Chapter 1

Removing the Tethers: Entering the Wireless World

In This Chapter

- Understanding the risks and the rewards of going wireless
- Sorting out acronyms and types of wireless networks
- Planning and installing your wireless network
- Administering and troubleshooting

Now is an exciting time for network administrators and users everywhere as we cast off the shackles of our wired world and move into the new frontier of wireless networking. This book shows you the steps to take to accomplish this as seamlessly and reliably as possible while protecting your corporate assets from unauthorized access.

In many office environments, the desk and the workstation it supports is a fixed entity. Every day you come to the office, sit at your desk, and power on your computer, ready to start the day. There is little other choice because your workstation needs a cable from it to the network in order for your applications and Internet support to work. You've been wired for years.

Perhaps, however, you've seen how wireless networking offers your business an opportunity to move beyond the expense of wires and cables into the less expensive world of air and radio waves. You've seen this already with the introduction of cell phones. Can you imagine waiting to reach someone until they returned to the office or home and their old-fashioned POTS?

What's POTS, you ask? *Plain Old Telephone Service.* Land lines. Cables. Restrictions. In the world today, if you are a teenager, you've never known that it was impossible to reach someone unless he was by his home phone, have you? You've always known about cell phones and probably have one or two yourself. Now you can move your computer into the same wireless world and free yourself from the same restrictions of needing to access a fixed, physical link. You can sit on the front porch and enjoy the sunshine with your laptop wirelessly connected to your local area network and the Internet. This wasn't possible only a few years ago.

Understanding the Risks and Rewards of Going Wireless

Going wireless has wonderful benefits, but wireless freedom comes with its share of problems as well. You need to be aware of these concerns as you move into this fascinating new world. As Oprah Winfrey once said, "I believe that one of life's greatest risks is never daring to risk." What we need to do is take calculated risks, with forethought and intelligent analysis.

What you risk

What types of risks do you face with wireless networking? Are they more or less than the risks you already face with cable-based networks? Chapter 9 provides insight on these risks, with later chapters offering solutions. In a nutshell, the risks in wireless networks are different than in cable-based networks in that physical security, like with door locks and surveillance cameras, helps protect us from the weaknesses in our local area networks. Attackers need to physically connect to the network in order to attack it. Now, I hear many of you saying that this isn't the case, and that dial-up or other remote access points offer vulnerabilities that can be abused. You are right, but this is only one aspect of gaining access to a network; and, if you disallow modems or external access, you are left with physical access as the sole entry point. This is not the case with wireless.

Many of you may recall using television antennae years ago to receive your TV stations. Some of you may still use antennae, especially in the country. This is a wireless model. Pick up an antenna, plug it into your TV, and off you go — free TV! Now you can do that with a computer. Add a wireless modem, an antenna (which may be part of the modem or integrated into the computer), and go looking for wireless signals to connect to and use. Free wireless! Okay, not really. Yes, you can do as we described; however, in many places, using someone else's network is illegal — and doing so will land you in the hoosegow.

In a wireless network, you broadcast your network to the world. "Hello? Here I am. Come and get me." Wireless networks beg to be used (or abused). And this is where they differ from land-line-based networks. Walk on by and see whether you can see a signal and use it. We point out in later chapters how people have been arrested for accessing pornography using the neighborhood wireless access points that were left unsecured and accessible to anyone. You really do not want the police knocking on your door one day asking about illegal network traffic, do you? Well, that is one of the risks of wireless.

Illegal use of your network is your biggest nightmare. This may include the scenario just mentioned or someone hacking into your network to steal commercial secrets. Neither is a good thing. Most of this risk comes from poor design and inadequate use of the security components available in a wireless network. Part III shows you how to properly secure your wireless network from intruders.

The benefits you gain

The benefits of a wireless network can be almost immeasurable. As we mention earlier, can you imagine a world without cell phones now? You almost automatically assume you can reach people any time you need to by calling their cell phone. Now imagine not being tied to your desk to accomplish your work. With the latest tablet PCs, you can roam around the office, from meeting to meeting, tablet PC in your hands, always connected, always available. In addition, you can sit in the cafeteria and grab a coffee and donut while still working on that big proposal. Or enjoy a few days of sun you would ordinarily miss, all while you work diligently away at your job.

Or imagine the usefulness of a wireless connection at the airport while you wait (and wait) for that never-on-time flight. At least now you can do some work, browse the Internet, or connect with other passengers to whittle away the interminable time waiting for flights.

The next few years will bring a revolution in networking, both personal and job-related, as wireless networking becomes *de rigueur*.

Applications of Wireless Networks

So where will you use this fancy wireless networking? Applications abound. We discuss using it in airports and in the office — major uses for any businessperson who travels. The amount of additional work that can be accomplished is immeasurable, hopefully resulting in added responsibilities and increased compensation for you. At the very least, perhaps it offers you more time with your family. What's that, you ask? How's that? Well, consider the work you need to get done each day and the deadlines you have to meet. You now have the time on the train coming home, the time spent traveling, and all that time you used to spend frustrated while waiting for a flight to get your work done so you can be with your family — instead of your work — when you finally arrive home.

The use of wireless networks doesn't end there though. If Bill Gates gets his way, we will see the wireless world in our fridges, stoves, coffee pots, and house alarms. Wait, some of those are already present.

Here are some other uses you may see:

- **Home or small office security:** Wireless cameras can be connected to your Web site, enabling you to visually check in with the office when you are away. We hope that you do this to view the premises after hours, making sure that it remains locked down and isn't broken into. Of course, there is nothing stopping you, local laws notwithstanding, from checking in on your staff while you are away to make sure they aren't partying.
- **Medicine:** Imagine a place where doctors can carry a small tablet PC around and access your records instantly from any location. While there, they might send a prescription directly to the pharmacy, bypassing the need for you to take that scrawl they call *handwriting* to your pharmacy and wait for it to be filled. The nurses could record your vital signs into a wireless device, providing instant access for your physician. Perhaps the doctor will send results to the lab, ask other doctors for advice, and generally serve you better by being fully connected.
- **Live data updates:** Data can be updated live without waiting for staff to return to the office to file paper-based reports on inspections or sales. These staff can just carry their wireless access device and input data, sending it immediately to the main computers for processing, thus speeding up a sales cycle or the collection of data that the business database requires each month.
- **Business applications:** On the business application side, companies like Microsoft, Peoplesoft, and SAP are building wireless into their products, all the better to serve the user and enable faster, more effective data use. Some real estate offices are using wireless to give brokers access to the property-listing database, which can have a dramatic effect on brokers' ability to do their job. For example, suppose a client makes an appointment to look at certain house types, such as bungalows, and the broker meets her with a list of properties fitting that description. Now, suppose that after looking at what's available, the client realizes that she actually wants a two-story home. The broker can immediately dial in a different search rather than rescheduling with the client. Presto, instant sales.

The use of wireless networks will skyrocket in the next few years, we predict, with more and more vendors applying the concept of liberating us from the desk or from manual methods of applying new data to our systems.

Sorting Out the Nets: Do I Need a WPAN, WLAN, or WMAN?

Acronyms are the bane of all professionals. Whether it's a nurse or doctor asking for an MRI or an accountant discussing ROI, you need to know the lingo if you want to be part of the talk. It's the same with wireless networks.

There are a number of different types of networks whose classifications are based primarily on the distances they reach. You see in Table 1-1 how they relate to the wired world and to each other.

Table 1-1 Different Types of Networks

Network Type	*Wired*	*Wireless*
LAN	IEEE 802.3 (Ethernet)	IEEE 802.11X
PAN	IEEE 1394 USB	IEEE 802.15.1
		IEEE 802.15.3
		IEEE 802.15.4
MAN	Broadband (DSL, cable)	IEEE 802.16

The IEEE (Institute of Electrical and Electronics Engineers) provides standards for everyone to follow. These include standards for wired and wireless networking. The numbers are assigned by the IEEE and quickly become well known to industry users. The 802 series dictates how each format must work. You can obtain lots of interesting information about these standards and their use from various Web sites. One of these is `www.dailywireless.org/index.php`. This site includes regular updates on what's happening in the wireless world.

Impress your friends by mentioning the 802.11 standard that your wireless network uses. It will be either a, b, or g. 802.11b is currently the most popular, but 802.11g is catching on fast.

Let's get personal: WPAN

The *Wireless Personal Area Network* (*WPAN*) consists of close-range wireless activities such as Bluetooth and FireWire. Wireless in this range is based on the IEEE 802.15 standard. Transmission in this network consists of a low range of around 30 feet, or 10 meters. It's right up there in your personal space, sort of like being in a crowd and getting jostled all the time. It uses low power consumption and is an ad hoc network. If you are in range and another device is present, you can reach out and touch it.

This spectrum is designed for interpersonal connections, such as connecting one PDA to another, or connecting a wireless keyboard, mouse, or printer to your computer. It is useful and helps free you from all the cables typically needed to perform these tasks. Data transfer occurs at around 1 Mbps in the Bluetooth protocol.

Many of you already indulge in the Wireless Personal Area Network world with your infrared-equipped PDA that you use to beam information to other PDA users. Others of you wander around airports with a Bluetooth-equipped headset on your cell phone. That we like. It's got to beat having that darn wire hanging around your neck although we are not sure you realize how many people initially think you are talking to them as you chat away.

Other neat uses of this spectrum include connecting your PDA to your workstation or laptop to synchronize data or adding a Bluetooth-enabled modem like those available from Zoom Telephonics. Why a Bluetooth modem? Well, if you travel, you can connect in your hotel with a dial-up line. Although many hotels are moving to wireless connectivity, many have not gotten there yet. So using a Bluetooth modem provides you a degree of that wireless connectivity as you roam around your hotel room or even step out onto the balcony — all while remaining connected.

Another use of this spectrum regards connecting with other laptop users to share files easily and quickly without the need for network cards or cables. Although you can also do this in the WLAN technology, using infrared allows you to quickly share files with another user, with little fuss and bother.

One quick note of clarification: Personal Area Networks (PAN) actually refer to using a near field electric field to send data across various devices using the body as a medium. The term was really meant to be used as it is in Wireless Personal Area Networks. Nonetheless, it is an accepted term now and is used interchangeably. If you want to read an article describing this original use, visit `www.wirelessdevnet.com/channels/bluetooth/features/pans.html`, a wireless developer's Web site.

The holy grail of wireless networking: WLAN

WLAN is the holy grail of wireless networking for most of the business world. Using the IEEE 802.11 standard, it is the main topic for most of this book. *Wireless Local Area Networking* (*WLAN*) gets you connected to the office with your laptop or tablet PC, allowing you to roam around at work while remaining connected. It won't be long before you're able to tell the boss you are working while standing around the water cooler and chatting with your friends. Look boss, I'm downloading that latest spreadsheet and discussing it with Harry while slaking my thirst.

This is where *Wi-Fi* — a term sometimes used interchangeably for the IEEE 802.11 standard — originates. This wireless connectivity expands beyond the area of our desks and moves us to further distances. Distances of up to 500 feet are possible with no interference, and even farther distances can be easily achieved using repeaters and additional access points. We guide you through understanding the protocols, the risks, implementing security, and more throughout this book.

You are probably most interested in WLAN, and so we focus on it in this book. A Wireless Local Area Network is analogous to the wired local area network you use each day at the office or even in your home. It is merely a connectivity of devices, allowing sharing of resources. Where WLANs are useful, though, is in freeing up your installation from cable worries and knocking holes in walls and floors to run those connecting cables.

This can be especially beneficial for small and medium businesses (SMBs) because you may not own the rights to your building and so may need to contract with the building maintenance people to get things done. This can be time-consuming and expensive. A WLAN, properly configured and secured, offers unprecedented access with none of those concerns. You can use a WLAN to extend your network beyond the walls and floors of your building, perhaps into an adjoining conference room or lunchroom, providing staff with access while they grab a quick bite to eat.

There are numerous considerations, of course, and security is paramount. Properly configured, however, WLAN can set you free and let you explore areas of connectivity you may never have considered.

Where the rubber hits the road: WMAN

The *Wireless Metropolitan Area Networks,* or *WMAN,* are also sometimes referred to as *Wi-Max* and *WirelessMan.* This is where the rubber hits the road almost literally as the distances reached are far greater than with the prior standards. Based on the IEEE 802.16 standard, the WMAN provides for large distances and high speeds of access. This standard focuses on the efficient use of bandwidth in the 10–66 GHz range, although an amendment to it, 802.16a, allows for access in the 2–11 GHz range.

WMAN offers wireless access to buildings through the use of external antennae accessing central base stations. WLAN is great for one building or a few floors, but if you are a large organization with geographically separate buildings, you might need the extended distance that WMAN offers. An advantage of this

protocol is the allowance for quality of service (QoS) to further enhance its use in business. This allows a reseller to guarantee a certain level of service. Of course, you might just buy space on such a network from any of the vendors putting WMANs in place. For example, in Portland, Oregon, VeriLAN Inc. (www.VeriLAN.com) began offering such a service in 2004.

One newer standard includes 802.20, providing connectivity speeds of up to 1 Mbps for vehicular traffic traveling at speeds of up to 250 kilometers (155 miles) per hour. This is cool: Not only can you illegally speed down the highway, but you can interface with a wireless network while doing it. Of course, I suspect the police are more interested in this particular band.

Using Wireless Networks

Using a wireless network takes a number of components and some fairly critical thinking up front before allowing anyone to connect. We discuss these components in the next few sections.

Accessing networks

You need tools to access a wireless network. You also need to be aware of the distances and transmission speeds you want to use in order to choose the correct technology. To quickly summarize, there are a number of competing wireless standards to consider. Table 1-2 covers the more popular ones.

Table 1-2 Popular Wireless Standards

Standard	*What It Means*
802.11a	54 Mbps speed in the 5 GHz band.
802.11b	11 Mbps transmission in the 2.4 GHz band.
802.11g	54 Mbps; remains backward-compatible with 802.11b.
802.15	Personal Area Network standard. Bluetooth is the typical name.

Many other standards exist. You can find a list of them all in Appendix B, but the ones covered in Table 1-2 are the current popular ones. To use them, your network card must support that standard, along with, of course, your wireless access point. After you add a wireless network card to your machine or PDA, you are off to the races and can enjoy mobility while remaining connected to your network.

Depending upon which wireless standard you use, your roaming can include your office floor or perhaps even the entire building, including part of your building's parking lot. We talk more about the pitfalls of that in later chapters.

Extending the network

Now that you are connected, it may occur to you that you need that degree of access in other locations. It's catching, this freedom. To accomplish this, you need to extend the network or extend your ability to reach the current network.

One easy method to extend your range is to improve the antenna you use. Typically, your network card uses a small antenna either right in the card or, with a Centrino or AirPort chipset, somewhere within the computer. These work great for the typical distances involved in your wireless network but fall short of anything substantial. Adding a high-gain antenna to your computer or PDA significantly improves your ability to reach the network from far greater distances.

The alternate method is to extend your network using repeaters and additional access points. This is where planning is effective to ensure that you understand your needs before you start and then implement the technologies necessary to manage those needs.

Connecting buildings

Perhaps you want to ensure that all the buildings your business uses are connected on one seamless network using wireless frequencies. There are a couple of methods you can use for this, including some really advanced methods if your buildings are a great distance apart.

Connecting networks based in separate buildings leads to major benefits, such as users accessing necessary data residing in central resources crossing large open spaces (office complexes and university campuses, for example).

Two common methods for bridging this gap include point-to-point and multipoint LAN bridges. Using these techniques, your wireless network can expand from one room, to one building, to multiple buildings, to across a city. This is a complex implementation, however, and is not likely something the target SMB this book is designed for will use. You can see in Figure 1-1 how each bridge works.

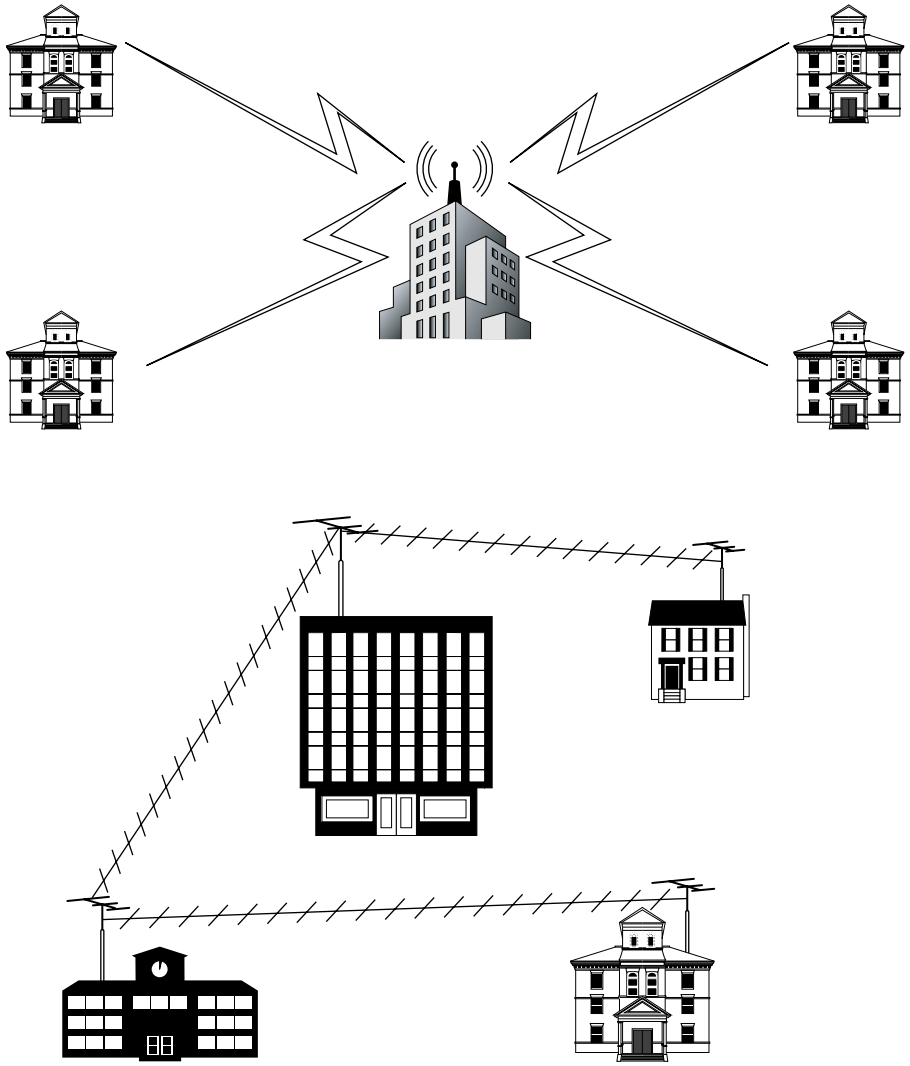

Figure 1-1: Point-to-point (top) and multipoint (bottom) network bridges.

Going mobile

As the song indicates, we're on the road again. We travel a lot, and getting access to our e-mail and office is essential. Most of the time, we gain access by using a local phone call to our network service provider and then using that access to cross over to our office and get connected.

For security purposes, Barry uses an encrypted tunnel to access his home office. After he's connected, he can easily access all his machines and obtain whatever files he needs. This way, everything he does while connected is protected from prying eyes.

One thing that is changing is the reduced need to use a land-line-based service provider like AT&T Global Services. As hotels, airports, and coffee shops add wireless access hotspots, it gets easier and easier to connect. As the familiar advertising phrase goes, "Can you hear me now?" The answer, increasingly, is *yes.*

There are numerous utilities, like Boingo, that offer wireless access around the world in coffee shops, restaurants, and hotels. Getting connected while mobile is often simple. Boingo offers free software that finds wireless network hotspots and makes the connection for you. You pay a fee to Boingo to access any of their *hotspots* around the world.

Getting mail on the road

One obvious need for mobile travelers is to retrieve their e-mail. Where would we be without it? This too is becoming simple. Years ago, Barry's business associate would carry alligator clips and a long telephone cable with stripped wires at one end. This was so he could connect to telephone systems in foreign countries where data access was limited or not even considered. Although this has changed and almost every hotel telephone system allows and accommodates telephone modem access today, wireless is also beginning to intrude and become the norm. That certainly is easier than ripping wires out of a wall to get connected!

After you have access to the Internet using a wireless access point, obtaining your e-mail is trivial. It is still ideal to use a Virtual Private Network (VPN) so that your e-mail and passwords are not traversing the network in clear text but traveling through an encrypted tunnel instead. This is even truer in the wireless world because those networks are vulnerable to anyone on the same network sniffing the traffic and seeing what you are up to at any given moment.

One other method involves using a PDA, such as the new Treo 600 or a Blackberry, to obtain e-mail. As data travels over the cell phone's GPRS network, it is slightly less vulnerable than a Wi-Fi connection. It's also very convenient: You merely turn on your device, connect to the local cell provider, and presto! You have mail!

Turning a Notion into a Network

Okay, so you are captured by the possibilities and want your own wireless network. As a small business owner, you cannot afford to hire a third party to install and maintain this network, so you need to understand how to accomplish such a thing by yourself.

It is one thing to desire something and quite another to obtain it in a useful, secure manner. You must take certain steps to protect your business and your wireless investment; *planning,* that awful bugaboo for many of you, is absolutely necessary.

Planning your wireless network

In Chapter 2, you find out all about creating a plan for your new wireless network. We cannot stress this enough: *Do not skip that chapter.* Implementing a wireless solution may be as simple as adding an access point onto your network and letting your staff connect.

But there are pitfalls even with this simple approach. Where will you place the access point? Far too many organizations place them inside the network, which is the absolute wrong place for a wireless connection to be. Your network needs to be protected from any potential wireless attacks; therefore, the access needs to be on the outside of your firewall, forcing users to authenticate their identities to gain access to the internal network.

Where will the wireless access be needed? It makes little sense to place it in the main office if attenuation from the building and its occupants results in the signal not reaching the intended audience. Finally, you need to configure the necessary degree of security to ensure your access is used only by authorized users.

Installing your wireless network

Depending on the size of your wireless network, installation may be as simple as placing an access point on a table or wall and plugging it into a power supply. However, you may also install a more complex system, using repeaters, bridges, and external antennae. These need careful placement and subsequent installation to ensure they meet all your needs and allow for flawless connectivity.

After you plan the installation, it is necessary to begin installing the components. When you do so, you want to follow some structure in order to make the implementation smooth. First, review your plan and ensure that it is

complete. Next, unpack the equipment you plan to install and ensure that all the parts are there and that nothing looks broken. Now, connect all the pieces. For an access point, this usually means adding the external antennae that came with the device. However, perhaps you are installing high-gain external antennae and they are to be located on a rooftop. Which comes first, the chicken or the egg? Install the antennae and cabling and then connect it to an access point.

Continue installing access points or repeaters as per your plan until you finish. Make sure that you install wireless network cards in a few workstations or laptops so that you can test accessibility after you configure and secure the network. After all the hardware is in place, you need to configure the network.

Configuring a wireless network

After installing all the access points, you must configure the network. Configuring the network sets up the software and all its components so that a wireless signal is transmitted clearly and is accessible to your network cards.

Configuration includes a number of activities. These include setting up the basic parameters that allow your access point and network cards to communicate, thus starting your progress into the wireless world. Other items include those shown in Table 1-3.

Table 1-3 Configuring Your Wireless Network

Parameter	*Description*
Set your IP address.	You need to set the IP address in your network card so it can recognize the access point.
Test connection with the `ping` command.	Use this command to ensure that you can reach the access point.
Enter the Administration menu.	To set the device parameters, you need the main menu of the device. You enter the vendor-supplied default account and password to accomplish this action.
Set the options.	You need to set the time, disable remote access, determine whether you need DHCP, and ensure that the IP addressing is appropriate for your needs.
Update to the latest firmware.	This is important. Make sure that you follow directions and visit the vendor Web site to get the latest firmware. This ensures that your device is up-to-date and all vendor patches are implemented.

Configuration allows your devices to connect to each other and, if appropriate, with your Local Area Network. After this is established, you need to ensure that your connections are secure.

Staying secure in the wireless world

Securing your network is the most important part of your wireless journey. Don't skip past it in your excitement at being connected to a wireless network. There are many risks to your network, your users, and your data in this new wild, wild west. Risks involve strange names such as war driving and war flying. You didn't know you were getting into a special arcane world of warfare did you?

War driving and *war flying* are exercises in which someone drives or even flies around, equipped with special software, a laptop with a wireless network card, and an external antenna. Using this equipment, they will find your wireless network and probe it to see whether you are using security. You offer an open door when you've skipped those steps and no security is in place.

Other risks include identity theft and data loss. Using that unsecured wireless access point, intruders steal information like credit card numbers, addresses, and even pass codes if you keep these on a computer somewhere on your network. They may even take the special fried chicken recipe you are working on to combat KFC's if you don't secure it well.

Fortunately, there are things you can do to prevent security breaches, or at least to make it exceedingly difficult to break into your network. It starts with turning on encryption and using techniques like Media Access Control (MAC) filtering and even more advanced authentication techniques like Extended Authentication Protocols (EAP) to ensure that only authorized users connect to your network. Finally, you can really improve access security by using techniques called Virtual Private Networking (VPN). We guide you through all these using step-by-step procedures and detailed discussions in later chapters.

Administering and maintaining a wireless network

After your network is set up securely, you'll want to use it all the time. Why not? That is one reason for implementing a wireless network, to set yourself free to wander with your machine, remaining connected as you walk to the conference room or sit in the park.

All this comes at a price, however, because nothing is permanent, and it all requires some degree of administration and support. Depending on the size of your client base, using a security technique such as MAC filtering can be very time-consuming. You need to keep lists of all the MAC addresses used and the corresponding individual network cards in order to track their use and change them when users' network cards fail or laptops change hands and no longer require access.

In addition, troubleshooting any sort of network requires constant surveillance and analysis. In the wireless world, there are issues such as changing *Fresnel zones,* where objects block your signal. Other issues needing constant maintenance might include free space loss, in which changing weather might cut off a fringe signal. And, of course, you need to be aware of typical and abnormal traffic loads. Users suddenly downloading copious quantities of files (they wouldn't be downloading music, would they?) can cause the network to slow to a crawl. Someone needs to monitor and ensure that steps are taken to limit such slowdowns to keep everyone happy.

Throughout this book, we provide a number of tools and several techniques for managing your wireless network after it is up and running. You must keep those happy faces that all your users received when they first signed on to the wireless world and found that freedom.

Convergence of Wireless Technologies — What Will the Future Hold?

Where will we all be in the years to come? No one really knows. We can take educated guesses, though. We are already seeing a huge increase in the use of wireless technologies. Where just a few years ago we would check into the hotel, locate the telephone, and plug in our modem, we now look for a wireless connection first. Barry uses his Treo 600 to send and retrieve e-mail, call home, and search the Web.

This is one area where wireless convergence will skyrocket in the future. We anticipate that all major hotels will be completely wireless in the next three to five years. According to a survey of Internet trends by Ipsos-Insight, it seems that wireless Internet usage grew 145 percent in 2003 with 79 million unique visitors. The study claims that roughly 40 percent of people with land-line Internet access have tried wireless networks. We can expect to see even these figures surpassed in the coming years.

At the airport, your connection will be announced over the wireless network, informing you of delays or arrivals as they occur. No longer will you hang around wondering what is going on when your plane is late, hoping some harried airline staffers will stop to actually consider their customers for a change. (I know — after all the travel Barry does, he still gets upset at the often-cavalier attitude he encounters from airlines.)

Wireless connectivity will continue to grow and become ever more intrusive in our lives. Look for wireless security systems for home and business to grow, coupled with instant messaging and Web page photos to provide greater security and faster notice of break-ins. This can ease the burden of getting up at 2 a.m. to respond to an alarm at the office. Perhaps in the next few years, you'll merely log on and check out the remote cameras to verify whether a break-in occurred before getting dressed and venturing forth. A friend of Barry's installed a Web-based camera at his cottage recently. He can now log on to the Internet, access his Web site, and check for snowfall or intrusions online. That's awesome; his cottage is a two-hour drive away.

Other interesting thoughts include an expansion of the wireless spectrum to include more bandwidth. This will be necessary as wireless access expands, perhaps matching the widely misinterpreted Moore's Law, suggesting that computing power doubles every 18 months. Voice over IP (VoIP) is already beginning to show up on wireless networks, and this will also grow, especially when it is seen as a less-expensive alternative to land-based phones and can offer instant access to those already logged on for other reasons.

Finally, the emerging 802.16 Wireless Metropolitan Network standard will likely expand across the continent as communities and governments extend the reach to more and more businesses, with smaller wireless networks paying to connect to this service in an effort to expand their reach.