

chapter
16

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

- **Explain wireless networking standards**
- **Describe the process for implementing Wi-Fi networks**
- **Describe troubleshooting techniques for wireless networks**

Every type of network covered thus far in the book assumes that your PCs connect to your network with some kind of physical cabling. Now it's time to cut the cord and look at one of the most exciting developments in network technology: wireless networking.

Historical/Conceptual

Instead of a physical set of wires running among networked PCs, servers, printers, or what-have-you, a **wireless network** uses radio waves to enable these devices to communicate with each other. This offers great promise to the folks who've spent time pulling cable up through ceiling spaces and down behind walls, and therefore know how time consuming that job can be.

But wireless networking is more than just convenient—sometimes it's the only networking solution that works. For example, I have a client whose offices are housed in a building designated as a historic landmark. Guess what? You can't go punching holes in historic landmarks to make room for network cable runs. Wireless networking is the solution.

Wireless networks operate at the same OSI layers and use the same protocols as wired networks. The thing that differs is the type of media—radio waves instead of cables—and the methods for accessing the media. Different wireless networking solutions have come and gone in the past, but the wireless networking market these days is dominated by the most common implementation of the IEEE 802.11 wireless Ethernet standard, **Wi-Fi**.

The chapter looks first at the standards for modern wireless networks, and then turns to implementing those networks. The chapter finishes with a discussion on troubleshooting Wi-Fi.



Because the networking signal is freed from wires, you'll sometimes hear the term "unbounded media" to describe wireless networking.

Test Specific

■ Wi-Fi Standards

Wi-Fi is by far the most widely adopted wireless networking type today. Not only do thousands 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.

Technically, only wireless devices that conform to the extended versions of the 802.11 standard—802.11a, 802.11b, 802.11g, and 802.11n—are Wi-Fi certified. Wi-Fi certification comes from the Wi-Fi Alliance, a nonprofit industry group made up of over 300 member companies that design and manufacture wireless networking products. Wi-Fi certification ensures compatibility between wireless networking devices made by different vendors. That's the way it's *supposed* to work, anyway, but see the last section of this chapter on troubleshooting for the real-world scoop.



Wi-Fi originally stood for *wireless fidelity* to make it cutely equated with high fidelity or Hi-Fi, but it doesn't really stand for anything any more.

802.11

The **802.11** standard defines both how wireless devices communicate and how to secure that communication. The communication standards take on the name of the IEEE subcommittee that sets those standards, such as 802.11b and 802.11n. The original 802.11 standard established the baseline features common to all subsequent Wi-Fi standards; we'll examine 802.11 before exploring variations in 802.11b, 802.11a, 802.11g, and 802.11n. The

section wraps up with a discussion on security standards, from authentication to encryption.

All Wi-Fi standards share certain features, such as a wireless network card, special configuration software, and the capability to run in multiple styles of networks. In addition, Wi-Fi implementations require a shared network name and channel for communication. Each standard has a certain top speed and range of networking capability. Finally, 802.11 defines how transmissions work, so we'll look at frequencies of radio signals, transmission methods, and collision avoidance.




• **Figure 16.1** Wireless PCI NIC

Hardware

Wireless networking hardware serves the same function as hardware used on wired PCs. Wireless Ethernet NICs take data passed down from the upper OSI layers, encapsulate it into data packets, send the packets out on the network media in strings of ones and zeroes, and receive data packets sent from other PCs. The only difference is that instead of charging up a network cable with electrical current or firing off pulses of light, these devices transmit and receive radio waves.

Wireless networking capabilities of one form or another are built into many modern computing devices. Wireless Ethernet capabilities are increasingly popular as integrated components, or can easily be added using PCI or PC Card add-on cards. In fact, many wireless PCI NICs are simply wireless PC Card NICs that have been permanently housed in a PCI component card. Figure 16.1 shows a wireless PCI Ethernet card.

You can also add wireless network capabilities using external USB wireless network adapters, as shown in Figure 16.2. The USB NICs have the added benefit of being *placeable*—that is, you can move them around to catch the wireless signal as strongly as possible, akin to moving the rabbit ears on old pre-cable television sets.



Tech Tip
USB Extender Cables
Many USB Wi-Fi NICs these days come as little USB sticks, similar in looks to a flash memory thumb drive. You can still position this type of NIC, though, by using a USB extender cable, with a male USB A connector on one end and a female USB A connector on the other.



• **Figure 16.2** External USB wireless NIC

Is the wireless network adapter all the hardware you need to connect wirelessly? Well, if your needs are simple—for example, if you’re connecting a small group of computers into a decentralized workgroup—then the answer is yes. However, if you need to extend the capabilities of a wireless Ethernet network—say, connecting a wireless network segment to a wired network—you need additional equipment. This typically means a wireless access point.

A **wireless access point (WAP)** connects wireless network nodes to wireless or wired networks. A basic WAP operates like a hub and works at OSI Layer 1. Many WAP manufacturers combine multiple devices into one box, however, to create a high-speed hub or switch, bridge, and router, all rolled into one and working at many different OSI layers. The Linksys device shown in Figure 16.3 is an example of this type of combo device.

Software

Every wireless network adapter needs two pieces of software to function with an operating system: a driver and a configuration utility. Installing drivers for wireless networking devices is usually no more difficult than for any other hardware device, but you should always consult your vendor’s instructions before popping that card into a slot. Most of the time, you simply have to let Plug and Play (PnP) work its magic and put in the driver disc when prompted, but some devices (particularly USB devices) require that you install the drivers beforehand. All modern operating systems come well equipped for wireless networking. Even so, it’s always a good idea to use the manufacturer’s drivers and configuration utilities.

You also need a utility for configuring how the wireless hardware connects to other wireless devices. Windows XP, Windows Vista, and Macintosh OS X have built-in tools for configuring these settings, but for previous versions of Windows, you need to rely on wireless client configuration tools provided by the wireless network adapter vendor. Figure 16.4 shows a typical wireless network adapter’s client configuration utility. Using this utility, you can determine important things like your **link state** (whether your wireless device is connected) and your **signal strength** (a measurement of how well your wireless device is connecting to other devices); you can also configure items such as your wireless networking *mode*, security encryption, power-saving options, and so on. I’ll cover each of these topics in detail later in this chapter.

You configure WAPs and routers through browser-based setup utilities. The section “Implementing Wi-Fi” covers this process in detail a bit later in this chapter. Let’s look at the different modes that wireless networks use.



Cross Check

Using Routers

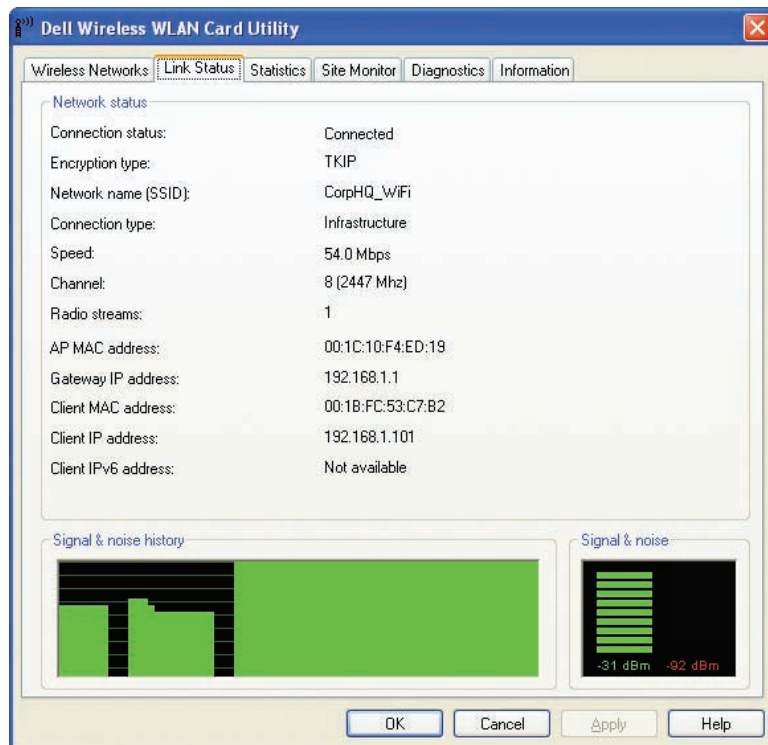
You’ve seen wired routers before, and wireless routers function similarly, so cross-check your memory. Turn to Chapter 2, “Building a Network with the OSI Model,” and see if you can answer these questions. What can a router do for your network? Can you use a router to connect to the Internet? At what layer of the OSI seven-layer model do routers function? How do routers handle addressing?



Some manufacturers drop the word “wireless” from wireless access points and simply call them access points. Further, many sources abbreviate both forms, so you’ll see the former written as WAP and the latter as AP.



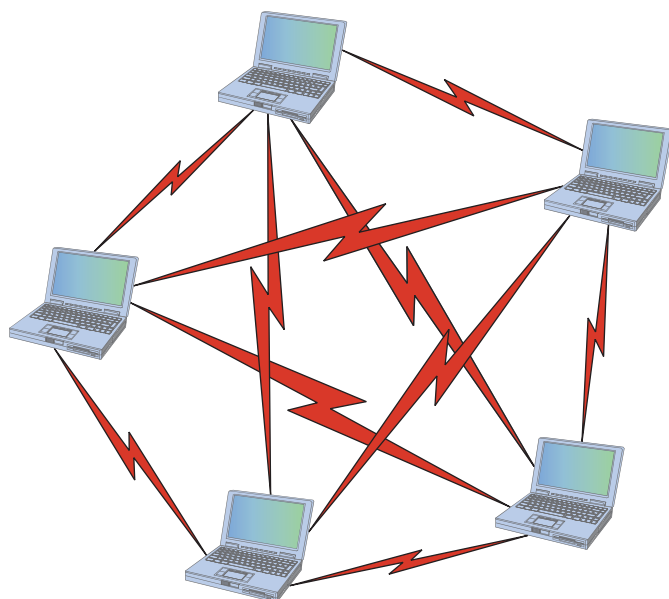
• **Figure 16.3** Linksys device that acts as wireless access point, switch, and DSL router



• Figure 16.4 Wireless client 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 an access point to centralize wireless communication, and to bridge wireless network segments to wired network segments. These two different methods, or *modes*, are called *ad hoc* mode and *infrastructure* mode.



• Figure 16.5 Wireless ad hoc mode network

Ad Hoc Mode **Ad hoc mode** is sometimes called **peer-to-peer mode**, with each wireless node in direct contact with each other node in a decentralized free-for-all, as shown in Figure 16.5. Ad hoc mode does not use an access point and instead uses a *mesh* topology, as discussed in Chapter 3, “Cabling and Topology.”

Two or more wireless nodes communicating in ad hoc mode form what’s called an **Independent Basic Service Set (IBSS)**. This is a basic unit of organization in wireless networks. Think of an IBSS as a wireless workgroup, and you’re not far off the mark.

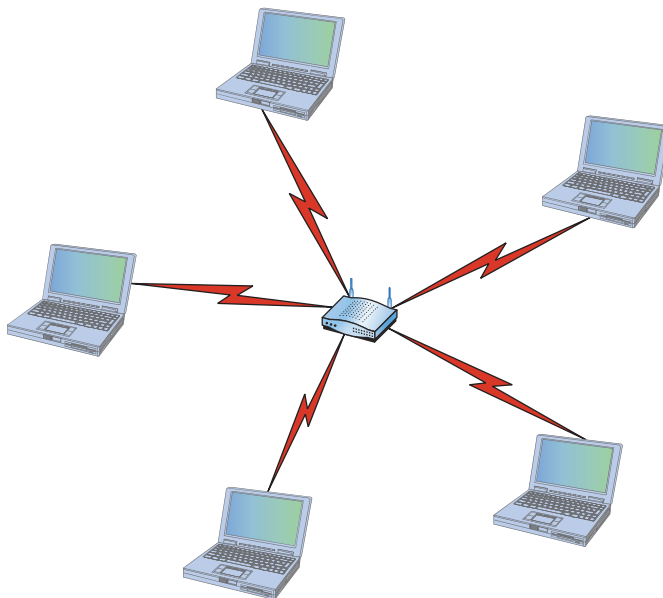
Ad hoc mode networks work well for small groups of computers (fewer than a dozen or so) that need to transfer files or share printers. Ad hoc networks are also good for temporary networks, such as study groups or business meetings.

Hardly anyone uses ad hoc networks for day-to-day work, simply because you can't use an ad hoc network to connect to other networks unless one of the machines is running Internet Connection Sharing (ICS) or some equivalent. More commonly, you'll find wireless networks configured in infrastructure mode.

Infrastructure Mode Wireless networks running in **infrastructure mode** use one or more WAPs to connect the wireless network nodes centrally, as shown in Figure 16.6. This configuration is similar to the *star* topology of a wired network. You also use infrastructure mode to connect wireless network segments to wired segments. If you plan to set up a wireless network for a large number of PCs, or you need to have centralized control over the wireless network, infrastructure mode is what you need.

A single WAP servicing a given area is called a **Basic Service Set (BSS)**. This service area can be extended by adding more access points. This is called, appropriately, an **Extended Service Set (ESS)**.

Wireless networks running in infrastructure mode require a little more planning—such as where you place the WAPs to provide adequate coverage—than ad hoc mode networks, and they provide a stable environment for permanent wireless network installations. Infrastructure mode is better suited to business networks or networks that need to share dedicated resources such as Internet connections and centralized databases. (See “Implementing Wi-Fi” later in this chapter.)



• **Figure 16.6** Wireless infrastructure mode network



Infrastructure mode is so much more commonly used than ad hoc mode that most wireless NICs come preconfigured to run on an infrastructure mode network. Getting them to run in ad hoc mode usually requires reconfiguration.



Cross Check

Topologies

The topology of a network represents the physical connectivity between nodes. This seems as good a time as any to cross-check your knowledge of topologies, so recall back to Chapter 3 and answer these questions. What are the four standard topologies? What are the hybrid topologies? If you connect a wireless network in infrastructure mode to a wired Ethernet network, what topology would that combined network have?



Tech Tip

EBSS vs. ESS

A lot of techs have dropped the word “basic” from the Extended Basic Service Set, the early name for an infrastructure-mode wireless network with more than one WAP. Accordingly, you’ll see the initials for the Extended Basic Service Set as ESS. Using either EBSS or ESS is correct.

Speed

Wireless networking data throughput speeds depend on a few 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 quick 300 Mbps. 802.11 topped out at 2 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 only achieved 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.

Finally, speed is 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, *very* effectively block a wireless network signal! Other culprits include electrical fuse boxes, metal plumbing, and air conditioning units.

Range

Wireless networking range is hard to define, and you'll see most descriptions listed with qualifiers such as “around 150 feet” and “about 300 feet.” 802.11 networks fell into the former category. Like throughput speed, wireless range is greatly affected by environmental factors. Interference from other wireless devices and solid objects affect range.

The maximum ranges listed in the sections that follow are those presented by wireless manufacturers as the *theoretical* maximum ranges. In the real world, you'll see these ranges only under the most ideal circumstances. True effective range is probably about half of what you see listed.

BSSID, SSID, and ESSID

Wireless devices connected together into a network, whether ad hoc or infrastructure, require some way to identify that network. Packets bound for computers within the network need to go where they're supposed to go, even when you have more than one Wi-Fi network overlapping. The jargon gets a little crazy here, especially because marketing has come into the mix.

The **Basic Service Set Identifier (BSSID)** defines the most basic infrastructure mode network, a BSS of one WAP and one or more wireless nodes. With such a simple network, the Wi-Fi folks didn't see any reason to create some new numbering or naming scheme, so they made the BSSID the same as the MAC address for the WAP. Simple! Ah, but what to do about ad-hoc networks that don't have a WAP? The nodes that connect in an IBSS randomly generate a 48-bit string of numbers that looks and functions just like a MAC address, and that BSSID goes in every packet.

You could, if required, discover the MAC address for the WAP in a BSS and manually type that into the network name field when setting up a wireless computer. But that brings up two problems. First, people don't want to remember strings of 48 digits, even if translated out as six hexadecimal

octets, like A9-45-F2-3E-CA-12. People want names. Second, how do you connect two or more computers together into an IBSS when the BSSID has to be randomly generated?

The Wi-Fi folks created another level of naming called a **Service Set Identifier (SSID)**, a standard name applied to the BSS or IBSS to help connection happen. The SSID—sometimes called a **network name**—is a 32-bit identification string that's inserted into the header of each data packet processed by a WAP. Every Wi-Fi device must share the same SSID to communicate in a single network.

So let's take it one step further into a Wi-Fi network that has multiple WAPs, an ESS. How do you determine the network name at this level? You simply repurpose the SSID, only apply it to the ESS as an **Extended Service Set Identifier (ESSID)**.

Unfortunately, most Wi-Fi devices just use the term SSID, not ESSID. When you configure a wireless device to connect to an ESS, you're technically using the ESSID rather than just the SSID, but the manufacturer often has tried to make it simple for you by using only the term SSID.



The CompTIA Network+ certification exam uses the two terms—SSID and ESSID—interchangeably. Concentrate on these two terms for the exam.

Broadcasting Frequency

One of the biggest issues with wireless communication is the potential for interference from other wireless devices. To solve this, different wireless devices must operate in specific broadcasting frequencies. Knowing these wireless frequency ranges will assist you in troubleshooting interference issues from other devices operating in the same wireless band. The original 802.11 standards use the 2.4-GHz frequency. Later standards use either 2.4-GHz or 5.0-GHz frequencies.

Broadcasting Methods

The original IEEE 802.11 wireless Ethernet standard defined methods by which devices may communicate using *spread-spectrum* radio waves. Spread-spectrum broadcasts data in small, discrete chunks over the different frequencies available within a certain frequency range.

802.11 defines three different spread-spectrum broadcasting methods: **direct-sequence spread spectrum (DSSS)**, **frequency-hopping spread spectrum (FHSS)** and **orthogonal frequency-division multiplexing (OFDM)**. DSSS sends data out on different frequencies at the same time, while FHSS sends data on one frequency at a time, constantly shifting (or *hopping*) frequencies. DSSS uses considerably more bandwidth than FHSS—around 22 MHz as opposed to 1 MHz. DSSS is capable of greater data throughput, but it's also more prone to interference than FHSS. OFDM is the latest method and combines the multiple frequencies of DSSS with FHSS's hopping capability. The 802.11 wireless networking implementation used DSSS and later OFDM.

Channels

Every Wi-Fi network communicates on a **channel**, a portion of the spectrum available. The 802.11 standard defined 14 channels, but different countries may limit exactly which channels may be used. In the United States, for example, a WAP may only use channels 1 through 11. These channels have some overlap, so it's not a good idea to have two nearby WAPs to use close

channels like 6 and 7. Most WAPs use channel 1, 6, or 11 by default to keep the channels as far apart as possible. You can fine-tune a network by moving WAPs to other channels to avoid overlap with other, nearby WAPs. This is especially important in environments with many wireless networks sharing the same physical space.



Wired Ethernet networks use carrier sense, multiple access/collision detection (CSMA/CD). Wi-Fi networks use carrier sense multiple access/collision avoidance (CSMA/CA).

CSMA/CA

Because only a single device can use any network at a time, network nodes must have a way to access the network media without stepping on each other's data packets. Wired Ethernet networks use *carrier sense, multiple access/collision detection* (CSMA/CD), as you'll recall from previous chapters, but Wi-Fi networks use **carrier sense multiple access/collision avoidance (CSMA/CA)**. Let's compare both methods.

How do multiple devices share the network media, such as a cable? This is fairly simple: each device listens in on the network media by measuring the level of voltage currently on the wire. If the level is below the threshold, the device knows that it's clear to send data. If the voltage level rises above a preset threshold, the device knows that the line is busy and it must wait before sending data. Typically, the waiting period is the length of the current frame plus a short, predefined silence period called an **interframe space (IFS)**. So far, so good—but what happens when two devices both detect that the wire is free and try to send data simultaneously? As you probably guessed, packets transmitted on the network from two different devices at the same time will corrupt each other, thereby canceling each other out. This is called a *collision*. Collisions are a fact of networking life. So, how do network nodes deal with collisions? They either react to collisions after they happen, or they take steps to avoid collisions in the first place.

CSMA/CD is the reactive method. With CSMA/CD, each sending node detects the collision and responds by generating a random timeout period for itself, during which it doesn't try to send any more data on the network—this is called a *backoff*. Once the backoff period expires (remember that we're only talking about milliseconds here), the node goes through the whole process again. This approach may not be very elegant, but it gets the job done.

CSMA/CD won't work for wireless networking as, wireless devices simply can't detect collisions; therefore, wireless networks need another way of dealing with them. The CSMA/CA access method, as the name implies, proactively takes steps to avoid collisions. The 802.11 standard defines two methods of collision avoidance: **Distributed Coordination Function (DCF)** and **Point Coordination Function (PCF)**. Currently, only DCF is implemented.

802.11 was the very oldest wireless standard (see Table 16.1). Over time, more detailed additions to 802.11 came along that improved speed and took advantage of other frequency bands.



Tech Tip

DCF

DCF specifies much stricter rules for sending data onto the network media. For instance, if a wireless network node detects that the network is busy, DCF defines a backoff period on top of the normal IFS wait period before a node can try to access the network again. DCF also requires that receiving nodes send an acknowledgment (ACK) for every packet that they process. The ACK also includes a value that tells other wireless nodes to wait a certain duration before trying to access the network media. This period is calculated to be the time that the data packet takes to reach its destination based on the packet's length and data rate. If the sending node doesn't receive an ACK, it retransmits the same data packet until it gets a confirmation that the packet reached its destination.



Current CSMA/CA devices use the Distributed Coordination Function (DCF) method for collision avoidance.

Table 16.1 802.11 Summary

Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11	2.4 GHz	DSSS	11 Mbps	~300'	802.11

802.11b

The first widely adopted Wi-Fi standard—**802.11b**—supports data throughput of up to 11 Mbps and a range of up to 300 feet under ideal conditions. The main downside to using 802.11b is, in fact, that it's so popular. The 2.4-GHz frequency is already a crowded place, so you're more likely to run into interference from other wireless devices. Table 16.2 gives you the 802.11b summary.

Table 16.2		802.11b Summary			
Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11b	2.4 GHz	DSSS	11 Mbps	~300'	802.11b

802.11a

Despite the *a* designation for this extension to the 802.11 standard, **802.11a** was available on the market *after* 802.11b. 802.11a differs from the other 802.11-based standards in significant ways. Foremost is that it operates in a different frequency range, 5 GHz. The 5-GHz range is much less crowded than the 2.4-GHz range, reducing the chance of interference from devices such as telephones and microwave ovens. 802.11a also offers considerably greater throughput than 802.11 and 802.11b, at speeds up to 54 Mbps. Range, however, suffers somewhat, and tops out at about 150 feet. Despite the superior speed of 802.11a, it never enjoyed the popularity of 802.11b.

Although you can get NICs and WAPs that support both 802.11b and 802.11a, the standards are not compatible with each other. A computer with an 802.11b NIC, for example, can't connect to a WAP that's only 802.11a, but could connect to an 802.11a/b WAP. Table 16.3 gives you the 802.11a summary.

Table 16.3		802.11a Summary			
Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11a	5.0 GHz	DSSS	54 Mbps	~150'	802.11a

802.11g

The **802.11g** standard offers data transfer speeds equivalent to 802.11a—up to 54 Mbps—and the wider 300-foot range of 802.11b. More importantly, 802.11g is backwardly compatible with 802.11b, so the same 802.11g WAP can service both 802.11b and 802.11g wireless nodes.

If an 802.11g network only has 802.11g devices connected, the network runs in *native mode*—at up to 54 Mbps—whereas when 802.11b devices connect, the network drops down to *mixed mode*—all communication runs only up to 11 Mbps. Table 16.4 gives you the 802.11g summary.

Table 16.4		802.11g Summary			
Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11g	2.4 GHz	OFDM	54 Mbps	~300'	802.11b/g

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 antennae to implement a feature called **multiple in/multiple out (MIMO)**, which enables the devices to make multiple simultaneous connections. With up to four antennae, 802.11n devices can do 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 antennae adjust the signal once the WAP discovers a client to optimize the radio signal.

Like 802.11g, 802.11n WAPs can support earlier, slower 802.11b/g devices. The so-called “dual-band” WAPs can run at both 5 GHz and 2.4 GHz simultaneously; some support 802.11a devices as well as 802.11b/g devices. Nice! Table 16.5 gives you the 802.11n summary.

Table 16.5 802.11n Summary

Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11n	2.4 GHz ¹	OFDM	100+ Mbps	~300'	802.11b/g/n ²
¹ Dual-band 802.11n devices can function simultaneously at both 2.4- and 5.0-GHz bands. ² Many dual-band 802.11n WAPs support 802.11a devices as well as 802.11b/g/n devices. This is not part of the standard, but something manufacturers have implemented.					



Tech Tip

802.16

Products that use the **802.16** wireless standard—often called **WiMax**—are expected on the market any time now. Although speed for 802.16-compliant devices is about the same as 802.11b, manufacturers claim a range of up to 30 miles! This kind of range would be perfect for so-called metropolitan area networks (MANs). Before you get too excited, though, keep in mind that the speed of the network will almost certainly decrease the farther away from the base station (the WAP) the nodes are. Effective range could be as little as three miles, but that still beats 300 feet in my book!

Wireless Networking Security

One of the biggest problems with wireless networking devices is that right out of the box, they provide *no* security. Vendors go out of their way to make it easy to set up their devices, so usually the only thing that you have to do to join a wireless network is turn your wireless devices on and let them find each other. Sure, from a configuration point of view, this is great—but from a security point of view, it’s a disaster!

Further, you have to consider that your network’s data packets float through the air on radio waves instead of zipping safely along wrapped up inside network cabling. What’s to stop an unscrupulous network tech with the right equipment from grabbing those packets out of the air and reading that data?

To address these issues, wireless networks use three methods: MAC address filtering, authentication, and data encryption. The first two methods secure access to the network itself, and the third secures the data that’s moving around the network. All three of these methods require you to configure the WAPs and wireless devices. Let’s take a look.

MAC Address Filtering

Most WAPs support **MAC address filtering**, a method that enables you to limit access to your network based on the physical addresses of wireless NICs. MAC address filtering creates a type of “accepted users” list to limit access to your wireless network. 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 WAPs also enable you to deny specific MAC addresses from logging onto the network. This works great in close quarters, such as apartments or office buildings, where your wireless network signal goes beyond your perimeter. You can check the WAP and see the MAC addresses of every node that connects to your network. Check that list against the list of your computers, and you can readily spot any unwanted interloper. Putting

an offending MAC address in the “deny” column effectively blocks that system from piggybacking onto your wireless connection.

While both methods work, a hacker can very easily *spoof* a MAC address—make the NIC report a legitimate address rather than its own—and access the network. Worse, a hacker doesn’t have to connect to your network to grab your network traffic out of thin air! If you have data so important that a hacker would want to get at it, you should seriously consider using a wired network, or separating the sensitive data from your wireless network in some fashion. MAC address filtering is also a bit of a maintenance nightmare, as every time you replace a NIC, you have to reconfigure your WAP with the new NIC’s MAC address.

Wireless Authentication

Implementing authentication enables you to secure a network so that only users with the proper credentials can access network resources. It’s not an all-or-nothing deal, of course; you can use authentication to restrict or enable what a specific user can do once inside the network as well.

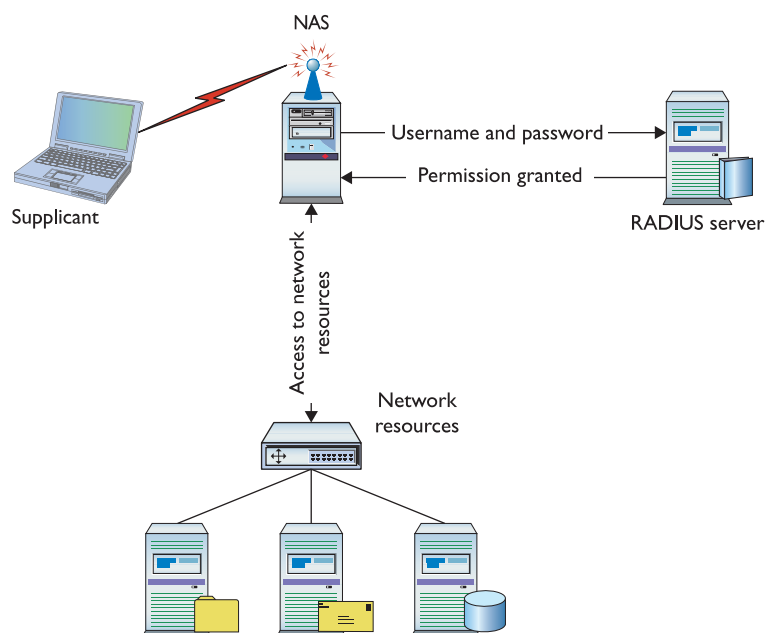
Authentication in a wired network, as you’ll recall from Chapter 11, “Securing TCP/IP Applications,” generally takes the form of a centralized security database that contains user names, passwords, and permissions, like the Active Directory in a Windows Server environment. Wireless network clients can use the same security database as wired clients, but it takes a couple of extra steps to get the wireless user authenticated.

The IEEE **802.1X** standard enables you to set up a network with some seriously secure authentication using a RADIUS server and passwords encrypted with **Extensible Authentication Protocol (EAP)**. Let’s look at the components and the process.

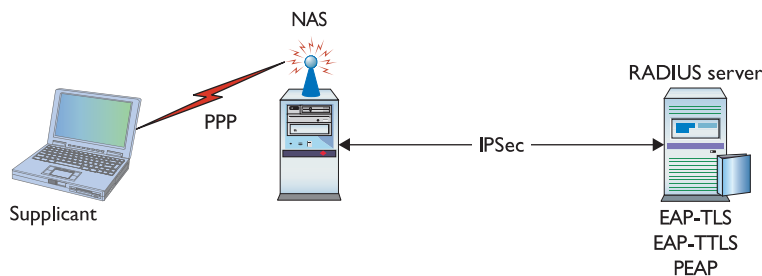
A **RADIUS server** enables remote users to connect to a network service. It provides authentication through a user name and password, and enables you to set a user’s rights once in the network. A RADIUS server functions like a typical server, but the remote aspect of it requires you to learn new jargon. The terms “client” and “server” are so Active Directory, after all.

Here’s how it works. The client computer, called a **supplicant**, contacts the WAP, called a **Network Access Server (NAS)**, and requests permission to access the network. The NAS contacts the RADIUS server to see if the supplicant appears in the RADIUS server’s security database. If the supplicant appears and the user name and password are correct, then the remote user gets access to the network resources. See Figure 16-7.

Here’s where it gets tricky. What are the points of potential failure of security here? All over the place, right? The connection between each of these devices must be secure; several protocols make certain of that security. PPP, for example, provides a secure dial-up connection between the supplicant and the NAS.



• **Figure 16.7** Authenticating using RADIUS

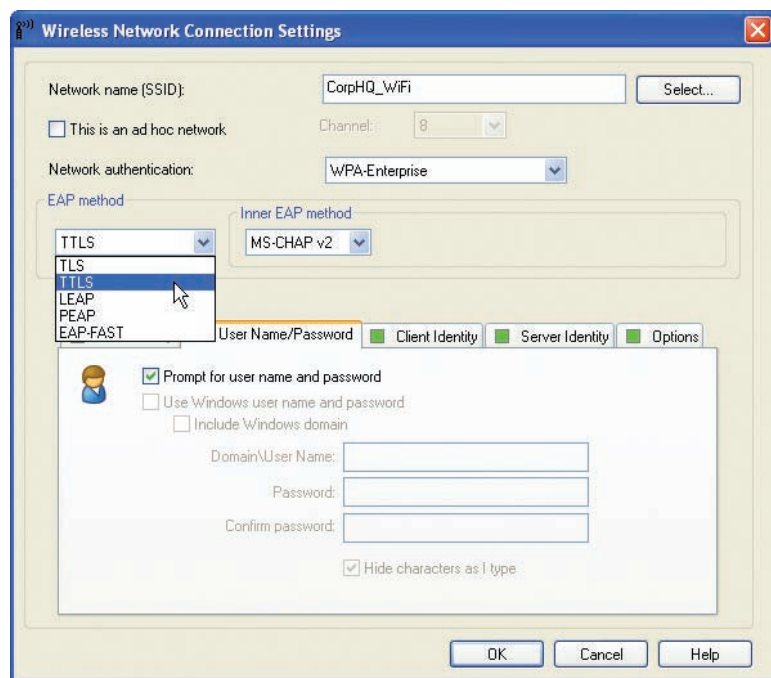


• **Figure 16.8** Authentication using RADIUS with protocols in place



EAP and RADIUS servers for authentication paint half the picture on 802.1X security implementation. The other half is WPA2, discussed below.

argument among geeks, but from a technician's perspective you simply use the scheme that your network hardware supports. Both the WAP and the wireless NICs have to use the same EAP authentication scheme. You set this in the firmware or software, as you can see in Figure 16.9.



• **Figure 16.9** Setting EAP authentication scheme

fact, WEP can be cracked in 60 seconds with just a regular laptop and open source software! WEP doesn't provide complete encryption for data packets. It works only on the two lowest OSI network layers: the Data Link and Physical layers. Encryption is stripped from the data packet before it travels up through the subsequent network layers to the application.

Another problem with WEP is that the encryption key is both static (never changes from session to session) and shared (the same key is used by all network nodes). There is also no mechanism for performing user authentication. That is, network nodes that use WEP encryption are identified by

IPSec often provides security between the NAS and the RADIUS server. Finally, the RADIUS server needs to use a protocol, such as one of the many implementations of the Extensible Authentication Protocol (EAP), for the authentication part of the deal. See Figure 16.8.

EAP defines a framework for authentication, but does not specify how the authentication happens. Developers have therefore come up with many ways to handle the specifics, such as EAP-TLS, EAP-TTLS, and PEAP, to name just a few. The differences among the many flavors of EAP cause countless hours of

Data Encryption

The final step in securing a wireless network is encrypting the data packets that are floating around. **Encryption** electronically scrambles data packets and locks them with a private encryption key before transmitting them onto the wireless network. The receiving network device has to possess the encryption key to unscramble the packet and process the data. Thus, a hacker who grabs any data packets out of the air can't read those packets unless he or she has the encryption key. Enabling wireless encryption through Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or WPA2 provides a good level of security to data packets in transit.

Data Encryption Using WEP **Wired Equivalent Privacy (WEP)** encryption uses a 64- or 128-bit encryption algorithm to scramble data packets, though even with the strongest encryption enabled, WEP isn't considered to be a particularly robust security solution. In

their MAC address, and no other credentials are offered or required. With just a laptop and some open source software, MAC addresses are very easy to sniff out and duplicate, thus opening up a possible spoofing attack.

Data Encryption Using WPA **Wi-Fi Protected Access (WPA)** addresses some of the weaknesses of WEP, and acts as a security protocol upgrade to WEP-enabled devices. WPA offers security enhancements such as dynamic encryption key generation (keys are issued on a per-user and per-session basis) and an encryption key integrity-checking feature.

WPA works by using an extra layer of security, called the **Temporal Key Integrity Protocol (TKIP)**, around the WEP encryption scheme. It's not, therefore, a complete replacement protocol for WEP. TKIP added a 128-bit encryption key that seemed unbreakable when first introduced. Within a couple of years of introduction, though, hackers could waltz through WPA security almost as quickly as through WEP security. Another solution had to be found.

Data Encryption Using WPA2 The IEEE **802.11i** standard amended the 802.11 standard to add much-needed security features. One of those features we've discussed already, the 802.1X authentication measure using EAP to provide secure access to Wi-Fi networks. Another key feature, **Wi-Fi Protected Access 2 (WPA2)**, changes the encryption algorithm used in WEP and WPA to the **Advanced Encryption Standard (AES)**, a 128-bit block cipher that's much tougher to crack than the 128-bit TKIP wrapper. WPA2 is not hack proof, but it definitely offers a much tougher encryption standard that stops the casual hacker cold.

Power Over Ethernet

Wireless access points need electrical power, but they're invariably placed into strange locations (like ceilings or high up on walls) where it's not convenient to provide electrical power. No worries! Better WAPs now support a standard called **Power over Ethernet (PoE)** where they can get their power from the same Ethernet cables that transfer their data. The switch that connects the WAPs must support PoE, but as long as both the WAP and the switches to which they connect support PoE, there's nothing you have to do other than just plug in Ethernet cables. PoE works automatically. As you might imagine, it costs extra to get WAPs and switches that support PoE, but the convenience of PoE for wireless networks makes it a popular option.

■ Implementing Wi-Fi

To install and configure a Wi-Fi network requires a number of discrete steps. You should start with a site survey to determine any obstacles you need to overcome. All wireless networks require clients, so that's your next step. That's all the hardware you'll need for an ad-hoc network, but an infrastructure network takes a few more pieces, such as installing an access point and configuring both the access point and clients. Unless you have a small, personal network, you need to look at ways to extend the network so you have the coverage you want. Finally, you should put your network to the test, verifying that it works as you intended.

Site Survey

A **site survey** enables you to determine any obstacles to creating the wireless network you want. You should discover any other wireless networks in the area and create a drawing with interference sources clearly marked. This enables you to get the right kind of hardware you need to employ and makes it possible to get the proper network coverage.

What Wireless Is Already There?

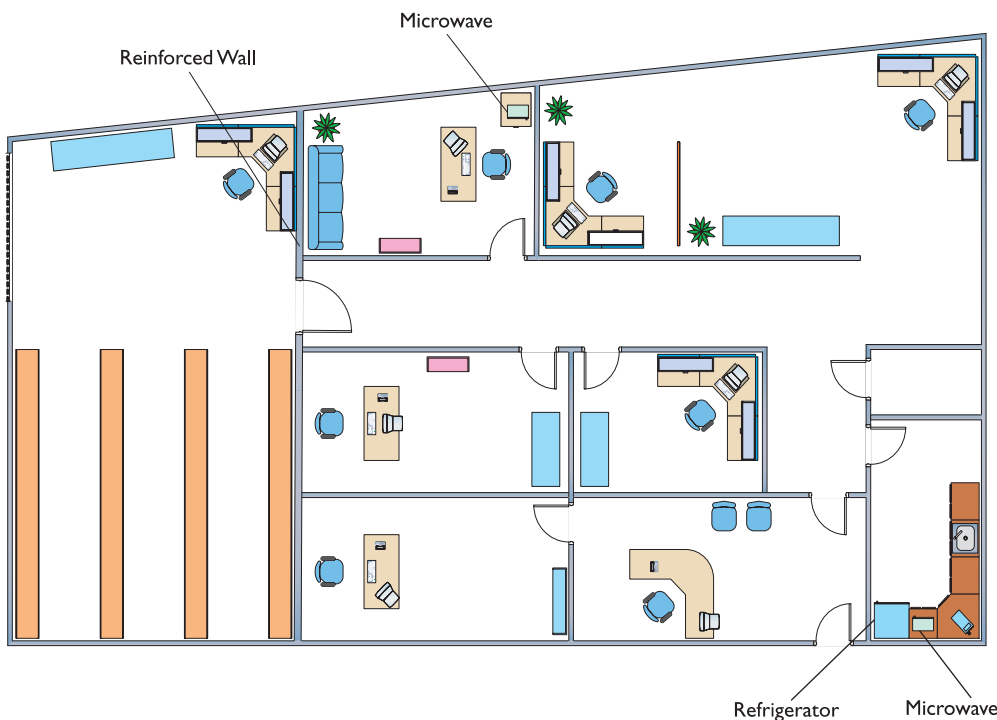
Discovering any wireless network signals other than your own in your space enables you to set both the SSID and channel to avoid networks that overlap. Wireless networks send out radio signals along the 2.4- or 5-GHz band and use channels 1–11. If you have an 802.11g WAP and clients, for example, those devices would use the 2.4-GHz band and could be set to channel 1. A quick scan of the Wi-Fi networks in my neighborhood, for instance, shows five Wi-Fi networks, two with the SSID of Linksys, three using Channel 6, and two with both distinctive nondefault names and channels. If my network SSID were set to Linksys, which WAP have I used when I log onto the Linksys network?

Even if you change the SSID, why run on the same channel as other Wi-Fi networks? You'll see better performance if you're on a unique channel.

Interference Sources

It might seem like overkill in a small network, but any network beyond a simple ad-hoc one should have a sketched-out site survey with any potential interference sources clearly marked (Figure 16.10). Refrigerators,

reinforced walls, metal plumbing, microwave ovens; all of these can create horrible dead spots where your network radio wave can't easily penetrate. With a difficult or high-interference area, you might need to move up to 802.11n equipment with three or four antennae just to get the kind of coverage you want. Or you might need to plan a multiple WAP network to wipe out the dead zones. A proper site survey gives you the first tool for implementing a network that works.



• **Figure 16.10** Site survey with interference sources noted

Installing the Client

Because every Wi-Fi network needs clients (otherwise, what's the point?), you need to install Wi-Fi client hardware and software. With a PCI or PCI Express NIC, power down the PC, disconnect from the AC source, and open the case. Following good CompTIA A+ technician procedures, locate a free slot on the motherboard, remove the slot cover, remove the NIC from its antistatic bag, install the NIC, and affix the retaining screw. See Figure 16.11. Often you'll need to attach the antenna. Button everything up, plug it in, and start the computer. When prompted, put in the disc that came from the manufacturer and install drivers and any other software necessary.

With a USB NIC, you should install the drivers and software before you connect the NIC to the computer. This is standard operating procedure for any USB device, as you most likely recall from your CompTIA A+ certification training (or from personal experience).



• **Figure 16.11** Wi-Fi PCI NIC installed

Setting Up an Ad Hoc Network

Configuring NICs for ad hoc mode networking requires you to address four things: SSID, IP addresses, channel, and sharing. (Plus, of course, you have to set the NICs to function in ad hoc mode!) Each wireless node must use the same network name (SSID). Also, no two nodes can use the same IP address—although this is unlikely with modern versions of Windows and the Automatic Private IP Addressing (APIPA) feature that automatically selects a Class B IP address for any node not connected to a DHCP server or hard-coded to an IP address. Finally, ensure that the File and Printer Sharing service is running on all nodes. Figure 16.12 shows a wireless network configuration utility with ad hoc mode selected.



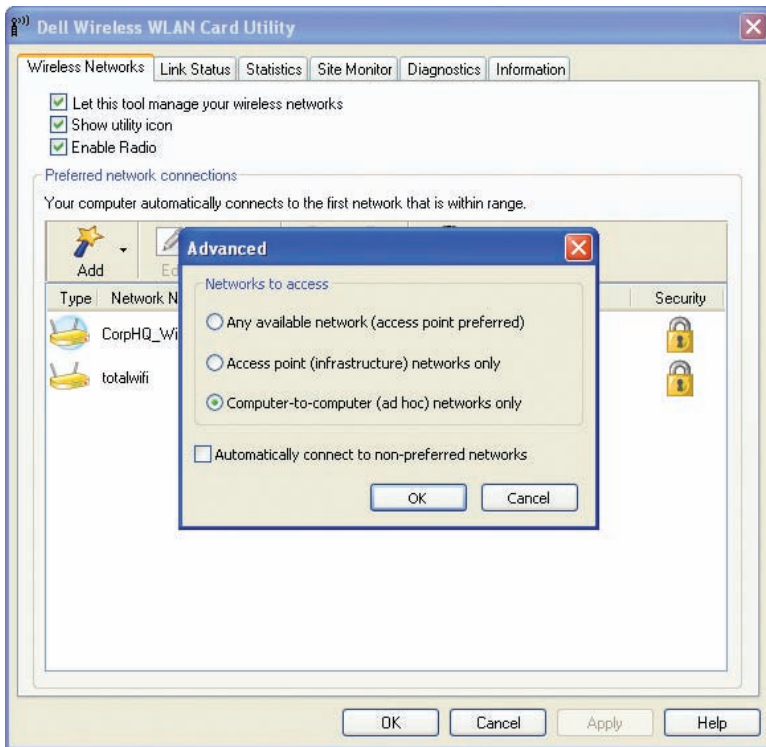
Try This!

Ad Hoc-ing

If you have access to a Wi-Fi-enabled device and a friend or classmate has one as well, try this! Set up your Wi-Fi for ad hoc using the configuration utility, and then try to connect with your partner. Use default settings. Once you connect with the defaults, you can start playing with your ad hoc network! Share a folder—such as Shared Pictures in Windows XP—and then copy the sample images from one machine to another. If you have one, throw a big file into the shared folder and try copying that one, too. Then do it again, but with variations of distance and channels. How far can you separate and still communicate? What happens if you change channels in the configuration utility, such as moving both devices from channel 6 to channel 4?

Setting Up an Infrastructure Network

Site survey in hand and Wi-Fi technology selected, you're ready to set up a wireless network in infrastructure mode. You need to determine the optimal location for your WAP, configure the WAP, and then configure any clients to access that WAP. Seems pretty straightforward, but the devil, they say, is in the details.



• **Figure 16.12** Selecting ad hoc mode in wireless configuration utility

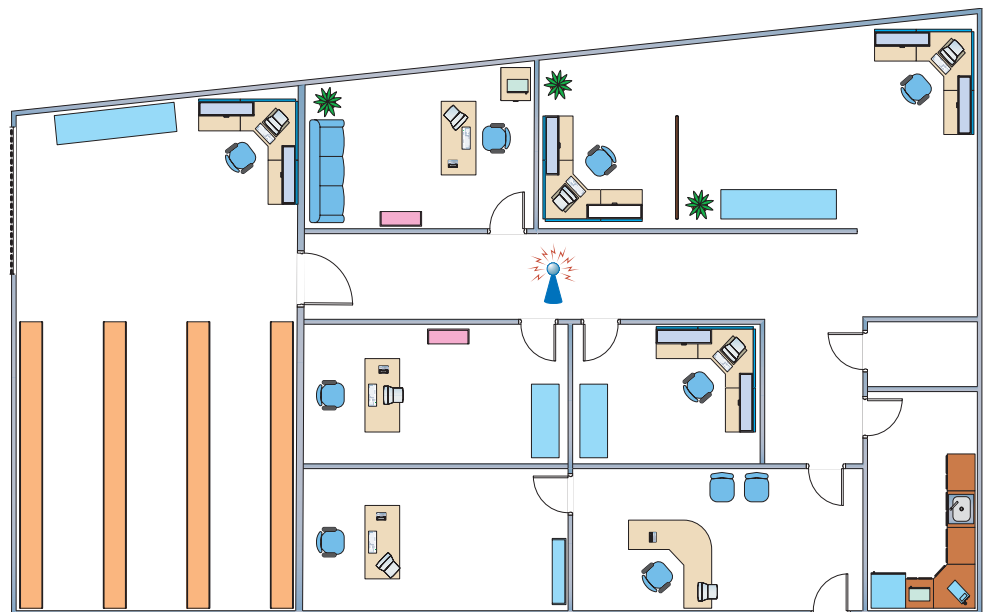
Placing Access Point

The optimal location for an access point depends on the area you want to cover and whether or not you care if the signal bleeds out beyond the borders. You also need to use antennae that provide enough signal and push that signal in the proper direction.

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 (Figure 16.13). 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 antennae that provide most omni-directional function are called **dipole antennae**.

The omni-directional and centered approach does not work for every network, for three reasons. First, if the signal exceeds the size of the network space, that signal

bleeds out. The signal can bleed out a lot in some cases, particularly if your specific space doesn't allow you to put the WAP in the center, but rather off-center. This presents a security risk, because someone outside your network



• **Figure 16.13** Room layout with WAP in the center

space could lurk, pick up the signal, and run software to try to hack into your network. Or, a hacker might use your wireless signal for purposes that you might not condone. Second, if your network space exceeds the signal of your WAP, you'll need to get some sort of signal booster (see "Gaining Gain," below). Third, any obstacles will produce glaring dead spots in network coverage. Too many dead spots make a less-than-ideal solution. To address these issues you might need to go to other solutions.

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 antennae that you can replace. To increase the signal in an omni-directional and centered setup, simply replace the factory antennae with one or more bigger antennae (Figure 16.14). Get a big enough antenna and you can crank it all the way up to 11!

Focusing the Wave When you don't necessarily want to broadcast to the world, you can use one or more directional antennae to create a nicely focused network. A **directional antenna**, as the name implies, focuses a radio wave into a beam of sorts. Directional antennae come in a variety of flavors, such as parabolic, dish, and Yagi, to name a just a few. A parabolic antenna looks like a satellite dish. A Yagi antenna (named for one of its Japanese inventors) is often called a beam antenna and can enable a focused radio wave to travel a long way, miles even.

Access Point Configuration

Wireless access points have a browser-based setup utility. Typically, you fire up the Web browser on one of your network client workstations and enter the access point'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 access point's documentation, to log in (Figure 16.15).



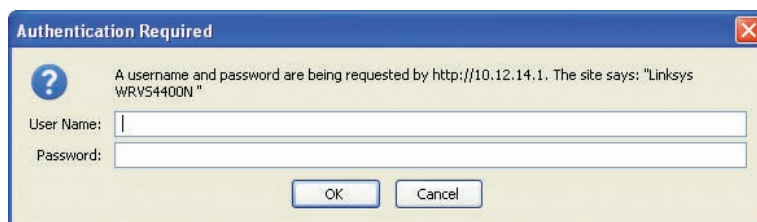
• Figure 16.14 Replacement antenna on WAP



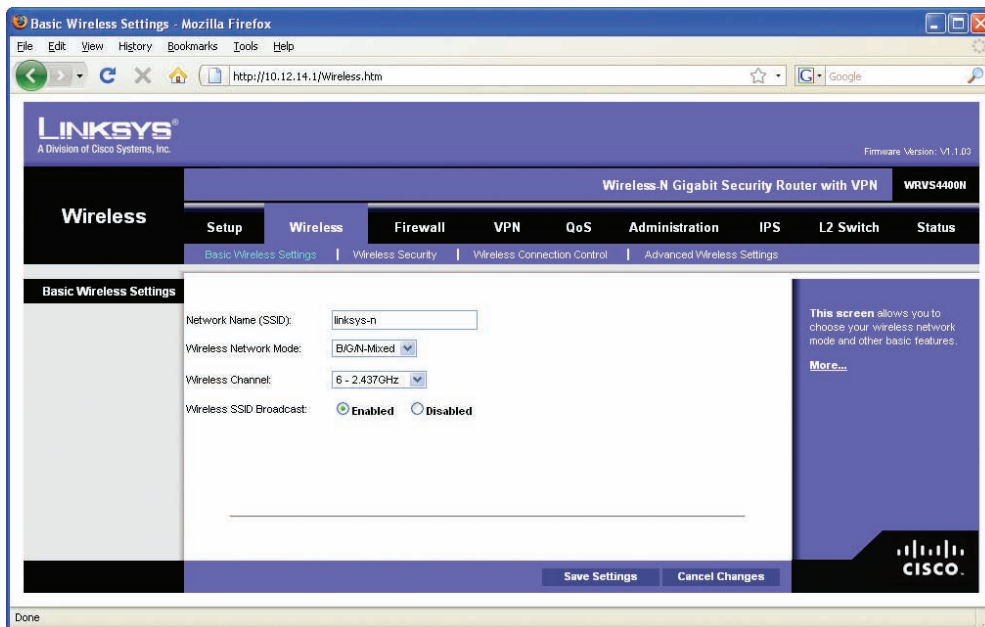
Tech Tip

Patch Antennae

Patch antennae are flat, plate-shaped antennae that generate a half-sphere beam. Patch antennas are always placed on walls. The half-sphere is perfect for indoor offices where you want to fill the room with a strong signal but not broadcast to the room behind the patch.



• Figure 16.15 Security login for Linksys WAP



• **Figure 16.16** Linksys WAP setup screen

Tech Tip

SSIDs and Overlapping Networks

One of the great benefits of SSIDs in the wild is the ability to configure multiple wireless networks in close proximity, even using the same frequency and channel, and still not conflict. For tight locations, such as dorm rooms, office complexes, and apartments, choose a unique SSID for each wireless network to avoid the potential for overlap problems.

Beacon Interval:	<input type="text" value="100"/>	(Default: 100 Msec, Range: 20 ~ 1000)
DTIM Interval:	<input type="text" value="1"/>	(Default: 1, Range: 1 ~ 255)
RTS Threshold:	<input type="text" value="2346"/>	(Default: 2346, Range: 256 ~ 2346)

• **Figure 16.17** Setting the beacon interval

Once you've logged in, you'll have configuration screens for changing your basic setup, access point password, security, and so on. Different access points offer different configuration options. Figure 16.16 shows the initial setup screen for a popular Linksys WAP/router.

Configuring the SSID (ESSID) and Beacon

The SSID option is usually located somewhere obvious on the configuration utility. On the Linksys model shown in Figure 16.16, it's on the Setup tab. Set your SSID to something unique.

You can choose not to broadcast the SSID, but this only stops casual users—sophisticated wireless intruders have tools to detect networks that do not broadcast their SSIDs.

Aside from the SSID (or ESSID in an extended network), broadcast traffic includes the *beacon*, essentially a timing packet sent from the WAP at regular intervals. The beacon packet enables Wi-Fi networks to function, so this is fairly important. Beacon traffic also makes up a major percentage of network traffic because most WAPs have beacons set to go off every 100 ms! You can adjust the rate of the beacon traffic down and improve your network traffic speeds, but you lower the speed at which devices can negotiate to get on the network, among other things. Figure 16.17 shows the Beacon Interval setting on a Linksys router.

Configuring MAC Address Filtering Increase security even further by using MAC address filtering. This builds a list of wireless network clients that are permitted or denied access to your wireless network based on their unique MAC addresses.

Figure 16.18 shows the MAC address filtering configuration screen on a Linksys WAP. Simply enter the MAC address of a wireless node that you want to allow (or deny) access to your wireless network.

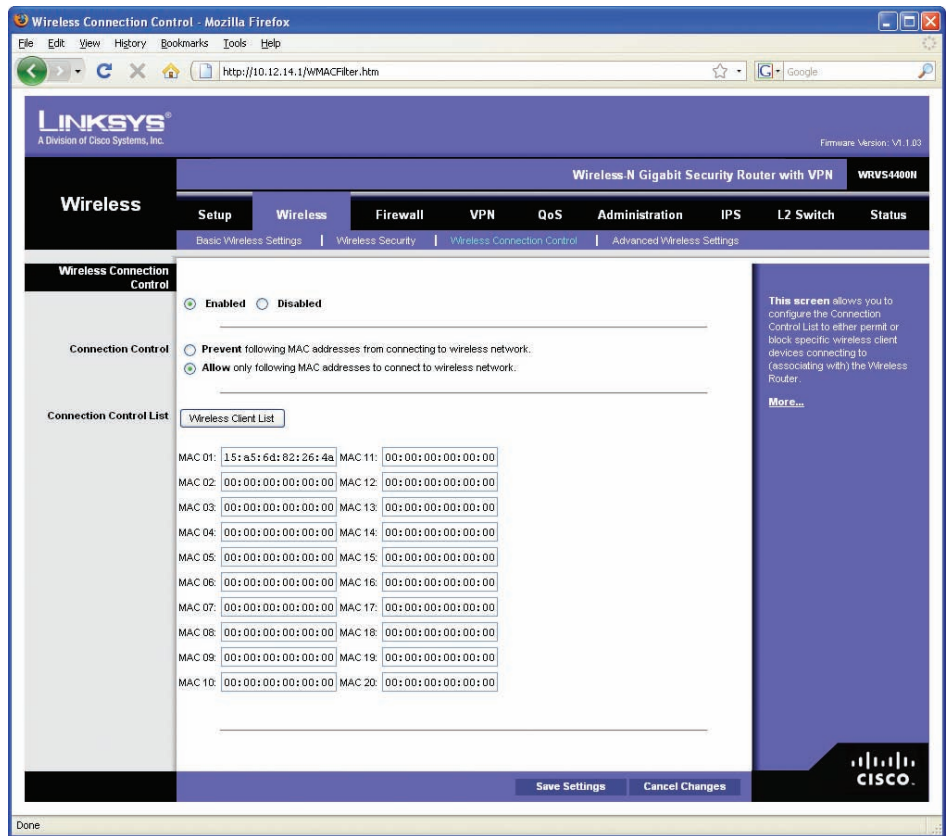
Configuring Encryption Enabling encryption ensures that data packets are secured against unauthorized access. To set up encryption, you turn on encryption at the WAP and generate a unique security key. Then you configure all connected wireless nodes on the network with the same key information. Figure 16.19 shows the WEP key configuration dialog box for a Linksys WAP.

You have the option of automatically generating a set of encryption keys or doing it manually. You can save yourself a certain

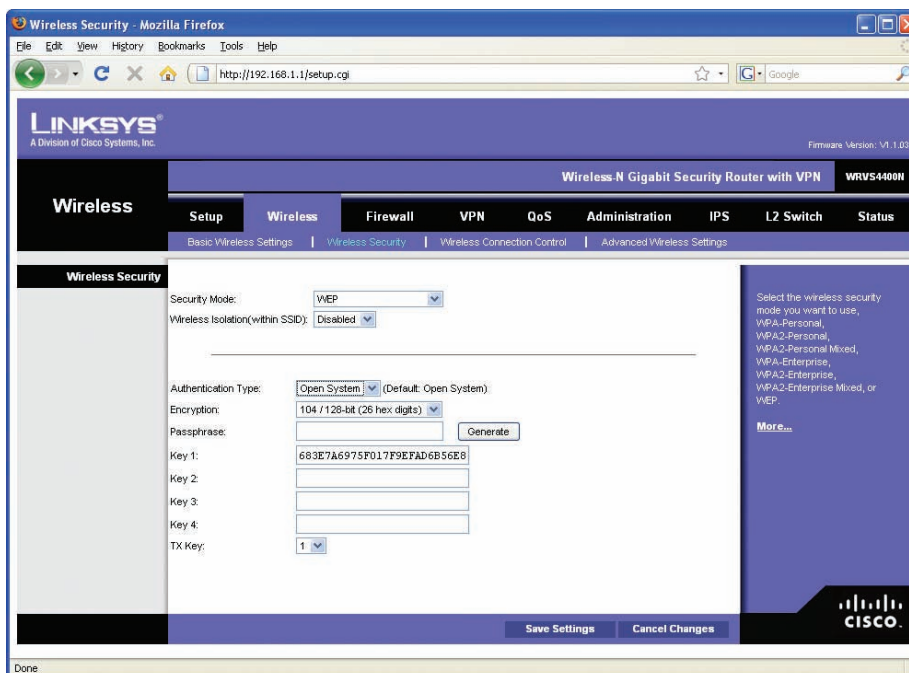
amount of effort by using the automatic method. Select an encryption level—the usual choices are either 64-bit or 128-bit—and then enter a unique *passphrase* and click the Generate button (or whatever the equivalent button is called in your WAP's software). Then select a default key and save the settings.

The encryption level, key, and passphrase must match on the wireless client node or communication fails. Many access points have the capability to export the encryption key data onto removable media for easy importing onto a client workstation, or you can configure encryption manually using the vendor-supplied configuration utility, as shown in Figure 16.20.

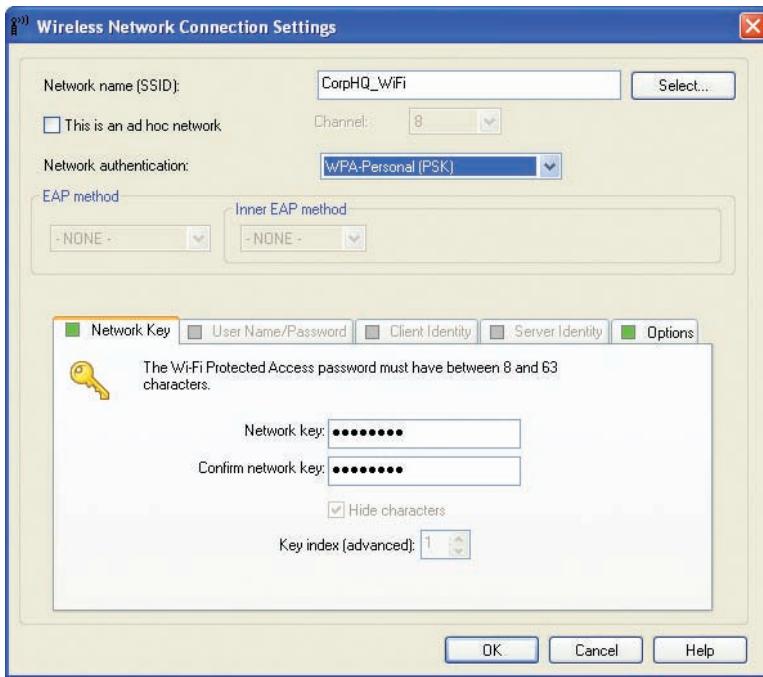
WPA encryption, if supported by your wireless equipment, is configured in



• Figure 16.18 MAC address filtering configuration screen for a Linksys WAP



• Figure 16.19 Encryption key configuration screen on Linksys WAP



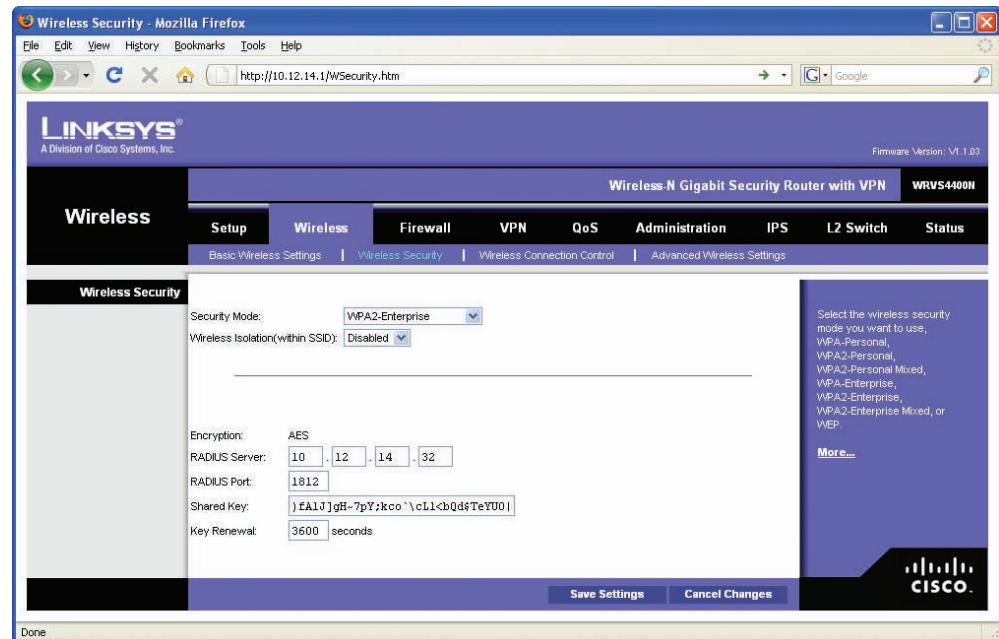
• **Figure 16.20** Encryption screen on client wireless network adapter configuration utility

much the same way. You may be required to input a valid user name and password to configure encryption using WPA.

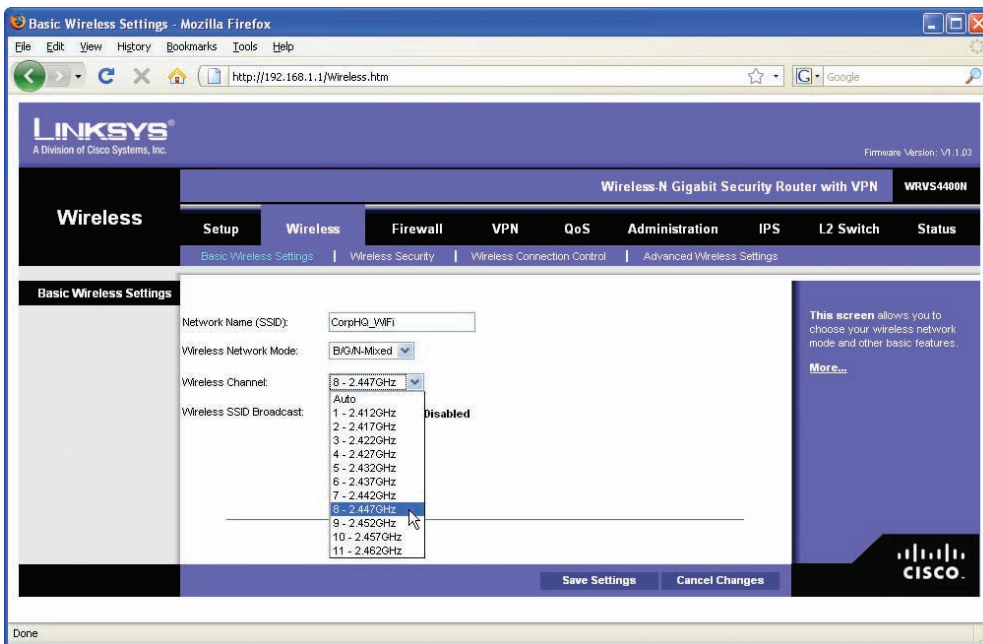
If you have the option, choose WPA2 encryption for both the WAP and the NICs in your network. You configure WPA2 the same way you would WPA. Note that the settings such as WPA2 for the Enterprise assume you'll enable authentication using a RADIUS server (Figure 16.21). Use the best encryption you can. If you have WPA2, use it. If not, use WPA. WEP is always a last choice.

Configure Channel and Frequency 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 16.22 shows the channel option in a Linksys WAP.

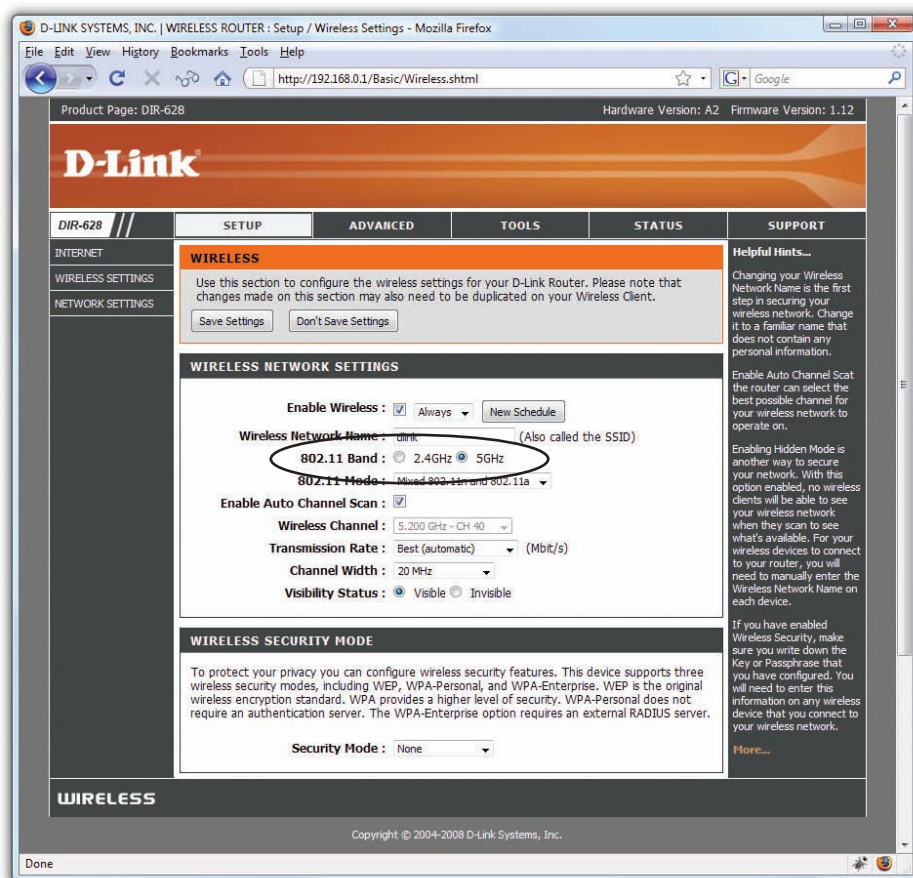
With dual-band 802.11n WAPs, you can choose which band to put 802.11n traffic on, either 2.4 GHz or 5 GHz. In an area with overlapping signals, most of the traffic will be on the 2.4-GHz frequency, because most devices are either 802.11b or 802.11g. You can avoid any kind of conflict with your 802.11n devices by using the 5-GHz frequency instead. Figure 16.23 shows the configuration screen for a dual-band 802.11n WAP.



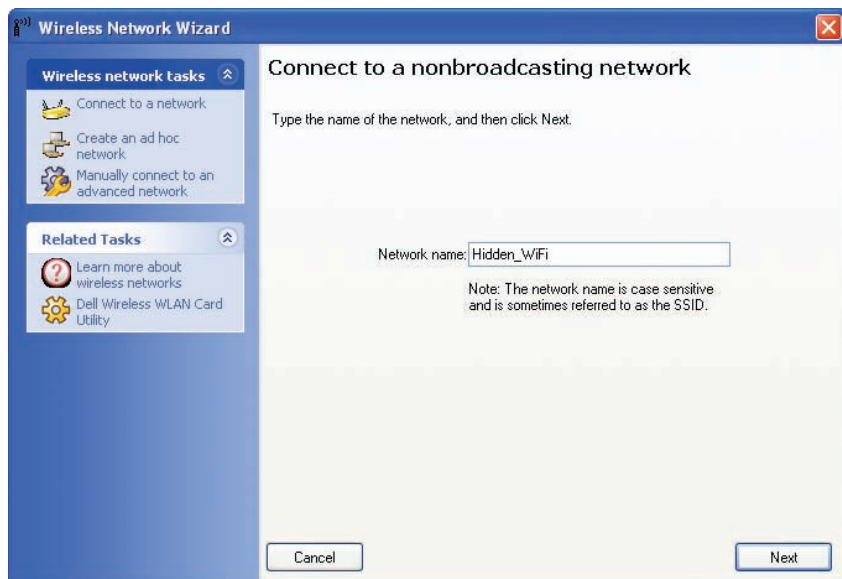
• **Figure 16.21** Encryption screen with RADIUS option



• Figure 16.22 Changing the channel



• Figure 16.23 Selecting frequency



• **Figure 16.24** Typing in an SSID manually



Some manufacturers market special Wi-Fi extenders or repeaters that pick up the Wi-Fi signal wirelessly and repeat it into a wider space.



• **Figure 16.25** Linksys wireless bridge device

Configuring the Client

As with ad hoc mode wireless networks, infrastructure mode networks require that the same SSID be configured on all nodes and access points. Normally, the client would pick up a broadcast SSID and all you need to do is type in the security passphrase or encryption key. With nonbroadcasting networks, on the other hand, you need to type in a valid SSID as well as the security information (Figure 16.24).

Extending the Network

Creating a Basic Service Set network with a single WAP and multiple clients works in a relatively small area, but you can extend a Wi-Fi network in a couple of ways if you have difficult spaces—with lots of obstructions, for

example—or a need to communicate beyond the ~300-foot range of the typical wireless network. Most commonly, you'd add one or more WAPs to create an Extended Service Set. You can also install a wireless bridge to connect two or more segments.

Adding a WAP

To add a WAP to a Wi-Fi network generally means to run a UTP cable from the new WAP to the main WAP. So they connect with wires. Configuration is pretty straightforward. Both WAPs require the same ESSID and channel, though the frequency can vary if the two are 802.11n WAPs.

Wireless Bridge

Dedicated **wireless bridges** are used to connect two wireless network segments together, or to join wireless and wired networks together in the same way that wired bridge devices do. You can also use wireless bridges to join wireless networks with other networked devices, such as printers.

Wireless bridges come in two different flavors: point-to-point and point-to-multipoint. **Point-to-point** bridges can only communicate with a single other bridge, and are used to connect two wireless network segments. **Point-to-multipoint** bridges can talk to more than one other bridge at a time, and are used to connect multiple network segments. Some vendors also offer repeating bridges, and bridges with access point and router functions. Figure 16.25 shows a wireless bridge.

Verify the Installation

Once you've completed the initial installation of a Wi-Fi network, check it. Move some traffic from one computer to another using the wireless connection. Never leave a job site without verifying the installation.

■ 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.

So, who's affected? If all machines on your network—wired and wireless—have lost connectivity, you have bigger problems than the wireless machines being unable to 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, then 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, then 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 CompTIA A+ certified technician in you.

Open Windows Device Manager and check to see if there's an error or conflict with the wireless adapter. If you see a big yellow exclamation point or a red X next to the device, you have either a driver error or a resource conflict. Reinstall the device driver or manually reset the IRQ resources as needed.



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!

If you don't see the device listed at all, it's possible that the device is not seated properly in its PCI slot, or not plugged all the way into its PC Card or USB slot. These problems are easy to fix. One thing to consider if you're using an older laptop and PC Card combination is that the wireless adapter may be a CardBus type of PC Card device. CardBus cards will not snap into a non-CardBus slot, even though both new and old cards are the same size. If your laptop is older than about five years, it may not support CardBus, meaning you need to get a different PC Card device. Or, if you've been looking for a reason to get a new laptop, now you have one!

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 (like 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 that shows the strength of your wireless signal. Figure 16.26 shows Windows XP Professional's



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.

built-in wireless configuration utility—called Wireless Zero Configuration (or just Zeroconf)—displaying the link state and signal strength.

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, 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 objects, you can try small adjustments to your antennae to see if the signal improves. You can swap out the standard antenna for one or more higher-gain antennae. 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.

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 that 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. Most wireless devices enable you to 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 floppy disk or other removable media. It's then a simple matter to import the encryption key onto the PC 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.



• **Figure 16.26** Windows XP Professional's wireless configuration utility



Tech Tip

Windows XP and Zeroconf

One trick that works for wireless networks that seem a bit flaky with a Windows XP client is to disable the Wireless Zero Configuration service on the client. To do this, simply open the Services applet in Administrative Tools and change the Startup Type option from Automatic to Disabled. Document your change, of course, so you'll remember to turn Zeroconf back on in case it doesn't provide the fix you want.



Try This!

Breaking Wi-Fi

You've read about it. Now it's time to see the movie (or at least the next best thing)! If you have a functional Wi-Fi network set up in infrastructure mode, try breaking it. What happens when you change channels? What if you stop broadcasting the SSID? Be creative here! The goal is to experience typical problems and to understand the specific causes.

Chapter 16 Review

■ Chapter Summary

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

Explain wireless networking standards

- Wireless networks operate much like their wired counterparts, but they eliminate network cabling by using radio waves as a network medium.
- The most common wireless networking standard is IEEE 802.11, also known as Wi-Fi. 802.11 includes extended standards such as 802.11a, 802.11b, 802.11g, and 802.11n.
- Computers that lack a built-in wireless Ethernet NIC can use a PCI expansion card, PC Card, or USB NIC. The benefit of a USB wireless NIC is the ability to use an extender cable, allowing the USB NIC to be placed in the optimum location for signal strength.
- Wireless NICs normally require configuration software supplied by the manufacturer. Microsoft Windows XP systems have wireless NIC configuration software built in.
- A wireless network can operate in one of two modes: ad hoc or infrastructure.
- Ad hoc mode, also known as peer-to-peer, creates an Independent Basic Service Set (IBSS).
- Infrastructure mode is more commonly used than ad hoc mode and allows wireless networks to connect to wired networks. A single wireless access point connecting computers in infrastructure mode is called a Basic Service Set (BSS). If multiple WAPs are used, an Extended Basic Service Set (EBSS) is created, though most techs simply refer to it as an Extended Service Set (ESS).
- Wireless networking speeds range from 2 Mbps to a theoretical limit of 300 Mbps. The speed is affected by the distance between wireless nodes, interference from other wireless devices such as cordless phones or baby monitors, and solid objects such as metal plumbing or air conditioning units.
- Wireless networking ranges are affected by environmental factors, interference from other wireless devices, and solid objects.
- The Basic Service Set Identifier (BSSID) identifies a network so that packets are delivered to the correct computer on the correct network.
- The Service Set Identifier (SSID) configuration parameter enables you to set a basic level of access security. Properly configured SSIDs, or network names, exclude any wireless network device that does not share the same SSID.
- A Wi-Fi network with multiple WAPs applies the SSID to the ESS, creating an Extended Service Set Identifier (ESSID).
- The original 802.11 standards use the 2.4-GHz frequency while later standards use either 2.4-GHz or 5.0-GHz frequencies. These frequencies allow the wireless networks to operate with less chance of interference from other wireless devices that are not part of the network.
- Spread-spectrum radio waves distribute data in small chunks over different frequencies to reduce interference from other wireless devices not part of the network. 802.11 networks use the direct-sequence spread spectrum (DSSS) implementation.
- Wi-Fi channels use a portion of the available frequency spectrum to further tune out potential interference. Most devices are preset to use channel 6.
- Wi-Fi networks use carrier sense media access/collision avoidance (CSMA/CA) to send packets. CSMA/CA is proactive in that it attempts to avoid collisions before they happen rather than simply detecting them when they occur.
- Currently, only the Distributed Coordination Function (DCF) method of CSMA/CA is implemented. DCF uses IFS wait periods, backoff periods, and acknowledgements (ACK) to avoid collisions.

- 802.11b supports data throughput up to 11 Mbps over 300 feet on the 2.4-GHz frequency.
- 802.11a, which was released after 802.11b, supports data throughput up to 54 Mbps over 150 feet on the 5.0-GHz frequency.
- 802.11g supports data throughput up to 54 Mbps over 300 feet on the 2.4-GHz frequency. 802.11g is also backward compatible with 802.11b.
- 802.11n supports data throughput up to 600 Mbps theoretically over 300 feet on the 2.4-GHz frequency. 802.11n requires MIMO and transmit beaming to achieve its greater data throughput. It is also backward compatible with 802.11b and 802.11g.
- 802.16, WiMax, is expected to support ranges up to 30 miles.
- Wireless networks may be secured with MAC address filtering, though this method can be easily hacked by spoofing.
- A RADIUS server allows remote users to connect to a network with a user name and password, providing better security than MAC address filtering. A supplicant contacts a NAS, which in turn contacts the RADIUS server.
- Data should be encrypted when being transferred across a wireless network. WEP offers very little protection because it is easily hacked. WPA is better because it uses the Temporal Key Integrity Protocol (TKIP). WPA2, which uses the Advanced Encryption Standard (AES), is the strongest of the three.
- Better WAPs and switches can use Power over Ethernet (PoE) to provide electrical power to the WAP via the Ethernet cable that connects it with the switch. Both WAP and switch must have this capability built in for it to work.

Describe the process for implementing Wi-Fi networks

- The first step in creating a wireless network is to create a site survey, which identifies other wireless networks or objects that may cause interference.
- Wireless networking hardware must be installed in all the clients. Most laptops have wireless NICs

built in, but a PC Card can be used as an alternative. Desktop computers may use a PCI expansion card. Any computer with a USB port can use a USB wireless NIC.

- Configuring a NIC for ad hoc networking requires the SSID, IP address, channel, and sharing to be configured.
- Configuring a NIC for infrastructure networking requires planning the optimal placement of the WAP. A replacement antenna can strengthen the wireless signal and extend the range. The WAP also needs to be configured with the proper settings for the SSID, security, and encryption options.
- A wireless network's range can be extended by adding multiple WAPs. The additional WAPs typically connect to each other via a hard cable.
- A wireless bridge connects two wireless segments together. A point-to-point bridge can only communicate with a single other bridge while a point-to-multipoint bridge can communicate with more than one other bridge at the same time.

Describe troubleshooting techniques for 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. Configuration settings on both the WAP and wireless NIC should be checked.

■ Key Terms

802.1X (437)
802.11 (427)
802.11a (435)
802.11b (435)
802.11g (435)
802.11i (439)
802.11n (435)
802.16 (436)
ad hoc mode (430)
Advanced Encryption Standard (AES) (439)
Basic Service Set (BSS) (431)
Basic Service Set Identifier (BSSID) (432)
carrier sense multiple access/collision avoidance (CSMA/CA) (434)
channel (433)
dipole antennae (442)
direct-sequence spread-spectrum (DSSS) (433)
directional antenna (443)
Distributed Coordination Function (DCF) (434)
encryption (438)
Extended Service Set (ESS) (431)
Extended Service Set Identifier (ESSID) (433)
Extensible Authentication Protocol (EAP) (437)
frequency-hopping spread-spectrum (FHSS) (433)
gain (443)
Independent Basic Service Set (IBSS) (430)
infrastructure mode (431)
interframe space (IFS) (434)
link state (429)
MAC address filtering (436)
multiple in/multiple out (MIMO) (435)
Network Access Server (NAS) (437)
Network Name (433)
orthogonal frequency-division multiplexing (OFDM) (433)
peer-to-peer mode (430)
Point Coordination Function (PCF) (434)
point-to-multipoint (448)
point-to-point (448)
Power over Ethernet (PoE) (439)
RADIUS server (437)
Service Set Identifier (SSID) (433)
signal strength (429)
site survey (440)
supplicant (437)
Temporal Key Integrity Protocol (TKIP) (439)
transmit beamforming (436)
Wi-Fi Protected Access (WPA) (439)
Wi-Fi Protected Access 2 (WPA2) (439)
WiMax (436)
wireless access point (WAP) (429)
wireless bridge (448)
Wired Equivalent Privacy (WEP) (438)
Wi-Fi (427)
wireless network (427)

■ Key Term Quiz

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

1. When a network uses the 802.11 standard, it is said to be a(n) _____.
2. Establishing a unique _____ or network name helps ensure that only wireless network devices configured similarly are permitted access to the network.
3. To connect wireless network segments together, you should use a(n) _____.
4. _____ wireless bridges are used to connect only two wireless network segments together, because they can only communicate with a single other bridge.
5. _____ wireless bridges are used to connect multiple network segments together, because they can talk to more than one other bridge at a time.
6. Of the two wireless encryption protocols, _____ is less secure.

7. Of the two different spread-spectrum broadcasting methods, _____ sends data out on different frequencies at the same time, and therefore uses considerably more bandwidth.
8. WPA uses _____ to encrypt data while WPA2 uses the more secure _____.
9. _____ allows 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. What was the first wireless standard?
 - A. 802.11b
 - B. 802.11a
 - C. 802.11g
 - D. 802.11
2. What are currently the most popular wireless standards? (Select two.)
 - A. 802.11a
 - B. 802.11b
 - C. 802.11g
 - D. 802.11i
3. Where would wireless access points likely be found? (Select three.)
 - A. Airport
 - B. Café
 - C. Historic buildings
 - D. Secure facilities
4. Which of the following statements about SSIDs are true? (Select three.)
 - A. All wireless networks use them.
 - B. Only one wireless device uses them.
 - C. They should be unique to your wireless LAN.
 - D. They are broadcast by default by most wireless network devices.
5. What is the best way to connect multiple wireless segments together?
 - A. Use an 802.11g network adapter.
 - B. Use an 802.11i network adapter.
 - C. Use a point-to-multipoint wireless bridge.
 - D. Use a point-to-point wireless bridge.
6. What should you use when you want to limit access to your wireless network based on the physical, hard-coded address of each wireless network device?
 - A. Bus scheduling
 - B. Encoding
 - C. Encryption
 - D. MAC address filtering
7. What process secures a wireless network by protecting data packets being transmitted?
 - A. Data packeting
 - B. Pulse encoding
 - C. Data encryption
 - D. MAC broadcasting
8. What are the two 802.11 standards that define data collision avoidance?
 - A. ACF
 - B. DCF
 - C. ECF
 - D. PCF
9. What is the predefined silence period between data transmissions called?
 - A. IEEE
 - B. IFS
 - C. ISM
 - D. IPX

10. What is the reactive method used for avoiding collisions on Ethernet networks?
 - A. CSMA/CA
 - B. CSMA/CD
 - C. CSMA/WEP
 - D. CSMA/WPA
11. Which of the following networking standards operates at a frequency of 5 GHz?
 - A. 802.11a
 - B. 802.11b
 - C. 802.11g
 - D. 802.11i
12. Which of the following is the wireless network encryption method that is most secure?
 - A. MAC address filtering
 - B. WEP
 - C. WPA
 - D. WPA2
13. Which of the following is known as a Basic Service Set in infrastructure mode?
 - A. A WAP
 - B. A WPA
 - C. A RADIUS server
 - D. A TKIP
14. In an attempt to maximize your wireless throughput while minimizing interference on your brand new 802.11b/g WAP, which setting should you change?
 - A. Change the WAP setting to not broadcast the SSID.
 - B. Change the channel to 6.
 - C. Change the channel to anything other than 6.
 - D. Change the frequency to 5.0 GHz.
15. What is true about the 802.16 standard?
 - A. It supports about the same speed as 802.11b, but has a range of up to 30 miles.
 - B. It supports a speed of about 600 Mbps at a range of about 300 feet.
 - C. It supports a speed of about 600 Mbps at a range of up to 30 miles.
 - D. There is no such thing as 802.16.

■ 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 as if it were printed on company stationary (or “letterhead”).
4. Write a few paragraphs describing the pros and cons of both wired and wireless networks. Specifically, compare 100BaseT to the 802.11b standard. Then conclude with a statement of your own personal preference.

Lab Projects

• Lab Project 16.1

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-class 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 10-Mbps hub 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 local stores' prices and equipment. 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				
Wireless NICs, PC Card				
Wireless Access Point				
Other				
TOTALS				

• Lab Project 16.2

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 802.11b and 802.11g wireless network standards. Create a brief, yet 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.