

Wireless Networking

The Network+ Certification exam expects you to know how to

- 1.6 Identify the purposes, features, and functions of wireless access points
- 1.7 Specify the general characteristics (for example: carrier speed, frequency, transmission type, and topology) of the following wireless technologies: 802.11 (frequency-hopping spread spectrum), 802.11x (direct-sequence spread spectrum), infrared, Bluetooth
- 1.8 Identify factors that affect the range and speed of wireless service (for example: interference, antenna type, and environmental factors).
- 2.17 Identify the following security protocols and describe their purpose and function: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), 802.1x

To achieve these goals, you must be able to

- Explain wireless networking hardware and software requirements, and configure wireless networking hardware
- Define wireless networking IEEE standards and FCC operation frequencies
- Define wireless network operation modes, limits, and methods
- Configure wireless networking security
- Describe troubleshooting techniques for wireless networks

Historical/Conceptual

In the last couple of chapters, we've had detailed discussions of the most common network implementations on the market. Even though Ethernet, Token Ring, ARCnet, LocalTalk, FDDI, and ATM networks all use wildly different hardware and protocols, one thing ties all these technologies together—the wires! Every type of network we've talked about thus far assumes that your PCs are tethered 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.

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 those of us 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.



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

Wireless networks operate at the same OSI layers and use the same protocols as wired networks. The difference lies in 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 two technologies: those based on the most common implementation of the IEEE 802.11 wireless Ethernet standard—namely *Wireless Fidelity (Wi-Fi)* and *Home Radio Frequency (HomeRF)*—and those based on *Bluetooth*, a newer wireless technology that enables PCs to communicate wirelessly with each other, as well as with a wide variety of peripheral gadgets and consumer electronics.



TIP The CompTIA Network+ exam focuses on Wi-Fi wireless networking, but I'm including HomeRF and Bluetooth because you're likely to see these wireless networking technologies in the field.

I'll start off the chapter with some wireless networking basics, and then discuss the accepted wireless networking standards. I'll also talk about how to configure wireless networking, and finish with a discussion of troubleshooting wireless networks. Let's get started!

Test Specific

Wireless Networking Basics

In this section, I'll talk about the basic things you need to know to get off the ground with wireless networking. I'll start with the hardware and software you need, and then talk about modes of wireless network operation, wireless security technologies, and wireless specifications, such as speed, range, and broadcast frequencies. Last, I'll discuss wireless network media access—that is, how wireless devices avoid stepping on each other's data packets.

Wireless Networking Hardware

Wireless networking hardware serves the same function as hardware used on wired PCs. Wireless Ethernet NICs and Bluetooth adapters 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 are transmitting and receiving radio waves.

Wireless networking capabilities of one form or another are built into many modern computing devices. Wireless Ethernet and Bluetooth 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 9-1 shows a wireless PCI Ethernet card.

You can also add wireless network capabilities using external USB wireless network adapters, as shown in Figure 9-2. 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.

Wireless network adapters aren't limited to PCs. Many networked printers use wireless NICs or Bluetooth adapters. Most handheld computers and *Personal Digital Assistants* (PDAs) also have wireless capabilities built in or available as add-on options. Figure 9-3 shows an older Handspring PDA accessing the Internet through a wireless network adapter card.

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, or connecting multiple wireless network segments together—you need additional equipment. This typically means wireless access points and wireless bridges.

A *wireless access point* connects wireless network nodes to wireless or wired networks. A basic WAP operates like a hub and works at OSI Layer 1. However, many wireless ac-

Figure 9-1
Wireless PCI NIC

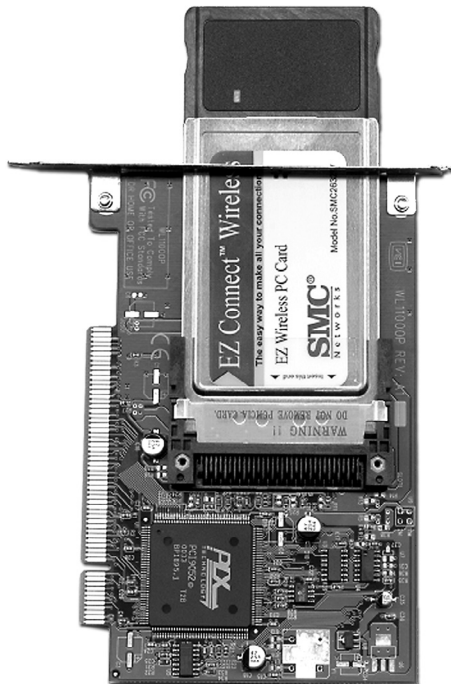




Figure 9-2 External USB wireless NIC

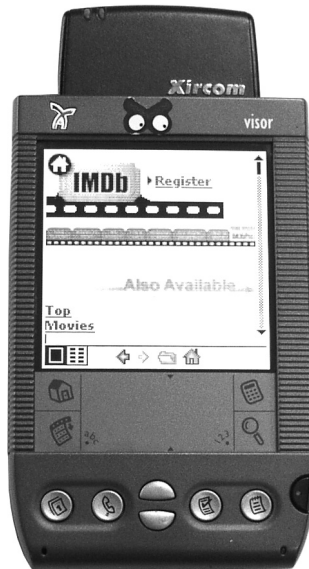


Figure 9-3 PDA with wireless capability

cess points are combination devices that act as high-speed hubs, switches, bridges, and routers, all rolled into one and working at many different OSI layers. The Linksys device shown in Figure 9-4 is an example of this type of combo device.



NOTE 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 9-4

Linksys device
that acts as
wireless access
point, switch, and
DSL router



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 9-5 shows a wireless bridge.

Wireless Bluetooth hardware is included as built-in equipment in many newer PCs, laptops, PDAs, and cell phones. When installed on a PC, Bluetooth add-on components almost always use the USB expansion bus, instead of an internally installed PCI card. Some devices use the PC Card bus, or even a Compact Flash socket. Bluetooth access points, hubs, and bridges are slowly making their way to the PC market, but haven't caught on as quickly as wireless Ethernet devices. Figure 9-6 shows a Bluetooth adapter plugged into a laptop USB port.

Figure 9-5

Linksys wireless
bridge device



Figure 9-6
External USB
Bluetooth
adapter



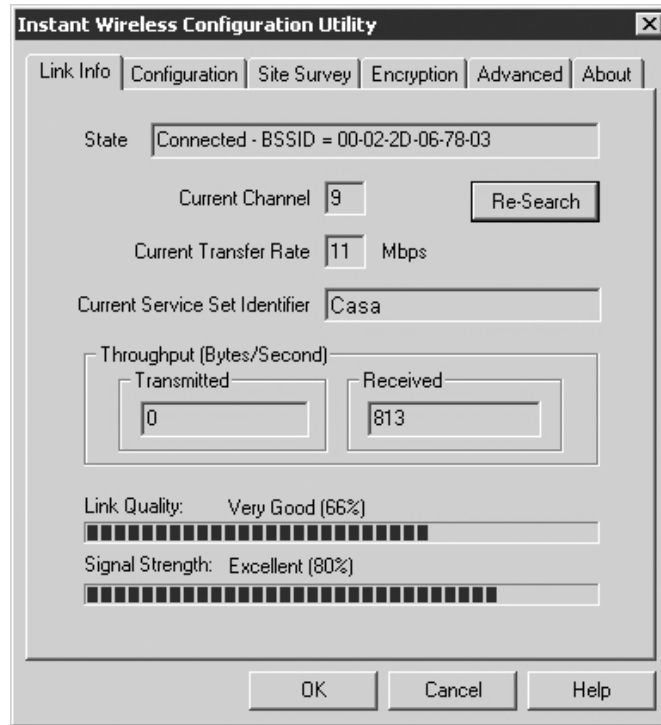
Wireless Networking Software

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. Windows XP Professional comes well equipped for wireless networking and has built-in drivers for many popular wireless NICs. Even so, it's always a better idea to use the drivers and configuration utilities that the vendor has supplied with your wireless adapter.

In addition to the driver, you also need a utility for configuring how the wireless hardware connects to other wireless devices. Windows XP has 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 9-7 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.

Wireless access points and routers are configured through browser-based setup utilities. Wireless bridges usually need a vendor-supplied configuration utility to get them to talk to your wireless network initially, and then are set up using the browser-based tool. I'll talk about configuring adapters and access points in the section called "SSID." Now let's look at the different modes wireless networks use.

Figure 9-7
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.

Ad-hoc Mode

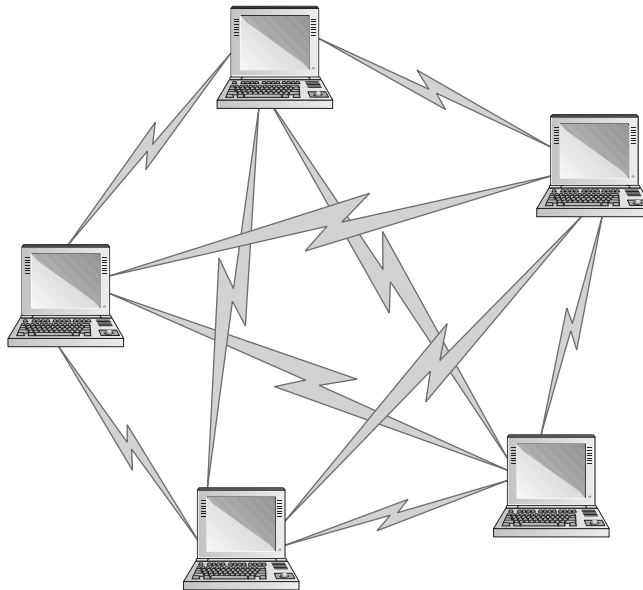
Ad-hoc mode is sometimes called peer-to-peer mode, with each wireless node in direct contact with each other node in a decentralized free-for-all, as shown in Figure 9-8. Ad-hoc mode is similar to the *mesh* topology discussed in Chapter 4, “Hardware Concepts.”

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 are suited for small groups of computers (fewer 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.

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.

Figure 9-8
Wireless ad-hoc
mode network



NOTE 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.

Infrastructure Mode

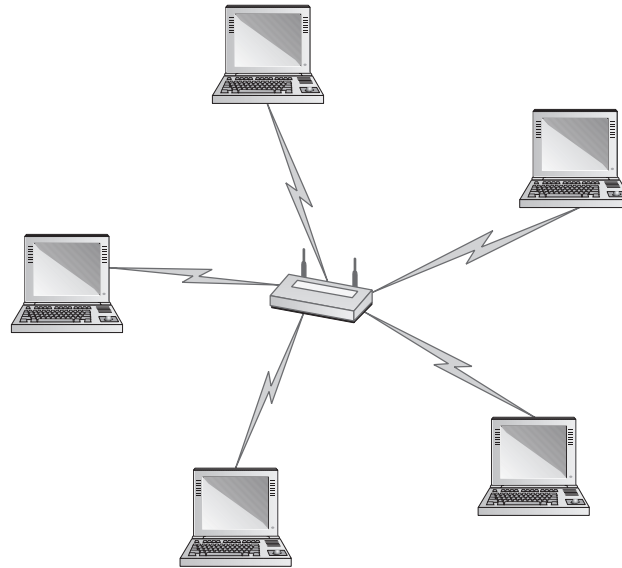
Wireless networks running in *infrastructure mode* use one or more wireless access points to connect the wireless network nodes centrally, as shown in Figure 9-9. This configuration is similar to the *star* topology of a wired network. You also use infrastructure mode to connect wireless network segments to wired segments. If you plan on setting 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 wireless access point 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 Basic Service Set (EBSS)*.

A lot of techs have begun dropping the word “basic” from the Extended Basic Service Set. Accordingly, you’ll see the initials for the Extended Service Set as ESS. Similarly to the Token Ring issue of MAUs and MSAUs, either EBSS or ESS is correct.

Wireless networks running in infrastructure mode require a little more planning—such as where you place the wireless access points 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 like Internet connections and centralized databases.

Figure 9-9
Wireless
infrastructure
mode network



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 are floating through the air instead of safely 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 four methods: Service Set Identification (SSID), MAC address filtering, port-based access control, and data encryption. The first three methods secure access to the network itself, and the fourth secures the data that's moving around the network. All of these methods require you to configure the wireless networking device. Let's take a look.

SSID

The *Service Set Identification (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 wireless access point. When properly configured, only wireless clients whose SSID matches that of the wireless access point are able to gain access to the wireless network. Data packets that lack the correct SSID in the header are rejected. The SSID, therefore, provides the most basic unit of wireless security.

Unfortunately, this isn't the way wireless access points come out of the box. By default, they're given a generic SSID that's widely publicized in the vendor's literature and online. For example, the default SSID for Linksys wireless access points is "linksys,"

3COM uses “101,” and Netgear uses “wireless” (although they’re migrating to “netgear”). Just in case you think I only know this because I have some sort of secret industry insider information, keep in mind that I found these SSID names with a two-minute search on Google. It’s that easy! To make matters worse, right out of the box, all wireless access points are configured to broadcast this SSID to make it easier for clients to join in on the wireless fun!

Generally speaking, if you want a secure network, you don’t go around yelling the network name to everyone within earshot, so configuring a unique SSID name should be one of the first things you do to secure a wireless network. You should also change the default login names and passwords, and possibly turn off the name-broadcast option. Finally, make sure that you configure all of your clients with the new unique SSID name. I’ll walk through the steps for doing this in the “Configuring Wireless Networking” section of this chapter.



TIP Most wireless access points broadcast their SSIDs by default, creating a security hole that Andre the Giant (may he rest in peace) could walk through. Detecting the SSID of a wireless network is the hacker’s first step for using the network without permission. Closing that security hole should be *your* first step to making your wireless network secure.

MAC Address Filtering

Most wireless access points support *MAC address filtering*, a method that enables you to limit access to your wireless network based on the physical, hard-wired addresses of the wireless network adapters you support. MAC address filtering is a handy way of creating a type of “accepted users” list to limit access to your wireless network. A table stored in the wireless access point 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 wireless access points 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 wireless access point 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 well, a seriously determined hacker can “spoof” a MAC address and access the network. Then again, if you have data so important that someone would go to this extreme, 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 wireless access point with the new NIC’s MAC address.

Encryption

The next step in securing a wireless network is encrypting the data packets that are floating around. With *encryption*, data packets are electronically scrambled and “locked” with a private encryption “key” before being transmitted onto the wireless network. The re-

ceiving network device has to possess the encryption key to unscramble the packet and process the data. Thus, any data packets surreptitiously grabbed out of the air are useless to the grabber unless they've got the encryption key. Enabling wireless encryption through either Wireless Equivalency Privacy (WEP) or Wi-Fi Protected Access (WPA) provides a good level of security to data packets in transit.

Data Encryption Using WEP Standard *Wireless Equivalency Privacy (WEP)* encryption uses a 64-bit encryption algorithm to scramble data packets, but most vendors now enable stronger 128-bit algorithms. If you have this option and are in a high-risk situation, you should always use the strongest encryption available for your wireless network devices.

Even with the strongest encryption enabled, WEP isn't considered to be a particularly robust security solution. Consider, for instance, that WEP doesn't provide complete encryption for data packets. That is, WEP 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 their MAC address, and no other credentials are offered or required. With the right equipment, MAC addresses are fairly easy to "sniff" out and duplicate, thus opening up a possible "spoofing" attack. If you want true, end-to-end data encryption with authentication, you need to use WPA.

Data Encryption Using WPA *Wi-Fi Protected Access (WPA)* addresses the weaknesses of WEP, and acts as a sort of 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), an encryption key integrity-checking feature, user authentication through the industry-standard *Extensible Authentication Protocol (EAP)*, and other advanced features that WEP lacks.

The downside is that WPA isn't available on all wireless networking devices. Even on those that do include it (or for which it's available as an upgrade option), WPA can be difficult to configure, requiring firmware updates for all access points, network adapters, and client software. Keep in mind also that WPA is intended only as a temporary security solution until the new IEEE 802.11i security standard is ratified.



NOTE WPA addresses the known weaknesses in the WEP encryption protocol, but it is not widely implemented.

Port Based Access Control: 802.1x

One other wireless security tool worth mentioning here is 802.1x. This security measure (which is all about authentication, rather than encryption) is meant to control access to a wireless LAN. The 802.1x authentication standard uses various flavors of EAP, the same authentication protocol that WPA uses; these include EAP over LAN (EAPOL), Protected EAP (PEAP), and EAP-Transport Level Security (EAP-TLS).

Basically, 802.1x uses the wireless access point as a kind of gatekeeper, keeping users out of the LAN until they have the approval of the network's 802.1x *authentication server*, typically a RADIUS server. When an 802.1x-enabled system tries to access the network, the client software (referred to in 802.1x-speak as the *supplicant*) sends an EAP packet to the access point (called the *authenticator*), which immediately shuts down the port the supplicant is using to all traffic except EAP packets. The access point passes authentication messages back and forth as needed between the supplicant and the authenticating server. When the server is satisfied of the supplicant's identity, it instructs the access point to open the supplicant's port to other kinds of traffic, as predetermined by the network administrator.

To use 802.1x, all the hardware involved—supplicant, authenticator, and authenticating server—must be 802.1x-enabled. On the PC end, a Windows XP machine should have the native capability to use 802.1x; older Windows operating systems can have the Microsoft 802.1x Authentication Client software added. Be sure to configure your wireless NIC to use 802.1x as well. If the server that will be authenticating users is running Windows 2003 Server, you should be good to go; although, an older Windows server OS will need an upgrade. Finally, your wireless access points must be configured to use 802.1x; if you have doubts about the capability of an access point to use 802.1x, you can poke around all of the setup screens, or contact the manufacturer.

Wireless Networking 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 respectable 54 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, are *very* effective at blocking a wireless network signal! Other culprits include electrical fuse boxes, metal plumbing, air conditioning units, and so on.

Exact wireless data transfer speeds are listed in the next section, where I describe the specific wireless networking standards.

Wireless Networking 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*." This is simply because, like throughput speed, wireless range is greatly affected by environmental 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 see these ranges only under the most ideal circumstances. True effective range is probably about half of what you see listed.

You have a couple of ways to increase wireless network range. First, you can install multiple wireless access points or bridges to permit "roaming" between one access point's coverage area and another—an EBSS, as described earlier in this chapter. Second, you can install a signal booster that increases a single wireless access point's signal strength, thus increasing its range.

Like wireless networking speeds, I'll discuss the ranges of each type of wireless standard in the section called "Wireless Networking Standards."

Wireless Network Broadcasting Frequencies

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.

Wireless networks in the U.S. use a range of airwave bandwidth set aside by the *Federal Communications Commission (FCC)* in 1989 called the *Industrial, Scientific, and Medical*, or ISM, frequencies. FCC regulations allocate 83.5 MHz of bandwidth in the 2.4-GHz frequency band and 125 MHz of bandwidth in the 5.8-GHz band for usage by ISM equipment. In 1997, the FCC released an additional 300 MHz of bandwidth called the *Unlicensed National Information Infrastructure*, or U-NII, split into three 100-MHz frequency bands. The first band is in the frequency range of 5.15 to 5.25 GHz; the second is in the range of 5.25 to 5.35 GHz; and the third is in the range of 5.725 to 5.825 GHz.

Wireless Networking Media Access Methods

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. Let's review the differences between the two most popular media access methods, *carrier sense media access/collision detection (CSMA/CD)* and *carrier sense media access/collision avoidance (CSMA/CA)*.

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*.

Unless you're using Token Ring, collisions are a fact of networking life. So, how do network nodes deal with collisions? They either react to collisions after they happen or 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.

The problem with using CSMA/CD for wireless networking is that 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.



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

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 *acknowledgement (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.

Optionally, the 802.11 standard defines the rules for using the *Request to Send/Clear to Send (RTS/CTS)* protocol. When RTS/CTS is enabled, transmitting nodes send an RTS frame to the receiving node before sending any data, just to make certain that the coast is clear. The receiving node responds with a CTS frame, telling the sending node that it’s okay to transmit. This process is decidedly more elegant, but using RTS/CTS introduces significant overhead to the process and can impede performance. Most network techs enable this option only on heavily populated wireless network segments where the collision rate is high.

Wireless Networking Standards

Like any other networking technology, wireless technology must conform to strict industry standards defined by the IEEE organization. This section describes the different 802.11 standards and the Bluetooth wireless standard.

IEEE 802.11-Based Wireless Networking

The IEEE 802.11 wireless Ethernet standard defines 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. All the 802.11-based wireless technologies broadcast and receive in the 2.4-GHz frequency, with the exception of 802.11a, which uses the 5-GHz band.

802.11 defines two different spread-spectrum broadcasting methods: *direct-sequence spread spectrum (DSSS)* and *frequency-hopping spread spectrum (FHSS)*. 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. HomeRF wireless networks are the only type that use FHSS; all the other 802.11-based wireless networking standards use DSSS.

The original 802.11 standard has been extended to 802.11a, 802.11b, and 802.11g variations used in Wi-Fi wireless networks, and also *hybridized* (combined with another wireless communication technology) to form the *Shared Wireless Access Protocol (SWAP)* used in HomeRF networks.

Wi-Fi Wireless Networking Standards

Wireless Fidelity, or *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, and 802.11g—are Wi-Fi certified. Wi-Fi certification comes from the Wi-Fi Alliance (formerly the Wireless Ethernet Compatibility Alliance, or WECA), a nonprofit industry group made up of over 175 member companies that design and manufacture wireless networking products. Wi-Fi certification ensures compatibility between wireless networking devices made by different vendors. First-generation devices that use the older 802.11 standard are not Wi-Fi certified, so they may or may not work well with devices made by different vendors.

Wireless devices can communicate only with other wireless devices that use the same standard. The exception to this is 802.11g, which is backward-compatible with 802.11b devices (although at the lower speed of 802.11b). The following paragraphs describe the important specifications of each of the popular 802.11-based wireless networking standards.

802.11 Devices that use the original 802.11 standard are a rarity these days. You're most likely to find them in service on some brave early adopter's network. 802.11 was hampered by both slow speeds (2 Mbps maximum) and limited range (about 150 feet tops), but 802.11 employed some of the same features that are in use in the current wireless standards. 802.11 uses the 2.4-GHz broadcast range, and security is provided by the use of industry-standard WEP and WPA encryption.

802.11a Despite the *a* designation for this extension to the 802.11 standard, *802.11a* was developed *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 isn't widely adopted in the PC world.

802.11b The currently reigning king in wireless networking, *802.11b* is practically ubiquitous. The 802.11b standard supports data throughput of up to 11 Mbps—on par with

Standard	802.11	802.11a	802.11b	802.11g
Max. throughput	2 Mbps	54 Mbps	11 Mbps	54 Mbps
Max. range	150 feet	150 feet	300 feet	300 feet
Frequency	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz
Security	SSID, MAC address filtering, industry-standard WEP, WPA	SSID, MAC address filtering, industry-standard WEP, WPA	SSID, MAC address filtering, industry-standard WEP, WPA	SSID, MAC address filtering, industry-standard WEP, WPA
Compatibility	802.11	802.11a	802.11b	802.11b, 802.11g
Spread-spectrum method	DSSS	DSSS	DSSS	DSSS
Communication mode	Ad-hoc or infrastructure	Ad-hoc or infrastructure	Ad-hoc or infrastructure	Ad-hoc or infrastructure
Description	The original 802.11 wireless standard. Only seen on first-generation wireless networking devices.	Products that adhere to this standard are considered “Wi-Fi Certified.” Eight available channels. Less prone to interference than 802.11b and 802.11g.	Products that adhere to this standard are considered “Wi-Fi Certified.” Fourteen channels available in the 2.4-GHz band (only 11 of which can be used in the U.S. due to FCC regulations). Three non-overlapping channels.	Products that adhere to this standard are considered “Wi-Fi Certified.” Improved security enhancements. Fourteen channels available in the 2.4-GHz band (only 11 of which can be used in the U.S. due to FCC regulations). Three non-overlapping channels.

Table 9-1 802.11

older wired 10BaseT networks—and range of up to 300 feet under ideal conditions. 802.11b networks can be secured through the use of WEP and WPA encryption. 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.

802.11g The latest-and-greatest version of 802.11, called *802.11g*, offers data transfer speeds equivalent to 802.11a—up to 54 Mbps—and the wider 300-foot range of 802.11b. More important, 802.11g is backward-compatible with 802.11b, so the same 802.11g wireless access point can service both 802.11b and 802.11g wireless nodes. Table 9-1 compares the main characteristics of the different versions of 802.11.



NOTE 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 wireless access point) the nodes are. Effective range could be as little as three miles, but that still beats 300 feet in my book!

HomeRF

Home Radio Frequency or *HomeRF*, as the name implies, is intended for home use, not for use in large business network environments. It is easy to set up and maintain, but it does not offer much in the way of range, topping out at about 150 feet. Speed on early HomeRF devices was also nothing to write home about, clocking in at a maximum of 2 Mbps. The

Table 9-2
HomeRF

Standard	HomeRF
Max. throughput	2 Mbps, or 10 Mbps in version 2.0
Max. range	150 feet
Frequency	2.4 GHz
Security	NWID, Proprietary 56-bit encryption algorithm (128-bit in version 2.0)
Compatibility	HomeRF 2.0 is compatible with the earlier version of HomeRF.
Spread-spectrum method	FHSS
Communication mode	Ad-hoc or infrastructure
Description	HomeRF is less prone to interference, and you can set up multiple HomeRF networks in the same area.

later version 2.0 of the HomeRF standard, however, bumps the speed up to a respectable 10 Mbps, and provides full backward compatibility with the earlier HomeRF technology. Also, because HomeRF devices use the FHSS spread-spectrum broadcasting method, they are less prone to interference and somewhat more secure than Wi-Fi devices.

HomeRF wireless networks use the *SWAP* protocol, a hybrid of the *Digital Enhanced Cordless Telecommunications (DECT)* standard for voice communication and the 802.11 wireless Ethernet standard for data. HomeRF uses seven channels in the 2.4-GHz range, six of which are dedicated to voice communication, with the remaining one used for data.

Security-wise, HomeRF uses a proprietary 56-bit encryption algorithm (128-bit in version 2.0) instead of the industry-standard WEP and WPA that 802.11 uses. Also, instead of an SSID name, HomeRF uses what's called a *Network ID (NWID)*. It serves the same purpose as an SSID, but is somewhat more secure. Table 9-2 lists HomeRF's important specifications.

Infrared Wireless Networking

Wireless networking using infrared technology is largely overlooked these days, due to the explosion of interest in the newer and faster wireless standards. Still, infrared technology is built into lots of existing devices, and it provides an easy and reasonably fast way to transfer data, often without the need to purchase or install any additional hardware or software on your PCs.

The Infrared Data Association Standard

Communication through infrared devices is enabled via the *Infrared Data Association*, or *IrDA*, protocol. The IrDA protocol stack is a widely supported industry standard, and has been included in all versions of Windows since Windows 95. Apple computers also support IrDA, as do Linux PCs.

In terms of speed and range, infrared isn't very impressive. Infrared devices are capable of transferring data at up to 4 Mbps—not too shabby, but hardly stellar. The maximum distance between infrared devices is 1 meter, and connections must be in direct line-of-sight, making them susceptible to interference. An infrared link can be disrupted

Table 9-3 Infrared	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
	Description	Infrared is best suited for quick, small transfers, such as zapping business card information from one PDA to another or sending print jobs to an infrared-capable printer.

by anything that breaks the beam of light; a soda can, a co-worker passing between desks, or even bright sunlight hitting the infrared transceiver can cause interference.

Infrared is only designed to make a point-to-point connection between two devices 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. Also, Infrared devices operate at half-duplex, so 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.

In terms of security, 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 arms' 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, it'll do in a pinch. Table 9-3 lists infrared's important specifications.

Bluetooth

Upon its introduction, there was some confusion among PC techs about what Bluetooth technology actually *does*. Much of the confusion has since been cleared up. *Bluetooth* creates small wireless networks, called *personal area networks (PANs)*, connecting PCs with peripheral devices such as PDAs and printers, input devices like keyboards and mice, and consumer electronics like cell phones, home stereos, televisions, home security systems, and so on. Interestingly, Bluetooth was *not* originally designed to be a full-function networking solution, although many vendors have adopted it for this purpose.

Bluetooth is the basis for the IEEE organization's forthcoming 802.15 standard for wireless PANs. Bluetooth uses the FHSS spread-spectrum broadcasting method, switching 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. Bluetooth transfers data at rates from 723 Kbps to 1, count 'em, 1 Mbps, with a maximum range of 10 meters (about 33 feet). At least, those are the specs according to the Bluetooth standard. Some high-powered Bluetooth devices have throughput speed and range on par with 802.11b, but these are still somewhat uncommon, so I'll concentrate on the published Bluetooth specifications.

Bluetooth Operation Modes

Bluetooth's operation mode is neither truly ad-hoc nor infrastructure. Bluetooth devices interoperate in a *master/slave* scheme, in which one master device controls up to seven

active slave devices. Don't worry about having to designate these roles—Bluetooth handles that automatically.

A Bluetooth PAN is called a *piconet*—"pico" literally translating into "one trillionth," and loosely translating into "very small." Note that more than seven Bluetooth slave devices (up to 255) can participate in a piconet, but only seven of those devices can be active at one time. Inactive slave devices are referred to as *parked* devices.

Bluetooth Communication

Bluetooth devices go through four stages to find each other and start talking: device discovery, name discovery, association, and service discovery.

During *device discovery*, the Bluetooth device broadcasts its MAC address, as well as a code identifying what type of device it is (PDA, printer, and so on). Note that you have the option of setting your Bluetooth device to *non-discovery* mode, thus skipping this stage. During the *name discovery* stage, the device identifies itself by a "friendly" name, such as *iPAQ Pocket PC*. Next comes the *association* stage, also called *bonding*, *pairing*, or *joining*, depending on your device's vendor. This is the stage where the device officially joins your Bluetooth network. Some devices require that you input a PIN code, providing a level of security. Finally, during *service discovery*, the Bluetooth device tells what kind(s) of service (profiles) it provides.

From your PC's perspective, Bluetooth devices manifest as a separate network accessible through Windows Explorer, as shown in Figure 9-10.

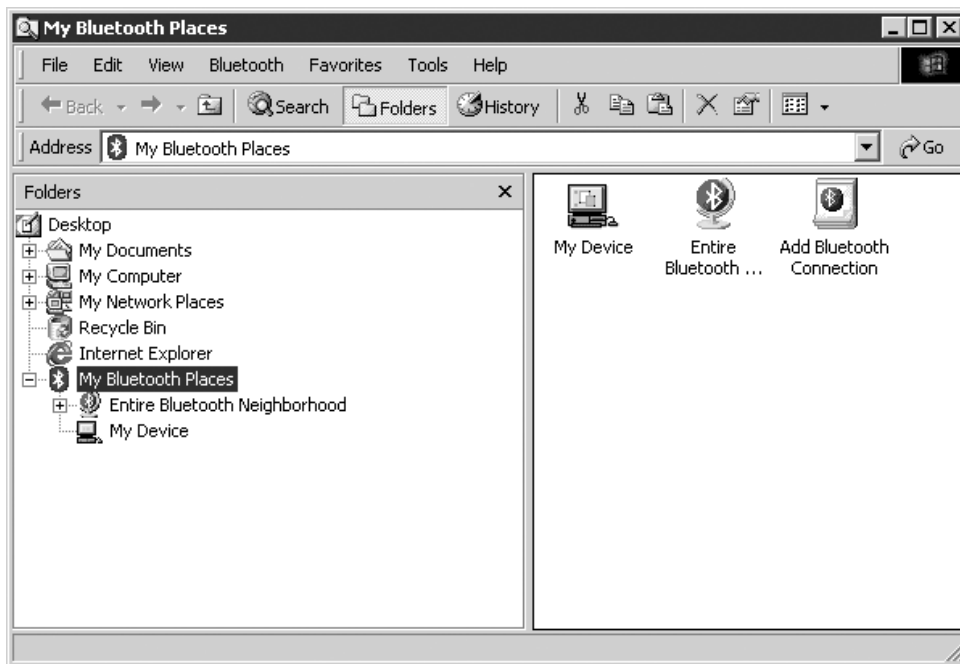


Figure 9-10 Windows Explorer showing My Bluetooth Places

Bluetooth uses two types of data transfer between master and slave nodes: *synchronous connection-oriented (SCO)* and *asynchronous connectionless (ACL)*. SCO connections guarantee that all data transmitted is received, and are better suited to things like file transfers during PDA-to-PC synchronization. ACL connections don't guarantee that all data is transferred successfully, but they're somewhat faster than SCO connections. ACL connections are suited to data transfers such as streaming media. Master nodes can support up to three SCO connections at a time with up to three slave units. ACL links are either *point-to-point* (master node to a single slave), or *broadcast* (master node to all slaves).

Bluetooth Services

The various services that are supported by Bluetooth, called *profiles*, are defined by Bluetooth specification 1.1. The 13 common Bluetooth profiles are as follows:

- **Generic Access Profile** Defines how Bluetooth units discover and establish a connection with each other.
- **Service Discovery Profile** Enables the Bluetooth device's Service Discovery User Application to query other Bluetooth devices to determine what services they provide. This profile is dependent on the Generic Access Profile.
- **Cordless Telephony Profile** Defines the Bluetooth wireless phone functionality.
- **Intercom Profile** Defines the Bluetooth wireless intercom functionality.
- **Serial Port Profile** Enables Bluetooth devices to emulate serial port communication using RS232 control signaling, the standard used on ordinary PC serial ports. This profile is dependent on the Generic Access Profile.
- **Headset Profile** Defines the Bluetooth wireless telephone and PC headset functionality.
- **Dial-up Networking Profile** Defines the Bluetooth device's capability to act as, or interact with, a modem.
- **Fax Profile** Defines the Bluetooth device's capability to act as, or interact with, a fax device.
- **LAN Access Profile** Defines how the Bluetooth device accesses a LAN and the Internet.
- **Generic Object Exchange Profile** Defines how Bluetooth devices exchange data with other devices. This profile is dependent on the Serial Port Profile.
- **Object Push Profile** Bluetooth devices use this profile to exchange small data objects, such as a PDA's Vcard, with other Bluetooth devices.
- **File Transfer Profile** Used to exchange large data objects, such as files, between Bluetooth devices. This profile is dependent on the Generic Object Exchange Profile.

- **Synchronization Profile** Used to synchronize data between Bluetooth PDAs and PCs.

Bluetooth devices have to support identical profiles to communicate; for example, your PDA and PC both have to support the Bluetooth Synchronization profile if you want them to synch up.

To use a particular Bluetooth service (profile), simply locate its icon in My Bluetooth Places and double-click it, as shown in Figure 9-11.

Bluetooth Security

Security-wise, Bluetooth offers proprietary 128-bit encryption and the capability to set per-user passwords to guard against unauthorized access to the Bluetooth network. Bluetooth also supports industry-standard *Point-to-Point Tunneling Protocol (PPTP)* and *Secure Sockets Layer (SSL)* security through browser-based remote access. Access to Bluetooth networks can be controlled through MAC address filtering, and Bluetooth devices can be set to non-discovery mode to effectively hide them from other Bluetooth devices. Table 9-4 lists Bluetooth's important specifications.

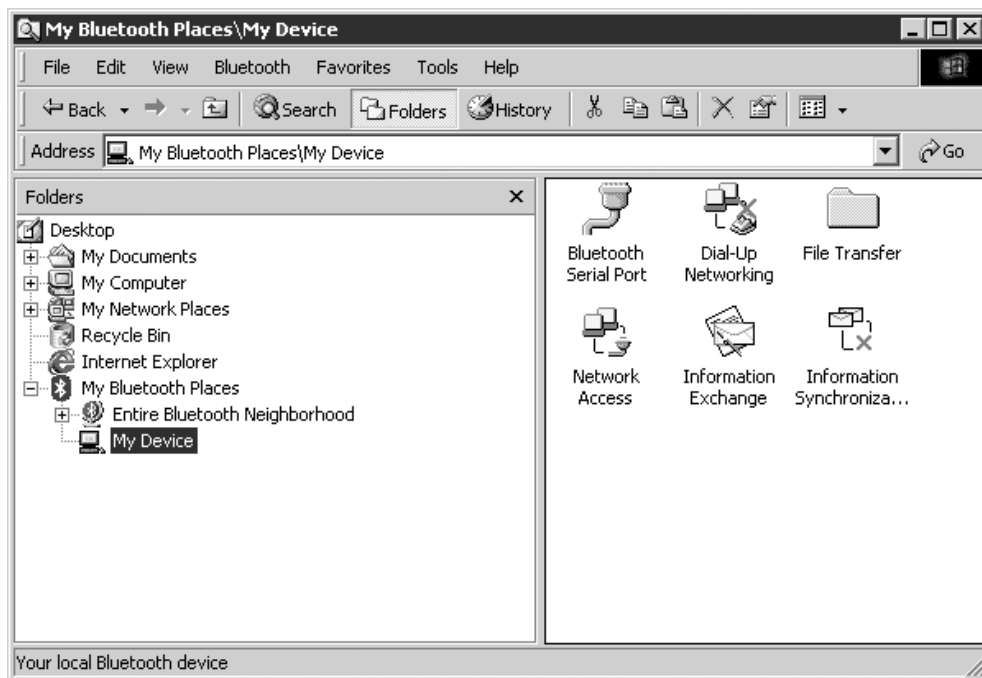


Figure 9-11 Bluetooth services listed in My Bluetooth Places

Standard	Bluetooth
Max. throughput	1 Mbps (some devices boast 2 Mbps)
Max. range	Typically 30 feet, but some high-powered Bluetooth devices have a maximum range of 300 feet
Frequency	2.45 GHz
Security	Proprietary 128-bit encryption, password-protected access, PPTP, SSL (through browser-based remote access client)
Compatibility	Bluetooth
Spread-spectrum method	FHSS
Communication mode	Master/slave: a single master device with to up to seven active slave devices. Connection links are either SCO (synchronous connection-oriented) or ACL (asynchronous connectionless).

Table 9-4 Bluetooth

Configuring Wireless Networking

As I mentioned earlier, wireless devices want to talk to each other, so communicating with an available wireless network is usually a fairly straightforward process. The trick is in configuring the wireless network so that only specific wireless nodes are able to use it, and in securing the data that’s sent through the air.

Wi-Fi and HomeRF

The mechanics of setting up a PC with a wireless network adapter aren’t very different from installing a wired NIC. All modern Wi-Fi or HomeRF wireless adapters, whether they’re internally installed PCI devices, PC Card devices, or USB, are completely PnP, so you won’t have to spend your time setting jumpers and manually configuring resources. The key is to follow the manufacturer’s instructions. Some makers insist that you install the device drivers and configuration utility software before you plug in the device. Failing to follow the vendor’s instructions will almost certainly lead to problems later.

Once you’ve got the gadget plugged in, open Windows Device Manager and check to see if any errors or conflicts are listed. If everything’s in the clear, then you’re ready to configure the adapter to use your network.

Wi-Fi and HomeRF wireless networks both 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.

Configuring a Network Adapter for Ad-hoc Mode

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

Figure 9-12
Selecting ad-hoc
mode in wireless
configuration
utility



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 9-12 shows a wireless network configuration utility with ad-hoc mode selected.

Configuring a Network Adapter for Infrastructure Mode

As with ad-hoc mode wireless networks, infrastructure mode networks require that the same SSID be configured on all nodes and access points. Figure 9-13 shows a wireless network access point configuration utility set to Infrastructure mode.

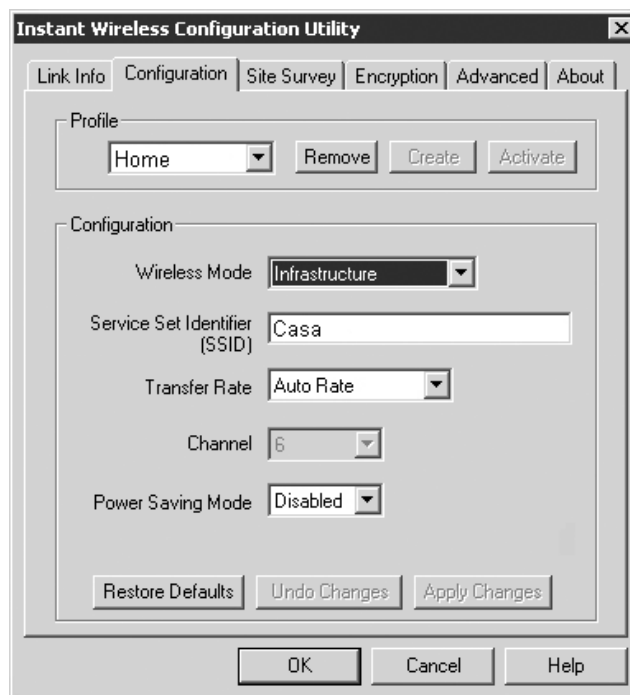
Depending on the capabilities of your access point, you can also configure DHCP options, filtering, client channels, and so on.

Access Point Configuration

Wireless access points have a browser-based setup utility. Typically, you fire up your 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 (see Figure 9-14).

Figure 9-13

Selecting infrastructure mode in wireless configuration utility



Once you've logged in, you'll have configuration screens for changing your basic setup (with SSID and so on), access point password, security, and other options. Different access points offer different configuration options. Figure 9-15 shows the initial setup screen for a popular Linksys wireless access point/router.

Configuring Access Point SSID The SSID option is usually located somewhere obvious on the configuration utility. On the Linksys model shown in Figure 9-15, it's on

Figure 9-14

Security login for Linksys wireless access point



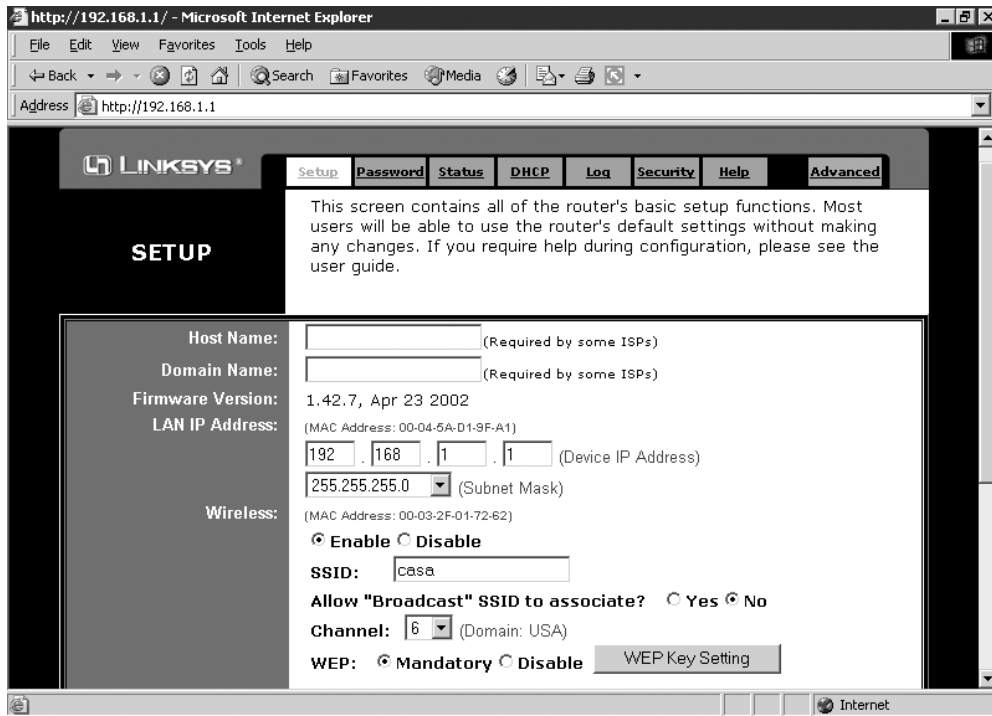


Figure 9-15 Linksys wireless access point setup screen

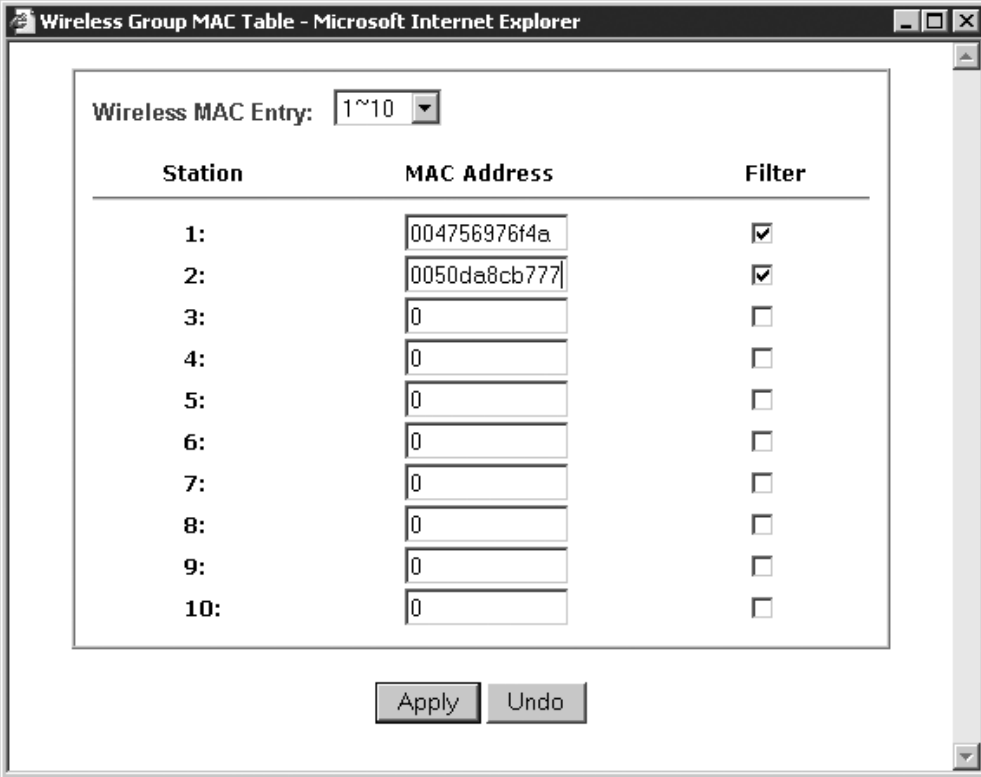
the Setup screen. Set your SSID to something unique, but not obvious. In other words, don't use "home" for your home network, or "office" for your work network, or anything else that's easy to guess. Why make a hacker's job easier?

In most circumstances, you should disable broadcasting of the SSID. This ensures that only wireless nodes specifically configured with the correct SSID can join the wireless network.



TIP 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.

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.



The screenshot shows a web browser window titled "Wireless Group MAC Table - Microsoft Internet Explorer". Inside the browser, there is a form for configuring MAC address filtering. At the top, there is a label "Wireless MAC Entry:" followed by a dropdown menu showing "1~10". Below this is a table with three columns: "Station", "MAC Address", and "Filter". The table has 10 rows, numbered 1 to 10. The first two rows have their "MAC Address" fields filled with "004756976f4a" and "0050da8cb777" respectively, and their "Filter" checkboxes are checked. The remaining rows have empty "MAC Address" fields and unchecked "Filter" checkboxes. At the bottom of the form, there are two buttons: "Apply" and "Undo".

Station	MAC Address	Filter
1:	004756976f4a	<input checked="" type="checkbox"/>
2:	0050da8cb777	<input checked="" type="checkbox"/>
3:		<input type="checkbox"/>
4:		<input type="checkbox"/>
5:		<input type="checkbox"/>
6:		<input type="checkbox"/>
7:		<input type="checkbox"/>
8:		<input type="checkbox"/>
9:		<input type="checkbox"/>
10:		<input type="checkbox"/>

Apply Undo

Figure 9-16 MAC address filtering configuration screen for a Linksys wireless access point

Figure 9-16 shows the MAC address filtering configuration screen on a Linksys wireless access point. 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 wireless access point and generate a unique security key. Then you configure all connected wireless nodes on the network with the same key information. Figure 9-17 shows the WEP key configuration dialog for a Linksys access point.

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 access point'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 will fail. Many access points have the capability to export the encryption key data onto a floppy diskette for easy importing onto a client workstation, or you

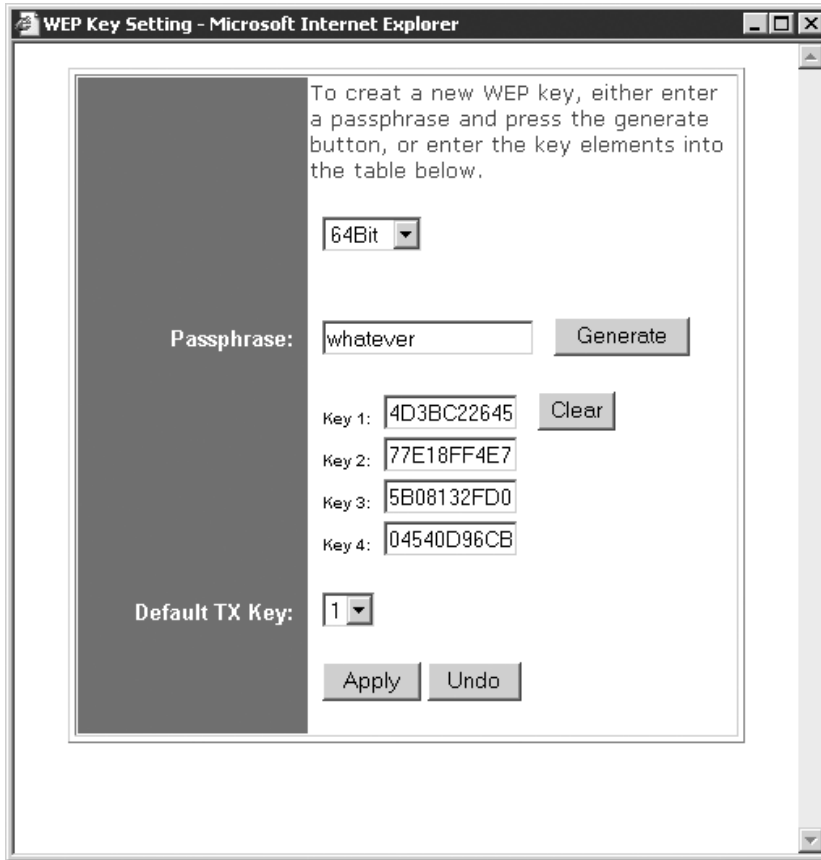


Figure 9-17 Encryption key configuration screen on Linksys wireless access point

can configure encryption manually using the vendor-supplied configuration utility, as shown in Figure 9-18.

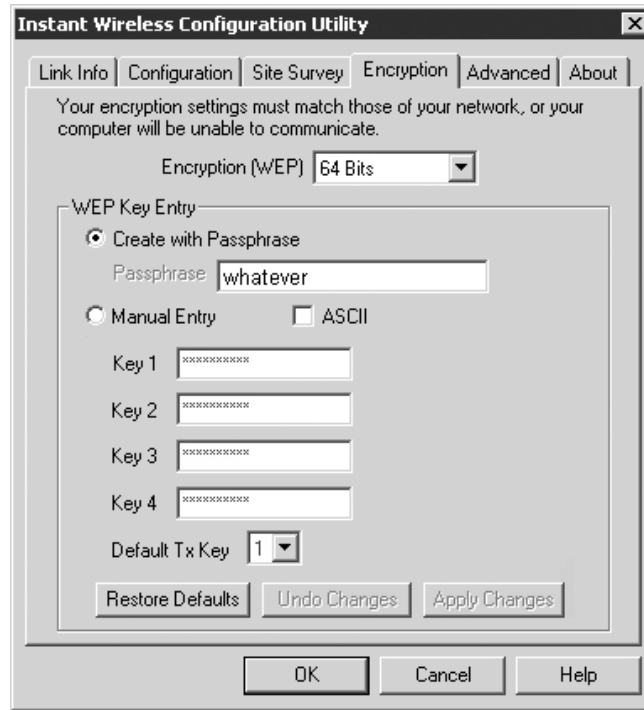
WPA encryption, if supported by your wireless equipment, is configured in much the same way. You may be required to input a valid user name and password to configure encryption using WPA.

Configuring Infrared

IrDA device support is very solid in the latest versions of Windows, so there's not much for us techs to configure. IrDA links are made between devices dynamically, without user interaction. Typically, there's nothing to configure on an infrared-equipped PC, although in some cases you may need to enable your infrared port by assigning it to a COM port in the CMOS setup program. If an infrared port is already enabled on your

Figure 9-18

Encryption screen
on client wireless
network adapter
configuration
utility



system, you can find it under *Infrared devices* in Device Manager, and check its properties to see if it's working properly. (see Figure 9-19).

As far as networking goes with infrared, your choices are somewhat limited. Infrared is designed to connect only two systems together in ad-hoc mode. This can be done simply to transfer files, or with a bit more configuration, you can configure the two PCs to use IrDA in *direct-connection* mode. You can also use a special infrared access point to enable Ethernet LAN access via IrDA.

Transferring Files via Infrared

File transfers via IrDA are as simple as can be. When two IrDA-enabled devices "see" each other, the sending (primary) device negotiates a connection to the receiving (secondary) device, and voilà. It's just "point and shoot"!

Figure 9-20 shows Windows XP's *Wireless Link* applet. Use this to configure file transfer options and the default location for received files.

You can send a file over the infrared connection in one of several ways:

- Specify a location and one or more files using the Wireless Link dialog box.
- Drag and drop files onto the Wireless Link icon.
- Using Windows Explorer, or My Computer, alternate-click a file or a selection of files, and then select Send To Infrared Recipient.
- Print to a printer configured to use an infrared port.

Figure 9-19
Properties for a
properly installed
infrared port

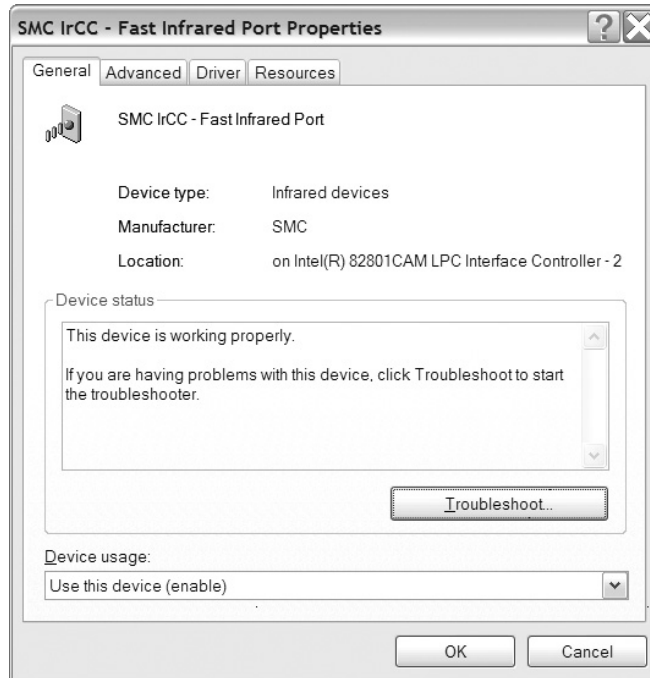


Figure 9-20
Windows XP's
Wireless Link
applet

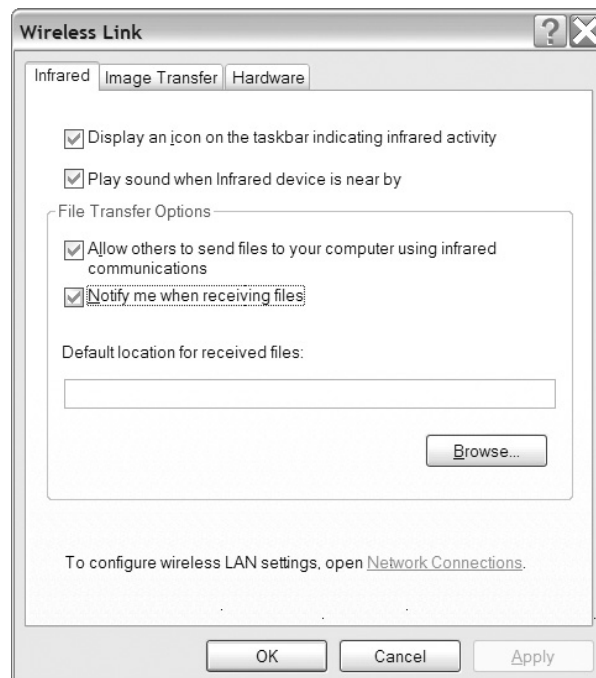


Figure 9-21
The Connection
Device screen
of the New
Connection
Wizard



Networking via Infrared

Direct network connections between two PCs using infrared are similar to using a null-modem cable to connect two PCs together via a serial port. Modern versions of Windows make this type of connection extremely easy via wizard-driven dialogs. Using the Windows XP New Connection Wizard, first select *Set up an advanced connection*, then select *Connect directly to another computer* on the next screen. Continue to follow the prompts, choosing your infrared port as the connection device (see Figure 9-21).

An infrared access point combines an infrared transceiver with an Ethernet NIC and translates the IrDA protocol into an Ethernet signal, enabling you to log on to your network and access resources. Figure 9-22 shows a laptop accessing an Ethernet LAN through an infrared access point.

Figure 9-22
Laptop using
infrared access
point



Bluetooth

Before I jump into Bluetooth configuration, I want to give you a word of warning. Although by this point, Bluetooth is a well-established standard with wide vendor support, setting up Bluetooth devices can still be a hit-or-miss affair. Many Bluetooth vendors tweak their products up so much that the devices have trouble talking to products from other vendors. If you want to save yourself a headache, be sure to read all the documentation that comes with your Bluetooth gadget, check the vendor's web site for any updated info or drivers, and allow yourself plenty of time for troubleshooting.

Installing Bluetooth Wireless Networking Hardware

Bluetooth hardware comes integrated into many newer portable electronic gadgets, like PDAs and cell phones. To add Bluetooth capabilities to a laptop or desktop PC, you often need an adapter of some sort. USB and PC Card adapters are the most common type, but you'll also see Compact Flash and PCI add-on peripheral cards, and even specialized Bluetooth adapters that plug into legacy serial and parallel ports.

Bluetooth networking is enabled through ad-hoc styled PC-to-PC (or PDA, handheld computer, or cell phone-to-PC) connections, or in an infrastructure-like mode through Bluetooth access points. Bluetooth access points are similar to 802.11-based access points, bridging wireless Bluetooth PAN segments to wired LAN segments.

Bluetooth Configuration

Follow your manufacturer's instructions to install your Bluetooth adapter. You'll probably have to install your driver and configuration utility beforehand, particularly if your Bluetooth adapter attaches via USB. Once the adapter is installed, your work is basically done. 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 9-23 shows a Compaq iPAQ

Figure 9-23
iPAQ Bluetooth
Manager software
connected to
Bluetooth access
point

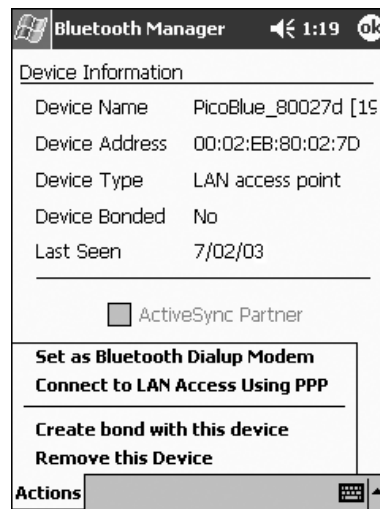
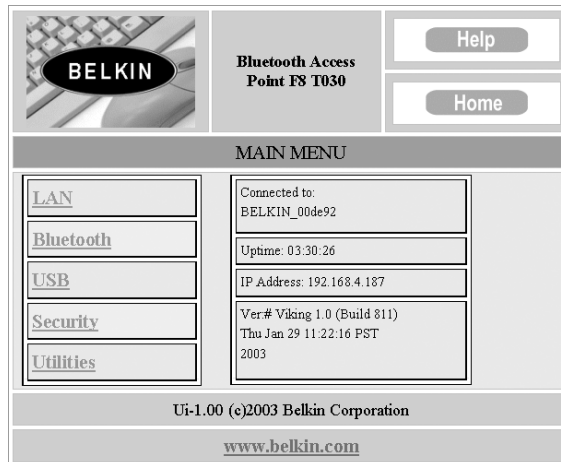


Figure 9-24
Belkin Bluetooth
access point
setup screen



handheld computer 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 9-24 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 address filtering, and other security settings; and access other utilities provided by the access point's vendor.

Troubleshooting Wireless Networks

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. Before I close out this chapter, I want to give you 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 wireless access point 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. Let's look at troubleshooting steps for Wi-Fi and HomeRF wireless networks first, and then tackle Bluetooth wireless networking.

Troubleshooting Wi-Fi and HomeRF Wireless Networks

Wi-Fi and HomeRF take different approaches to their implementation, but troubleshooting procedures are practically identical for both technologies.

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 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've got either a driver error or a resource conflict. Reinstall the device driver or manually reset the IRQ resources as needed.

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!



NOTE 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!

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 wireless access point'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 wireless access point 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

Confirm wireless connectivity using 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 9-25 shows Windows XP Professional's built-in wireless configuration utility displaying the link state and *signal strength*.



NOTE 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.

If your *link state* indicates that you're currently disconnected, you may have a problem with your wireless access point. If your signal is too weak to receive a signal, you may be

Figure 9-25
Windows XP's
wireless
configuration utility



out of range of your access point, or there may be a device causing interference. Relocate the PC or access point, or locate and move the device causing interference.

Remember, 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 WEP configuration.

Verify SSID configuration on your access point first, and then check on the affected wireless nodes. Most wireless devices allow 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 WEP configuration to make sure that all wireless nodes and access points match. Mistyping a WEP 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 of exporting WEP keys onto a floppy disk or other removable media. It's then a simple matter to import the WEP 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 wireless access point is configured for 128-bit encryption, all nodes must also use 128-bit encryption. Although it's not as secure, lowering the encryption level might solve an encryption-related connectivity issue.

Troubleshooting Bluetooth

Bluetooth technology might have outgrown its infancy, but it's still something of a toddler when it comes to industry-wide standard implementation. Like any toddler, Bluetooth falls down a lot. This section can help you get your Bluetooth wireless network back on its feet.

Hardware Troubleshooting

Check your Bluetooth hardware to make sure the device is detected and there are no driver or resource conflicts. Make sure the device is properly seated. Because practically all Bluetooth networking devices attach to the PC via USB, this should be a no-brainer,

but check it anyway. Make sure the device is compatible with your USB version. Some newer Bluetooth devices only work with USB 2.0.

Typically, a Bluetooth device comes with its own configuration utility that enables you to confirm and change system resource usage. You can also look in Device Manager to see quickly if the device driver is incorrectly installed or missing, and if any resource conflicts need to be resolved.

Software Troubleshooting

More than most networking technologies, Bluetooth suffers from “proprietary-itis.” Hence, you may find that one manufacturer’s instructions for setting up a Bluetooth device differ completely from the setup instructions for another manufacturer’s device. That’s why it’s particularly important for you to remember to RTFM—*Read The Furnished Manual*—when it comes to setting up software on Bluetooth networking devices. Check your documentation and make sure there are no special steps that you may have skipped or performed out of order.

An important consideration is whether your OS supports Bluetooth. Currently, the only desktop operating systems that offer native Bluetooth support are Windows XP (with Service Pack 1) and Apple OSX (with the Bluetooth software update installed). Support for Windows 9x/Me or 2000 is spotty and completely dependent on third-party drivers and utilities.

Connectivity Troubleshooting

Check connectivity on your Bluetooth device the same way you do with Wi-Fi and HomeRF devices. Chances are your Bluetooth device lacks a link light, so you’ll have to trust the vendor-supplied configuration utility to tell you whether you’re connected. Remember, Bluetooth range is only about 30 feet, so it’s quite easy to lose connectivity by wandering too far away from your access point or other networked Bluetooth device.

Bluetooth tends to be more resistant to interference than other wireless solutions, but don’t rule it out entirely. If you have other Bluetooth devices operating in the same area, shut them down one by one until you confirm that they aren’t causing you to lose connectivity.

Configuration Troubleshooting

Once you confirm that your Bluetooth hardware is in good working order with the correct drivers installed and within range of your other networked devices, it’s time to check your configuration.

Troubleshoot Profiles I mentioned earlier that Bluetooth devices have to support the same services, or profiles, to communicate. The LAN Access profile is the most common networking profile for Bluetooth devices, though your device may use a different name for the same profile. Make sure all devices are configured to use the same networking profile.

Troubleshoot Bluetooth Association Bluetooth devices are typically set to discover and associate with any other Bluetooth devices in range. As a security measure, you can set your Bluetooth device to *non-discovery mode* to keep it from automatically an-

nouncing its presence to other Bluetooth devices. If you're having trouble connecting to it from another device, confirm that your device isn't set to hide itself from the network.

If you receive a message telling you the discovery and association process has failed—typically something like “pairing unsuccessful”—you need to check your password or PIN.

Troubleshoot Bluetooth Power Options Although Bluetooth devices consume very little power to begin with, some devices are configured by default to cut power usage even further by dropping into a sleep mode from time to time. If your device goes to sleep, you may have to wake it up manually by using the configuration utility to switch it back on. While you're there, you may want to disable the power-saving option.

Chapter Review

Questions

1. Which wireless networking technology uses the 5-GHz frequency range?
 - A. 802.11
 - B. 802.11a
 - C. 802.11b
 - D. 802.11g
2. The original 802.11 wireless specification enables a maximum throughput speed of _____.
 - A. 2 Mbps
 - B. 11 Mbps
 - C. 54 Mbps
 - D. 4 Mbps
3. Which of the following use DSSS broadcasting? (Select all that apply.)
 - A. HomeRF
 - B. 802.11a
 - C. 802.11g
 - D. 802.11b
4. What is the maximum range of current Bluetooth devices?
 - A. 1 meter
 - B. 3 feet
 - C. 10 meters
 - D. 300 feet

5. What function does CSMA/CA provide that CSMA/CD does not?
 - A. Data packet collision detection
 - B. End-to-end data packet encryption
 - C. Data packet collision avoidance
 - D. Data packet error checking
6. Why should you configure a unique SSID for your wireless network?
 - A. A unique SSID enables backward compatibility between 802.11g and 802.11b.
 - B. A unique SSID boosts wireless network range.
 - C. A unique SSID boosts wireless network data throughput.
 - D. A unique SSID prevents access by any network device that does not have the same SSID configured.
7. Which of these consumer electronics may cause interference with 802.11b wireless networks? (Select all that apply.)
 - A. Wireless telephones
 - B. Wireless baby monitors
 - C. Bluetooth-enabled cellular telephones
 - D. Television remote controls
8. Which of the following advantages does WPA have over WEP? (Select all that apply.)
 - A. End-to-end data packet encryption
 - B. EAP user authentication
 - C. Encryption key integrity checking
 - D. 128-bit data encryption
9. What hardware enables wireless PCs to connect to resources on a wired network segment in infrastructure mode? (Select all that apply.)
 - A. An access point
 - B. A router
 - C. A hub
 - D. A bridge

10. What do you call a wireless Ethernet network in infrastructure mode with more than one access point?
- A. BSS
 - B. EBSS
 - C. PAN
 - D. Piconet

Answers

1. B. 802.11a operates in the 5-GHz frequency range.
2. A. Early 802.11 wireless networks ran at a maximum of 2 Mbps.
3. B, C, D. HomeRF uses FHSS. 802.11a, b, and g all use DSSS.
4. C. Current Bluetooth devices have a maximum range of 10 meters, or about 30 feet.
5. C. CSMA/CA uses the RTS/CTS protocol to provide data packet collision avoidance.
6. D. A unique SSID prevents wireless devices that do not have the same SSID from accessing the network.
7. A, B. Many wireless telephones and baby monitors operate in the same 2.4-GHz frequency range as 802.11b wireless networking equipment and may cause interference. Bluetooth devices operate in the same frequency, but are unlikely to cause interference because they use FHSS instead of DSSS. Television remote controls use infrared signals.
8. A, B, C. WPA upgrades WEP to provide end-to-end data packet encryption, user authentication via EAP, and encryption key integrity checking.
9. A, D. A wireless access point or bridge enables you to connect wireless PCs to a wired network segment.
10. B. A wireless network with more than one access point is called EBSS, or Extended Basic Service Set.

