-speed spread spectrum radio could just as easily be a form of magic, because we don't need to understand the things that happen inside a transmitter and a receiver; they're just about invisible when we connect a computer to the Internet. As mentioned earlier in this chapter, you don't need to understand these technical details about how a Wi-Fi transmitter splits your data into tiny pieces and reassembles them into data unless you're a radio circuit designer.

But when you know that there's a well-defined set of rules and methods that make the connection work (even if you don't know all the details), you are in control. You know that it's not magic, and if you think about it, you might also know some of the right questions to ask when the system doesn't work correctly. If knowledge is power, then knowledge about the technology you use every day is the power to control that technology rather than just use it.

Benefits of Wireless

Wireless broadband provides Internet access to mobile devices in addition to allowing network operators to extend their networks beyond the range of their wired connections. For our purposes, two-way radio is the most sensible approach to wireless broadband, but other methods (such as infrared light or visible signaling) are also possible. Connecting your computer to the Internet (or a local network) by radio offers several advantages over connecting the same computer through a wired connection. First, wireless provides convenient access for portable computers; it's not necessary to find a cable or network data outlet. And second, it allows a user to make a connection from more than one location and to maintain a connection as the user moves from place to place. For network managers, a wireless connection makes it possible to distribute access to a network without the need to string wires or cut holes through walls.

In practice, access without cables means that the owner of a laptop or other portable computer can walk into a classroom, a coffee shop, or a library and connect to the Internet by simply turning on the computer and running a communication program. Depending on the type of wireless network you're using, you might also be able to maintain the same connection in a moving vehicle.

When you're installing your own network, it's often easier to use Wi-Fi links to extend your network and your Internet connection to other rooms because a wired system requires a physical path for the cables between the network router or switch and each computer. Unless you can route those cables through a false ceiling or some other existing channel, this almost always means that you must cut holes in your walls for data connectors and feed wires inside the walls and under the floors. A radio signal that passes through those same walls is often a lot neater and easier.

Wireless Data Services

Because radio signals move through the air, you can set up a network connection from any place within range of the network base station's transmitter; it's not necessary to use a telephone line, television cable, or some other dedicated wiring to connect your computer to the network. Just turn on the radio connected to the computer and it will find the network signal. Therefore, a radio (or wireless) network connection is often a lot more convenient than a wired one.

This is not to say that wireless is always the best choice. A wired network is usually more secure than a wireless system because it's a lot more difficult for unauthorized eavesdroppers and other snoops to monitor data as it moves through the network, and a wired link doesn't require as many complex negotiations between the sender and receiver on protocols and so forth. In an environment where your computer never moves away from your desk and there are no physical obstacles between the computer and the network access point, it's often easier to install a data cable between the computer and a modem.

So now we have a bunch of radio transmitters and receivers that all operate on the same frequencies and all use the same kind of modulation. (*Modulation* is the method a radio uses to add some kind of content, such as voice or digital data, to a radio wave.) The next step is to send some network data through those radios. Several different wireless data systems and services are available to connect computers and other devices to local networks and to the Internet, including Wi-Fi, WiMAX, and a handful of services based on the latest generations of cellular mobile telephone technology.

Wi-Fi

The IEEE (Institute of Electrical and Electronics Engineers) has produced a set of standards and specifications for wireless networks under the title *IEEE 802.11* that define the formats and structures of the relatively short-range signals that provide Wi-Fi service. The original 802.11 standard (without any letter at the end) was released in 1997. It covers several types of wireless media: two kinds of radio transmissions and networks that use infrared light. The

802.11b standard provides additional specifications for wireless Ethernet networks. A related document, IEEE 802.11a, describes wireless networks that operate at higher speeds on different radio frequencies. Still other 802.11 radio networking standards with other letters are also available or moving toward public release.

The specifications in widest use today are 802.11a, 802.11b, and 802.11g. They're the de facto standards used by just about every wireless Ethernet LAN that you are likely to encounter in offices and public spaces and in most home networks. It's worth the trouble to keep an eye on the progress of those other standards, but for the moment, 802.11a and 802.11g are the ones to use for short-range wireless networks, especially if you're expecting to connect to networks where you don't control all the hardware yourself.

NOTE *Many first-generation 802.11b Wi-Fi network adapters are still compatible with today's networks, but their manufacturers don't offer the device drivers that are necessary to make them work with the latest operating systems (such as Windows XP or Windows Vista).*

The 802.11n standard is the next one in the pipeline, and when it's released, it will replace both 802.11b and 802.11g because it's faster, more secure, and more reliable. The older standards will still work, so new Wi-Fi equipment will support all three (often along with 802.11a, which uses different radio frequencies) and automatically match your network interface to the signals it detects from each base station.

NOTE *Until the new 802.11n standard is formally approved and released, some manufacturers offer "pre-n" network adapters and access points that include many of the features that will be in the final 802.11n standard. These preliminary versions generally work best on networks that are limited to equipment (adapters and access points) made by a single manufacturer, although they all generally work with any existing 802.11b or 802.11g network. Your best bet is to wait until the final standard is released before you upgrade your system, but if you do buy a pre-n device, the manufacturer will probably offer a free firmware upgrade to the final 802.11n specifications.*

There are two more names in the alphabet soup of wireless LAN standards that you ought to know about: WECA and Wi-Fi. *WECA (Wireless Ethernet Compatibility Alliance)* is an industry group that includes all of the major manufacturers of wireless Ethernet equipment. Their twin missions are to test and certify that the wireless network devices from all of their member companies can operate together in the same network, and to promote 802.11 networks as the worldwide standard for wireless LANs. WECA's marketing geniuses have adopted the more friendly name of Wi-Fi (short for *wireless fidelity*) for the 802.11 specifications.

Once or twice per year, the Wi-Fi Alliance conducts an "interoperability bake-off" where engineers from many hardware manufacturers confirm that their hardware will communicate correctly with equipment from other suppliers. Network equipment that carries a Wi-Fi logo has been certified by the Wi-Fi Alliance to meet the relevant standards and to pass interoperability tests. Figure 2-7 shows one version of the Wi-Fi logo.

Wi-Fi was originally intended to be a wireless extension of a wired LAN, so the distances between Wi-Fi base stations and the computers that communicate through them are limited to about 100 feet (35 meters) indoors or up to 300 feet (100 meters) outdoors, assuming there are no obstructions between the access point and the computer. When 802.11n equipment becomes available, it will support connections between computers and base stations at least as far apart as the older Wi-Fi versions. There are ways to extend the range of a Wi-Fi signal, but those techniques require special equipment and careful installation.

Figure 2-7: A Wi-Fi logo

NOTE *See "Extending the Network" on page 167 for more about long-range Wi-Fi operation.*

Because most Wi-Fi signals have such a limited range, you must find a new access point, or *hot spot*, and set up a new connection every time you move your computer to a new location. And because many Wi-Fi access points don't permit strangers to connect through them, you may have to establish a separate account for each location.

The Wi-Fi networks described in this book follow the 802.11a, b, and g standards, but much of the same information will also apply to the new 802.11n networks when they become available.

Metropolitan Wi-Fi Services

In some metropolitan areas, a large number of interconnected Wi-Fi base stations are being installed by either local government agencies or private businesses to provide wireless service throughout an entire region or in selected neighborhoods as an economical alternative to cable and telephone (DSL) services. The base stations for these services are often mounted on utility poles or rooftops.

These same networks might also provide a variety of special data services to the local government and major subscribers. For example, the local natural gas, electric, and water utilities could add small Wi-Fi adapters to their meters and use the system to send readings once a month. And city buses might have transponders that report their locations to a central tracking system, like the one in Seattle at *http://busview.org/busview_launch.jsp*, as shown in Figure 2-8.

It's not yet clear whether these city-wide Wi-Fi services will be able to overcome possible interference problems and competition from other wireless data alternatives, or whether they will attract enough business to remain viable. But if they do, any computer within the coverage area that has a Wi-Fi adapter should detect the signal and have access to a broadband Internet connection.

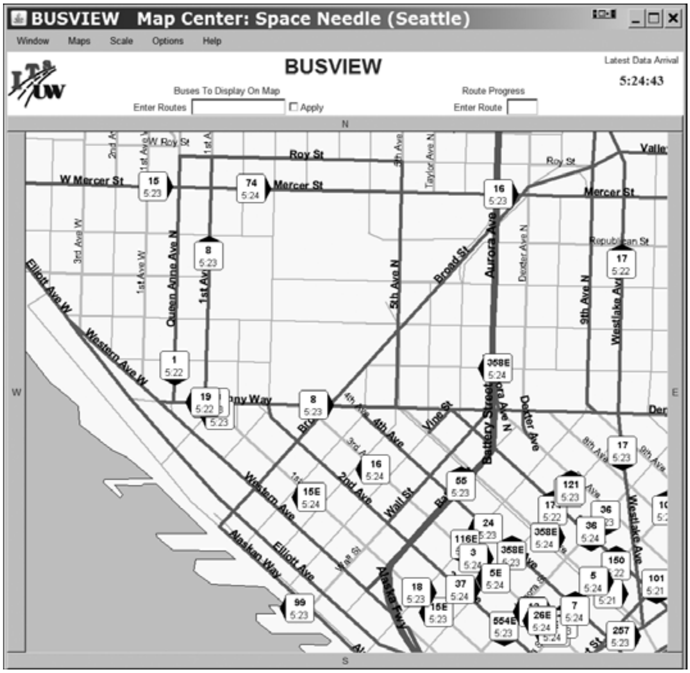

Figure 2-8: Wireless technology tracks city buses in Seattle and reports locations on a website.

Cellular Mobile Wireless Services

Several broadband wireless data services are extensions of cellular mobile telephone technology. You might see them described as 3G services because they're based on the third generation of cellular telephone technology. If you have been using a mobile telephone for more than a year or two, you probably remember that the earliest phones were only good for voice calls, but as each new generation was introduced, your mobile carrier offered more and better features. Table 2-2 describes the various generations.

For people who use their computers away from their home or office, the great advantage of a mobile broadband service is that it covers a much wider territory than any Wi-Fi base station; you can connect your computer to the Internet without the need to search for a new hot spot and use a different access account in each new location, and you can even keep the same connection alive in a moving vehicle. Each of the major wireless broadband services offers coverage in most metropolitan areas and much of the countryside between cities.

Table 2-2: Cellular Mobile Telephone Generations

Name	Features
1G	Analog voice communication only

2G	System can handle more calls
	Digital voice
	  Uses less power
	  Less background noise
	Digital data
	  Simple text messages
	  Email

2.5G	Packet-switched signaling Faster data transfer (up to 144Kbps) Supports relatively slow Internet connections
3G	Even more calls at the same time Much faster data transfer rates (up to 2.4Mbps) Broadband Internet Video and music
4G (not yet available)	Based on Internet technology Packet signaling Very high speed (100Mbps–1Gbps) Will combine telephone, computer, and other technologies

Of course, computer technology has also been improving at the same time, so today's 2.5G and 3G mobile telephones often incorporate enough computing power to allow them to double as pocket-size Internet terminals (as well as cameras and media players). And equally important, from the perspective of this book, broadband data adapters that use 2.5G and 3G technology can attach to a laptop or other portable computer and provide a direct wireless connection to the Internet through the same cellular telephone company that offers mobile telephone service.

Today, most cellular broadband wireless services offer credit card–size adapters that connect to your computer through the PC Card socket on the side of a laptop or into the front or back panel of a desktop computer. In another year or two, many new laptops will come with internal adapters and integrated antennas for both Wi-Fi and 3G wireless or WiMAX that mount directly on the motherboard, just as they contain internal Wi-Fi adapters and dial-up modems today.

NOTE *Some cellular service providers also offer mobile telephones that can connect a computer to the Internet through a USB cable linked to the phone, but separate PC Card adapters are a lot more convenient and easy to use.*

WiMAX

Worldwide Interoperability for Microwave Access (WiMAX) is yet another method for distributing broadband wireless data over wide geographic areas. It's a *metropolitan area network* service that typically uses one or more base stations that can each provide service to users within a 30-mile radius. The IEEE 802.16 specification contains the technical details of WiMAX networks.

In the United States, the earliest WiMAX services were offered by Clearwire as a wireless alternative to DSL and cable broadband Internet access in fixed locations (such as homes and businesses), but mobile WiMAX access is not far behind. By early 2008, Clearwire plans to offer access to their wireless networks through an adapter on a PC Card. When those adapters become available, WiMAX, 3G cellular data services, and metropolitan Wi-Fi networks will compete for the same commercial niche: wireless access to the Internet through a service that covers an entire metropolitan area.

Each WiMAX service provider uses one or more licensed operating frequencies somewhere between 2 GHz and 11 GHz. A WiMAX link can transfer data (including handshaking and other overhead) at up to 70Mbps, but most commercial WiMAX services are significantly slower than that. And as more and more users share a single WiMAX tower and base station, some users report that their signal quality deteriorates.

Unlike the cellular broadband wireless data services that piggyback on existing mobile telephone networks, WiMAX is a separate radio system that is designed to either supplement or replace the existing broadband Internet distribution systems. In practice, WiMAX competes with both 3G wireless services and with Internet service providers that distribute Internet access to fixed locations through telephone lines and cable television utilities. Home and business subscribers to a WiMAX service usually use either a wired LAN or Wi-Fi to distribute the network within their buildings. Figure 2-9 shows a typical WiMAX network.

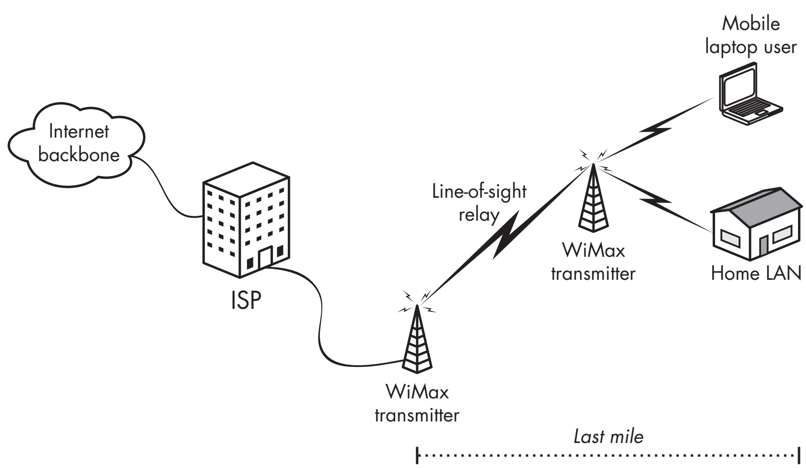

Figure 2-9: WiMAX provides last mile *Internet connections to homes and businesses.*

What About Bluetooth?

Bluetooth is the other type of wireless networking technology that we ought to describe. Bluetooth uses radio signals to replace the wires and cables that connect a computer or a mobile telephone to peripheral devices, such as a keyboard, a mouse, or a set of speakers. You can also use Bluetooth to transfer data between a computer and a mobile telephone, smartphone, BlackBerry, or other PDA (personal digital assistant).

Bluetooth is an FHSS system that splits the radio signal into tiny pieces. It moves among 79 different frequencies 1,600 times per second in the same unlicensed 2.4 GHz range as 802.11b and 802.11g Wi-Fi services.

Bluetooth is not practical for connecting a computer to the Internet because it's slow (the maximum data transfer rate is only about 700Kbps), and it has a very limited signal range (most often about 33 feet, or 10 meters, or less).

In order to prevent interference between Bluetooth and Wi-Fi signals, many computers that use both technologies (including the widely used Intel Centrino chip set) coordinate the two services. When either module is active, it notifies the other, and the active service takes priority. This coordinated operation is slightly slower than either service operating alone, but the difference is insignificant.

Frequency Allocations

Each type of broadband wireless service uses a specific set of radio frequencies. Some of these frequencies are reserved for the exclusive use of a specific licensed service provider while others are free-for-all bands that are open for anybody to use.

Wi-Fi Services

The 802.11b, 802.11g, and 802.11n Wi-Fi services all operate in a frequency range at or slightly above 2.4 GHz. The 802.11a signal uses a band close to 5.3 GHz. The specific center frequencies of each Wi-Fi channel are listed in Table 2-3.

Unless you're a radio engineer, the important things to know about the different Wi-Fi services are the maximum data transmission rate and the signal range. Table 2-3 shows the important characteristics of each Wi-Fi specification.

The differences between the maximum data speeds and the typical speeds are caused by the handshaking and other nondata information that must attach itself to each data packet. Obviously, there's a tremendous amount of overhead involved in moving information through any kind of Wi-Fi network.

Table 2-3: Wi-Fi Characteristics

Type	Radio Frequency	Signal Range	Maximum Data Speed	Typical Speed
802.11b	2.4 GHz	~30 meters (indoor) ~100 meters (outdoor)	11Mbps	4Mbps
802.11a	5 GHz	~35 meters (indoor) ~110 meters (outdoor)	54Mbps	23Mbps
802.11g	2.4 GHz	~35 meters (indoor) ~110 meters (outdoor)	54Mbps	20Mbps
802.11n (proposed)	2.4 GHz	~70 meters (indoor) ~160 meters (outdoor)	300Mbps	120Mbps

Other Broadband Services

National broadband wireless data service providers use a different variation on spread spectrum technology and a different range of radio frequencies. The broadband wireless services provided by Sprint, AT&T, and Verizon all share the frequencies around 800 MHz and 1,900 MHz used by those companies' digital mobile telephone networks. WiMAX services, such as Clearwire, use signals in the 2.3 to 2.5 GHz and 3.5 GHz bands.

Many new radio frequencies may open up for mobile telephone and data services in the United States after February 17, 2009, when all the existing analog television stations move to new digital channels, and the old VHF channels will close down. The newly vacant radio spectrum will become available for new services, including broadband wireless data.

NOTE *Don't panic. All your favorite television stations will still be available after the changeover. You will need either an inexpensive converter box or a new digital television set to receive them, but they'll still be there for you.*

The exact frequencies that the WiMAX and broadband wireless data services use are less important to you as a user than the frequencies of Wi-Fi signals because service providers control the base stations and access points. The network interface device in your computer automatically finds the right signal and sets up the connection without forcing you to choose a specific channel.

Choosing a Service

Each type of wireless access to the Internet offers a different combination of cost, coverage areas, reliability, ease of use, and security. Your choice will depend on your particular needs and the availability of signals in the locations where you need wireless Internet access.

For example, if you use your computer in just a few places and all of those places are within range of Wi-Fi hot spots, the built-in Wi-Fi adapter (or an inexpensive plug-in adapter) is probably your best choice. It's likely that Wi-Fi hot spots already exist at your workplace and in the libraries, coffee shops, schools, and conference centers where you regularly spend time, and it's relatively easy and inexpensive to install one or more access points at home. However, you will probably need a separate account to log in to each Wi-Fi network. Some of these Wi-Fi services are free, but others charge for access by the hour, by the day, or by the month; if you need paid accounts at several locations, the total cost can be more than a single account with a cellular service.

Wi-Fi also allows you to add portable computers to an existing LAN at home or in your school or workplace. And if cost is a primary concern, you will probably choose to use free public Wi-Fi hot spots instead of a cellular or WiMAX service that charges a monthly fee.

On the other hand, if you want constant Internet access wherever you go, the cellular data and WiMAX metropolitan area network services are better choices. Both systems provide coverage throughout large geographic regions, and both allow you to maintain a connection while you're moving from one place to another. You can use the same account and the same login and password every time you set up a connection. However, it's important to make sure that there's a usable cellular or WiMAX signal in all the places where you expect to use them *before* you commit to a long-term contract. Most wireless data service providers offer a free or low cost trial period that you can use to test the system.

As WiMAX and cellular data services become more common, many laptop computers and add-on network adapters will operate with both types of wireless services. When the computer detects a high-speed Wi-Fi signal, it will automatically try to establish a connection to that network. But when there is no local Wi-Fi signal, or if you haven't configured your computer to use any of the local signals, it will automatically shift over to your WiMAX or cellular data account and use that service to connect to the Internet.

All three types of wireless Internet services—Wi-Fi, cellular, and WiMAX—offer fast and reliable connections, but each has a different set of strengths and weaknesses. For short-range coverage and for access to local area networks, Wi-Fi is the obvious choice. If you are outside of the service areas of a DSL or cable Internet service, WiMAX is a huge improvement over a slow dial-up service. But when you carry your computer to many locations, a single account with a cellular or WiMAX service will allow you to connect to the Internet without the need to search for a new hot spot and set up a new account.