chapter 23

Wireless Networking

"The wireless telegraph is not difficult to understand. The ordinary telegraph is like a very long cat. You pull the tail in New York, and it meows in Los Angeles. The wireless is the same, only without the cat."

—Albert Einstein

In this chapter, you will learn how to

- **Discuss wireless networking components**
- **Analyze and explain wireless networking standards**
- **Install and configure wireless networks**
- **Troubleshoot wireless networks**

Wireless networks have been popular for many years now, but unlike wired networks, so much of how wireless works continues to elude people. Part of the problem might be that a simple wireless network is so inexpensive and easy to configure that most users and techs never really get into the *hows* of wireless. The chance to get away from all the cables and mess and just *connect* has a phenomenal appeal. Well, let's change all that and dive deeply into wireless networking.

Historical/Conceptual

The CompTIA A+ exams assume you know the names and connectors (or lack thereof) in wireless networking.

Wireless Networking Components

Instead of a physical set of wires running between network nodes, wireless networks use either radio waves or beams of infrared light to communicate with each other. Various kinds of wireless networking solutions have come and gone in the past. The wireless radio wave networks you'll find yourself supporting these days are based on the **IEEE 802.11** wireless Ethernet standard—marketed as Wi-Fi—and on Bluetooth technology. Wireless networks using infrared light are limited to those that use the Infrared Data Association (IrDA) protocol. Finally, the cell phone companies have gotten into the mix and offer access to the Internet through cellular networks.

Wireless networking capabilities of one form or another are built into many modern computing devices. Infrared *transceiver* ports have been standard issue on portable computers, personal digital assistants (PDAs), and high-end printers for years, although they're absent from most of the latest PCs and portable computers. Figure 23.1 shows the infrared transceiver ports on an older laptop and PDA. Wireless Ethernet and often Bluetooth capabilities are now ubiquitous as integrated components, or you can easily add them by using PCI, PCI Express, or PC Card adapters. Figure 23.2 shows a desktop PCI Wi-Fi adapter. You can also add wireless network capabilities by using external USB wireless network adapters, as shown in Figure 23.3.

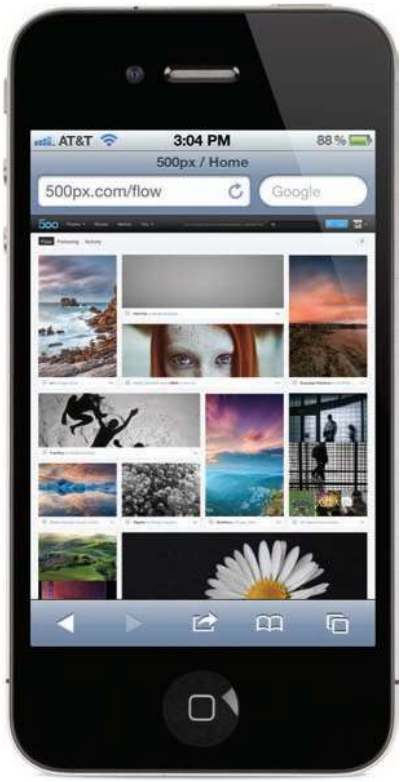
• **Figure 23.1** Infrared transceiver ports on a laptop and PDA

• **Figure 23.2** Wireless PCI add-on card

• **Figure 23.3** External USB wireless NIC

See Chapter 26 for the scoop on mobile devices like smartphones and tablets.

Wireless networking is not limited to PCs. Most smartphones and tablets have wireless capabilities built-in or available as add-on options. Figure 23.4 shows a smartphone accessing the Internet over a Wi-Fi connection.



• **Figure 23.4** Smartphone with wireless capability

801

To extend the capabilities of a wireless Ethernet network, such as connecting to a wired network or sharing a high-speed Internet connection, you need a **wireless access point (WAP)**. A WAP centrally connects wireless network nodes in the same way that a hub connects wired Ethernet PCs. Many WAPs also act as switches and Internet routers, such as the Linksys device shown in Figure 23.5.

Most WAPs draw their power from a wall outlet, like any other electronic device. More advanced WAPs, especially those used in corporate settings, can also use a feature called **Power over Ethernet (PoE)**. Using PoE, you only need to plug a single Ethernet cable into the WAP to provide both power and a network connection.

Wireless communication via Bluetooth comes as a built-in option on newer PCs and peripheral devices, or you can add it to an older PC via an external USB Bluetooth adapter. Figure 23.6 shows a Bluetooth adapter with a Bluetooth-enabled mouse and keyboard.

Wireless Networking Software

Wireless devices use the same networking protocols and client that their wired counterparts use, and they operate by using the **carrier sense multiple access/collision avoidance (CSMA/CA)** networking scheme. The *collision avoidance* aspect differs slightly from the *collision detection* standard used in wired Ethernet. A wireless node listens in on the wireless medium to

PoE is often used with WAPs, but other network devices take advantage of this feature, too.

Wireless access points are commonly known as WAPs, APs, access points, or simply wireless routers.

• **Figure 23.5** Linksys device that acts as wireless access point, switch, and router

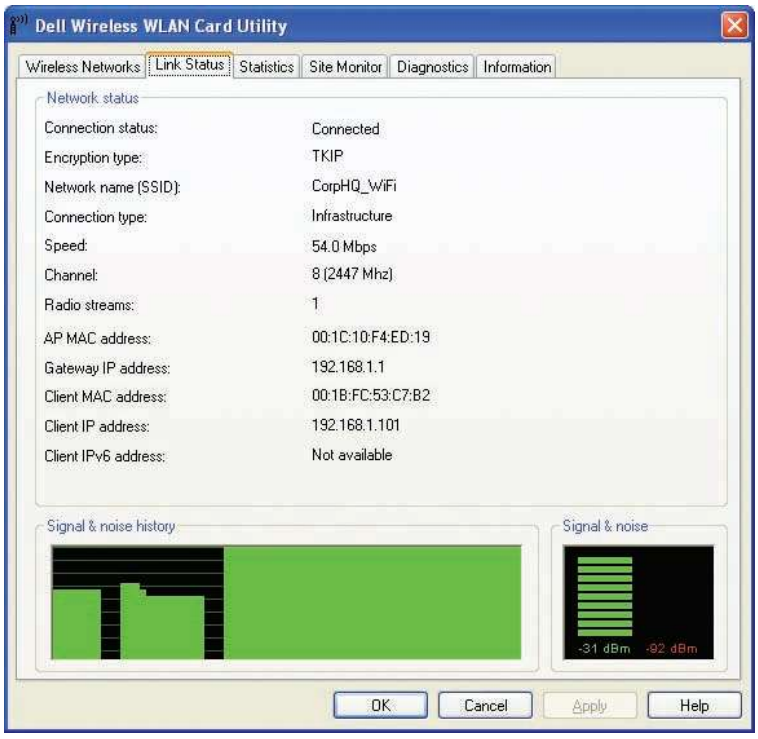
• **Figure 23.6** External USB Bluetooth adapter, keyboard, and mouse

see if another node is currently broadcasting data. If so, it waits a random amount of time before retrying. So far, this method is exactly the same as the method used by wired Ethernet networks. Because wireless nodes have a more difficult time detecting data collisions, however, they offer the option of using the *Request to Send/Clear to Send* (*RTS/CTS*) protocol. When enabled, a transmitting node that determines that the wireless medium is clear to use sends an RTS frame to the receiving node. The receiving node responds with a CTS frame, telling the sending node that it's okay to transmit. Then, once the data is sent, the transmitting node waits for an acknowledgment (ACK) from the receiving node before sending the next data packet. This option is very elegant, but keep in mind that using RTS/CTS introduces significant overhead to the process and can impede performance.

In terms of configuring wireless networking software, you need to do very little. Wireless network adapters are plug and play, so any modern version of Windows immediately recognizes one when it is installed, prompting you to load any needed hardware drivers. You will, however, need a utility to set parameters such as the network name.

Windows XP and later include built-in tools for configuring these settings, but some wireless adapters also come with configuration tools provided by the wireless network adapter vendor (see Figure 23.7). Using this utility, you can determine your link state and signal strength, configure your wireless networking *mode* (discussed next), and set security encryption, power saving options, and so on.

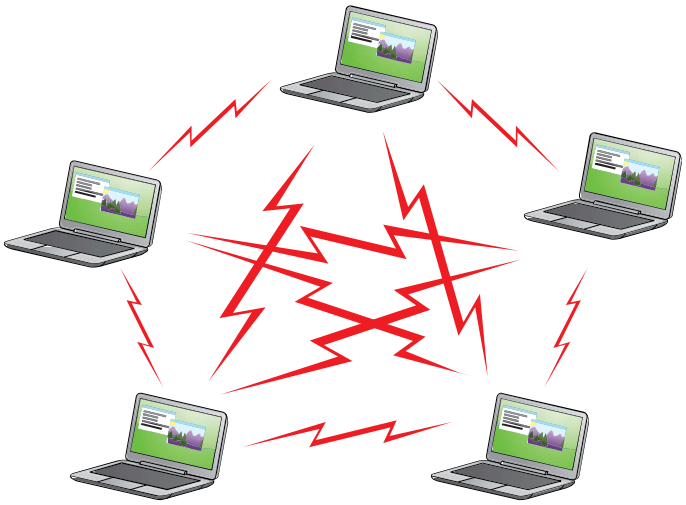
Wireless networks use the carrier sense multiple access/collision avoidance (CSMA/CA) standard, while wired Ethernet networks use carrier sense multiple access/collision detection (CSMA/CD).



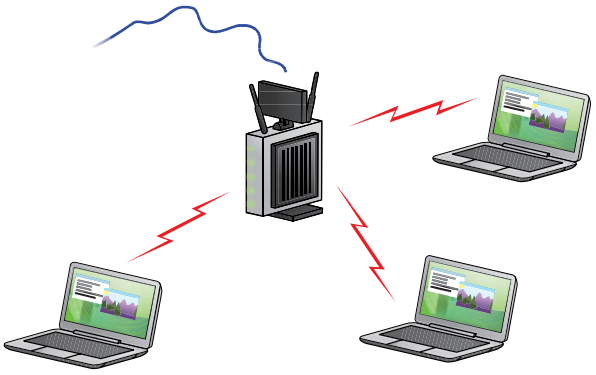
• **Figure 23.7** Wireless configuration utility

Wireless Network Modes

The simplest wireless network consists of two or more PCs communicating directly with each other without cabling or any other intermediary hardware. More complicated wireless networks use a WAP to centralize wireless communication and bridge wireless network segments to wired network segments. These two methods are called ad hoc mode and infrastructure mode.



• **Figure 23.8** Wireless ad hoc mode network



• **Figure 23.9** Wireless infrastructure mode network

Ad hoc Mode

Ad hoc mode is sometimes called *peer-to-peer mode*, with each wireless node in direct contact with every other node in a decentralized free-for-all, as shown in Figure 23.8. Two or more wireless nodes communicating in ad hoc mode form what's called an *Independent Basic Service Set* (*IBSS*). Ad hoc mode networks are suited for small groups of computers (less than a dozen or so) that need to transfer files or share printers. Ad hoc mode networks are also good for temporary networks such as study groups or business meetings.

Infrastructure Mode

Wireless networks running in **infrastructure mode** use one or more WAPs to connect the wireless network nodes to a wired network segment, as shown in Figure 23.9. A single WAP servicing a given area is called a *Basic Service Set* (*BSS*). This service area can be extended by adding more WAPs. This is called, appropriately, an *Extended Basic Service Set* (*EBSS*).

Wireless networks running in infrastructure mode require more planning and are more complicated to configure than ad hoc mode networks, but they also give you finer control over how the network operates. Infrastructure mode is better suited to networks that need to share dedicated resources such as Internet connections and centralized databases.

Wireless Networking Security

One of the major complaints against wireless networking is that it offers weak security. In many cases, all you need to do to access a wireless network is walk into a WAP's coverage area, turn on your wireless device, and connect! Furthermore, data packets are floating through the air instead of safely wrapped up inside network cabling. What's to stop an unscrupulous PC tech with the right equipment from grabbing those packets out of the air and reading that data himself?

Wireless networks use three methods to secure access to the network itself and secure the data that's being transferred. The **service set identifier (SSID)** parameter—also called the *network name*—is used to define the wireless network. This is very handy when you have a number of wireless networks in the same area.

SSID

One of the main security weaknesses with wireless networks is that, out of the box, *no* security is configured at all. Wireless devices *want* to be heard, and WAPs are usually configured to broadcast their presence to their maximum range and welcome all other wireless devices that respond.

Always change the default SSID to something unique, and change the password right away. Configuring a unique SSID name and password is the very least that you should do to secure a wireless network. The default SSID names and passwords are well known and widely available online. This is intended to make setting up a wireless network as easy as possible but can cause problems in places with a lot of overlapping wireless networks. Each wireless network node and access point needs to be configured with the same unique SSID name. This SSID name is then included in the header of every data packet broadcast in the wireless network's coverage area. Data packets that lack the correct SSID name in the header are rejected.

Changing the default SSID for the WAP is the first step in setting up a new wireless network.

Another trick often seen in wireless networks is to tell the wireless device not to broadcast the SSID. People not authorized to access the network will have a harder time knowing it's there.

MAC Address Filtering

Most WAPs also support **MAC address filtering**, a method that enables you to limit access to your wireless network based on the physical, hard-wired address of the units' wireless NIC. MAC address filtering is a handy way of creating a type of "accepted users" list to limit access to your wireless network, but it works best when you have a small number of users. A table stored in the WAP lists the MAC addresses that are permitted to participate in the wireless network. Any data packets that don't contain the MAC address of a node listed in the table are rejected.

Many techs shorten the term "MAC address filtering" to simply "MAC filtering." Either way works.

WEP

Early on, Wi-Fi developers introduced the **Wired Equivalent Privacy (WEP)** protocol to attempt to ensure that data is secured while in transit over the airwaves. WEP encryption uses a standard 40-bit encryption to scramble data packets. Many vendors also support 104-bit encryption. Note that some vendors advertise 128-bit encryption, but they actually use a 104-bit encryption key. Unfortunately, WEP encryption includes a flaw that makes it extremely vulnerable to attack. Although WEP is better than no encryption at all, keep in mind that WEP will not protect you from knowledgeable intruders.

WEP doesn't provide complete end-to-end encryption. WEP provides encryption only between the WAP and the wireless device. Encryption is stripped from the data packet as it travels "up" through the subsequent network layers. For true end-to-end encryption, you need to upgrade to WPA or WPA2.

WPA

The **Wi-Fi Protected Access (WPA)** protocol addresses the weaknesses of WEP and acts as a security protocol upgrade to WEP. WPA uses the **Temporal Key Integrity Protocol (TKIP)**, which provides a new encryption key for every sent packet. This protects WPA from many of the attacks that make

WEP vulnerable, though TKIP has since been deprecated, as it has flaws of its own. WPA also offers security enhancements over WEP such as an encryption key integrity-checking feature and user authentication through the industry-standard **Extensible Authentication Protocol (EAP)**. EAP provides a huge security improvement over WEP encryption. After all, MAC addresses are fairly easy to "sniff" out, because they're transmitted in unencrypted, clear text format. User names and passwords are encrypted and therefore much more secure. Even with these enhancements, WPA was intended only as an interim security solution until the IEEE 802.11i security standard was finalized and implemented.

WPA2

Today, Mac OS X and Windows support the full IEEE 802.11i standard, more commonly known as **Wi-Fi Protected Access 2 (WPA2)**, to lock down wireless networks. WPA2 uses the **Advanced Encryption Standard (AES)**, among other improvements, to provide a secure wireless environment. If you haven't upgraded to WPA2, you should.

WPS

While most techs can configure wireless networks blindfolded, the thought of passwords and encryption might intimidate the average user. If anything, most people plug in their wireless router and go on their merry way. Because everyone should secure their wireless network, the developers of Wi-Fi created **Wi-Fi Protected Setup (WPS)**, a standard included on most WAPs and clients to make secure connections easier to configure.

• **Figure 23.10** WPS button on an e2500 Router

WPS works in one of two ways. Some devices use a push button, such as the one shown in Figure 23.10, and others use a password or code.

Let's say you want to connect a WPS-capable wireless printer to a WPS-capable WAP. First, you would press the button on the printer for a short moment (usually two seconds). You then have a set time (usually two minutes) to press the button on the WAP. This should automatically configure a secure connection.

Some devices enable you to use a code. A WPS-capable WAP will have an eight-digit numeric code printed on the device. To access the WAP, just enter the code in Windows as you would a WPA/WPA2 password. Now you're on the network.

Sadly, WPS has a security flaw. A hacker can use a program to repeatedly guess the eight-digit code. Because of how the code is set up, it's very easy to guess. As long you have WPS enabled on your WAP, you are vulnerable. The only way to stop this hack is to shut down WPS. Check the WAP manufacturer's Web site for instructions on turning off WPS.

Access Point Placement and Radio Power

When setting up your wireless network, keep your space in mind. While encryption can protect your network from intruders, you can also limit your risk by hiding your network from outsiders altogether. When using

an omni-directional antenna, keep it near the center of your home or office. The closer you place it to a wall, the further away someone outside your home or office can be and still detect your wireless network.

Your wireless access point might also enable you to adjust the radio power levels of your antenna. Decrease the radio power until you can get reception at the furthest point *inside* your home or office, but not outside. This will take some trial and error.

Don't forget to physically protect the WAP, too. Most WAPs have physical Ethernet ports in addition to their wireless capabilities. These ports are not password-protected or encrypted. Keep the WAP in a location where unscrupulous folk can't get to it.

Speed and Range Issues

Wireless networking data throughput speeds depend on several factors. Foremost is the standard that the wireless devices use. Depending on the standard used, wireless throughput speeds range from a measly 2 Mbps to a snappy 100+ Mbps. One of the other factors affecting speed is the distance between wireless nodes (or between wireless nodes and centralized access points). Wireless devices dynamically negotiate the top speed at which they can communicate without dropping too many data packets. Speed decreases as distance increases, so the maximum throughput speed is achieved only at extremely close range (less than 25 feet or so). At the outer reaches of a device's effective range, speed may decrease to around 1 Mbps before it drops out altogether.

Speed is also affected by interference from other wireless devices operating in the same frequency range—such as cordless phones or baby monitors—and by solid objects. So-called *dead spots* occur when something capable of blocking the radio signal comes between the wireless network nodes. Large electrical appliances such as refrigerators are *very* effective at blocking a wireless network signal. Other culprits include electrical fuse boxes, metal plumbing, air conditioning units, and similar objects.

Wireless networking range is difficult to define, and you'll see most descriptions listed with qualifiers, such as "*around* 150 feet" and "*about* 300 feet." This is simply because, like throughput speed, range is greatly affected by outside factors. Interference from other wireless devices affects range, as does interference from solid objects. The maximum ranges listed in the next section are those presented by wireless manufacturers as the theoretical maximum ranges. In the real world, you'll experience these ranges only under the most ideal circumstances. True effective range is probably about half what you see listed.

You can increase range in a couple of ways. You can install multiple WAPs to permit "roaming" between one WAP's coverage area and another's—an EBSS, described earlier in this chapter. Or you can install a replacement that increases a single WAP's signal strength, thus increasing its range. If that is still not enough, signal boosters are available that can give you even more power.

Tech Tip

Checking Signal Strength

You can see the speed and signal strength on your wireless network by looking at the wireless NIC's properties. In Windows XP, open the Network Connections applet in Control Panel, right-click your wireless NIC, and select Properties. In Vista/7, open the Network and Sharing Center, select Change Adapter Settings, then right-click your wireless NIC and select Properties.

Look for basic troubleshooting questions on the CompTIA A+ certification exams dealing with factors that affect wireless connectivity, range, and speed.

Wireless Networking Standards

Today's wireless world is dominated by *radio frequency* (*RF*) technologies, in particular the 802.11 (Wi-Fi) standards. Other standards, such as infrared, Bluetooth, and cellular, have a place in today's market. To help you gain

a better understanding of wireless network technologies, this section provides a brief look at the standards they use.

IEEE 802.11-Based Wireless Networking

In the early days of wireless networking, many techs and marketing people assumed Wi-Fi stood for *Wireless Fidelity*, a sort of play on the common sound signal of high fidelity. It might have at one time, but the Wi-Fi Alliance, the governing standards body for 802.11-based networking, just uses the term Wi-Fi today.

Wi-Fi is by far the most widely adopted wireless networking type today. Not only do millions of private businesses and homes have wireless networks, but many public places such as coffee shops and libraries also offer Internet access through wireless networks.

Devices that use the original 802.11 (with no letter) standard are obsolete these days. You're likeliest to find them in service on some brave early wireless adopter's network—or in a museum. The original 802.11 standard was hampered by both slow speeds (2 Mbps maximum) and limited range (about 150 feet). The 802.11 standard employed some of the same features that are in use in the current wireless standards; 802.11 uses the 2.4-GHz broadcast range.

The IEEE 802.11 wireless Ethernet standard, more commonly known as **Wi-Fi**, defines methods by which devices may communicate by using *spread-spectrum* radio waves. Spread-spectrum broadcasts data in small, discrete chunks over the frequencies available within a certain frequency range.

The 802.11-based wireless technologies broadcast and receive on one of two license-free industrial, scientific, and medical (ISM) radio bands: 2.4 GHz and 5.8 GHz. Even though the ISM band is 5.8 GHz, we just say "5 GHz" for reasons I can't answer. Over the years, the original 802.11 standard has been extended to 802.11*a*, 802.11*b*, 802.11*g*, and 802.11*n* variations used in Wi-Fi wireless networks. Each of these versions of 802.11 uses one of the two ISM bands, with the exception of 802.11n, which uses one but may use both. Don't worry; I'll break this down for you in a moment.

Newer wireless devices can communicate with older wireless devices, so if you are using an 802.11n WAP, all of your 802.11g devices can use it. The exception to this is 802.11a, which requires that all of the equipment directly support it. The following paragraphs describe the important specifications of each of the popular 802.11-based wireless networking standards.

802.11a Despite the "a" designation for this extension to the 802.11 standard, **802.11a** was actually on the market *after* 802.11b. The 802.11a standard differs from the other 802.11-based standards in significant ways. Foremost is that it operates in the 5-GHz frequency range. This means that devices that use this standard are less prone to interference from other devices that use the same frequency range. 802.11a also offers considerably greater throughput than 802.11 and 802.11b at speeds up to 54 Mbps, though its actual throughput is no more than 25 Mbps in normal traffic conditions. Although its theoretical range tops out at about 150 feet, its maximum range will be lower in a typical office environment. Despite the superior speed of 802.11a, it isn't as widely adopted in the PC world as some of the following 802.11 versions.

802.11b **802.11b** was the first standard to take off and become ubiquitous in wireless networking. The 802.11b standard supports data throughput of up to 11 Mbps (with actual throughput averaging 4 to 6 Mbps)—on par with older wired 10BaseT networks—and a maximum range of 300 feet under ideal conditions. In a typical office environment, its maximum range is lower. The main downside to using 802.11b is, in fact, that it uses a very popular frequency. The 2.4-GHz ISM band is already crowded with baby monitors, garage door openers, microwaves, and wireless phones, so you're likely to run into interference from other wireless devices.

802.11g **802.11g** came out in 2003, taking the best of 802.11a and b and rolling them into a single standard. 802.11g offers data transfer speeds equivalent to 802.11a, up to 54 Mbps, with the wider 300-foot range of 802.11b. More important, 802.11g runs in the 2.4-GHz ISM band, so it is backward compatible with 802.11b, meaning that the same 802.11g WAP can service

both 802.11b and 802.11g wireless nodes. 802.11g was incredibly popular but has pretty much lost out to the newest version of 802.11, 802.11n.

802.11n The **802.11n** standard brings several improvements to Wi-Fi networking, including faster speeds and new antenna technology implementations.

The 802.11n specification requires all but hand-held devices to use multiple antennas to implement a feature called **multiple in/multiple out (MIMO)**, which enables the devices to make multiple simultaneous connections. With up to four antennas, 802.11n devices can achieve amazing speeds. (The official standard supports throughput of up to 600 Mbps, although practical implementation drops that down substantially.)

Many 802.11n WAPs employ *transmit beamforming*, a multiple-antenna technology that helps get rid of dead spots—or at least make them not so bad. The antennas adjust the signal once the WAP discovers a client to optimize the radio signal.

Like 802.11g, 802.11n WAPs can run in the 2.4-GHz ISM band, supporting earlier, slower 802.11b/g devices. However, 802.11n also has a more powerful, so-called *dual-band*. To use dual-band 802.11n, you need a more advanced (and more expensive) WAP that runs at both 5 GHz and 2.4 GHz simultaneously; some support 802.11a devices as well as 802.11b/g devices. Nice!

Table 23.1 compares the important differences among the versions of 802.11.

Know the differences among 802.11a, 802.11b, 802.11g, and 802.11n.

Table 23.1 Comparison of 802.11 Standards

Standard	802.11a	802.11b	802.11g	802.11n
Max. throughput	54 Mbps	11 Mbps	54 Mbps	100+ Mbps
Max. range	150 feet	300 feet	300 feet	300+ feet
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4 and 5 GHz
Security	SSID, MAC filtering, industry-standard WEP, WPA	SSID, MAC filtering, industry-standard WEP, WPA	SSID, MAC filtering, industry-standard WEP, WPA	SSID, MAC filtering, industry-standard WEP, WPA
Compatibility	802.11a	802.11b	802.11b, 802.11g	802.11b, 802.11g, 802.11n (802.11a in some cases)
Communication mode	Ad hoc or infrastructure	Ad hoc or infrastructure	Ad hoc or infrastructure	Ad hoc or infrastructure
Description	Eight available channels. Less prone to interference than 802.11b and 802.11g.	Fourteen channels available in the 2.4-GHz band (only eleven of which can be used in the U.S. due to FCC regulations). Three non-overlapping channels.	Improved security enhancements. Fourteen channels available in the 2.4-GHz band (only eleven of which can be used in the U.S. due to FCC regulations). Three non-overlapping channels.	Same as 802.11g but adds the 5-GHz band that 802.11a uses. 802.11n can also make use of multiple antennas (MIMO) to increase its range and speed.

Try This!

What's Available Now?

802.11n was the hot Wi-Fi standard when this book went to print, but other technologies were on the horizon. Take a trip to your local computer store and see what's available "now." Is there anything on the market that can run faster than 100 Mbps? Are 2.4 and 5.0 GHz still the only two standards?

Other Wireless Standards

While Wi-Fi dominates the wireless networking market, it isn't the only standard. A lot of smaller networks (we're talking two computers small) use infrared or Bluetooth to connect devices. Mobile devices, such as smartphones and some tablets, connect wirelessly via cellular networks.

Infrared Wireless Networking

Wireless networking using infrared technology is largely overlooked these days, probably because of the explosion of interest for newer and faster wireless standards. But it is still a viable method to transfer files on some older devices.

Apple computers also support IrDA, as do Linux PCs.

Communication through infrared devices is enabled via the **Infrared Data Association (IrDA)** protocol. The IrDA protocol stack is a widely supported industry standard and has been included in all versions of Windows since Windows 95.

In speed and range, infrared isn't very impressive. Infrared devices are capable of transferring data up to 4 Mbps—not too shabby, but hardly stellar. The maximum distance between infrared devices is 1 meter. Infrared links are direct line-of-sight and are susceptible to interference. Anything that breaks the beam of light can disrupt an infrared link: a badly placed can of Mountain Dew, a coworker passing between desks, or even bright sunlight hitting the infrared transceiver can cause interference.

Many modern laptops still come with a little infrared window, but don't let that fool you into thinking the laptop has IrDA networking. These IR receivers are for use with remotes so you can use the laptop just like a TV or DVD player.

Infrared is designed to make a point-to-point connection between two devices only in ad hoc mode. No infrastructure mode is available. You can, however, use an infrared access point device to enable Ethernet network communication using IrDA. Infrared devices operate at half-duplex, meaning that while one is talking, the other is listening—they can't talk and listen at the same time. IrDA has a mode that emulates full-duplex communication, but it's really half-duplex. The IrDA protocol offers exactly nothing in the way of encryption or authentication. Infrared's main security feature is the fact that you have to be literally within arm's reach to establish a link. Clearly, infrared is not the best solution for a dedicated network connection, but for a quick file transfer or print job without getting your hands dirty, it'll do in a pinch.

Table 23.2 lists infrared's important specifications.

Table 23.2 Infrared Specs

Standard	Infrared (IrDA)
Max. throughput	Up to 4 Mbps
Max. range	1 meter (39 inches)
Security	None
Compatibility	IrDA
Communication mode	Point-to-point ad hoc

Bluetooth

Bluetooth wireless technology (named for ninth-century Danish king Harald Bluetooth) is designed to create small wireless networks preconfigured to do very specific jobs. Some great examples are audio devices such as headsets that connect to your smartphones, **personal area networks (PANs)** that link two PCs for a quick-and-dirty wireless network, and input devices such as keyboards and mice. Bluetooth is *not* designed to be a full-function networking solution, nor is it meant to compete with Wi-Fi. If anything, Bluetooth has replaced infrared as a means to connect PCs to peripherals.

Bluetooth, like any technology, has been upgraded over the years to make it faster and more secure. Two major versions of Bluetooth are widespread today. The first generation (versions 1.1 and 1.2) supports speeds around 1 Mbps. The second generation (2.0 and 2.1) is backward compatible with its first-generation cousins and adds support for more speed by introducing Enhanced Data Rate (EDR), which pushes top speeds to around 3 Mbps.

The Bluetooth 3.0 and 4.0 standards were released several years ago, though neither has seen the same level of adoption as earlier standards.

The IEEE organization has made first-generation Bluetooth the basis for its 802.15 standard for wireless PANs. Bluetooth uses a broadcasting method that switches among any of the 79 frequencies available in the 2.45-GHz range. Bluetooth hops frequencies some 1600 times per second, making it highly resistant to interference.

Generally, the faster and further a device sends data, the more power it needs to do so, and the Bluetooth designers understood a long time ago that some devices (such as a Bluetooth headset) could save power by not sending data as quickly or as far as other Bluetooth devices may need. To address this, all Bluetooth devices are configured for one of three classes that define maximum power usage in milliwatts (mW) and maximum distance:

Class 1	100 mW	100 meters
Class 2	2.5 mW	10 meters
Class 3	1 mW	1 meter

Bluetooth is made to replace the snake's nest of cables that currently connects most PCs to their various peripheral devices—keyboard, mouse, printer, speakers, scanner, and the like—but you won't be swapping out your 802.11-based networking devices with Bluetooth-based replacements anytime soon.

Having said that, Bluetooth-enabled wireless networking is comparable to other wireless technologies in a few ways:

- Like infrared, Bluetooth is acceptable for quick file transfers where a wired connection (or a faster wireless connection) is unavailable.
- Almost all wireless headsets are now Bluetooth.
- Bluetooth's speed and range make it a good match for wireless print server solutions.

Bluetooth hardware comes either integrated into many newer portable electronic gadgets such as smartphones or as an adapter added to an internal or external expansion bus. Bluetooth networking is enabled through ad hoc–styled device-to-device connections, or in an infrastructure-like mode through Bluetooth access points. Bluetooth access points are very similar to 802.11-based access points, bridging wireless Bluetooth PAN segments to wired LAN segments.

Cellular

A **cellular wireless network** enables you to connect to the Internet through a network-aware smartphone, tablet, or other mobile device. To learn more about cellular data networks, check out Chapter 24.

802

Installing and Configuring Wireless Networking

The mechanics of setting up a wireless network don't differ much from a wired network. Physically installing a wireless network adapter is the same as installing a wired NIC, whether it's an internal PCI card, a PC Card, or an external USB device. Simply install the device and let plug and play handle the rest. Install the device's supplied driver when prompted, and you're practically finished.

As mentioned earlier, wireless devices want to talk to each other, so communicating with an available wireless network is usually a no-brainer. The trick is in configuring the wireless network so that only specific wireless nodes are able to use it and securing the data that's being sent through the air.

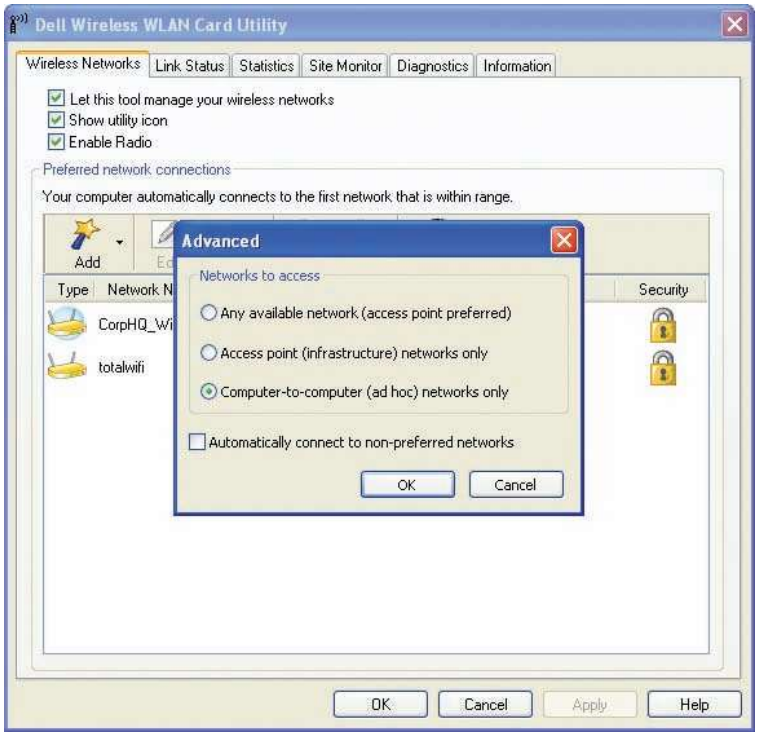
Wi-Fi Configuration

Wi-Fi networks support ad hoc and infrastructure operation modes. Which mode you choose depends on the number of wireless nodes you need to support, the type of data sharing they'll perform, and your management requirements.

Ad hoc Mode

Ad hoc mode wireless networks don't need a WAP. The only requirements in an ad hoc mode wireless network are that each wireless node be configured with the same network name (SSID) and that no two nodes use the same IP address. Figure 23.11 shows a wireless network configuration utility with ad hoc mode selected.

The only other configuration steps to take are to make sure that no two nodes are using the same IP address (this step is usually unnecessary if all PCs are using DHCP) and ensuring that the File and Printer Sharing service is running on all nodes.



• **Figure 23.11** Selecting ad hoc mode in a wireless configuration utility

Infrastructure Mode

Typically, infrastructure mode wireless networks employ one or more WAPs connected to a wired network segment, a corporate intranet or the Internet, or both. As with ad hoc mode wireless networks, infrastructure mode networks require that the same SSID be configured on all nodes and WAPs. Figure 23.12 shows a NETGEAR Wi-Fi configuration screen set to infrastructure mode and using WPA security.

WAPs have an integrated Web server and are configured through a browser-based setup utility. Typically, you fire up your Web browser on one of your network client workstations and enter the WAP's default IP address, such as 192.168.1.1, to bring up the configuration page. You will need to supply an administrative password, included with your WAP's

• **Figure 23.12** Selecting infrastructure mode in a wireless configuration utility

• **Figure 23.13** Security login for Linksys WAP

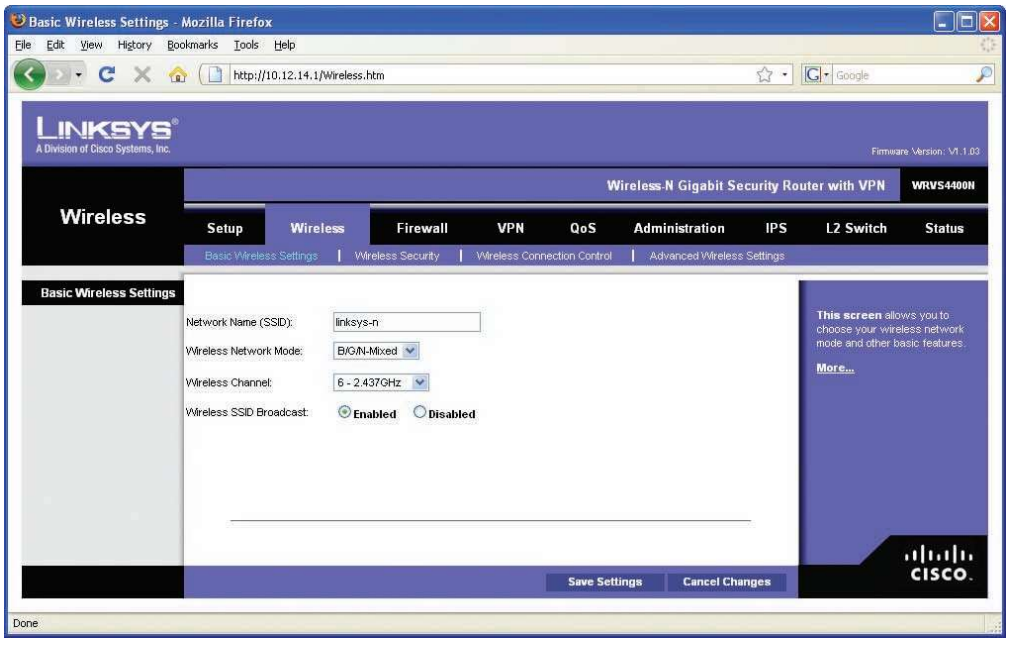
documentation, to log in (see Figure 23.13). Setup screens vary from vendor to vendor and from model to model. Figure 23.14 shows the initial setup screen for a popular Linksys WAP/router.

Configure the SSID option where indicated. Channel selection is usually automatic, but you can reconfigure this option if you have particular needs in your organization (for example, if you have multiple wireless networks operating in the same area). Remember that it's always more secure to configure a unique SSID than it is to accept the well-known default one. You should also make sure that the option to allow broadcasting of the SSID is disabled. This ensures that only wireless nodes specifically configured with the correct SSID can join the wireless network.

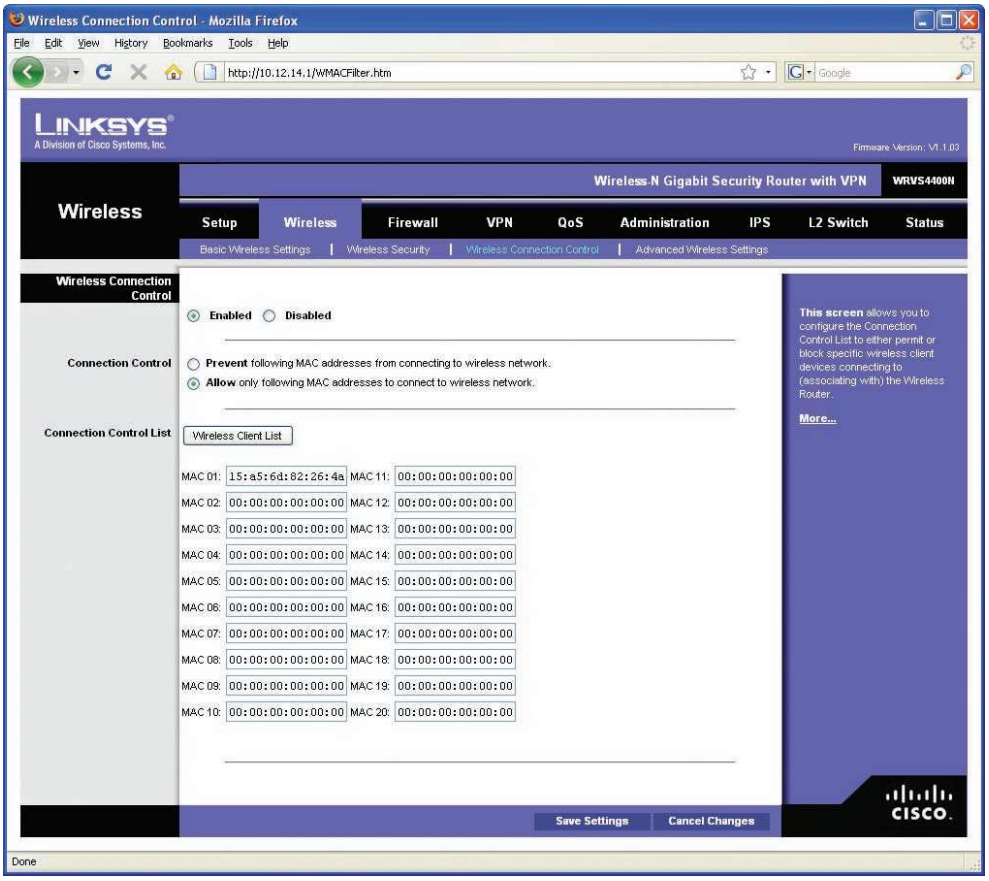
As noted earlier in the chapter, the WEP protocol provides security, but it's easily cracked. Use WPA2 or, if you have older equipment, settle for WPA until you can upgrade.

To increase security even more, use MAC filtering. Figure 23.15 shows the MAC filtering configuration screen for a Linksys WAP. Simply enter the MAC address of a wireless node that you wish to allow (or deny) access to your wireless network. Set up encryption by turning encryption on at the WAP and then generating a unique security key. Then configure all connected wireless nodes on the network with the same key information. Figure 23.16 shows the WEP key configuration screen for a Linksys WAP.

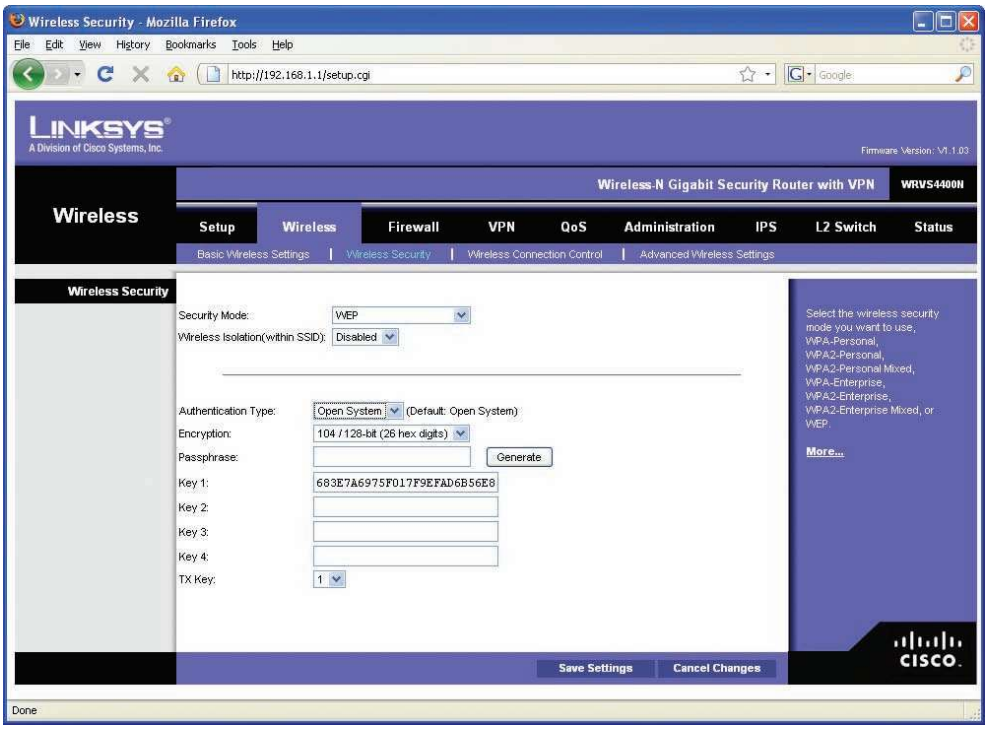
When setting up WEP, you have the option of automatically generating a set of encryption keys or doing it manually; save yourself a headache and use the automatic method. Select an encryption level—the usual choices are either 64-bit or 128-bit—and then enter a unique passphrase and click the Generate button (or whatever the equivalent button is called on your WAP). Then select a default key and save the settings. The encryption level,



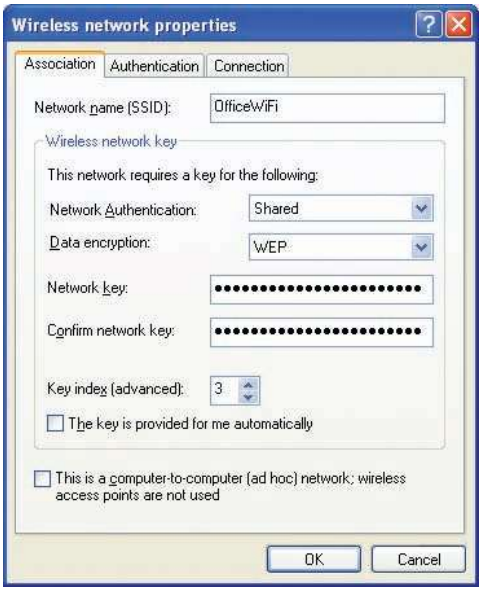
• **Figure 23.14** Linksys WAP setup screen



• **Figure 23.15** MAC filtering configuration screen for a Linksys WAP



• **Figure 23.16** WEP encryption key configuration screen for a Linksys WAP



• **Figure 23.17** WEP encryption screen on client wireless network adapter configuration utility

key, and passphrase must match on the wireless client node or communication will fail. Many WAPs have the capability to export the WEP encryption key data onto a media storage device for easy importing onto a client workstation, or you can manually configure encryption by using the vendor-supplied configuration utility, as shown in Figure 23.17.

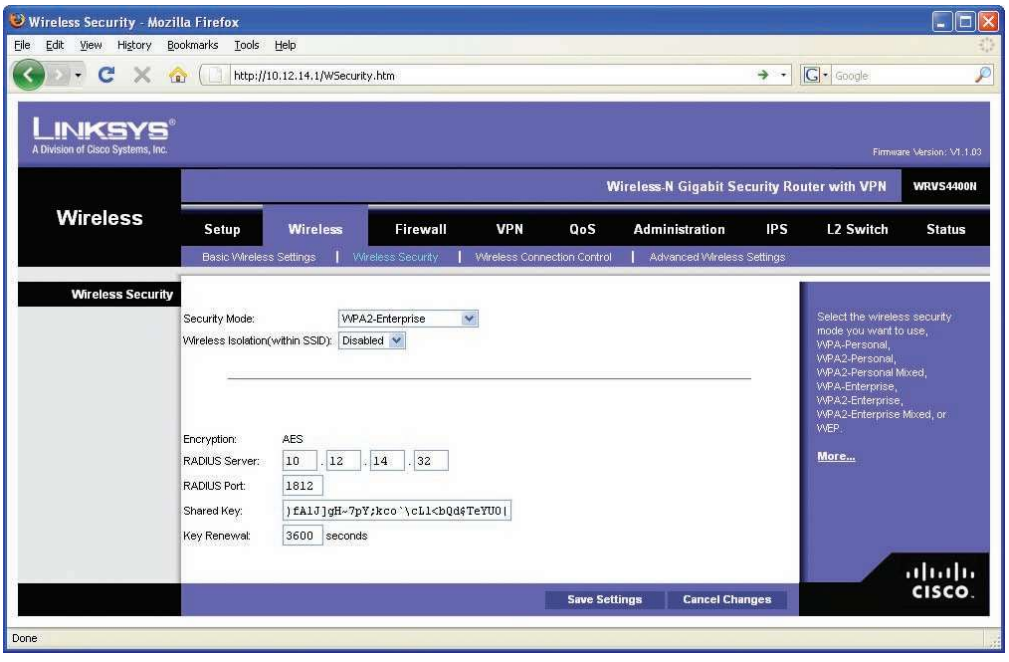
WPA and WPA2 encryption is configured in much the same way as WEP. There are two ways to set up WPA/WPA2: Pre-shared Key (PSK) or Enterprise. WPA/WPA2-PSK is the most common for small and home networks. Enterprise is much more complex, requires extra equipment (a RADIUS server), and is only used in the most serious and secure wireless networks.

If you have the option, choose WPA2 encryption for the WAP as well as the NICs in your network. You configure WPA2 the same way you would WPA. Note that the settings such as WPA2 for the Enterprise assume you'll enable authentication by using a device called a RADIUS server (see Figure 23.18). This way, businesses can allow only people with the proper credentials to connect to their Wi-Fi networks. For home use, select the PSK version of WPA/WPA2. Use the best encryption you can. If you have WPA2, use it. If not, use WPA. WEP is always a last choice.

Always try WPA2-PSK first. If you then have wireless computers that can't connect to your WAP, fall back to WPA-PSK.

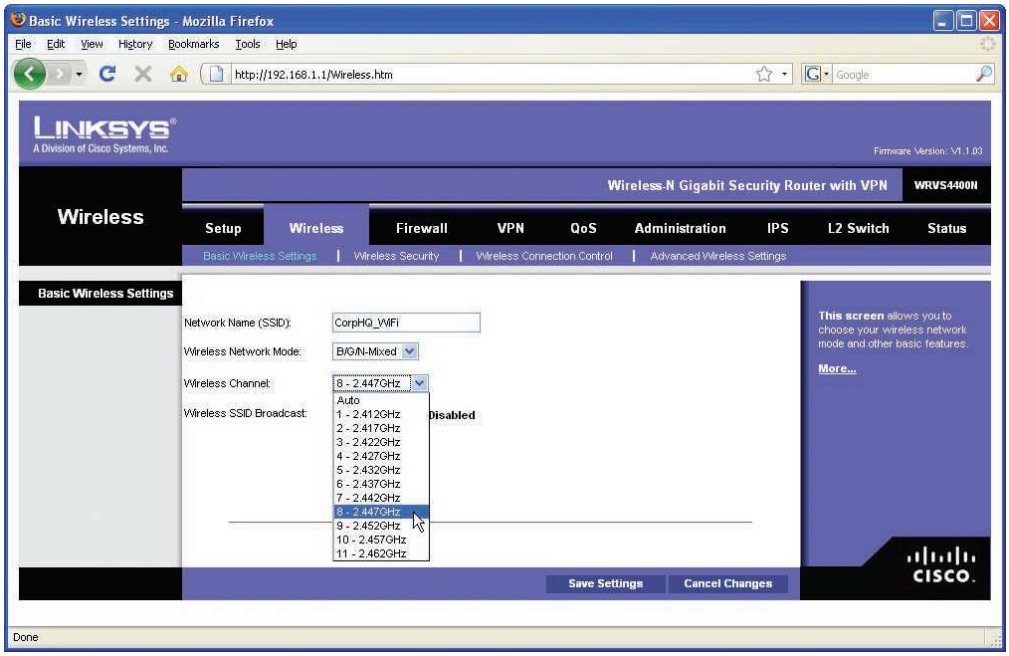
With most home networks, you can simply leave the channel and frequency of the WAP at the factory defaults, but in an environment with overlapping Wi-Fi signals, you'll want to adjust one or both features. To adjust the channel, find the option in the WAP configuration screens and simply change it. Figure 23.19 shows the channel option in a Linksys WAP.

With dual-band 802.11n WAPs, you can choose which band to put 802.11n traffic on, either 2.4 GHz or 5 GHz. In an area with overlapping signals,

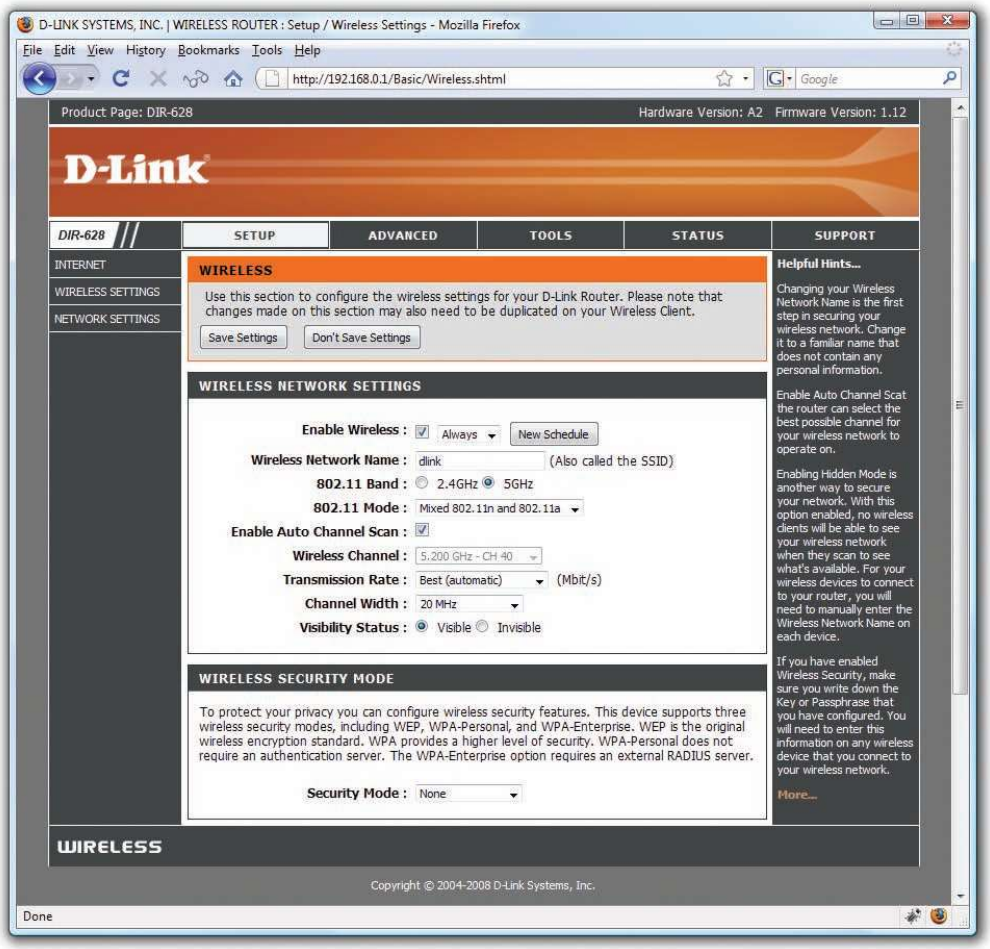


• **Figure 23.18** Encryption screen with RADIUS option

most of the traffic will be on the 2.4-GHz frequency, because most devices are either 802.11b or 802.11g. In addition to other wireless devices (such as cordless phones), microwaves also use the 2.4-GHz frequency and can cause a great deal of interference. You can avoid any kind of conflict with your 802.11n devices by using the 5-GHz frequency instead. Figure 23.20 shows the configuration screen for a dual-band 802.11n WAP.



• **Figure 23.19** Changing the channel



• **Figure 23.20** Selecting frequency

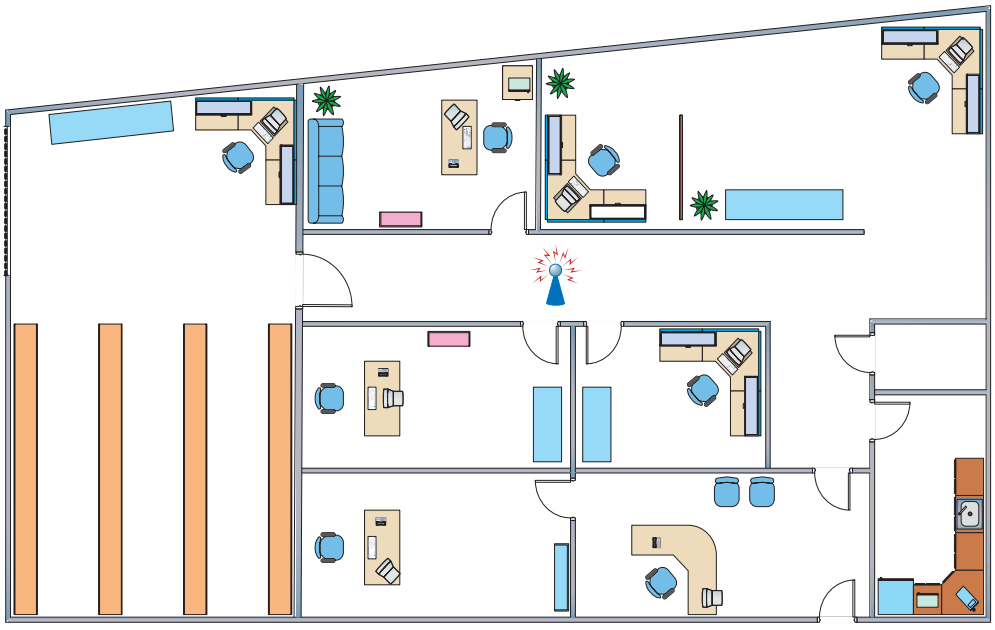
Placing the Access Point(s)

The optimal location for an access point depends on the area you want to cover, whether you care if the signal bleeds out beyond the borders, and what interference exists from other wireless sources. You start by doing a site survey. A site survey can be as trivial as firing up a wireless-capable laptop and looking for existing SSIDs. Or it can be a complex job where you hire people with specialized equipment to come in and make lots of careful plans, defining the best place to put WAPs and which wireless channels to use. To make sure the wireless signal goes where you want it to go and not where you don't, you need to use the right antenna. Let's see what types of antennas are available.

Omni-directional and Centered For a typical network, you want blanket coverage and would place a WAP with an omni-directional antenna in the center of the area (see Figure 23.21). With an omni-directional antenna, the radio wave flows outward from the WAP. This has the advantage of ease of use—anything within the signal radius can potentially access the network. Most wireless networks use this combination, especially in the consumer space. The standard straight-wire antennas that provide most omni-directional function are called **dipole antennas**.

If you want to know whether your local café, bookstore, airport, or other public place has a Wi-Fi access point (otherwise known as a *hotspot*), you can use a *Wi-Fi* or *wireless locator*. The locator is usually the size of your car remote and lights up or otherwise signals you whenever you are in range of a Wi-Fi access point.

Gaining Gain An antenna strengthens and focuses the radio frequency (RF) output from a WAP. The ratio of increase—what's called **gain**—is measured in decibels (dB). The gain from a typical WAP is 2 dB, enough to cover a reasonable area but not a very large room. To increase that signal requires a bigger antenna. Many WAPs have removable antennas that you can replace. To increase the signal in an omni-directional and centered setup, simply replace the factory antennas with one or more bigger antennas (see Figure 23.22). Get a big enough antenna and you can crank it all the way up to 11 dB!



• Figure 23.21 Room layout with WAP in the center

• Figure 23.22 Replacement antenna on WAP

Bluetooth Configuration

As with other wireless networking solutions, Bluetooth devices are completely plug and play. Just connect the adapter and follow the prompts to install the appropriate drivers and configuration utilities (these are supplied by your hardware vendor). Once they're installed, you have little to do: Bluetooth devices seek each other out and establish the master/slave relationship without any intervention on your part.

Connecting to a Bluetooth PAN is handled by specialized utility software provided by your portable device or Bluetooth device vendor. Figure 23.23 shows a screen of an older PDA running the Bluetooth Manager software to connect to a Bluetooth access point. Like their Wi-Fi counterparts, Bluetooth access points use a browser-based configuration utility. Figure 23.24 shows the main setup screen for a Belkin Bluetooth access point. Use this setup screen to check on the status of connected Bluetooth devices; configure encryption, MAC filtering, and other security settings; and use other utilities provided by the access point's vendor.

Cellular Configuration

There is no single standard for configuring a cellular network card because the cards and software change based on your service provider. Fortunately, those same cell phone companies have made the process of installing their cards very simple. All that is required in most cases is to plug in the card and install the software.

Bluetooth network access points are a rare sight out in the real world. Today small portables, PDAs, and smartphones almost certainly connect by using a Wi-Fi or cellular network.

• Figure 23.23 iPAQ Bluetooth Manager software connected to Bluetooth access point

• **Figure 23.24** Belkin Bluetooth access point

With most cellular cards, you simply plug the card into your computer, usually via USB, and the setup program automatically launches. These cards almost always have all the required software and drivers built into the cards themselves, so there are no optical discs to worry about. Once you've installed the necessary software, launch the connection application. Follow the instructions that came with the software; in Figure 23.25, for example, double-click on the VZAccess network listed in the window. This initiates the connection to Verizon's network. You can also go to the Options menu and select Statistics to see the specifics of your connection, as shown in Figure 23.26.

The key thing to remember about cellular Internet access is that it is almost completely configured and controlled by the provider. A tech has very little to do except to make sure the cellular card is plugged in, recognized by the computer, and properly installed.

• **Figure 23.25** VZAccess Manager

Troubleshooting Wi-Fi

Wireless networks are a real boon when they work right, but they can also be one of the most vexing things to troubleshoot when they don't. Let's turn to some practical advice on how to detect and correct wireless hardware, software, and configuration problems.

As with any troubleshooting scenario, your first step in troubleshooting a wireless network is to break down your tasks into logical steps. Your first step should be to figure out the scope of your wireless networking problem. Ask yourself *who*, *what*, and *when*:

- Who is affected by the problem?
- What is the nature of their network problem?
- When did the problem start?

The answers to these questions dictate at least the initial direction of your troubleshooting.

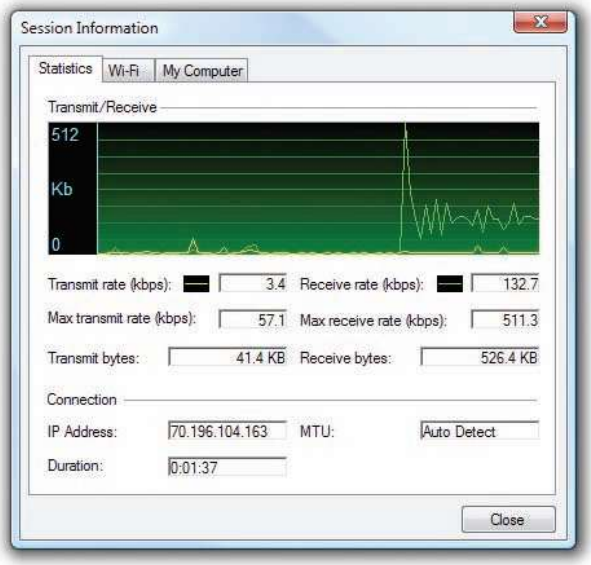


Figure 23.26 Session statistics for VZAccess Manager

So, who's affected? If all machines on your network—wired and wireless—have lost connectivity, you have bigger problems than that the wireless machines cannot access the network. Troubleshoot this situation the way you'd troubleshoot any network failure. Once you determine which wireless nodes are affected, it's easier to pinpoint whether the problem lies in one or more wireless clients or in one or more access points.

After you narrow down the number of affected machines, your next task is to figure out specifically what type of error the users are experiencing. If they can access some, but not all, network services, it's unlikely that the problem is limited to their wireless equipment. For example, if they can browse the Internet but can't access any shared resources on a server, they're probably experiencing a permissions-related issue rather than a wireless one.

Finally, determine when the problem started. What has changed that might explain your loss of connectivity? Did you or somebody else change the wireless network configuration? For example, if the network worked fine two minutes ago, and then you changed the WEP key on the access point, and now nobody can see the network, you have your solution—or at least your culprit! Did your office experience a power outage, power sag, or power surge? Any of these might cause a WAP to fail.

Once you figure out the who, what, and when, you can start troubleshooting in earnest. Typically, your problem is going to center on your hardware, software, connectivity, or configuration.

Hardware Troubleshooting

Wireless networking hardware components are subject to the same kind of abuse and faulty installation as any other hardware component. Troubleshooting a suspected hardware problem should bring out the technician in you.

As with all things computing, don't forget to do the standard PC troubleshooting thing and reboot the computer before you do any configuration or hardware changes!

Open Windows Device Manager and look for an error or conflict with the wireless adapter. If you see a big exclamation point or a red *X* next to the device, you have a driver error. Reinstall the device driver as needed.

If you don't see the device listed at all, perhaps it is not seated properly in its expansion slot or not plugged all the way into its PC Card or USB slot. These problems are easy to fix. Just remove them and reinstall the device.

Software Troubleshooting

Because you've already checked to confirm that your hardware is using the correct drivers, what kind of software-related problems are left to check? Two things come immediately to mind: the wireless adapter configuration utility and the WAP's firmware version.

As I mentioned earlier, some wireless devices won't work correctly unless you install the vendor-provided drivers and configuration utility before plugging in the device. This is particularly true of wireless USB devices. If you didn't do this, go into Device Manager and uninstall the device; then start again from scratch.

Some WAP manufacturers (I won't name names here, but they're popular) are notorious for shipping devices without the latest firmware installed. This problem often manifests as a device that enables clients to connect, but only at such slow speeds that the devices experience frequent timeout errors. The fix for this is to update the access point's firmware. Go to the manufacturer's Web site and follow the support links until you find the latest version. You'll need your device's exact model and serial number—this is important, because installing the wrong firmware version on your device is a guaranteed way of rendering it unusable!

Again, follow the manufacturer's instructions for updating the firmware to the letter. Typically, you need to download a small executable updating program along with a data file containing the firmware software. The process takes only minutes, and you'll be amazed at the results.

Connectivity Troubleshooting

Properly configured wireless clients should automatically and quickly connect to the desired SSID. If this isn't taking place, it's time for some troubleshooting. Most wireless connectivity problems come down to either an incorrect configuration (such as an incorrect password) or low signal strength. Without a strong signal, even a properly configured wireless client isn't going to work. Wireless clients use a multi-bar graph (usually five bars) to give an idea of signal strength: zero bars indicates no signal and five bars indicates maximum signal.

Whether configuration or signal strength, the process to diagnose and repair uses the same methods you use for a wired network. First, check the wireless NIC's link light to see whether it's passing data packets to and from the network. Second, check the wireless NIC's configuration utility. Typically the utility has an icon in your system tray/notification area that shows the strength of your wireless signal. Figure 23.27 shows Windows XP Professional's built-in wireless configuration utility—called Wireless Zero Configuration (or just Zeroconf)—displaying the link state and signal

• **Figure 23.27** Windows XP Professional's wireless configuration utility

strength. Wireless Zero Configuration was first introduced with Windows XP. In Windows Vista and Windows 7, the service is called WLAN AutoConfig.

The link state defines the wireless NIC's connection status to a wireless network: connected or disconnected. If your link state indicates that your computer is currently disconnected, you may have a problem with your WAP. If your signal is too weak to receive a signal (referred to on the CompTIA A+ exams as a "low RF signal"), you may be out of range of your access point, or there may be a device causing interference.

You can fix these problems in a number of ways. Because Wi-Fi signals bounce off of objects, you can try small adjustments to your antennas to see if the signal improves. You can swap out the standard antenna for one or more higher-gain antennas. You can relocate the PC or access point, or locate and move the device causing interference.

Other wireless devices that operate in the same frequency range as your wireless nodes can cause interference as well. Look for wireless telephones, intercoms, and so on as possible culprits. One fix for interference caused by other wireless devices is to change the channel your network uses. Another is to change the channel the offending device uses, if possible. If you can't change channels, try moving the interfering device to another area or replacing it with a different device.

If you're lucky enough to have a laptop with an internally installed NIC (instead of a PC Card), your device may not have a link light.

Configuration Troubleshooting

With all due respect to the fine network techs in the field, the most common type of wireless networking problem is misconfigured hardware or software. That's right—the dreaded *user error*! Given the complexities of wireless networking, this isn't so surprising. All it takes is one slip of the typing finger to throw off your configuration completely. The things you're most likely to get wrong are the SSID and security configuration.

Verify SSID configuration on your access point first, and then check on the affected wireless nodes. With most wireless devices, you can use any characters in the SSID, including blank spaces. Be careful not to add blank characters where they don't belong, such as trailing blank spaces behind any other characters typed into the name field.

If you're using MAC address filtering, make sure the MAC address of the client that's attempting to access the wireless network is on the list of accepted users. This is particularly important if you swap out NICs on a PC, or if you introduce a new PC to your wireless network.

Check the security configuration to make sure that all wireless nodes and access points match. Mistyping an encryption key prevents the affected node from talking to the wireless network, even if your signal strength is 100 percent! Remember that many access points have the capability to export encryption keys onto a thumb drive or other removable media. It's then a simple matter to import the encryption key onto the PC by using the wireless NIC's configuration utility. Remember that the encryption level must match on access points and wireless nodes. If your WAP is configured for 128-bit encryption, all nodes must also use 128-bit encryption.

Chapter 23 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about wireless networking.

Discuss wireless networking components

- The wireless radio wave networks you'll find yourself supporting these days are those based on the IEEE 802.11 wireless Ethernet standard Wi-Fi and on the newer Bluetooth technology. Many cellular phone providers also provide Internet access through their networks. Wireless networks using infrared light use the IrDA protocol.
- Wireless networking capabilities of one form or another are built into many modern computing devices. Wireless Ethernet and Bluetooth are almost ubiquitous as integrated components or can easily be added by using USB, PCI, PCI Express, or PC Card adapters. Many smartphones and tablets have wireless capabilities built in or available as add-on options.
- To extend the capabilities of a wireless Ethernet network, such as connecting to a wired network or sharing a high-speed Internet connection, you need a WAP. A WAP centrally connects wireless network nodes in the same way that a hub connects wired Ethernet PCs.

Analyze and explain wireless networking standards

- Wireless devices use the same networking protocols and client that their wired counterparts use, and they operate by using the CSMA/CA networking scheme, where nodes check before broadcasting. Wireless nodes also use the RTS/CTS protocol. When enabled, a transmitting node that determines that the wireless medium is clear to use sends an RTS frame to the receiving node. The receiving node responds with a CTS frame, telling the sending node that it's okay to transmit. Then, once the data is sent, the transmitting node waits for an acknowledgment (ACK) from the receiving node before sending the next data packet.
- You will need a utility to set parameters such as your SSID. Windows XP and up have built-in tools for this, but many adapters come with configuration tools provided by the wireless network adapter vendor.
- The simplest wireless network consists of two or more PCs communicating directly with each other without cabling or any other intermediary hardware (ad hoc mode). More complicated (and more common) wireless networks use a WAP to centralize wireless communication and bridge wireless network segments to wired network segments (infrastructure mode).
- Ad hoc networks are also good for temporary networks such as study groups or business meetings.
- Infrastructure mode is better suited to business networks or networks that need to share dedicated resources such as Internet connections and centralized databases.
- Out of the box, wireless networks have no security configured at all. Wireless devices want to be heard, and WAPs are usually configured to broadcast their presence to their maximum range and welcome all other wireless devices that respond. Further, data packets are floating through the air instead of safely wrapped up inside network cabling.
- Most WAPs support MAC address filtering, a method that enables you to limit access to your wireless network based on the physical, hard-wired address of the unit's wireless network adapter.
- Enabling WEP encrypts your data to secure it while in transit over the airwaves, but the WEP encryption standard itself is flawed and cannot be relied upon to protect your data against a knowledgeable and motivated attacker.
- WPA and WPA2 address the weaknesses of WEP and act as a sort of security protocol upgrade to WEP-enabled devices. WPA and WPA2 offer security enhancements such as an encryption key integrity-checking feature and user authentication through the industry-standard EAP.
- Wi-Fi Protected Setup (WPS) was designed to make connecting wireless devices as easy as pushing a button. Because of its security flaws, however, you should avoid using WPS and disable it entirely.

- Depending on the standard used, wireless throughput speeds range from a measly 2 Mbps to a snappy 100+ Mbps. Wireless devices dynamically negotiate the top speed at which they can communicate without dropping too many data packets.
- Wireless networking speed and range are greatly affected by outside factors, such as interference from other wireless devices or solid objects. A wireless device's true effective range is probably about half the theoretical maximum listed by the manufacturer.
- 802.11a differs from the other 802.11-based standards in significant ways. Foremost, it operates in a different frequency range, 5 GHz, so 802.11a devices are less prone to interference. 802.11a also offers considerably greater throughput than 802.11 and 802.11b at speeds up to 54 Mbps, but its range tops out at only about 150 feet. 802.11a isn't widely adopted in the PC world.
- The 802.11b standard supports data throughput of up to 11 Mbps—on par with older wired 10BaseT networks—and a range of up to 300 feet under ideal conditions.
- The 802.11g standard offers data transfer speeds equivalent to 802.11a, up to 54 Mbps, with the wider 300-foot range of 802.11b. Because 802.11g is backward compatible with 802.11b, the same 802.11g WAP can service both 802.11g and 802.11b wireless nodes.
- 802.11n ups the speed even more to 100+ Mbps and extends the range to greater than 300 feet by using MIMO (multiple in/multiple out) with extra antennas. You can also configure it to use the less crowded 5-GHz band if you are using a dual-mode WAP.
- Wireless networking using infrared (IR) technology is enabled via the Infrared Data Association—IrDA—protocol stack, a widely supported industry standard, and has been included in all versions of Windows since Windows 95. IR is designed to make only a point-to-point connection between two devices in ad hoc mode of up to 4 Mbps, at a maximum distance of 1 meter.
- Bluetooth wireless technology is designed to create small wireless personal area networks (PANs) that link PCs to peripheral devices such as PDAs and printers, input devices such as keyboards and mice, and even consumer electronics such as cell phones, home stereos, televisions, home security systems, and so on. Bluetooth is not designed to be a full-function networking solution.
- Cellular wireless networks enable you to connect to the Internet through a smartphone or portable device with an access card.

Install and configure wireless networks

- The mechanics of setting up a wireless network don't differ much from a wired network. Physically installing a wireless network adapter is the same as installing a wired NIC, whether it's an internal expansion card, a PC Card, or an external USB device. Simply install the device and let plug and play handle the rest.
- Wi-Fi networks support ad hoc and infrastructure operation modes. Which mode you choose depends on the number of wireless nodes you need to support, the type of data sharing they'll perform, and your management requirements.
- Ad hoc mode wireless networks don't need a WAP. The only requirements in an ad hoc mode wireless network are that each wireless node be configured with the same network name (SSID) and that no two nodes use the same IP address. You may also have to select a common channel for all ad hoc nodes.
- Typically, infrastructure mode wireless networks employ one or more WAPs connected to a wired network segment, a corporate intranet or the Internet, or both. As with ad hoc mode wireless networks, infrastructure mode networks require that the same SSID be configured on all nodes and WAPs.
- WAPs have an integrated Web server and are configured through a browser-based setup utility. Typically, you enter the WAP's default IP address to bring up the configuration page and supply an administrative password, included with your WAP's documentation, to log in.
- Set up WEP encryption—if that's your only option—by turning encryption on at the WAP and then generating a unique security key. Then configure all connected wireless nodes on the network with the same key information. WPA and WPA2 encryption are configured in much the same way. You may be required to input a valid user name and password to configure encryption by using WPA/WPA2.

- As with other wireless networking solutions, Bluetooth devices are completely plug and play. Just connect the adapter and follow the prompts to install the appropriate drivers and configuration utilities. Connecting to a Bluetooth PAN is handled by specialized utility software provided by your portable device or Bluetooth device vendor.

Troubleshoot wireless networks

- As with any troubleshooting scenario, your first step should be to figure out the scope of your wireless networking problem. Ask yourself *who*, *what*, and *when*. This helps you focus your initial troubleshooting on the most likely aspects of the network.
- Hardware troubleshooting for Wi-Fi devices should touch on the usual hardware process. Go to Device Manager and check for obvious conflicts. Check the drivers to make sure you have them installed and up-to-date. Make certain you have proper connectivity between the device and the PC.
- Software troubleshooting involves checking configuration settings, such as the SSID, WEP, MAC address filtering, and encryption levels. Be sure to check configuration settings on both the WAP and the wireless NIC.

Key Terms

802.11a *(878)*
802.11b *(878)*
802.11g *(878)*
802.11n *(879)*
ad hoc mode *(874)*
Advanced Encryption Standard (AES) *(876)*
Bluetooth *(881)*
carrier sense multiple access/collision avoidance (CSMA/CA) *(872)*
cellular wireless network *(882)*
dipole antennas *(888)*
Extensible Authentication Protocol (EAP) *(876)*
gain *(888)*
IEEE 802.11 *(871)*
Infrared Data Association (IrDA) *(880)*
infrastructure mode *(874)*
MAC address filtering *(875)*
multiple in/multiple out (MIMO) *(879)*
personal area network (PAN) *(881)*
Power over Ethernet (PoE) *(872)*
service set identifier (SSID) *(874)*
Temporal Key Integrity Protocol (TKIP) *(875)*
Wi-Fi *(878)*
Wi-Fi Protected Access (WPA) *(875)*
Wi-Fi Protected Access 2 (WPA2) *(876)*
Wi-Fi Protected Setup (WPS) *(876)*
Wired Equivalent Privacy (WEP) *(875)*
wireless access point (WAP) *(872)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. A technology for setting up wireless PANs and connecting to some peripherals is called _____.
2. Establishing a unique _____ or network name helps ensure that only wireless network devices configured similarly are permitted access to the network.
3. The wireless Ethernet standard that operates at a maximum of 54 Mbps on the 2.4-GHz frequency is _____.
4. Computers are in _____ when they connect directly together without using a WAP.
5. The 802.11 protocol is more commonly known as _____.
6. Of the three common wireless encryption protocols, _____ is the *least* secure.
7. The wireless Ethernet standard that runs at speeds up to 54 Mbps but has limited range because it uses the 5-GHz frequency is _____.
8. If you need to share an Internet connection or connect to a wired network through your wireless network, you would use _____.

9. The _____ feature enables devices on 802.11n networks to make multiple simultaneous connections, allowing for a theoretical throughput of 600 Mbps.

10. 802.11 implements _____, which proactively avoids network packet collisions rather than simply detecting them when they occur.

Multiple-Choice Quiz

1. Two wireless nodes that are communicating directly with each other, without any intermediary systems or hardware, are using what wireless mode?
   - **A.** Ad hoc
   - **B.** Bluetooth
   - **C.** Infrastructure
   - **D.** 802.11
2. What device centrally connects wireless network nodes in the same way that a hub or switch connects wired Ethernet PCs?
   - **A.** Bluetooth adapter
   - **B.** Wireless NIC
   - **C.** SSID
   - **D.** WAP
3. What is the approximate range of an 802.11b/g network?
   - **A.** ~1000 ft
   - **B.** ~300 ft
   - **C.** ~150 ft
   - **D.** ~500 ft
4. Which encryption method used on wireless networks is the most secure?
   - **A.** WEP
   - **B.** Wi-Fi
   - **C.** WINS
   - **D.** WPA2
5. What can limit wireless connectivity to a list of accepted users based on the hard-wired address of their wireless NIC?
   - **A.** Encryption
   - **B.** MAC filtering
   - **C.** NWLink
   - **D.** WEP
6. Which wireless standard combines the longest range with the most throughput?
   - **A.** 802.11a
   - **B.** 802.11b
   - **C.** 802.11g
   - **D.** 802.11n
7. Personal area networks are created by what wireless technology?
   - **A.** Bluetooth
   - **B.** IrDA
   - **C.** Wi-Fi
   - **D.** Cellular wireless
8. What is the best technology if you need Internet access from anywhere in the country?
   - **A.** Bluetooth
   - **B.** IrDA
   - **C.** Wi-Fi
   - **D.** Cellular wireless
9. What standard gained a speed boost in its second version with Enhanced Data Rate technology?
   - **A.** Bluetooth
   - **B.** IrDA
   - **C.** Wi-Fi
   - **D.** Cellular wireless
10. Which of these Wi-Fi security protocols is the least secure and is easily hacked?
    - **A.** WEP
    - **B.** WAP
    - **C.** WINS
    - **D.** WPA2
11. What is a cheap and easy way to extend the range of a WAP?
    - **A.** Upgrade the antenna.
    - **B.** Buy a WAP that advertises a longer range.
    - **C.** You can't easily boost range.
    - **D.** Upgrade the wireless NICs.

12. What is the technical name of a wireless network?
    - **A.** SSID
    - **B.** BSSID
    - **C.** SSD
    - **D.** WPA
13. What is the approximate range of a Bluetooth PAN?
    - **A.** ~100 ft
    - **B.** ~30 ft
    - **C.** ~5 ft
    - **D.** ~50 ft
14. Which of the following 802.11 standards can make use of both the 2.4- and 5-GHz bands?
    - **A.** 802.11a
    - **B.** 802.11b
    - **C.** 802.11g
    - **D.** 802.11n
15. Which of the following devices is a major source of interference for Wi-Fi networks?
    - **A.** Cell phones
    - **B.** Small FM radio transmitters
    - **C.** Microwaves
    - **D.** Fluorescent lights

Essay Quiz

1. Some friends of yours insist that wireless network standard 802.11a was available before 802.11b. They also say 802.11a is "better" than 802.11b. Find the pages in this chapter that discuss these standards, and jot down some notes to explain the facts.
2. You are enrolled in a writing class at the local community college. This week's assignment is to write on a technical subject. Write a short paragraph about each of the wireless standards that can reach theoretical speeds of 54 Mbps.
3. Prepare a short memo to your instructor (or friend) that outlines the basic differences between WEP and WPA encryption methods. Use any standard memo format you are familiar with. Include a company or school logo on the top of the page to make the memo appear to be printed on company stationery (or "letterhead").
4. Write a few paragraphs describing the pros and cons of both wired and wireless networks. Specifically, compare 100BaseT to the 802.11n standard. Then conclude with a statement of your own personal preference. You'll need to draw on information you found in this chapter and in Chapter 22.

Lab Projects

• Lab Project 23.1

You just received a nice tax return and want to expand your home network. Your current wired home network setup consists of two Intel Core 2 Duo desktop PCs with 10/100-Mbps NICs and a relative's older laptop with both an RJ-45 port and 802.11b wireless built in. The main Internet connection coming into your home enters your more powerful desktop system first and then spreads out to a 100-Mbps switch from there. With your own money to be spent buying equipment, you seek a solution that will satisfy your needs for a long time.

You want to buy your new equipment locally so you can set it up right away. Use the Internet to explore prices and equipment in local stores. Also check out reviews of the items you are interested in obtaining. After you have done sufficient research, prepare an itemized price list with your choices arranged like the following table:

ITEM	STORE/MODEL	PRICE	QUANTITY	TOTAL
Wireless NICs, PCI\PCIe				
Wireless NICs, PC Card				
Wireless Access Point				
Other				
TOTALS				

• Lab Project 23.2

You have been tasked with expanding your company's wireless network. Your IT manager asked you to create a presentation that explains wireless routers and their functions. She specifically said to focus on the 802.11g and 802.11n wireless network standards. Create a brief but informative PowerPoint presentation that includes comparisons of these two technologies. You may include images of actual wireless bridges from vendor Web sites as needed, being sure to cite your sources. Include any up-to-date prices from your research as well.